AURA - OFFENSIVE INTELLIGENCE

CONFIDENTIAL | Generated: 2026-03-01 16:39:01

Mission Executive Summary

Mission Target Profile	**Consolidated Domain Audit**
Total Assets Analyzed	**1**
Critical Attack Paths Identified	**0**
Total Vulnerabilities Detected	**6**
Current Security Stance	**■ AT RISK**

Aura Intelligence Context (Threat Landscape)

This assessment utilizes the Ghost v4 Neural Engine to evaluate the external attack surface. Our analysis includes deep-reconnaissance across subdomains, visual fingerprinting of front-end technologies, and entropy-based secret hunting. The current mission scope focused on identifying immediate high-impact entry points and sensitive data leaks.

Vulnerability Breakdown

Windows Service	1
Information Disclosure	4
SQL Injection	1

Detailed Mission Analytics

Target: testasp.vulnweb.com

Risk Score: 8.8 | Priority: HIGH

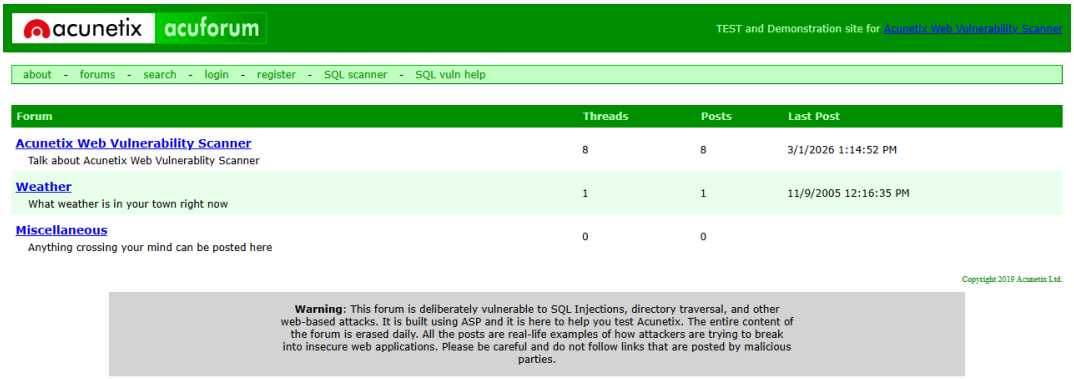
Aura Intelligence Methodology

Reconnaissance	Passive discovery of subdomains, IP space, and DNS records using global OSINT and rapid-fire active resolution.

Intelligence	Aggregating threat intelligence from Shodan, Censys, and VirusTotal to map the target's attack surface and WAF presence.
Visual Analysis	Deep-learning based visual inspection of web interfaces to identify technology stacks and sensitive entry points.
Vulnerability Discovery	Humanized DAST routines combined with entropy-based secret hunting and automated CVE correlation.
Exploitation	Context-aware automated exploitation and iterative AI-driven debugging of zero-day proof-of-concepts.

Intelligence Coverage Indicators

- Shodan: ACTIVE
- AlienVault OTX: MISSING KEY
- GreyNoise: ACTIVE
- VirusTotal: ACTIVE
- Censys: MISSING KEY



Finding Identification & Business Impact	Type	MITRE ATT&CK	CVSS / Sev

Service Fingerprint on 44.238.29.244:80 | Banner: 'HTTP/1.1 200 OK Content-Length: 701 Content-Type: text/html Last-Modified: Mon, 16 Nov 2020 14:34:05 GMT Accept-Rang' | Version fingerprinting for patch gap analysis *Business Impact:* Potential security compromise. **[REMEDIATION]:** Standard security patching required. **MITRE ATT&CK:** None	Windows Service	A00:2021-Unknown	MEDIUM
Hidden Path Discovered: http://testasp.vulnweb.com/robots.txt *Business Impact:* Exposure of system metadata or internal file structures which could aid an attacker in identifying high-value targets. **[REMEDIATION]:** Standard security patching required. **MITRE ATT&CK:** None	Information Disclosure	A01:2021-Broken Access Control	MEDIUM
Hidden Path Discovered: http://testasp.vulnweb.com/images *Business Impact:* Exposure of system metadata or internal file structures which could aid an attacker in identifying high-value targets. **[REMEDIATION]:** Standard security patching required. **MITRE ATT&CK:** None	Information Disclosure	A01:2021-Broken Access Control	MEDIUM
Hidden Path Discovered: http://testasp.vulnweb.com/templates *Business Impact:* Exposure of system metadata or internal file structures which could aid an attacker in identifying high-value targets. **[REMEDIATION]:** Standard security patching required. **MITRE ATT&CK:** None	Information Disclosure	A01:2021-Broken Access Control	MEDIUM
Hidden Path Discovered: http://testasp.vulnweb.com/cgi-bin *Business Impact:* Exposure of system metadata or internal file structures which could aid an attacker in identifying high-value targets. **[REMEDIATION]:** Standard security patching required. **MITRE ATT&CK:** None	Information Disclosure	A01:2021-Broken Access Control	MEDIUM

[OCR Visual Intel] Page text contains 'sql injection', confirming this is a vulnerable target. *Business Impact:* Unauthorized database access, data theft, or complete system compromise. **[REMEDIATION]:** Standard security patching required. **MITRE ATT&CK:** None	SQL Injection	A03:2021-Injection	HIGH

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:
- **3-Stage AI Escalation:** Audited 9 potential parameters/routes on this asset.
- **Blind Detection:** All inputs verified for Timing-based SQLi (5000ms threshold).
- **WAF Evasion:** Multi-layered encoding and polymorphism applied to all probes.
- **AI Engine:** Behavioral reasoning verified by Gemini-1.5-Flash (Ghost v5).