URL: https://owasp.org/www-project-juice-shop/

SQL Summary:
SQL Injection Test Results:
Potential SQL Injection vulnerability detected with payload: ' OR '1'='1
Potential SQL Injection vulnerability detected with payload: ' AND '1'='1
Potential SQL Injection vulnerability detected with payload: ' OR 'x'='x
Potential SQL Injection vulnerability detected with payload: ' OR 1=1 --
Potential SQL Injection vulnerability detected with payload: ' OR 1=1 /*
Potential SQL Injection vulnerability detected with payload: ' OR 'a'='a

SQL Logs:
SQL Injection test URL: https://owasp.org/www-project-juice-shop/?id=' OR '1'='1
Response Code: 200
Response Time: 0.456963 seconds
Response Length: 88462 bytes
SQL Injection test URL: https://owasp.org/www-project-juice-shop/?id=' AND '1'='1
Response Code: 200
Response Time: 0.689774 seconds
Response Length: 88462 bytes
SQL Injection test URL: https://owasp.org/www-project-juice-shop/?id=' OR 'x'='x
Response Code: 200
Response Time: 0.57722 seconds
Response Length: 88462 bytes
SQL Injection test URL: https://owasp.org/www-project-juice-shop/?id=' OR 1=1 --
Response Code: 200
Response Time: 0.614041 seconds
Response Length: 88462 bytes
SQL Injection test URL: https://owasp.org/www-project-juice-shop/?id=' OR 1=1 /*
Response Code: 200
Response Time: 0.588622 seconds
Response Length: 88462 bytes
SQL Injection test URL: https://owasp.org/www-project-juice-shop/?id=' OR 'a'='a
Response Code: 200
Response Time: 0.531038 seconds
Response Length: 88462 bytes

XSS Summary:
No XSS vulnerabilities detected.

XSS Logs:
No alert found for payload <script>alert('XSS')</script>: Message: no such alert   (Session info:
chrome=127.0.6533.72) Stacktrace: GetHandleVerifier [0x00007FF7BE0A9632+30946]   (No
symbol) [0x00007FF7BE05E3C9]   (No symbol) [0x00007FF7BDF56E09]   (No symbol)
[0x00007FF7BDF41EF4]   (No symbol) [0x00007FF7BDF6A111]   (No symbol)
[0x00007FF7BDF7A6C7]   (No symbol) [0x00007FF7BDFCCB1D]   (No symbol)
[0x00007FF7BDF7A54B]   (No symbol) [0x00007FF7BDFCC813]   (No symbol)
[0x00007FF7BDF9A6E5]   (No symbol) [0x00007FF7BDF9B021]   GetHandleVerifier
[0x00007FF7BE1DF83D+1301229]   GetHandleVerifier [0x00007FF7BE1EBDB7+1351783]

GetHandleVerifier [0x00007FF7BE1E2A03+1313971]   GetHandleVerifier [0x00007FF7BE0DDD06+245
(No symbol) [0x00007FF7BE06758F]   (No symbol) [0x00007FF7BE063804]   (No symbol)
[0x00007FF7BE063992]   (No symbol) [0x00007FF7BE05A3EF]   BaseThreadInitThunk
[0x00007FFD6860257D+29]   RtlUserThreadStart [0x00007FFD6938AF28+40]
No alert found for payload '"><img src=x onerror=alert('XSS')>: Message: no such alert   (Session
info: chrome=127.0.6533.72) Stacktrace: GetHandleVerifier [0x00007FF7BE0A9632+30946]
(No symbol) [0x00007FF7BE05E3C9]   (No symbol) [0x00007FF7BDF56E09]   (No symbol)
[0x00007FF7BDF41EF4]   (No symbol) [0x00007FF7BDF6A111]   (No symbol)
[0x00007FF7BDF7A6C7]   (No symbol) [0x00007FF7BDFCCB1D]   (No symbol)
[0x00007FF7BDF7A54B]   (No symbol) [0x00007FF7BDFCC813]   (No symbol)
[0x00007FF7BDF9A6E5]   (No symbol) [0x00007FF7BDF9B021]   GetHandleVerifier
[0x00007FF7BE1DF83D+1301229]   GetHandleVerifier [0x00007FF7BE1EBDB7+1351783]
GetHandleVerifier [0x00007FF7BE1E2A03+1313971]   GetHandleVerifier [0x00007FF7BE0DDD06+245
(No symbol) [0x00007FF7BE06758F]   (No symbol) [0x00007FF7BE063804]   (No symbol)
[0x00007FF7BE063992]   (No symbol) [0x00007FF7BE05A3EF]   BaseThreadInitThunk
[0x00007FFD6860257D+29]   RtlUserThreadStart [0x00007FFD6938AF28+40]
No alert found for payload <svg/onload=alert('XSS')>: Message: no such alert   (Session info:
chrome=127.0.6533.72) Stacktrace: GetHandleVerifier [0x00007FF7BE0A9632+30946]   (No
symbol) [0x00007FF7BE05E3C9]   (No symbol) [0x00007FF7BDF56E09]   (No symbol)
[0x00007FF7BDF41EF4]   (No symbol) [0x00007FF7BDF6A111]   (No symbol)
[0x00007FF7BDF7A6C7]   (No symbol) [0x00007FF7BDFCCB1D]   (No symbol)
[0x00007FF7BDF7A54B]   (No symbol) [0x00007FF7BDFCC813]   (No symbol)
[0x00007FF7BDF9A6E5]   (No symbol) [0x00007FF7BDF9B021]   GetHandleVerifier
[0x00007FF7BE1DF83D+1301229]   GetHandleVerifier [0x00007FF7BE1EBDB7+1351783]
GetHandleVerifier [0x00007FF7BE1E2A03+1313971]   GetHandleVerifier [0x00007FF7BE0DDD06+245
(No symbol) [0x00007FF7BE06758F]   (No symbol) [0x00007FF7BE063804]   (No symbol)
[0x00007FF7BE063992]   (No symbol) [0x00007FF7BE05A3EF]   BaseThreadInitThunk
[0x00007FFD6860257D+29]   RtlUserThreadStart [0x00007FFD6938AF28+40]

CSRF Summary:
No CSRF vulnerabilities detected.

CSRF Logs:
Error during CSRF test: HTTPSConnectionPool(host='owasp.org', port=443): Read timed out. (read
timeout=10)

DIR Summary:
Directory Traversal Test Results:
Potential Directory Traversal vulnerability detected with payload: ../

DIR Logs:
Directory Traversal test URL: https://owasp.org/www-project-juice-shop//../
Response Code: 200
Response Time: 0.652571 seconds
Response Length: 88462 bytes
Directory Traversal test URL: https://owasp.org/www-project-juice-shop//..\
Response Code: 404
Response Time: 1.00682 seconds

Response Length: 29394 bytes
Directory Traversal test URL: https://owasp.org/www-project-juice-shop///etc/passwd
Response Code: 404
Response Time: 0.912137 seconds
Response Length: 29394 bytes
Directory Traversal test URL: https://owasp.org/www-project-juice-shop//C:\Windows\System32
Response Code: 404
Response Time: 0.905119 seconds
Response Length: 29394 bytes

VER Summary:
No version-based vulnerabilities detected.

VER Logs:
Version-based vulnerability test URL: https://owasp.org/www-project-juice-shop/
Response Code: 200
Response Time: 0.614209 seconds
Response Length: 88462 bytes

Overall Status:
Scan Successful