

Passive Reconnaissance Scan Report

Scan target : Halisans.com (66.29.153.49)

Date of recon: 20 Jan 2026

**Cybersecurity Analyst
Onwusa Precious**

Scope: halisans.com and publicly resolvable subdomains only (passive OSINT).

Out-of-scope: Active vulnerability exploitation, authenticated access and service disruption, rate-aggressive crawling.

Executive Summary

- The target domain resolves and serves a public website with recent content.
- This report enumerates: WHOIS/RDAP, authoritative DNS data, HTTPS surface (at a high level), presence of a WAF/CDN (fingerprinted passively) and open-source footprint across common OSINT sources.
- No intrusive scans were performed; all findings are from passive lookups and single-request fetches of public pages.

Methodology (Passive Only)

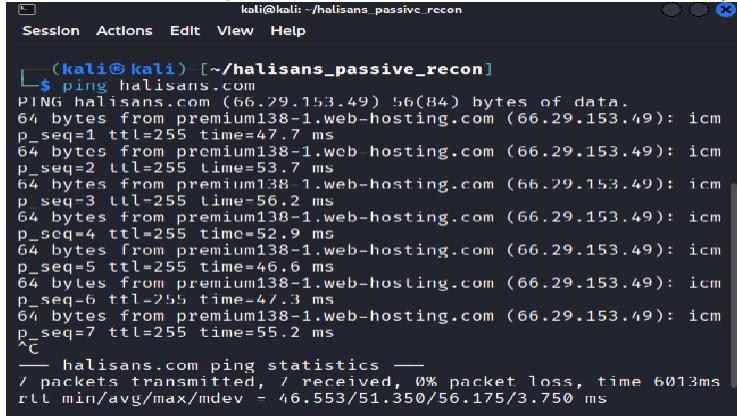
Tools & Modes

- **whois / RDAP:** Registration & registrar metadata
- **dig, host, dnsrecon:** Passive DNS lookups (A/AAAA, NS, MX, TXT/SOA/CAA where present) via public resolvers.
- **waf00f:** Single HTTP(S) request fingerprint (headers/body markers) to infer WAF/CDN; *no evasion, no burst*.
- **SpiderFoot (SF):** *Passive modules only* (DNS, CT logs, WHOIS, netblocks, leak/site mentions, social).
- **Wapiti:** *Listing only* and passive banner/headers check.
- **OSINT Framework:** As a directory to guide passive pivoting, CT logs, public paste sites, reputation lists, search operators.

Findings

3.1 Public Web Presence (Landing Page)

- **Site reachable:** <https://halisans.com/> returns content; homepage shows recent posts.



A screenshot of a terminal window titled "kali@kali: ~/halisans_passive_recon". The window shows the command "ping halisans.com" being run. The output displays several ICMP echo requests sent to the IP address 66.29.153.49, which is the IP of premium138-1.web-hosting.com. The results show TTL values ranging from 255 to 56, and round-trip times (time) between 47.7 ms and 55.2 ms. The terminal also shows the ping statistics at the bottom, indicating 7 packets transmitted, 0 received, 0% packet loss, and a time of 6013ms.

```
(kali㉿kali) [~/halisans_passive_recon]
$ ping halisans.com
PING halisans.com (66.29.153.49) 56(84) bytes of data.
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp
p_seq=1 ttl=255 time=47.7 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp
p_seq=2 ttl=255 time=53.7 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp
p_seq=3 ttl=255 time=56.2 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp
p_seq=4 ttl=255 time=52.9 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp
p_seq=5 ttl=255 time=46.6 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp
p_seq=6 ttl=255 time=47.3 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp
p_seq=7 ttl=255 time=55.2 ms
^C
--- halisans.com ping statistics ---
7 packets transmitted, 0 received, 0% packet loss, time 6013ms
rtt min/avg/max/mdev = 46.553/51.350/56.175/3.750 ms
```

3.2 Registration (WHOIS)

- **Registrar / Dates:** Use ICANN RDAP as the primary source of truth (GDPR-redacted where applicable). Query via ICANN Lookup and registrar RDAP.

```

kali@kali: ~/halisans_passive_recon
Session Actions Edit View Help
(kali㉿kali)-[~/halisans_passive_recon]
$ whois halisans.com
Domain Name: HALISANS.COM
Registry Domain ID: 2917253114_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2025-08-24T11:14:13Z
Creation Date: 2024-09-16T04:57:11Z
Registry Expiry Date: 2026-09-16T04:57:11Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/e
pp#clientTransferProhibited
Name Server: DNS1.REGISTRAR-SERVERS.COM
Name Server: DNS2.REGISTRAR-SERVERS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://w
ww.icann.org/wicf/
>>> Last update of whois database: 2026-01-19T19:09:42Z <<<

```

- vulnerability search against **Namecheap**, as a web application and domain registrar, was performed to identify any publicly disclosed CVEs directly associated with its services or infrastructure. By querying the CVE.org database using “Namecheap” as a keyword, the intent was to determine whether reported vulnerabilities affected Namecheap systems themselves or referenced Namecheap in a supporting or mitigation role.

CVE-2024-38537 PUBLISHED

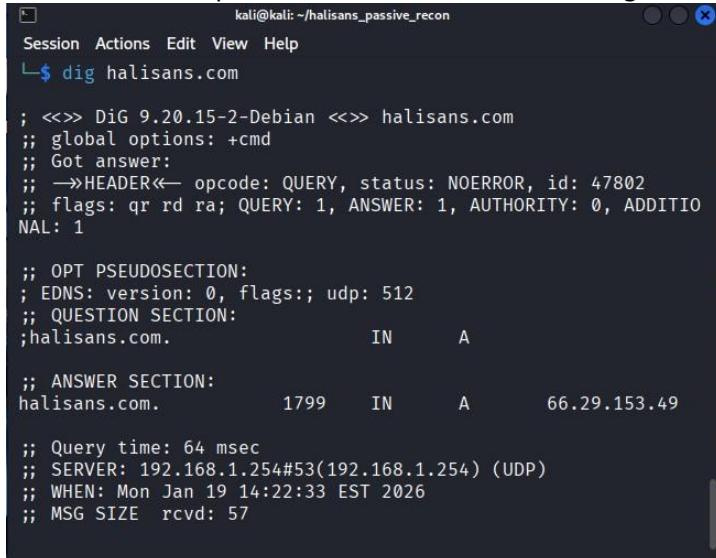
[View JSON](#) | [User Guide](#)

[Collapse all](#)

Required CVE Record Information

CNA: GitHub (maintainer security advisories)	
Published:	2024-07-02
Updated:	2024-07-02
Title: Inclusion of Untrusted polyfill.io Code Vulnerability in fides.js	
Description <p>Fides is an open-source privacy engineering platform. `fides.js`, a client-side script used to interact with the consent management features of Fides, used the `polyfill.io` domain in a very limited edge case, when it detected a legacy browser such as IE11 that did not support the fetch standard. Therefore it was possible for users of legacy, pre-2017 browsers who navigate to a page serving `fides.js` to download and execute malicious scripts from the `polyfill.io` domain when the domain was compromised and serving malware. No exploitation of `fides.js` via `polyfill.io` has been identified as of time of publication. The vulnerability has been patched in Fides version `2.39.1`. Users are advised to upgrade to this version or later to secure their systems against this threat. On Thursday, June 27, 2024, Cloudflare and Namecheap intervened at a domain level to ensure `polyfill.io` and its subdomains could not resolve to the compromised service, rendering this vulnerability unexploitable. Prior to the domain level intervention, there were no server-side workarounds and the confidentiality, integrity, and availability impacts of this vulnerability were high. Clients could ensure they were not affected by using a modern browser that supported the fetch standard.</p>	

- **Name servers:** Capture NS from RDAP and confirm against `dig` NS.



```

Session Actions Edit View Help
└$ dig halisans.com

; <>> DiG 9.20.15-2-Debian <>> halisans.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 47802
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;halisans.com.           IN      A

;; ANSWER SECTION:
halisans.com.        1799    IN      A       66.29.153.49

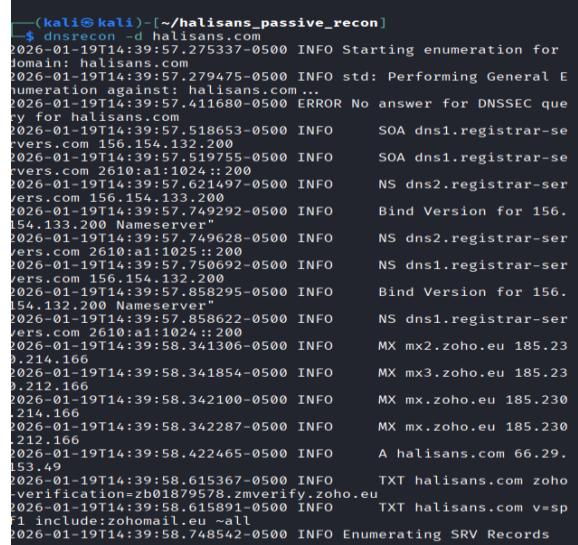
;; Query time: 64 msec
;; SERVER: 192.168.1.254#53(192.168.1.254) (UDP)
;; WHEN: Mon Jan 19 14:22:33 EST 2026
;; MSG SIZE rcvd: 57

```

3.3 DNS Surface (A/AAAA, NS, MX, TXT, SOA, CAA)

- **Records collected passively:**

- `A/AAAA` for apex and `www`.
- `NS` to identify hosting/DNS provider.
- `MX` for mail handling (and whether any third-party service is used).
- `TXT` for SPF/DMARC/DKIM indicators.
- `SOA` for primary NS and serial.



```

(kali㉿kali)-[~/halisans_passive_recon]
└$ dnsrecon -d halisans.com
2026-01-19T14:39:57.275337-0500 INFO Starting enumeration for domain: halisans.com
2026-01-19T14:39:57.279475-0500 INFO std: Performing General Enumeration against: halisans.com ...
2026-01-19T14:39:57.411680-0500 ERROR No answer for DNSSEC query for halisans.com
2026-01-19T14:39:57.518653-0500 INFO      SOA dns1.registrar-servers.com 156.154.132.200
2026-01-19T14:39:57.519755-0500 INFO      SOA dns1.registrar-servers.com 2610:a1:1024::200
2026-01-19T14:39:57.62497-0500 INFO      NS dns2.registrar-servers.com 156.154.132.200
2026-01-19T14:39:57.692992-0500 INFO      Bind Version for 156.154.132.200 Nameserver"
2026-01-19T14:39:57.749628-0500 INFO      NS dns2.registrar-servers.com 2610:a1:1025::200
2026-01-19T14:39:57.750692-0500 INFO      NS dns1.registrar-servers.com 156.154.132.200
2026-01-19T14:39:57.858295-0500 INFO      Bind Version for 156.154.132.200 Nameserver"
2026-01-19T14:39:57.858622-0500 INFO      NS dns1.registrar-servers.com 2610:a1:1024::200
2026-01-19T14:39:58.341306-0500 INFO      MX mx2.zoho.eu 185.23.0.214.166
2026-01-19T14:39:58.341854-0500 INFO      MX mx3.zoho.eu 185.23.0.212.166
2026-01-19T14:39:58.342100-0500 INFO      MX mx.zoho.eu 185.230.214.166
2026-01-19T14:39:58.342287-0500 INFO      MX mx.zoho.eu 185.230.212.166
2026-01-19T14:39:58.422465-0500 INFO      A halisans.com 66.29.153.49
2026-01-19T14:39:58.615367-0500 INFO      TXT halisans.com zohov-verification=z0b019798.4mverif.y.zoho.eu
2026-01-19T14:39:58.616891-0500 INFO      TXT halisans.com v=spf1 include:zohomail.eu ~all
2026-01-19T14:39:58.748542-0500 INFO      INFO Enumerating SRV Records

```

3.5 Web Application Firewall

- **Passive approach:**

```
(kali㉿kali)-[~]
$ wafw00f halisans.com
```

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

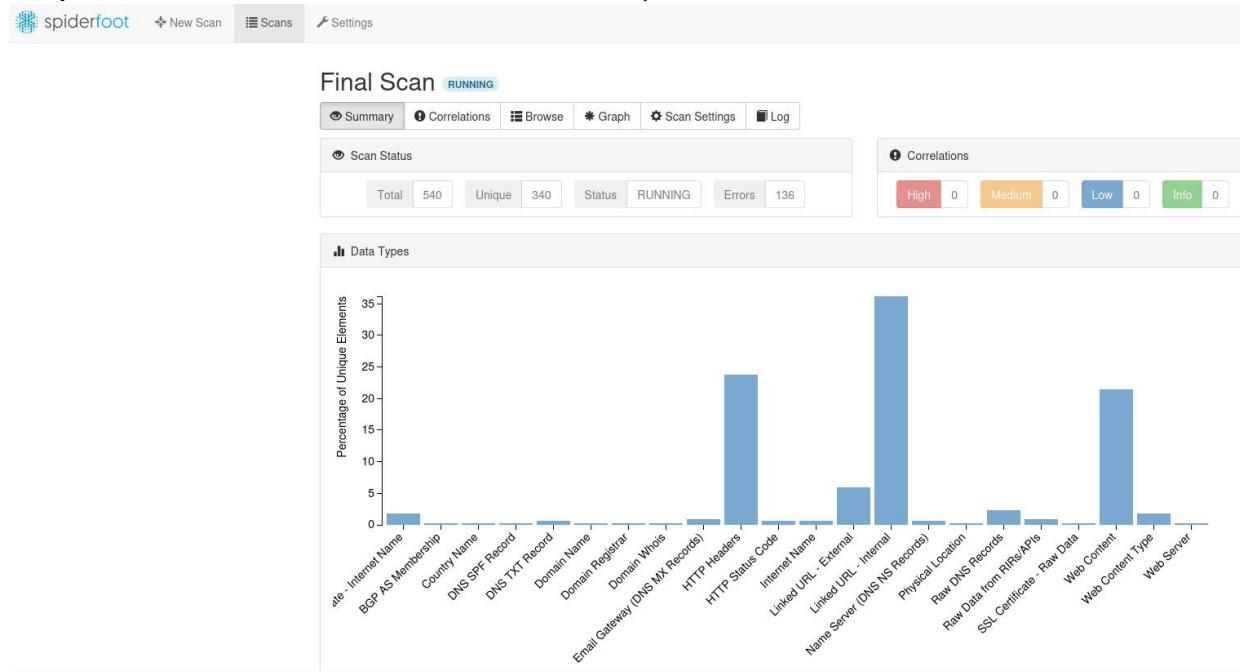
~ WAFW00F : v2.3.1 ~
The Web Application Firewall Fingerprinting Toolkit

- [*] Checking https://halisans.com
- [+] The site <https://halisans.com> is behind **LiteSpeed (LiteSpeed Technologies) WAF**.
- [~] Number of requests: 2

3.6 OSINT: Mentions, Accounts, and Exposure

- SpiderFoot (passive modules):

- DNS/Hosts: Passive resolution of subdomains from CT/DNS.



spiderfoot New Scan Scans Settings

Final Scan RUNNING

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	Domain Name: HALISANS.COM Registry Domain ID: 2917253114_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2025-08-24T11:14:13Z Creation Date: 2024-09-16T04:57:11Z Registry Expiry Date: 2026-09-16T04:57:11Z Registrar: NameCheap, Inc. Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS1.REGISTRAR-SERVERS.COM Name Server: DNS2.REGISTRAR-SERVERS.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2026-01-20T00:11:54Z <<< For more information on Whois status codes, please visit https://icann.org/epp NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the re	halisans.com	sfp_whois	2026-01-20 04:12:12

- **Credential exposure:** Only passive checks; no repository cloning or brute forcing.

spiderfoot New Scan Scans Settings

Final Scan RUNNING

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	Certificate: Data: Version: 3 (0x2) Serial Number: 1f:6d:6c:5e:49:79:47:3b:78:4d:a6:28:60:92:87:64 Signature Algorithm: sha256WithRSAEncryption Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA Validity Not Before: Sep 16 00:00:00 2024 GMT Not After : Sep 16 23:59:59 2025 GMT Subject: CN=halisans.com Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit) Modulus: 00:eb:4b:a1:64:46:0f:19:8f:31:33:7f:75:02:c5: 07:bd:fc:8a:4e:9e:21:38:c0:9d:1d:f0:be:64:0d: 96:ca:e2:d4:41:3b:d1:5f:31:4e:64:92:00:f7:a2: cb:08:d3:77:68:62:08:55:ab:c0:68:a4:44:6c:1b: 8e:34:a6:9d:f5:e8:98:5f:39:95:5a:6e:73:f2:6e: 7c:ed:0a:c0:e5:79:f3:a2:e9:a9:7d:ca:fdee:bf: 47:fd:	halisans.com	sfp_crt	2026-01-20 04:09:24
<input type="checkbox"/>	Certificate: Data: Version: 3 (0x2)	halisans.com	sfp_crt	2026-01-20 04:09:25

Wapiti: Vulnerability Assessment on Web Application

```
(kali㉿kali)-[~]
$ wapiti -u https://halisans.com


Wapiti 3.2.8 (wapiti-scanner.github.io)
[*] Be careful! New moon tonight.

[*] Launching module exec
[*] 70 pages were previously attacked and will be skipped
96 requests were skipped due to network issues

[*] Launching module ssrf

[*] Launching module file
1 requests were skipped due to network issues

[*] Launching module ssl
Certificate subject: *.web-hosting.com
Alt. names: *.web-hosting.com, web-hosting.com
Issuer: Sectigo RSA Domain Validation Secure Server CA
Requested hostname doesn't match those in the certificate
Key: RSA 2048 bits
Signature Algorithm: sha256WithRSAEncryption
Certificate expires in 2 months, 13 days, 21 hours, 35 minutes and 59.22 seconds
Certificate doesn't use Extended Validation
OCSP Must-Staple extension is missing
Certificate transparency: No
Strict Transport Security (HSTS) is not set
Server is vulnerable to OpenSSL CCS (CVE-2014-0224)

Accepted cipher suites for TLSv1.1:
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA acceptable
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA acceptable
* TLS_RSA_WITH_AES_128_CBC_SHA acceptable
* TLS_RSA_WITH_AES_256_CBC_SHA acceptable


```

```
Accepted cipher suites for TLSv1.2:
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 strong
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 strong
* TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 strong
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA acceptable
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA acceptable
* TLS_RSA_WITH_AES_128_GCM_SHA256 acceptable
* TLS_RSA_WITH_AES_256_GCM_SHA384 acceptable
* TLS_RSA_WITH_AES_128_CBC_SHA acceptable
* TLS_RSA_WITH_AES_256_CBC_SHA acceptable

Accepted cipher suites for TLSv1.3:
* TLS_AES_128_GCM_SHA256 strong
* TLS_AES_256_GCM_SHA384 strong
* TLS_CHACHA20_POLY1305_SHA256 strong

Accepted cipher suites for TLSv1.0:
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA acceptable
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA acceptable
* TLS_RSA_WITH_AES_128_CBC_SHA acceptable
* TLS_RSA_WITH_AES_256_CBC_SHA acceptable
The following protocols are deprecated and/or insecure and should be deactivated: TLSv1.0, TLSv1.1

[*] Launching module sql
[*] Launching module redirect
[*] Launching module upload
[*] Launching module xss
[*] Launching module permanentxss

[*] Generating report ...
A report has been generated in the file /home/kali/.wapiti/generated_report
Open /home/kali/.wapiti/generated_report/halisans.com_01202026_0953.html with a browser to see this report.
```

Recommendations (Based on Passive Posture Only)

- HTTP Security Headers:** Verify presence of Strict-Transport-Security, Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy.

Wapiti vulnerability report

Target: https://halisans.com/

Date of the scan: Tue, 20 Jan 2026 09:53:32 +0000. Scope of the scan: folder. Crawled pages: 105

Summary

Category	Number of vulnerabilities found
Backup file	0
Cleartext Submission of Password	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Fingerprint web application framework	0
Fingerprint web server	0
Htaccess Bypass	0
HTML Injection	0
Clickjacking Protection	1
HTTP Strict Transport Security (HSTS)	1

Category	Number of vulnerabilities found
MIME Type Confusion	1
HttpOnly Flag cookie	0
Unencrypted Channels	0
Inconsistent Redirection	0
Information Disclosure - Full Path	1
LDAP Injection	0
Log4Shell	0
NS takeover	0
Open Redirect	0
Reflected Cross Site Scripting	0
Secure Flag cookie	0
Spring4Shell	0
SQL Injection	0
TLS/SSL misconfigurations	10
Server Side Request Forgery	0
Stored HTML Injection	0
Stored Cross Site Scripting	0
Subdomain takeover	0
Blind SQL Injection	0
Unrestricted File Upload	0

Category	Number of vulnerabilities found
Vulnerable software	0
Internal Server Error	0
Resource consumption	0
Review Webserver Metafiles for Information Leakage	0
Fingerprint web technology	0
HTTP Methods	0
TLS/SSL misconfigurations	8

Content Security Policy Configuration

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
CSP is not set for URL: https://halisans.com/			

Solutions

Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control what resources the user agent is allowed to load for that page.

References

- Mozilla: Content Security Policy (CSP)
- OWASP: Content Security Policy Cheat Sheet
- OWASP: How to do Content Security Policy (PDF)

- OWASP: Content Security Policy
-

Clickjacking Protection

Description

Clickjacking is a technique that tricks a user into clicking something different from what the user perceives, potentially revealing confidential information or taking control of their computer.

Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
X-Frame-Options is not set			

Solutions

Implement X-Frame-Options or Content Security Policy (CSP) frame-ancestors directive.

References

- OWASP: Clickjacking
 - KeyCDN: Preventing Clickjacking
-

HTTP Strict Transport Security (HSTS)

Description

HSTS is a web security policy mechanism that helps to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking.

Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
Strict-Transport-Security is not set			

Solutions

Implement the HTTP Strict Transport Security header to enforce secure connections to the server.

References

- OWASP: HTTP Strict Transport Security
- KeyCDN: Enabling HSTS

MIME Type Confusion

Description

MIME type confusion can occur when a browser interprets files as a different type than intended, which could lead to security vulnerabilities like cross-site scripting (XSS).

Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
X-Content-Type-Options is not set			

Solutions

Implement X-Content-Type-Options to prevent MIME type sniffing.

References

- OWASP: MIME Sniffing
- KeyCDN: Preventing MIME Type Sniffing

Information Disclosure - Full Path

Description

The application response discloses full system paths. This information can help attackers understand the server environment, directory structure, and operating system, which can facilitate further attacks.

Vulnerability found in /steps-involved-in-performing-sql-injectionfor-

educational-purposes-only/

Description	HTTP Request	cURL command line	WSTG Code
Response contains potential system path: /usr/share/webshells/sql/			

Solutions

Ensure that error messages and application responses do not disclose full filesystem paths or other sensitive system information. Use generic error messages for end users and log detailed errors only on the server side.

References

- OWASP: Information Leakage
- CWE-209: Generation of Error Message Containing Sensitive Information
- WASC-13: Information Leakage

TLS/SSL misconfigurations

Description

The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. Over the years numerous vulnerabilities have been discovered in some SSL/TLS version or specific ciphers making the integrity of the communications at risk (eavesdropping, alteration...)

Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
Requested hostname doesn't match those in the certificate			

Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
Certificate doesn't use Extended Validation			

🟡 Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
OCSP Must-Staple extension is missing			

🔴 Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
Certificate transparency: No			

🔴 Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
Strict Transport Security (HSTS) is not set			

🔥 Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
Server is vulnerable to OpenSSL CCS (CVE-2014-0224)			

🟠 Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
The following ciphers are acceptable for TLSv1.1: TLS_ECDHE_RSA_WITH_AES_128_CBC_			

🟠 Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
The following ciphers are acceptable for TLSv1.2: TLS_ECDHE_RSA_WITH_AES_128_CBC_			

🟠 Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
The following ciphers are acceptable for TLSv1.0: TLS_ECDHE_RSA_WITH_AES_128_CBC_			

🔥 Vulnerability found in /

Description	HTTP Request	cURL command line	WSTG Code
The following protocols are deprecated and/or insecure and should be deactivated:			

Solutions

To protect against SSL/TLS vulnerabilities, make sure that deprecated versions of the protocol are disabled. Refer to up-to-date recommendations to only allow modern versions of TLS with Perfect Forward Secrecy.

References

- SSL Labs: SSL and TLS Deployment Best Practices
- Mozilla: Server Side TLS recommended configurations
- Beagle Security: Importance of TLS 1.3, SSL and TLS Vulnerabilities
- Security of TLS cipher suites
- Trail of Bits: What Application Developers Need To Know About TLS Early Data (0RTT)
- OWASP: Weak SSL/TLS Ciphers Insufficient Transport Layer Protection

TLS/SSL misconfigurations

Description

The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. Over the years numerous vulnerabilities have been discovered in some SSL/TLS version or specific ciphers making the integrity of the communications at risk (eavesdropping, alteration...)

Additional found in /

Description	HTTP Request	cURL command line	WSTG Code
Certificate subject: *.web-hosting.com			

Additional found in /

Description	HTTP Request	cURL command line	WSTG Code
Alt. names: *.web-hosting.com, web-hosting.com			

🕵️ Additional found in /

Description	HTTP Request	cURL command line	WSTG Code
Issuer: Sectigo RSA Domain Validation Secure Server CA			

🕵️ Additional found in /

Description	HTTP Request	cURL command line	WSTG Code
Key: RSA 2048 bits			

🕵️ Additional found in /

Description	HTTP Request	cURL command line	WSTG Code
Signature Algorithm: sha256WithRSAEncryption			

🕵️ Additional found in /

Description	HTTP Request	cURL command line	WSTG Code
Certificate expires in 2 months, 13 days, 21 hours, 35 minutes and 59.22 seconds			

🕵️ Additional found in /

Description	HTTP Request	cURL command line	WSTG Code

The following ciphers are strong for TLSv1.2: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA2

Additional found in /

Description	HTTP Request	cURL command line	WSTG Code
The following ciphers are strong for TLSv1.3: TLS_AES_128_GCM_SHA256, TLS_AES_256			

Solutions

To protect against SSL/TLS vulnerabilities, make sure that deprecated versions of the protocol are disabled. Refer to up-to-date recommendations to only allow modern versions of TLS with Perfect Forward Secrecy.

References

- SSL Labs: SSL and TLS Deployment Best Practices
- Mozilla: Server Side TLS recommended configurations
- Beagle Security: Importance of TLS 1.3, SSL and TLS Vulnerabilities
- Security of TLS cipher suites
- Trail of Bits: What Application Developers Need To Know About TLS Early Data (0RTT)
- OWASP: Weak SSL/TLS Ciphers Insufficient Transport Layer Protection

Wapiti 3.2.8 © Nicolas SURRIBAS 2006-2025

Conclusion

This assessment combined passive OSINT reconnaissance with a non-intrusive Wapiti scan to evaluate the external security posture of halisans.com within a clearly defined scope. The findings show that while the website is publicly accessible, functional, and does not expose critical application-level vulnerabilities such as SQL injection, XSS, or authentication weaknesses, there are notable security hygiene gaps at the configuration and transport layers.

The most significant issues relate to missing HTTP security headers (CSP, HSTS, X-Frame-Options, X-Content-Type-Options), instances of information disclosure, and multiple TLS/SSL misconfigurations, including deprecated protocol support and certificate inconsistencies. These weaknesses do not indicate active exploitation but increase the attack surface and could be leveraged in chained or future attacks if left unaddressed.

Overall, the security posture can be classified as moderate but improvable. By implementing recommended header hardening, tightening TLS configurations to modern standards, and reducing informational leakage, the site's resilience against common web-based threats can be significantly

strengthened. This work demonstrates the value of passive reconnaissance as an effective first step in identifying security risks without disrupting production systems, while highlighting areas that would benefit from deeper, authorized active testing in the future.