AURA - OFFENSIVE INTELLIGENCE

CONFIDENTIAL | Generated: 2026-02-28 12:31:03

Mission Executive Summary

Mission Target Profile	**Consolidated Domain Audit**
Total Assets Analyzed	**10**
Critical Vulnerabilities	**0**
Current Security Stance	SECURE

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.

Detailed Mission Analytics

Target: www.riva-jo.me

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: BYPASSED
- AlienVault OTX: BYPASSED
- GreyNoise: BYPASSED
- VirusTotal: BYPASSED
- Censys: BYPASSED

[✔] No significant vulnerabilities or sensitive leaks discovered for this asset in this mission phase.

Target: dev.riva-jo.me

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: BYPASSED
- AlienVault OTX: BYPASSED
- GreyNoise: BYPASSED
- VirusTotal: BYPASSED
- Censys: BYPASSED

[✔] No significant vulnerabilities or sensitive leaks discovered for this asset in this mission phase.

Target: api.riva-jo.me

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: BYPASSED
- AlienVault OTX: BYPASSED
- GreyNoise: BYPASSED
- VirusTotal: BYPASSED
- Censys: BYPASSED

[✔] No significant vulnerabilities or sensitive leaks discovered for this asset in this mission phase.

Target: staging.riva-jo.me

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: BYPASSED
- AlienVault OTX: BYPASSED
- GreyNoise: BYPASSED
- VirusTotal: BYPASSED
- Censys: BYPASSED

[✔] No significant vulnerabilities or sensitive leaks discovered for this asset in this mission phase.

Target: admin.riva-jo.me

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: BYPASSED
- AlienVault OTX: BYPASSED
- GreyNoise: BYPASSED
- VirusTotal: BYPASSED
- Censys: BYPASSED

[✔] No significant vulnerabilities or sensitive leaks discovered for this asset in this mission phase.

Target: vpn.riva-jo.me

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: BYPASSED
- AlienVault OTX: BYPASSED
- GreyNoise: BYPASSED
- VirusTotal: BYPASSED
- Censys: BYPASSED

[✔] No significant vulnerabilities or sensitive leaks discovered for this asset in this mission phase.

Target: mail.riva-jo.me

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: BYPASSED
- AlienVault OTX: BYPASSED
- GreyNoise: BYPASSED
- VirusTotal: BYPASSED
- Censys: BYPASSED

[✔] No significant vulnerabilities or sensitive leaks discovered for this asset in this mission phase.

Target: blog.riva-jo.me

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: BYPASSED

• AlienVault OTX: BYPASSED

• GreyNoise: BYPASSED

• VirusTotal: BYPASSED

• Censys: BYPASSED

[✔] No significant vulnerabilities or sensitive leaks discovered for this asset in this mission phase.

Target: test.riva-jo.me

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: BYPASSED

• AlienVault OTX: BYPASSED

• GreyNoise: BYPASSED

• VirusTotal: BYPASSED

• Censys: BYPASSED

[✔] No significant vulnerabilities or sensitive leaks discovered for this asset in this mission phase.

Target: riva-jo.me

Risk Score: 0 **|** Priority: MEDIUM

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: BYPASSED
- AlienVault OTX: BYPASSED
- GreyNoise: BYPASSED
- VirusTotal: BYPASSED
- Censys: BYPASSED

[✔] No significant vulnerabilities or sensitive leaks discovered for this asset in this mission phase.