Acunetix by Invicti

Comprehensive Report

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.

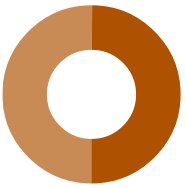
Scan Detail

Target	http://192.168.1.18:3128
Scan Type	Full Scan
Start Time	Nov 6, 2025, 7:57:58 AM GMT
Scan Duration	16 minutes
Requests	1961
Average Response Time	2ms
Maximum Response Time	30004ms
Application Build	v24.6.240626115
Authentication Profile	-

0	0	2	0	1
Critical	High	Medium	Low	Informational

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

Medium Severity



	Instances
Insecure HTTP Usage	1
SSL/TLS Not Implemented	1

Informational

	Instances
Permissions-Policy header not implemented	1

Impacts

SEVERITY	IMPACT	
Medium	1	Insecure HTTP Usage
Medium	1	SSL/TLS Not Implemented
Informational	1	Permissions-Policy header not implemented

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://192.168.1.18:3128/

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: 192.168.1.18:3128
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://192.168.1.18:3128/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.18:3128/
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: 192.168.1.18:3128
Connection: Keep-alive
```

Recommendation

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

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

http://192.168.1.18:3128/

Locations without Permissions-Policy header:

- http://192.168.1.18:3128/

Request

```
GET / HTTP/1.1
Referer: http://192.168.1.18:3128/
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: 192.168.1.18:3128
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

Coverage

http://192.168.1.18:3128