DAST Scanning Report

Site: http://127.0.0.1:8080

Generated on: Wed, 02 Oct 2024 02:04:17

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	0
Informational	6

Category Summary

Category	Number of Instances
Host Information	0
Open Ports	6

All Headers:

Connection	keep-alive
Content-Length	0
Date	Tue, 01 Oct 2024 16:02:43 GMT

Security Headers:

Strict-Transport-Security	Missing	High	Enforces secure (HTTP over SSL/TLS) connections to the server.
Content-Security-Policy	Missing	High	Prevents cross-site scripting (XSS) and data injection attacks.
X-Frame-Options	Missing	Medium	Protects against clickjacking attacks.
X-Content-Type-Options	Missing	Medium	Prevents MIME types from being sniffed.
Referrer-Policy	Missing	Low	Controls the amount of referrer information sent with requests.
Permissions-Policy	Missing	Low	Allows or denies the use of browser features.

Open Ports
Endpoint/IP: 127.0.0.1

Port	Issue	Description	Severity
135	Unknown Issues	No specific vulnerabilities known for port 135.	Informational
445	Unknown Issues	No specific vulnerabilities known for port 445.	Informational
8080	Weak Authentication on Web Server	Port 8080 is used by web servers that may have weak authentication mechanisms.	Medium
8080	Cross-Site Scripting (XSS)	Potential XSS vulnerability found on web server running on port 8080.	High
9090	Weak Authentication	Port 9090 is often used by applications with weak or misconfigured authentication.	Medium
9090	Directory Traversal	Applications running on port 9090 may be vulnerable to directory traversal attacks.	High
49157	Unknown Issues	No specific vulnerabilities known for port 49157.	Informational
49159	Unknown Issues	No specific vulnerabilities known for port 49159.	Informational