DAST Scanning Report

Site: http://127.0.0.1:8080

Generated on: Wed, 02 Oct 2024 02:32:29

Summary of Alerts

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

Category Summary

Category	Number of Instances
Host Information	0
Broken Access Control	6

All Headers:

Connection	keep-alive
Content-Length	0
Date	Tue, 01 Oct 2024 16:32:29 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.

Broken Access Control
Endpoint/IP: http://127.0.0.1:8080/WebGoat/AccessControl/attack

Issue	Description	Severity
Broken Access Control	Access control issue: 200 detected with payload: {'user_role': 'admin'}. This role or action should not have access to this resource.	High
Broken Access Control	Access control issue: 200 detected with payload: {'user_role': 'guest'}. This role or action should not have access to this resource.	High
Broken Access Control	Access control issue: 200 detected with payload: {'user_role': 'user', 'resource': 'restricted_resource'}. This role or action should not have access to this resource.	High
Broken Access Control	Access control issue: 200 detected with payload: {'user_role': 'user', 'action': 'delete'}. This role or action should not have access to this resource.	High
Broken Access Control	Access control issue: 200 detected with payload: {'user_role': 'anonymous', 'resource': 'private_data'}. This role or action should not have access to this resource.	High
Broken Access Control	Access control issue: 200 detected with payload: {'user_role': 'user', 'action': 'edit'}. This role or action should not have access to this resource.	High