AURA - OFFENSIVE INTELLIGENCE

CONFIDENTIAL | Generated: 2026-02-28 14:37:20

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 critical vulnerabilities discovered in this phase.

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:

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

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 critical vulnerabilities discovered in this phase.

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:
- **3-Stage AI Escalation:** Audited 3 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).

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 critical vulnerabilities discovered in this phase.

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:
- **3-Stage AI Escalation:** Audited 3 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).

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	• VirusTotal: BYPASSED
• AlienVault OTX: BYPASSED	• Censys: BYPASSED
• GreyNoise: BYPASSED	

[✔] No critical vulnerabilities discovered in this phase.

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:
- **3-Stage AI Escalation:** Audited 3 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).

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 critical vulnerabilities discovered in this phase.

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:
- **3-Stage AI Escalation:** Audited 3 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).

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 critical vulnerabilities discovered in this phase.

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:

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

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 critical vulnerabilities discovered in this phase.

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:
- **3-Stage AI Escalation:** Audited 3 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).

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

[✔] No critical vulnerabilities discovered in this phase.

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:
- **3-Stage AI Escalation:** Audited 3 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).

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 critical vulnerabilities discovered in this phase.

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:

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

Target: riva-jo.me

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

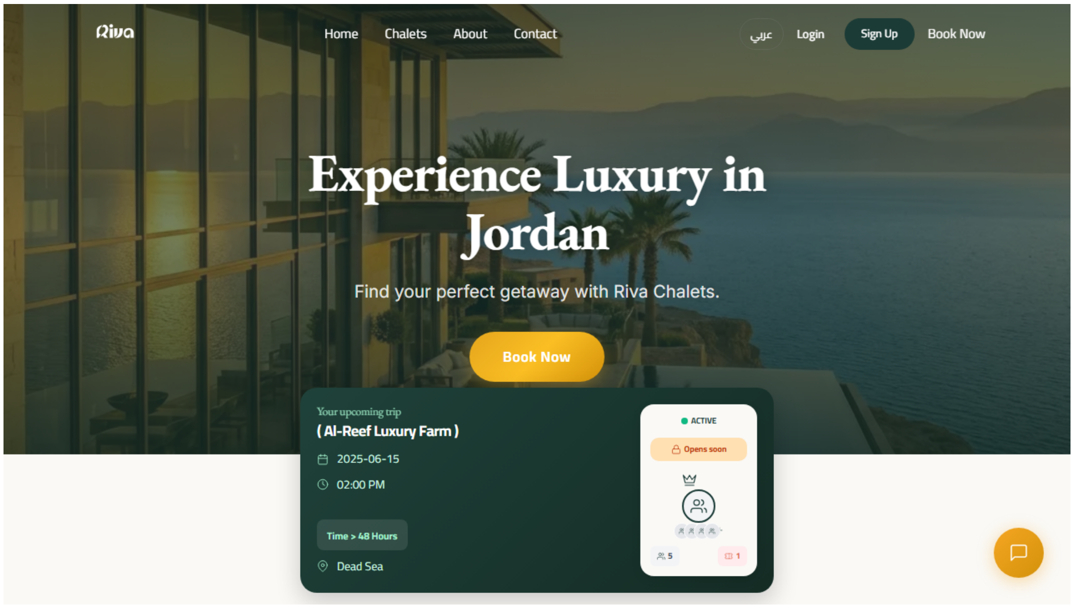
Aura Intelligence Methodology

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



Experience Luxury in Jordan

Find your perfect getaway with Riva Chalets.

Your upcoming trip
(Al-Reef Luxury Farm)
2025-06-15
02:00 PM
Time > 48 Hours
Dead Sea

[✔] No critical vulnerabilities discovered in this phase.

Aura AI Diagnostic History (Proof of Audit)

The following assets were subjected to Weaponized AI Behavioral Analysis:
- **3-Stage AI Escalation:** Audited 3 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).