Security Scan Report

Scan ID: 51
Scanned URL: http://localhost:3000
Timestamp: 2025-04-07 10:57:05

scans

csrf: {'scans': {'CSRFScanner': {'http://localhost:3000': [{'action': 'http://localhost:3000/login', 'method': 'POST', 'severity': 'High', 'form_number': 1, 'csrf_protection': False, 'severity_description': 'Critical CSRF vulnerability. A malicious user can perform actions on behalf of another user.'}]}}}
http: {'scans': {'URLSecurityScanner': {'http://localhost:3000': {'secure': False, 'protocol': 'HTTP', 'severity': 'High', 'severity_description': 'Insecure connection using HTTP. HTTPS is recommended for security.'}, 'http://localhost:3000/login': {'secure': False, 'protocol': 'HTTP', 'severity': 'High', 'severity_description': 'Insecure connection using HTTP. HTTPS is recommended for security.'}}}, 'execution_times': {'http': 0.18}}
sql_injection: {'scans': {'SQLInjectionScanner': {'http://localhost:3000/login': [{'payload': "' OR '1'='1", 'severity': 'High', 'vulnerable': True, 'severity_description': 'SQL Injection is critical and can lead to complete database compromise.'}]}}}
broken_authentication: {'scans': {'BrokenAuthScanner': {'http://localhost:3000/login': {'Overall Severity': 'High', 'Weak Passwords Severity': 'High', 'Session Management Severity': 'High', 'Brute Force Protection Severity': 'High'}}}}

scan_time

2025-04-07 10:57:05

execution_times

http: 0.18