DAST Scanning Report

Site: http://webgoat:8080

Generated on: Wed, 16 Oct 2024 23:06:48

Summary of Alerts

Risk Level	Number of Alerts
High	28
Medium	50
Low	1
Informational	0

Category Summary

Category	Number of Instances
Broken Access Control	6
Broken Authentication	1
Cryptographic Failures Within Endpoint	4
Cryptographic Failures Domain-wide	1
Security Misconfiguration	48
Open Ports	2
SSRF	7
Insecure Deserialization	10

All Headers:

Connection	keep-alive
Content-Length	0
Date	Wed, 16 Oct 2024 23:06:45 GMT

Security Headers:

Header	Status	Severity	Description
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://webgoat:8080/WebGoat/AccessControl/attack

Issue	Description	Severity
Hijack a session	Session hijacked successfully with session token: sample_token_to_hijack	High
Insecure Direct Object References (IDOR)	IDOR vulnerability found with object reference: 1234	High
Missing Function Level Access Control	Unauthorized access detected for role: admin	High
Missing Function Level Access Control	Unauthorized access detected for role: guest	High
Missing Function Level Access Control	Unauthorized access detected for role: user	High
Spoofing an Authentication Cookie	Spoofed cookie allowed unauthorized access with auth token: fake_auth_token	High

Broken Authentication
Endpoint/IP: http://webgoat: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

Cryptographic Failures Within Endpoint
Endpoint/IP: http://webgoat:8080/WebGoat/Auth/login

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

Cryptographic Failures Within Endpoint
Endpoint/IP: http://webgoat:8080/WebGoat/login

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

Cryptographic Failures Domain-wide
Endpoint/IP: webgoat

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

Security Misconfiguration
Endpoint/IP: http://webgoat: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

Security Misconfiguration
Endpoint/IP: http://webgoat: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

Open Ports
Endpoint/IP: webgoat

Port	Issue	Description	Severity
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

SSRF
Endpoint/IP: http://webgoat:8080/WebGoat/SSRF

Issue	Description	Details	Severity
Server-Side Request Forgery (SSRF)	Access to AWS EC2 metadata endpoint indicates exposure of sensitive cloud data.	Payload: http://169.254.169.254/latest/meta-data/, Status Code: 200	High
Server-Side Request Forgery (SSRF)	Localhost SSH port (22) is accessible, indicating potential internal exposure.	Payload: http://127.0.0.1:22, Status Code: 200	High
Server-Side Request Forgery (SSRF)	Internal service on localhost:8080 is accessible, which may expose admin interfaces.	Payload: http://localhost:8080/, Status Code: 200	Medium
Server-Side Request Forgery (SSRF)	Internal IP (10.x.x.x range) is reachable, posing a risk of network probing.	Payload: http://10.0.0.1/, Status Code: 200	Medium
Server-Side Request Forgery (SSRF)	Access to internal router/admin panel at 192.168.1.1 is possible.	Payload: http://192.168.1.1/, Status Code: 200	Medium

Server-Side Request Forgery (SSRF)	Non-standard port 22 on example.com is accessible, indicating potential external service exposure.	Payload: http://example.com:22/, Status Code: 200	Low
Server-Side Request Forgery (SSRF)	Apache server-status page on localhost is accessible, potentially revealing server details.	Payload: http://localhost/server-status, Status Code: 200	Medium

Insecure Deserialization
Endpoint/IP:
http://webgoat:8080/WebGoat/InsecureDeserialization/attack

Issue	Description	Severity
Potential Insecure Deserialization	The application accepted and processed payload without validation: Simple string payload to test basic deserialization handling.	Medium
Potential Insecure Deserialization	The application accepted and processed payload without validation: Attempt to perform path traversal through deserialization.	Medium
Potential Insecure Deserialization	The application accepted and processed payload without validation: Injected script tag to test for XSS via deserialization.	Medium
Potential Insecure Deserialization	The application accepted and processed payload without validation: Serialized JSON object attempting to escalate privileges.	Medium
Potential Insecure Deserialization	The application accepted and processed payload without validation: Payload attempting to execute system commands via deserialization.	Medium

Insecure Deserialization
Endpoint/IP:
http://webgoat:8080/WebGoat/SerializationBasics/attack

Issue	Description	Severity
Potential Insecure Deserialization	The application accepted and processed payload without validation: Simple string payload to test basic deserialization handling.	Medium
Potential Insecure Deserialization	The application accepted and processed payload without validation: Attempt to perform path traversal through deserialization.	Medium

Potential Insecure Deserialization	The application accepted and processed payload without validation: Injected script tag to test for XSS via deserialization.	Medium
Potential Insecure Deserialization	The application accepted and processed payload without validation: Serialized JSON object attempting to escalate privileges.	Medium
Potential Insecure Deserialization	The application accepted and processed payload without validation: Payload attempting to execute system commands via deserialization.	Medium