

Developer Report

Acunetix Security Audit

27 February 2018

Scan of http://172.21.2.5/nextstep/

Scan details



Scan information	
Start time	27/02/2018, 16:14:36
Start url	http://172.21.2.5/nextstep/
Host	http://172.21.2.5/nextstep/
Scan time	3 minutes, 10 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	3
 High	0
 Medium	0
 Low	2
 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

OPTIONS method is enabled

Classification		
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial 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: 7.5 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

Microsoft IIS version disclosure

Classification	
	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None

CVSS2	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
Web Server		1

Alerts details

ⓘ Clickjacking: X-Frame-Options header missing

Severity	Low
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

[The X-Frame-Options response header](https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options) (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)
[Clickjacking](http://en.wikipedia.org/wiki/Clickjacking) (http://en.wikipedia.org/wiki/Clickjacking)
[OWASP Clickjacking](https://www.owasp.org/index.php/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) (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) (http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server
Details
Request headers
GET / HTTP/1.1 Host: 172.21.2.5 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: */*

ⓘ OPTIONS method is enabled

Severity	Low
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 \(OWASP-CM-008\)](https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASP-CM-008))

([https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_\(OWASP-CM-008\)](https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASP-CM-008)))

Affected items

Web Server
Details
Methods allowed: OPTIONS, TRACE, GET, HEAD, POST.
Request headers
OPTIONS / HTTP/1.1 Host: 172.21.2.5 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: */*

Microsoft IIS version disclosure

Severity	Informational
Reported by module	Scripting (ASP_NET_Error_Message.script)

Description

The HTTP responses returned by this web application include a header named **Server**. The value of this header includes the version of Microsoft IIS server.

Impact

The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Microsoft IIS should be configured to remove unwanted HTTP response headers from the response. Consult web references for more information.

References

[Remove Unwanted HTTP Response Headers](http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx) (<http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx>)

Affected items

Web Server
Details
Version information found:
Microsoft-IIS/10.0
Request headers
GET / ~.aspx HTTP/1.1

Host: 172.21.2.5
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)

<http://172.21.2.5/>

<http://172.21.2.5/nextstep>

<http://172.21.2.5/nextstep/assets>

<http://172.21.2.5/nextstep/assets/leader-line.min.js>

<http://172.21.2.5/nextstep/fontawesome-webfont.db812d8a70a4e88e8887.woff2>

<http://172.21.2.5/nextstep/glyphicons-halflings-regular.448c34a56d699c29117a.woff2>

<http://172.21.2.5/nextstep/inline.405b40949cd112fb1f94.bundle.js>

<http://172.21.2.5/nextstep/main.092c760a86bd90f33c25.bundle.js>

<http://172.21.2.5/nextstep/polyfills.4f5b1985bceb78db2b0c.bundle.js>

<http://172.21.2.5/nextstep/scripts.19af43f20c63766ce76c.bundle.js>

<http://172.21.2.5/nextstep/styles.d631d25873c7f44d1556.bundle.css>