Developer Report

Acunetix Security Audit

19 June 2018

Scan of https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/#/maturity

Scan details

Scan information	
Start time	19/06/2018, 16:57:51
Start url	https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/#/maturity
Host	https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/#/maturity
Scan time	3 minutes, 14 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	2
🔴 High	0
🟠 Medium	0
ⓘ Low	1
ⓘ Informational	1

Alerts summary

⊘ Clickjacking: X-Frame-Options header missing

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

Affected items	Variation
Web Server	1

ⓘ Email address found

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/stp-agile-assesment/agile	1

Alerts details

ⓘ 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
```

ⓘ Email address found

Severity	**Informational**
Reported by module	/Scripts/PerFolder/Text_Search_Dir.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

[Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)](https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

/stp-agile-assesment/agile
Details
Pattern found:

```
chart.js@2.7.0
```

Request headers

```
GET /stp-agile-assesment/agile/ 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
```

Scanned items (coverage report)

https://nxtstep.eastus.cloudapp.azure.com/
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/inline.05468d4f17f22ef910a7.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/main.2f2017dce23849a49682.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/polyfills.ff635d9590cf6dbc2517.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/scripts.ff6c2ba102667a643212.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/styles.1465ca4c358a5c2cbc46.bundle.css

https://nxtstep.eastus.cloudapp.azure.com/
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/inline.05468d4f17f22ef910a7.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/main.2f2017dce23849a49682.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/polyfills.ff635d9590cf6dbc2517.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/scripts.ff6c2ba102667a643212.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/stp-agile-assesment/agile/styles.1465ca4c358a5c2cbc46.bundle.css