DAST Scanning Report

Site: http://127.0.0.1:8080

Generated on: Tue, 01 Oct 2024 14:08:19

Summary of Alerts

Risk Level	Number of Alerts
High	22
Medium	38
Low	0
Informational	6

Category Summary

Category	Number of Instances
Host Information	0
Broken Authentication	1
Security Misconfiguration	48
Cryptographic Failures Within Endpoint	4
Broken Access Control	6
Cryptographic Failures Domain-wide	1
Open Ports	6

All Headers:

Connection	keep-alive
Content-Length	0
Date	Tue, 01 Oct 2024 04:06:44 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 Authentication
Endpoint/IP: http://127.0.0.1:8080/WebGoat/Auth/login

Issue	Description	Severity
Broken Authentication	Possible broken authentication detected. The application did not reject the request with an incorrect password. Parameters: {'username': 'test', 'password': 'incorrect_password'}.	High

Security Misconfiguration
Endpoint/IP: http://127.0.0.1:8080/WebGoat/Auth/login

Issue	Description	Severity
Missing Security Header	The 'X-Frame-Options' security header is not set.	Medium
Missing Security Header	The 'X-Content-Type-Options' security header is not set.	Medium
Missing Security Header	The 'Content-Security-Policy' security header is not set.	Medium
Missing Security Header	The 'Strict-Transport-Security' security header is not set.	Medium

Missing Security Header	The 'Referrer-Policy' security header is not set.	Medium
Missing Security Header	The 'Feature-Policy' security header is not set.	Medium
Improper Logging	Sensitive data found in logs: 'password'. This may expose critical information.	High
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data. Vulnerable Payload:]>&xxe;	High
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data. Vulnerable Payload:]>&xxe;	High
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data. Vulnerable Payload:]>&xxe;	High
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data. Vulnerable Payload:]>&xxe;	High
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data. Vulnerable Payload:]>&xxe;	High
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: admin12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: admin12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: johnalert('Tag Injection')	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: john12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: john12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: &ext;12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: johnyes12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: john12345	Medium

Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: john112345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: ' OR '<script>alert(1)</script>12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: admin	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: johnAdmin	Medium

Cryptographic Failures Within Endpoint

Endpoint/IP: http://127.0.0.1:8080/WebGoat/Auth/login

Issue	Description	Severity	Details
Binary Data Detected	Binary data detected, this might be sensitive information.	Medium	b'\xa2\xb8?\xd7\xdf}\xff\x18m'
Digital Signature	No digital signature detected or missing key components for proper usage.	High	RSA Used: False, ECDSA Used: False, Signature Present: False, Public Key Present: False, Signed Data Present: False

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

Security Misconfiguration
Endpoint/IP: http://127.0.0.1:8080/WebGoat/login

Issue	Description	Severity
Missing Security Header	The 'X-Frame-Options' security header is not set.	Medium
Missing Security Header	The 'X-Content-Type-Options' security header is not set.	Medium
Missing Security Header	The 'Content-Security-Policy' security header is not set.	Medium
Missing Security Header	The 'Strict-Transport-Security' security header is not set.	Medium
Missing Security Header	The 'Referrer-Policy' security header is not set.	Medium
Missing Security Header	The 'Feature-Policy' security header is not set.	Medium
Improper Logging	Sensitive data found in logs: 'password'. This may expose critical information.	High
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data. Vulnerable Payload:]>&xxe;	High
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data. Vulnerable Payload:]>&xxe;	High
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data. Vulnerable Payload:]>&xxe;	High
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data. Vulnerable Payload:]>&xxe;	High

XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data. Vulnerable Payload:]>&xxe;	High
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: admin12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: admin12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: johnalert('Tag Injection')	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: john12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: john12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: &ext;12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: johnyes12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: john12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: john112345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: ' OR '<script>alert(1)</script>12345	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: admin	Medium
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags on payload: johnAdmin	Medium

Cryptographic Failures Within Endpoint

Endpoint/IP: http://127.0.0.1:8080/WebGoat/login

Issue	Description	Severity	Details
Binary Data Detected	Binary data detected, this might be sensitive information.	Medium	b'\xa2\xb8?\xd7\xdf}\xff\x18m'

Digital Signature	No digital signature detected or missing key components for proper usage.	High	RSA Used: False, ECDSA Used: False, Signature Present: False, Public Key Present: False, Signed Data Present: False

Cryptographic Failures Domain-wide
Endpoint/IP: 127.0.0.1

Issue	Description	Severity
Insecure Data Transmission	The connection is not using HTTPS.	High

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