Web Application Vulnerability Reconnaissance

Report on

www.halisans.com (66.29.153.49)

Prepared By: Aliu B. Sanusi

Date : March 3, 2025

1. Executive Summary

This report provides an assessment of potential vulnerabilities discovered during the reconnaissance phase for the target domain **www.halisans.com**. The analysis focuses on domain enumeration, network mapping, and identification of misconfigurations or exposed services that could be exploited by malicious actors.

2. Scope of Assessment

- **Target Domain:** www.halisans.com
- **Assessment Type:** Passive and Active Reconnaissance
- **Tools Used:** Fierce, Wapiti, DNSRecon, WAFW00F, WHOIS, and DIG
- **Date of Assessment:** March 3, 2025

3. Methodology

The following reconnaissance techniques were used to gather information:

- **DNS Enumeration:** Identified authoritative name servers and possible misconfigurations.
- **Subdomain Discovery:** Attempted to enumerate subdomains associated with the target.
- **WHOIS Lookup:** Gathered domain registration and ownership details.
- **Port Scanning:** Identified open ports and exposed services
- **Service Fingerprinting:** Determined running services and versions.
- **Web Vulnerability Scanning:** Analyzed potential web security issues.

4. Findings

4.1 DNS Enumeration (Fierce Tool Output)

- **Name Servers Identified:**
  - dns1.registrar-servers.com
  - dns2.registrar-servers.com
- **SOA Record:**
  - Primary Server: dns1.registrar-servers.com
  - IP Address: 156.154.132.200
- **Zone Transfer:** Failed (No misconfiguration found)
- **Wildcard Records:** Not enabled (reduces attack surface)

4.2 Web Security Scan (Wapiti)

Findings:

- **Content Security Policy (CSP) Missing:** No CSP is set, making the site vulnerable to XSS and data injection attacks.
- **X-Frame-Options Missing:** The site can be embedded in an iframe, leading to clickjacking risks.
- **X-XSS-Protection Missing:** No built-in XSS protection enabled in browsers.
- **X-Content-Type-Options Missing:** Possible MIME-type sniffing attacks.
- **Strict-Transport-Security (HSTS) Missing:** HTTPS enforcement is not enabled.
- **7 URLs/forms discovered:** Further manual analysis needed for potential SQL Injection, XSS, SSRF, or command execution risks.
- **Detailed Wapiti report available:** generated_report/www.halisans.com_03032025_0320.html

4.3 DNS and WHOIS Information

WHOIS Details:

- **Registrar:** Namecheap
- **Registered On:** September 16, 2024
- **Expiration Date:** September 16, 2025
- **Name Servers:**
  - dns1.registrar-servers.com
  - dns2.registrar-servers.com

DNS Records:

- **A Record:** 66.29.153.49
- **MX Records (Zoho Mail):**

    - mx.zoho.eu (185.230.212.166)
    - mx2.zoho.eu (185.230.214.166)
    - mx3.zoho.eu (185.230.212.166)
- **SPF Record:** v=spf1 include:zohomail.eu ~all (Only Zoho Mail is authorized to send emails)
- **DNSSEC:** Not configured (Risk of DNS spoofing).
- **SRV Records:** None found.

4.4 Web Application Firewall (WAF) Detection

- **LiteSpeed WAF detected:** Provides basic protection, but requires configuration review to prevent bypass techniques.

5. Risk Analysis

Finding	Description	Risk	Mitigation Recommendation
DNS Enumeration (Fierce Tool Output)			
Name Servers Identified	dns1.registrar-servers.com, dns2.registrar-servers.com	Moderate risk: Knowing name servers can aid attackers in further reconnaissance.	Consider using hidden or third-party DNS providers for increased security.
SOA Record	Primary Server: dns1.registrar-servers.com, IP Address: 156.154.132.200	Moderate risk: Exposes information about the DNS server, making it a potential target.	Ensure that only necessary information is exposed in the SOA record.
Zone Transfer	Failed	Low risk: No misconfiguration found, zone transfer is not allowed.	No action required, zone transfer is correctly restricted.
Wildcard Records	Not enabled	Low risk: Reduces attack surface as wildcard DNS records are not in use.	No action required, this is a secure configuration.
Web Security Scan (Wapiti)			
CSP Missing	No Content Security Policy (CSP) set	High risk: The site is vulnerable to XSS and data injection attacks.	Implement a strict Content Security Policy (CSP) to prevent script injections.
X-Frame-Options Missing	The site can be embedded in an iframe, leading to clickjacking risks.	High risk: Potential for clickjacking attacks.	Implement X-Frame-Options with the 'DENY' or 'SAMEORIGIN' directive.
X-XSS-Protection Missing	No built-in XSS protection enabled in browsers.	High risk: Site is susceptible to cross-site scripting (XSS) attacks.	Enable X-XSS-Protection to protect against reflected XSS attacks.
X-Content-Type-Options Missing	Missing protection against MIME-type sniffing.	Moderate risk: Possible MIME-type sniffing attacks could	Implement X-Content-Type-Options: nosniff to

		result in content misinterpretation.	prevent MIME-type sniffing.
HSTS Missing	HTTPS enforcement is not enabled.	High risk: The site is vulnerable to man-in-the-middle attacks and session hijacking.	Implement HTTP Strict Transport Security (HSTS) to enforce HTTPS connections.
URLs/Forms Discovered	7 URLs/forms discovered, manual analysis needed for vulnerabilities like SQL Injection, XSS, SSRF, or command execution.	High risk: These URLs/forms might have hidden vulnerabilities that attackers can exploit.	Conduct thorough manual testing and apply necessary input sanitization and validation to prevent common web vulnerabilities.
DNS and WHOIS Information			
DNSSEC Not Configured	No DNSSEC configured	High risk: DNS spoofing or man-in-the-middle attacks could compromise DNS integrity.	Configure DNSSEC to secure DNS lookups and prevent DNS spoofing attacks.
Web Application Firewall (WAF) Detection			
LiteSpeed WAF Detected	Provides basic protection but requires configuration review to prevent bypass techniques.	Moderate risk: Basic protection may be bypassed if not configured properly.	Review and configure the WAF settings to prevent known bypass techniques, ensuring it provides robust protection.

6. Security Recommendations

Immediate Actions:

1. **Implement Security Headers:**
   - Set Content-Security-Policy to prevent XSS and data injection.
   - Add X-Frame-Options: DENY to mitigate clickjacking.
   - Enable Strict-Transport-Security (HSTS) to enforce HTTPS.
   - Set X-XSS-Protection: 1; mode=block to enhance XSS protection.
   - Enable X-Content-Type-Options: nosniff to prevent MIME-type sniffing.
2. **Review and Harden LiteSpeed WAF:**
   - Assess firewall rule configuration.
   - Conduct penetration testing to identify potential bypass methods.
3. **Enable DNSSEC:**
   - Protect against DNS spoofing and cache poisoning attacks.
4. **Perform Further Security Testing:**
   - Conduct a **directory brute-force attack** using tools like Gobuster or Dirb to check for exposed sensitive files.
   - Manually inspect **Wapiti results** for SQL Injection, XSS, SSRF, or command execution vulnerabilities.
   - Run **TLS/SSL security tests** using tools like SSL Labs.

7. Conclusion

The website **halisans.com** currently has multiple security misconfigurations that could expose it to cyber threats. Immediate action is recommended to enhance its security posture, starting with implementing security headers, reviewing WAF settings, enabling DNSSEC, and conducting further security assessments.