AURA - OFFENSIVE INTELLIGENCE

CONFIDENTIAL | Generated: 2026-03-01 18:54:35

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	4
Information Disclosure	6

Detailed Mission Analytics

Target: zero.webappsecurity.com

Risk Score: 0 | Priority: LOW

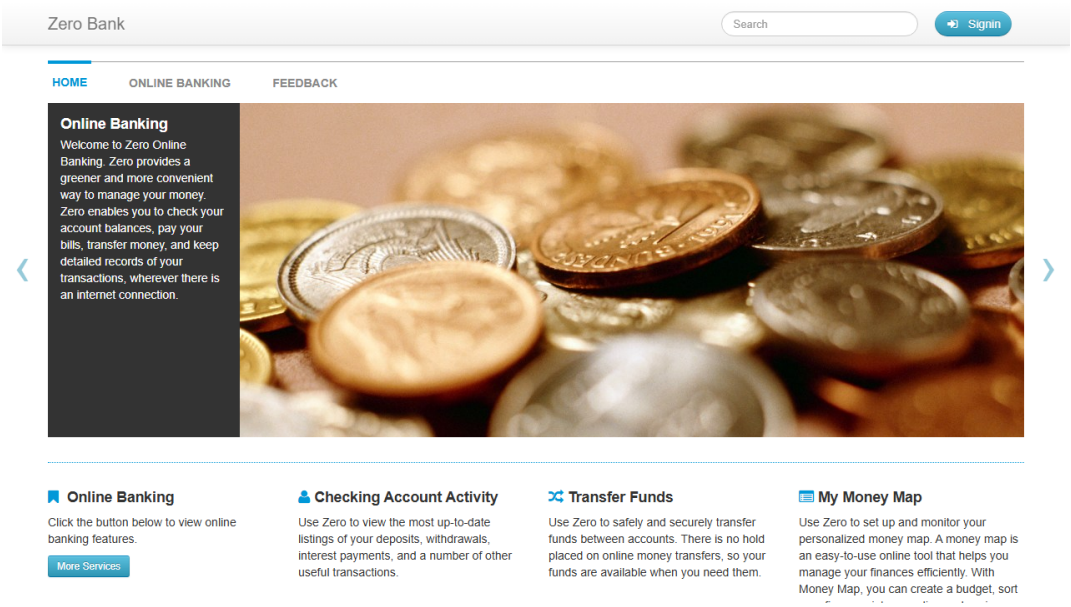
Aura Intelligence Methodology

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



Finding Identification & Business Impact	Type	MITRE ATT&CK	CVSS / Sev
Service Fingerprint on 54.82.22.214:80 | Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 14:06:53 GMT Server: Apache-Coyote/1.1 Access-Control-Allow-Origin: * Cache-C' | Check version for known CVEs (mod_cgi, etc.) *Business Impact:* Potential security compromise. **[REMEDIATION]:** Standard security patching required. **MITRE ATT&CK:** None	Web Server	A00:2021-Unknown	MEDIUM

Service Fingerprint on 54.82.22.214:80 | Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 14:19:10 GMT Server: Apache-Coyote/1.1 Access-Control-Allow-Origin: * Cache-C' | Check version for known CVEs (mod_cgi, etc.) *Business Impact:* Potential security compromise. **[REMEDIATION]:** Standard security patching required. **MITRE ATT&CK:** None	Web Server	A00:2021-Unknown	MEDIUM
Service Fingerprint on 54.82.22.214:80 | Banner: 'HTTP/1.1 200 OK Date: Sun, 01 Mar 2026 15:45:29 GMT Server: Apache-Coyote/1.1 Access-Control-Allow-Origin: * Cache-C' | Check version for known CVEs (mod_cgi, etc.) *Business Impact:* Potential security compromise. **[REMEDIATION]:** Standard security patching required. **MITRE ATT&CK:** None	Web Server	A00:2021-Unknown	MEDIUM
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.) *Business Impact:* Potential security compromise. **[REMEDIATION]:** Standard security patching required. **MITRE ATT&CK:** None	Web Server	A00:2021-Unknown	MEDIUM
Hidden Path Discovered: http://zero.webappsecurity.com/admin *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://zero.webappsecurity.com:8080/admin *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://zero.webappsecurity.com/manager *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://zero.webappsecurity.com:8080/manager *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://zero.webappsecurity.com/docs *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://zero.webappsecurity.com:8080/docs *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

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).