Passive Reconnaissance Scan Report

Scan target: Halisans.com (66.29.153.49)

Date of recon: November 27, 2025

Cybersecurity Analyst
Adebayo Fijabi

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

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

1.1 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.

2.1 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.
- **wafw00f:** 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

3. Findings

3.1 Public Web Presence (Landing Page)

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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ 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_seq=1 ttl=255 time=47.0 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=2 ttl=255 time=35.9 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=3 ttl=255 time=37.0 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=4 ttl=255 time=39.3 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=8 ttl=255 time=37.4 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=9 ttl=255 time=39.9 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=10 ttl=255 time=36.6 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=11 ttl=255 time=37.9 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=12 ttl=255 time=37.8 ms
^C
── halisans.com ping statistics ──
12 packets transmitted, 9 received, 25% packet loss, time 11156ms
rtt min/avg/max/mdev = 35.855/38.749/46.971/3.137 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)-[~]
└─$ 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/epp#clientT
ransferProhibited
   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.o
rg/wicf/
>>> Last update of whois database: 2025-11-27T06:45:23Z <<<

For more information on Whois status codes, please visit https://icann.o
rg/epp
```

3.3 Name servers: Capture NS from RDAP and confirm against ‘dig NS’.

```
┌──(kali㉿kali)-[~]
└─$ dig halisans.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> halisans.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33832
;; 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: 204 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Thu Nov 27 01:29:41 EST 2025
;; MSG SIZE  rcvd: 57
```

3.4 Host

- This give the corresponding ip address of the domain ‘halisans.com’
- Shows the mail is handled and hosted by ‘zoho’.

```
┌──(kali㉿kali)-[~]
└─$ host halisans.com
halisans.com has address 66.29.153.49
halisans.com mail is handled by 50 mx3.zoho.eu.
halisans.com mail is handled by 20 mx2.zoho.eu.
halisans.com mail is handled by 10 mx.zoho.eu.
```

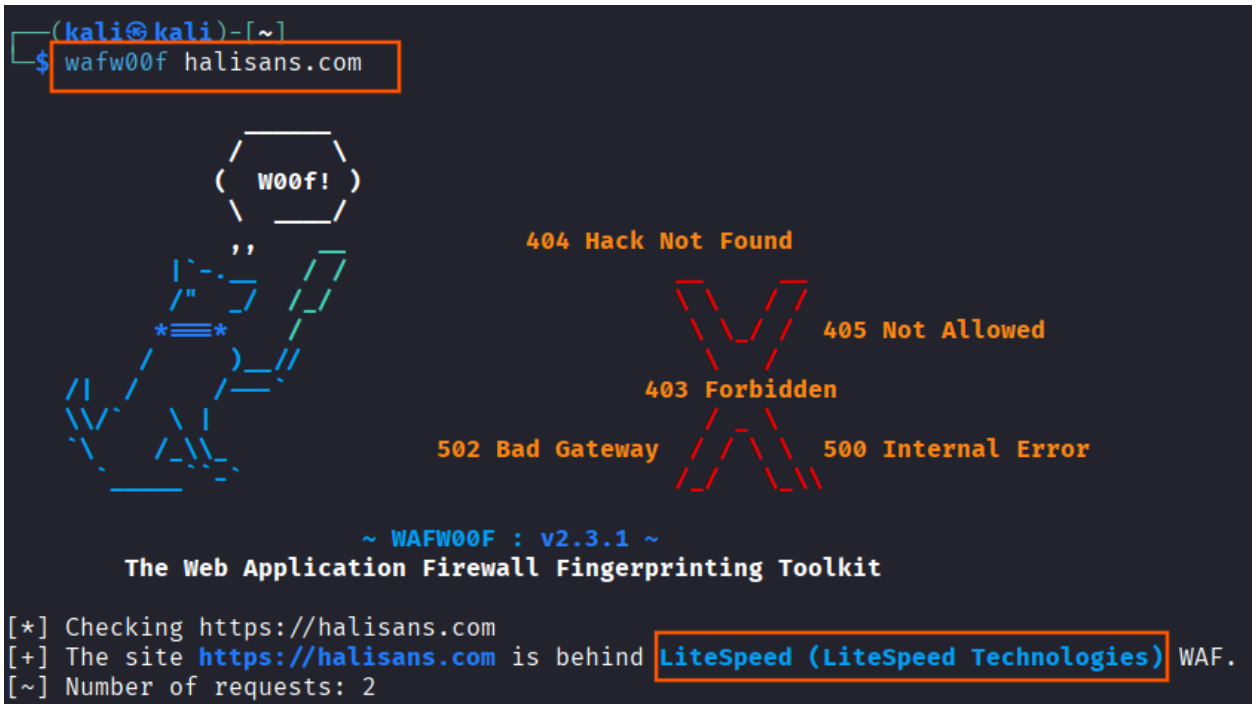
3.5 DNS Surface (A/AAAA, NS, MX, TXT, SOA, CAA)

- Records collected passively:
  - A/AAAA for apex and www.
  - NS to identify hosting/DNS providers.
- MX for mail handling (and whether any third-party service is used).
  - TXT for SPF/DMARC/DKIM indicators.
  - mx.zoho.eu (185.230.212.166)
  - mx2.zoho.eu (185.230.214.166)
  - mx3.zoho.eu (185.230.212.166)

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d halisans.com
[*] std: Performing General Enumeration against: halisans.com...
[-] DNSSEC is not configured for halisans.com
[*]     SOA dns1.registrar-servers.com 156.154.132.200
[*]     SOA dns1.registrar-servers.com 2610:a1:1024::200
[*]     NS dns2.registrar-servers.com 156.154.133.200
[*]     Bind Version for 156.154.133.200 Nameserver"
[*]     NS dns2.registrar-servers.com 2610:a1:1025::200
[*]     NS dns1.registrar-servers.com 156.154.132.200
[*]     Bind Version for 156.154.132.200 Nameserver"
[*]     NS dns1.registrar-servers.com 2610:a1:1024::200
[*]     MX mx2.zoho.eu 185.230.212.166
[*]     MX mx.zoho.eu 185.20.209.166
[*]     MX mx3.zoho.eu 185.20.209.166
[*]     A halisans.com 66.29.153.49
[*]     TXT halisans.com zoho-verification=zb01879578.zmverify.zoho.eu
[*]     TXT halisans.com v=spf1 include:zohomail.eu ~all
[*] Enumerating SRV Records
[-] No SRV Records Found for halisans.com
```

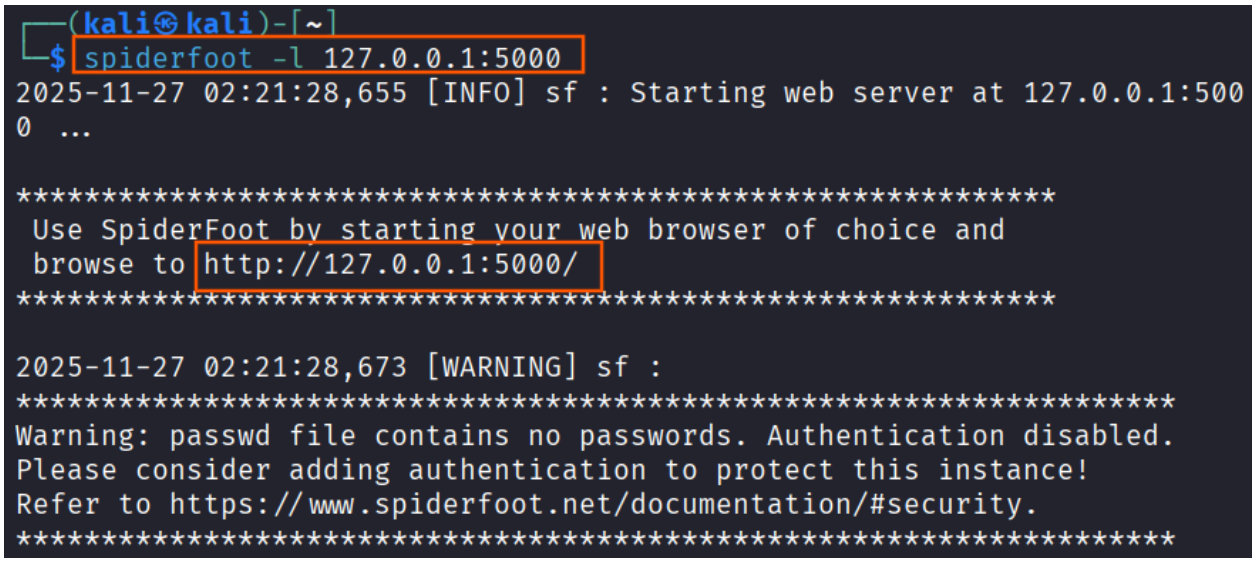
3.6 Web Application Firewall

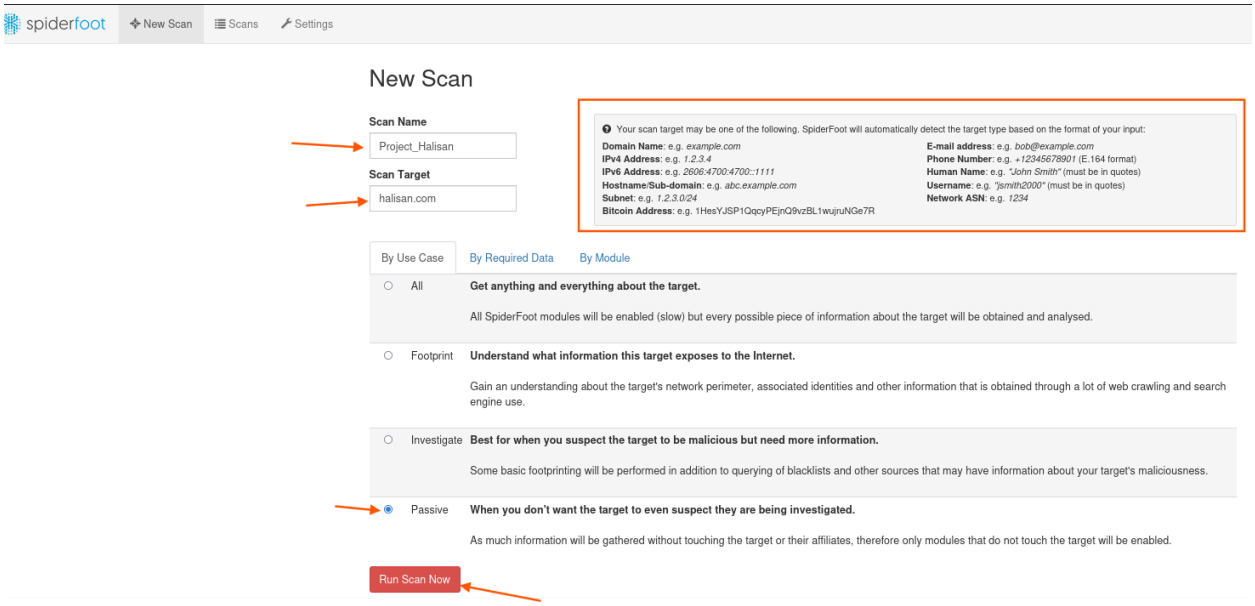
- **Passive approach**

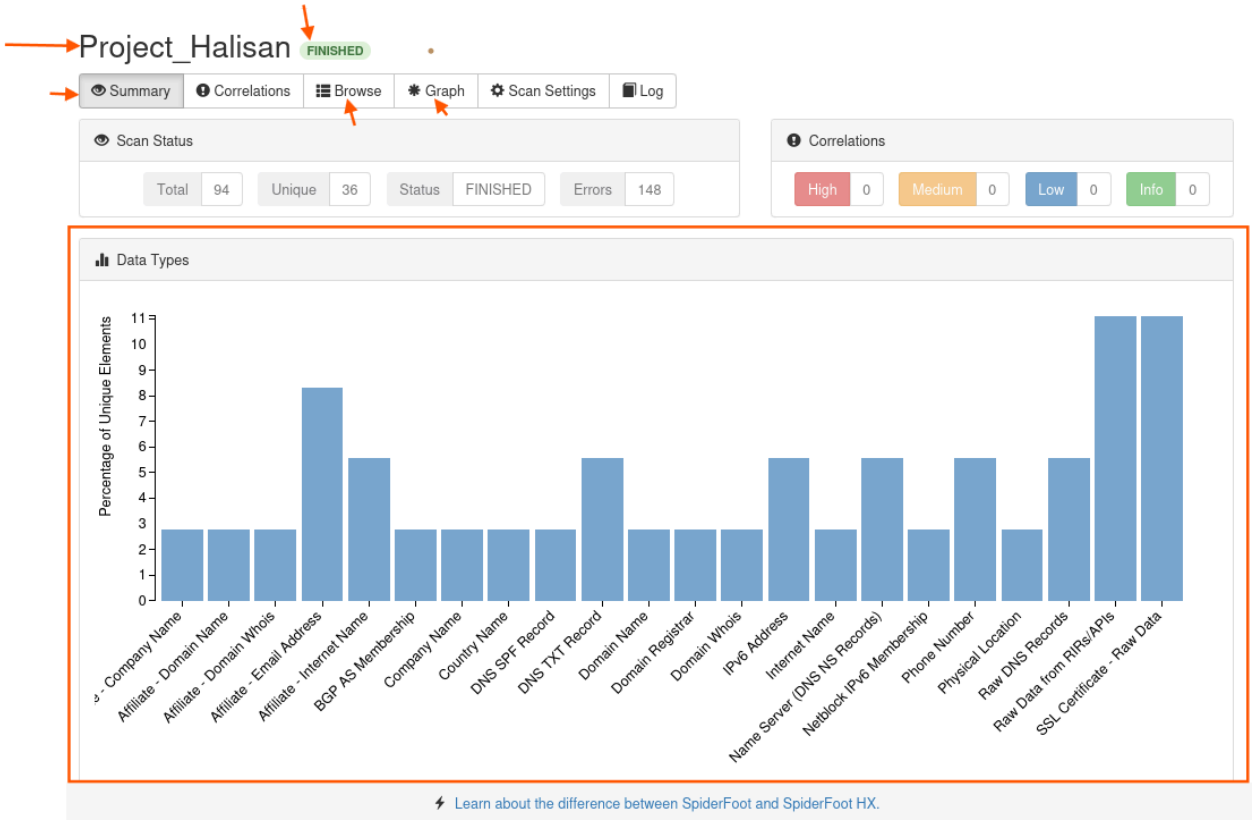


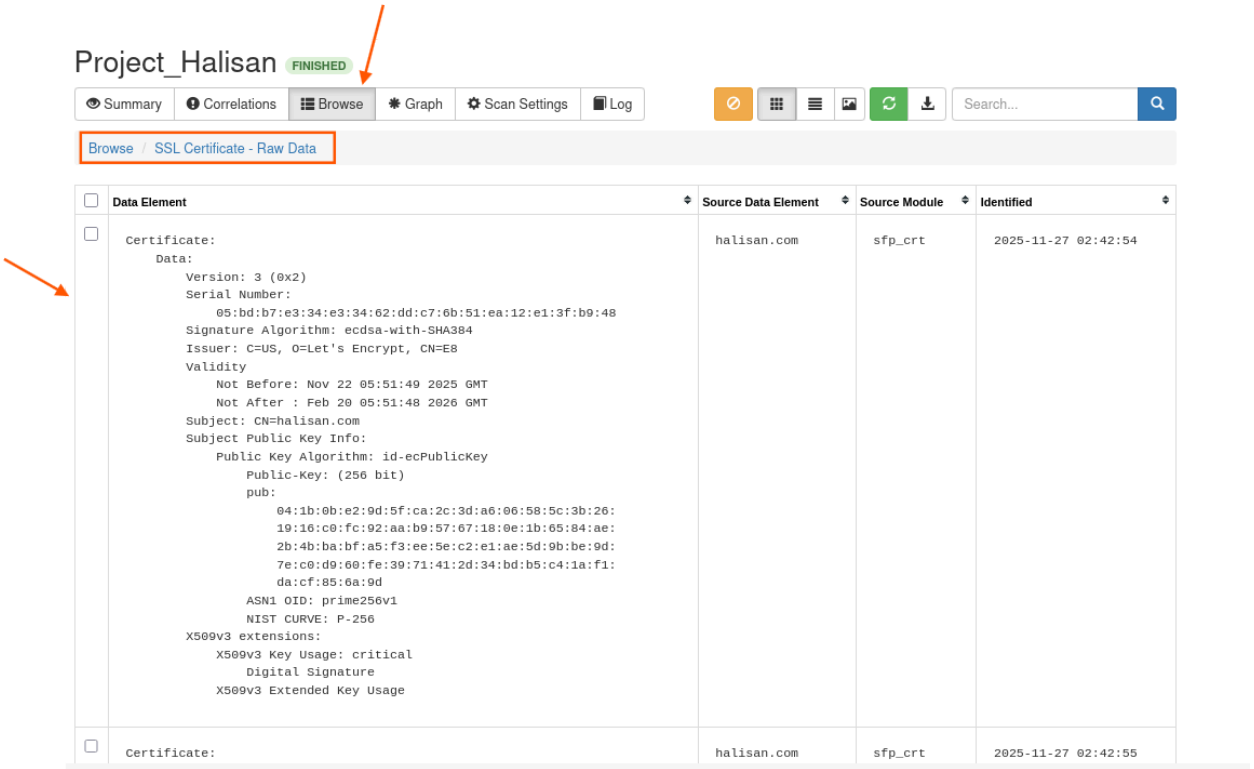
3.7 OSINT: Mentions, Accounts, and Exposure

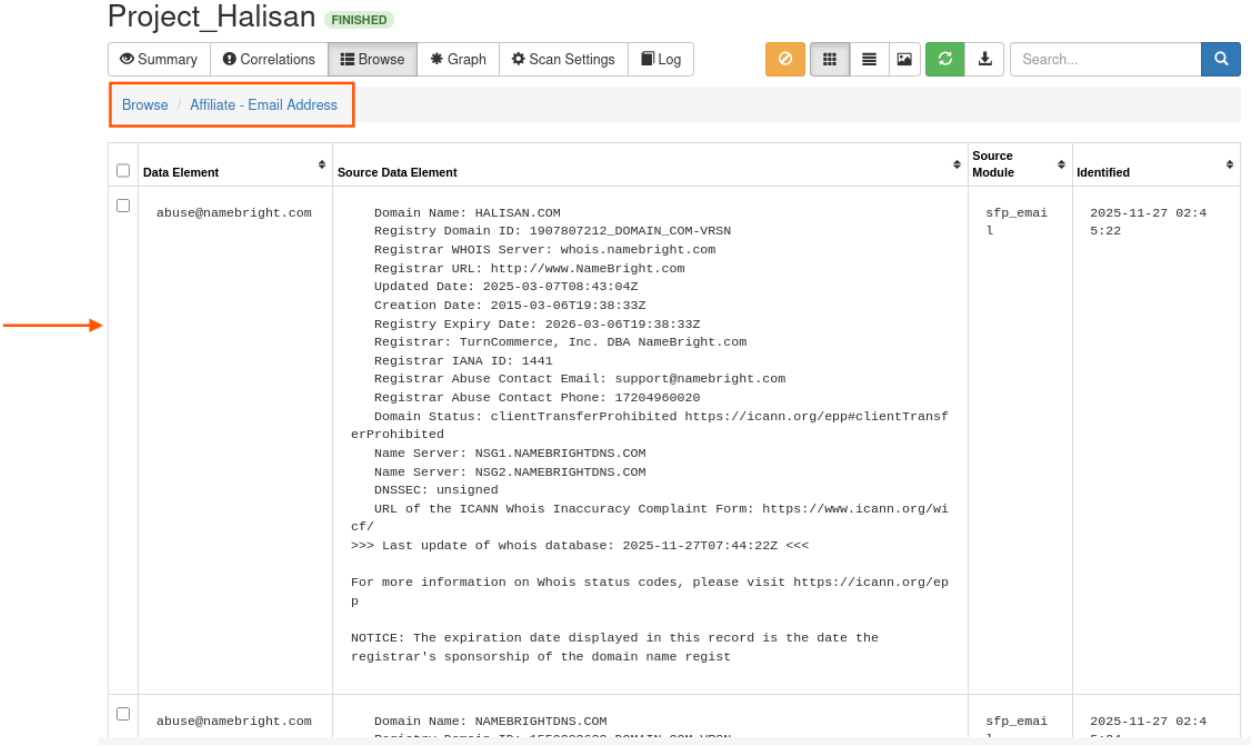
- **SpiderFoot** (passive modules):
    - o DNS/Hosts: Passive resolution of subdomains from CT/DNS.

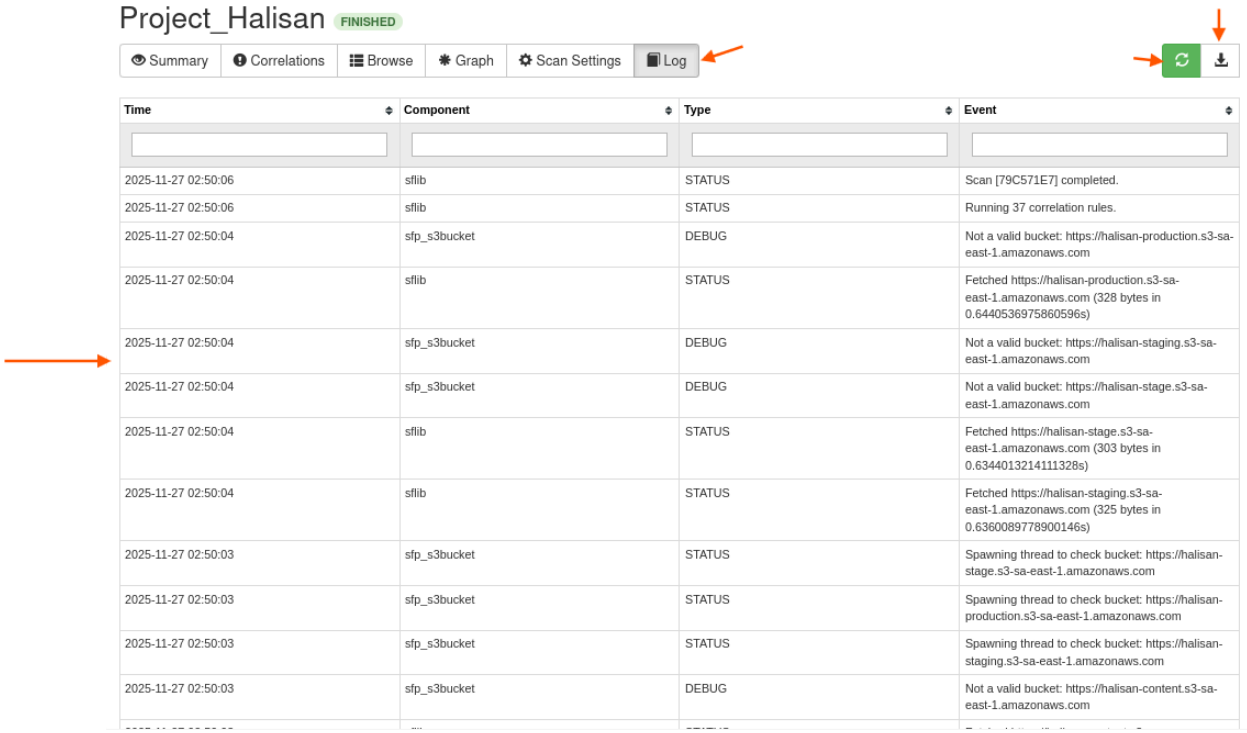


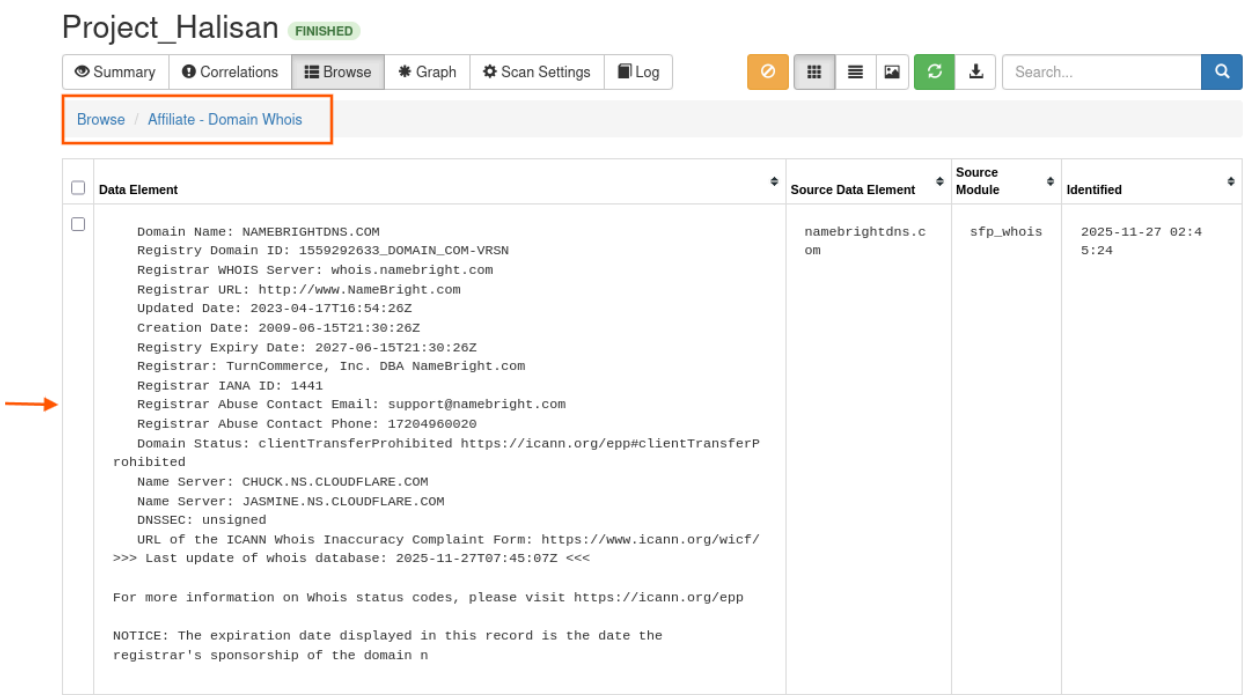

spiderfoot
New Scan
Scans
Settings
New Scan
Scan Name
Project_Halisan
Scan Target
halisan.com
Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:
Domain Name: e.g. example.com
IPv4 Address: e.g. 1.2.3.4
IPv6 Address: e.g. 2606:4700:4700::1111
Hostname/Sub-domain: e.g. abc.example.com
Subnet: e.g. 1.2.3.0/24
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R
E-mail address: e.g. bob@example.com
Phone Number: e.g. +12345678901 (E.164 format)
Human Name: e.g. "John Smith" (must be in quotes)
Username: e.g. "jsmith2000" (must be in quotes)
Network ASN: e.g. 1234
By Use Case
By Required Data
By Module
All
Get anything and everything about the target.
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.
Footprint
Understand what information this target exposes to the Internet.
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.
Investigate
Best for when you suspect the target to be malicious but need more information.
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.
Passive
When you don't want the target to even suspect they are being investigated.
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.
Run Scan Now


Project_Halisan
FINISHED
Summary
Correlations
Browse
Graph
Scan Settings
Log
Scan Status
Total 94
Unique 36
Status FINISHED
Errors 148
Correlations
High 0
Medium 0
Low 0
Info 0
Data Types
Percentage of Unique Elements
0
1
2
3
4
5
6
7
8
9
10
11
Affiliate - Company Name
Affiliate - Domain Name
Affiliate - Domain Whois
Affiliate - Email Address
Affiliate - Internet Name
BGP AS Membership
Company Name
Country Name
DNS SPF Record
DNS TXT Record
Domain Name
Domain Registrar
Domain Whois
IPv6 Address
Internet Name
Name Server (DNS NS Records)
Netblock IPv6 Membership
Phone Number
Physical Location
Raw DNS Records
Raw Data from RIRs/APIs
SSL Certificate - Raw Data
Learn about the difference between SpiderFoot and SpiderFoot HX.


Project_Halisan
FINISHED
Summary
Correlations
Browse
Graph
Scan Settings
Log
Search...
Browse / SSL Certificate - Raw Data
Data Element
Source Data Element
Source Module
Identified
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
05:bd:b7:e3:34:e3:34:62:dd:c7:6b:51:ea:12:e1:3f:b9:48
Signature Algorithm: ecdsa-with-SHA384
Issuer: C=US, O=Let's Encrypt, CN=E8
Validity
Not Before: Nov 22 05:51:49 2025 GMT
Not After : Feb 20 05:51:48 2026 GMT
Subject: CN=halisan.com
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
04:1b:0b:e2:9d:5f:ca:2c:3d:a6:06:58:5c:3b:26:
19:16:c0:fc:92:aa:b9:57:67:18:0e:1b:65:84:ae:
2b:4b:ba:bf:a5:f3:ee:5e:c2:e1:ae:5d:9b:be:9d:
7e:c0:d9:60:fe:39:71:41:2d:34:bd:b5:c4:1a:f1:
da:cf:85:6a:9d
ASN1 OID: prime256v1
NIST CURVE: P-256
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature
X509v3 Extended Key Usage
halisan.com
sfp_crt
2025-11-27 02:42:54
Certificate:
halisan.com
sfp_crt
2025-11-27 02:42:55


Project_Halisan
FINISHED
Summary
Correlations
Browse
Graph
Scan Settings
Log
Search...
Browse / Affiliate - Email Address
Data Element
Source Data Element
Source Module
Identified
abuse@namebright.com
Domain Name: HALISAN.COM
Registry Domain ID: 1907807212_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namebright.com
Registrar URL: http://www.NameBright.com
Updated Date: 2025-03-07T08:43:04Z
Creation Date: 2015-03-06T19:38:33Z
Registry Expiry Date: 2026-03-06T19:38:33Z
Registrar: TurnCommerce, Inc. DBA NameBright.com
Registrar IANA ID: 1441
Registrar Abuse Contact Email: support@namebright.com
Registrar Abuse Contact Phone: 17204960020
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NSG1.NAMEBRIGHTDNS.COM
Name Server: NSG2.NAMEBRIGHTDNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-11-27T07:44:22Z <<<
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 regist
sfp_email
2025-11-27 02:45:22
abuse@namebright.com
Domain Name: NAMEBRIGHTDNS.COM
sfp_email
2025-11-27 02:45:24

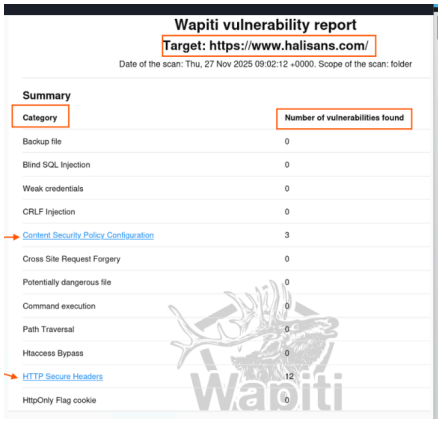

Project_Halisan
FINISHED
Summary
Correlations
Browse
Graph
Scan Settings
Log
Time
Component
Type
Event
2025-11-27 02:50:06 sflib STATUS Scan [79C571E7] completed.
2025-11-27 02:50:06 sflib STATUS Running 37 correlation rules.
2025-11-27 02:50:04 sfp_s3bucket DEBUG Not a valid bucket: https://halisan-production.s3-sa-east-1.amazonaws.com
2025-11-27 02:50:04 sflib STATUS Fetched https://halisan-production.s3-sa-east-1.amazonaws.com (328 bytes in 0.6440536975860596s)
2025-11-27 02:50:04 sfp_s3bucket DEBUG Not a valid bucket: https://halisan-staging.s3-sa-east-1.amazonaws.com
2025-11-27 02:50:04 sfp_s3bucket DEBUG Not a valid bucket: https://halisan-stage.s3-sa-east-1.amazonaws.com
2025-11-27 02:50:04 sflib STATUS Fetched https://halisan-stage.s3-sa-east-1.amazonaws.com (303 bytes in 0.6344013214111328s)
2025-11-27 02:50:04 sflib STATUS Fetched https://halisan-staging.s3-sa-east-1.amazonaws.com (325 bytes in 0.6360089778900146s)
2025-11-27 02:50:03 sfp_s3bucket STATUS Spawning thread to check bucket: https://halisan-stage.s3-sa-east-1.amazonaws.com
2025-11-27 02:50:03 sfp_s3bucket STATUS Spawning thread to check bucket: https://halisan-production.s3-sa-east-1.amazonaws.com
2025-11-27 02:50:03 sfp_s3bucket STATUS Spawning thread to check bucket: https://halisan-staging.s3-sa-east-1.amazonaws.com
2025-11-27 02:50:03 sfp_s3bucket DEBUG Not a valid bucket: https://halisan-content.s3-sa-east-1.amazonaws.com


Project_Halisan
FINISHED
Summary
Correlations
Browse
Graph
Scan Settings
Log
Search...
Browse / Affiliate - Domain Whois
Data Element
Source Data Element
Source Module
Identified
Domain Name: NAMEBRIGHTDNS.COM
Registry Domain ID: 1559292633_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namebright.com
Registrar URL: http://www.NameBright.com
Updated Date: 2023-04-17T16:54:26Z
Creation Date: 2009-06-15T21:30:26Z
Registry Expiry Date: 2027-06-15T21:30:26Z
Registrar: TurnCommerce, Inc. DBA NameBright.com
Registrar IANA ID: 1441
Registrar Abuse Contact Email: support@namebright.com
Registrar Abuse Contact Phone: 17204960020
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: CHUCK.NS.CLOUDFLARE.COM
Name Server: JASMINE.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-11-27T07:45:07Z <<<
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 n
namebrightdns.com
sfp_whois
2025-11-27 02:45:24

3.8 Wapiti

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

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Resuming scan from previous session, please wait
[*] Saving scan state, please wait...

 Note
========
This scan has been saved in the file /home/kali/.wapiti/scans/www.halisans.com_folder_1e6c5232.db
[*] Wapiti found 3 URLs and forms during the scan
[*] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, h
ttp_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set
```

```
Report
------
A report has been generated in the file /home/kali/.wapiti/generated_report
Open /home/kali/.wapiti/generated_report/www.halisans.com_11272025_0902.html with a browser to see this re
port.

┌──(kali㉿kali)-[~]
└─$ firefox /home/kali/.wapiti/generated_report/www.halisans.com_11272025_0902.html
```



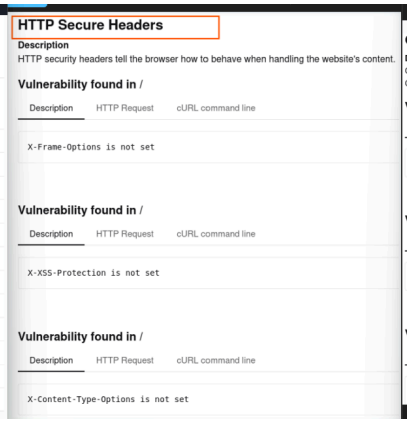
Wapiti vulnerability report

Target: https://www.halisans.com/

Date of the scan: Thu, 27 Nov 2025 09:02:12 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	3
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	12
HttpOnly Flag cookie	0



HTTP Secure Headers

Description

HTTP security headers tell the browser how to behave when handling the website's content.

Vulnerability found in /

Description | HTTP Request | cURL command line

X-Frame-Options is not set

Vulnerability found in /

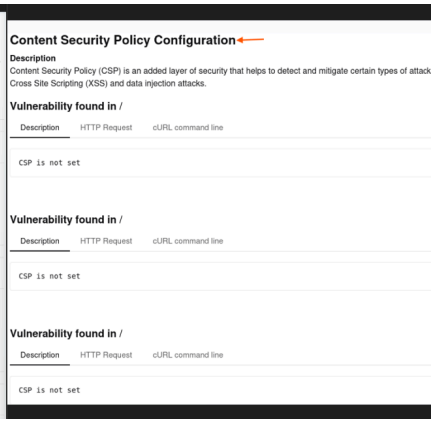
Description | HTTP Request | cURL command line

X-XSS-Protection is not set

Vulnerability found in /

Description | HTTP Request | cURL command line

X-Content-Type-Options is not set



Content Security Policy Configuration

Description

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

Vulnerability found in /

Description | HTTP Request | cURL command line

CSP is not set

Vulnerability found in /

Description | HTTP Request | cURL command line

CSP is not set

Vulnerability found in /

Description | HTTP Request | cURL command line

CSP is not set

4.0 Security Recommendations

Based on the findings, the following actions are recommended to strengthen the security posture of **halisans.com**. Recommendations are prioritized by impact and urgency.

Immediate Actions (High Priority)

4.1 Implement Missing Security Headers

These headers help prevent common web attacks such as XSS, clickjacking, and code injection.

- Content-Security-Policy (CSP): Mitigates XSS, data injection, and unauthorized script execution.
- X-Frame-Options: DENY – Prevents clickjacking by blocking page rendering in iframes.
- Strict-Transport-Security (HSTS): Enforces HTTPS and prevents protocol downgrade attacks.
- X-XSS-Protection: 1; mode=block – Provides additional browser-based XSS filtering.
- X-Content-Type-Options: nosniff – Prevents MIME-type sniffing attacks.

4.2 Review and Harden LiteSpeed Web Application Firewall (WAF)

- Validate that all LiteSpeed WAF rules are enabled and properly tuned.
- Conduct targeted penetration testing to identify possible WAF bypass techniques.
- Ensure logging and alerting are configured for suspicious activity.

4.3. Enable DNSSEC

DNSSEC ensures DNS responses are authenticated, protecting against:

- DNS spoofing
- Cache poisoning
- Domain hijacking

This is critical for maintaining trust and preventing redirection attacks.

4.4. Perform Additional Security Testing

4.4a. Directory Enumeration

Use tools like **Gobuster** or **Dirb** to check for:

- Exposed backup files

- Sensitive directories
- Admin panels
- Misconfigurations

4.4b. Web Application Vulnerability Review

Manually analyze Wapiti results for:

- SQL Injection
- XSS
- SSRF
- Command injection
- File inclusion vulnerabilities

5.0 Conclusion

The assessment of **halisans.com** reveals several security misconfigurations and missing protective controls that may expose the website to cyber threats. Addressing these issues starting with the implementation of essential security headers, WAF hardening, and dnsSEC will significantly improve the overall security posture.

Further testing is recommended to uncover deeper vulnerabilities and ensure that existing defenses cannot be bypassed. Taking these corrective actions promptly will reduce the risk of exploitation and enhance resilience against evolving web-based attacks.