acunetix WEB APPLICATION SECURITY

Acunetix Website Audit

6 July, 2015

Developer Report

Generated by Acunetix WVS Reporter (v10.0 Build 20150623)

Scan of http://www.myhealthalerts18f.com

Scan details

Scan information	
Start time	7/6/2015 9:57:06 PM
Finish time	7/6/2015 10:01:01 PM
Scan time	3 minutes, 56 seconds
Profile	High_Risk_Alerts
Server information	
Responsive	True
Server banner	nginx/0.7.67
Server OS	Unknown

Threat level

Acunetix Threat Level 1

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

Alerts distribution

Total alerts found	**1**	
High	0	|
Medium	0	|
Low	1	████████████████
Informational	0	|

Knowledge base

List of files with inputs

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

- / - 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).

- dyn.com
- ec2-54-175-250-1.compute-1.amazonaws.com

Alerts summary

Clickjacking: X-Frame-Options header missing

Classification	
CVSS	Base Score: 6.8 - 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

Alert details

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 Protection for Java EE
Frame Buster Buster
Defending with Content Security Policy frame-ancestors directive
Original Clickjacking paper
Clickjacking
The X-Frame-Options response header

Affected items

Web Server

Details

No details are available.

Request headers

```
GET / HTTP/1.1
Host: www.myhealthalerts18f.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
Acunetix-Product: WVS/9.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Accept: */*
```

Scanned items (coverage report)

Scanned 1 URLs. Found False vulnerable.

URL: http://www.myhealthalerts18f.com/
No vulnerabilities have been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
Host	HTTP Header