DAST Scanning Report

Site: http://127.0.0.1:8080

Generated on: Sat, 28 Sep 2024 03:50:11

Summary of Alerts

Risk Level	Number of Alerts
High	20
Medium	36
Low	0
Informational	6

Category Summary

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

Alerts Organized by Category

Broken Authentication

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

Security Misconfiguration

Issue	Description	Severity	Endpoint
Missing Security Header	The 'X-Frame-Options' security header is not set.	Medium	N/A
Missing Security Header	The 'X-Content-Type-Options' security header is not set.	Medium	N/A
Missing Security Header	The 'Content-Security-Policy' security header is not set.	Medium	N/A
Missing Security Header	The 'Strict-Transport-Security' security header is not set.	Medium	N/A
Missing Security Header	The 'Referrer-Policy' security header is not set.	Medium	N/A
Missing Security Header	The 'Feature-Policy' security header is not set.	Medium	N/A
Improper Logging	Sensitive data found in logs: 'password'. This may expose critical information.	High	N/A
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data.	High	N/A
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data.	High	N/A
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data.	High	N/A
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data.	High	N/A
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data.	High	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A

Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A

Broken Access Control

Issue	Description	Severity	Endpoint
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	N/A
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	N/A
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	N/A

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	N/A
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	N/A
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	N/A

Security Misconfiguration

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

XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data.	High	N/A
XML External Entity (XXE) Injection detected	Possible XXE vulnerability detected. Application may be processing untrusted XML data.	High	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A
Tag Injection Vulnerability detected	Detected potential tag injection vulnerability. Application may be vulnerable to injecting arbitrary tags.	Medium	N/A

Cryptographic Failures Domain-wide

Issue	Description	Severity	Endpoint
Insecure Data Transmission	The connection is not using HTTPS.	High	127.0.0.1

Open Ports

Issue	Description	Severity	Endpoint
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A