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:
purelyess.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

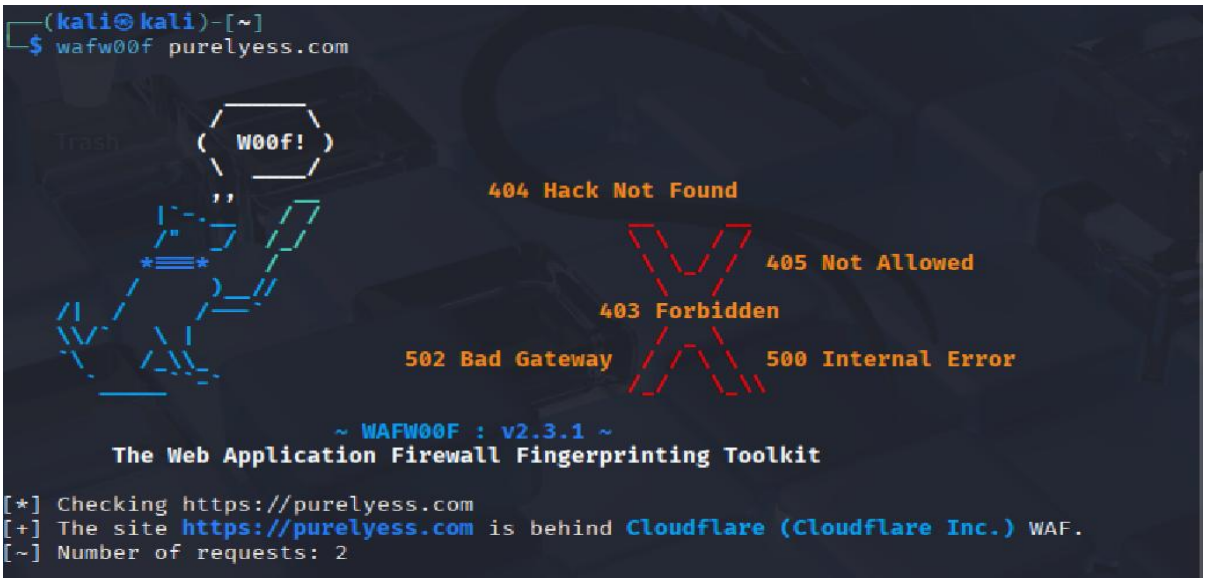
Records identified via passive lookups:

- **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
```

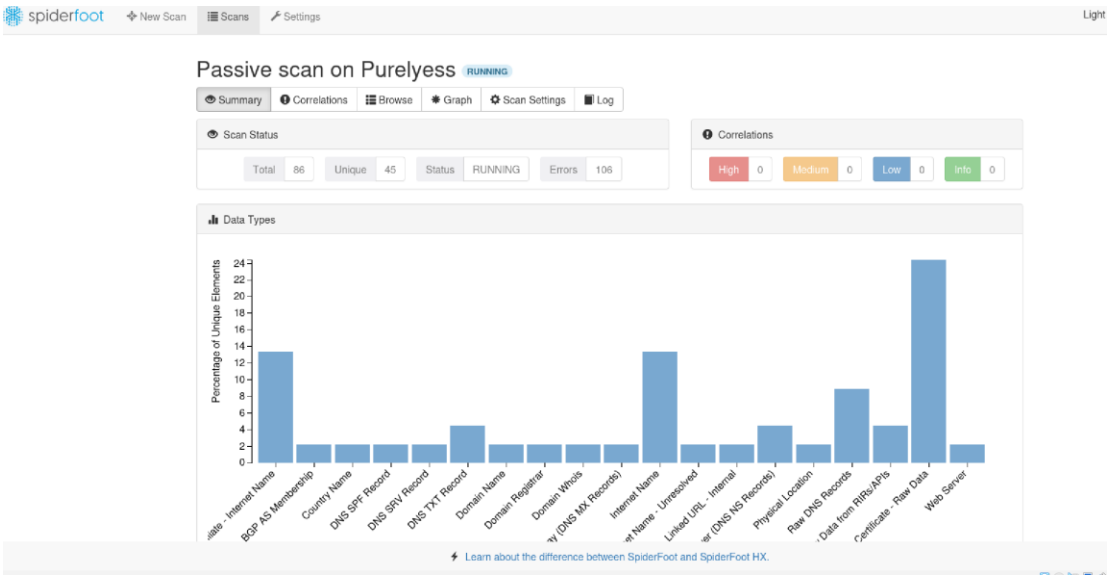
3.4 Web Application Firewall (WAF/CDN)

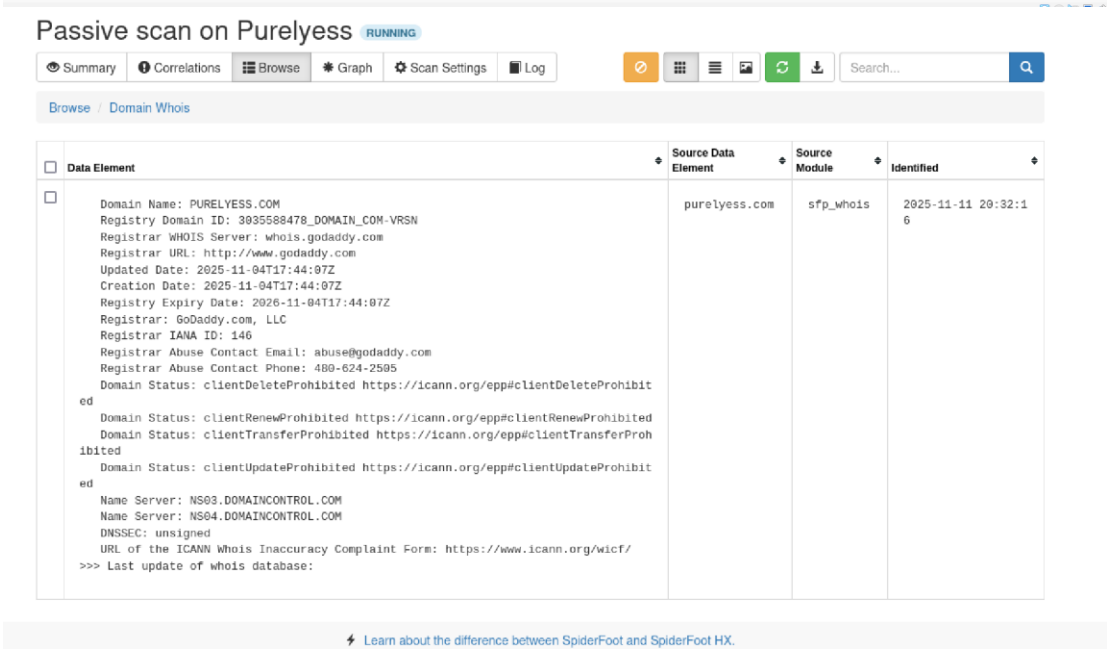
- **Observed Provider:** Shopify CDN (Cloud-based WAF)
- **Verification:** `wafw00f` fingerprint confirmed Shopify infrastructure.



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.





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