Digicon Website Audit

2 July, 2015

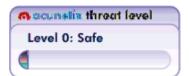# Developer Report

Scan of http://gsa-agile.digicon.com/demo/

Scan details

Scan information	
Start time	7/2/2015 10:09:14 AM
Finish time	7/2/2015 10:15:50 AM
Scan time	6 minutes, 36 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache Tomcat/7.0.56
Server OS	Unknown
Server technologies	

Threat level

Acunetix Threat Level 0
No vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	**3**	
🔴 **High**	0	
🟠 **Medium**	0	
🔵 **Low**	0	
🟢 **Informational**	3	

Knowledge base

Apache Tomcat version

Apache Tomcat version: 7.0.56.

List of file extensions

File extensions can provide information on what technologies are being used on this website.
List of file extensions detected:

- css => 4 file(s)
- js => 4 file(s)
- cfm => 4 file(s)
- cfc => 1 file(s)

List of client scripts

These files contain Javascript code referenced from the website.

- /demo/js/jqcloud/dist/jqcloud.min.js
- /demo/js/bootstraptable/bootstrap-table.js
- /demo/js/bootstrap.min.js
- /demo/js/ie10-viewport-bug-workaround.js

List of files with inputs

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

- /demo - 1 inputs
- /demo/homecontent.cfm - 1 inputs
- /demo/footer.cfm - 1 inputs
- /demo/search.cfm - 1 inputs
- /demo/labels.cfc - 1 inputs
- /demo/about.cfm - 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).

- ajax.googleapis.com

List of email addresses

List of all email addresses found on this host.

- wenzhixin2010@gmail.com

Alerts summary

Broken links

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-16

Affected items	Variation
/demo/css/bootstraphero.css	1

Email address found

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
/demo/js/bootstraptable/bootstrap-table.css	1

GHDB: Apache Tomcat Error message

Affected items	Variation
/demo/css/bootstraphero.css	1

Alert details

Broken links

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

Description

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

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

/demo/css/bootstraphero.css

Details

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

Request headers

```
GET /demo/css/bootstraphero.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://gsa-agile.digicon.com/demo/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: cfid=a40b2528-9fa9-471c-895b-efead930ec0d; cftoken=0
Host: gsa-agile.digicon.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 1003
Date: Thu, 02 Jul 2015 14:09:16 GMT
```

🔴 Email address found

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

Description

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

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

[Email Address Disclosed on Website Can be Used for Spam](#)

Affected items

/demo/js/bootstraptable/bootstrap-table.css

Details

Pattern found: wenzhixin2010@gmail.com

Request headers

```
GET /demo/js/bootstraptable/bootstrap-table.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://gsa-agile.digicon.com/demo/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: cfid=a40b2528-9fa9-471c-895b-efead930ec0d; cftoken=0
Host: gsa-agile.digicon.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"5067-1431346756000"
Last-Modified: Mon, 11 May 2015 12:19:16 GMT
Content-Type: text/css
Content-Length: 5067
Date: Thu, 02 Jul 2015 14:09:16 GMT
```

GHDB: Apache Tomcat Error message

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

Description

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

Apache Tomcat Error messages. These can reveal various kinds information depending on the type of error.

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

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

Acunetix Google hacking
The Google Hacking Database (GHDB) community

Affected items

/demo/css/bootstraphero.css

Details

We found intitle:"Apache Tomcat" "Error Report"

Request headers

```
GET /demo/css/bootstraphero.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://gsa-agile.digicon.com/demo/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: cfid=a40b2528-9fa9-471c-895b-efead930ec0d; cftoken=0
Host: gsa-agile.digicon.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Response headers

```
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 1003
Date: Thu, 02 Jul 2015 14:09:16 GMT
```