

Affected Items Report

Acunetix Security Audit

19 August 2019

Scan of www.secevery.com

Scan details





Scan information	
Start time	19/08/2019, 02:41:16
Start url	http://www.secevery.com
Host	www.secevery.com
Scan time	28 seconds
Profile	Full Scan
Server information	Apache/2.4.7 (Ubuntu)
Responsive	True
Server OS	Unix

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	6
 High	0
 Medium	1
 Low	2
 Informational	3

Affected items

/js/jquery-1.8.3.min.js	
Alert group	Vulnerable Javascript library
Severity	Medium
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.
Recommendations	Upgrade to the latest version.
Alert variants	
Details	<p>Detected Javascript library jquery version 1.8.3. The version was detected from filename, file content.</p> <p>References:</p> <ul style="list-style-type: none">• https://github.com/jquery/jquery/issues/2432• http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
<pre>GET /js/jquery-1.8.3.min.js HTTP/1.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip,deflate Host: www.secevery.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36 Connection: Keep-alive</pre>	

Web Server	
Alert group	Clickjacking: X-Frame-Options header missing
Severity	Low
Description	<p>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.</p> <p>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.</p>
Recommendations	Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	
<pre>GET / HTTP/1.1 Connection: keep-alive Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip,deflate Host: www.secevery.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36</pre>	

/img/debug.log	
Alert group	Possible sensitive files

Severity	Low
Description	A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.
Recommendations	Restrict access to this file or remove it from the website.
Alert variants	
Details	
<pre>GET /img/debug.log HTTP/1.1 Accept: acunetix/wvs Connection: keep-alive Accept-Encoding: gzip,deflate Host: www.secevery.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36</pre>	

Web Server	
Alert group	Content Security Policy (CSP) not implemented
Severity	Informational
Description	<p>Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.</p> <p>Content Security Policy (CSP) can be implemented by adding a Content-Security-Policy header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:</p> <pre>Content-Security-Policy: default-src 'self'; script-src 'self' https://code.jquery.com;</pre> <p>It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.</p>
Recommendations	It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.
Alert variants	
Details	
<pre>GET / HTTP/1.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip,deflate Host: www.secevery.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36 Connection: Keep-alive</pre>	

/img/debug.log	
Alert group	Content type is not specified
Severity	Informational

Description	This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.
Recommendations	Set a Content-Type header value for this page.
Alert variants	
Details	
GET /img/debug.log HTTP/1.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip,deflate Host: www.secevery.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36 Connection: Keep-alive	

Web Server	
Alert group	Error page web server version disclosure
Severity	Informational
Description	Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker. Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.
Recommendations	Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.
Alert variants	
Details	
GET /HEMc47KB0K HTTP/1.1 Connection: keep-alive Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip,deflate Host: www.secevery.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36	

Scanned items (coverage report)

<http://www.secevery.com/>
<http://www.secevery.com/HEMc47KBOK>
<http://www.secevery.com/css/>
<http://www.secevery.com/css/animate.min.css>
<http://www.secevery.com/css/main.css>
<http://www.secevery.com/css/normalize.css>
<http://www.secevery.com/css/owl.carousel.css>
<http://www.secevery.com/css/owl.theme.css>
<http://www.secevery.com/img/>
<http://www.secevery.com/img/debug.log>
<http://www.secevery.com/js/>
<http://www.secevery.com/js/jquery-1.8.3.min.js>
<http://www.secevery.com/js/jquery.sidr.min.js>
<http://www.secevery.com/js/main.js>
<http://www.secevery.com/js/owl.carousel.js>
<http://www.secevery.com/js/picturefill.min.js>