FLAWSTRIKE — DAST ORCHESTRATION

Vulnerability Assessment Report

OWASP ZAP · sqlmap · Nuclei · Nikto — normalized, correlated, and OWASP Top 10:2021 mapped

Target	https://app.example.com
Report ID	Scan #98
Scanners run	zap, sqlmap, nuclei, nikto
Scan completed	—
Scan duration	742.0 seconds
Report generated	2026-11-04 01:39 UTC

Executive Summary

Unique findings	Raw findings	Confirmed by 2+ tools
7	10	2

Risk rating (High / Medium / Low)

High	Medium	Low
3	**2**	**2**

Severity breakdown

Severity	Critical	High	Medium	Low	Info
Count	1	2	2	1	1

Scanner Coverage

Each tool contributes a different slice of the OWASP Top 10; overlap is where multi-tool confirmation happens.

Tool	Raw findings	Status	Duration (s)
zap	5	success	300.0
sqlmap	1	success	300.0

nuclei	1	success	300.0
nikto	3	success	300.0

OWASP Top 10:2021 Coverage

OWASP category	Findings
A01:2021 - Broken Access Control	0
A02:2021 - Cryptographic Failures	0
A03:2021 - Injection	2
A04:2021 - Insecure Design	0
A05:2021 - Security Misconfiguration	4
A06:2021 - Vulnerable and Outdated Components	1
A07:2021 - Identification and Authentication Failures	0
A08:2021 - Software and Data Integrity Failures	0
A09:2021 - Security Logging and Monitoring Failures	0
A10:2021 - Server-Side Request Forgery (SSRF)	0
Unmapped	0

Note: A01:2021 Broken Access Control is the number-one OWASP risk yet cannot be reliably detected by automated DAST tooling — it requires authenticated, business-context manual testing. A near-zero count here is a known blind spot, not proof of security.

Detailed Findings

CRITICAL **1. SQL Injection**

Risk rating	High
OWASP category	A03:2021 - Injection
CWE	CWE-89
Found by	sqlmap, zap (2 tools)
Confidence	High — raised by multi-tool agreement
Location	GET https://app.example.com/search
Parameter	q
Evidence	Demo data: boolean-based blind injection in the q parameter.
Remediation	Use parameterised queries / prepared statements and an allow-list input validation; contextually output-encode to stop XSS. Never build queries or markup from raw user input.

HIGH	2. Cross Site Scripting (Reflected)
Risk rating	High
OWASP category	A03:2021 - Injection
CWE	CWE-79
Found by	zap (1 tool)
Confidence	Medium
Location	GET https://app.example.com/profile
Parameter	name
Evidence	Demo data: the name parameter is reflected without encoding.
Remediation	Use parameterised queries / prepared statements and an allow-list input validation; contextually output-encode to stop XSS. Never build queries or markup from raw user input.

HIGH	3. Exposed Configuration File
Risk rating	High
OWASP category	A05:2021 - Security Misconfiguration
CWE	CWE-538
Found by	nuclei (1 tool)
Confidence	High
Location	GET https://app.example.com/config.bak
Parameter	—
Evidence	Demo data: a backup configuration file is publicly readable.
Remediation	Harden defaults: remove sample apps, disable directory listing, set security headers, restrict HTTP methods, and keep configuration under review.

MEDIUM	4. Content Security Policy Header Not Set
Risk rating	Medium
OWASP category	A05:2021 - Security Misconfiguration
CWE	CWE-693
Found by	zap, nikto (2 tools)
Confidence	High — raised by multi-tool agreement
Location	GET https://app.example.com/
Parameter	—
Evidence	Demo data: the response has no Content-Security-Policy header.

Remediation	Harden defaults: remove sample apps, disable directory listing, set security headers, restrict HTTP methods, and keep configuration under review.

MEDIUM 5. Outdated Server Software

Risk rating	Medium
OWASP category	A06:2021 - Vulnerable and Outdated Components
CWE	CWE-1104
Found by	nikto (1 tool)
Confidence	Medium
Location	GET https://app.example.com/
Parameter	—
Evidence	Demo data: the Server header reports an old version.
Remediation	Inventory all components and versions, remove unused dependencies, and patch known-vulnerable software promptly against a CVE feed.

LOW 6. Cookie Without Secure Flag

Risk rating	Low
OWASP category	A05:2021 - Security Misconfiguration
CWE	CWE-614
Found by	zap (1 tool)
Confidence	High
Location	GET https://app.example.com/login
Parameter	—
Evidence	Demo data: the session cookie is set without the Secure flag.
Remediation	Harden defaults: remove sample apps, disable directory listing, set security headers, restrict HTTP methods, and keep configuration under review.

INFO 7. Server Version Disclosure

Risk rating	Low
OWASP category	A05:2021 - Security Misconfiguration
CWE	CWE-200
Found by	nikto (1 tool)
Confidence	Medium
Location	GET https://app.example.com/
Parameter	—

Evidence	Demo data: the Server header discloses version details.
Remediation	Harden defaults: remove sample apps, disable directory listing, set security headers, restrict HTTP methods, and keep configuration under review.

Generated by FlawStrike, a security testing platform. Only scan systems you own or are explicitly authorised to test. Automated scanning cannot establish business authorisation or reliably detect broken access control.