Passive Reconnaissance Scan Report

Scan target : Jiji.com(210.152.253.83)

Date of recon: 17 October 2025

Cybersecurity Analyst
Junaid AbdulRahman A

Scope: Jiji.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)

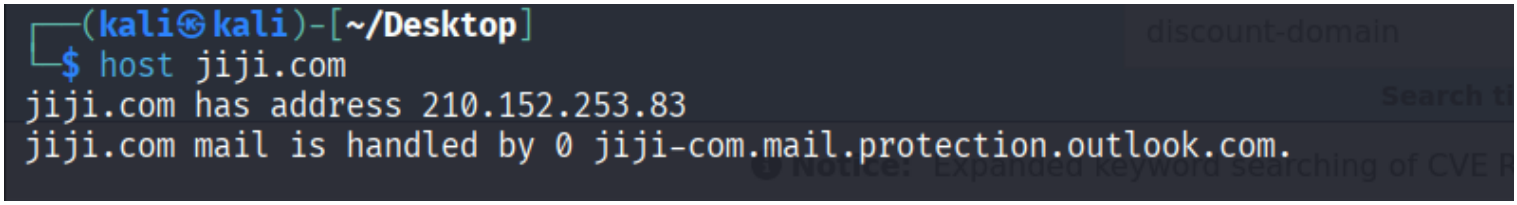
Tools & Modes

- whois / RDAP: Registration & registrar metadata
- dig, host, dnsrecon: Passive DNS lookups (A/AAAA, NS, MX, TXT/SOA/CAA where present) via public resolvers.
- 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).

Findings

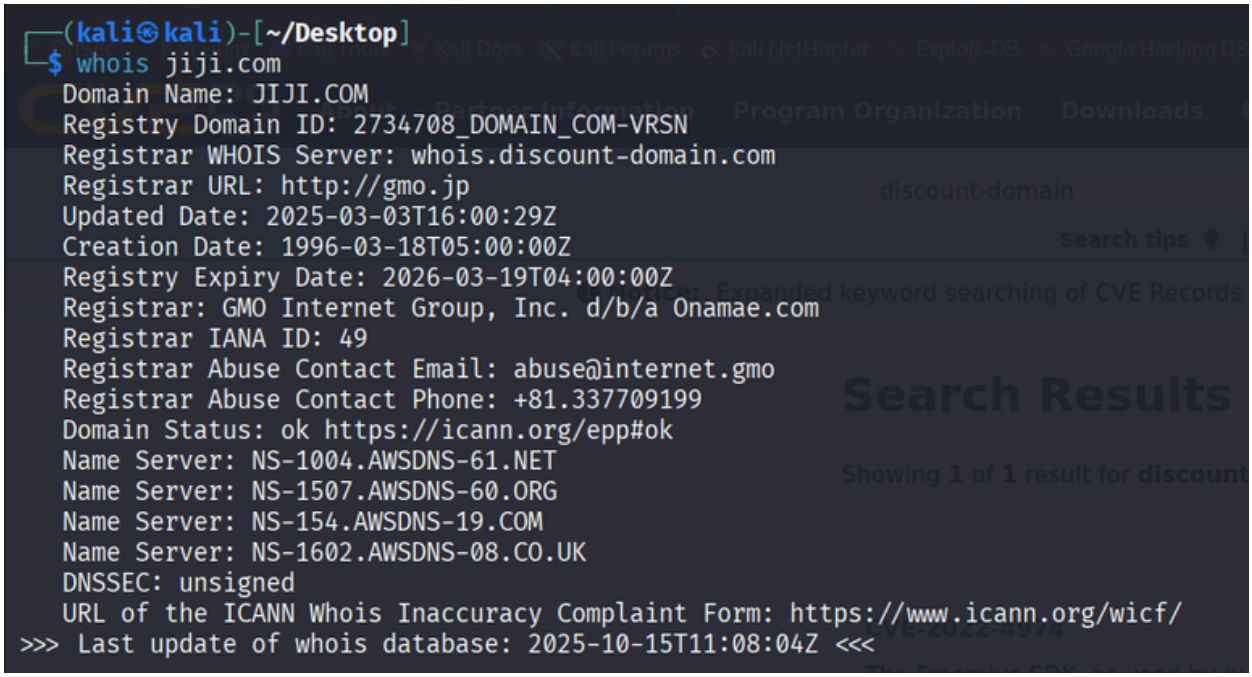
3.1 Public Web Presence using the host command (Landing Page)

- Site reachable:https://jiji.com

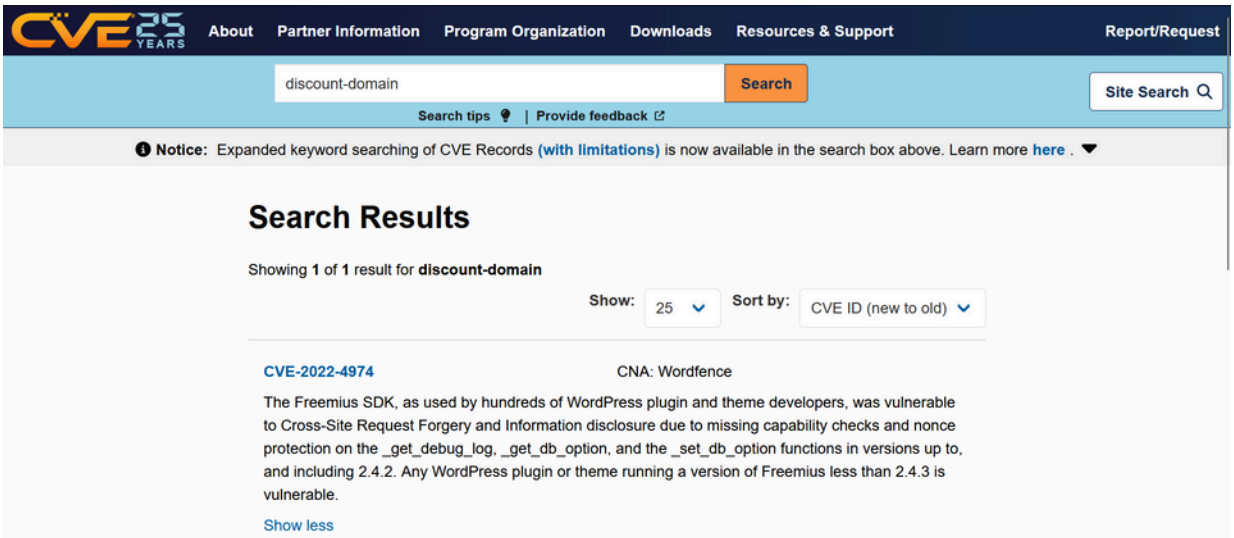


3.2 Registration (WHOIS)

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



- Confirmed through common vulnerability exposure (CVE) if the domain registrar had been reported for any kind of vulnerability, which can also give me a clue to the domain vulnerability



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

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig jiji.com
;; communications error to 192.168.8.1#53: timed out
dig;; communications error to 192.168.8.1#53: timed out

; <<>> DiG 9.20.9-1-Debian <<>> jiji.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33688
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;jiji.com.                      IN      A

;; ANSWER SECTION:
jiji.com.               845     IN      A       210.152.253.83
```

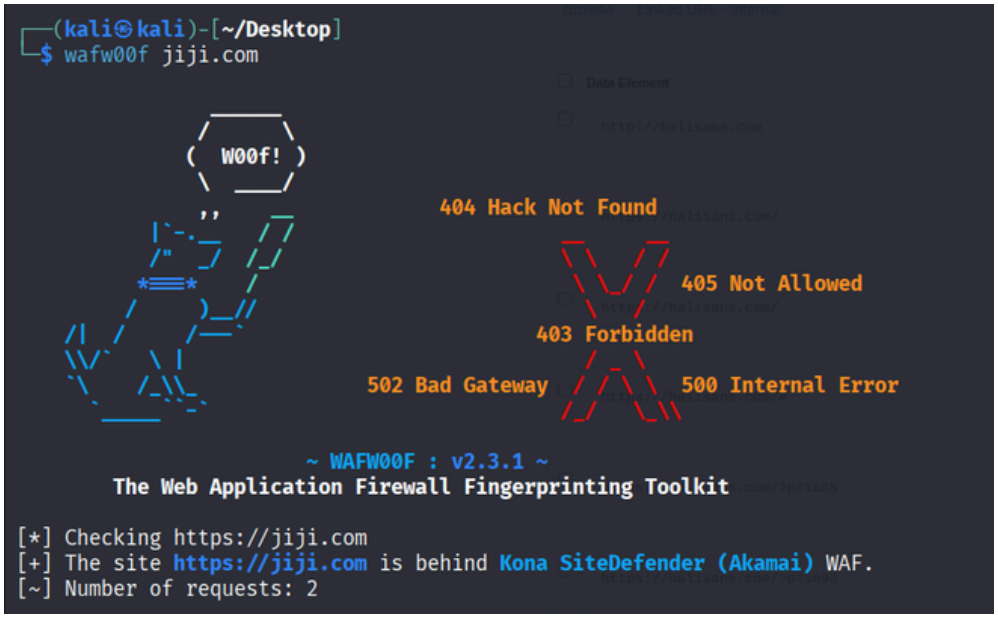
3.3 DNS Surface (A/AAAA, NS, MX, TXT, SOA, CAA)

- 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)-[~/Desktop]
└─$ dnsrecon -d jiji.com
[*] std: Performing General Enumeration against: jiji.com...
[-] DNSSEC is not configured for jiji.com
[*]     SOA ns-1602.awsdns-08.co.uk 205.251.198.66
[*]     SOA ns-1602.awsdns-08.co.uk 2600:9000:5306:4200::1
[*]     NS ns-1602.awsdns-08.co.uk 205.251.198.66
[*]     NS ns-1602.awsdns-08.co.uk 2600:9000:5306:4200::1
[*]     NS ns-154.awsdns-19.com 205.251.192.154
[*]     NS ns-154.awsdns-19.com 2600:9000:5300:9a00::1
[*]     NS ns-1507.awsdns-60.org 205.251.197.227
[*]     NS ns-1507.awsdns-60.org 2600:9000:5305:e300::1
[*]     NS ns-1004.awsdns-61.net 205.251.195.236
[*]     NS ns-1004.awsdns-61.net 2600:9000:5303:ec00::1
[*]     MX jiji-com.mail.protection.outlook.com 52.101.124.5
[*]     MX jiji-com.mail.protection.outlook.com 52.101.124.6
[*]     MX jiji-com.mail.protection.outlook.com 52.101.157.11
[*]     MX jiji-com.mail.protection.outlook.com 52.101.157.10
[*]     MX jiji-com.mail.protection.outlook.com 2a01:111:f403:cc1a::1
[*]     MX jiji-com.mail.protection.outlook.com 2a01:111:f403:cc1a::2
[*]     MX jiji-com.mail.protection.outlook.com 2a01:111:f403:cc24::
[*]     MX jiji-com.mail.protection.outlook.com 2a01:111:f403:cc1f::1
[*]     A jiji.com 210.152.253.83
[*]     TXT jiji.com v=spf1 +ip4:210.164.31.192/26 +ip4:210.158.210.0/23 +ip4:52.193.26.38 +ip4:52.198.42.254 +ip4:210.140.246.0/26 +ip4:210.152.253.76/26 include:spf.protection.outlook.com include:spf.spcloud.jp include:spf-bma.mpme.jp include:spf-rmb.mpme.jp include:fc4082.cuenote.jp include:amazonses.com -all
[*]     TXT jiji.com google-site-verification=wrVJNAFQNEKczHjfHJSsC2-bo_roPXlenccOIYkwALs
[*]     TXT jiji.com MS=ms91222109
[*]     TXT _dmarc.jiji.com v=DMARC1; p=none; rua=mailto:dmarc-rua@jiji.com; ruf=mailto:dmarc-ruf@jiji.com; pct=100; adkim=r; aspf=r;
[*] Enumerating SRV Records
[-] No SRV Records Found for jiji.com
```

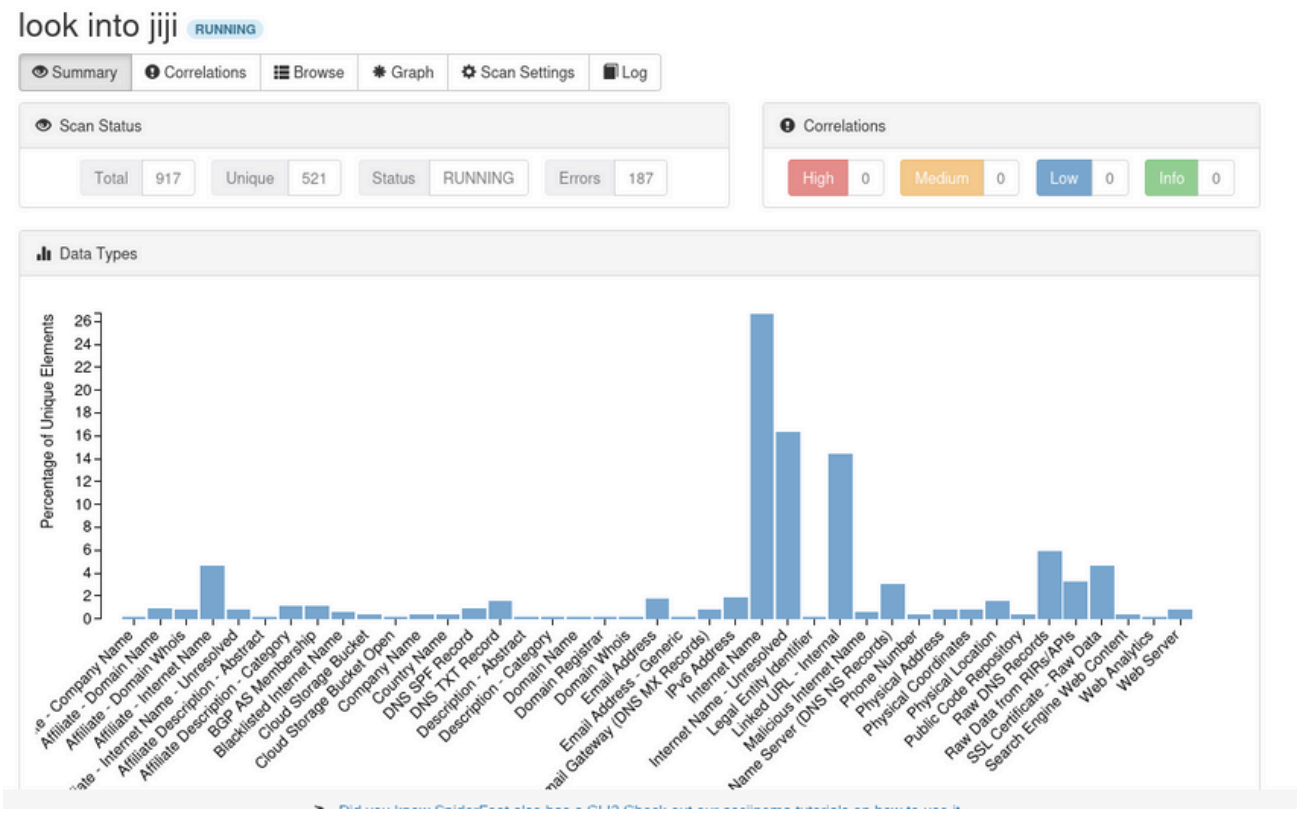
3.5 Web Application Firewall

- Passive approach:which shows the domain is behind Kona Site Defender (Akamai)

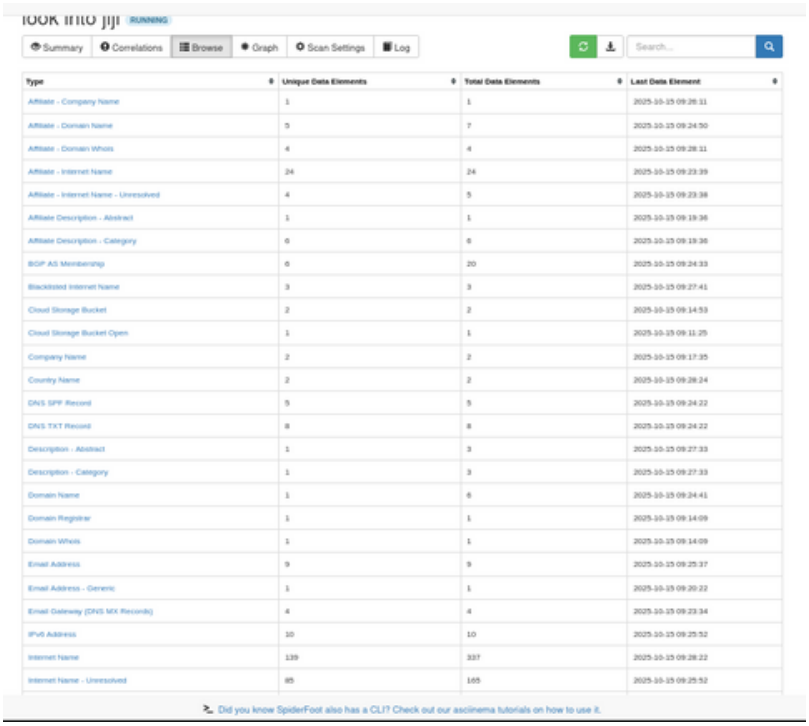


3.6 OSINT: Mentions, Accounts, and Exposure

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



- Other info gathered with the passive module more can also be gathered using the spiderfoot active module.

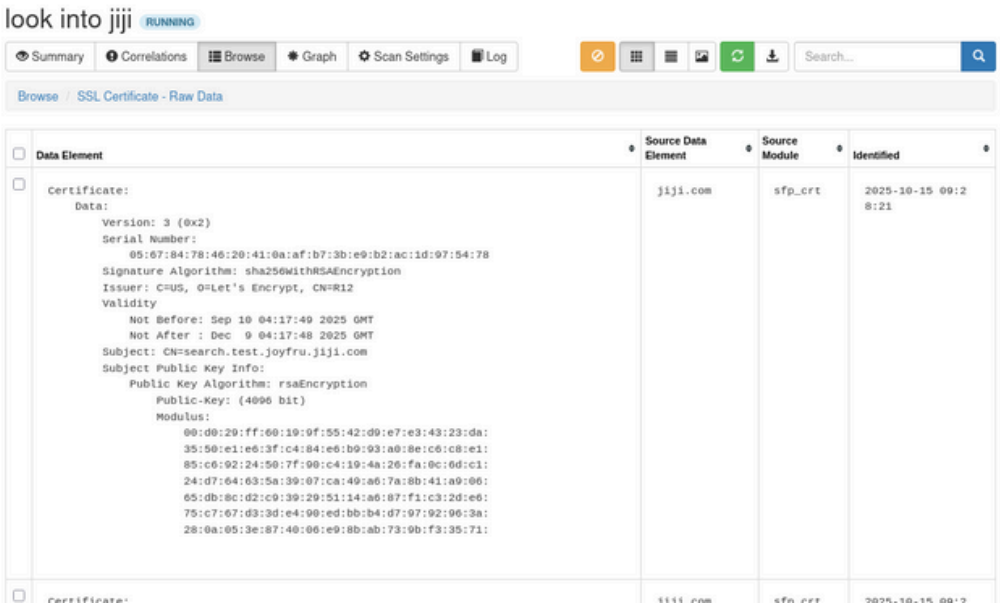

look into jiji RUNNING

Summary | Correlations | Browse | Graph | Scan Settings | Log

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Company Name	1	1	2025-10-15 09:28:11
Affiliate - Domain Name	5	7	2025-10-15 09:24:50
Affiliate - Domain Whois	4	4	2025-10-15 09:28:11
Affiliate - Internet Name	24	24	2025-10-15 09:23:39
Affiliate - Internet Name - Unresolved	4	5	2025-10-15 09:23:38
Affiliate Description - Abstract	1	1	2025-10-15 09:19:36
Affiliate Description - Category	6	6	2025-10-15 09:19:36
BGP AS Membership	6	20	2025-10-15 09:24:33
Blacklisted Internet Name	3	3	2025-10-15 09:27:41
Cloud Storage Bucket	2	2	2025-10-15 09:14:53
Cloud Storage Bucket Open	1	1	2025-10-15 09:11:25
Company Name	2	2	2025-10-15 09:17:35
Country Name	2	2	2025-10-15 09:28:24
DNS SPF Record	5	5	2025-10-15 09:24:22
DNS TXT Record	8	8	2025-10-15 09:24:22
Description - Abstract	1	3	2025-10-15 09:27:33
Description - Category	1	3	2025-10-15 09:27:33
Domain Name	1	6	2025-10-15 09:24:41
Domain Registrar	1	1	2025-10-15 09:14:09
Domain Whois	1	1	2025-10-15 09:14:09
Email Address	9	9	2025-10-15 09:25:37
Email Address - Generic	1	1	2025-10-15 09:20:22
Email Gateway (DNS MX Records)	4	4	2025-10-15 09:23:34
IPv6 Address	10	10	2025-10-15 09:25:52
Internet Name	139	337	2025-10-15 09:28:22
Internet Name - Unresolved	85	165	2025-10-15 09:25:52

Did you know SpiderFoot also has a CLI? Check out our asciinema tutorials on how to use it.

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


look into jiji RUNNING

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: 05:67:84:78:46:20:41:0a:af:b7:3b:e9:b2:ac:1d:97:54:78 Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, O=Let's Encrypt, CN=R12 Validity Not Before: Sep 10 04:17:49 2025 GMT Not After : Dec 9 04:17:48 2025 GMT Subject: CN=search.test.joyfru.jiji.com Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (4096 bit) Modulus: 00:d0:29:ff:60:19:9f:55:42:d9:e7:e3:43:23:da: 35:50:e1:e6:3f:c4:84:e6:b9:03:a0:8e:c6:c8:e1: 85:c6:92:24:50:7f:90:c4:19:4a:26:fa:0c:6d:c1: 24:d7:64:63:5a:39:07:ca:49:a6:7a:8b:41:a9:06: 65:db:8c:d2:c9:39:29:51:14:a6:87:f1:c3:2d:e6: 75:c7:67:d3:3d:e4:90:ed:bb:b4:d7:97:92:96:3a: 28:0a:05:3e:87:40:06:e9:8b:ab:73:9b:f3:35:71:	jiji.com	sfp_crt	2025-10-15 09:28:21
Certificate:	jiji.com	sfp_crt	2025-10-15 09:2

Conclusion:

This passive reconnaissance exercise has provided valuable insight into the target domain exposed surface. By leveraging publicly available information and OSINT techniques, have identify potential vulnerabilities and area of concern. These findings can be used to inform future security assessments, improve defensive measures and enhance overall cybersecurity posture.

Recomendations:

1. Domain Security: Review DNS record and ensure proper configuration to prevent DNS enumeration attacks.
2. Security Monitoring: Monitor domain reputation and security feeds regularly for potential threats.
3. Incident Response: Develop and regularly test incident response plan to address potential security incidents.