

Affected Items Report

Acunetix Security Audit

2025-11-17

Generated by Acunetix

Scan of 192.168.1.8

Scan details

Scan information	
Start time	2025-11-17T05:02:08.437290+00:00
Start url	http://192.168.1.8/site/war-is-over/
Host	192.168.1.8
Scan time	5 minutes, 24 seconds
Profile	Full Scan
Server information	Apache/2.4.29 (Ubuntu)
Responsive	True
Server OS	Unix
Application build	24.6.240626115

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	7
⚠ Critical	0
⚠ High	0
⚠ Medium	4
▼ Low	0
ⓘ Informational	3

Affected items

Web Server	
Alert group	Directory listings (verified)
Severity	Medium
Description	Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.
Recommendations	You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.
Alert variants	
Details	<p>Folders with directory listing enabled:</p> <ul style="list-style-type: none"> • http://192.168.1.8/

GET / HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36

Host: 192.168.1.8

Connection: Keep-alive

Web Server	
Alert group	Insecure HTTP Usage
Severity	Medium
Description	It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.
Recommendations	It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information
Alert variants	
Details	

GET / HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36

Host: 192.168.1.8

Connection: Keep-alive

Web Server	
Alert group	SSL/TLS Not Implemented (verified)
Severity	Medium
Description	This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.
Recommendations	The site should send and receive data over a secure (HTTPS) connection.
Alert variants	
Details	

```

GET /site/war-is-over/ HTTP/1.1
Referer: http://192.168.1.8/site/war-is-over/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.1.8
Connection: Keep-alive

```

Web Server	
Alert group	Virtual host directory listing
Severity	Medium
Description	This web server is responding with a directory listing when the Host header is manipulated and various common virtual hosts and/or IP addresses are tested. This is a web server misconfiguration and should be fixed as it may disclose sensitive information to an attacker. Consult Attack details for more information.
Recommendations	Fix virtual hosts configuration to resolve this problem.
Alert variants	
Details	<p>Virtual host: GXuUiTco Response: Last modified</p>

```

GET / HTTP/1.1
Host: GXuUiTco
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Connection: Keep-alive

```

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 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	<p>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.</p>
Alert variants	
Details	<p>Paths without CSP header:</p> <ul style="list-style-type: none"> • http://192.168.1.8/site/war-is-over/
<pre>GET /site/war-is-over/ HTTP/1.1 Referer: http://192.168.1.8/site/war-is-over/ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip,deflate,br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 Host: 192.168.1.8 Connection: Keep-alive</pre>	

Web Server	
Alert group	Error page web server version disclosure
Severity	Informational
Description	<p>Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.</p> <p>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.</p>
Recommendations	<p>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.</p>
Alert variants	
Details	

```
GET /X5kcKGI1p7 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.1.8
Connection: Keep-alive
```

Web Server	
Alert group	Permissions-Policy header not implemented
Severity	Informational
Description	The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.
Recommendations	
Alert variants	
Details	<p>Locations without Permissions-Policy header:</p> <ul style="list-style-type: none">• http://192.168.1.8/site/war-is-over/

```
GET /site/war-is-over/ HTTP/1.1
Referer: http://192.168.1.8/site/war-is-over/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.1.8
Connection: Keep-alive
```

Scanned items (coverage report)

<http://192.168.1.8/>

<http://192.168.1.8/site/>

<http://192.168.1.8/site/war-is-over/>