Affected Items Report

Acunetix Security Audit

2025-11-15

Generated by Acunetix

Scan of 10.136.108.235

Scan details

Scan information	
Start time	2025-11-15T16:38:41.111426+00:00
Start url	http://10.136.108.235/
Host	10.136.108.235
Scan time	2 minutes, 57 seconds
Profile	Full Scan
Server information	Apache/2.4.38 (Debian)
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	5
⚠ Critical	0
⌃ High	0
⌃ Medium	2
⌄ Low	0
ⓘ Informational	3

Affected items

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: 10.136.108.235
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 / HTTP/1.1
Referer: http://10.136.108.235/
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: 10.136.108.235
Connection: Keep-alive
```

Web Server	
Alert group	**Content Security Policy (CSP) Not Implemented**
Severity	Informational

Description	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.

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:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

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. |
| 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 | Paths without CSP header:

- http://10.136.108.235/

- http://10.136.108.235/index.html |

```
GET / HTTP/1.1
Referer: http://10.136.108.235/
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: 10.136.108.235
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 /M5A0pe8vUE 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: 10.136.108.235
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	Locations without Permissions-Policy header: • http://10.136.108.235/ • http://10.136.108.235/index.html

```
GET / HTTP/1.1
Referer: http://10.136.108.235/
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: 10.136.108.235
Connection: Keep-alive
```

Scanned items (coverage report)

http://10.136.108.235/
http://10.136.108.235/index.html