Comprehensive Report

Medium

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.

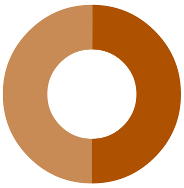
Scan Detail

Target	http://192.168.1.8:54787/
Scan Type	Critical / High / Medium Risk
Start Time	Nov 1, 2025, 6:25:19 AM GMT
Scan Duration	7 minutes
Requests	17043
Average Response Time	1ms
Maximum Response Time	30496ms
Application Build	v24.6.240626115
Authentication Profile	-

0	0	2	1	0
Critical	High	Medium	Low	Informational

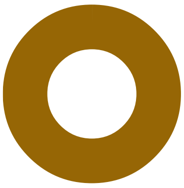
Severity	Vulnerabilities	Instances
Critical	0	0
High	0	0
Medium	2	2
Low	1	1
Informational	0	0
Total	3	3

Medium Severity



		Instances
🟧	Insecure HTTP Usage	1
🟫	SSL/TLS Not Implemented	1

Low Severity



		Instances
🟫	Version Disclosure (PHP)	1

Impacts

SEVERITY	IMPACT	
⌃ Medium	1	Insecure HTTP Usage
⌃ Medium	1	SSL/TLS Not Implemented
⌄ Low	1	Version Disclosure (PHP)

Insecure HTTP Usage

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

http://192.168.1.8:54787/

Request

```
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: 192.168.1.8:54787
Connection: Keep-alive
```

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections
https://infosec.mozilla.org/guidelines/web_security#http-redirections

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

http://192.168.1.8:54787/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.8:54787/
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: 192.168.1.8:54787
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Version Disclosure (PHP)

The web server is sending the X-Powered-By: response headers, revealing the PHP version.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

http://192.168.1.8:54787/

Version detected: **PHP/7.3.14-1~deb10u1**.

Recommendation

Configure your web server to prevent information leakage from its HTTP response.

References

PHP Documentation: header_remove()
https://www.php.net/manual/en/function.header-remove.php

PHP Documentation: php.ini directive expose_php
https://www.php.net/manual/en/ini.core.php#ini.expose-php

Coverage

- http://192.168.1.8:54787
  - admin
  - api
  - axis2
    - axis2-admin
      - welcome
  - cacti
  - cognos_express
    - manager
      - html
  - console
  - extrahop
  - host-manager
    - html
    - text
  - lc
    - system
      - console
  - manager
    - html
    - status
  - nagios
  - otrs
  - rockmongo
  - system
    - console
  - tomcat
    - host-manager
      - html
      - text
    - manager

    - html
    - status
- ui
  - authentication
- webtools
- zabbix