acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

17 June, 2016

Developer Report

Generated by Acunetix WVS Reporter (v9.5 Build 20150119)

Scan of http://192.168.155.13:80/b2b2c/

Scan details

Scan information	
Start time	2016/6/17 11:53:57
Finish time	2016/6/17 02:36:21
Scan time	2 hours, 42 minutes
Profile	OneSolution

Server information	
Responsive	True
Server banner	Apache/2.4.4 (Win32) OpenSSL/0.9.8y PHP/5.4.16
Server OS	Windows
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	**39**
High	12
Medium	25
Low	0
Informational	2

Knowledge base

List of client scripts

These files contain Javascript code referenced from the website.

- /b2b2c/js/cssmenu/script.js
- /b2b2c/js/jquery-1.11.1.min.js
- /b2b2c/js/general.js
- /b2b2c/js/modernizr.custom.38310.js
- /b2b2c/js/jquery.placeholder.js
- /b2b2c/js/jquery.marquee.js
- /b2b2c/js/owl.carousel.min.js
- /b2b2c/js/jquery-ui-1.11.4/jquery-ui.min.js
- /b2b2c/js/jquery-ui-1.11.4/external/jquery/jquery.js
- /b2b2c/js/jquery-ui-1.11.4/jquery-ui.js
- /b2b2c/js/noUiSlider.8.3.0/nouislider.min.js
- /b2b2c/js/jquery-ias.min.js
- /b2b2c/js/select2-4.0.2/js/select2.min.js
- /b2b2c/js/stacktable/stacktable.min.js
- /b2b2c/js/elevatezoom/jquery-1.8.3.min.js
- /b2b2c/js/elevatezoom/jquery.elevatezoom.js

List of files with inputs

These files have at least one input (GET or POST).

- /b2b2c - 1 inputs
- /b2b2c/member_login_post.php - 2 inputs
- /b2b2c/page_content.php - 1 inputs
- /b2b2c/product_catalog.php - 7 inputs
- /b2b2c/currency_change.php - 1 inputs
- /b2b2c/language_change.php - 1 inputs
- /b2b2c/js/jquery-ui-1.11.4 - 1 inputs
- /b2b2c/js/verification_code/captcha/vCodeImage.php - 1 inputs
- /b2b2c/product_detail.php - 1 inputs
- /b2b2c/contact_us_post.php - 1 inputs
- /b2b2c/registration_post.php - 1 inputs
- /b2b2c/"page_content.php - 1 inputs
- /b2b2c/search_results.php - 1 inputs

List of external hosts

These hosts were linked from this website but they were not scanned because they are not listed in the list of hosts allowed. (Configuration-> Scan Settings ->Scanning Options-> List of hosts allowed).

- fonts.googleapis.com
- www.youtube.com
- www.hkosl.com
- www.facebook.com
- graph.qq.com
- api.weibo.com
- b2b2c.hkosl.com
- twitter.com
- www.shareasale.com
- github.com
- www.maxcdn.com
- files-stackablejs.netdna-ssl.com
- static.shareasale.com
- s3.amazonaws.com
- platform.twitter.com
- ajax.googleapis.com
- www.elevateweb.co.uk
- www.acunetix-referrer.com

Alerts summary

Cross site scripting

Classification	
CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-79

Affected items	Variation
/b2b2c/product_detail.php	2

Cross site scripting (verified)

Classification	
CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-79

Affected items	Variation
/b2b2c/product_catalog.php	4

SQL injection

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-89

Affected items	Variation
/b2b2c/page_content.php	1
/b2b2c/product_catalog.php	4
/b2b2c/search_results.php	1

Application error message

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/b2b2c/	2
/b2b2c/page_content.php	4
/b2b2c/product_catalog.php	8
/b2b2c/search_results.php	2

HTML form without CSRF protection

Classification	
CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-352

Affected items	Variation
/b2b2c	1
/b2b2c/contact_us.php	1
/b2b2c/js/jquery-ui-1.11.4	1
/b2b2c/member_login.php	1
/b2b2c/product_catalog.php (5b8d0c962e8a023b0ac9f56f54517359)	1
/b2b2c/registration.php	1

User credentials are sent in clear text

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-310

Affected items	Variation
/b2b2c	1
/b2b2c/member_login.php	1
/b2b2c/registration.php	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/b2b2c/registration.php	2

Alert details

Cross site scripting

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

/b2b2c/product_detail.php

Details

URL encoded GET input cid was set to 8_908111'():;939271
The input is reflected inside <script> tag between single quotes.

Request headers

```
GET /b2b2c/product_detail.php?cid=8_908111'():;939271&id=27&pcid=0 HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/product_detail.php

Details

URL encoded GET input id was set to 27_957009'():;989781
The input is reflected inside <script> tag between single quotes.

Request headers

```
GET /b2b2c/product_detail.php?cid=33&id=27_957009'():;989781&pcid=1 HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
```

```
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

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

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

Affected items

/b2b2c/product_catalog.php

Details

URL encoded GET input id was set to 10'"()&%<acx><ScRiPt >prompt(940843)</ScRiPt>

Request headers

```
GET
/b2b2c/product_catalog.php?id=10'%22()%26%25<acx><ScRiPt%20>prompt(940843)</ScRiPt>&solo
=1 HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/product_catalog.php

Details

URL encoded GET input p was set to 2'"()&%<acx><ScRiPt >prompt(945747)</ScRiPt>

Request headers

```
GET
/b2b2c/product_catalog.php?id=0&limit=12&p=2'%22()%26%25<acx><ScRiPt%20>prompt(945747)</
ScRiPt>&sort=1 HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
```

```
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/product_catalog.php

Details

URL encoded GET input sort was set to 1'"()&%<acx><ScRiPt >prompt(996740)</ScRiPt>

Request headers

```
GET
/b2b2c/product_catalog.php?id=0&limit=12&p=2&sort=1'%22()%26%25<acx><ScRiPt%20>prompt(99
6740)</ScRiPt> HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/product_catalog.php

Details

URL encoded GET input sort was set to 1'"()&%<acx><ScRiPt >prompt(914873)</ScRiPt>

Request headers

```
GET
/b2b2c/product_catalog.php?id=0&limit=12&sort=1'%22()%26%25<acx><ScRiPt%20>prompt(914873
)</ScRiPt> HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

SQL injection

Severity	**High**
Type	Validation
Reported by module	Scripting (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

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

Affected items

/b2b2c/page_content.php

Details

URL encoded GET input id was set to 1'"
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/page_content.php?id=1'%22 HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/product_catalog.php

Details

URL encoded GET input id was set to 1'"
Error message found: You have an error in your SQL syntax

Request headers

```
POST /b2b2c/product_catalog.php?id=1'%22 HTTP/1.1
Content-Length: 138
Content-Type: multipart/form-data; boundary=-----AcunetixBoundary_HYCQHORMMF
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*

-------AcunetixBoundary_HYCQHORMMF
Content-Disposition: form-data; name="product_keywords"

1
-------AcunetixBoundary_HYCQHORMMF--
```

/b2b2c/product_catalog.php

Details

URL encoded GET input id was set to 1'"
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/product_catalog.php?id=1'%22 HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/product_catalog.php

Details

POST (multipart) input product_keywords was set to 1'"
Error message found: You have an error in your SQL syntax

Request headers

```
POST /b2b2c/product_catalog.php?id=-1 HTTP/1.1
Content-Length: 140
Content-Type: multipart/form-data; boundary=-----AcunetixBoundary_FKWFTAWISA
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*

-------AcunetixBoundary_FKWFTAWISA
Content-Disposition: form-data; name="product_keywords"

1'"
-------AcunetixBoundary_FKWFTAWISA--
```

/b2b2c/product_catalog.php

Details

URL encoded GET input sort was set to @@ABmG6
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/product_catalog.php?id=0&limit=12&sort=%40%40ABmG6 HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/search_results.php

Details

URL encoded GET input keywords was set to \
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/search_results.php?keywords=%5c HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

Application error message

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

Description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

PHP Runtime Configuration
How to: Display Safe Error Messages

Affected items

/b2b2c/

Details

Cookie input php-console-server was set to acu7353%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca7353
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/ HTTP/1.1
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22;
php-console-server=acu7353%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca7353
Referer: http://192.168.155.13:80/b2b2c/
Host: 192.168.155.13
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: */*
```

/b2b2c/

Details

HTTP Header input Referer was set to acu3766%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca3766
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/ HTTP/1.1
Referer: acu3766%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca3766
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*
```

/b2b2c/page_content.php

Details

URL encoded GET input id was set to acu4264%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca4264
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/page_content.php?id=acu4264%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca4264
HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/page_content.php

Details

URL encoded GET input id was set to
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/page_content.php?id= HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/page_content.php

Details

Cookie input php-console-server was set to acu8012%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca8012
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/page_content.php HTTP/1.1
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22;
php-console-server=acu8012%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca8012
Referer: http://192.168.155.13:80/b2b2c/
Host: 192.168.155.13
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: */*
```

/b2b2c/page_content.php

Details

HTTP Header input Referer was set to acu7188%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca7188
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/page_content.php HTTP/1.1
Referer: acu7188%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca7188
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*
```

/b2b2c/product_catalog.php

Details

URL encoded GET input id was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'ð??c
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/product_catalog.php?id=12345'"\'\");|]*{%0d%0a<%00>%bf%27'?’c HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
```

```
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/product_catalog.php

Details

URL encoded GET input id was set to acu6844%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca6844
Error message found: You have an error in your SQL syntax

Request headers

```
POST /b2b2c/product_catalog.php?id=acu6844%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca6844
HTTP/1.1
Content-Length: 138
Content-Type: multipart/form-data; boundary=-----AcunetixBoundary_ACMTSCFGOY
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*

-------AcunetixBoundary_ACMTSCFGOY
Content-Disposition: form-data; name="product_keywords"

1
-------AcunetixBoundary_ACMTSCFGOY--
```

/b2b2c/product_catalog.php

Details

URL encoded GET input id was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'ð??c
Error message found: You have an error in your SQL syntax

Request headers

```
POST /b2b2c/product_catalog.php?id=12345'"\'\");|]*{%0d%0a<%00>%bf%27'?’c HTTP/1.1
Content-Length: 138
Content-Type: multipart/form-data; boundary=-----AcunetixBoundary_GJWPEYOTVL
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*

-------AcunetixBoundary_GJWPEYOTVL
Content-Disposition: form-data; name="product_keywords"

1
-------AcunetixBoundary_GJWPEYOTVL--
```

/b2b2c/product_catalog.php

Details

URL encoded GET input p was set to 2
Error message found: Internal Server Error

Request headers

```
GET /b2b2c/product_catalog.php?id=0&limit=12&p[]=2&sort=1 HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/product_catalog.php

Details

Cookie input php-console-server was set to acu9560%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca9560
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/product_catalog.php?id=0 HTTP/1.1
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22;
php-console-server=acu9560%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca9560
Referer: http://192.168.155.13:80/b2b2c/
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: */*
Host: 192.168.155.13
```

/b2b2c/product_catalog.php

Details

POST (multipart) input product_keywords was set to
acu5164%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca5164
Error message found: You have an error in your SQL syntax

Request headers

```
POST /b2b2c/product_catalog.php?id=-1 HTTP/1.1
Content-Length: 187
Content-Type: multipart/form-data; boundary=-----AcunetixBoundary_EAILMQNFUI
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*

-------AcunetixBoundary_EAILMQNFUI
Content-Disposition: form-data; name="product_keywords"

acu5164%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca5164
-------AcunetixBoundary_EAILMQNFUI--
```

/b2b2c/product_catalog.php

Details

POST (multipart) input product_keywords was set to
Error message found: You have an error in your SQL syntax

Request headers

```
POST /b2b2c/product_catalog.php?id=-1 HTTP/1.1
Content-Length: 137
Content-Type: multipart/form-data; boundary=-----AcunetixBoundary_QVJYLNEUSK
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*

-------AcunetixBoundary_QVJYLNEUSK
Content-Disposition: form-data; name="product_keywords"
```

```
-------AcunetixBoundary_QVJYLNEUSK--
```

/b2b2c/product_catalog.php

Details

HTTP Header input Referer was set to acu6190%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca6190
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/product_catalog.php?id=0 HTTP/1.1
Referer: acu6190%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca6190
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*
Host: 192.168.155.13
```

/b2b2c/search_results.php

Details

URL encoded GET input keywords was set to
Error message found: You have an error in your SQL syntax

Request headers

```
GET /b2b2c/search_results.php?keywords= HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/search_results.php

Details

URL encoded GET input keywords was set to acu9549%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca9549
Error message found: You have an error in your SQL syntax

Request headers

```
GET
/b2b2c/search_results.php?keywords=acu9549%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca9549
HTTP/1.1
Referer: http://192.168.155.13:80/b2b2c/
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

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

/b2b2c

Details

Form name: login-form
Form action: http://192.168.155.13/b2b2c/member_login_post.php
Form method: POST

Form inputs:

- tel [Text]
- password [Password]

Request headers

```
GET /b2b2c/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/contact_us.php

Details

Form name: contact_us
Form action: http://192.168.155.13/b2b2c/contact_us_post.php
Form method: POST

Form inputs:

- user_title [Radio]
- user_firstname [Text]
- user_lastname [Text]
- tel [Text]
- email [Text]
- content [TextArea]
- verification [Text]

Request headers

```
GET /b2b2c/contact_us.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.155.13/b2b2c/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/js/jquery-ui-1.11.4

Details

Form name: <empty>
Form action: http://192.168.155.13/b2b2c/js/jquery-ui-1.11.4/
Form method: GET

Form inputs:

- radio [Radio]

Request headers

```
GET /b2b2c/js/jquery-ui-1.11.4/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.155.13/b2b2c/js/jquery-ui-1.11.4/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/member_login.php

Details

Form name: login-form
Form action: http://192.168.155.13/b2b2c/member_login_post.php
Form method: POST

Form inputs:

- tel [Text]
- password [Password]

Request headers

```
GET /b2b2c/member_login.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.155.13/b2b2c/member_login_post.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/product_catalog.php (5b8d0c962e8a023b0ac9f56f54517359)

Details

Form name: <empty>
Form action: http://192.168.155.13/b2b2c/product_catalog.php?id=-1
Form method: POST

Form inputs:

- product_keywords [Text]

Request headers

```
GET /b2b2c/product_catalog.php?category_name=ALL_PRODUCTS&id=0 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.155.13/b2b2c/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/registration.php

Details

Form name: registration
Form action: http://192.168.155.13/b2b2c/registration_post.php
Form method: POST

Form inputs:

- qq_id [Hidden]
- sina_id [Hidden]
- gender [Radio]
- first_name [Text]
- last_name [Text]
- yyyy [Hidden]
- mm [Hidden]
- dd [Hidden]
- email [Text]
- tel [Text]
- country_code [Select]
- identity_id [Text]
- identity_type [Hidden][... (line truncated)

Request headers

```
GET /b2b2c/registration.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.155.13/b2b2c/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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	Configuration
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

/b2b2c

Details

Form name: login-form
Form action: http://192.168.155.13/b2b2c/member_login_post.php
Form method: POST

Form inputs:

- tel [Text]
- password [Password]

Request headers

```
GET /b2b2c/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/member_login.php

Details

Form name: login-form
Form action: http://192.168.155.13/b2b2c/member_login_post.php
Form method: POST

Form inputs:

- tel [Text]
- password [Password]

Request headers

```
GET /b2b2c/member_login.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.155.13/b2b2c/member_login_post.php
Acunetix-Aspect: enabled
```

```
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/registration.php

Details

Form name: registration
Form action: http://192.168.155.13/b2b2c/registration_post.php
Form method: POST

Form inputs:

- qq_id [Hidden]
- sina_id [Hidden]
- gender [Radio]
- first_name [Text]
- last_name [Text]
- yyyy [Hidden]
- mm [Hidden]
- dd [Hidden]
- email [Text]
- tel [Text]
- country_code [Select]
- identity_id [Text]
- identity_type [Hidden][... (line truncated)

Request headers

```
GET /b2b2c/registration.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.155.13/b2b2c/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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 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

/b2b2c/registration.php

Details

Password type input named confirm_password from form named registration with action registration_post.php has autocomplete enabled.

Request headers

```
GET /b2b2c/registration.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.155.13/b2b2c/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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: */*
```

/b2b2c/registration.php

Details

Password type input named password from form named registration with action registration_post.php has autocomplete enabled.

Request headers

```
GET /b2b2c/registration.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.155.13/b2b2c/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=kusndh2lepjvr0bvl61l52sk22; php-console-server=5
Host: 192.168.155.13
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 207 URLs. Found 6 vulnerable.

URL: http://192.168.155.13/b2b2c/

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
Host	HTTP Header

URL: http://192.168.155.13/b2b2c/member_login_post.php

No vulnerabilities has been identified for this URL

4 input(s) found for this URL

Inputs

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

Input scheme 2	
Input name	Input type
password	POST (multipart)
tel	POST (multipart)

URL: http://192.168.155.13/b2b2c/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/style.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/owl.theme.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/owl.carousel.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/font-awesome.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/ie.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/gird.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/form.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/reset.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/slider.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/navegation.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/flexslider.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/css/fonts

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/contact_us.php

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/registration.php

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/currency_change.php

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
currency_code	URL encoded GET

URL: http://192.168.155.13/b2b2c/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/whatshot/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/slideshow/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/flag/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/thumb/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/brand/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/brand/logo/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/brand/logo/original/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/brand/banner/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/brand/banner/original/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/Thumbs.db

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/banner/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/refund/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/large_img/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/member_img/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/gift_images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/color_images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/profile_images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/product_images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/product_images/large/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/product_images/thumb/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/images/comment_product/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/cssmenu/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/cssmenu/styles.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/cssmenu/script.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery-1.11.1.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/general.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/modernizr.custom.38310.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.placeholder.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.marquee.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/owl.carousel.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/html5shiv.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery-ui-1.11.4/

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
radio	URL encoded GET

URL: http://192.168.155.13/b2b2c/js/jquery-ui-1.11.4/jquery-ui.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery-ui-1.11.4/jquery-ui.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery-ui-1.11.4/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery-ui-1.11.4/external/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery-ui-1.11.4/external/jquery/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery-ui-1.11.4/external/jquery/jquery.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery-ui-1.11.4/jquery-ui.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/noUiSlider.8.3.0/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/noUiSlider.8.3.0/nouislider.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/noUiSlider.8.3.0/nouislider.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/noUiSlider.8.3.0/nouislider.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/noUiSlider.8.3.0/nouislider.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/noUiSlider.8.3.0/nouislider.pips.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/noUiSlider.8.3.0/nouislider.tooltips.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery-ias.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/images

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/selectivizr-and-extra-selectors.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/verification_code/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/verification_code/captcha/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/verification_code/captcha/font/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/css/select2.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/css/select2.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/select2.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/ja.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/it.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/is.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/ko.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/mk.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/lv.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/lt.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/he.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/gl.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/fr.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/hi.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/id.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/hu.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/hr.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/sv.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/sr.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/sk.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/th.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/vi.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/uk.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/tr.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/nl.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/nb.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/ms.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/pl.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/ru.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/ro.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/pt.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/fi.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/et.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/da.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/eu.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/en.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/es.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/de.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/ca.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/az.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/bg.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/cs.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/ar.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/fa.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/pt-BR.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/zh-CN.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/zh-TW.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/i18n/sr-Cyrl.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/select2.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/select2.full.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/select2-4.0.2/js/select2.full.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/tipso/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/tipso/tipso.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/tipso/tipso.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/!general.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/stacktable/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/stacktable/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/stacktable/css/style.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/stacktable/stacktable.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/stacktable/stacktable.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/elevatezoom/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/elevatezoom/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/elevatezoom/images/small/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/elevatezoom/images/thumb/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/elevatezoom/images/large/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/elevatezoom/demo.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/elevatezoom/jquery-1.8.3.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/elevatezoom/jquery.elevatezoom.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/elevatezoom/jquery.elevateZoom-3.0.8.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/lib/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/lib/jquery-1.9.0.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/lib/jquery-1.10.1.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/lib/jquery.mousewheel-3.0.6.pack.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/source/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/source/helpers/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/source/helpers/jquery.fancybox-media.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/source/helpers/jquery.fancybox-thumbs.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/source/helpers/jquery.fancybox-thumbs.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/source/helpers/jquery.fancybox-buttons.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/source/helpers/jquery.fancybox-buttons.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/source/jquery.fancybox.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/source/jquery.fancybox.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/fancybox_2.0/source/jquery.fancybox.pack.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/rateit-1.0.23/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/rateit-1.0.23/rateit.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/rateit-1.0.23/jquery.rateit.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/rateit-1.0.23/jquery.rateit.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/rateit-1.0.23/jquery.rateit.min.js.map

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/countdown-2.1.0/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/countdown-2.1.0/jquery.countdown.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/countdown-2.1.0/jquery.countdown.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/multiple_select/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/multiple_select/multiple-select.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/multiple_select/jquery.multiple.select.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.easing.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/general_20141119.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/images/icons-png/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/images/icons-svg/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile-1.4.5.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile-1.4.5.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/table_reflow.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile-1.4.5.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile-1.4.5.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile-1.4.5.min.map

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.external-png-1.4.5.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.theme-1.4.5.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.icons-1.4.5.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.icons-1.4.5.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.theme-1.4.5.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.structure-1.4.5.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.inline-png-1.4.5.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.inline-svg-1.4.5.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.structure-1.4.5.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.inline-svg-1.4.5.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.inline-png-1.4.5.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5/jquery.mobile.external-png-1.4.5.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mousewheel.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.smoothscroll.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/html5shiv-printshiv.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.flexslider-min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/js/jquery.mobile-1.4.5.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/fonts/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/"member_login.php"

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/"page_content.php

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://192.168.155.13/b2b2c/member_login.php
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/faq.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://192.168.155.13/b2b2c/search_results.php
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
keywords	URL encoded GET

URL: http://192.168.155.13/b2b2c/checkout.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL