acunetix

# Developer Report

Acunetix Security Audit

19 June 2018

Generated by Acunetix

# Scan of https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/

## Scan details

| Scan information | |
|---|---|
| Start time | 19/06/2018, 17:07:45 |
| Start url | https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/ |
| Host | https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/ |
| Scan time | 12 minutes, 51 seconds |
| Profile | Full Scan |

### Threat level

#### Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

### Alerts distribution

| | |
|---|---|
| Total alerts found | 3 |
| High | 0 |
| Medium | 1 |
| Low | 1 |
| Informational | 1 |

## Alerts summary

### Vulnerable Javascript library

| Classification | |
|---|---|
| CVSS2 | Base Score: 6.4<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: Partial<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CVSS3 | Base Score: 6.5<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CWE | CWE-16 |

| Affected items | Variation |
|---|---|
| /stp-cognitivemkplace/shared/jquery.min.js | 1 |

### Clickjacking: X-Frame-Options header missing

| Classification | |
|---|---|
| CVSS2 | Base Score: 6.8<br>Access Vector: Network_accessible<br>Access Complexity: Medium<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: Partial<br>Availability Impact: Partial<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-693 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Web Application Firewall detected

| Classification | |
|---|---|
| | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None |

| | |
|---|---|
| CVSS2 | Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CVSS3 | Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CWE | CWE-16 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

## Alerts details

### Vulnerable Javascript library

| | |
|---|---|
| Severity | **Medium** |
| Reported by module | /Scripts/PerFile/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 References for more information.

#### Recommendation

Upgrade to the latest version.

#### Affected items

**/stp-cognitivemkplace/shared/jquery.min.js**

Details

Detected Javascript library **jquery** version **1.12.4**.
The version was detected from **file content**.

References:

- https://github.com/jquery/jquery/issues/2432

Request headers

```
GET /stp-cognitivemkplace/shared/jquery.min.js HTTP/1.1
Accept: */*
Accept-Encoding: gzip,deflate
Host: nxtstep.eastus.cloudapp.azure.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Proxy-Connection: Keep-alive
```

### Clickjacking: X-Frame-Options header missing

| | |
|---|---|
| Severity | **Low** |
| Reported by module | /Scripts/PerServer/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

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)
Clickjacking (http://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)
Defending with Content Security Policy frame-ancestors directive (https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)
Frame Buster Buster (http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

### Affected items

| Web Server |
| --- |
| Details |
| |
| Request headers |

```
GET / HTTP/1.1
Accept: */*
Accept-Encoding: gzip,deflate
Host: nxtstep.eastus.cloudapp.azure.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Proxy-Connection: keep-alive
```

## Web Application Firewall detected

| | |
| --- | --- |
| Severity | **Informational** |
| Reported by module | /Scripts/PerServer/WAF_Detection.script |

### Description

This server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or an WAF (Web Application Firewall). Acunetix detected this by sending various malicious payloads and detecting changes in the response code, headers and body.

### Impact

You may receive incorrect/incomplete results when scanning a server protected by an IPS/IDS/WAF. Also, if the WAF detects a number of attacks coming from the scanner, the IP address can be blocked after a few attempts.

### Recommendation

If possible, it's recommended to scan an internal (development) version of the web application where the WAF is not active.

### Affected items

| Web Server |
| --- |
| Details |
| Detected unknown Web Application Firewall from active probing. |
| Request headers |

```
GET /stp-cognitivemkplace/?
param=-1+UNION+SELECT+GROUP_CONCAT(table_name)+FROM+information_schema.tables HTTP/1.1
Connection: keep-alive
```

## Scanned items (coverage report)

https://nxtstep.eastus.cloudapp.azure.com/
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/__assets__
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/__assets__/shiny-server-client.min.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/__assets__/shiny-server.css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/__assets__/sockjs-0.3.4.min.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/AdminLTE-2.0.6
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/AdminLTE-2.0.6/_all-skins.min.css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/AdminLTE-2.0.6/AdminLTE.min.css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/AdminLTE-2.0.6/app.min.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/AdminLTE-2.0.6/fonts
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/crosstalk-1.0.0
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/crosstalk-1.0.0/css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/crosstalk-1.0.0/css/crosstalk.css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/crosstalk-1.0.0/js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/crosstalk-1.0.0/js/crosstalk.min.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/datatables-binding-0.4
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/datatables-binding-0.4/datatables.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/datatables-css-0.0.0
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/datatables-css-0.0.0/datatables-crosstalk.css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/htmlwidgets-1.0
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/htmlwidgets-1.0/htmlwidgets.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/img
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/plotly-binding-4.7.1
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/plotly-binding-4.7.1/plotly.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/bootstrap
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/bootstrap/css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/bootstrap/css/bootstrap.min.css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/bootstrap/fonts
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/bootstrap/fonts/glyphicons-halflings-regular.woff2
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/bootstrap/js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/bootstrap/js/bootstrap.min.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/bootstrap/shim
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/bootstrap/shim/html5shiv.min.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/bootstrap/shim/respond.min.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/font-awesome
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/font-awesome/css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/font-awesome/css/font-awesome.min.css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/font-awesome/fonts
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/font-awesome/fonts/fontawesome-webfont.woff2
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/jquery.min.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/json2-min.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/shiny.css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shared/shiny.min.js
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shinydashboard-0.7.0
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shinydashboard-0.7.0/shinydashboard.css
https://nxtstep.eastus.cloudapp.azure.com/stp-cognitivemkplace/shinydashboard-0.7.0/shinydashboard.min.js