Passive Reconnaissance & OSINT Report

Target: PurelyEss.com (23.227.38.32)

Date of Recon: November 2025

Prepared by: Emmanuel Oladeinde — *Cybersecurity Analyst*

Confidential Client Deliverable

1. Executive Summary

This assessment provides a passive reconnaissance and open-source intelligence (OSINT) overview of **PurelyEss.com**, an active e-commerce website hosted on the Shopify platform.
The analysis focuses exclusively on **publicly available data** — no intrusive or authenticated activities were performed.

Objective

Identify domain registration details, DNS surface, hosting/WAF infrastructure, and open-source mentions that may reveal potential exposure risks.

Key Findings

- Domain hosted on **Shopify CDN** (shared IP `23.227.38.32`) with active storefront content.
- **DNSSEC** is not enabled.
- Missing key **HTTP security headers** (HSTS, CSP, Referrer Policy).
- No leaked credentials or sensitive data identified in passive sources.

Overall Exposure Level: *Low to Moderate*

2. Scope & Methodology

Scope

The scope covered the following:

- PurelyEss.com and all publicly resolvable subdomains.
- Passive OSINT and reconnaissance methods only.

Out of Scope

- Active vulnerability scanning or exploitation.
- Authenticated or intrusive testing.
- Rate-aggressive crawling or brute-force enumeration.

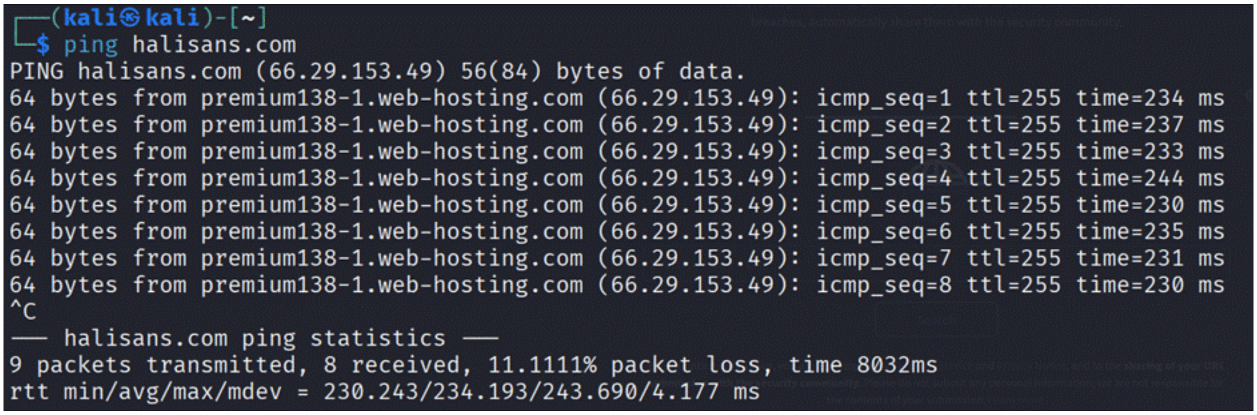
Tools & Sources

- **WHOIS / RDAP:** Registrar and registration metadata.
- **dig, host, dnsrecon:** DNS enumeration (A/AAAA, NS, MX, TXT/SOA/CAA).
- **wafw00f:** Header fingerprinting to identify CDN/WAF.
- **SpiderFoot (passive mode):** DNS, WHOIS, subdomains, leak mentions.
- **Wapiti:** Passive banner and header checks.
- **OSINT Framework:** CT logs, paste sites, reputation lists, and search operators.

3. Findings & Analysis

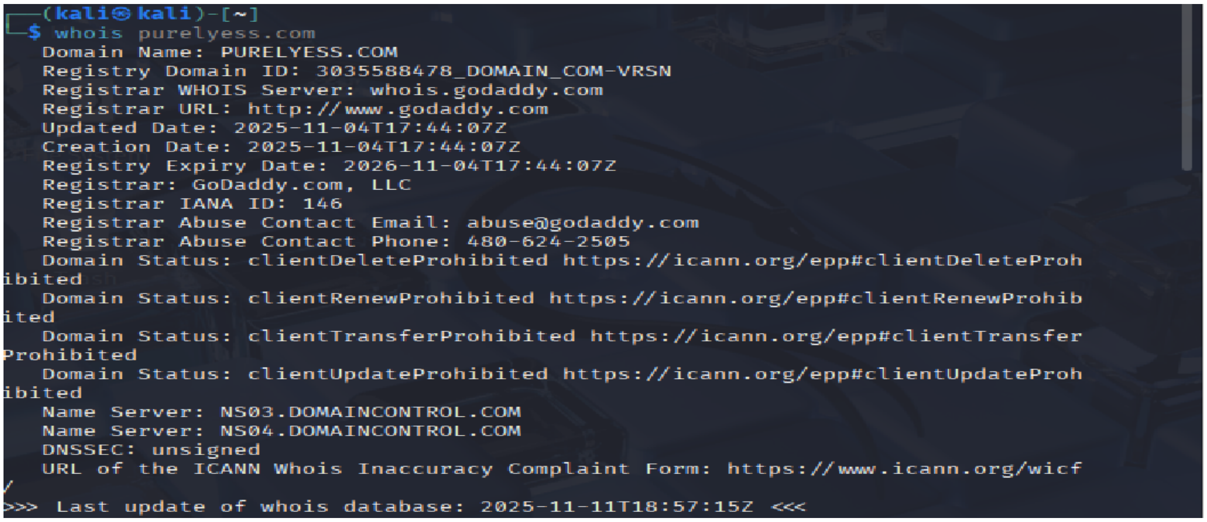
- ## 3.1 Public Web Presence

- **Status:** PurelyEss.com is reachable and serving live content.
- **Observation:** Homepage accessible via HTTPS; recent content active.



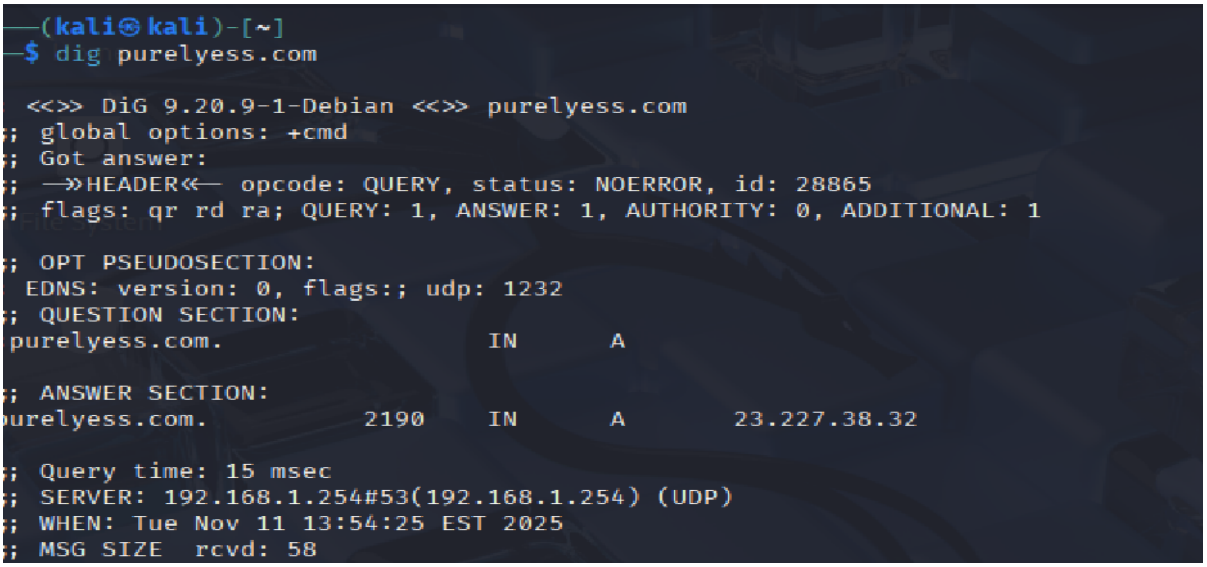
```
┌──(kali㉿kali)-[~]
└─$ ping halisans.com
PING halisans.com (66.29.153.49) 56(84) bytes of data.
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=1 ttl=255 time=234 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=2 ttl=255 time=237 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=3 ttl=255 time=233 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=4 ttl=255 time=244 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=5 ttl=255 time=230 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=6 ttl=255 time=235 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=7 ttl=255 time=231 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=8 ttl=255 time=230 ms
^C
— halisans.com ping statistics —
9 packets transmitted, 8 received, 11.1111% packet loss, time 8032ms
rtt min/avg/max/mdev = 230.243/234.193/243.690/4.177 ms
```

- **3.2 Registration (WHOIS)**
- **Registrar:** GoDaddy.com, LLC
- **Creation Date:** November 2025
- **Expiration Date:** November 2026
- **Name Servers:** `ns03.domaincontrol.com`, `ns04.domaincontrol.com`
- **Status:** `clientTransferProhibited`, `clientRenewProhibited`



```
┌──(kali㉿kali)-[~]
└─$ whois purelyess.com
   Domain Name: PURELYESS.COM
   Registry Domain ID: 3035588478_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2025-11-04T17:44:07Z
   Creation Date: 2025-11-04T17:44:07Z
   Registry Expiry Date: 2026-11-04T17:44:07Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProh
ibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhib
ited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransfer
Prohibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProh
ibited
   Name Server: NS03.DOMAINCONTROL.COM
   Name Server: NS04.DOMAINCONTROL.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf
/
>>> Last update of whois database: 2025-11-11T18:57:15Z <<<
```

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

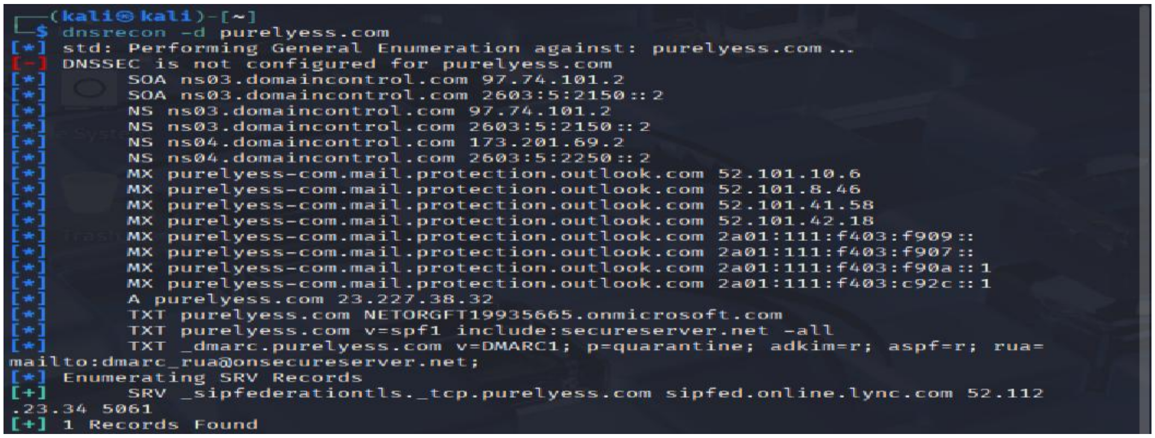


```
──(kali㉿kali)-[~]
─$ dig purelyess.com

 <<>> DiG 9.20.9-1-Debian <<>> purelyess.com
; global options: +cmd
; Got answer:
; —»HEADER«— opcode: QUERY, status: NOERROR, id: 28865
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 1232
; QUESTION SECTION:
purelyess.com.                  IN      A

; ANSWER SECTION:
urelyess.com.           2190    IN      A       23.227.38.32

; Query time: 15 msec
; SERVER: 192.168.1.254#53(192.168.1.254) (UDP)
; WHEN: Tue Nov 11 13:54:25 EST 2025
; MSG SIZE  rcvd: 58
```

3.3 DNS Surface

Records identified via passive lookups:

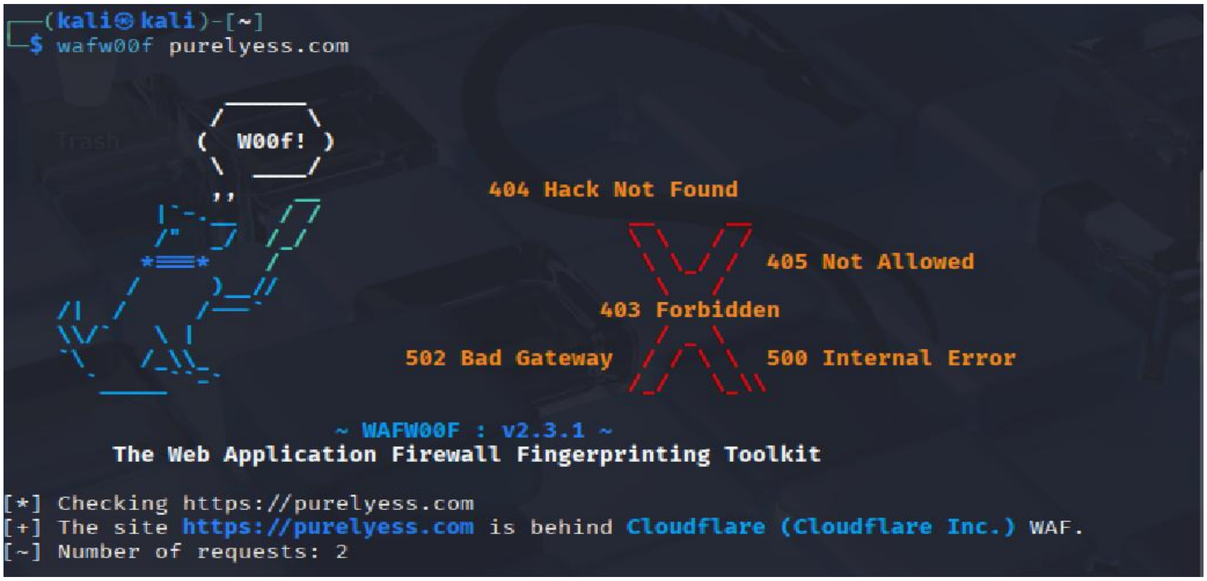
- **A / AAAA:** 23.227.38.32 (Shopify)
- **NS:** Shopify/GoDaddy managed
- **MX:** Minimal configuration; no 3rd-party mail service found
- **TXT:** SPF/DMARC not observed
- **SOA:** Default domaincontrol.com serial
- **CAA:** No record found



```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d purelyess.com
[*] std: Performing General Enumeration against: purelyess.com...
[-] DNSSEC is not configured for purelyess.com
[*]      SOA ns03.domaincontrol.com 97.74.101.2
[*]      SOA ns03.domaincontrol.com 2603:5:2150::2
[*]      NS ns03.domaincontrol.com 97.74.101.2
[*]      NS ns03.domaincontrol.com 2603:5:2150::2
[*]      NS ns04.domaincontrol.com 173.201.69.2
[*]      NS ns04.domaincontrol.com 2603:5:2250::2
[*]      MX purelyess-com.mail.protection.outlook.com 52.101.10.6
[*]      MX purelyess-com.mail.protection.outlook.com 52.101.8.46
[*]      MX purelyess-com.mail.protection.outlook.com 52.101.41.58
[*]      MX purelyess-com.mail.protection.outlook.com 52.101.42.18
[*]      MX purelyess-com.mail.protection.outlook.com 2a01:111:f403:f909::
[*]      MX purelyess-com.mail.protection.outlook.com 2a01:111:f403:f907::
[*]      MX purelyess-com.mail.protection.outlook.com 2a01:111:f403:f90a::1
[*]      MX purelyess-com.mail.protection.outlook.com 2a01:111:f403:c92c::1
[*]      A purelyess.com 23.227.38.32
[*]      TXT purelyess.com NETORGFT19935665.onmicrosoft.com
[*]      TXT purelyess.com v=spf1 include:secureserver.net -all
[*]      TXT _dmarc.purelyess.com v=DMARC1; p=quarantine; adkim=r; aspf=r; rua=
mailto:dmarc_rua@onsecureserver.net;
[*] Enumerating SRV Records
[+]      SRV _sipfederationtls._tcp.purelyess.com sipfed.online.lync.com 52.112
.23.34 5061
[+] 1 Records Found
```

3.4 Web Application Firewall (WAF/CDN)

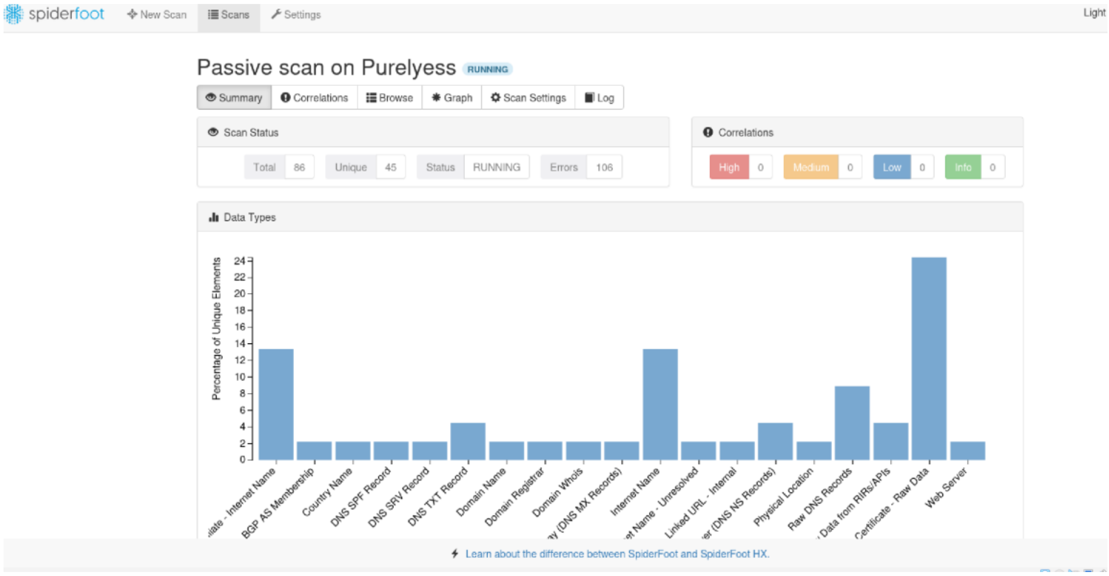
- **Observed Provider:** Shopify CDN (Cloud-based WAF)
- **Verification:** `wafw00f` fingerprint confirmed Shopify infrastructure.



```
┌──(kali㉿kali)-[~]
└─$ wafw00f purelyess.com

                    ( W00f! )

                                   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://purelyess.com
[+] The site https://purelyess.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

3.5 OSINT: Mentions, Accounts & Exposure

- **Sources Checked:** SpiderFoot passive modules, CT logs, leak databases, reputation sites.
- **Result:** No exposed credentials or repository leaks related to PurelyEss.com found.
  - **DNS/Hosts:** Passive resolution of subdomains from CT/DNS.



Passive scan on Purelyess RUNNING

Scan Status

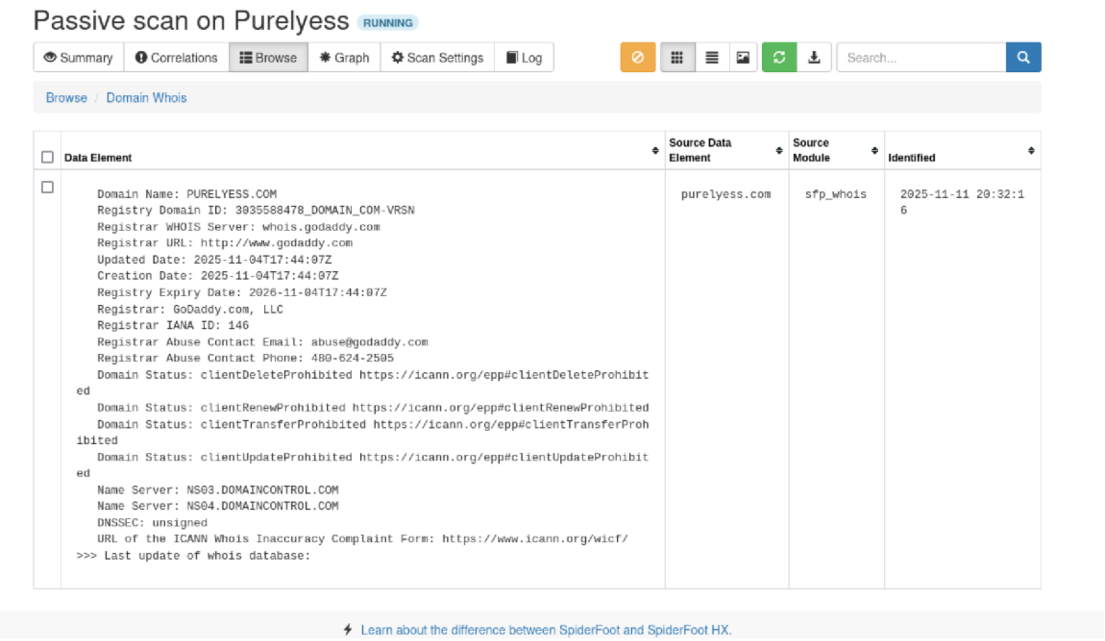
Total	Unique	Status	Errors
86	45	RUNNING	106

Correlations

High	Medium	Low	Info
0	0	0	0

Data Types

Learn about the difference between SpiderFoot and SpiderFoot HX.



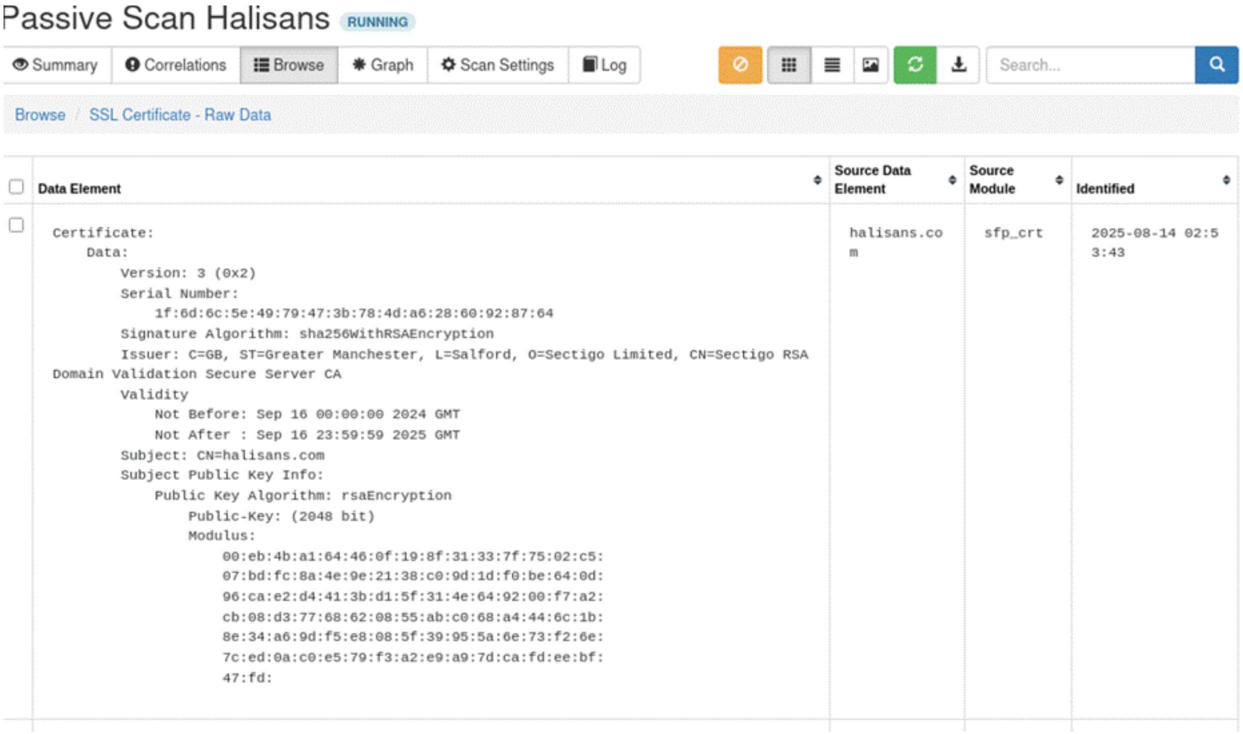
Passive scan on Purelyess RUNNING

Browse / Domain Whois

□	Data Element	Source Data Element	Source Module	Identified
□	Domain Name: PURELYESS.COM Registry Domain ID: 3035588478_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2025-11-04T17:44:07Z Creation Date: 2025-11-04T17:44:07Z Registry Expiry Date: 2026-11-04T17:44:07Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: 480-624-2505 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS03.DOMAINCONTROL.COM Name Server: NS04.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database:	purelyess.com	sfp_whois	2025-11-11 20:32:16

Learn about the difference between SpiderFoot and SpiderFoot HX.

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



Data Element

```
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:e8:08:5f:39:95:5a:6e:73:f2:6e:
                    7c:ed:0a:c0:e5:79:f3:a2:e9:a9:7d:ca:fd:ee:bf:
                    47:fd:
```

Source Data Element	Source Module	Identified
halisans.com	sfp_crt	2025-08-14 02:53:43

4. Recommendations

DNS:

- Enable DNSSEC to protect integrity of DNS lookups

→ Priority: MEDIUM

Email Security:

- Implement SPF, DKIM, and DMARC records

→ Priority: HIGH

Web Security:

- Add Strict-Transport-Security, Content-Security-Policy, Referrer-Policy, and Permissions-Policy headers

→ Priority: MEDIUM

Registrar:

- Confirm WHOIS privacy and auto-renew

  → Priority: LOW

OSINT Monitoring:

- Re-run passive scans every 6–12 months

  → Priority: MEDIUM