

AURA - OFFENSIVE INTELLIGENCE

CONFIDENTIAL | Generated: 2026-03-01 20:52:16

Mission Executive Summary

Mission Target Profile	Consolidated Domain Audit
Total Assets Analyzed	1
Critical Attack Paths Identified	0
Total Vulnerabilities Detected	10
Current Security Stance	■ VULNERABLE

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

Web Server (Systemic Pattern — 9 Instances)	1@ /Service Fingerprint on 54.82.22.214:80 Banner
Web Server	1
Information Disclosure	8

Detailed Mission Analytics

Target: zero.webappsecurity.com

Risk Score: 0 | Priority: LOW

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**

Zero Bank

[HOME](#)
[ONLINE BANKING](#)
[FEEDBACK](#)

Online Banking
Welcome to Zero Online Banking. Zero provides a greener and more convenient way to manage your money. Zero enables you to check your account balances, pay your bills, transfer money, and keep detailed records of your transactions, wherever there is an internet connection.

Online Banking
Click the button below to view online banking features.

Checking Account Activity
Use Zero to view the most up-to-date listings of your deposits, withdrawals, interest payments, and a number of other useful transactions.

Transfer Funds
Use Zero to safely and securely transfer funds between accounts. There is no hold placed on online money transfers, so your funds are available when you need them.

My Money Map
Use Zero to set up and monitor your personalized money map. A money map is an easy-to-use online tool that helps you manage your finances efficiently. With Money Map, you can create a budget, sort

Finding Identification & Business Impact

Type

MITRE ATT&CKVSS / Sev

<p>[■ PREDATOR ALERT] SYSTEMIC PATTERN DETECTED: 'Web Server' was identified across 9 separate endpoints residing under root /Service Fingerprint on 54.82.22.214:80 Banner: 'HTTP. This indicates a framework-wide or server-level misconfiguration.</p> <p>■ MOST DANGEROUS PATHS (EXPOSED):</p> <ul style="list-style-type: none"> • Service Fingerprint on 54.82.22.214:80 Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 14:06:53 G • Service Fingerprint on 54.82.22.214:80 Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 14:19:10 G • Service Fingerprint on 54.82.22.214:80 Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 15:45:29 G • Service Fingerprint on 54.82.22.214:80 Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 16:20:23 G • Service Fingerprint on 54.82.22.214:80 Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 16:37:39 G • Service Fingerprint on 54.82.22.214:80 Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 16:47:23 G • Service Fingerprint on 54.82.22.214:80 Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 17:09:58 G • Service Fingerprint on 54.82.22.214:80 Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 17:11:49 G <p>... and 1 more paths.</p> <p><i>Business Impact:</i> This finding type (Web Server) was detected across 9 endpoints under '/Service Fingerprint on 54.82.22.214:80 Banner: 'HTTP', indicating a systemic misconfiguration rather than an isolated case. The attack surface is significantly larger than a single vulnerability.</p> <p>[REMEDIATION]: Implement a global response-level header policy and path-based access controls for all instances.</p> <p>MITRE ATT&CK: T1592 — Gather Victim Information</p> <p>■ PATCH PRIORITY: HIGH</p>	Web Server (Systemic Pattern)	A00:2021-Unknown	MEDIUM
<p>Service Fingerprint on 54.82.22.214:8080 Banner: 'HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Cache-Control: no-cache, max-age=0, must-revalidate, no-store Content-Type:' Check version for known CVEs (mod_cgi, etc.)</p> <p><i>Business Impact:</i> Potential security compromise.</p> <p>[REMEDIATION]: Standard security patching required.</p> <p>MITRE ATT&CK: None</p>	Web Server	A00:2021-Unknown	MEDIUM

<p>Hidden Path Discovered: http://zero.webappsecurity.com/admin</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>[REMEDIATION]: Standard security patching required. MITRE ATT&CK: None</p>	Information Disclosure	A01:2021-Broken Access Control	MEDIUM
<p>Hidden Path Discovered: http://zero.webappsecurity.com:8080/admin</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>[REMEDIATION]: Standard security patching required. MITRE ATT&CK: None</p>	Information Disclosure	A01:2021-Broken Access Control	MEDIUM
<p>Hidden Path Discovered: http://zero.webappsecurity.com/manager</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>[REMEDIATION]: Standard security patching required. MITRE ATT&CK: None</p>	Information Disclosure	A01:2021-Broken Access Control	MEDIUM
<p>Hidden Path Discovered: http://zero.webappsecurity.com:8080/manager</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>[REMEDIATION]: Standard security patching required. MITRE ATT&CK: None</p>	Information Disclosure	A01:2021-Broken Access Control	MEDIUM
<p>Hidden Path Discovered: http://zero.webappsecurity.com/docs</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>[REMEDIATION]: Standard security patching required. MITRE ATT&CK: None</p>	Information Disclosure	A01:2021-Broken Access Control	MEDIUM

Hidden Path Discovered: http://zero.webappsecurity.com:8080/docs <i>Business Impact:</i> 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://zero.webappsecurity.com/server-status <i>Business Impact:</i> 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://zero.webappsecurity.com:8080/server-status <i>Business Impact:</i> 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

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:

- **3-Stage AI Escalation:** Audited 13 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).