

# DAST Scanning Report

**Site:** http://127.0.0.1:8080/

**Generated on:** Tue, 17 Sep 2024 18:06:13

## Summary of Alerts

Risk Level	Number of Alerts
High	91
Medium	108
Low	0

## Category Summary

Category	Number of Instances
Cryptographic Failure	19
Broken Authentication	6
Broken Access Control	36
Security Misconfigurations	114
Open Ports	36

## Alerts Organized by Category

### Cryptographic Failure

Issue	Description	Severity	Endpoint
Insecure Data Transmission	The connection is not using HTTPS.	High	127.0.0.1
Encoding Check	No Base64 encoding detected.	Informational	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Hashing Algorithm Check	No weak or deprecated hashing algorithms detected.	Informational	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Digital Signature	No digital signature detected.	High	http://127.0.0.1:8080/WebGoat/SqlInjection/attack

Encoding Check	No Base64 encoding detected.	Informational	http://127.0.0.1:8080/WebGoat/XSS/attack
Hashing Algorithm Check	No weak or deprecated hashing algorithms detected.	Informational	http://127.0.0.1:8080/WebGoat/XSS/attack
Digital Signature	No digital signature detected.	High	http://127.0.0.1:8080/WebGoat/XSS/attack
Encoding Check	No Base64 encoding detected.	Informational	http://127.0.0.1:8080/WebGoat/Auth/login
Hashing Algorithm Check	No weak or deprecated hashing algorithms detected.	Informational	http://127.0.0.1:8080/WebGoat/Auth/login
Digital Signature	No digital signature detected.	High	http://127.0.0.1:8080/WebGoat/Auth/login
Encoding Check	No Base64 encoding detected.	Informational	http://127.0.0.1:8080/WebGoat/SensitiveData
Hashing Algorithm Check	No weak or deprecated hashing algorithms detected.	Informational	http://127.0.0.1:8080/WebGoat/SensitiveData
Digital Signature	No digital signature detected.	High	http://127.0.0.1:8080/WebGoat/SensitiveData
Encoding Check	No Base64 encoding detected.	Informational	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Hashing Algorithm Check	No weak or deprecated hashing algorithms detected.	Informational	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Digital Signature	No digital signature detected.	High	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Encoding Check	No Base64 encoding detected.	Informational	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Hashing Algorithm Check	No weak or deprecated hashing algorithms detected.	Informational	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Digital Signature	No digital signature detected.	High	http://127.0.0.1:8080/WebGoat/Deserialization/attack

## Broken Authentication

Issue	Description	Severity	Endpoint
Broken Authentication	Possible broken authentication detected.	High	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Broken Authentication	Possible broken authentication detected.	High	http://127.0.0.1:8080/WebGoat/XSS/attack
Broken Authentication	Possible broken authentication detected.	High	http://127.0.0.1:8080/WebGoat/Auth/login

Broken Authentication	Possible broken authentication detected.	High	http://127.0.0.1:8080/WebGoat/SensitiveData
Broken Authentication	Possible broken authentication detected.	High	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Broken Authentication	Possible broken authentication detected.	High	http://127.0.0.1:8080/WebGoat/Deserialization/attack

## Broken Access Control

Issue	Description	Severity	Endpoint
Broken Access Control	Access control issue detected for payload: {'user_role': 'admin'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'guest'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'resource': 'restricted_resource'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'delete'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'anonymous', 'resource': 'private_data'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'edit'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'admin'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/XSS/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'guest'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/XSS/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'resource': 'restricted_resource'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/XSS/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'delete'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/XSS/attack

Broken Access Control	Access control issue detected for payload: {'user_role': 'anonymous', 'resource': 'private_data'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/XSS/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'edit'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/XSS/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'admin'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Auth/login
Broken Access Control	Access control issue detected for payload: {'user_role': 'guest'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Auth/login
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'resource': 'restricted_resource'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Auth/login
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'delete'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Auth/login
Broken Access Control	Access control issue detected for payload: {'user_role': 'anonymous', 'resource': 'private_data'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Auth/login
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'edit'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Auth/login
Broken Access Control	Access control issue detected for payload: {'user_role': 'admin'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SensitiveData
Broken Access Control	Access control issue detected for payload: {'user_role': 'guest'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SensitiveData
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'resource': 'restricted_resource'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SensitiveData
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'delete'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SensitiveData
Broken Access Control	Access control issue detected for payload: {'user_role': 'anonymous', 'resource': 'private_data'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SensitiveData

Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'edit'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/SensitiveData
Broken Access Control	Access control issue detected for payload: {'user_role': 'admin'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'guest'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'resource': 'restricted_resource'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'delete'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'anonymous', 'resource': 'private_data'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'edit'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'admin'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'guest'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'resource': 'restricted_resource'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'delete'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'anonymous', 'resource': 'private_data'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Broken Access Control	Access control issue detected for payload: {'user_role': 'user', 'action': 'edit'}. Status code: 200	High	http://127.0.0.1:8080/WebGoat/Deserialization/attack

## Security Misconfigurations

Issue	Description	Severity	Endpoint
Missing Security Header	X-Frame-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Missing Security Header	X-Content-Type-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Missing Security Header	Content-Security-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Missing Security Header	Strict-Transport-Security header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Missing Security Header	Referrer-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Missing Security Header	Feature-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Improper Logging	Sensitive data found in logs: password	High	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnalert('Tag Injection')	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: &ext;12345	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnyes12345	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: john112345	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: ' OR <script>alert(1)</script>12345	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnAdmin	Medium	http://127.0.0.1:8080/WebGoat/SqlInjection/attack

Missing Security Header	X-Frame-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Missing Security Header	X-Content-Type-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Missing Security Header	Content-Security-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Missing Security Header	Strict-Transport-Security header is not set.	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Missing Security Header	Referrer-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Missing Security Header	Feature-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Improper Logging	Sensitive data found in logs: password	High	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnalert('Tag Injection')	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: &ext;12345	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnyes12345	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: john112345	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: ' OR '<script>alert(1)</script>12345	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnAdmin	Medium	http://127.0.0.1:8080/WebGoat/XSS/attack
Missing Security Header	X-Frame-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Auth/login



Missing Security Header	X-Content-Type-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Missing Security Header	Content-Security-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Missing Security Header	Strict-Transport-Security header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Missing Security Header	Referrer-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Missing Security Header	Feature-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Improper Logging	Sensitive data found in logs: password	High	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: johnalert('Tag Injection')	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: &ext;12345	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: johnyes12345	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: john112345	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: ' OR '<script>alert(1)</script>12345	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: admin	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Tag Injection	Tag Injection vulnerability detected with payload: johnAdmin	Medium	http://127.0.0.1:8080/WebGoat/Auth/login
Missing Security Header	X-Frame-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Missing Security Header	X-Content-Type-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData



Missing Security Header	Content-Security-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Missing Security Header	Strict-Transport-Security header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Missing Security Header	Referrer-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Missing Security Header	Feature-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Improper Logging	Sensitive data found in logs: password	High	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: johnalert('Tag Injection')	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: &ext;12345	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: johnyes12345	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: john112345	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: ' OR '<script>alert(1)</script>12345	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: admin	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Tag Injection	Tag Injection vulnerability detected with payload: johnAdmin	Medium	http://127.0.0.1:8080/WebGoat/SensitiveData
Missing Security Header	X-Frame-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Missing Security Header	X-Content-Type-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Missing Security Header	Content-Security-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack

Missing Security Header	Strict-Transport-Security header is not set.	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Missing Security Header	Referrer-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Missing Security Header	Feature-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Improper Logging	Sensitive data found in logs: password	High	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnalert('Tag Injection')	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: &ext;12345	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnyes12345	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: john112345	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: ' OR '<script>alert(1)</script>12345	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnAdmin	Medium	http://127.0.0.1:8080/WebGoat/AccessControl/attack
Missing Security Header	X-Frame-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Missing Security Header	X-Content-Type-Options header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Missing Security Header	Content-Security-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Missing Security Header	Strict-Transport-Security header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack

Missing Security Header	Referrer-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Missing Security Header	Feature-Policy header is not set.	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Improper Logging	Sensitive data found in logs: password	High	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin12345	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnalert('Tag Injection')	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: &ext;12345	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnyes12345	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: john12345	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: john112345	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: ' OR '<script>alert(1)</script>12345	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: admin	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack
Tag Injection	Tag Injection vulnerability detected with payload: johnAdmin	Medium	http://127.0.0.1:8080/WebGoat/Deserialization/attack

## Open Ports

Issue	Description	Severity	Endpoint
Open Port: 111	Detected vulnerability: Portmap service: Denial of Service	High	127.0.0.1:111
Open Port: 111	Detected vulnerability: Remote code execution	High	127.0.0.1:111
Open Port: 8080	Detected vulnerability: Weak authentication on web servers	High	127.0.0.1:8080

Open Port: 8080	Detected vulnerability: Cross-Site Scripting (XSS)	High	127.0.0.1:8080
Open Port: 9090	Detected vulnerability: Weak authentication	High	127.0.0.1:9090
Open Port: 9090	Detected vulnerability: Directory traversal	High	127.0.0.1:9090
Open Port: 111	Detected vulnerability: Portmap service: Denial of Service	High	127.0.0.1:111
Open Port: 111	Detected vulnerability: Remote code execution	High	127.0.0.1:111
Open Port: 8080	Detected vulnerability: Weak authentication on web servers	High	127.0.0.1:8080
Open Port: 8080	Detected vulnerability: Cross-Site Scripting (XSS)	High	127.0.0.1:8080
Open Port: 9090	Detected vulnerability: Weak authentication	High	127.0.0.1:9090
Open Port: 9090	Detected vulnerability: Directory traversal	High	127.0.0.1:9090
Open Port: 111	Detected vulnerability: Portmap service: Denial of Service	High	127.0.0.1:111
Open Port: 111	Detected vulnerability: Remote code execution	High	127.0.0.1:111
Open Port: 8080	Detected vulnerability: Weak authentication on web servers	High	127.0.0.1:8080
Open Port: 8080	Detected vulnerability: Cross-Site Scripting (XSS)	High	127.0.0.1:8080
Open Port: 9090	Detected vulnerability: Weak authentication	High	127.0.0.1:9090
Open Port: 9090	Detected vulnerability: Directory traversal	High	127.0.0.1:9090
Open Port: 111	Detected vulnerability: Portmap service: Denial of Service	High	127.0.0.1:111
Open Port: 111	Detected vulnerability: Remote code execution	High	127.0.0.1:111
Open Port: 8080	Detected vulnerability: Weak authentication on web servers	High	127.0.0.1:8080
Open Port: 8080	Detected vulnerability: Cross-Site Scripting (XSS)	High	127.0.0.1:8080
Open Port: 9090	Detected vulnerability: Weak authentication	High	127.0.0.1:9090
Open Port: 9090	Detected vulnerability: Directory traversal	High	127.0.0.1:9090

Open Port: 111	Detected vulnerability: Portmap service: Denial of Service	High	127.0.0.1:111
Open Port: 111	Detected vulnerability: Remote code execution	High	127.0.0.1:111
Open Port: 8080	Detected vulnerability: Weak authentication on web servers	High	127.0.0.1:8080
Open Port: 8080	Detected vulnerability: Cross-Site Scripting (XSS)	High	127.0.0.1:8080
Open Port: 9090	Detected vulnerability: Weak authentication	High	127.0.0.1:9090
Open Port: 9090	Detected vulnerability: Directory traversal	High	127.0.0.1:9090
Open Port: 111	Detected vulnerability: Portmap service: Denial of Service	High	127.0.0.1:111
Open Port: 111	Detected vulnerability: Remote code execution	High	127.0.0.1:111
Open Port: 8080	Detected vulnerability: Weak authentication on web servers	High	127.0.0.1:8080
Open Port: 8080	Detected vulnerability: Cross-Site Scripting (XSS)	High	127.0.0.1:8080
Open Port: 9090	Detected vulnerability: Weak authentication	High	127.0.0.1:9090
Open Port: 9090	Detected vulnerability: Directory traversal	High	127.0.0.1:9090