

# AURA - OFFENSIVE INTELLIGENCE

CONFIDENTIAL | Generated: 2026-03-01 17:00:10

## 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	<span style="color: red;">■ AT RISK</span>

### ***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.
----------------	---

<b>Intelligence</b>	Aggregating threat intelligence from Shodan, Censys, and VirusTotal to map the target's attack surface and WAF presence.
<b>Visual Analysis</b>	Deep-learning based visual inspection of web interfaces to identify technology stacks and sensitive entry points.
<b>Vulnerability Discovery</b>	Humanized DAST routines combined with entropy-based secret hunting and automated CVE correlation.
<b>Exploitation</b>	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**

The screenshot shows a forum interface with the following structure:

- Header:** acunetix acuforum TEST and Demonstration site for Acunetix Web Vulnerability Scanner
- Navigation Bar:** about - forums - search - login - register - SQL scanner - SQL vuln help
- Forum Categories:**
  - Acunetix Web Vulnerability Scanner:** Talk about Acunetix Web Vulnerability Scanner (Threads: 64, Posts: 64, Last Post: 3/1/2026 1:47:03 PM)
  - Weather:** What weather is in your town right now (Threads: 1, Posts: 1, Last Post: 11/9/2005 12:16:35 PM)
  - Miscellaneous:** Anything crossing your mind can be posted here (Threads: 0, Posts: 0)
- Warning Message:** A gray box contains the following text:
 

**Warning:** This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.
- Copyright:** Copyright 2019 Acunetix Ltd.

Finding Identification & Business Impact	Type	MITRE ATT&CICVSS / Sev
--	------	------------------------

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

<p><b>[OCR Visual Intel]</b> Page text contains 'sql injection', confirming this is a vulnerable target.</p> <p><i>Business Impact:</i> Unauthorized database access, data theft, or complete system compromise.</p> <p><b>[REMEDIATION]:</b> Standard security patching required.  <b>MITRE ATT&amp;CK:</b> None</p>	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).