



Acunetix Website Audit

11 May, 2024

Developer Report

Scan of http://testhtml5.vulnweb.com:80/

Scan details

Scan information	
Start time	5/11/2024 10:35:20 PM
Finish time	5/11/2024 10:49:51 PM
Scan time	14 minutes, 31 seconds
Profile	Default
Server information	
Responsive	True
Server banner	nginx/1.19.0
Server OS	Unknown

Threat level





 acunetix threat level

Level 3: High

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	32
 High	21 <div></div>
 Medium	4 <div></div>
 Low	6 <div></div>
 Informational	1 <div></div>

Knowledge base

Amazon S3 Buckets

List of Amazon S3 Buckets used by this web application:

- bxss.s3.amazonaws.com

List of file extensions

File extensions can provide information on what technologies are being used on this website.

List of file extensions detected:

- css => 1 file(s)
- js => 5 file(s)
- html => 7 file(s)

List of client scripts

These files contain Javascript code referenced from the website.

- /static/app/app.js
- /static/app/libs/sessvars.js
- /static/app/post.js
- /static/app/controllers/controllers.js
- /static/app/services/itemsService.js

List of files with inputs

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

- / - 2 inputs
- /login - 1 inputs
- /ajax/popular - 1 inputs
- /ajax/latest - 1 inputs
- /forgotpw - 1 inputs
- /contact - 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).

- www.acunetix.com
- fonts.googleapis.com
- www.facebook.com
- www.twitter.com
- netdna.bootstrapcdn.com
- code.jquery.com
- ajax.googleapis.com
- bxss.s3.amazonaws.com
- www.python.org
- nginx.org
- flask.pocoo.org
- couchdb.apache.org
- angularjs.org
- twitter.github.io

Alerts summary

AngularJS client-side template injection

Classification	
CVSS	Base Score: 4.4
	<ul style="list-style-type: none"> - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 5.3
	<ul style="list-style-type: none"> - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None
CWE	CWE-79
Affected items	
/contact	Variation 8

Cross site scripting (verified)

Classification		
CVSS	Base Score: 6.4	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: Partial- Availability Impact: None	
CVSS3	Base Score: 5.3	
	<ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: None- Integrity Impact: Low- Availability Impact: None	
CWE	CWE-79	
Affected items		Variation
/		1

DOM-based cross site scripting

Classification		
CVSS	Base Score: 4.4	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Medium- Authentication: None- Confidentiality Impact: None- Integrity Impact: Partial- Availability Impact: None	
CVSS3	Base Score: 5.3	
	<ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: None- Integrity Impact: Low- Availability Impact: None	
CWE	CWE-79	
Affected items		Variation
/		12

🚨 HTML form without CSRF protection

Classification		
CVSS	Base Score: 2.6	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: High- Authentication: None- Confidentiality Impact: None- Integrity Impact: Partial- Availability Impact: None	
CVSS3	Base Score: 4.3	
	<ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: Required- Scope: Unchanged- Confidentiality Impact: None- Integrity Impact: Low- Availability Impact: None	
CWE	CWE-352	
Affected items		Variation
/		2

🚨 User credentials are sent in clear text

Classification		
CVSS	Base Score: 5.0	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None	
CVSS3	Base Score: 9.1	
	<ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: High- Availability Impact: None	
CWE	CWE-310	
Affected items		Variation
/		1

Vulnerable Javascript library

Classification		
CVSS	Base Score: 6.4	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: Partial- Availability Impact: None	
CVSS3	Base Score: 6.5	
	<ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: Low- Integrity Impact: Low- Availability Impact: None	
CWE	CWE-16	
Affected items		Variation
/static/app/libs/sessvars.js		1

Clickjacking: X-Frame-Options header missing

Classification		
CVSS	Base Score: 6.8	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Medium- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: Partial- Availability Impact: Partial	
CWE	CWE-693	
Affected items		Variation
Web Server		1

Cookie without HttpOnly flag set

Classification		
CVSS	Base Score: 0.0	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None	
CWE	CWE-16	
Affected items		Variation
/		1

❗ Insecure response with wildcard '*' in Access-Control-Allow-Origin

Classification		
CVSS	Base Score: 0.0	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None	
CWE	CWE-16	
Affected items		Variation
/		1

❗ Login page password-guessing attack

Classification		
CVSS	Base Score: 5.0	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None	
CVSS3	Base Score: 5.3	
	<ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: Low	
CWE	CWE-307	
Affected items		Variation
/login		1

❗ OPTIONS method is enabled

Classification		
CVSS	Base Score: 5.0	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None	
CVSS3	Base Score: 7.5	
	<ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None	
CWE	CWE-200	
Affected items		Variation
Web Server		1

Possible sensitive directories

Classification		
CVSS	Base Score: 5.0	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: Partial- Integrity Impact: None- Availability Impact: None	
CVSS3	Base Score: 7.5	
	<ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None	
CWE	CWE-200	
Affected items		Variation
/static/app/services		1

Password type input with auto-complete enabled

Classification		
CVSS	Base Score: 0.0	
	<ul style="list-style-type: none">- Access Vector: Network- Access Complexity: Low- Authentication: None- Confidentiality Impact: None- Integrity Impact: None- Availability Impact: None	
CVSS3	Base Score: 7.5	
	<ul style="list-style-type: none">- Attack Vector: Network- Attack Complexity: Low- Privileges Required: None- User Interaction: None- Scope: Unchanged- Confidentiality Impact: High- Integrity Impact: None- Availability Impact: None	
CWE	CWE-200	
Affected items		Variation
/		1

Alert details

AngularJS client-side template injection

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

Description

This web application is vulnerable to AngularJS client-side template injection vulnerability. AngularJS client-side template injection vulnerabilities occur when user-input is dynamically embedded on a page where AngularJS client-side templating is used. By using curly braces it's possible to inject AngularJS expressions in the AngularJS client-side template that is being used by the application. These expressions will be evaluated on the client-side by AngularJS and when combined with a sandbox escape they allow an attacker to execute arbitrary JavaScript code.

Impact

An attacker can inject AngularJS expressions that will be evaluated on the client-side. Normally AngularJS expressions are not very dangerous, but when combined with a sandbox escape they allow an attacker to execute arbitrary JavaScript code.

Recommendation

It should not be possible for an attacker to inject AngularJS expressions by using curly braces. The application needs to either treat curly braces in user input as highly dangerous or avoid server-side reflection of user input entirely.

References

- [AngularJS security features and best practices](#)
- [XSS without HTML: Client-Side Template Injection with AngularJS](#)

Affected items

/contact

Details

URL encoded POST input firstName was set to sbqpviwsekvb3{{1==1}}0kiwb. The input was reflected inside an AngularJS template.

Request headers

POST /contact HTTP/1.1
Content-Length: 128
Content-Type: application/x-www-form-urlencoded
Referer: http://testhtml5.vulnweb.com:80/
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*

address=3137%20Laguna%20Street&firstName=sbqpviwsekvb3%7b%7b1%3d%3d1%7d%7d0kiwb&lastName=laehbjkn&message=20&subject=suggestions

/contact

Details

URL encoded POST input firstName was set to sbqpviwsrjnyw{{1==1}}kql9r. The input was reflected inside an AngularJS template.

Request headers

POST /contact HTTP/1.1
Content-Length: 124
Content-Type: application/x-www-form-urlencoded
Referer: http://testhtml5.vulnweb.com:80/
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*

address=3137%20Laguna%20Street&firstName=sbqpviwsrjnyw%7b%7b1%3d%3d1%7d%7dkql9r&lastName=laehbjkn&message=20&subject=product

/contact

Details

URL encoded POST input firstName was set to sbqpviwsi9jdv{{1==1}}arjva. The input was reflected inside an AngularJS template.

Request headers

POST /contact HTTP/1.1
Content-Length: 119
Content-Type: application/x-www-form-urlencoded
Referer: http://testhtml5.vulnweb.com:80/
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*

address=3137%20Laguna%20Street&firstName=sbqpviwsi9jdv%7b%7b1%3d%3d1%7d%7darjva&lastName=laehbjkn&message=20&subject=na

/contact

Details

URL encoded POST input firstName was set to sbqpviwsvzv9h{{1==1}}q4si7. The input was reflected inside an AngularJS template.

Request headers

POST /contact HTTP/1.1
Content-Length: 124
Content-Type: application/x-www-form-urlencoded
Referer: http://testhtml5.vulnweb.com:80/
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*

address=3137%20Laguna%20Street&firstName=sbqpviwsvzv9h%7b%7b1%3d%3d1%7d%7dq4si7&lastName=laehbjkn&message=20&subject=service

/contact

Details

URL encoded POST input lastName was set to laehbjknu3s4j{{1==1}}3pmlly. The input was reflected inside an AngularJS template.

Request headers

POST /contact HTTP/1.1
Content-Length: 128
Content-Type: application/x-www-form-urlencoded
Referer: http://testhtml5.vulnweb.com:80/
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*

address=3137%20Laguna%20Street&firstName=hvirhmq&lastName=laehbjknu3s4j%7b%7b1%3d%3d1%7d%7d3pmlly&message=20&subject=suggestions

/contact
Details
URL encoded POST input lastName was set to laehbjkn8igyk{{1==1}}wvepo. The input was reflected inside an AngularJS template.
Request headers
POST /contact HTTP/1.1 Content-Length: 124 Content-Type: application/x-www-form-urlencoded Referer: http://testhtml5.vulnweb.com:80/ Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*
address=3137%20Laguna%20Street&firstName=hvirhmq&lastName=laehbjkn8igyk%7b%7b1%3d%3d1%7d%7dwvepo&message=20&subject=product

/contact
Details
URL encoded POST input lastName was set to laehbjknkp31v{{1==1}}ob2jo. The input was reflected inside an AngularJS template.
Request headers
POST /contact HTTP/1.1 Content-Length: 124 Content-Type: application/x-www-form-urlencoded Referer: http://testhtml5.vulnweb.com:80/ Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*
address=3137%20Laguna%20Street&firstName=hvirhmq&lastName=laehbjknkp31v%7b%7b1%3d%3d1%7d%7dob2jo&message=20&subject=service

/contact
Details
URL encoded POST input lastName was set to laehbjknit4pg{{1==1}}nwnza. The input was reflected inside an AngularJS template.
Request headers
POST /contact HTTP/1.1 Content-Length: 119 Content-Type: application/x-www-form-urlencoded Referer: http://testhtml5.vulnweb.com:80/ Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*
address=3137%20Laguna%20Street&firstName=hvirhmq&lastName=laehbjknit4pg%7b%7b1%3d%3d1%7d%7dnwnza&message=20&subject=na

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

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

Affected items

/
Details
Cookie input username was set to 1<script>tWtm(9540)</script> The input is reflected inside a text element.
Request headers
GET / HTTP/1.1 Cookie: username=1<script>tWtm(9540)</script> Referer: http://testhtml5.vulnweb.com:80/ Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*

DOM-based cross site scripting

Severity	High
Type	Validation
Reported by module	DeepScan

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.

While a traditional cross-site scripting vulnerability occurs on the server-side code, document object model based cross-site scripting is a type of vulnerability which affects the script code in the client's 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

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

Affected items

/

Details

Source: Referrer Header

Referrer: http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,""><xsstag>()refdxss")

Execution Sink: set HTML code (innerHTML/outerHTML/...)

HTML code set:

```
<div class="navbar navbar-fixed-top">
  <div class="navbar-inner">
    <div class="container-fluid">
      <button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
      </button>
      <a class="brand" href="https://www.acunetix.com/">&nbsp; ... Stack Trace:
```

- removeChild@[native code]
- remove@http://code.jquery.com/jquery-1.9.1.min.js:4:26918
- c@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:19:182
- removeBackdrop@http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js:7:2690
- http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js:7:2592
- i@http://code.jquery.com/jquery-1.9.1.min.js:4:2289
- dispatch@http://code.jquery.com/jquery-1.9.1.min.js:3:28590
- handle@http://code.jquery.com/jquery-1.9.1.min.js:3:25295

/

Details

Source: Referrer Header

Referrer: http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,""><xsstag>()refdxss")

Execution Sink: set HTML code (innerHTML/outerHTML/...)

HTML code set:

```
<div class="navbar navbar-fixed-top">
  <div class="navbar-inner">
    <div class="container-fluid">
      <button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
      </button>
      <a class="brand" href="https://www.acunetix.com/">&nbsp; ... Stack Trace:
```

- removeChild@[native code]
- remove@http://code.jquery.com/jquery-1.9.1.min.js:4:26918
- c@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:19:182
- ln@http://code.jquery.com/jquery-1.9.1.min.js:5:5489
- un@http://code.jquery.com/jquery-1.9.1.min.js:5:5096
- rn@http://code.jquery.com/jquery-1.9.1.min.js:5:1646
- show@http://code.jquery.com/jquery-1.9.1.min.js:5:2136
- http://code.jquery.com/jquery-1.9.1.min.js:5:23165
- http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js:7:1345
- i@http://code.jquery.com/jquery-1.9.1.min.js:4:2289
- dispatch@http://code.jquery.com/jquery-1.9.1.min.js:3:28590
- handle@http://code.jquery.com/jquery-1.9.1.min.js:3:25295

/

Details

Source: location.hash

location.hash: `#!/popular/page/javascript:domxssExecutionSink(1,"\"><xsstag>()hashxss")`

Execution Sink: set HTML code (innerHTML/outerHTML/...)

HTML code set: `javascript:domxssExecutionSink(1,"\"><xsstag>()hashxss")</xsstag>` ... Stack Trace:

- `http://code.jquery.com/jquery-1.9.1.min.js:4:27657`
- `access@http://code.jquery.com/jquery-1.9.1.min.js:3:6852`
- `html@http://code.jquery.com/jquery-1.9.1.min.js:4:27282`
- `c@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:19:182`
- `https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:142:173`
- `$digest@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:86:339`
- `https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:61:148`
- `https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:31:85`
- `forEach@[native code]`
- `n@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:6:199`
- `h@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:31:69`
- `dispatch@http://code.jquery.com/jquery-1.9.1.min.js:3:28590`
- `handle@http://code.jquery.com/jquery-1.9.1.min.js:3:25295`

/

Details

Source: location.hash

location.hash: `#!/latest/page/javascript:domxssExecutionSink(1,"\"><xsstag>()hashxss")`

Execution Sink: set HTML code (innerHTML/outerHTML/...)

HTML code set: `javascript:domxssExecutionSink(1,"\"><xsstag>()hashxss")</xsstag>` ... Stack Trace:

- `http://code.jquery.com/jquery-1.9.1.min.js:4:27657`
- `access@http://code.jquery.com/jquery-1.9.1.min.js:3:6852`
- `html@http://code.jquery.com/jquery-1.9.1.min.js:4:27282`
- `c@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:19:182`
- `https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:142:173`
- `$digest@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:86:339`
- `https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:61:148`
- `https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:31:85`
- `forEach@[native code]`
- `n@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:6:199`
- `h@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:31:69`
- `dispatch@http://code.jquery.com/jquery-1.9.1.min.js:3:28590`
- `handle@http://code.jquery.com/jquery-1.9.1.min.js:3:25295`

/

Details

Source: Referrer Header

Referrer: http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,"\"><xsstag>()refdxss")

Execution Sink: set HTML code (innerHTML/outerHTML/...)

HTML code set:

```
<div class="navbar navbar-fixed-top">
  <div class="navbar-inner">
    <div class="container-fluid">
      <button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
      </button>
      <a class="brand" href="https://www.acunetix.com/">&nbsp; ... Stack Trace:
```

- appendChild@[native code]
- http://code.jquery.com/jquery-1.9.1.min.js:4:26272
- domManip@http://code.jquery.com/jquery-1.9.1.min.js:4:28538
- append@http://code.jquery.com/jquery-1.9.1.min.js:4:26170
- http://code.jquery.com/jquery-1.9.1.min.js:4:30403
- ln@http://code.jquery.com/jquery-1.9.1.min.js:5:5441
- un@http://code.jquery.com/jquery-1.9.1.min.js:5:5096
- rn@http://code.jquery.com/jquery-1.9.1.min.js:5:1646
- show@http://code.jquery.com/jquery-1.9.1.min.js:5:2136
- http://code.jquery.com/jquery-1.9.1.min.js:5:23165
- http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js:7:1345
- i@http://code.jquery.com/jquery-1.9.1.min.js:4:2289
- dispatch@http://code.jquery.com/jquery-1.9.1.min.js:3:28590
- handle@http://code.jquery.com/jquery-1.9.1.min.js:3:25295

/

Details

Source: Referrer Header

Referrer: http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,"\"><xsstag>()refdxss")

Execution Sink: document.write

HTML code written: <iframe name="ads_ads_frame"

src="http://ads.bxss.me/ad_server.php?zone_id=234&ad_client=723898932&u_h=768&u_w=1366&pn=&ref=http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,"\"><xsstag>()refdxss")&url=http://testhtml5 ... (line truncated)

Stack Trace:

- http://bxss.s3.amazonaws.com/ad.js:30:19
- global code@http://bxss.s3.amazonaws.com/ad.js:32:2

/

Details

Source: Referrer Header

Referrer: http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,"\"><xsstag>()refdxss")

Execution Sink: set HTML code (innerHTML/outerHTML/...)

HTML code set: unknown is coming from

http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,"\"><xsstag>()refdxss")</xsstag> and has visited this page 1 times. ... Stack Trace:

- http://code.jquery.com/jquery-1.9.1.min.js:4:27657
- access@http://code.jquery.com/jquery-1.9.1.min.js:3:6852
- html@http://code.jquery.com/jquery-1.9.1.min.js:4:27282
- c@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:19:182
- global code@http://testhtml5.vulnweb.com/static/app/post.js:114:17

/

Details

Source: window.name

window.name: javascript:domxssExecutionSink(2,"\"><xsstag>()wildxss")

Execution Sink: evaluate code (eval/setTimeout/setInterval/...)

Evaluated code: this.myObj=javascript:domxssExecutionSink(2,"\"><xsstag>()wildxss") ... Stack Trace:

- toObject@http://testhtml5.vulnweb.com/static/app/libs/sessvars.js:105:17
- init@http://testhtml5.vulnweb.com/static/app/libs/sessvars.js:76:36
- http://testhtml5.vulnweb.com/static/app/libs/sessvars.js:202:13
- global code@http://testhtml5.vulnweb.com/static/app/libs/sessvars.js:204:2

/

Details

Source: Referrer Header

Referrer: http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,"\"><xsstag>()refdxss")

Execution Sink: set HTML code (innerHTML/outerHTML/...)

HTML code set:

```
<div class="navbar navbar-fixed-top">
  <div class="navbar-inner">
    <div class="container-fluid">
      <button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
      </button>
      <a class="brand" href="https://www.acunetix.com/">&nbsp; ... Stack Trace:
```

- appendChild@[native code]
- http://code.jquery.com/jquery-1.9.1.min.js:3:23057
- c@http://code.jquery.com/jquery-1.9.1.min.js:3:8110
- fireWith@http://code.jquery.com/jquery-1.9.1.min.js:3:16713
- ready@http://code.jquery.com/jquery-1.9.1.min.js:3:3525
- H@http://code.jquery.com/jquery-1.9.1.min.js:3:948

/

Details

Source: Referrer Header

Referrer: http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,""><xsstag>())refdxss")

Execution Sink: set HTML code (innerHTML/outerHTML/...)

HTML code set: <head>

<meta charset="utf-8">

<title>SecurityTweets - HTML5 test website for Acunetix Web Vulnerability Scanner</title>

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

<meta name="description" content="">

<meta name="author" content="">

<!-- Le styles -->

<link href="http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/css/bootstrap-combined.min.css" rel="stylesheet">

<link href="http://fonts.googleapis.com/css?family=Lora:400,700,400italic,700italic" ... Stack Trace:

- addClass@http://code.jquery.com/jquery-1.9.1.min.js:3:18884
- C@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:38:361
- https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:38:284
- https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:16:88
- \$eval@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:88:272
- \$apply@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:88:384
- https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:16:50
- d@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:27:273
- c@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:15:477
- rb@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:16:162
- jc@https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:15:316
- https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js:162:153
- c@http://code.jquery.com/jquery-1.9.1.min.js:3:8110
- fireWith@http://code.jquery.com/jquery-1.9.1.min.js:3:16713
- ready@http://code.jquery.com/jquery-1.9.1.min.js:3:3525
- H@http://code.jquery.com/jquery-1.9.1.min.js:3:948

/

Details

Source: Referrer Header

Referrer: http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,""><xsstag>())refdxss")

Execution Sink: set HTML code (innerHTML/outerHTML/...)

HTML code set:

<div class="navbar navbar-fixed-top">

<div class="navbar-inner">

<div class="container-fluid">

<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">

</button>

 ... Stack Trace:

- appendChild@[native code]
- http://code.jquery.com/jquery-1.9.1.min.js:4:26272
- domManip@http://code.jquery.com/jquery-1.9.1.min.js:4:28538
- append@http://code.jquery.com/jquery-1.9.1.min.js:4:26170
- http://code.jquery.com/jquery-1.9.1.min.js:4:30403
- backdrop@http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js:7:2924
- show@http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js:7:1199
- http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js:7:3619
- each@http://code.jquery.com/jquery-1.9.1.min.js:3:5509
- each@http://code.jquery.com/jquery-1.9.1.min.js:3:2265
- modal@http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js:7:3434
- http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js:7:4036
- dispatch@http://code.jquery.com/jquery-1.9.1.min.js:3:28590
- handle@http://code.jquery.com/jquery-1.9.1.min.js:3:25295
- dispatchEvent@[native code]

/

Details

Source: Referrer Header

Referrer: [http://www.acunetix-referrer.com/javascript:domxssExecutionSink\(0,"" "><xsstag>\(\)refdxss"\)](http://www.acunetix-referrer.com/javascript:domxssExecutionSink(0,)

Execution Sink: set HTML code (innerHTML/outerHTML/...)

HTML code set:

```
<div class="navbar navbar-fixed-top">
  <div class="navbar-inner">
    <div class="container-fluid">
      <button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
      </button>
      <a class="brand" href="https://www.acunetix.com/">&nbsp; ... Stack Trace:
```

- removeChild@[native code]
- http://code.jquery.com/jquery-1.9.1.min.js:3:24323
- c@http://code.jquery.com/jquery-1.9.1.min.js:3:8110
- fireWith@http://code.jquery.com/jquery-1.9.1.min.js:3:16713
- ready@http://code.jquery.com/jquery-1.9.1.min.js:3:3525
- H@http://code.jquery.com/jquery-1.9.1.min.js:3:948

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://testhtml5.vulnweb.com/login Form method: POST Form inputs: - username [Text] - password [Password]
Request headers
GET / HTTP/1.1 Pragma: no-cache Cache-Control: no-cache Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*
/
Details
Form name: <empty> Form action: http://testhtml5.vulnweb.com/contact Form method: POST Form inputs: - firstName [Text] - lastName [Text] - address [Text] - subject [Select] - message [TextArea]
Request headers
GET / HTTP/1.1

```
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
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

/
Details
Form name: <empty> Form action: http://testhtml5.vulnweb.com/login Form method: POST Form inputs: - username [Text] - password [Password]
Request headers
GET / HTTP/1.1 Pragma: no-cache Cache-Control: no-cache Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*

Vulnerable Javascript library

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

Description

You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult Web References for more information.

Recommendation

Upgrade to the latest version.

References

<http://www.thomasfrank.se/sessionvars.html>

Affected items

/static/app/libs/sessvars.js

Details

Detected Javascript library sessvars version 1.00.
The version was detected from file content.

Request headers

```
GET /static/app/libs/sessvars.js HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testhtml5.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

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 inside 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](#)
[OWASP Clickjacking](#)
[Defending with Content Security Policy frame-ancestors directive](#)
[Frame Buster Buster](#)
[Clickjacking Protection for Java EE](#)
[The X-Frame-Options response header](#)

Affected items

Web Server
Details
No details are available.
Request headers
GET / HTTP/1.1 Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*

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: "username"
Cookie domain: "testhtml5.vulnweb.com"
Request headers
GET / HTTP/1.1
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

Insecure response with wildcard '*' in Access-Control-Allow-Origin

Severity	Low
Type	Configuration
Reported by module	Scripting (Access_Control-Allow-Origin_Dir.script)

Description

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based by returning the value of the Origin request header, "*", or "null" in the response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHttpRequest) requests to your site and access the responses. It's not recommended to use the Access-Control-Allow-Origin: * header.

Impact

Any website can make XHR requests to your site and access the responses.

Recommendation

Is recommended not to use Access-Control-Allow-Origin: *. Instead the Access-Control-Allow-Origin header should contain the list of origins that can make COR requests.

References

[Test Cross Origin Resource Sharing \(OTG-CLIENT-007\)](#)

[Cross-origin resource sharing](#)

[Cross-Origin Resource Sharing](#)

[CrossOriginRequestSecurity](#)

Affected items

/
Details
No details are available.
Request headers
GET / HTTP/1.1 Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 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

/login
Details
The scanner tested 10 invalid credentials and no account lockout was detected.
Request headers
POST /login HTTP/1.1 Content-Length: 35 Content-Type: application/x-www-form-urlencoded Referer: http://testhtml5.vulnweb.com:80/ Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */* password=nuSdc7uO&username=x3sPHOIo

OPTIONS method is enabled

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

Description

HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

Impact

The OPTIONS method may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

It's recommended to disable OPTIONS Method on the web server.

References

[Testing for HTTP Methods and XST \(OWASP-CM-008\)](#)

Affected items

Web Server
Details
Methods allowed: HEAD, OPTIONS, GET
Request headers
OPTIONS / HTTP/1.1 Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*

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

/static/app/services

Details

No details are available.

Request headers

```
GET /static/app/services HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Host: testhtml5.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

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

/
Details
Password type input named password from form with ID loginForm with action /login has autocomplete enabled.
Request headers
GET / HTTP/1.1 Pragma: no-cache Cache-Control: no-cache Host: testhtml5.vulnweb.com Connection: Keep-alive Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*

Scanned items (coverage report)

Scanned 30 URLs. Found 5 vulnerable.

URL: <http://testhtml5.vulnweb.com/>

Vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
/	Path Fragment

Input scheme 2

Input name	Input type
Host	HTTP Header

URL: <http://testhtml5.vulnweb.com/login>

Vulnerabilities have 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://testhtml5.vulnweb.com/static>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://testhtml5.vulnweb.com/static/img/>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://testhtml5.vulnweb.com/static/css/>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://testhtml5.vulnweb.com/static/css/style.css>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://testhtml5.vulnweb.com/static/app/>

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://testhtml5.vulnweb.com/static/app/app.js>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://testhtml5.vulnweb.com/static/app/libs/>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://testhtml5.vulnweb.com/static/app/libs/sessvars.js>

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: <http://testhtml5.vulnweb.com/static/app/post.js>

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://testhtml5.vulnweb.com/static/app/controllers/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/controllers/controllers.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/services/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/services/itemsService.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/partials/
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/partials/popular.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/partials/itemsList.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/partials/latest.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/partials/carousel.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/partials/archive.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/partials/about.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/static/app/partials/contact.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/logout
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/ajax
No vulnerabilities have been identified for this URL
No input(s) found for this URL
URL: http://testhtml5.vulnweb.com/ajax/popular
No vulnerabilities have been identified for this URL
1 input(s) found for this URL
Inputs

Input scheme 1	
Input name	Input type
offset	URL encoded GET
URL: http://testhtml5.vulnweb.com/ajax/latest	
No vulnerabilities have been identified for this URL	
1 input(s) found for this URL	
Inputs	
Input scheme 1	
Input name	Input type
offset	URL encoded GET
URL: http://testhtml5.vulnweb.com/ajax/archive	
No vulnerabilities have been identified for this URL	
No input(s) found for this URL	
URL: http://testhtml5.vulnweb.com/forgotpw	
No vulnerabilities have been identified for this URL	
2 input(s) found for this URL	
Inputs	
Input scheme 1	
Input name	Input type
text/xml	Custom POST
forgot.username#text	XML
URL: http://testhtml5.vulnweb.com/contact	
Vulnerabilities have been identified for this URL	
5 input(s) found for this URL	
Inputs	
Input scheme 1	
Input name	Input type
address	URL encoded POST
firstName	URL encoded POST
lastName	URL encoded POST
message	URL encoded POST
subject	URL encoded POST