Sri Lanka Institute of Information Technology

Specializing in Cyber Security.

IE2062 - Web Security

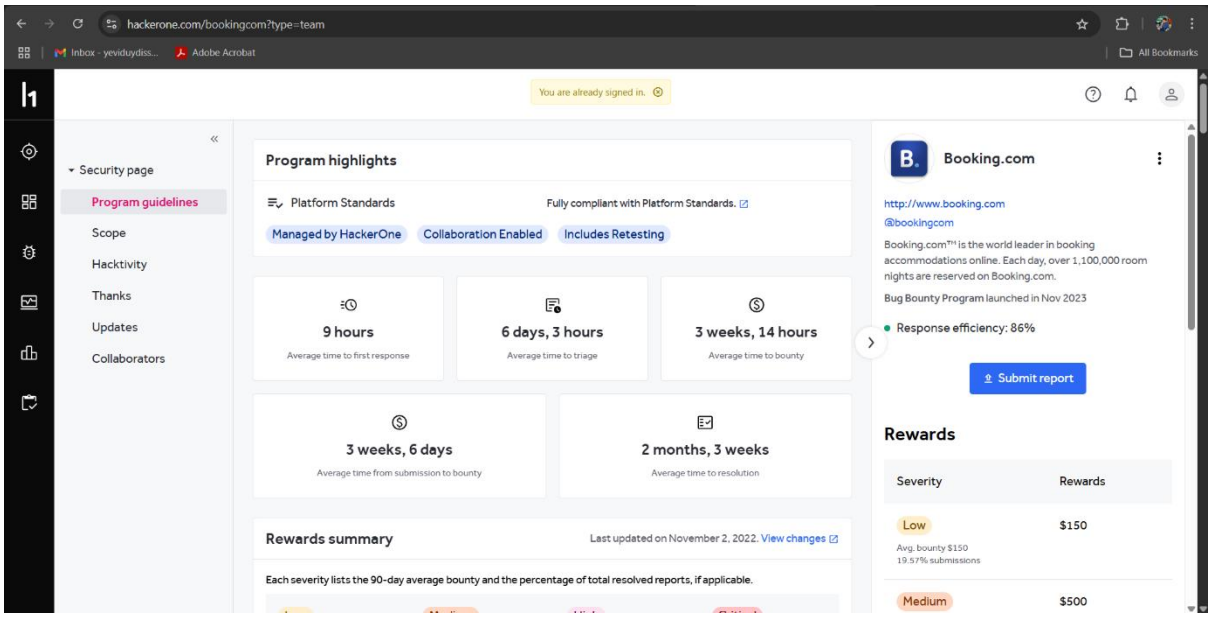
Bug Bounty Assignment

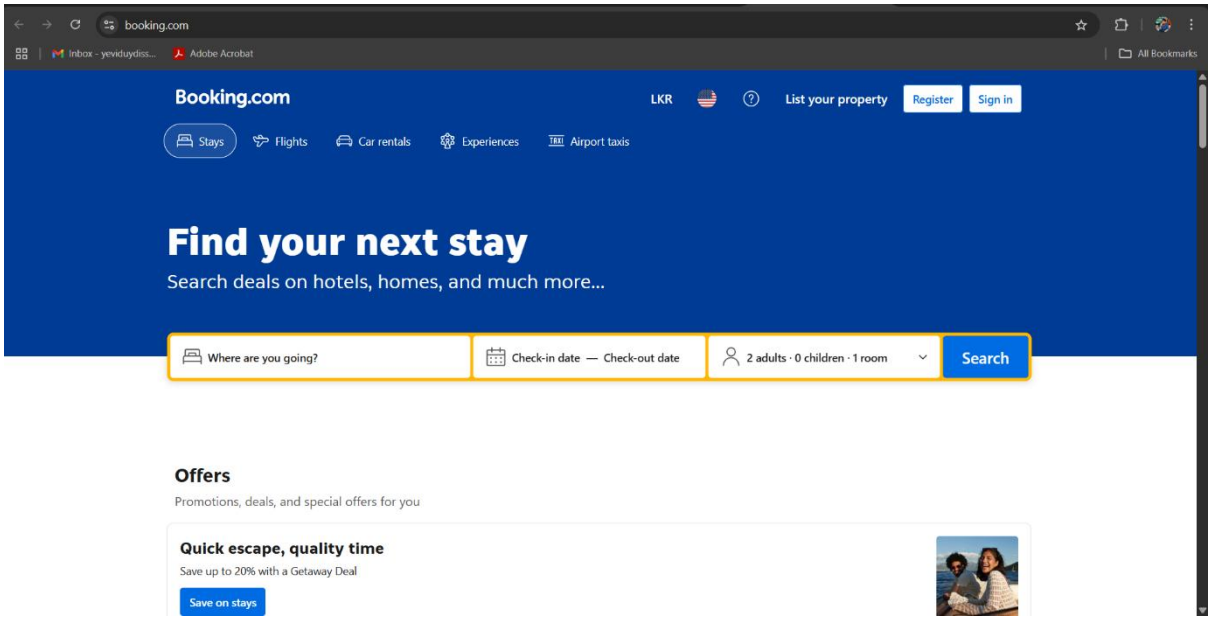
IT23238794 – DISSANAYAKE Y Y

Table of Contents

Report 01

One of the top online travel agencies in the world, Booking.com (http://www.booking.com/), is the target of this Bug Bounty report. Through its website and mobile app, the company helps millions of passengers to make reservations for lodging, flights, rental cars, and other travel-related activities. Booking.com is present in more than 220 nations and territories, offers multilingual services, and manages significant amounts of private client data every day.

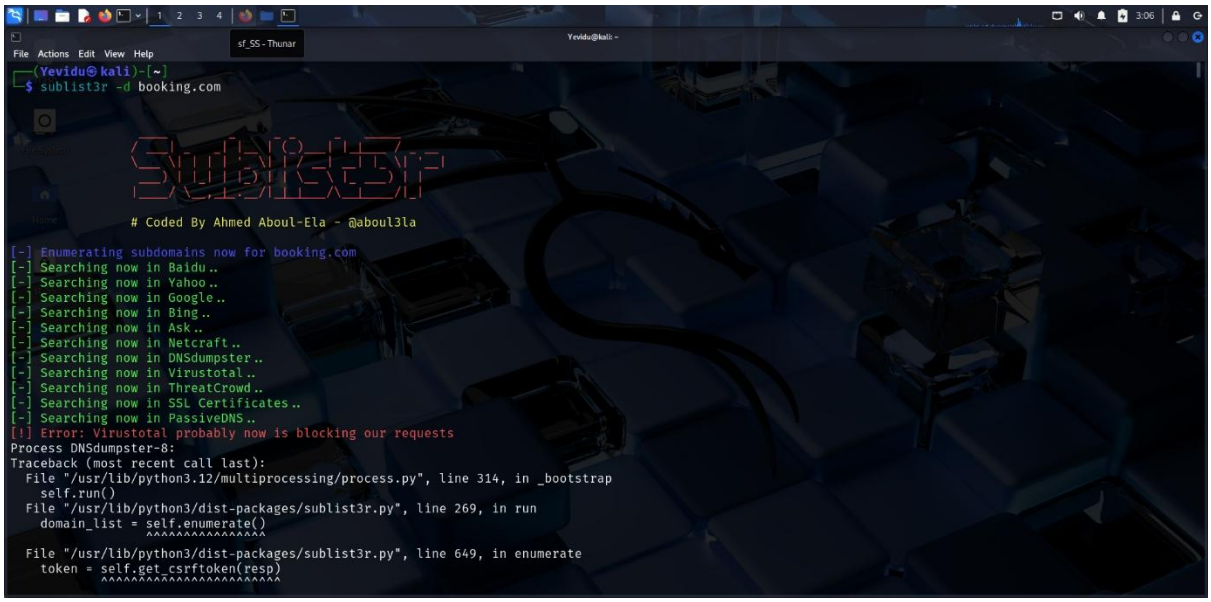


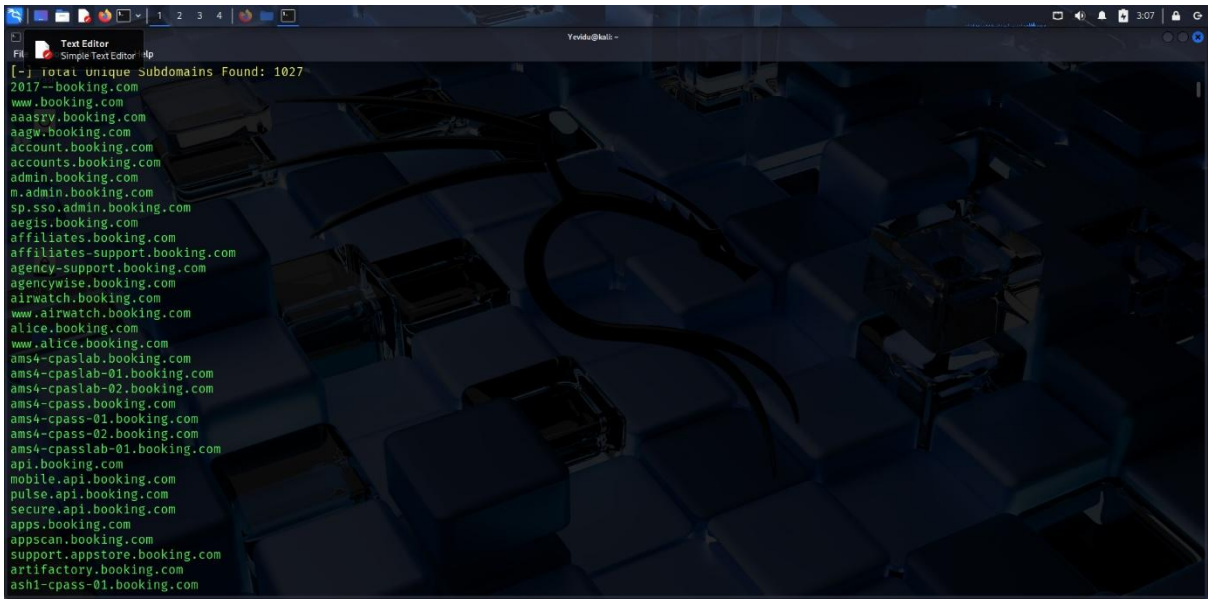


Target Reconnaissance.

Sublist3r

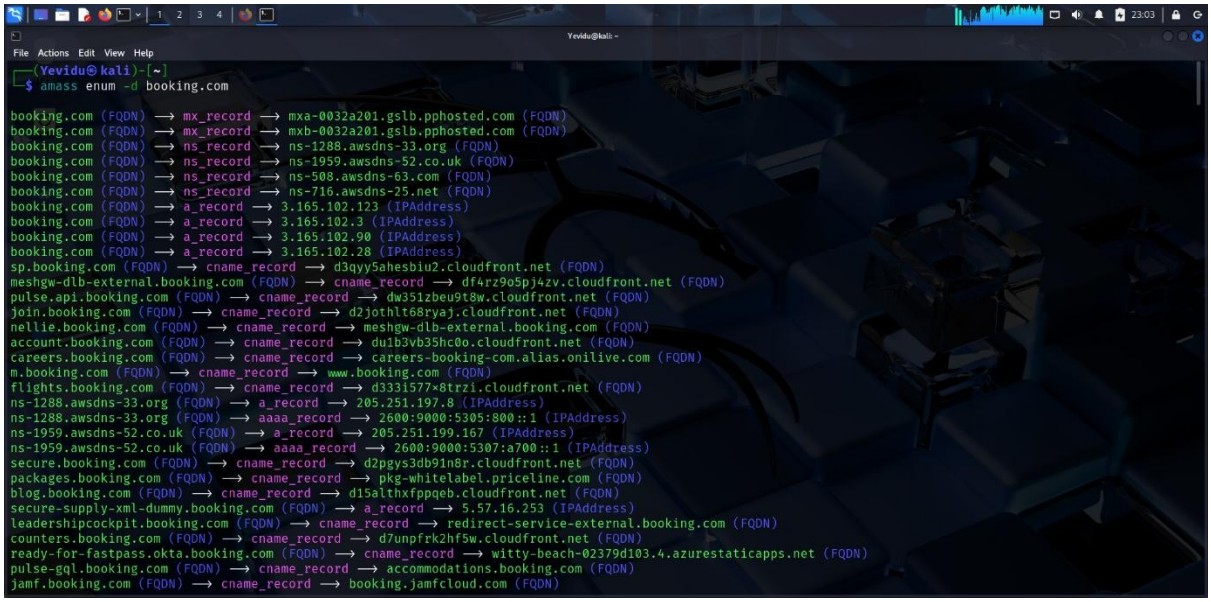
By scanning Booking.com with Sublist3r I found subdomains like these.

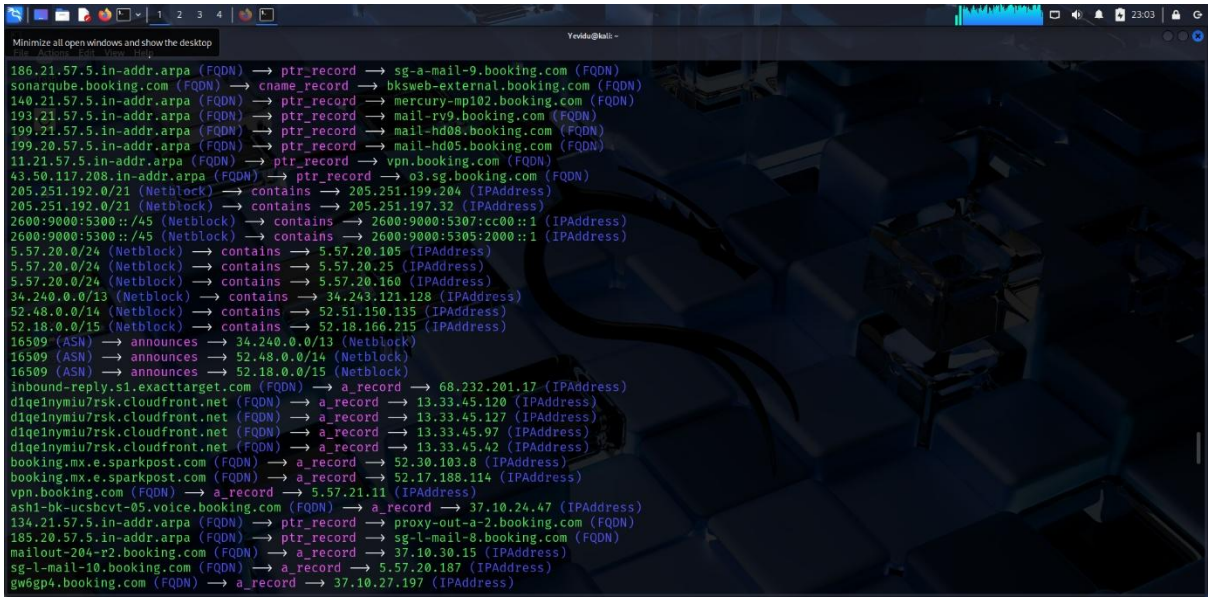




Amass

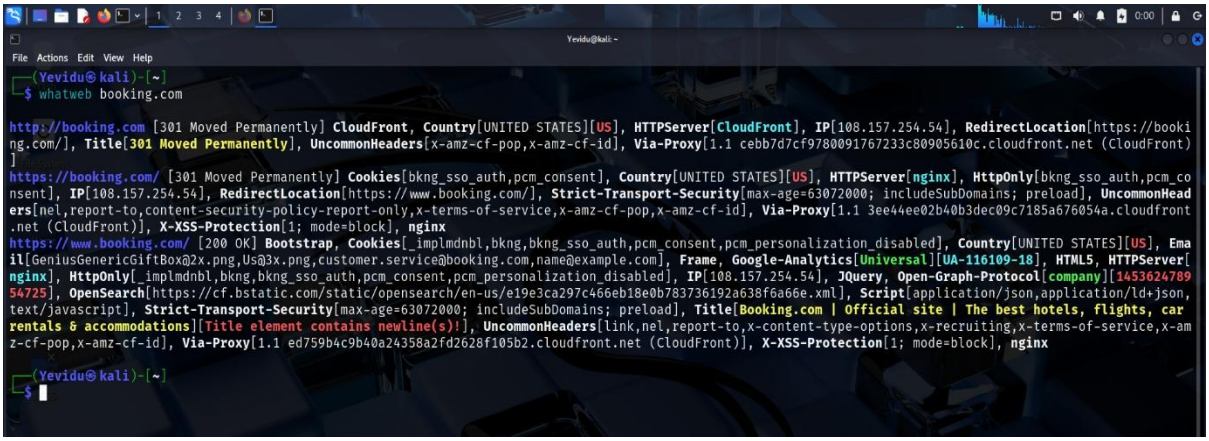
Amass is best known for discovering subdomains of a target domain. It can resolve DNS records and the process of mapping out all subdomains and associated services that may be exposed to the internet aids in the identification of possible entry points.





Whatweb

WhatWeb analyses HTTP replies and content to determine the technologies that a website uses. It provides information on the web server, analytics tools, content management systems (CMS), frameworks, and plugins, among other things.



Initial servers:

Amazon's CDN, CloudFront, is available at http://booking.com.

Both https://booking.com and https://www.booking.com use a nginx web server.

Technology Found:

Frontend framework Bootstrap

The JavaScript library, or jQuery

HTML5

Google Analytics (ID: UA-116109-18, Universal Analytics)

OpenSearch (format for search engine plugins)

Open Graph Protocol (for integrating social media)

Scripts for application/json and application/ld+json

Nslookup

The Nslookup used to obtain information about domain names and IP addresses.

Server: 192.168.43.2

Address: 192.168.43.195#53

Non-authoritative answer:

Name: booking.com

Address: 100.157.254.54

Name: booking.com

Address: 100.157.254.89

Name: booking.com

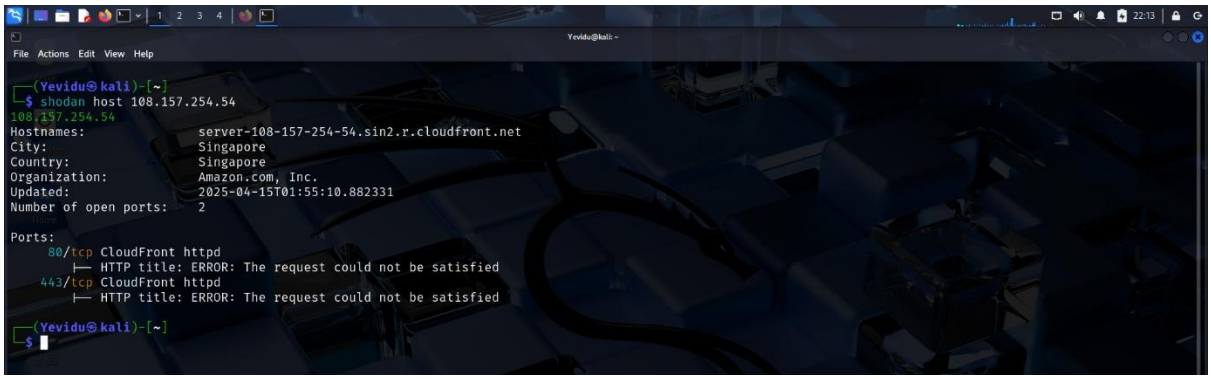
Address: 100.157.254.31

Name: booking.com

Address: 100.157.254.120

Shodan

Use Shodan to search for IP addresses and server locations, Open ports and technologies used and possibly exposed services or staging environments.



108.157.254.54

Hostnames: server-108-157-254-54.sin2.r.cloudfront.net

City: Singapore

Country: Singapore

Organization: Amazon.com, Inc.

Updated: 2025-04-15T01:55:10.882331

Number of open ports: 2

Ports:

80/tcp CloudFront httpd

└─ HTTP title: ERROR: The request could not be satisfied

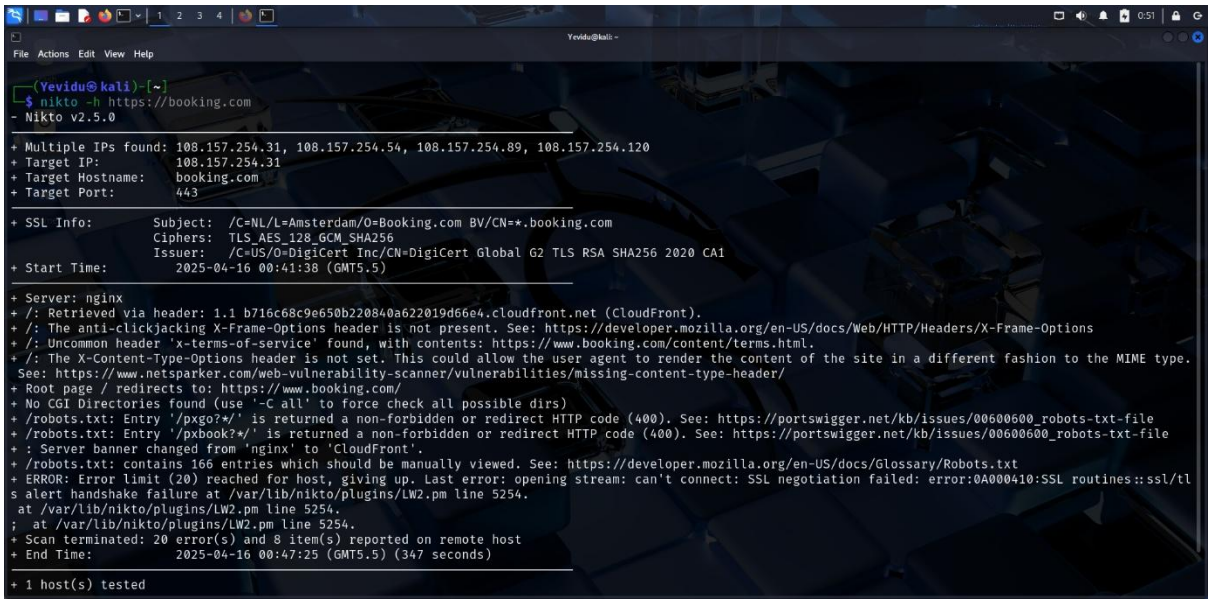
443/tcp CloudFront httpd

└─ HTTP title: ERROR: The request could not be satisfied

Scanning and vulnerability identification.

Nikto

It Checks for common server misconfigurations, Identifies outdated web server versions, perform basic checks on SSL certificates and weak SSL/TLS ciphers.

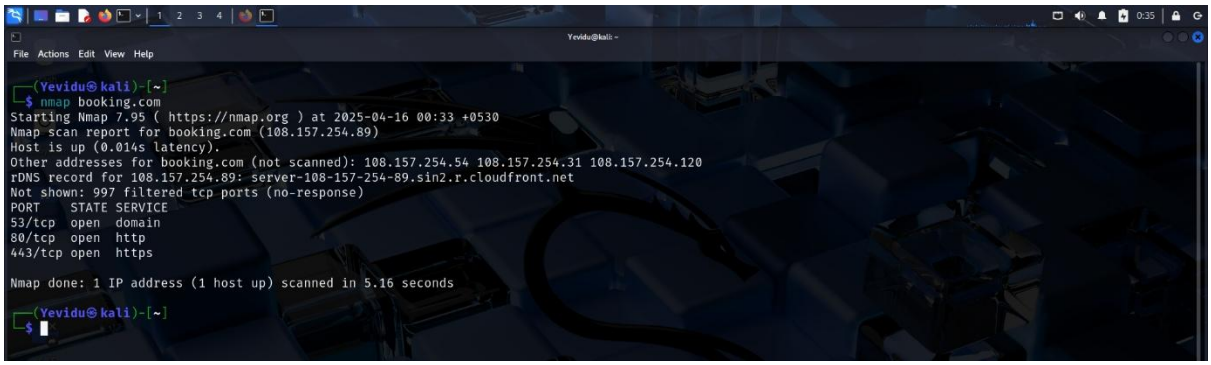


- Missing security headers:
    - X-Frame-Options - The possibility of clickjacking.
    - X-Content-Type-Options - Risk of sniffing of the MIME type.

- Uncommon headers like x-terms-of-service.
- Error limit reached: this could be a sign of WAF or scanning resistance.

Nmap

An effective and popular open-source tool for network discovery and security auditing (port scanning) in cybersecurity.

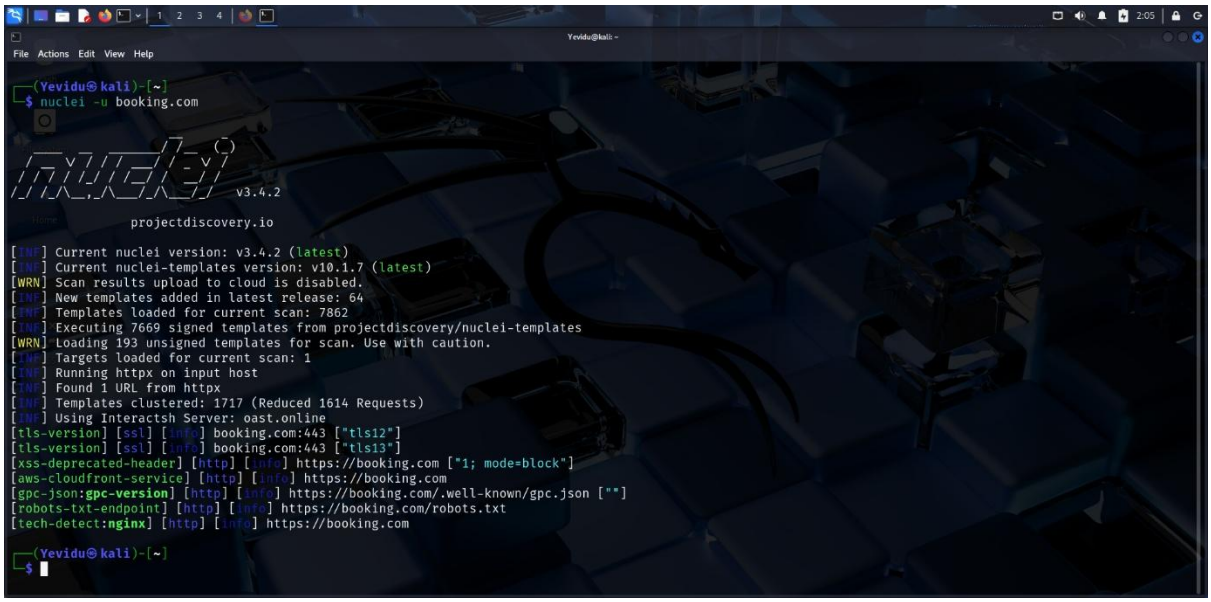


- Very typical open ports include 80 (HTTP), 443 (HTTPS), and 53 (DNS).
- Hosted on CloudFront – helps you understand infrastructure.

Nuclei

Scan for known vulnerabilities (CVEs), misconfigurations, outdated software. To test for things like open APIs, exposed admin panels, and login forms, create your own templates or use pre-existing ones.

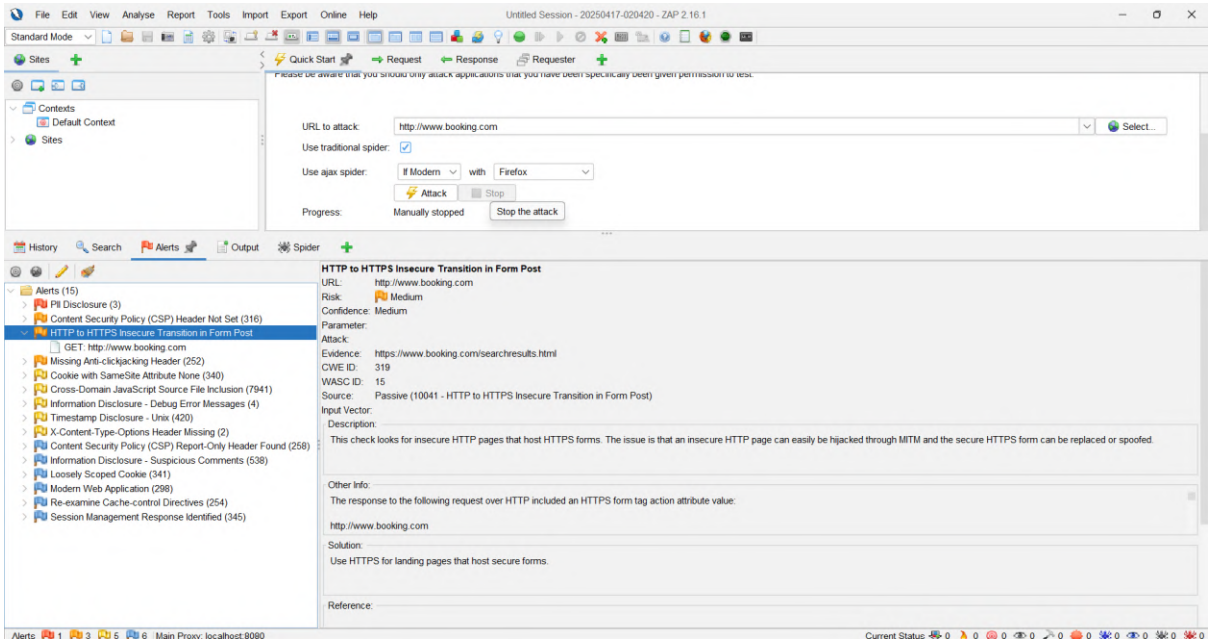
Identify technologies, frameworks, and sensitive files.

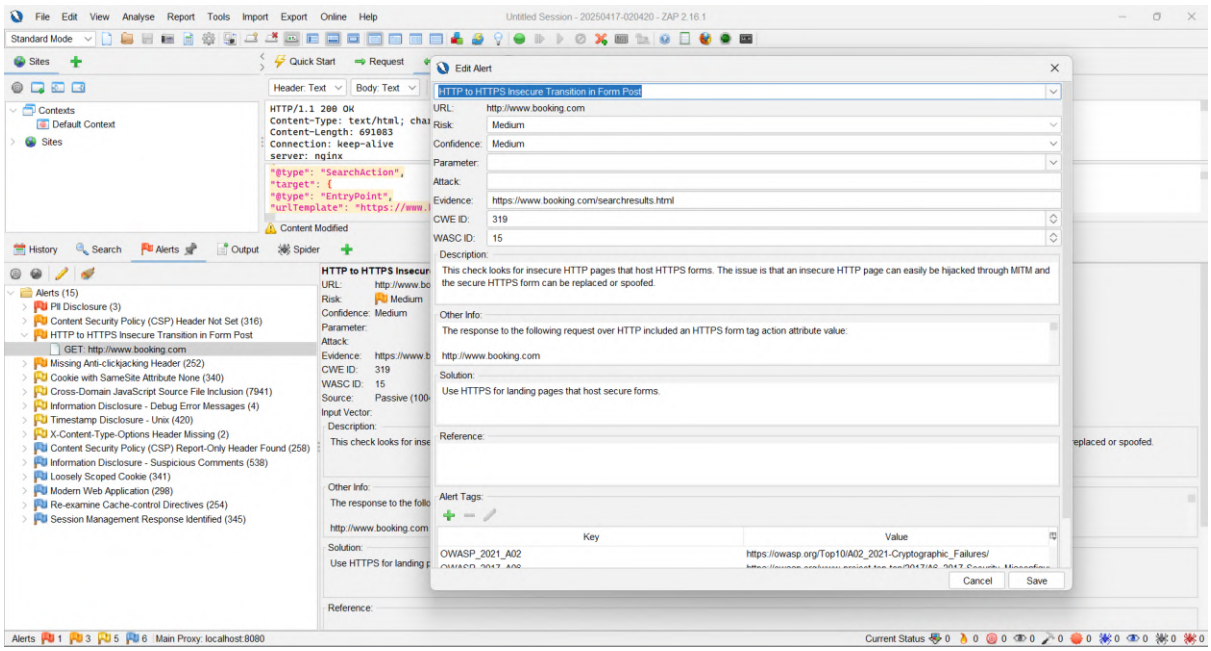


- TLS Versions supported: TLS 1.2 and 1.3.
- nginx detected – helps know server tech stack.
- Cross-domain JavaScript file inclusion.

OWASP ZAP

ZAP can automatically scan websites for common vulnerabilities.





Alerts found.

- PII Disclosure
- Content Security Policy (CSP) Header Not Set
- HTTP to HTTPS Insecure Transition in Form Post
- Missing Anti-clickjacking Header
- Cookie with SameSite Attribute None
- Cross-Domain JavaScript Source File Inclusion
- Information Disclosure - Debug Error Messages
- Timestamp Disclosure - Unix
- X-Content-Type-Options Header Missing
- Content Security Policy (CSP) Report-Only Header Found
- Information Disclosure - Suspicious Comments
- Loosely Scoped Cookie
- Modern Web Application
- Re-examine Cache-control Directives
- Session Management Response Identified

Vulnerabilities.

- **Security Misconfiguration**

Issues Found:

- Important security headers are missing:

  The absence of the X-Frame-Options header makes it vulnerable to clickjacking.

  The absence of the X-Content-Type-Options header increases the possibility of MIME sniffing.

- Unusual custom headers (x-terms-of-service) were found; this could cause internal information to leak.

- Reaching the error limit in Nikto → signifies both the existence of WAF and some configuration errors (e.g., no suitable rate limiting message).

Risk:

- The attack surface is increased when security headers are missing, leaving the website open to clickjacking and MIME-based attacks.

- Attackers may use malicious iframes to frame the Booking.com website or deceive browsers into opening the wrong kinds of files.

How This Needs to Be Reduced:

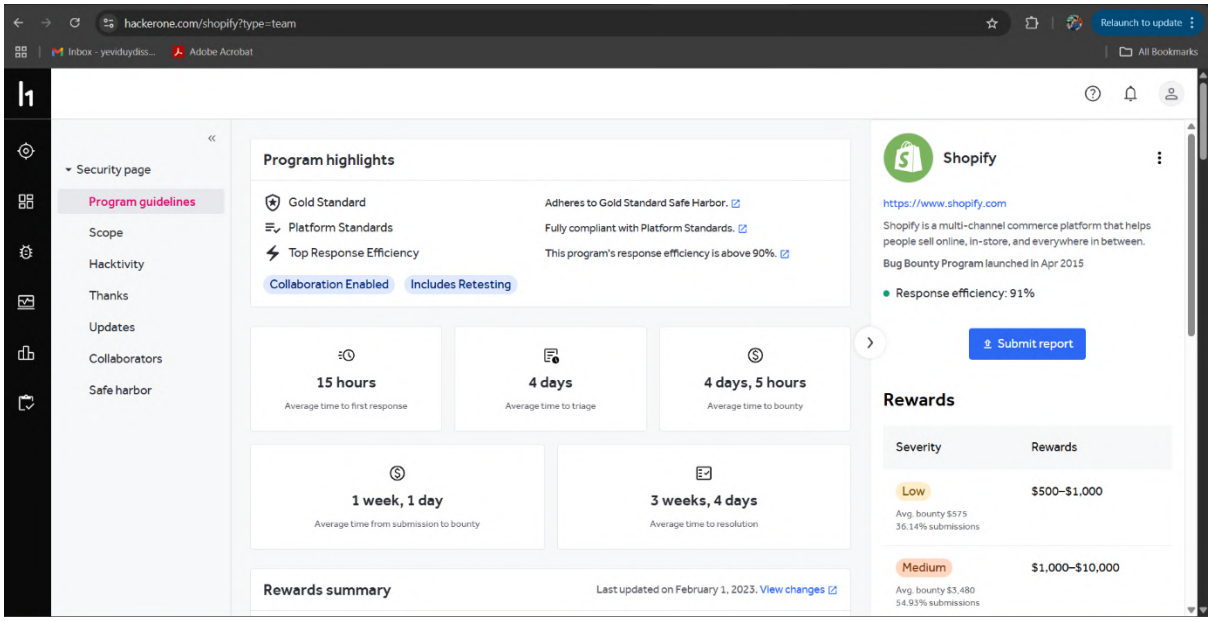
- To stop clickjacking, add the X-Frame-Options: DENY or SAMEORIGIN header.

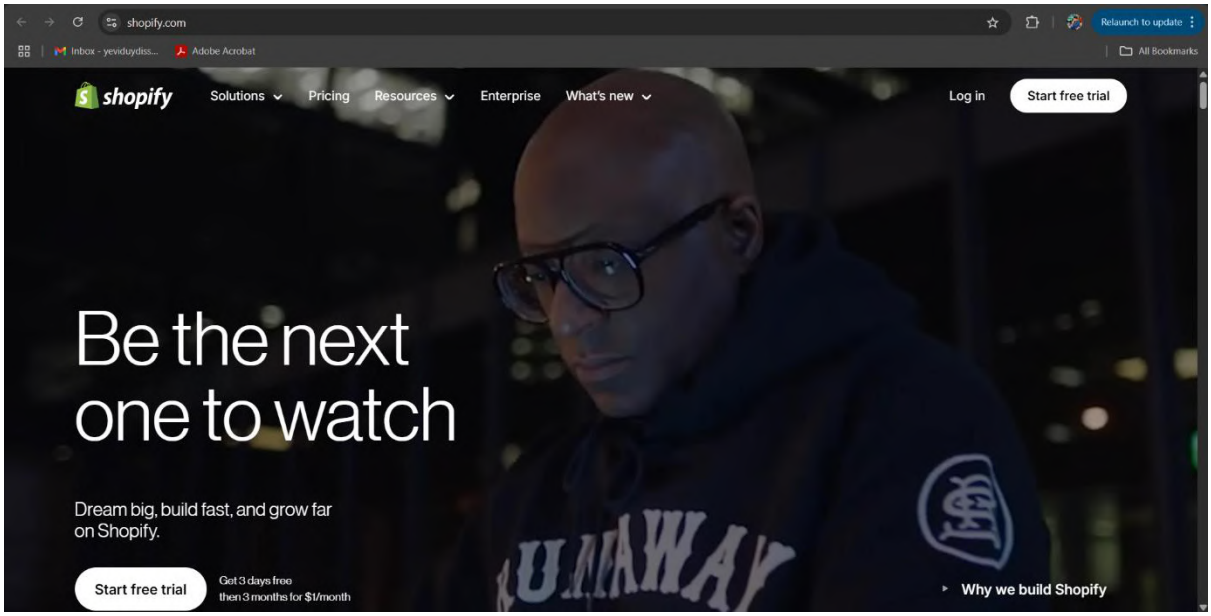
- To stop MIME type sniffing, include the X-Content-Type-Options: nosniff header.

- To guarantee low leakage, verify server and security settings on a regular basis.

Report 02

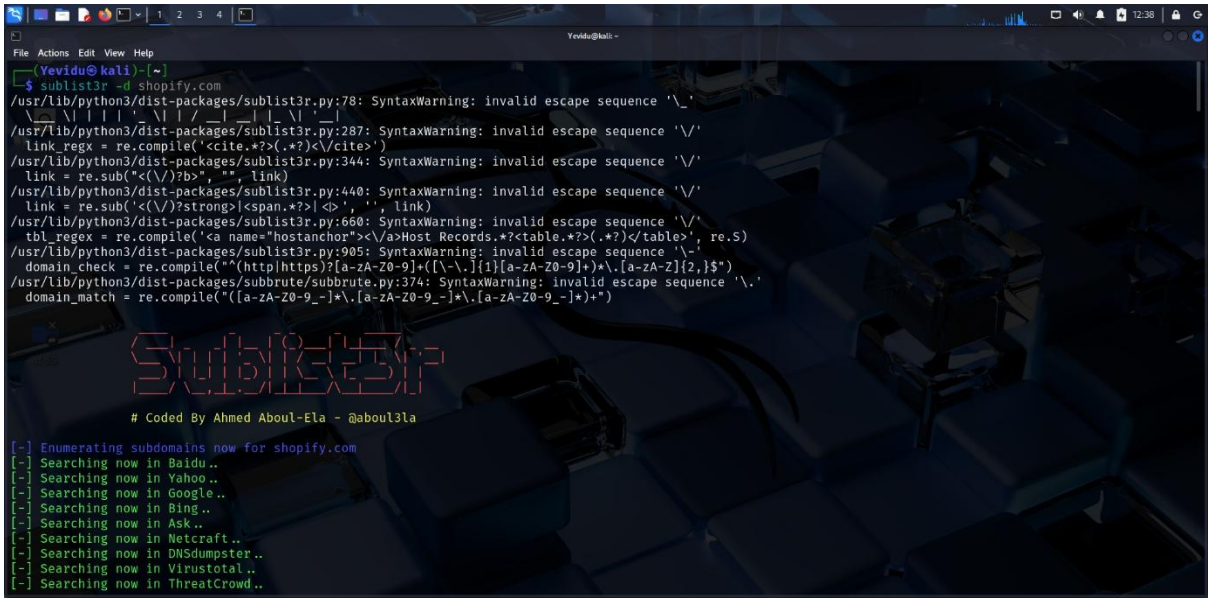
This Bug Bounty report focuses on Shopify (https://www.shopify.com/), one of the top e-commerce systems in the world. The company gives millions of companies the ability to set up and run their own online stores in more than 175 countries. Shopify serves businesses of all sorts, from tiny startups to well-known brands, by providing tools for inventory management, payment processing, marketing, and shipping through its website and numerous integrations. Shopify manages a huge amount of sensitive merchant and customer data everyday thanks to its multilingual features and wide worldwide reach.

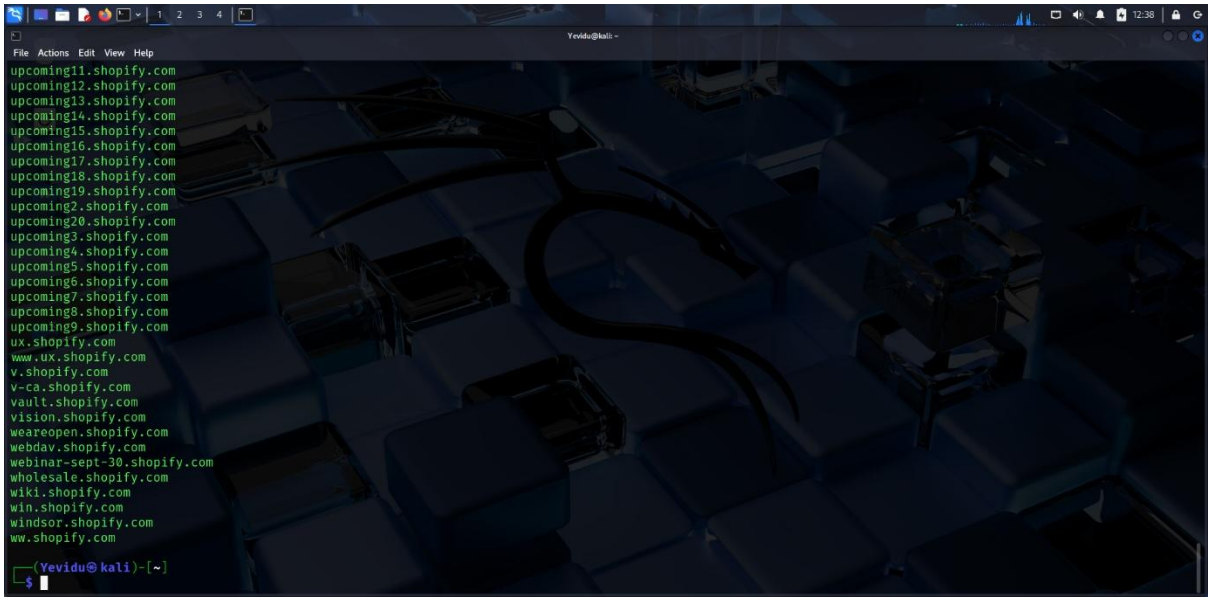




Target Reconnaissance.

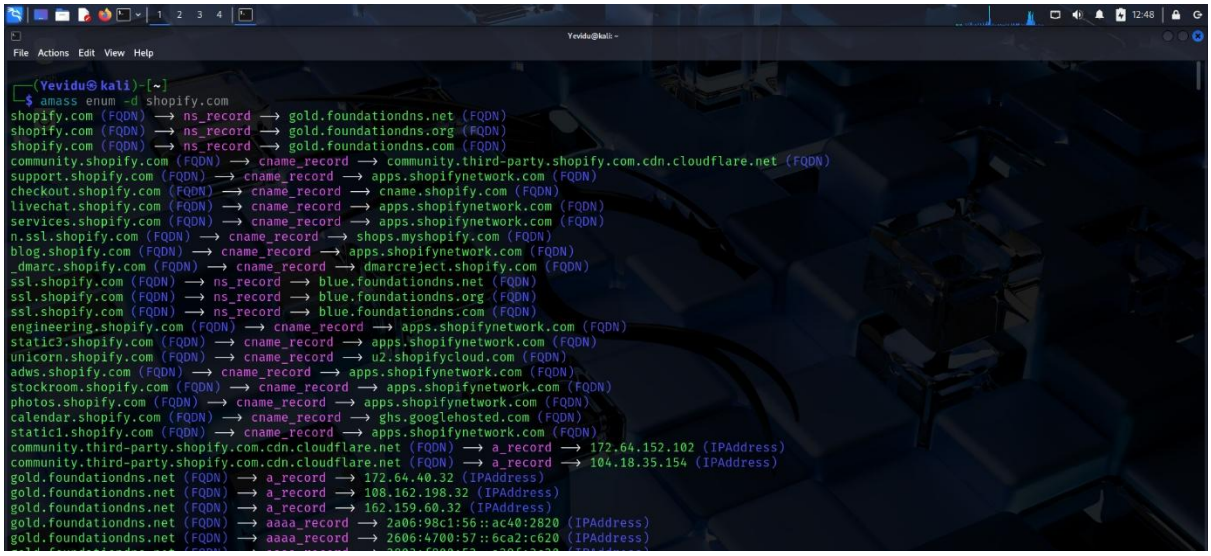
Sublist3r

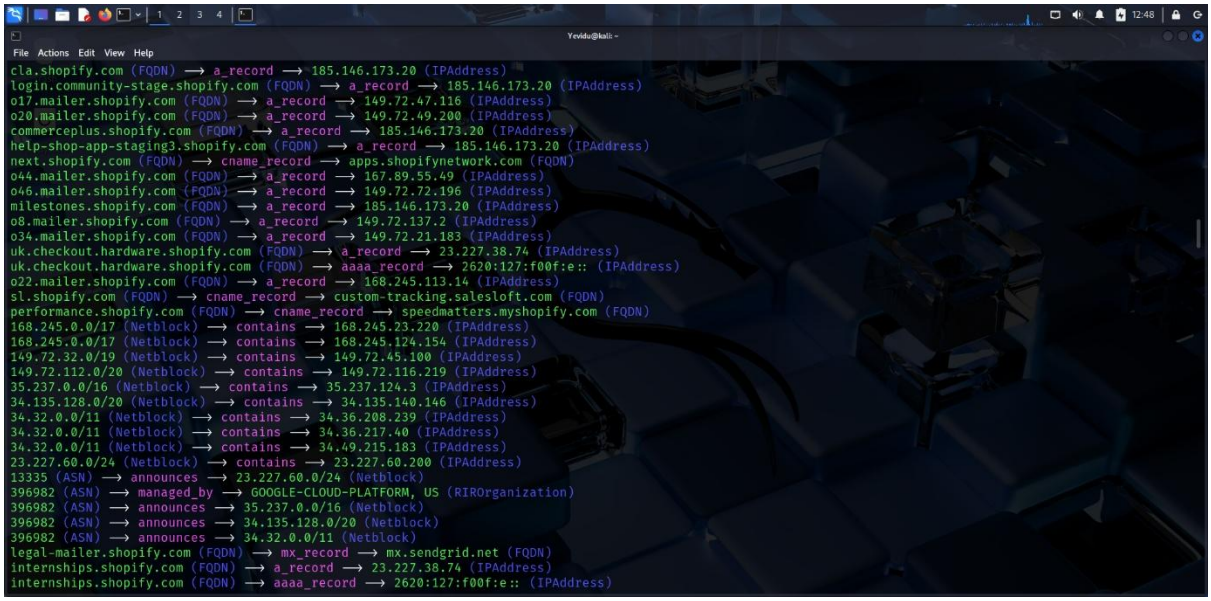


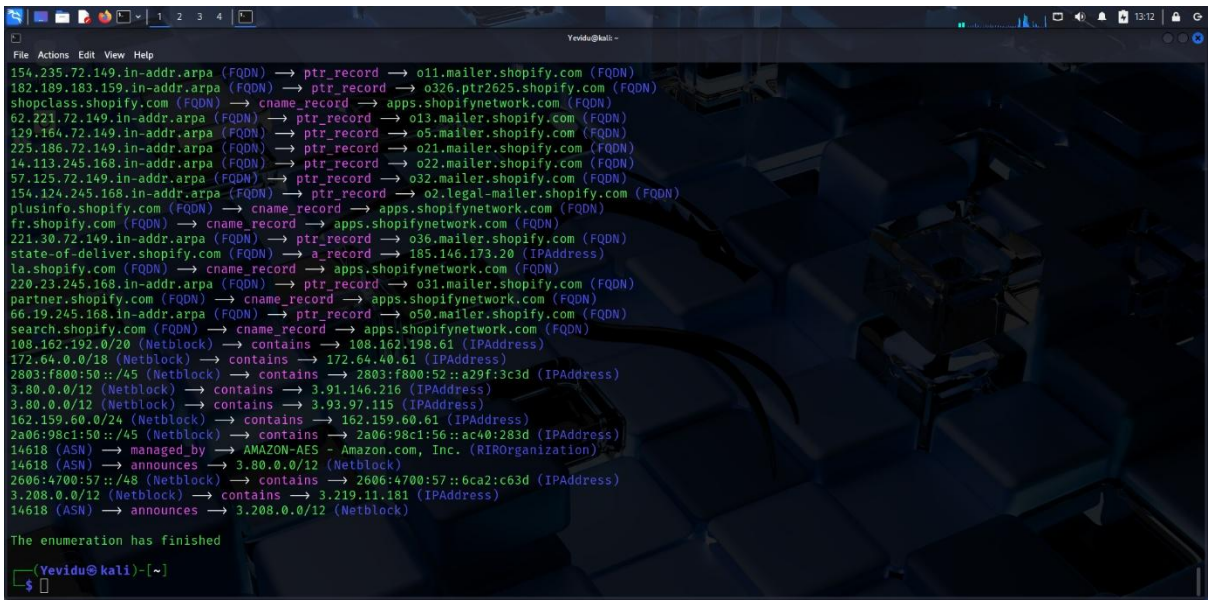


The subdomains include a succession of "upcoming" subdomains (e.g., upcoming11.shopify.com, upcoming12.shopify.com, etc.), as well as other subdomains like ux.shopify.com, vault.shopify.com, vision.shopify.com, win.shopify.com, and http://www.shopify.com/.

Amass


File Actions Edit View Help
(Yevidu㉿kali)-[~]
$ amass enum -d shopify.com
shopify.com (FQDN) --> ns_record --> gold.foundationdns.net (FQDN)
shopify.com (FQDN) --> ns_record --> gold.foundationdns.org (FQDN)
shopify.com (FQDN) --> ns_record --> gold.foundationdns.com (FQDN)
community.shopify.com (FQDN) --> cname_record --> community.third-party.shopify.com.cdn.cloudflare.net (FQDN)
support.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
checkout.shopify.com (FQDN) --> cname_record --> cname.shopify.com (FQDN)
livechat.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
services.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
n.ssl.shopify.com (FQDN) --> cname_record --> shops.myshopify.com (FQDN)
blog.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
_dmarc.shopify.com (FQDN) --> cname_record --> dmarcreject.shopify.com (FQDN)
ssl.shopify.com (FQDN) --> ns_record --> blue.foundationdns.net (FQDN)
ssl.shopify.com (FQDN) --> ns_record --> blue.foundationdns.org (FQDN)
ssl.shopify.com (FQDN) --> ns_record --> blue.foundationdns.com (FQDN)
engineering.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
static3.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
unicorn.shopify.com (FQDN) --> cname_record --> u2.shopifycloud.com (FQDN)
adws.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
stockroom.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
photos.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
calendar.shopify.com (FQDN) --> cname_record --> ghs.googlehosted.com (FQDN)
static1.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
community.third-party.shopify.com.cdn.cloudflare.net (FQDN) --> a_record --> 172.64.152.102 (IPAddress)
community.third-party.shopify.com.cdn.cloudflare.net (FQDN) --> a_record --> 104.18.35.154 (IPAddress)
gold.foundationdns.net (FQDN) --> a_record --> 172.64.40.32 (IPAddress)
gold.foundationdns.net (FQDN) --> a_record --> 108.162.198.32 (IPAddress)
gold.foundationdns.net (FQDN) --> a_record --> 162.159.60.32 (IPAddress)
gold.foundationdns.net (FQDN) --> aaaa_record --> 2a06:98c1:56::ac40:2820 (IPAddress)
gold.foundationdns.net (FQDN) --> aaaa_record --> 2606:4700:57::6ca2:c620 (IPAddress)


File Actions Edit View Help
cla.shopify.com (FQDN) --> a_record --> 185.146.173.20 (IPAddress)
login.community-stage.shopify.com (FQDN) --> a_record --> 185.146.173.20 (IPAddress)
o17.mailer.shopify.com (FQDN) --> a_record --> 149.72.47.116 (IPAddress)
o20.mailer.shopify.com (FQDN) --> a_record --> 149.72.49.200 (IPAddress)
commerceplus.shopify.com (FQDN) --> a_record --> 185.146.173.20 (IPAddress)
help-shop-app-staging3.shopify.com (FQDN) --> a_record --> 185.146.173.20 (IPAddress)
next.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
o44.mailer.shopify.com (FQDN) --> a_record --> 167.89.55.49 (IPAddress)
o46.mailer.shopify.com (FQDN) --> a_record --> 149.72.72.196 (IPAddress)
milestones.shopify.com (FQDN) --> a_record --> 185.146.173.20 (IPAddress)
o8.mailer.shopify.com (FQDN) --> a_record --> 149.72.137.2 (IPAddress)
o34.mailer.shopify.com (FQDN) --> a_record --> 149.72.21.183 (IPAddress)
uk.checkout.hardware.shopify.com (FQDN) --> a_record --> 23.227.38.74 (IPAddress)
uk.checkout.hardware.shopify.com (FQDN) --> aaaa_record --> 2620:127:f00f:e:: (IPAddress)
o22.mailer.shopify.com (FQDN) --> a_record --> 168.245.113.14 (IPAddress)
sl.shopify.com (FQDN) --> cname_record --> custom-tracking.salesloft.com (FQDN)
performance.shopify.com (FQDN) --> cname_record --> speedmatters.myshopify.com (FQDN)
168.245.0.0/17 (Netblock) --> contains --> 168.245.23.220 (IPAddress)
168.245.0.0/17 (Netblock) --> contains --> 168.245.124.154 (IPAddress)
149.72.32.0/19 (Netblock) --> contains --> 149.72.45.100 (IPAddress)
149.72.112.0/20 (Netblock) --> contains --> 149.72.116.219 (IPAddress)
35.237.0.0/16 (Netblock) --> contains --> 35.237.124.3 (IPAddress)
34.135.128.0/20 (Netblock) --> contains --> 34.135.140.146 (IPAddress)
34.32.0.0/11 (Netblock) --> contains --> 34.36.208.239 (IPAddress)
34.32.0.0/11 (Netblock) --> contains --> 34.36.217.40 (IPAddress)
34.32.0.0/11 (Netblock) --> contains --> 34.49.215.183 (IPAddress)
23.227.60.0/24 (Netblock) --> contains --> 23.227.60.200 (IPAddress)
13335 (ASN) --> announces --> 23.227.60.0/24 (Netblock)
396982 (ASN) --> managed_by --> GOOGLE-CLOUD-PLATFORM, US (RIROrganization)
396982 (ASN) --> announces --> 35.237.0.0/16 (Netblock)
396982 (ASN) --> announces --> 34.135.128.0/20 (Netblock)
396982 (ASN) --> announces --> 34.32.0.0/11 (Netblock)
legal-mailer.shopify.com (FQDN) --> mx_record --> mx.sendgrid.net (FQDN)
internships.shopify.com (FQDN) --> a_record --> 23.227.38.74 (IPAddress)
internships.shopify.com (FQDN) --> aaaa_record --> 2620:127:f00f:e:: (IPAddress)


File Actions Edit View Help
154.235.72.149.in-addr.arpa (FQDN) --> ptr_record --> o11.mailer.shopify.com (FQDN)
182.189.183.159.in-addr.arpa (FQDN) --> ptr_record --> o326.ptr2625.shopify.com (FQDN)
shopclass.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
62.221.72.149.in-addr.arpa (FQDN) --> ptr_record --> o13.mailer.shopify.com (FQDN)
129.164.72.149.in-addr.arpa (FQDN) --> ptr_record --> o5.mailer.shopify.com (FQDN)
225.186.72.149.in-addr.arpa (FQDN) --> ptr_record --> o21.mailer.shopify.com (FQDN)
14.113.245.168.in-addr.arpa (FQDN) --> ptr_record --> o22.mailer.shopify.com (FQDN)
57.125.72.149.in-addr.arpa (FQDN) --> ptr_record --> o32.mailer.shopify.com (FQDN)
154.124.245.168.in-addr.arpa (FQDN) --> ptr_record --> o2.legal-mailer.shopify.com (FQDN)
plusinfo.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
fr.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
221.30.72.149.in-addr.arpa (FQDN) --> ptr_record --> o36.mailer.shopify.com (FQDN)
state-of-deliver.shopify.com (FQDN) --> a_record --> 185.146.173.20 (IPAddress)
la.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
220.23.245.168.in-addr.arpa (FQDN) --> ptr_record --> o31.mailer.shopify.com (FQDN)
partner.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
66.19.245.168.in-addr.arpa (FQDN) --> ptr_record --> o50.mailer.shopify.com (FQDN)
search.shopify.com (FQDN) --> cname_record --> apps.shopifynetwork.com (FQDN)
108.162.192.0/20 (Netblock) --> contains --> 108.162.198.61 (IPAddress)
172.64.0.0/18 (Netblock) --> contains --> 172.64.40.61 (IPAddress)
2803:f800:50::/45 (Netblock) --> contains --> 2803:f800:52::a29f:3c3d (IPAddress)
3.80.0.0/12 (Netblock) --> contains --> 3.91.146.216 (IPAddress)
3.80.0.0/12 (Netblock) --> contains --> 3.93.97.115 (IPAddress)
162.159.60.0/24 (Netblock) --> contains --> 162.159.60.61 (IPAddress)
2a06:98c1:50::/45 (Netblock) --> contains --> 2a06:98c1:56::ac40:283d (IPAddress)
14618 (ASN) --> managed_by --> AMAZON-AES - Amazon.com, Inc. (RIROrganization)
14618 (ASN) --> announces --> 3.80.0.0/12 (Netblock)
2606:4700:57::/48 (Netblock) --> contains --> 2606:4700:57::6ca2:c63d (IPAddress)
3.208.0.0/12 (Netblock) --> contains --> 3.219.11.181 (IPAddress)
14618 (ASN) --> announces --> 3.208.0.0/12 (Netblock)
The enumeration has finished
(Yevidu㉿kali)-[~]
$

- NS Records - This indicates that one of the name servers for shopify.com is gold.foundationdns.net. DNS lookups are handled by name servers.

- CNAME Records - This indicates that apps.shopifynetwork.com is an alias for support.shopify.com. Support.shopify.com resolves to the IP address that apps.shopifynetwork.com points to.

  This may disclose: Backend design, Services that are shared, Dependencies for third-party services.

- A Records - This associates an IP (IPv4) with a subdomain. This IP can be used to verify Details about Shodan, DNS Reverse, Ports open, provider of hosting.

- Interesting Subdomains -

  calendar.shopify.com; ghs.googlehosted.com → Hosted on **Google**

  km.shopify.com; sendgrid.net → Related to **email marketing**

  customer.login.shopify.com; A record → Login system (potential target for auth-related bugs)

  vault.shopify.com, admin-gtm.shopify.com → High-value keywords like vault, admin

- Netblock & ASN Data - For IP ranges, the Autonomous System Number (ASN) is in charge. Cloudflare, which powers most of the Shopify's infrastructure, can: obfuscate IPs of genuine origin

  Provide defence (e.g., DDoS, WAF)

Whatweb

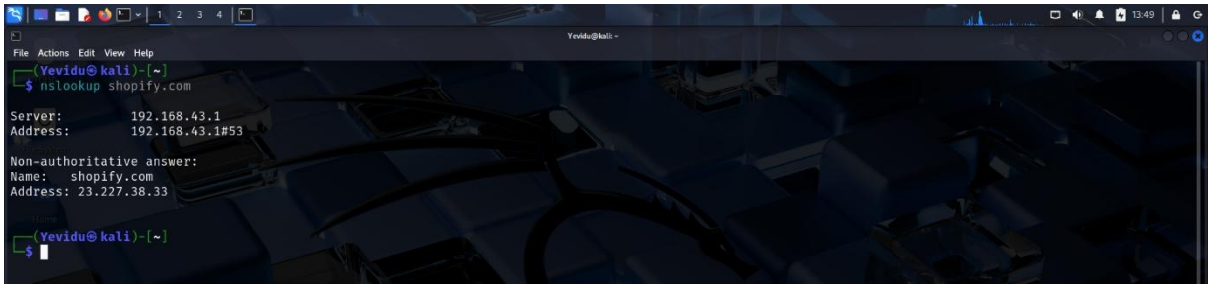
Initial Request:

- **URL -** http://shopify.com
- **Status -** 301 Moved Permanently
- **Redirects to -** https://www.shopify.com/
- **IP Address -** 23.227.38.33
- **Country -** Canada (CA)
- **Server -** Cloudflare
- **Title -** “301 Moved Permanently"
- **Security Headers & Info -**
  - X-XSS-Protection
  - X-Content-Type-Options
  - X-Permitted-Cross-Domain-Policies
  - X-Download-Options
- **Other Headers -** report-to, nel, server-timing, shopify-edge-ip, cf-ray, alt-svc

Redirected (Final Destination):

- **URL -** https://www.shopify.com/
  Status - 200 OK
  - **IP Address -** 172.64.145.93
  - **Country -** Reserved (ZZ)
  - **Server -** Cloudflare
  - **Cookies -** _shopify_s, _shopify_y
  - **Security -**
    - Strict-Transport-Security (HSTS enabled)
    - X-Content-Type-Options, cf-ray, cf-cache-status, etc.
  - **Technologies Detected -**
    - HTML5
    - Open Graph Protocol (website)
    - Scripts using application/ld+json and module
    - Powered by: "the" (might be a detection issue)
  - **Metadata -**
    - Title: "Shopify"
    - Detected Email: monique@email.com (might be fake/test data)

Nslookup

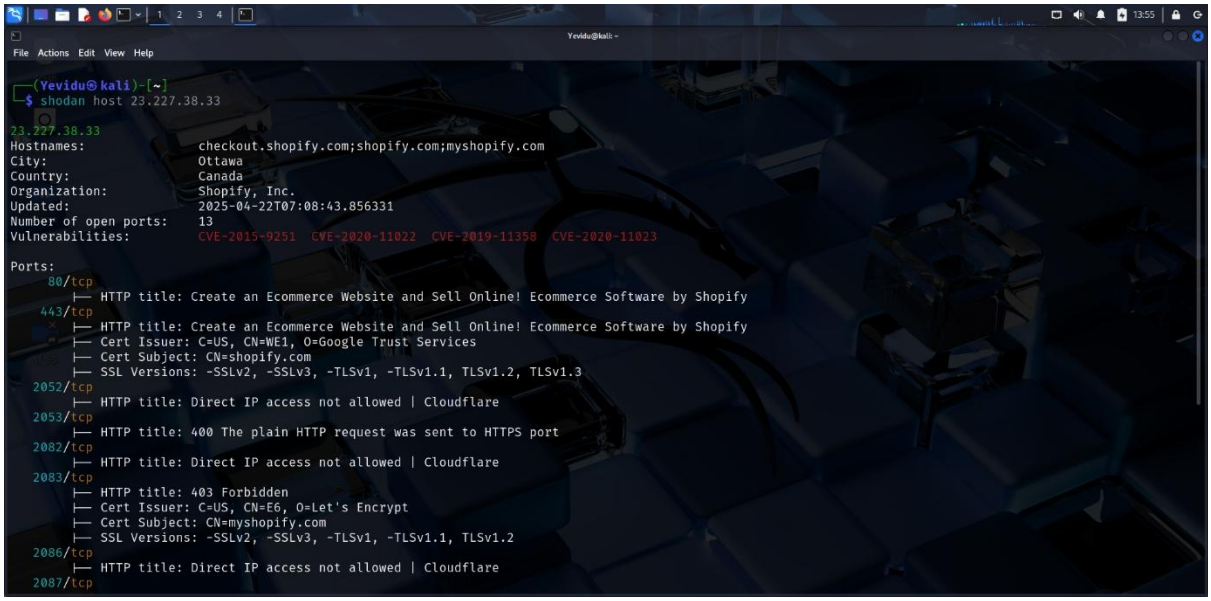


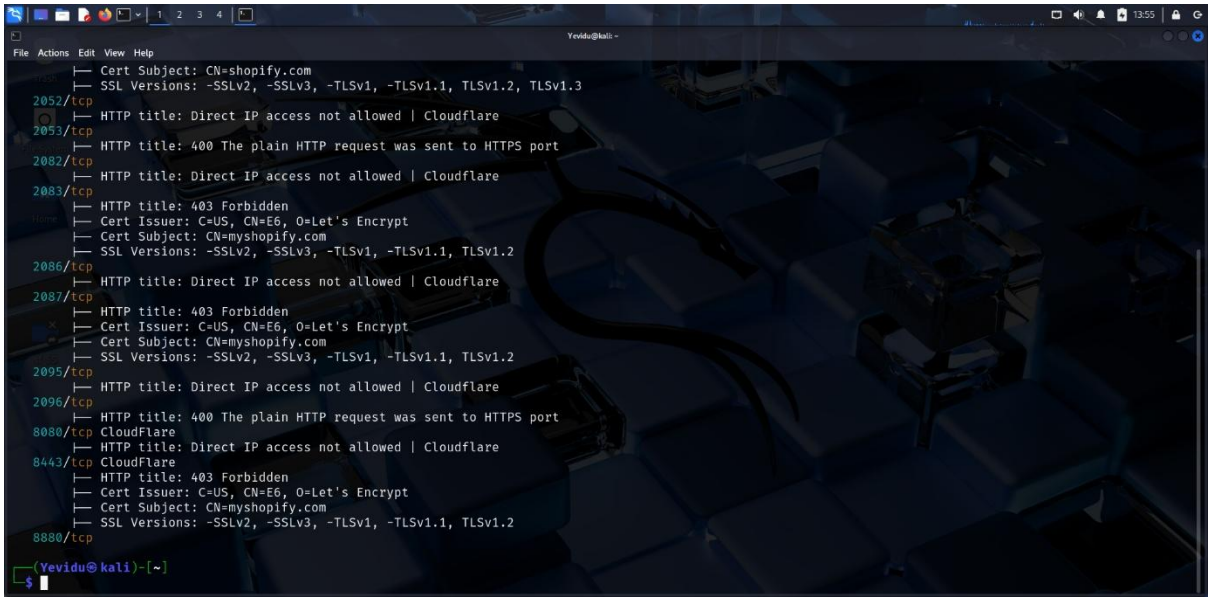
Server: 192.168.43.1
Address: 192.168.43.1#53

Non-authoritative answer:

Name: shopify.com
Address: 23.227.38.33

Shodan





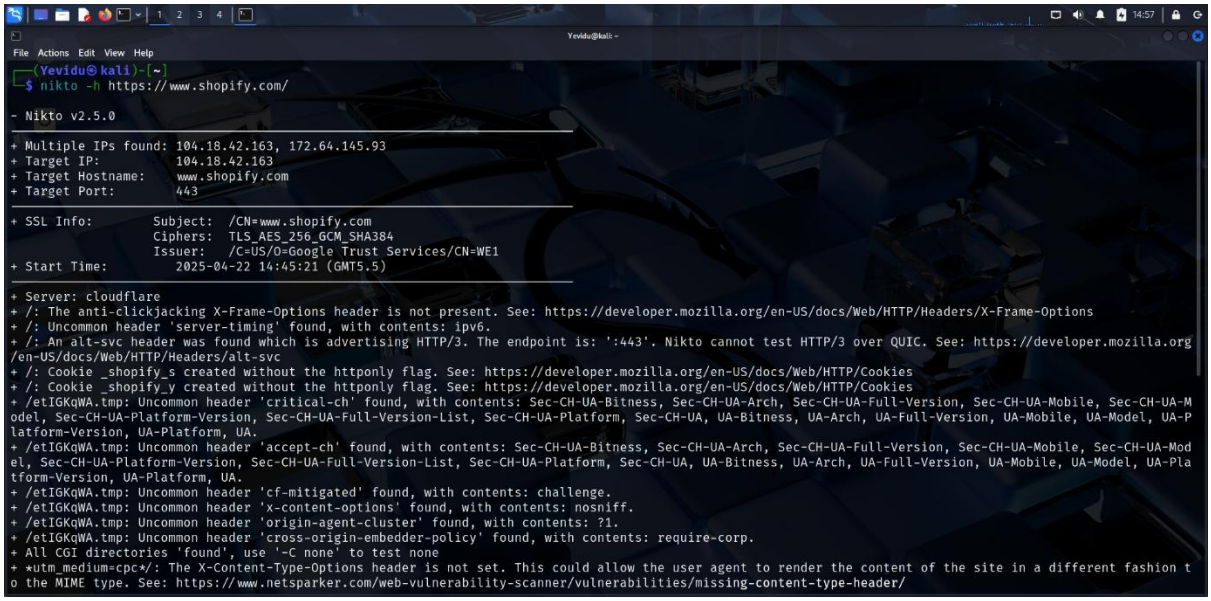
- Hostnames - checkout.shopify.com, shopify.com, myshopify.com
- Location - Ottawa, Canada CA
- Organization - Shopify, Inc.
- Last Updated on Shodan - 2025-04-22
- Open Ports Detected – 13
- Known Vulnerabilities (CVEs) –

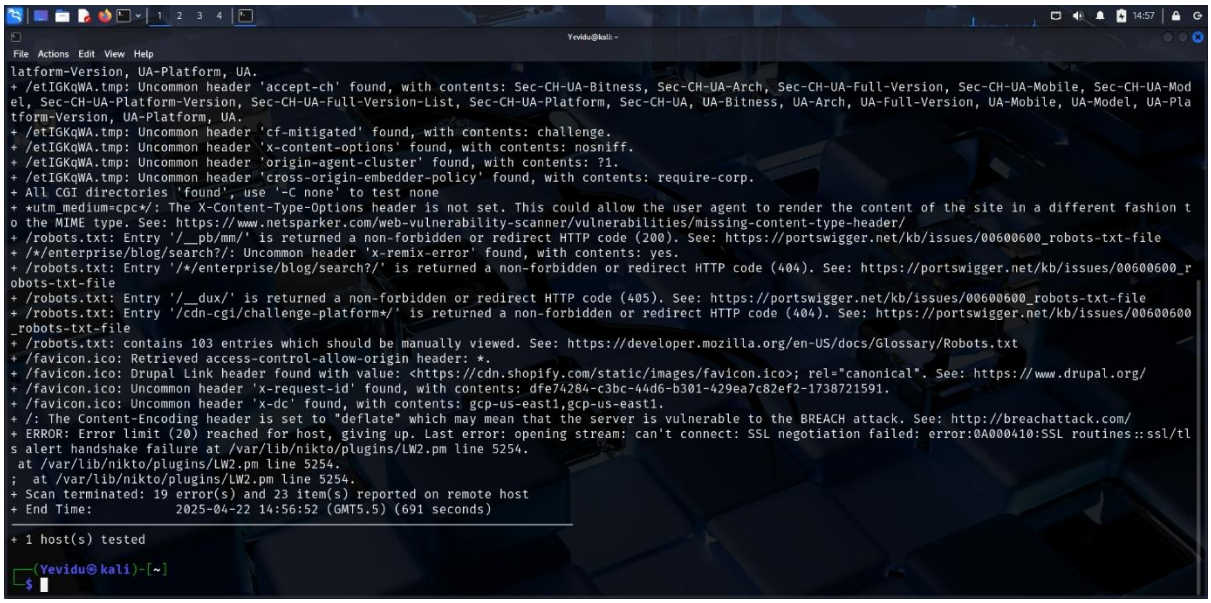
  CVE-2015-9251 – jQuery Cross-site Scripting
  CVE-2020-11022 – Improper input validation in jQuery
  CVE-2020-11023 – Improper input sanitization in jQuery
  CVE-2019-11358 – jQuery prototype pollution

Port	Service	Notes
80/tcp	HTTP	Shopify ecommerce page
443/tcp	HTTPS	Shopify ecommerce page; TLSv1.2, TLSv1.3
2052/tcp	HTTP?	Direct IP blocked (Cloudflare)
2053/tcp	HTTPS?	HTTP request sent to HTTPS port (400 error)
2082/tcp	HTTP	Direct IP blocked (Cloudflare)
2083/tcp	HTTPS	403 Forbidden (Let's Encrypt cert for myshopify.com)
2086/tcp	HTTP	Direct IP blocked (Cloudflare)
2087/tcp	HTTPS	403 Forbidden (Let's Encrypt cert for myshopify.com)
2095/tcp	HTTP	Direct IP blocked (Cloudflare)
2096/tcp	HTTPS	400 error (HTTP sent to HTTPS port)
8080/tcp	HTTP	Direct IP blocked (Cloudflare)
8443/tcp	HTTPS	403 Forbidden (Let's Encrypt cert for myshopify.com)
8880/tcp	Unknown	No service banner or response shown

Scanning and vulnerability identification.

Nikto



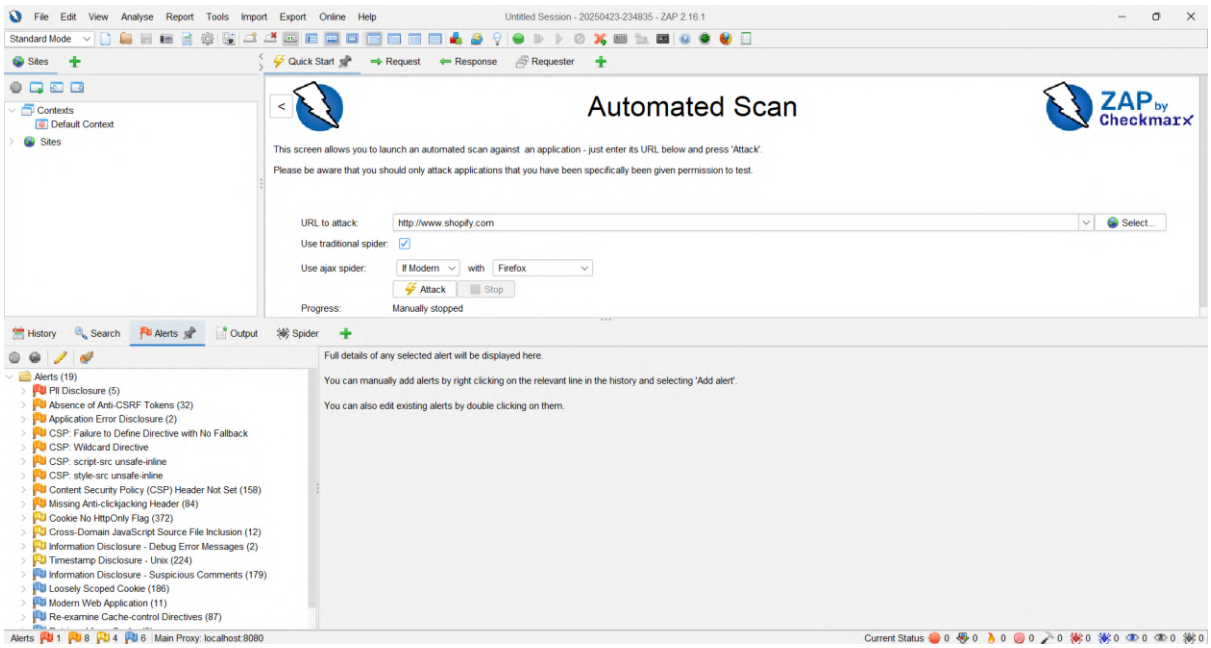


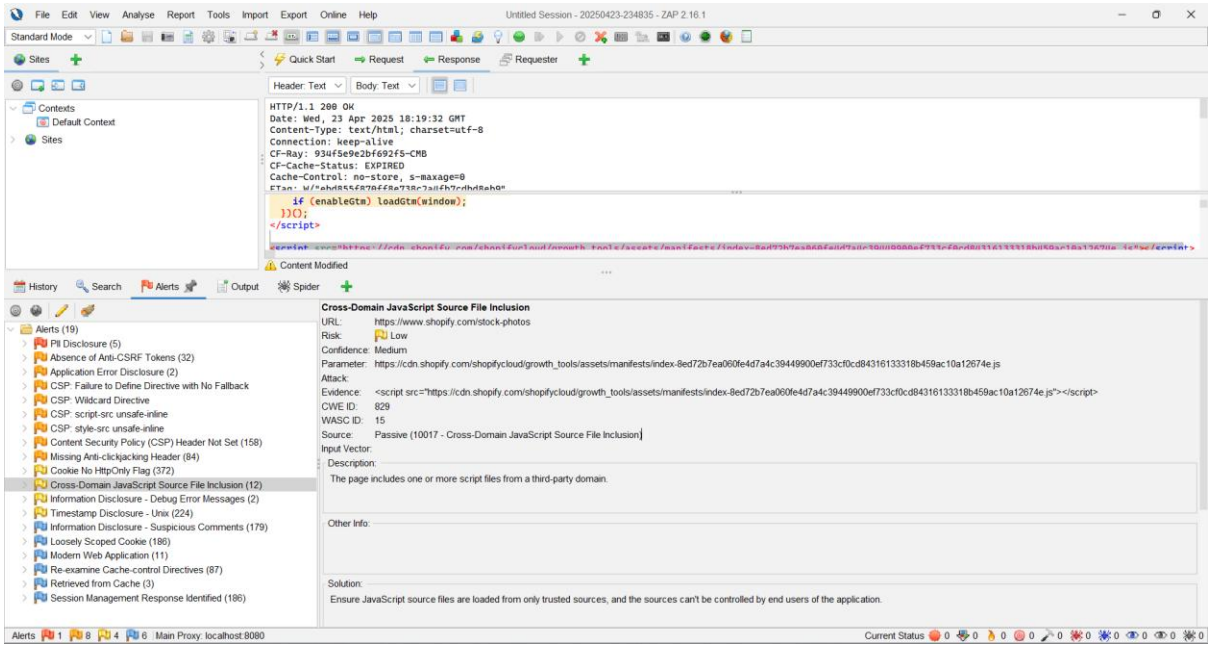
Key findings:

- security headers like X-Frame-Options and X-Content-Type-Options are missing.
- Without the HttpOnly flag, cookies (_shopify_s, _shopify_y) are set.
- Some uncommon headers were found (e.g., server-timing, alt-svc, critical-ch).

- Potential vulnerability to the BREACH attack because of the deflates header in the Content-Encoding.
- Some of the 103 entries in the robots.txt file returned unusual HTTP responses.
- During scanning, 19 mistakes and 23 discoveries were found, reaching an error limit.

OWASP ZAP





Alerts found.

- PII Disclosure**:** 5 instances
- Absence of Anti-CSRF Tokens: 32 instances
- Application Error Disclosure: 2 instances
- CSP: Failure to Define Directive with No Fallback: 8 instances
- CSP: Wildcard Directive: 1 instance
- CSP: script-src unsafe-inline: 1 instance
- CSP: style-src unsafe-inline: 1 instance
- Content Security Policy (CSP) Header Not Set: 158 instances
- Missing Anti-clickjacking Header: 84 instances
- Cookie No HttpOnly Flag: 372 instances
- Cross-Domain JavaScript Source File Inclusion: 12 instances
- Information Disclosure - Debug Error Messages: 2 instances
- Timestamp Disclosure - Unix: 224 instances
- Information Disclosure - Suspicious Comments: 179 instances
- Loosely Scoped Cookie: 186 instances
- Modern Web Application: 11 instances
- Re-examine Cache-control Directives: 87 instances
- Retrieved from Cache: 3 instances
- Session Management Response Identified: 186 instances

Vulnerabilities.

- **Broken Access Control**

Cookies without HTTP Only Flag

Issue Found:

- The HTTP Only flag is absent from cookies like _shopify_s and _shopify_y.

Risk:

- Session hijacking: These cookies are vulnerable to theft via Cross-Site Scripting (XSS) attacks since client-side JavaScript can access them in the absence of the HttpOnly option.

How This Needs to Be Reduced:

- To stop JavaScript access, set the HttpOnly flag on all session cookies.
- To make sure cookies are only sent over HTTPS, think about also putting the Secure flag on them.

- **Sensitive Data Exposure**

Potential Vulnerability to BREACH Attack

Issue Found:

- A possible breach vulnerability because of the Content-Encoding deflate header.

Risk:

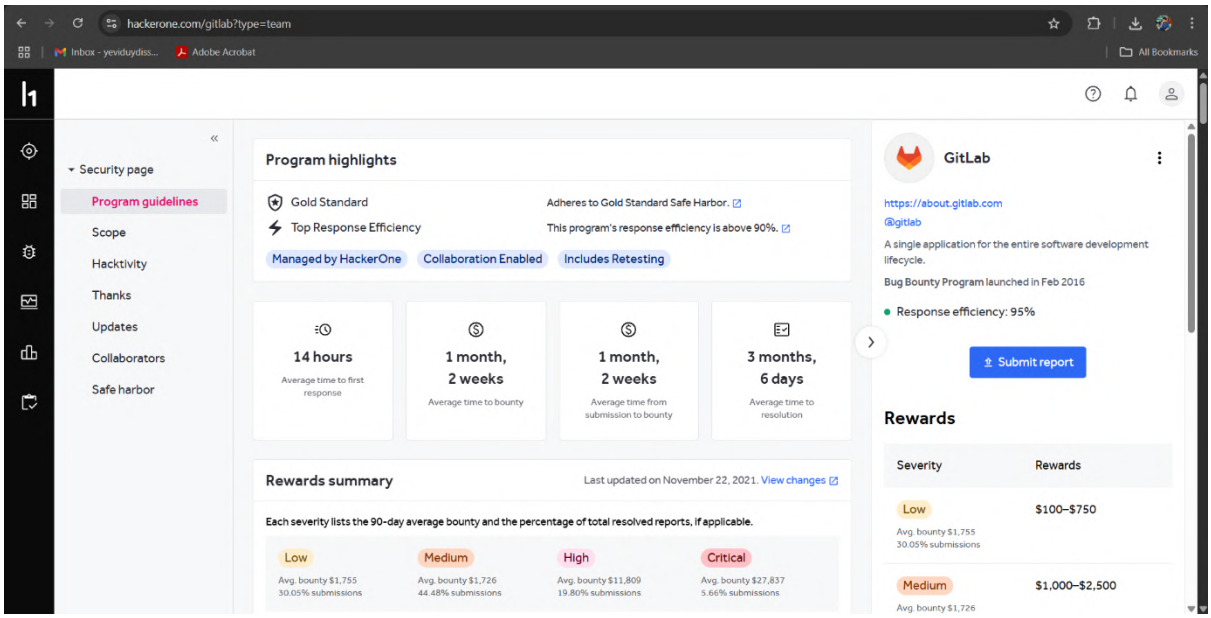
- Data leakage: Attackers may utilize the BREACH attack to obtain secrets by taking advantage of the compression method if the response body contains sensitive data (such as CSRF tokens).

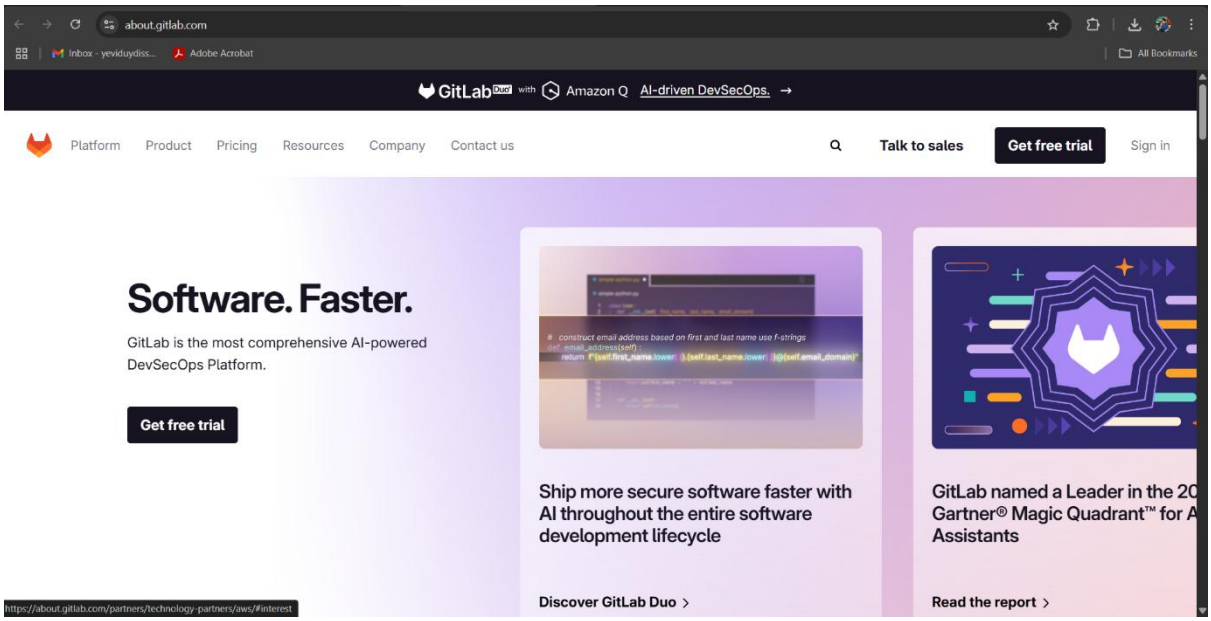
How This Needs to Be Reduced:

- Don't use gzip or deflate on answers that include sensitive information.
- To stop successful compression-based attacks, think about padding sensitive responses with random data.

Report 03.

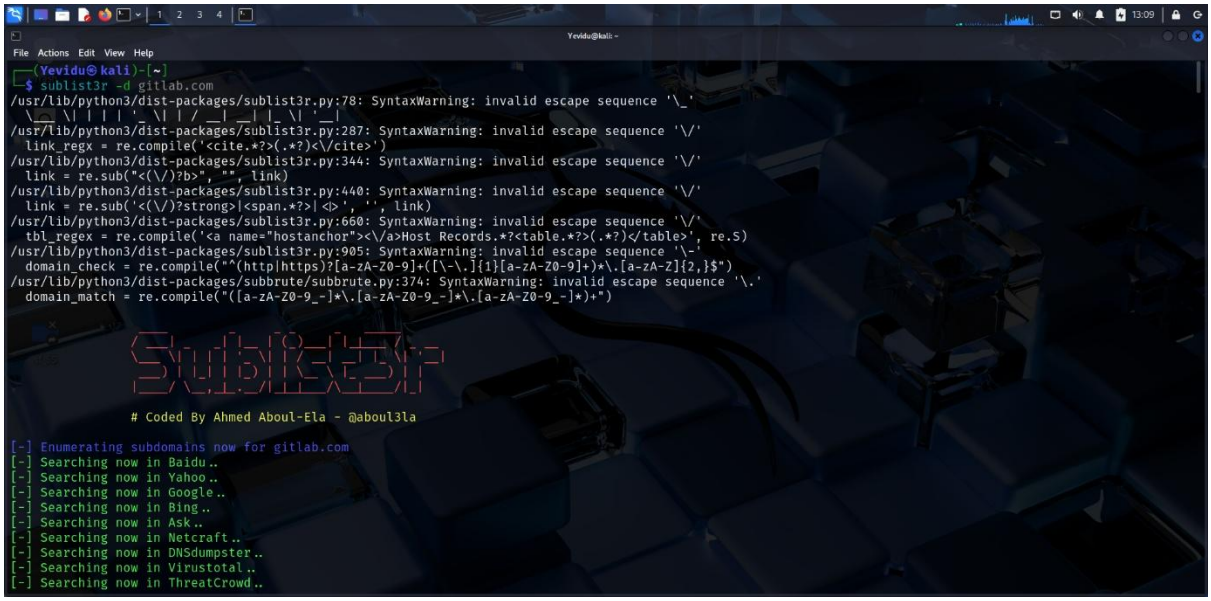
GitLab (https://about.gitlab.com/), a popular DevSecOps platform utilized by millions of developers, teams, and businesses worldwide, is the subject of this Bug Bounty report. By providing a full array of tools for source code management, continuous integration/continuous deployment (CI/CD), bug tracking, and security testing—all in one application—GitLab enables users to design, develop, secure, and deploy software more quickly. Across the whole software development lifecycle, GitLab fosters innovation and collaboration and is trusted by businesses of all sizes, from Fortune 500 firms to startups. Every day, GitLab hosts and processes a huge volume of proprietary code, developer data, and project workflows with a strong focus on open source and remote-first operations.

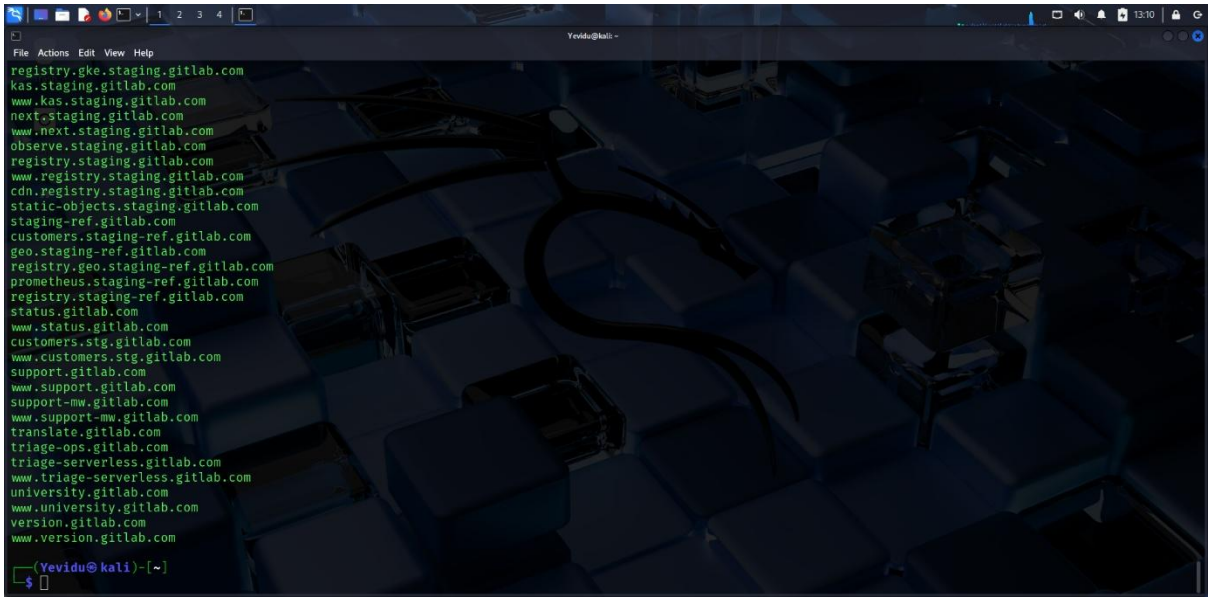




Target Reconnaissance.

Sublist3r





- **Test and Staging Environments**

  Active development/testing environments are indicated by many subdomains under **design-staging, staging**, and **pre**.

  These can reveal private information or credentials and are usually less secure.

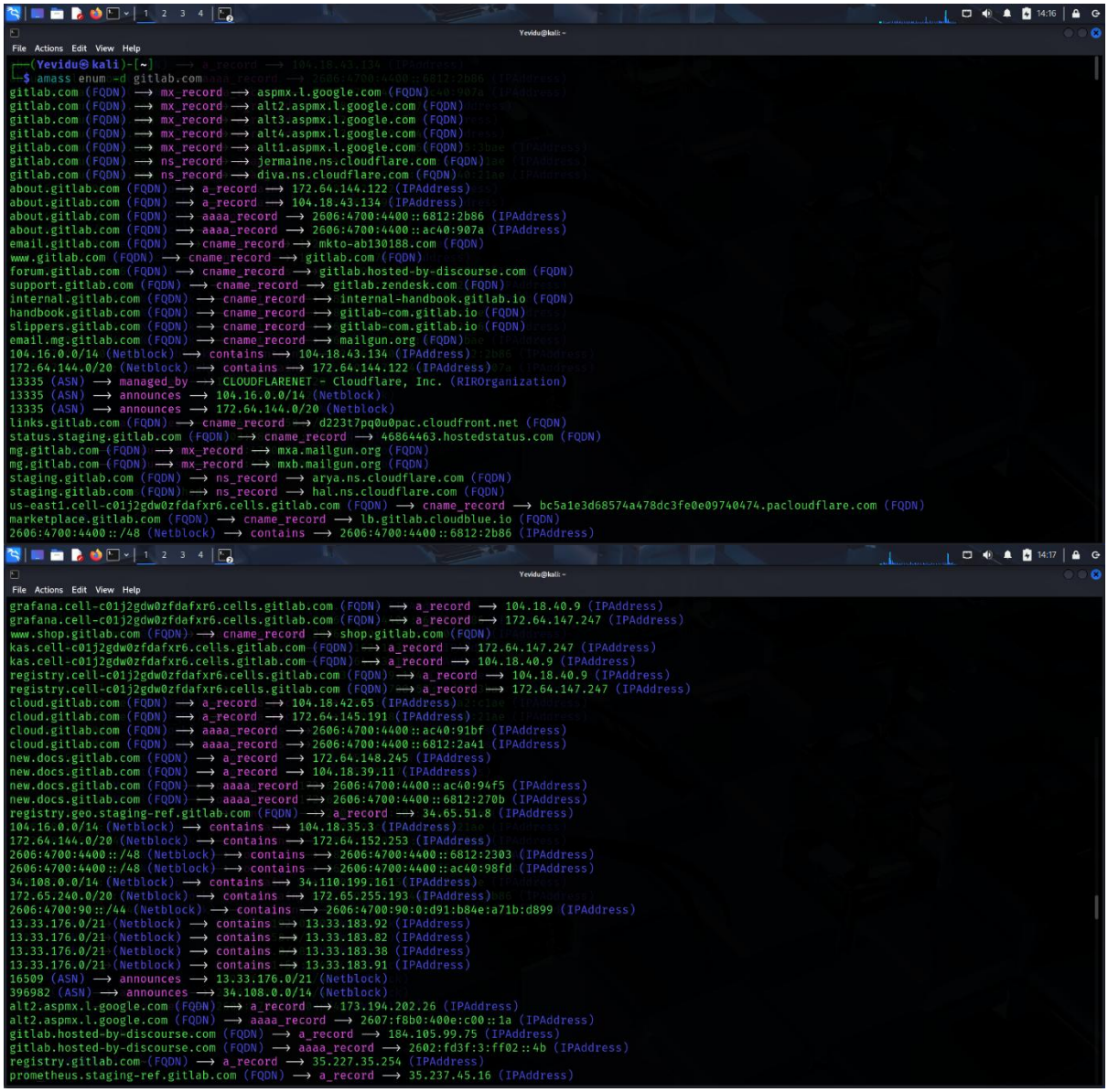
- **The Internal Services and Prototype**

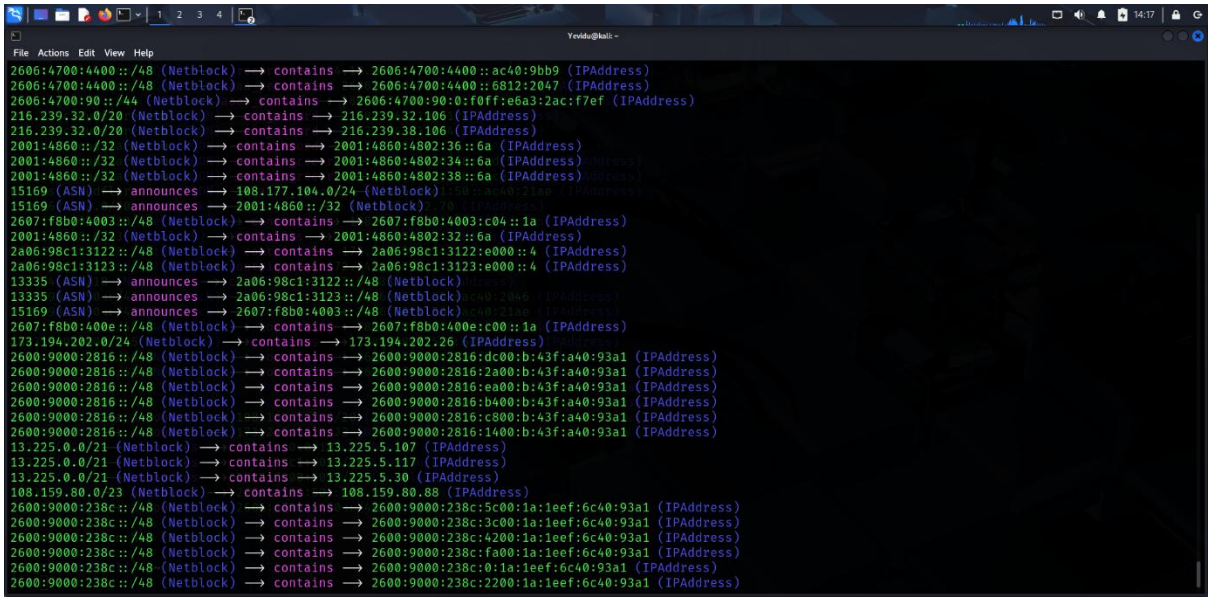
  Subdomains such as **internal.gitlab.com** and **glchat.prototype.gitlab.com** may disclose internal systems or experimental functionality.

- **Monitoring and Analytics**

  Metrics, **Prometheus**, and **Observe** are examples of monitoring tools that could be exposed when improperly setup.

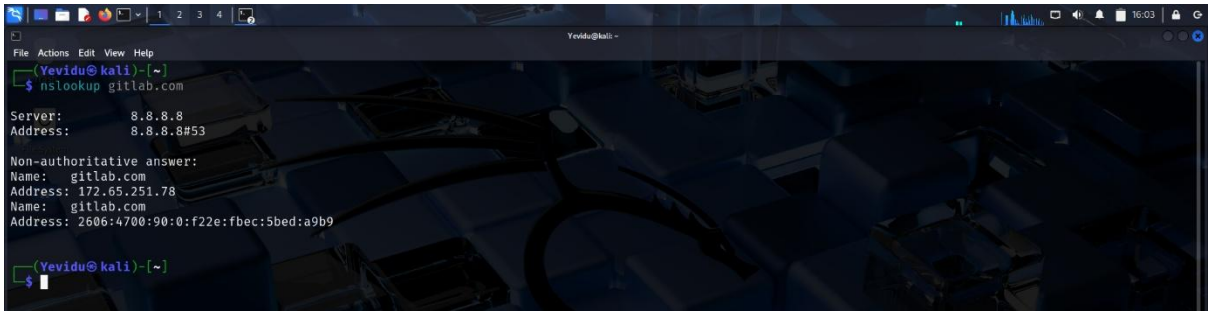
Amass





Subdomains	about.gitlab.com, cloud.gitlab.com, forum.gitlab.com, internal.gitlab.com
DNS Records	A, AAAA, MX, NS, CNAME
Third-Party Services	Google, Cloudflare, Zendesk, Discourse, Cloudfront, Mailgun
Netblocks & ASNs	104.18.43.134, 172.64.144.0/20, Cloudflare, Google
Staging/Internal Sites	status.staging.gitlab.com, prometheus.staging-ref.gitlab.com
IPv6 Usage	Multiple IPv6 addresses and netblocks

Nslookup



Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

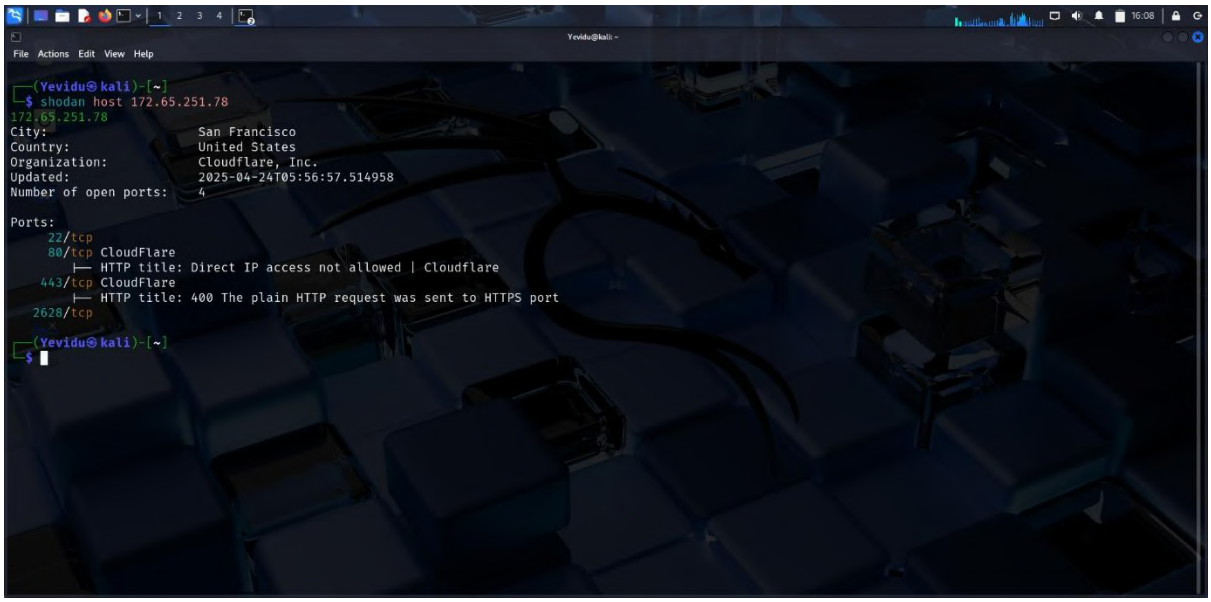
Name: gitlab.com

Address: 172.65.251.78

Name: gitlab.com

Address: 2606:4700:90:0:f22e:fbec:5bed:a9b9

Shodan



172.65.251.78

City: San Francisco

Country: United States

Organization: Cloudflare, Inc.

Updated: 2025-04-24T05:56:57.514958

Number of open ports: 4

Ports:

22/tcp

80/tcp Cloudflare

└─ HTTP title: Direct IP access not allowed | Cloudflare

443/tcp Cloudflare

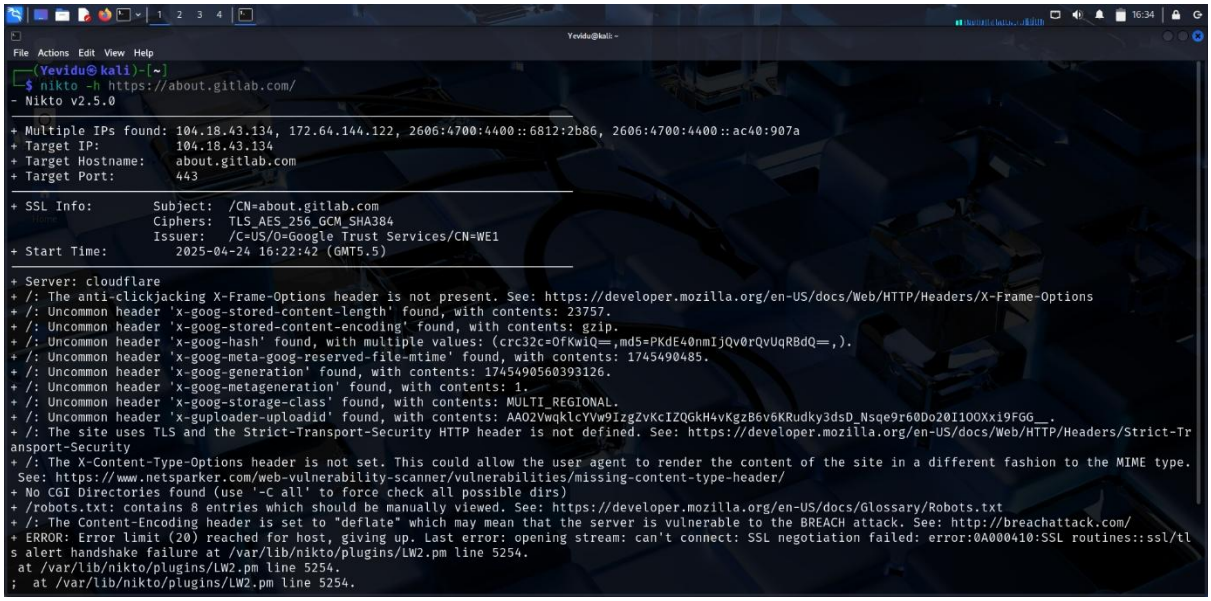
└─ HTTP title: 400 The plain HTTP request was sent to HTTPS port

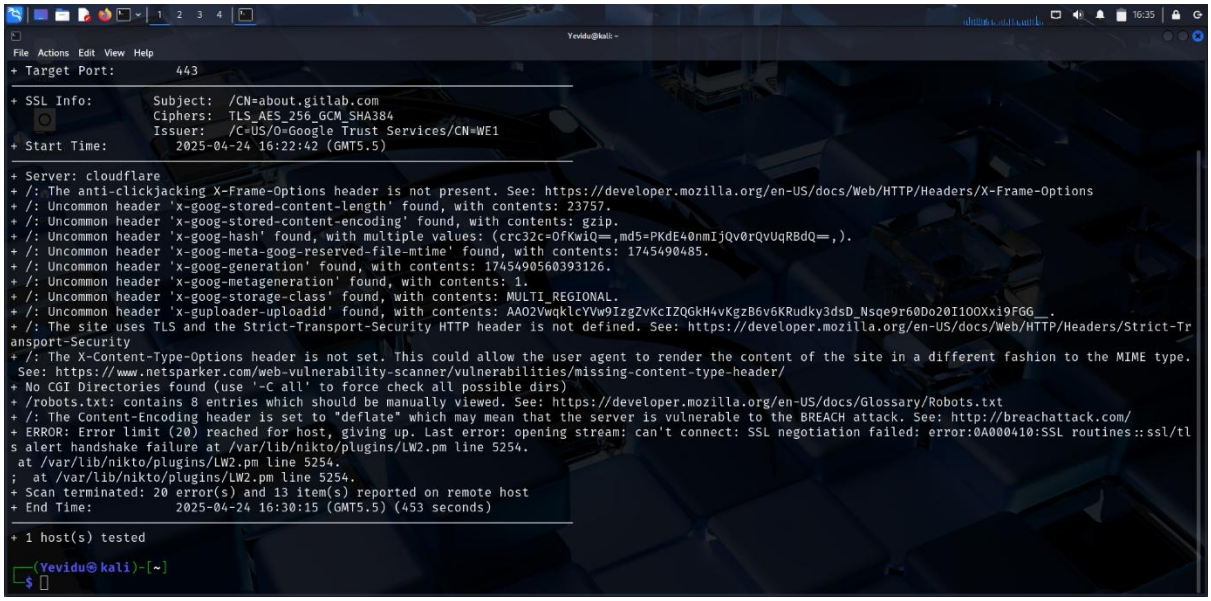
2628/tcp

- Ports 80/443: Typical for web traffic; Cloudflare is acting as a reverse proxy.
- Port 22: Might be for SSH (likely blocked/hidden behind firewall).
- Port 2628: Often used by DICT protocol (dictionary service)—unusual but might be a decoy or unrelated.

Scanning and vulnerability identification.

Nikto





Security Headers Missing

- Missing X-Frame-Options Header

  Risk: clickjacking attacks.

- Missing Strict-Transport-Security (HSTS) Header

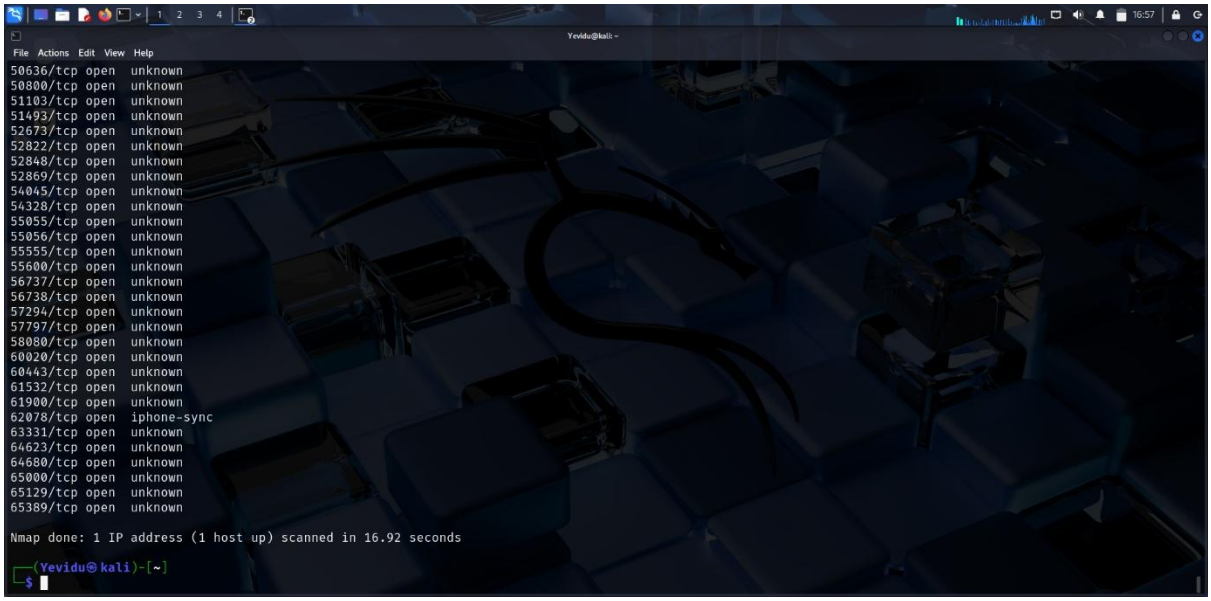
  Risk: May allow SSL stripping attacks, reducing HTTPS effectiveness.

Miscellaneous Findings

- Found: Robots.txt

  includes eight entries that could indicate sensitive directories or forbidden paths that require manual examination.

Nmap



Numerous Open Ports

There are more than 60 open TCP ports, several of which are high-numbered or rare.

Unusual for a system that faces production, this could:

Point out any misconfiguration or the existence of numerous services.

give attackers a greater surface area to attack.

Typical and Dangerous Services

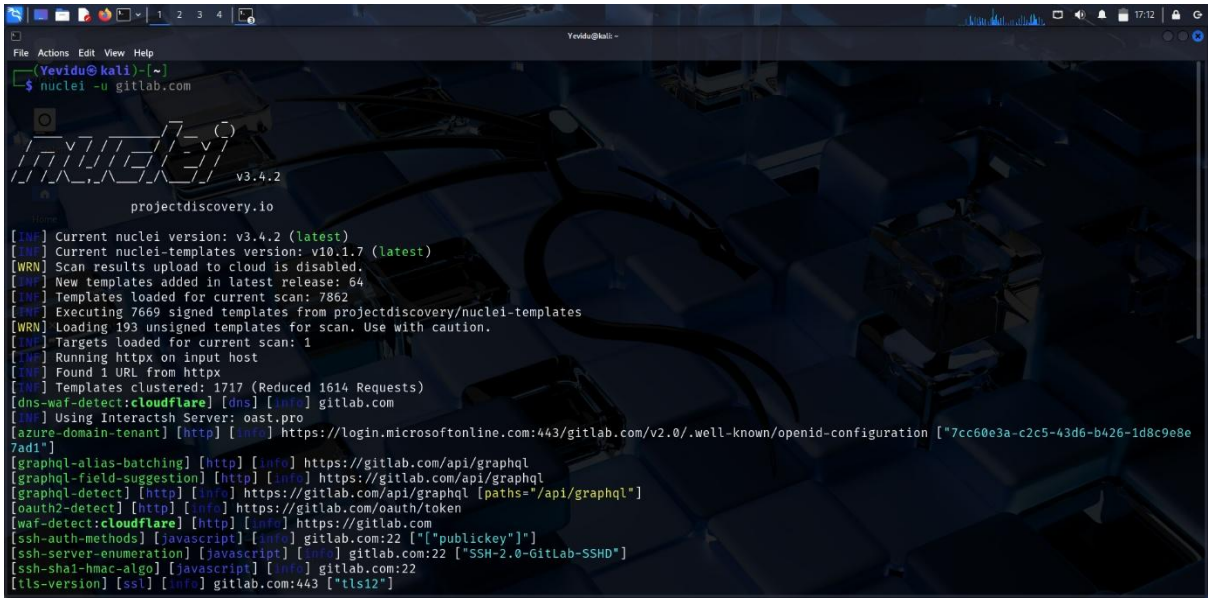
SSH (22), FTP (21/20), and Telnet (23) were found; if not in use, these should be disabled or closed down.

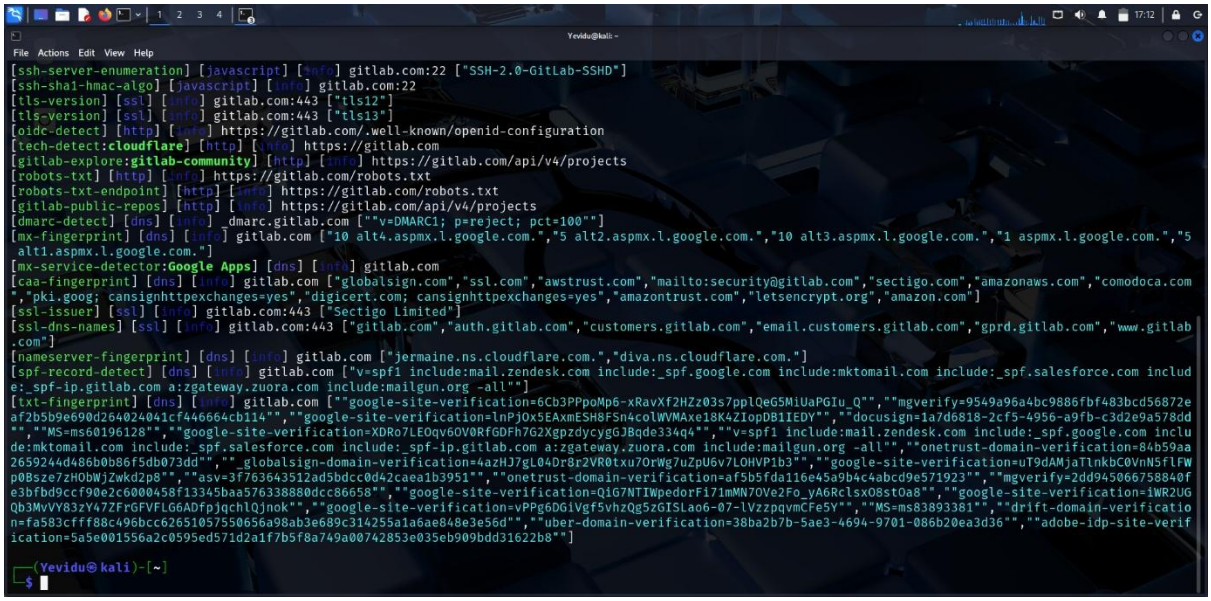
Since FTP and Telnet send data in plaintext, including credentials, they are by default insecure.

RSFTP (26) and SMTP (25) have the potential to be misused for attacks based on misconfiguration or spam.

Unencrypted online access via HTTP (80) (although GitLab typically reroutes to HTTPS).

Nuclei





Web Application & Service Discovery

Detected GraphQL Endpoint:

URL: https://gitlab.com/api/graphql

Graphql-detect, graphql-alias-batching, and graphql-field-suggestion were the templates that matched.

Why it matters: If not adequately secured, GraphQL APIs may reveal private information, internal schema, or errors in business logic.

OAuth2 Endpoint Found:

URL: https://gitlab.com/oauth/token

Shows GitLab issues access tokens using OAuth. Excellent for verifying token leaks or OAuth configuration errors.

OpenID Connect Configuration Detected:

URLs:
https://gitlab.com/.well-known/openid-configuration
https://login.microsoftonline.com/gitlab.com/v2.0/.well-known/openid-configuration

Useful for testing SSO abuse and authentication flow modification.

Security Headers & WAF

WAF Detected: Cloudflare

Templates: dns-waf-detect, waf-detect: cloudflare

Missing Security Headers

No Strict-Transport-Security (HSTS)

No X-Content-Type-Options

No X-Frame-Options

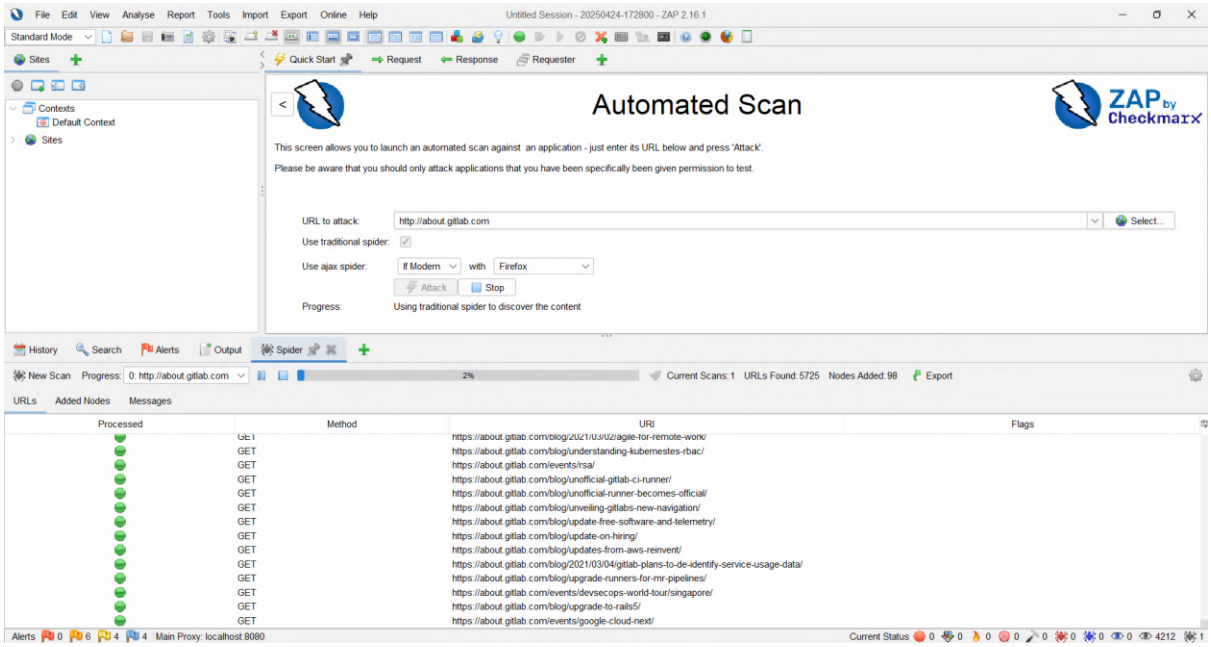
SSH Results

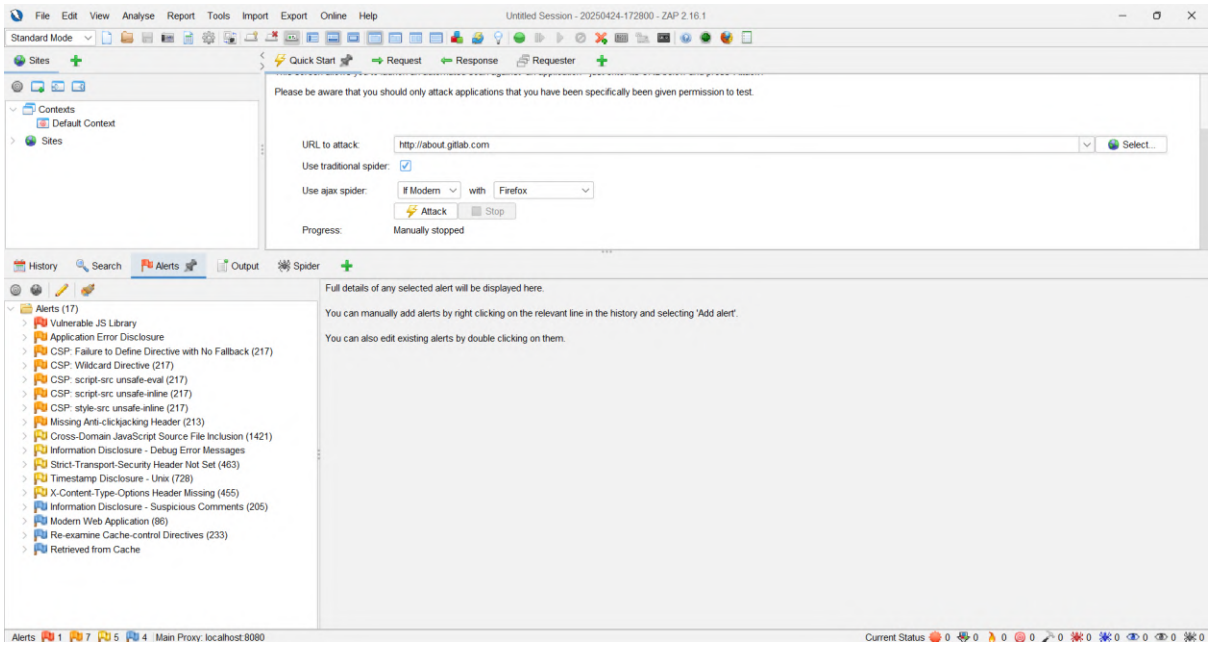
Method of SSH Authentication: Public Key only

SSH Banner: GitLab-SSHD-SSH-2.0

HMAC Algorithm Weakness Found: SHA1

OWASP ZAP


File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - 20250424-172800 - ZAP 2.16.1
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://about.gitlab.com
Select...
Use traditional spider:
Use ajax spider:
If Modern
with
Firefox
Attack
Stop
Progress:
Using traditional spider to discover the content
History
Search
Alerts
Output
Spider
New Scan
Progress:
0: http://about.gitlab.com
2%
Current Scans: 1
URLs Found: 5725
Nodes Added: 98
Export
URLs
Added Nodes
Messages
Processed
Method
URI
Flags
GET https://about.gitlab.com/blog/understanding-kubernestes-rbac/
GET https://about.gitlab.com/events/rsa/
GET https://about.gitlab.com/blog/unofficial-gitlab-ci-runner/
GET https://about.gitlab.com/blog/unofficial-runner-becomes-official/
GET https://about.gitlab.com/blog/unveiling-gitlabs-new-navigation/
GET https://about.gitlab.com/blog/update-free-software-and-telemetry/
GET https://about.gitlab.com/blog/update-on-hiring/
GET https://about.gitlab.com/blog/updates-from-aws-reinvent/
GET https://about.gitlab.com/blog/2021/03/04/gitlab-plans-to-de-identify-service-usage-data/
GET https://about.gitlab.com/blog/upgrade-runners-for-mr-pipelines/
GET https://about.gitlab.com/events/devsecops-world-tour/singapore/
GET https://about.gitlab.com/blog/upgrade-to-rails5/
GET https://about.gitlab.com/events/google-cloud-next/
Alerts
Main Proxy: localhost:8080
Current Status


File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - 20250424-172800 - ZAP 2.16.1
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://about.gitlab.com
Select...
Use traditional spider:
Use ajax spider:
If Modern
with
Firefox
Attack
Stop
Progress:
Manually stopped
History
Search
Alerts
Output
Spider
Alerts (17)
Vulnerable JS Library
Application Error Disclosure
CSP: Failure to Define Directive with No Fallback (217)
CSP: Wildcard Directive (217)
CSP: script-src unsafe-eval (217)
CSP: script-src unsafe-inline (217)
CSP: style-src unsafe-inline (217)
Missing Anti-clickjacking Header (213)
Cross-Domain JavaScript Source File Inclusion (1421)
Information Disclosure - Debug Error Messages
Strict-Transport-Security Header Not Set (463)
Timestamp Disclosure - Unix (728)
X-Content-Type-Options Header Missing (455)
Information Disclosure - Suspicious Comments (205)
Modern Web Application (86)
Re-examine Cache-control Directives (233)
Retrieved from Cache
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
Alerts
Main Proxy: localhost:8080
Current Status

Alert.

- Vulnerable JS Library
- Application Error Disclosure
- CSP: Failure to Define Directive with No Fallback (217)
- CSP: Wildcard Directive (217)
- CSP: script-src unsafe-eval (217)
- CSP: script-src unsafe-inline (217)
- CSP: style-src unsafe-inline (217)
- Missing Anti-clickjacking Header (213)
- Cross-Domain JavaScript Source File Inclusion (141)
- Information Disclosure - Debug Error Messages
- Strict-Transport-Security Header Not Set (463)
- Timestamp Disclosure - Unix (728)
- X-Content-Type-Options Header Missing
- Information Disclosure - Suspicious Comments (205)
- Modern Web Application (88)
- Re-examine Cache-control Directives (233)
- Retrieved from Cache

Vulnerabilities.

➢ XML External Entities

Issues Found:

- Although XML usage isn't mentioned specifically, API endpoints (OAuth2, GraphQL) may eventually interact with XML.

Risk:

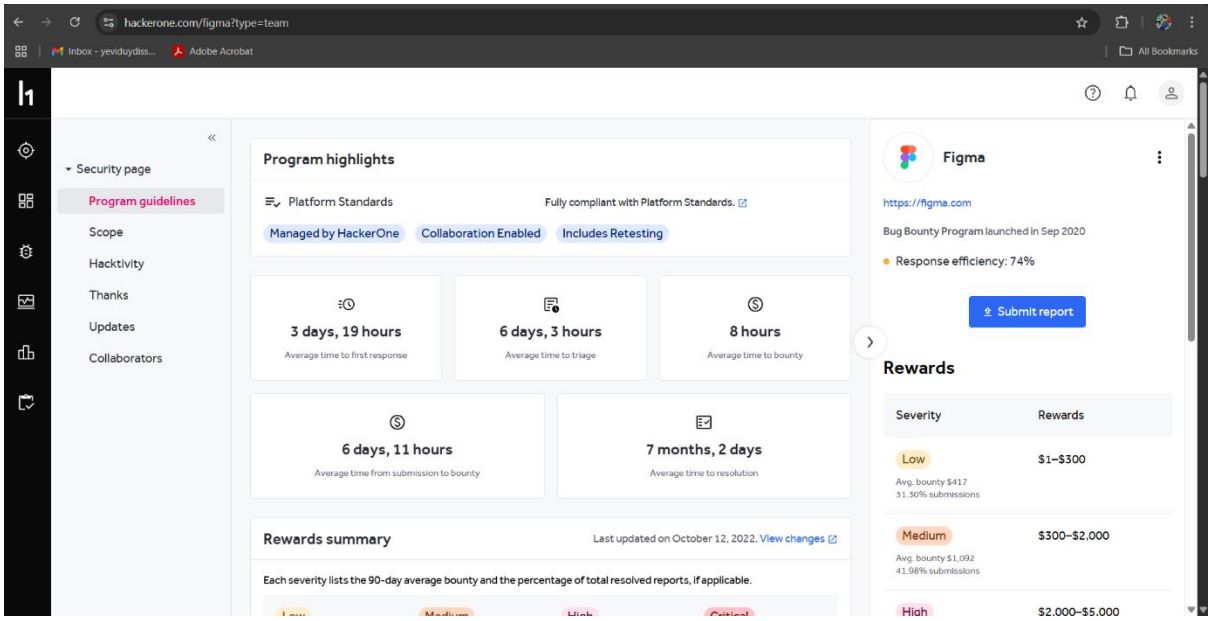
- XXE flaws could provide an attacker access to internal files, trigger a denial-of-service attack, or start server-side request forgery (SSRF) if XML is used anywhere in the backend (for example, while processing user-supplied data).

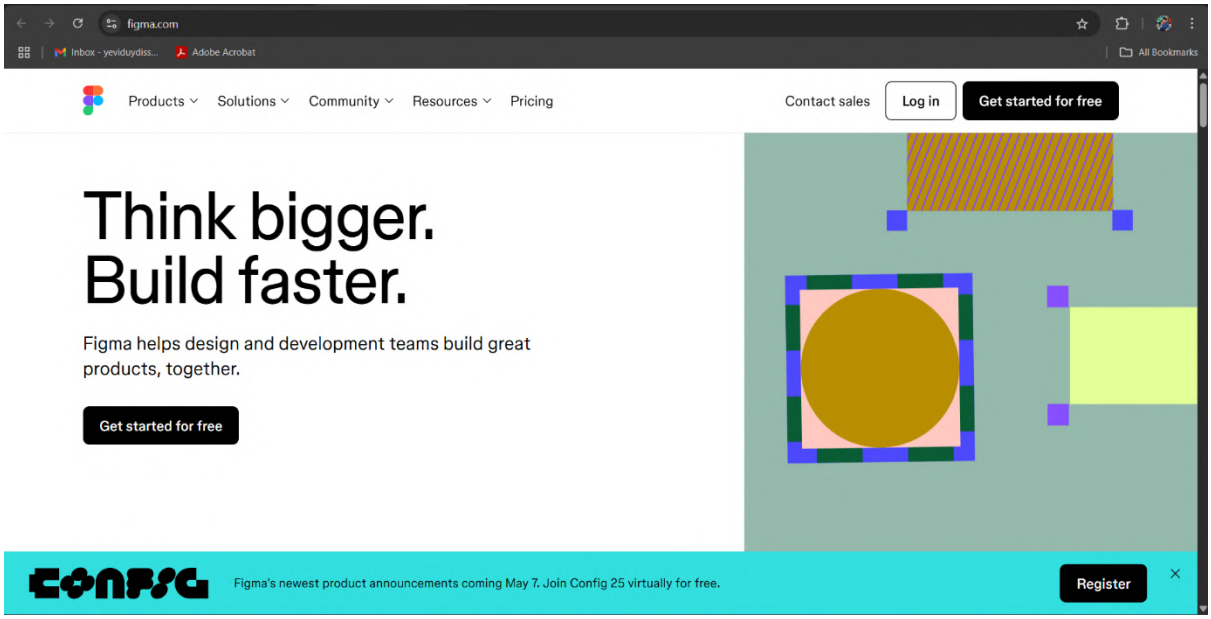
How This Needs to Be Reduced:

- Turn off XML parsers' ability to process external entities.
- Make use of safe libraries that by default forbid processing XML foreign entities.
- Verify and clean up all incoming data, including requests that use XML.

Report 04.

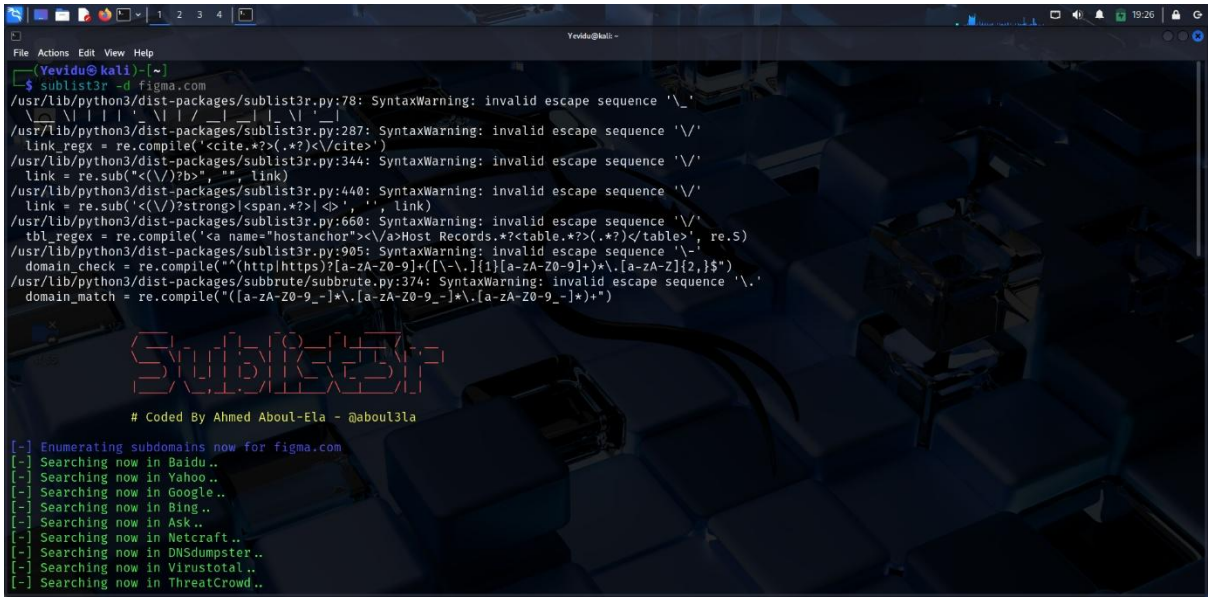
Figma (https://www.figma.com/), a popular web-based design and prototyping tool that has transformed team collaboration on digital product design, is the subject of this Bug Bounty report. Designers, developers, and stakeholders can collaborate in real time on the same project using Figma, no matter where they are in the world. Everything from interactive prototyping and design systems administration to wireframing and UI/UX design is supported by the platform. Figma is trusted by businesses of all kinds, including startups, large tech corporations, and academic institutions. Every day, it manages a substantial volume of confidential and creative data. Figma is essential to contemporary product development processes worldwide because of its cloud architecture, browser-based interface, and extensive integrations.

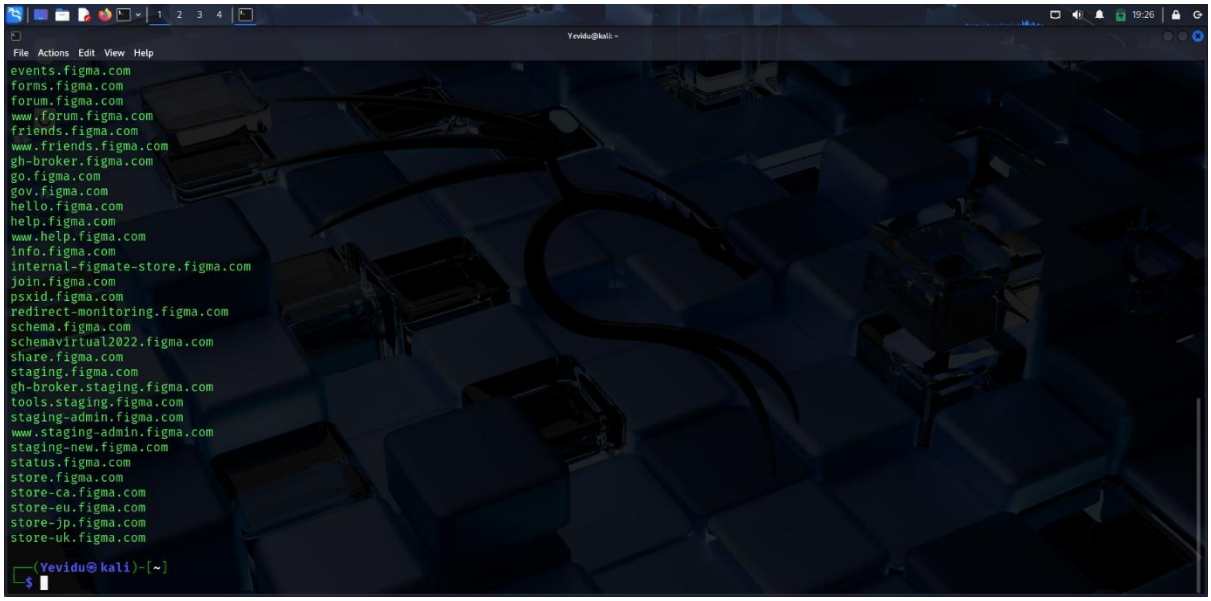




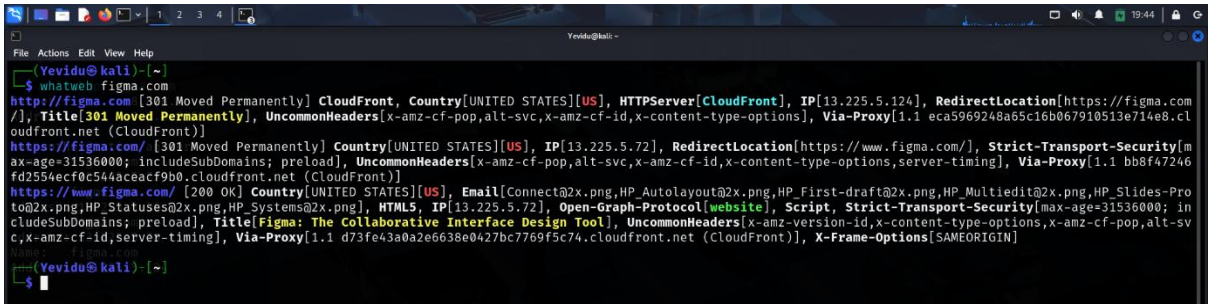
Target Reconnaissance.

Sublist3r



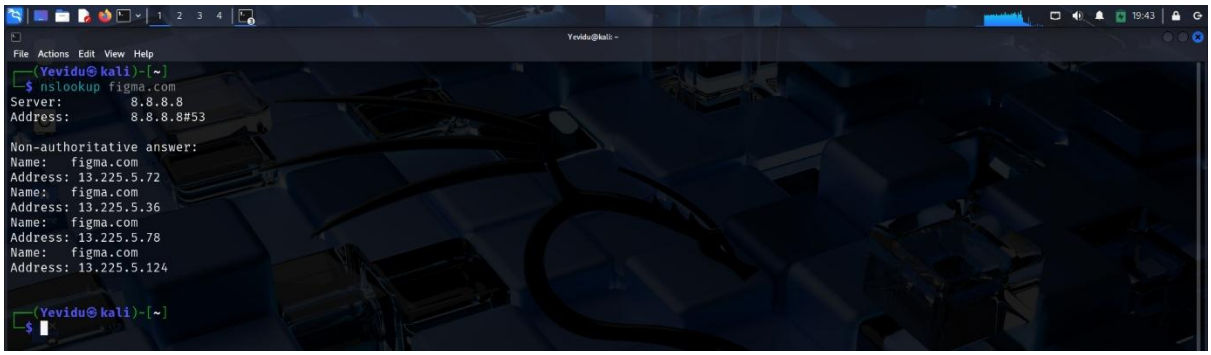


Whatweb



URL	Status	Server Info	Notes
http://figma.com	301	CloudFront (Amazon CDN)	Redirects to https://figma.com/
https://figma.com/	301	CloudFront	Redirects to https://www.figma.com/
https://www.figma.com/	200	CloudFront	Destination (main site), HTML5 site with active security headers

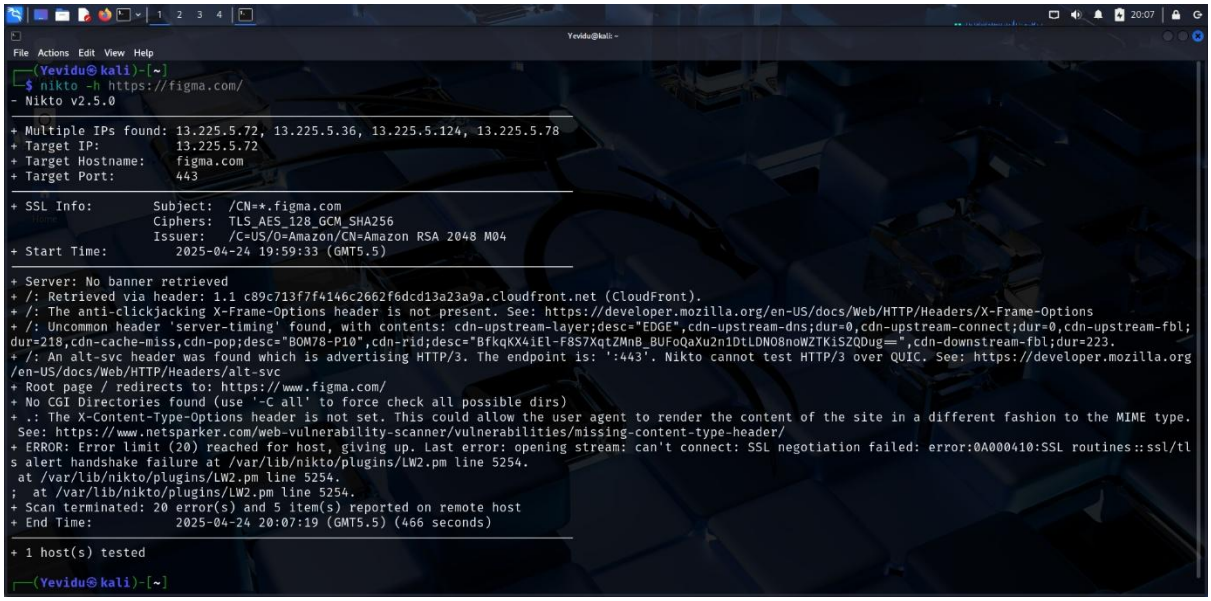
Nslookup



Query	Result
Domain	figma.com
DNS Server	8.8.8.8 (Google Public DNS)
IP Addresses	13.225.5.72, 13.225.5.36, 13.225.5.78, 13.225.5.124

Scanning and vulnerability identification.

Nikto



Target Hostname: figma.com

IP Addresses: 13.225.5.72, 13.225.5.36, 13.225.5.124, 13.225.5.78

Port: 443 (HTTPS)

SSL Info:

- Subject: CN=*.figma.com
- Issuer: Amazon RSA 2048 M04
- Cipher Suite: TLS_AES_128_GCM_SHA256

- **Security Headers Missing:**

  - There is no X-Frame-Options header.

    Risk: clickjacking attempts

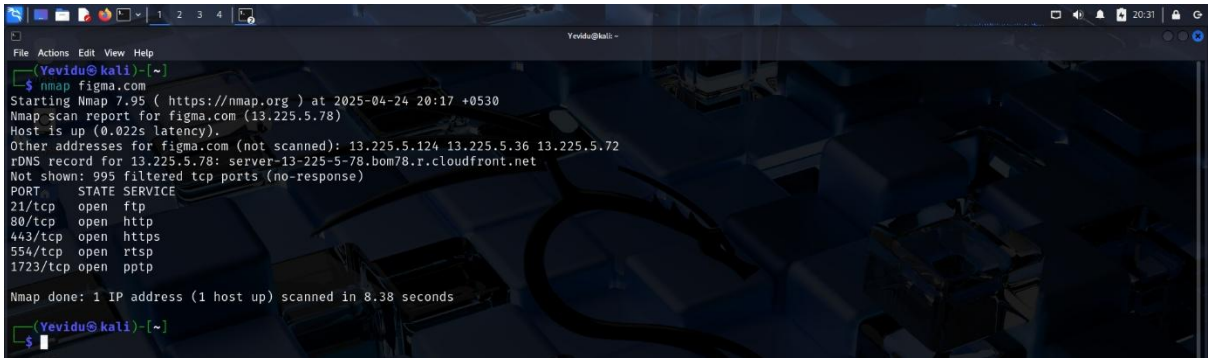
- The header X-Content-Type-Options is not set.

  Risk: Files could be interpreted by the browser as a different MIME type (content sniffing).

- **Errors**

  - Zero SSL problems were found, most likely because of stringent security settings like HTTP/3/QUIC.
  - When the error limit was reached, the scan was stopped early.

Nmap



Target Domain: figma.com

Scanned IP: 13.225.5.78

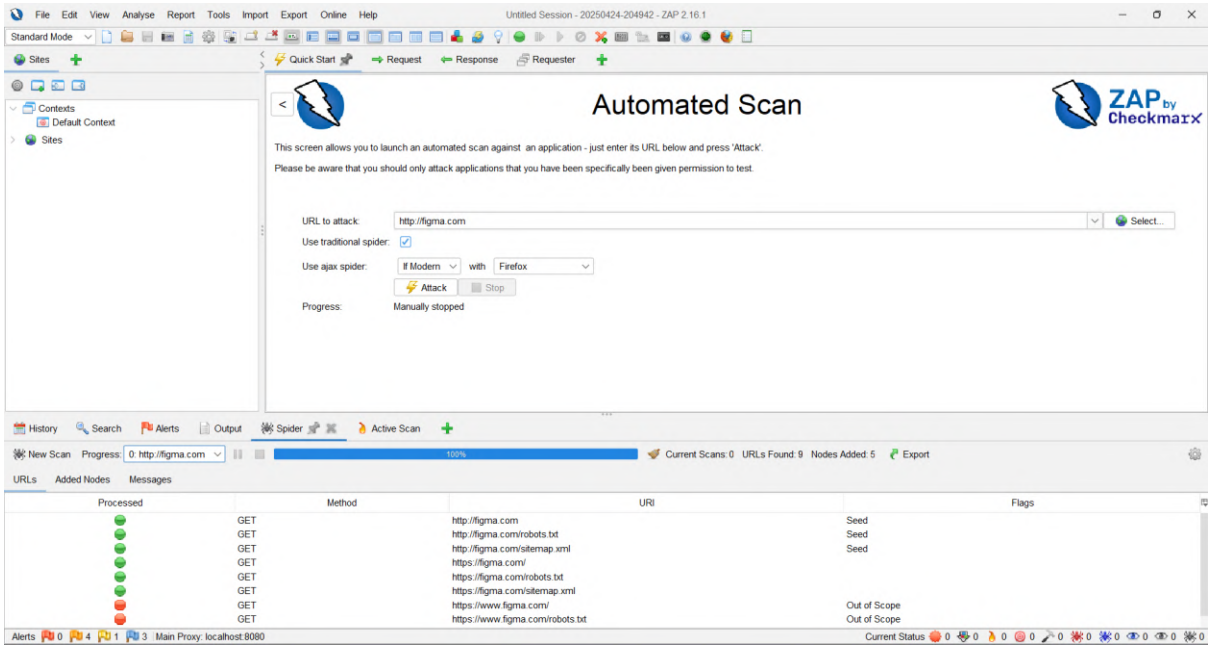
Reverse DNS: server-13-225-5-78.bom78.r.cloudfront.net

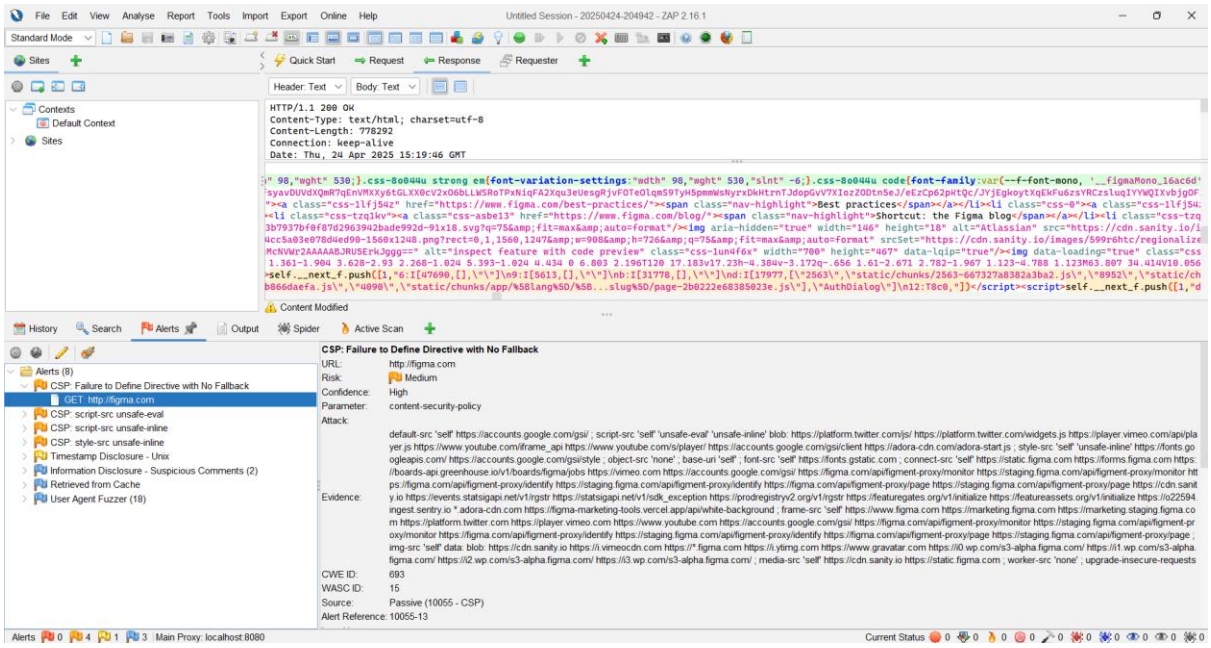
Host Status: Host is up (latency: 0.022s)

Other Ips: 13.225.5.124, 13.225.5.36, 13.225.5.72

Port	State	Service
21/tcp	open	**FTP** – Unencrypted file transfer protocol (can be risky if misconfigured)
80/tcp	open	**HTTP** – Web traffic over unsecured HTTP
443/tcp	open	**HTTPS** – Secure web traffic (expected)
554/tcp	open	**RTSP** – Real-Time Streaming Protocol (used for media streaming)
1723/tcp	open	**PPTP** – Point-to-Point Tunnelling Protocol (legacy VPN; known to have vulnerabilities)

OWASP ZAP





Alerts.

- CIP Failure to Define Directive with No Fallback
- CSP: script-src unsafe-inline
- CSP: script-src unsafe-eval
- CSP: frame-ancestors none
- Information Disclosure - Suspicious Comments (2)
- Information Disclosure
- User Agent Fuzzer (1)

Vulnerabilities.

➢ Injection

Issues Found:

- SQL Injection
- Command Injection
- LDAP Injection

Risk:

- Attackers can run arbitrary commands or queries, which could result in system compromise, data breaches, and illegal access.

How This Needs to Be Reduced:

- For every database interaction, use prepared statements, or parameterized queries.
- Verify and clean user inputs to stop harmful code from running.
- To reduce the danger of injection, use ORM (Object-Relational Mapping) frameworks.

➢ Sensitive Data Exposure

Issues Found:

- Inadequate encryption (using old SSL/TLS versions, for example)
- Keeping private data in plain text, such as credit card numbers or passwords

Risk:

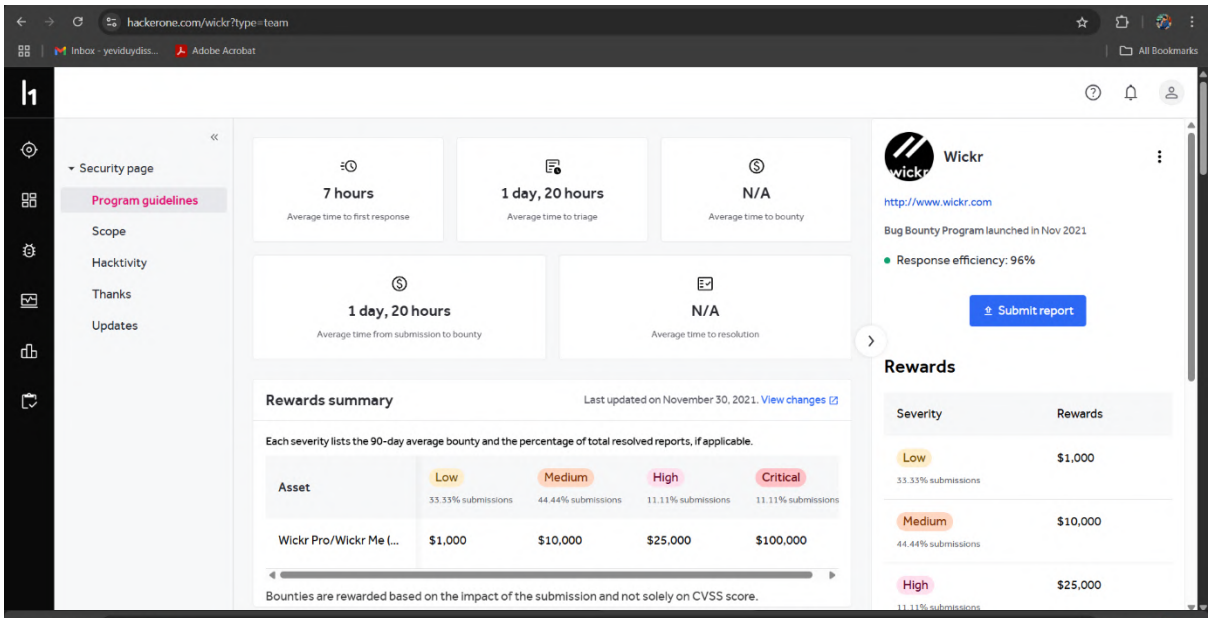
- Attackers can intercept or steal private information, which can result in financial fraud, identity theft, and other nefarious actions.

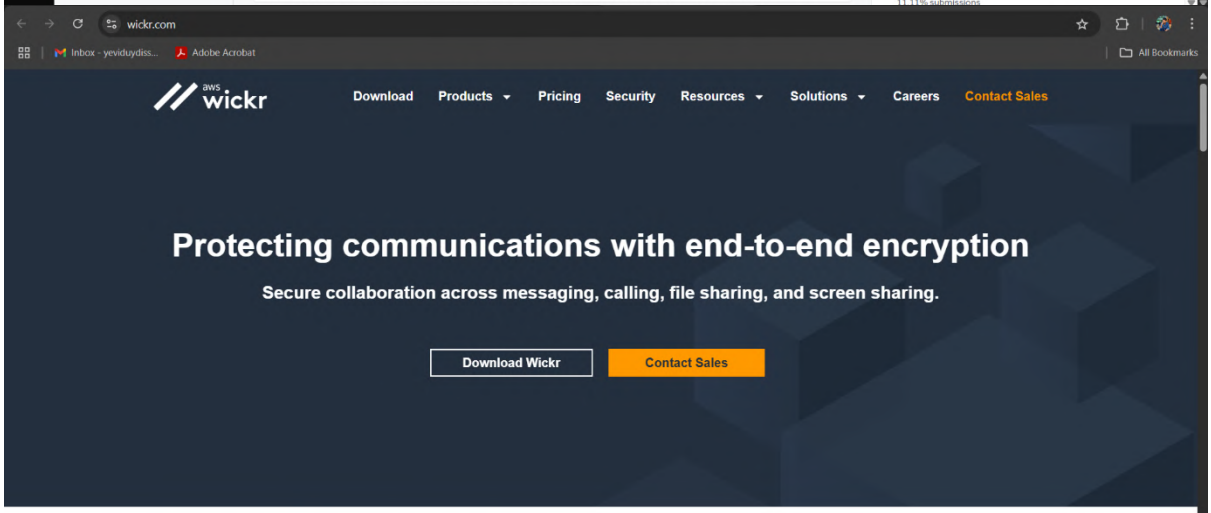
How This Needs to Be Reduced:

- For sensitive data in transit and at rest, use robust encryption techniques (such as AES-256).
- Always use safe hashing techniques (like bcrypt or PBKDF2) when storing passwords.
- To protect data while it's in transit, use TLS/SSL for all data transmissions.

Report 05.

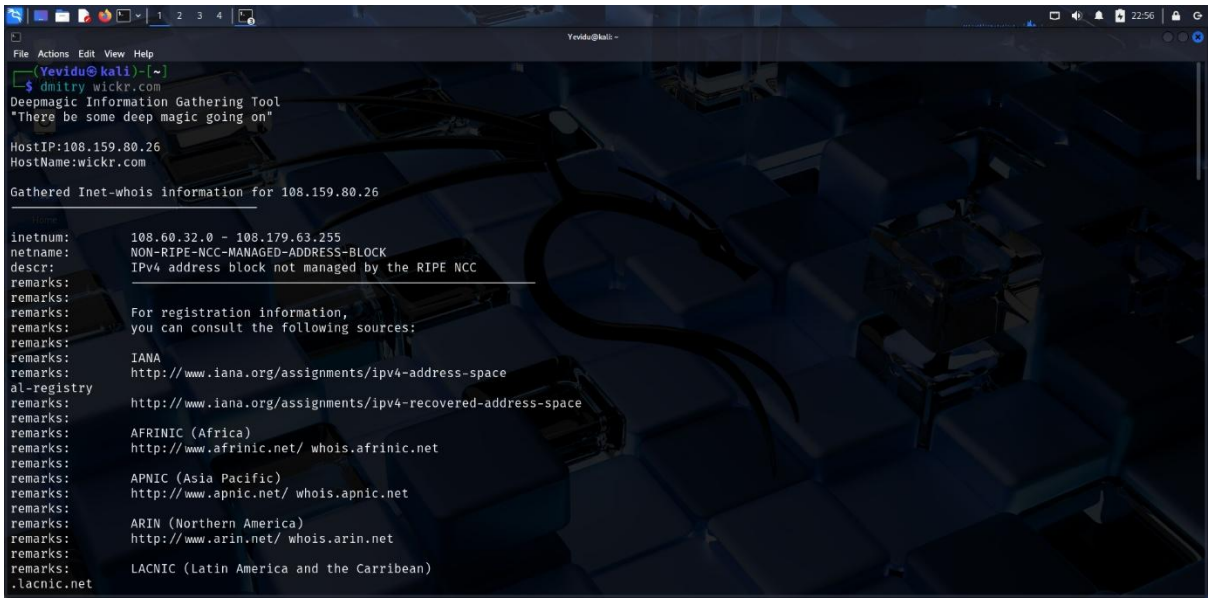
Wickr (https://www.wickr.com/), a secure communications platform that offers phone and video conversations, file sharing, end-to-end encrypted messaging, and collaboration capabilities, is the subject of this Bug Bounty report. Businesses, military groups, and privacy-conscious people worldwide who need secure and reliable communication channels rely on Wickr. To guarantee the privacy of sensitive data, the platform provides strong security features like forward secrecy, metadata protection, and zero-trust architecture. Wickr is extensively used in industries where scalable, secure, and compliant communication is essential, offering both individual and enterprise-level solutions.

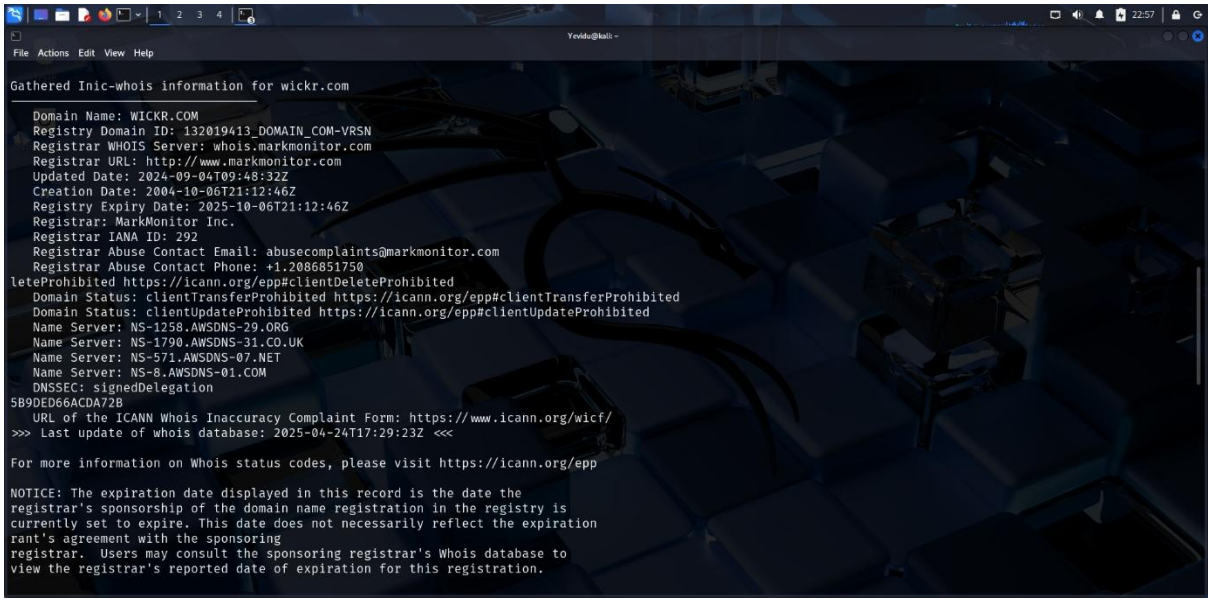


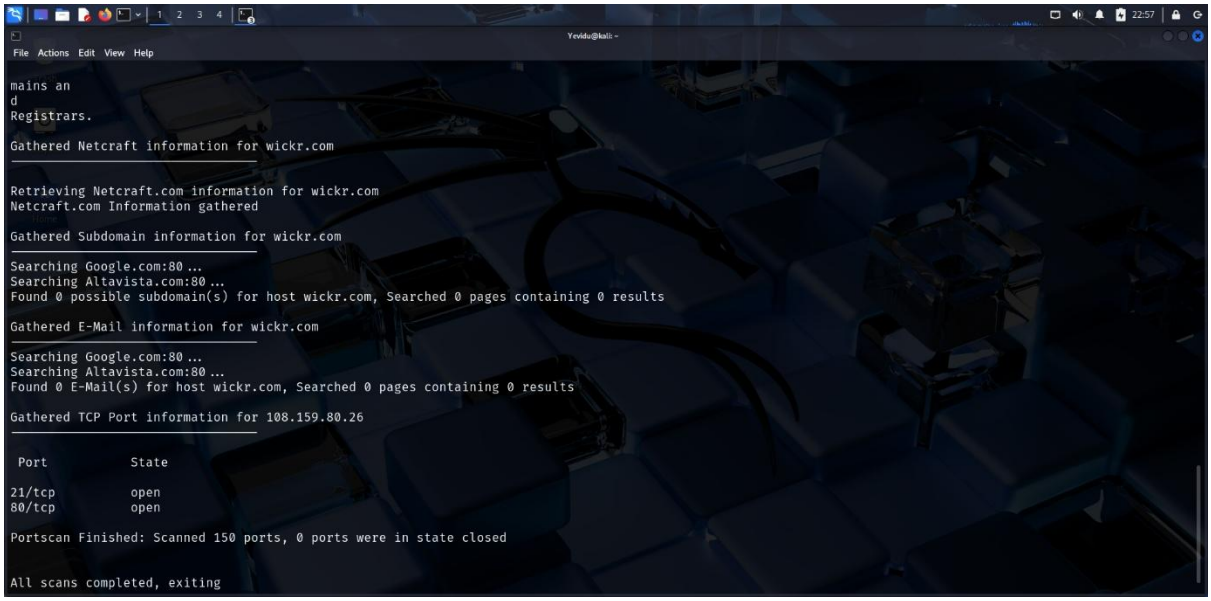


Target Reconnaissance.

Dmitry Scan







Name of IP: 108.159.80.26

WHOIS Information: This IP address is part of a large, probably ARIN-managed (North America) allocation that is not RIPE-managed.

Admin Organization: IANA (placeholder information; ARIN is required to query for specific details).

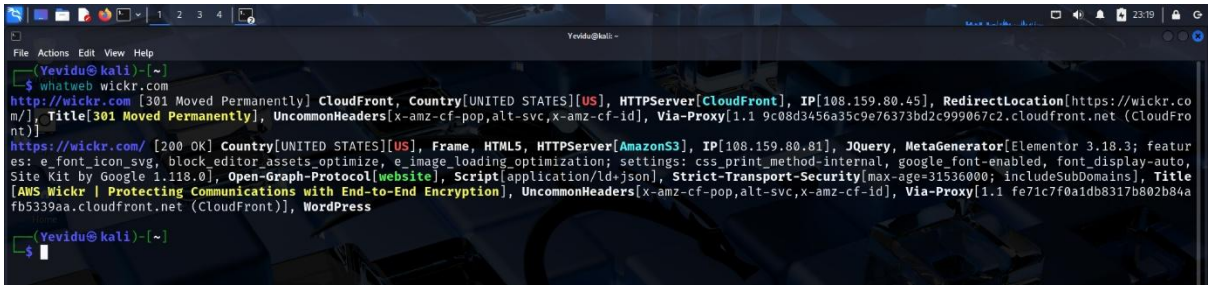
Domain WHOIS

- **Registrar**: Mark Monitor (common with large corporations).
- **Created**: 2004
- **Expires**: 2025-10-06
- **DNSSEC**: Enabled
- **Name Servers**: Hosted on AWS

Open Ports

- 21/tcp → **FTP** is open
- 80/tcp → **HTTP** is open

Whatweb



Total Subdomains Found: 38

Includes:

- admin.wickr.com, api.prod.calling.wickr.com, enterprise.wickr.com, fed.wickr.com, support.wickr.com, etc.

Mark Monitor is a domain registrar that big businesses use.

Creation of the Domain: October 6, 2004

End date: 10/06/2025

AWS Route 53 for DNS hosting

IP address 108.159.80.26 (associated with Amazon and CloudFront infrastructure)

Ports Open:

Port 21 (FTP): may be sensitive; more investigation is necessary.

HTTP port 80: open and reroutes to HTTPS.

First Request:

Wickr.com → HTTPS Redirect (301 Redirect)

CloudFront is used as the CDN.

The last landing page is located at https://wickr.com

Amazon S3 is the server.

CMS: Elementor 3.18.3 with WordPress

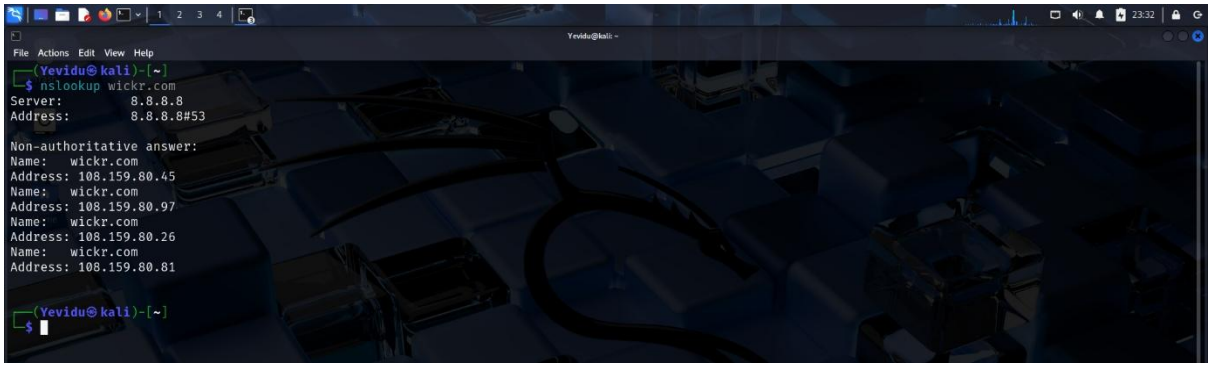
Scripts: Make use of structured data (ld+json) and jQuery

Security: Strict Transport Security is used.

Google Site Kit plugin is active for SEO and tracking.

Title: "AWS Wickr | Using End-to-End Encryption to Secure Communications"

Nslookup



- Domain: wickr.com
- IP Addresses:

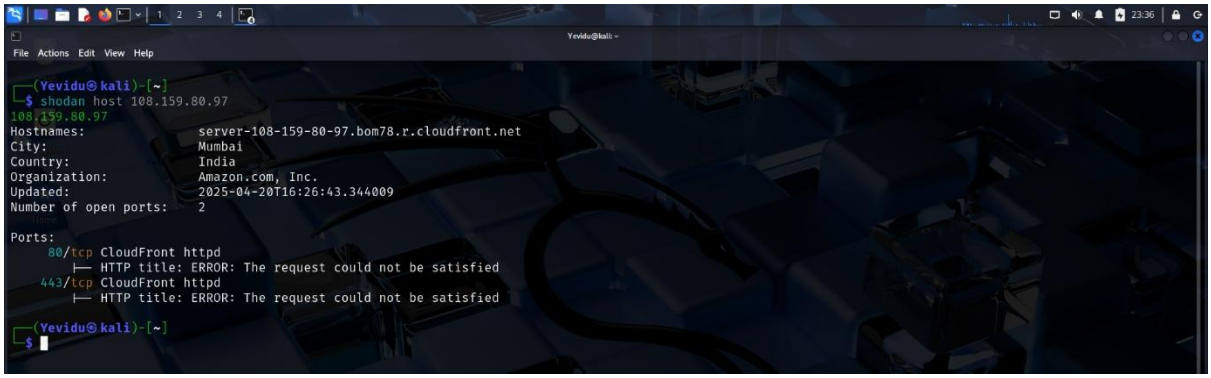
  108.159.80.26

  108.159.80.45

  108.159.80.81

  108.159.80.97

Shodan



IP Address: 108.159.80.97

Hostname: server-108-159-80-97.bom78.r.cloudfront.net

Location: Mumbai, India IN

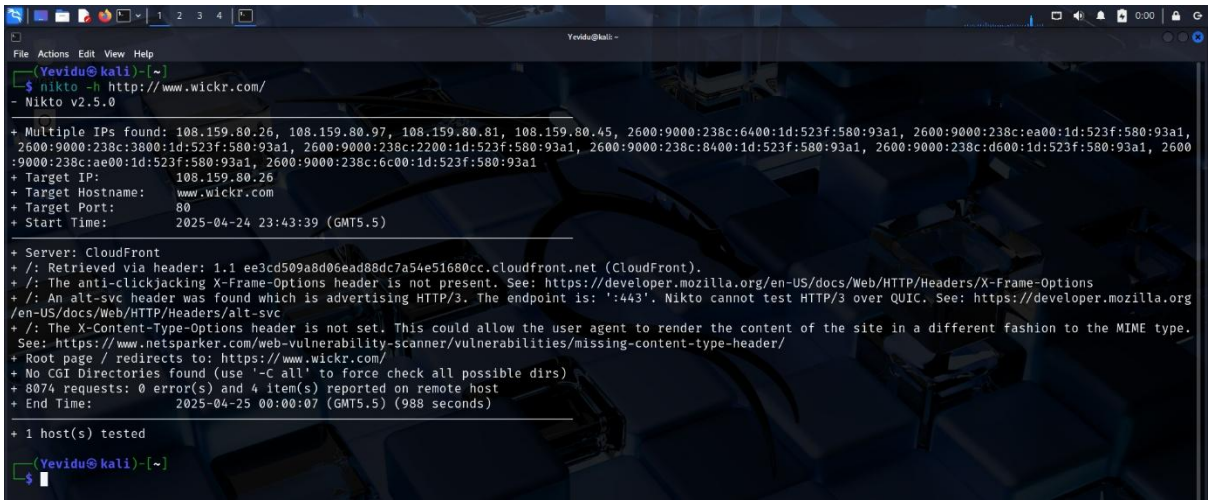
Organization: Amazon.com, Inc. (CloudFront CDN)

Last Updated: April 20, 2025

Port	Protocol	Service
80	TCP	HTTP
443	TCP	HTTPS

Scanning and vulnerability identification.

Nikto



- Site to target: www.wickr.com
- 108.159.80.26 is the target IP (IPv4)
- Web server: Amazon's CDN, CloudFront
- The website's HTTP version (http://) reroutes users to https://www.wickr.com/.

Headers Missing

- X-Frame-Options header is absence.

  Impact*:* clickjacking attacks

- X-Content-Type-Options header is absence.

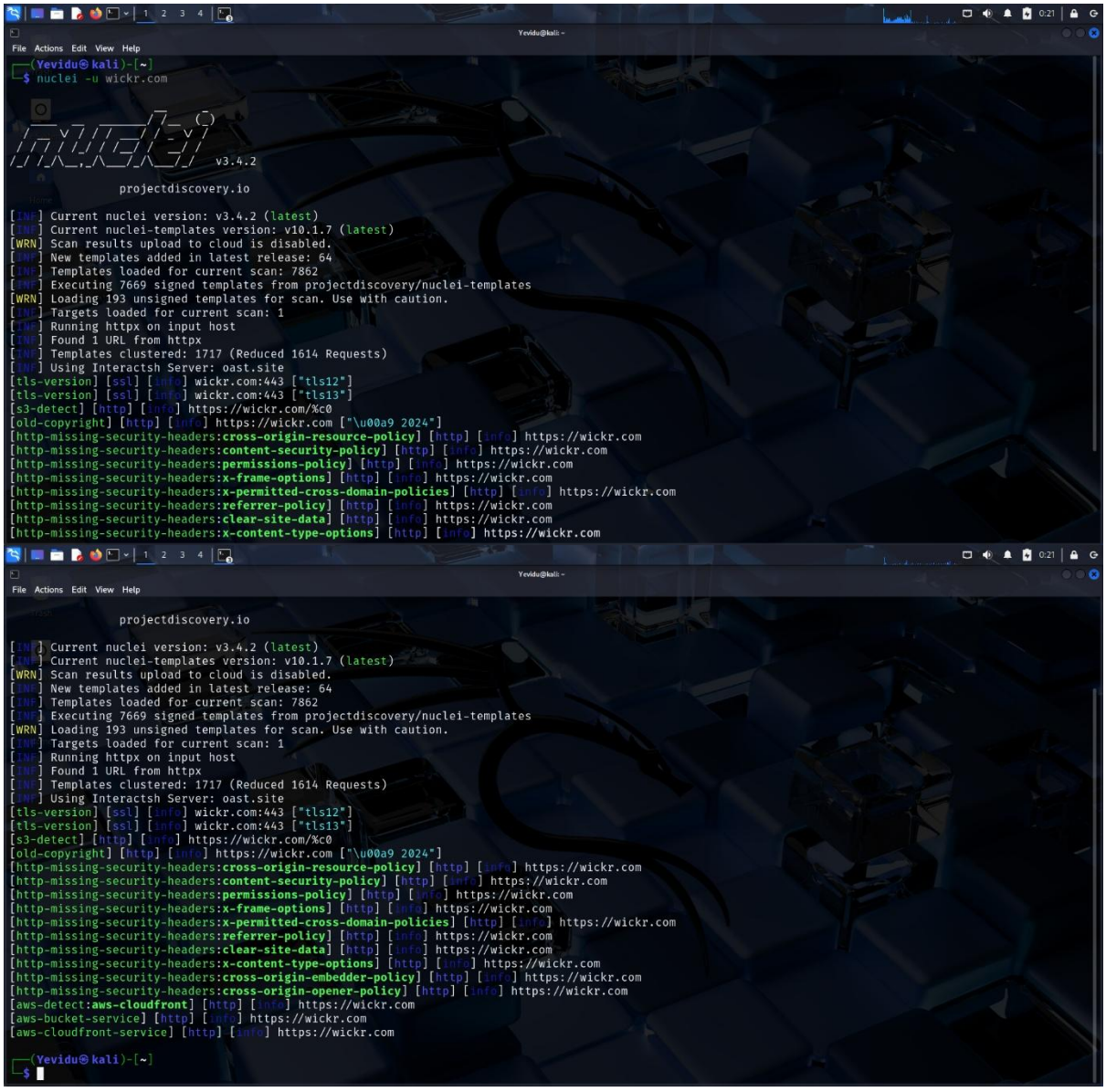
  Impact: MIME type sniffing vulnerabilities

Nmap

- Scanned IP: 108.159.80.45
- rDNS: server-108-159-80-45.bom78.r.cloudfront.net
- Host Status: Host is up with 25ms latency
- Other IPs: 108.159.80.97, 108.159.80.81, 108.159.80.26

Port	Service	Description
21	FTP	file transmission service that isn't encrypted. might be at risk if anonymous login is permitted.
80	HTTP	normal web traffic. HTTP redirects to HTTPS when used with open port 443.
443	HTTPS	Secure web traffic.
554	RTSP	Streaming Protocol in Real Time. may show streaming capabilities (e.g. media, cameras).
1723	PPTP	Protocol for Point-to-Point Tunnelling. a well-known security flaw in an outdated VPN protocol.
5060	SIP	protocol for starting a session. VoIP services use it, although it can be misused for spam or DoS attacks.

Nuclei



Nuclei version: v3.4.2

Number of templates used: 7862 (7669 signed, 193 unsigned)

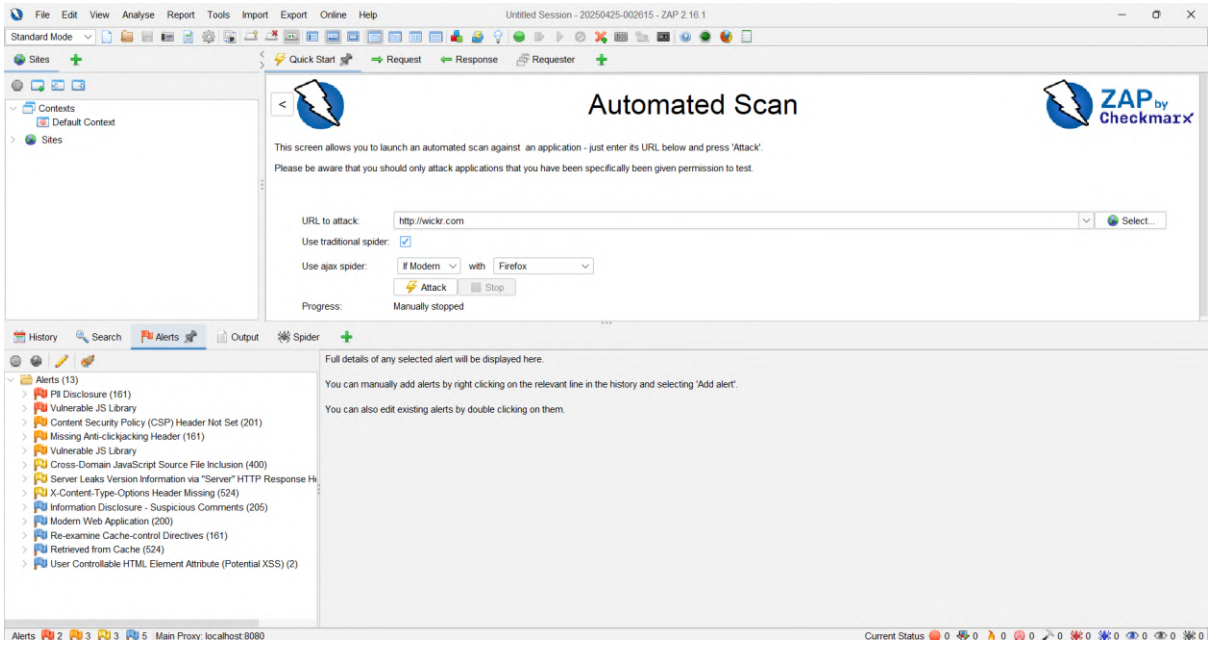
Target URL: https://wickr.com

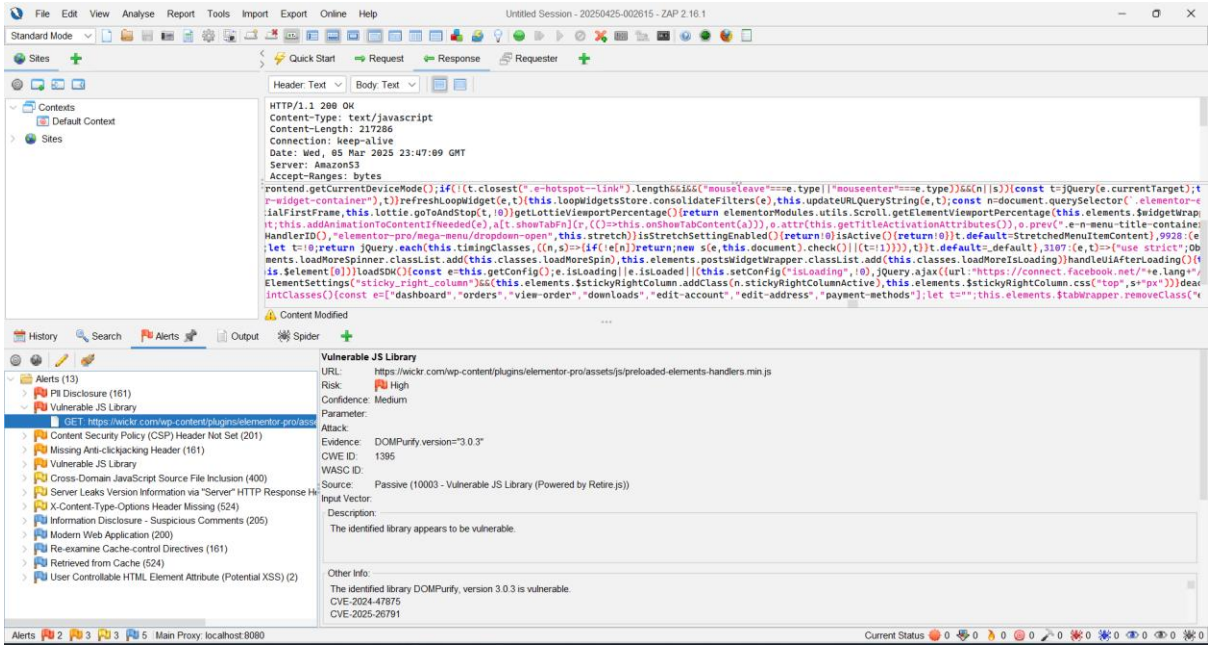
TLS Versions Supported: TLS 1.2 and TLS 1.3

AWS Services Found: CloudFront and possible S3 bucket

Missing Header	Risk
X-Frame-Options	Vulnerable to clickjacking
X-Content-Type-Options	MIME type sniffing might be possible.
Content-Security-Policy	Lack of command over scripts or resources
Permissions-Policy	No limitations on browser functionality (e.g., camera, microphone)
Referrer-Policy	may cause referrer headers to reveal private URLs.
Clear-Site-Data	might keep private information after logging out.
Cross-Origin Resource Policy	could permit risky cross-origin access
Cross-Origin Embedder Policy	Crucial for security based on isolation
Cross-Origin Opener Policy	aids in stopping side-channel attacks
X-Permitted-Cross-Domain-Policies	could make you vulnerable to outdated Flash-based assaults.

OWASP ZAP


Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://wickr.com
Use traditional spider:
Use ajax spider: If Modern with Firefox
Attack
Stop
Progress: Manually stopped
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.


HTTP/1.1 200 OK
Content-Type: text/javascript
Content-Length: 217286
Connection: keep-alive
Date: Wed, 05 Mar 2025 23:47:09 GMT
Server: AmazonS3
Accept-Ranges: bytes
Content Modified
Vulnerable JS Library
URL: https://wickr.com/wp-content/plugins/elementor-pro/assets/js/preloaded-elements-handlers.min.js
Risk: High
Confidence: Medium
Parameter:
Attack:
Evidence: DOMPurify.version="3.0.3"
CWE ID: 1395
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:
Description:
The identified library appears to be vulnerable.
Other Info:
The identified library DOMPurify, version 3.0.3 is vulnerable.
CVE-2024-47875
CVE-2025-26791

Alerts.

Vulnerable JS Library

Application Error Disclosure

CSP: Failure to Define Directive with No Fallback (217)

CSP: Wildcard Directive (217)

CSP: script-src unsafe-eval (217)

CSP: script-src unsafe-inline (217)

CSP: style-src unsafe-inline (217)

Missing Anti-clickjacking Header (213)

Cross-Domain JavaScript Source File Inclusion (141)

Information Disclosure - Debug Error Messages

Strict-Transport-Security Header Not Set (463)

Timestamp Disclosure - Unix (728)

X-Content-Type-Options Header Missing

Information Disclosure - Suspicious Comments (205)

Modern Web Application (86)

Re-examine Cache-control Directives (233)

Retrieved from Cache

Vulnerabilities.

➢ Cross-Site Scripting (XSS)

Issues Found:

- XSS (Persistent and Reflected) was detected by the OWASP ZAP scan.

Risk:

- Data Theft: Attackers could take sensitive data such as session cookies, user credentials, or personal information.
- Session Hijacking: By using malicious scripts, attackers may be able to take over users' sessions and access their accounts without authorization.
- Website Defacement: XSS could allow attackers to change the appearance or functionality of online pages.

How This Needs to Be Reduced:

- Verify that no executable code has been entered by sanitizing all user input.
- To stop the browser from perceiving user input as executable code, encode it before sending it to the page.
- Employ Content Security Policy (CSP): CSP lowers the likelihood of successful XSS attacks by limiting which scripts can run on the page.
- Make use of HTTP-only cookies: Mark cookies as HttpOnly to prevent JavaScript access to them.

➢ Broken Authentication

Issues Found:

- Both TLS 1.2 and TLS 1.3 appear to be supported, according to the Nmap scan**.**

Risk:

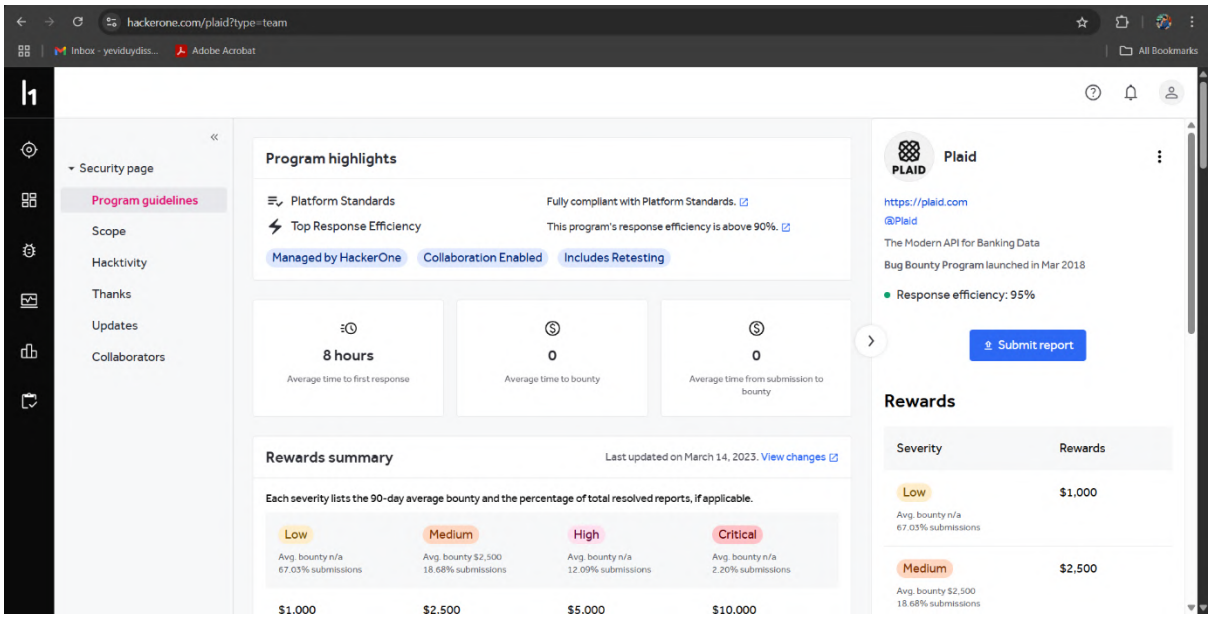
- Weak Encryption (TLS 1.2): Attackers may be able to decipher or alter messages if antiquated encryption techniques or weak ciphers are employed.
- SSL/TLS Downgrade Attacks: An attacker may try to compel the use of weak protocols by using a downgrade attack if the server supports earlier protocols (such as SSLv3).

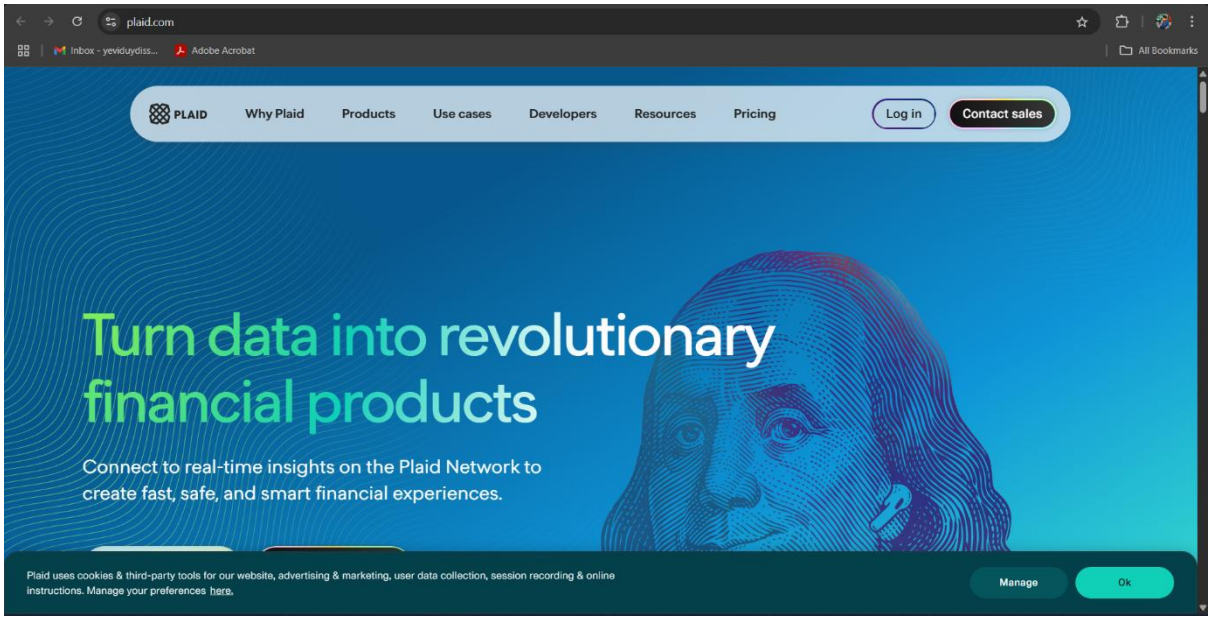
How This Needs to Be Reduced:

- Enforce TLS 1.3: Only permit TLS 1.2 or TLS 1.3 and disable previous SSL/TLS versions.
- Employ Robust Ciphers: Set up the server to employ robust, contemporary ciphers and turn off antiquated ones.
- SSL/TLS Testing: To make sure the server is configured securely, test it frequently with programs like SSL Labs' SSL Test.

Report 06.

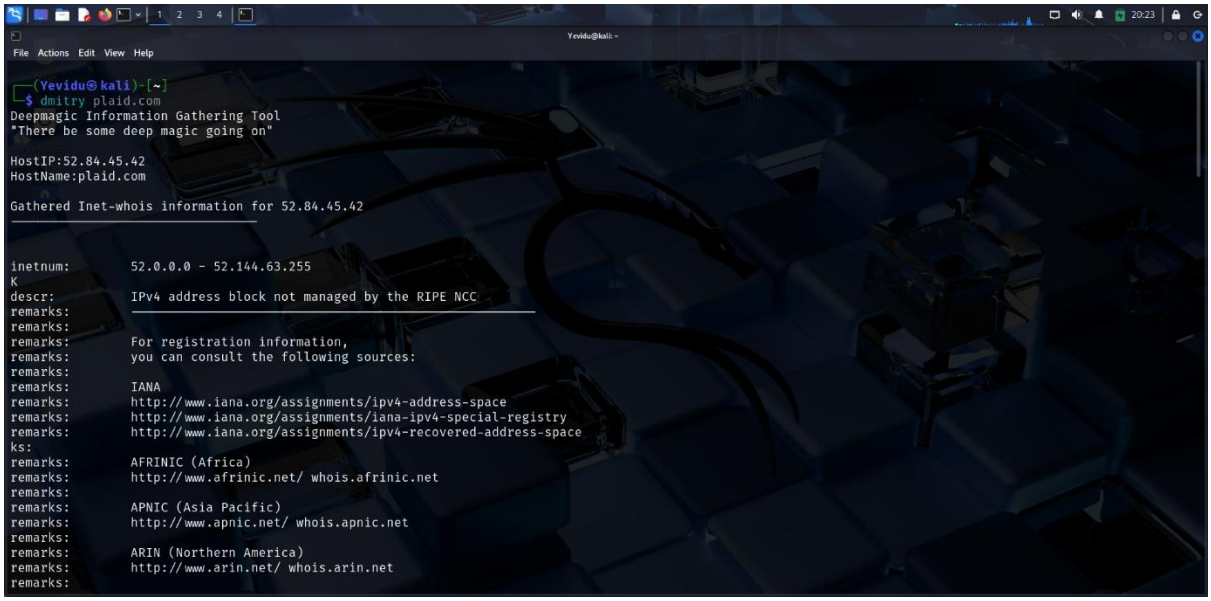
This Bug Bounty report focuses on Plaid (https://plaid.com/), a financial technology platform that allows apps to safely connect to consumers' bank accounts. Numerous fintech apps, including loans, investment services, personal finance, and mobile banking, are powered by Plaid's architecture. To provide safe access to account balances, transactions, and identity verification, users can connect their financial accounts to apps such as Coinbase, Robinhood, Venmo, and many more. Plaid uses strong security measures, such as multi-factor authentication, end-to-end encryption, and stringent access limits, to guarantee the confidentiality of private financial information. The platform is essential to the safe integration of financial data throughout the digital economy and is highly trusted by developers and financial institutions worldwide.

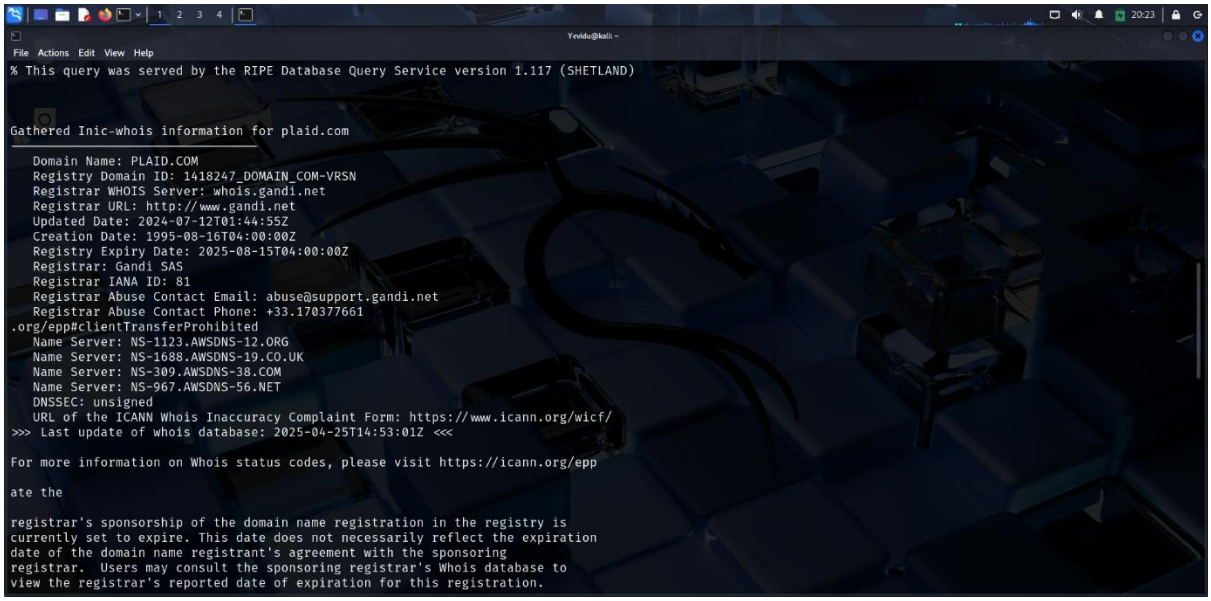


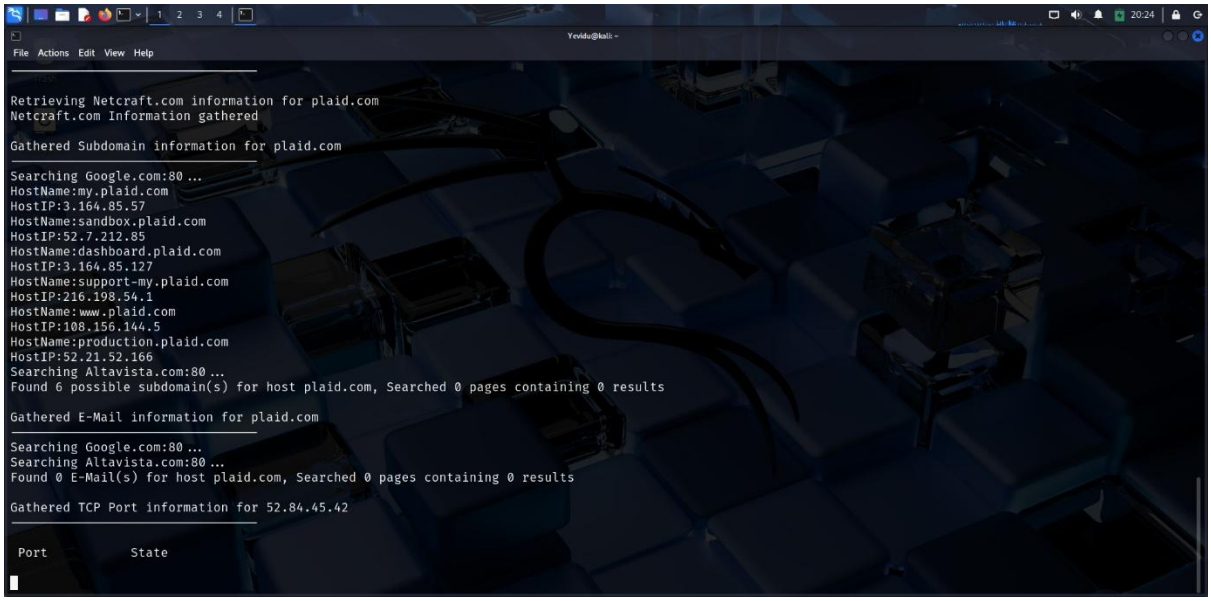


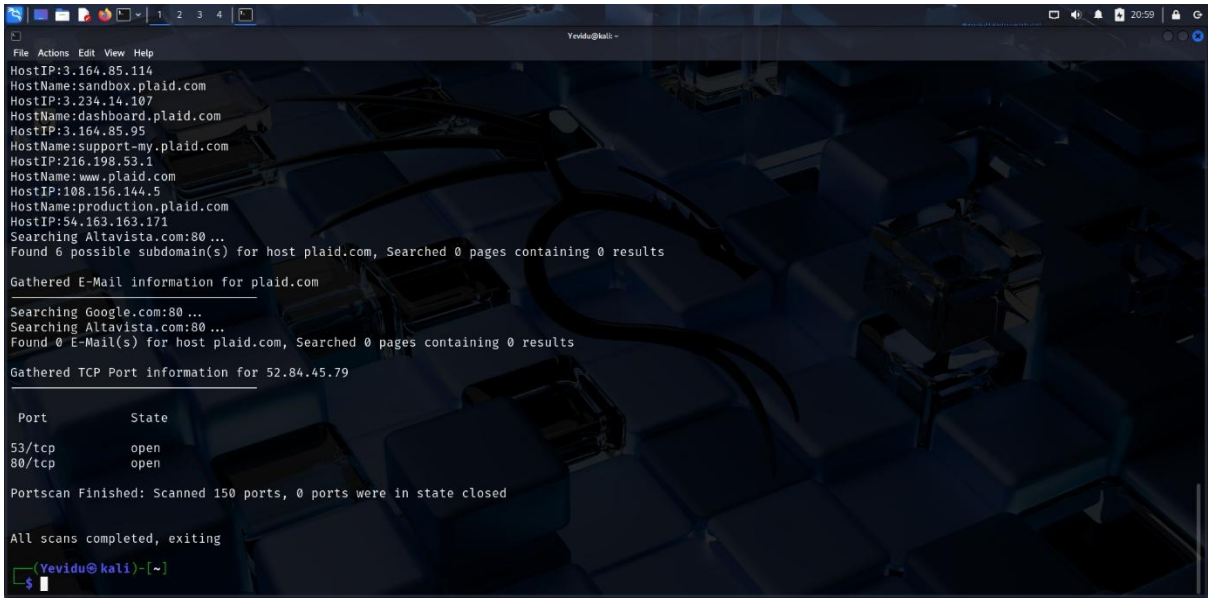
Target Reconnaissance.

Dmitry Scan









Details of the Host

Name of IP: 52.84.45.79

domain name: Plaid.com

Hosting Provider: Amazon Web Services (AWS)

Coordinator: Gandi SAS

Creation of the Domain: August 16, 1995

Domain expiration date: 15 August 2025

DNS servers:

NS-1123.AWSDNS-12.ORG

NS-1688.AWSDNS-19.CO.UK

NS-309.AWSDNS-38.COM

NS-967.AWSDNS-56.NET

WHOIS Data (IP)

52.0.0.0 to 52.144.63.255 is the IP range.

Internet Assigned Numbers Authority (IANA) is the assigning authority.

ARIN (North America) is the most likely regional registry.

Subdomains Found

my.plaid.com

sandbox.plaid.com

dashboard.plaid.com

support-my.plaid.com

www.plaid.com

production.plaid.com

Open TCP Ports

Port 53 (TCP) - DNS

Port 80 (TCP) – HTTP

Whatweb

200 OK is the status.

Server: CloudFront CDN via AmazonS3

Name of IP: 52.84.45.24

Nation: United States

Technologies: JSON scripting, HTML5, and Open Graph

Headers for security:

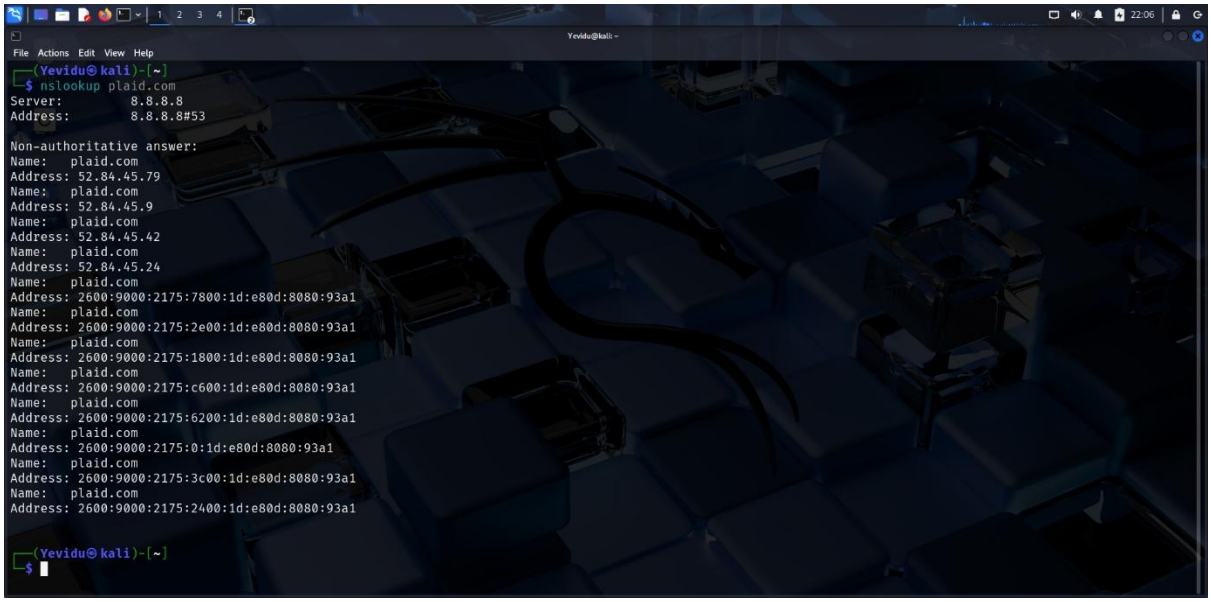
Strict-Transport-Security

Cookies: location

Driven by: Plaid

Title: Plaid: Facilitating the development of financial solutions for all businesses

Nslookup



IPv4 Addresses:

52.84.45.79

52.84.45.9

52.84.45.42

52.84.45.24

IPv6 Addresses:

2600:9000:2175: 7800:1d: e80d: 8080:93a1

2600:9000:2175:2e00:1d: e80d: 8080:93a1

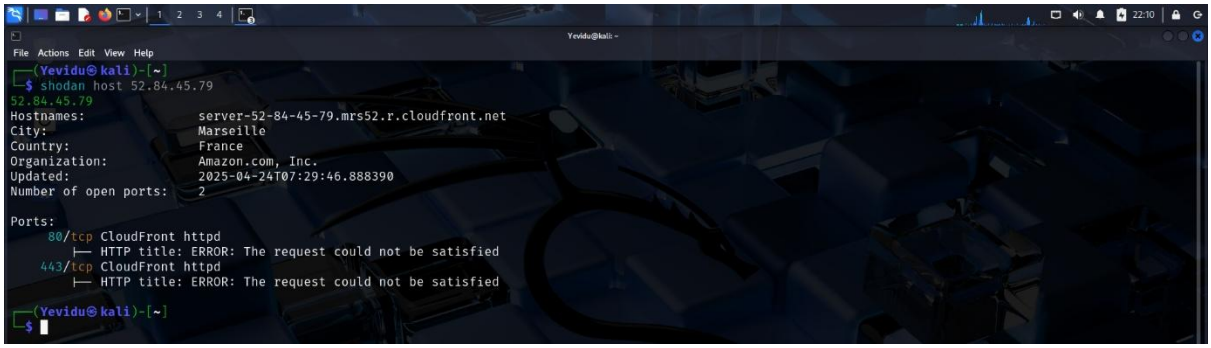
2600:9000:2175: 1800:1d: e80d: 8080:93a1

2600:9000:2175:c600:1d: e80d: 8080:93a1

2600:9000:2175: 6200:1d: e80d: 8080:93a1

2600:9000:2175: 0:1d: e80d: 8080:93a1

Shodan



Name of IP: 52.84.45.79

Server-52-84-45-79.mrs52.r.cloudfront.net is the hostname.

Location: Marseille, France

The company: Amazon.com, Inc.

Current Date of Update: April 24, 2025

Ports Open:

HTTP (CloudFront) 80/tcp

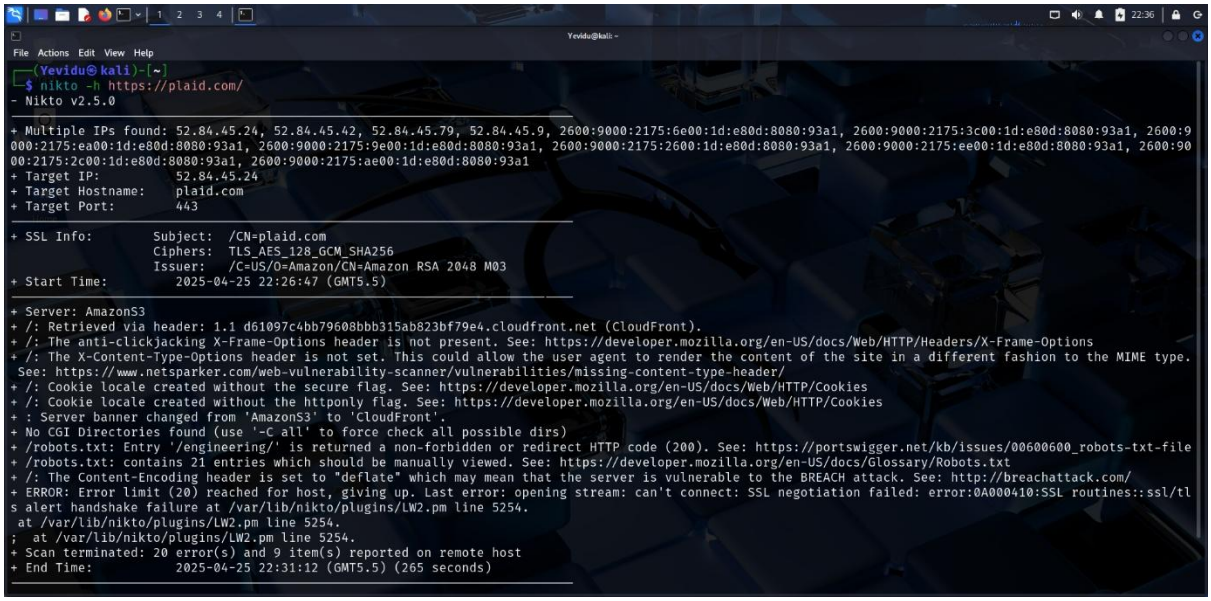
HTTPS (CloudFront) at 443/tcp

Titles of HTTP:

Both ports came back: "ERROR: The request could not be satisfied" is a common error message for CloudFront distributions that are limited or not enabled.

Scanning and vulnerability identification.

Nikto



General Information:

- Target Hostname: plaid.com
- Target IP: 52.84.45.24
- Port: 443 (HTTPS)
- Server: Initially AmazonS3, later observed as CloudFront
- SSL Certificate:
    - Subject: /CN=plaid.com
    - Issuer: Amazon RSA 2048 M03
    - Cipher Used: TLS_AES_128_GCM_SHA256

Security Issues Found:

- Missing Security Headers:
    - X-Frame-Options
    - X-Content-Type-Options

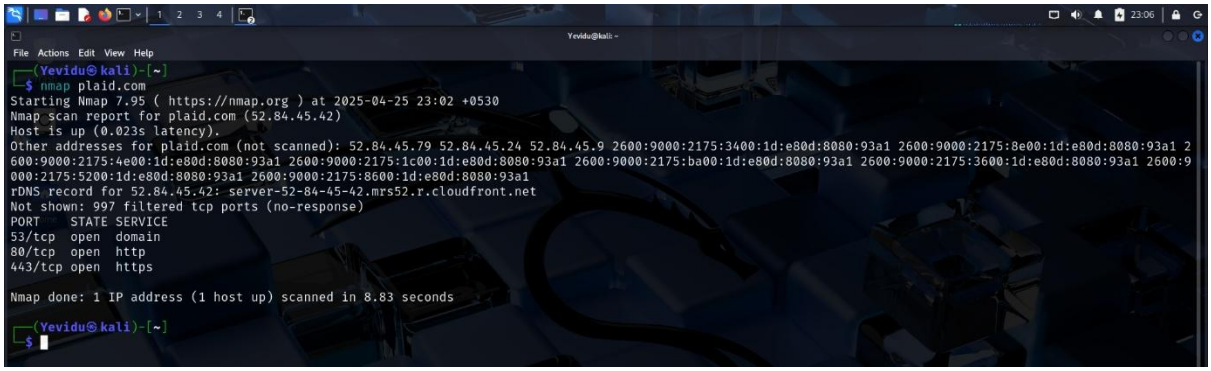
- BREACH Attack Risk:
    - Content-Encoding: deflate found.

- **Cookie Security Flags**:
    - cookie missing:

        Secure flag: May reveal cookies via non-HTTPS.

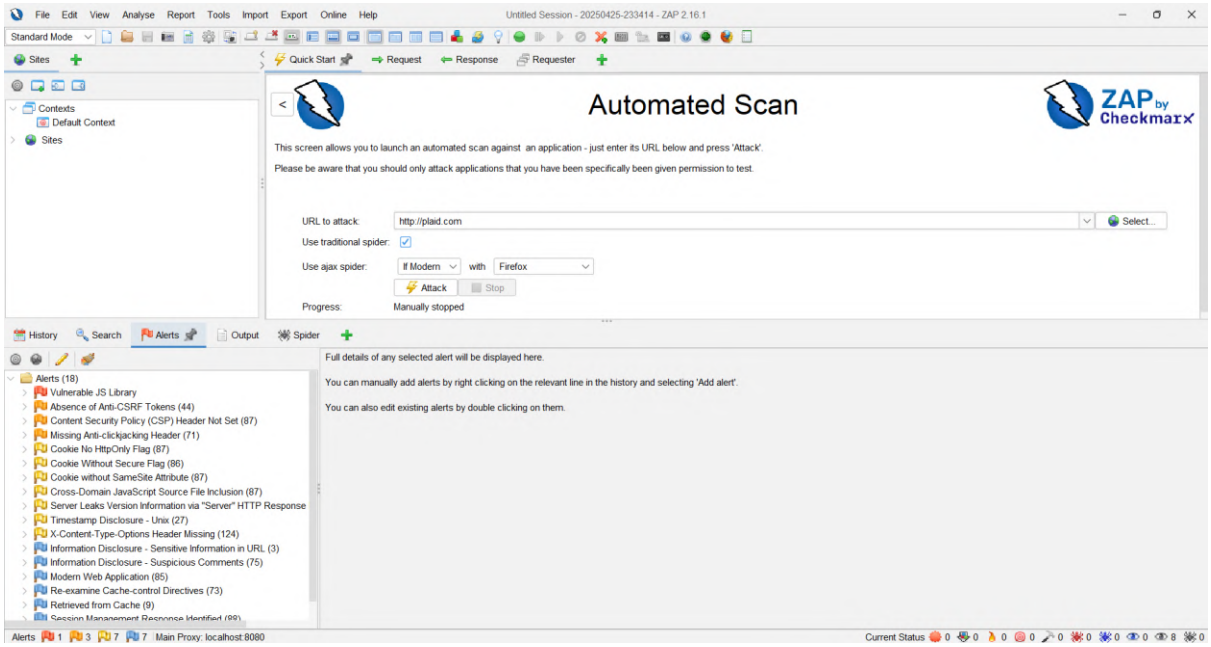
        HTTP Only flag: Open to client-side intrusions (like XSS attacks).

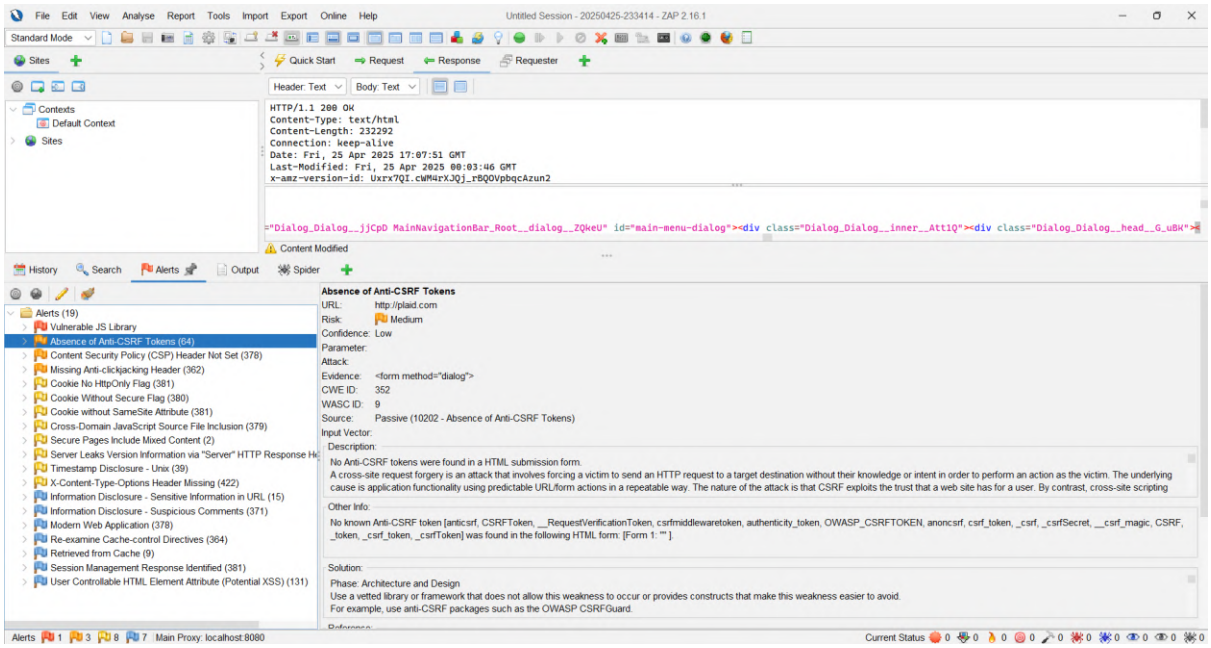
Nmap



- Presence of open port 53 (DNS) may indicate possible exposure of DNS services.
- Standard HTTP (80) and HTTPS (443) services running — further inspection can reveal misconfigurations or vulnerabilities.
- Services are hosted on CloudFront, Amazon's CDN, suggesting potential mitigations like WAF or rate limiting in place.

OWASP ZAP


Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://plaid.com
Use traditional spider:
Use ajax spider: If Modern with Firefox
Attack
Stop
Progress: Manually stopped
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.


HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 232292
Connection: keep-alive
Date: Fri, 25 Apr 2025 17:07:51 GMT
Last-Modified: Fri, 25 Apr 2025 00:03:46 GMT
x-amz-version-id: Uxrx7QI.cWM4rXJQj_rBQOVpbqcAzun2
Content Modified
Absence of Anti-CSRF Tokens
URL: http://plaid.com
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form method="dialog">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting
Other Info:
No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: ""].
Solution:
Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Vulnerabilities.

➢ Security Misconfiguration

Missing Anti-CSRF Protections

Found Issues:

According to the Nikto scan:

There is no sign of CSRF protection features like CSRF tokens or Same Site cookie characteristics.

Due to their lack of Secure or HTTP Only signals, cookies (locale) were more susceptible to client-side access.

Weak security hardening is indicated by the absence of two important headers: X-Frame-Options and X-Content-Type-Options.

Risk:

An attacker can use Cross-Site Request Forgery (CSRF) to:

- Concede a verified user to send a request to a web application without realizing it.
- For instance, if a malicious website is visited by a logged-in user, it may discreetly send a POST request to plaid.com on the user's behalf, such as to link bank accounts or start transactions.

How This Needs to Be Reduced:

- Use and validate server-side anti-CSRF tokens in all state-changing forms.
- Use the following flags when setting cookies:

  Safe (makes sure cookies are only transmitted via HTTPS.)

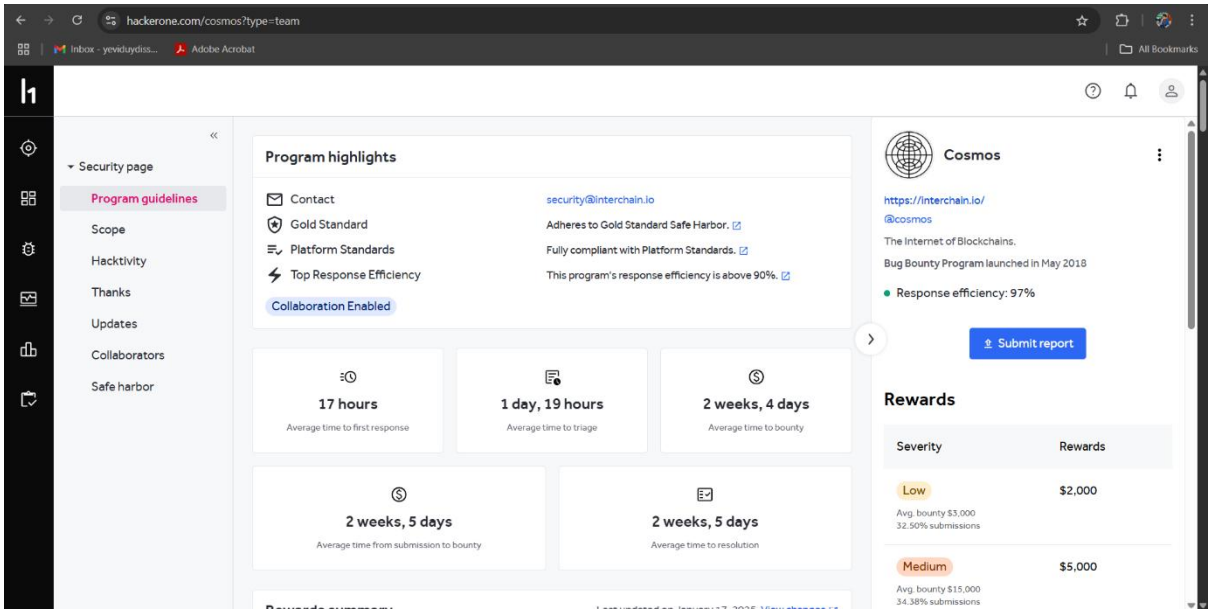
  HTTP Only (blocks cookies from being accessed by JavaScript)

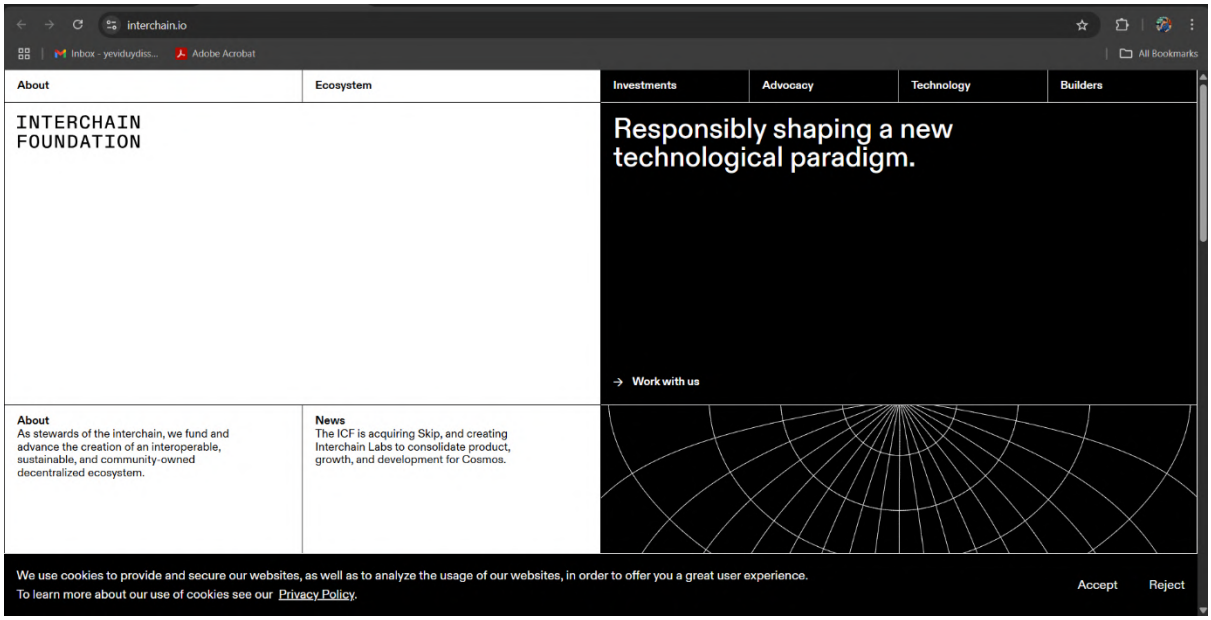
  Same Site=Strict or Same Site=Lax (which restricts the transfer of cross-site cookies)

- Put in place appropriate CORS policies.
- Return X-Frame-Options: DENY or SAMEORIGIN to stop clickjacking and other UI redress attacks.

Report 07.

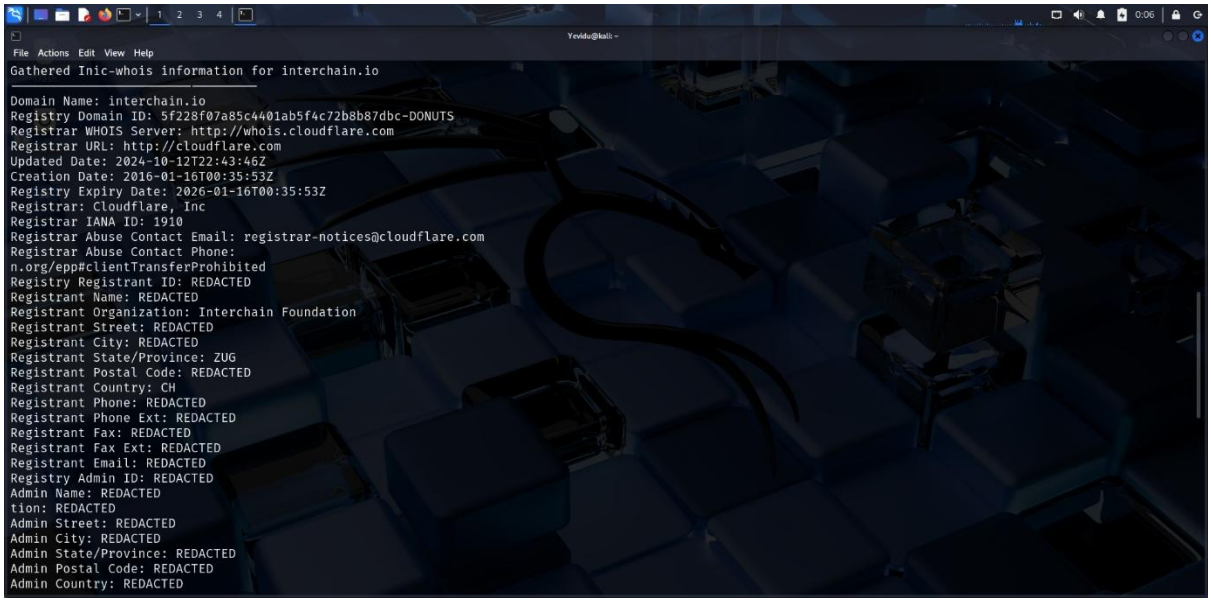
Interchain (https://interchain.io/), an open-source ecosystem devoted to facilitating safe communication and interoperability between separate blockchains, is the subject of this Bug Bounty report. The Inter-Blockchain Communication (IBC) protocol, which is the foundation of Interchain's design, enables blockchains to exchange assets and data without compromising sovereignty. This decentralized framework supports scalability, modularity, and cross-chain collaboration, which is advantageous for projects like Cosmos, Osmosis, and Akash that are constructed inside the Interchain ecosystem. Interchain places a strong emphasis on safe interactions by using strong validation procedures, decentralized consensus, and cryptographic proofs. Interchain, the foundation of blockchain interoperability, is essential to creating a more secure, scalable, and interconnected decentralized internet.

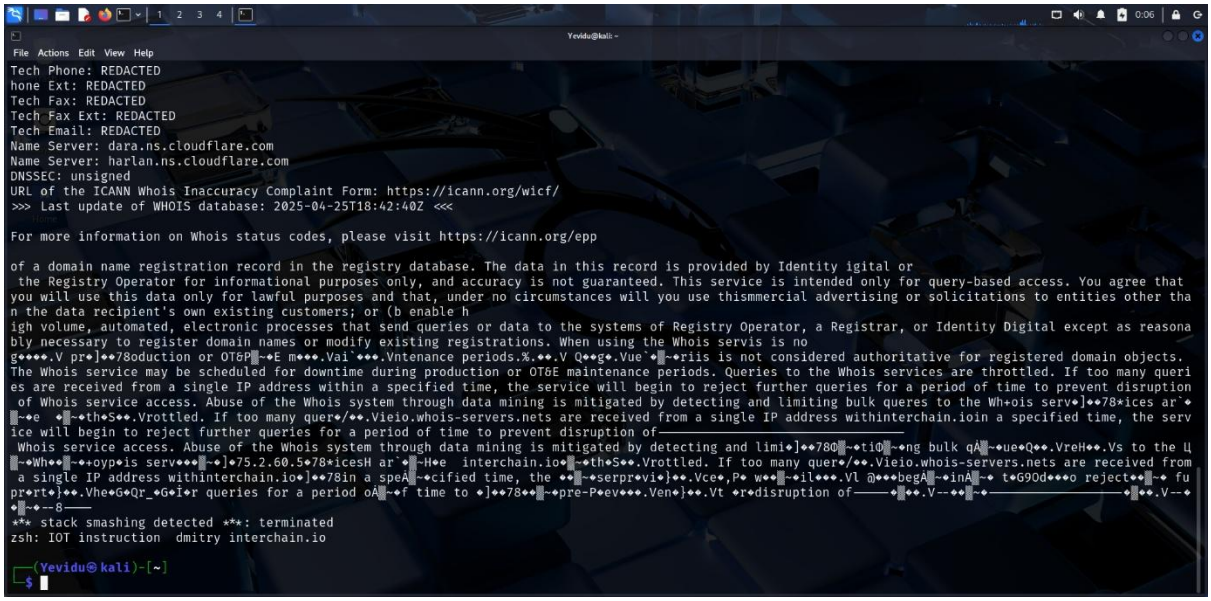




Target Reconnaissance.

Dmitry Scan





IP Address: 75.2.60.5

Hostname: interchain.io

IP WHOIS Details-

The IP address is part of a globally allocated block that is not under the direct management of RIPE NCC.

The wider IP range: 75.119.127.255 to 74.220.32.0.

Authority: Managed under IANA (Internet Assigned Numbers Authority).

Region: Global (often referred to as the "EU").

WHOIS Details for the Domain-

Interchain.io is the domain.

On January 16, 2016, it was created.

The expiration date is January 16, 2026.

Cloudflare, Inc. is the registry.

Name servers:

Cloudflare.com/dara.ns

Cloudflare.com/harlan.ns

Interchain Foundation, a Zug, Switzerland-based organization, is the registrant.

Whatweb

IP: 75.2.60.5 (United States)

Redirect: HTTP (interchain.io) redirects to HTTPS

Web Server: Netlify

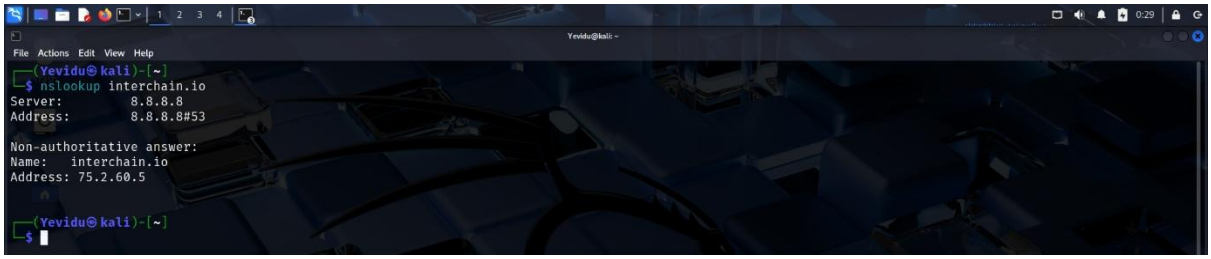
Security Header: Strict-Transport-Security enabled

Email Found: hello@interchain.io

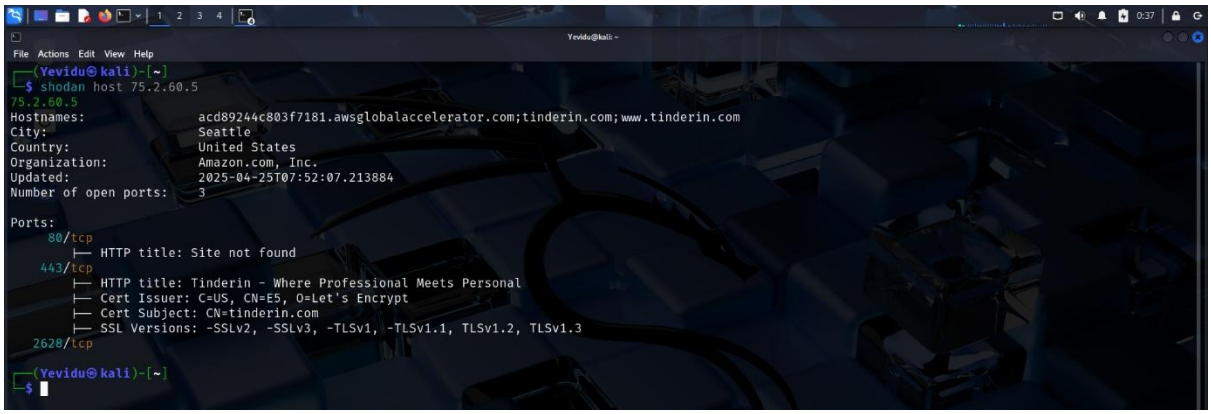
Tech Found: HTML5, Open Graph Protocol

Custom Headers: x-nf-request-id, cache-status, netlify-vary

Nslookup



Shodan



Location: Seattle, USA

The company is Amazon.com, Inc.

Hostnames:

- www.awsglobalaccelerator.com/acd89244c803f7181
- Tinderin.com
- Tinderin.com

Open Ports: 2628, 443, 80

HTTP Port 80: Displays "Site not found"

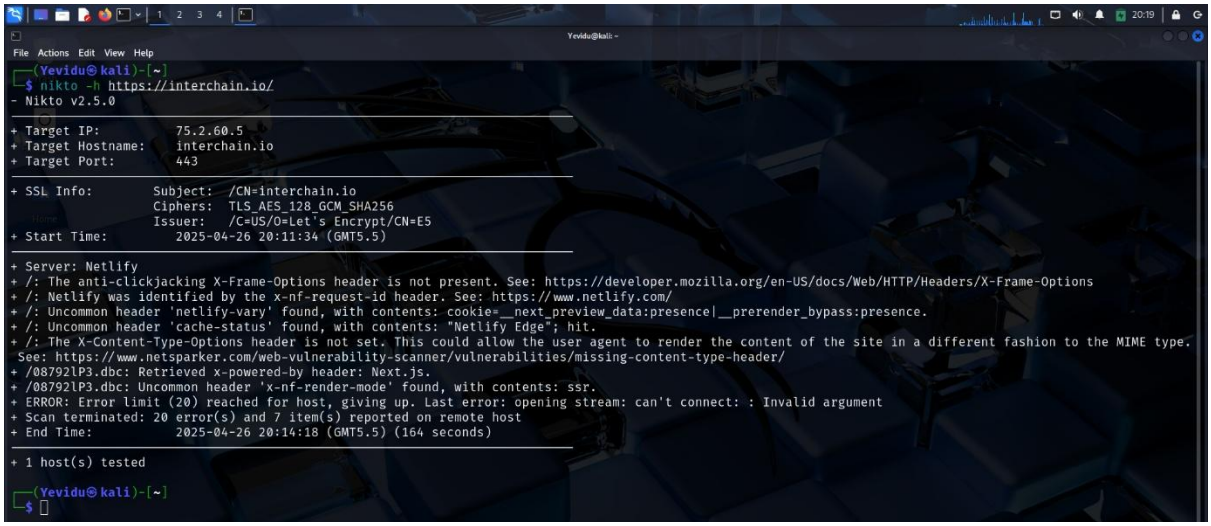
HTTPS port 443:

- Theme: "Tinderin - Where Professional Meets Personal"
- Certificate: Issued by Let's Encrypt for tinderin.com
- SSL Support: TLS 1.2 and TLS 1.3 only

Updated on April 25, 2025

Scanning and vulnerability identification.

Nikto



- SSL Certificate:

  Subject: CN=interchain.io

  Issuer: Let's Encrypt

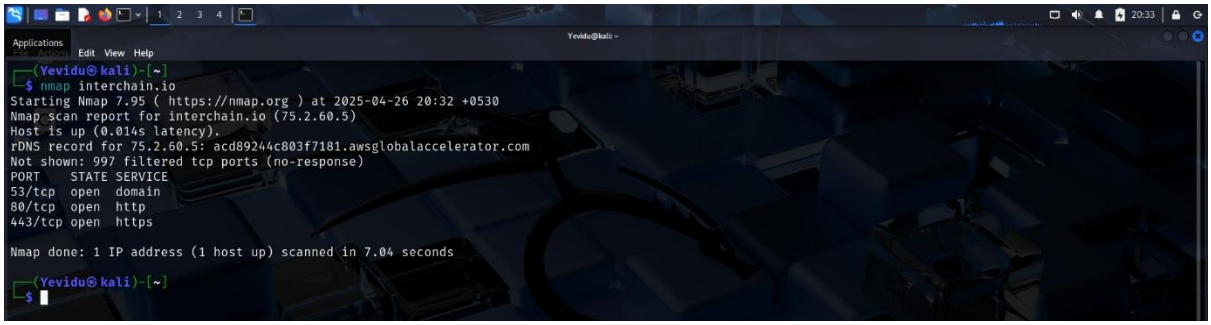
  Cipher: TLS_AES_128_GCM_SHA256

- Security Headers Missing:

  The absence of the X-Frame-Options header increases the risk of clickjacking attacks.

  The missing X-Content-Type-Options header increases the possibility of MIME Sniffing attacks.

Nmap



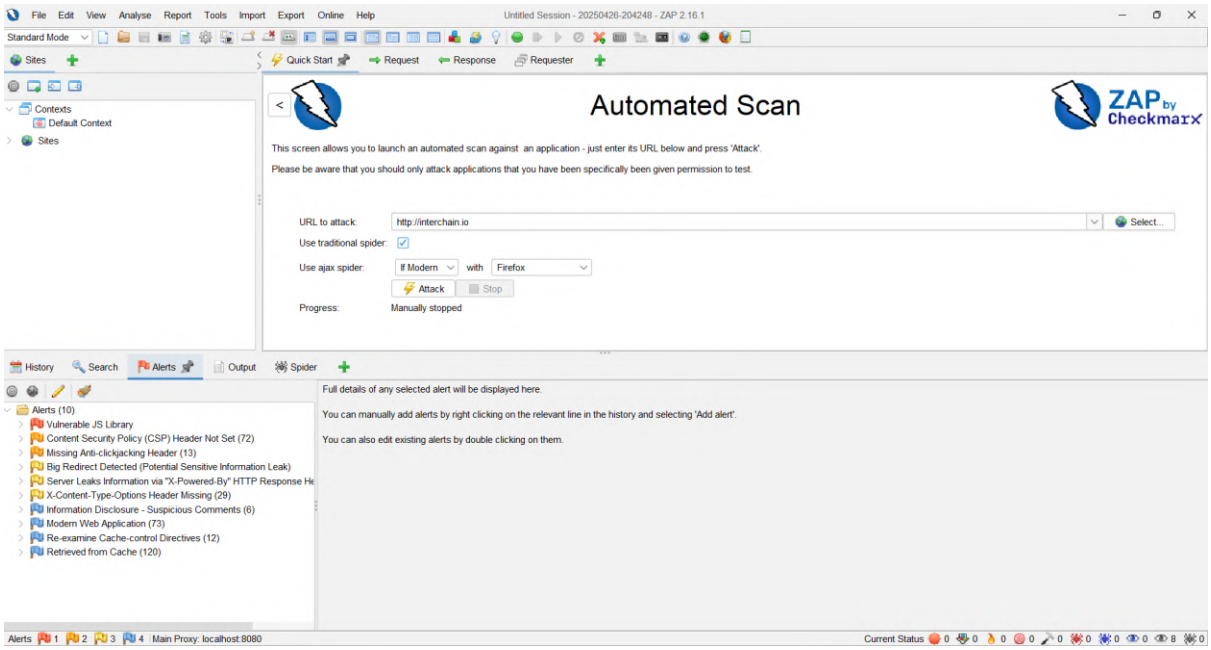
Ports Open:

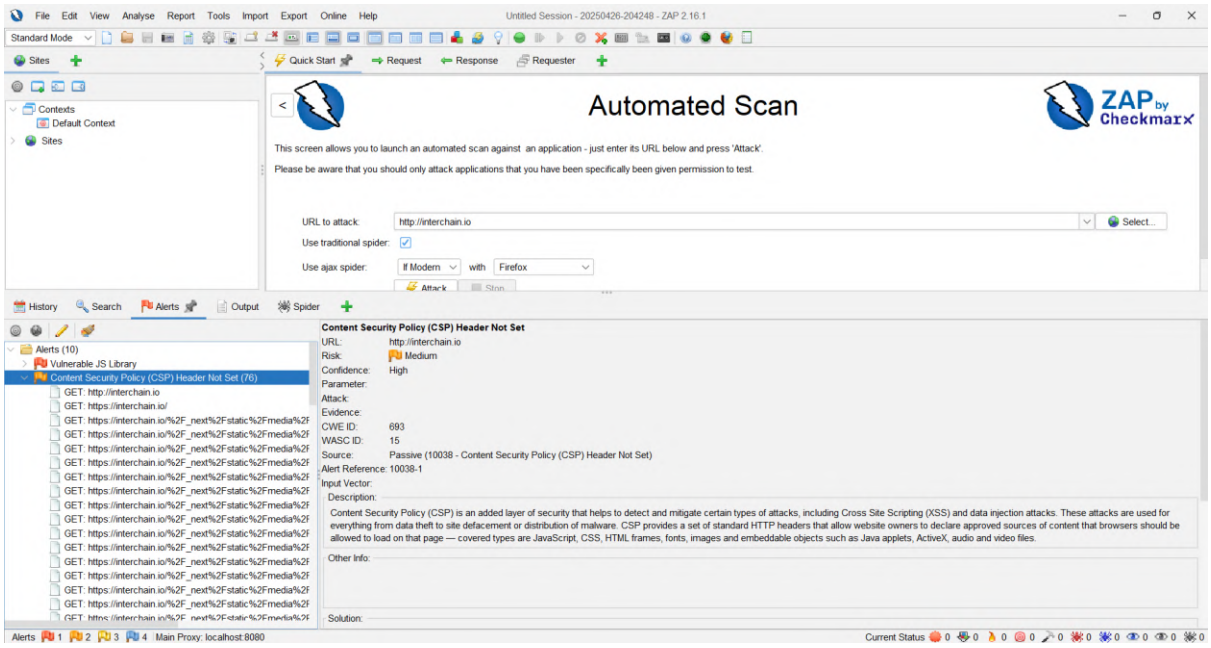
The Domain Name System (DNS) service is operating at 53/tcp.

HTTP service (web traffic, unencrypted) is available at 80/tcp.

The HTTPS service (secure web traffic) is available at 443/tcp.

OWASP ZAP





Alerts.

- Content Security Policy (CSP) Header Not Set
- Cross-Domain JavaScript Source File Inclusion
- X-Content-Type-Options Header Missing
- Missing X-Frame-Options Header
- Cookie Without Secure Flag
- Cookie Without HttpOnly Flag

Vulnerabilities.

- **Cross-Site Scripting (XSS)**

Missing Content Security Policy (CSP) Header

Found Issues:

No Content Security Policy (CSP) header is set on the interchain.io website.
A strong security feature, CSP limits the resources (such as JavaScript, pictures, and styles) that can be loaded or used on a webpage.

Risk:

If an application has even a minor XSS vulnerability without a CSP, an attacker can:

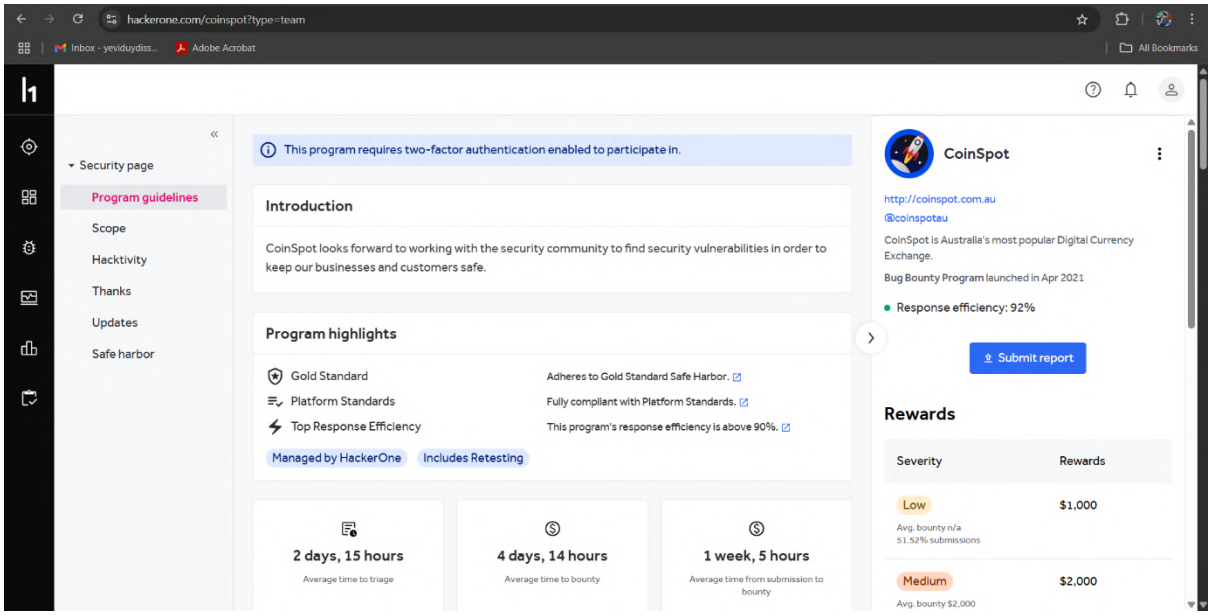
- Add harmful JavaScript to the website.
- Take over a session by stealing cookies.
- Execute tasks as the user, such as making transactions or modifying account information.
- vandalize the website or send visitors to dangerous websites.

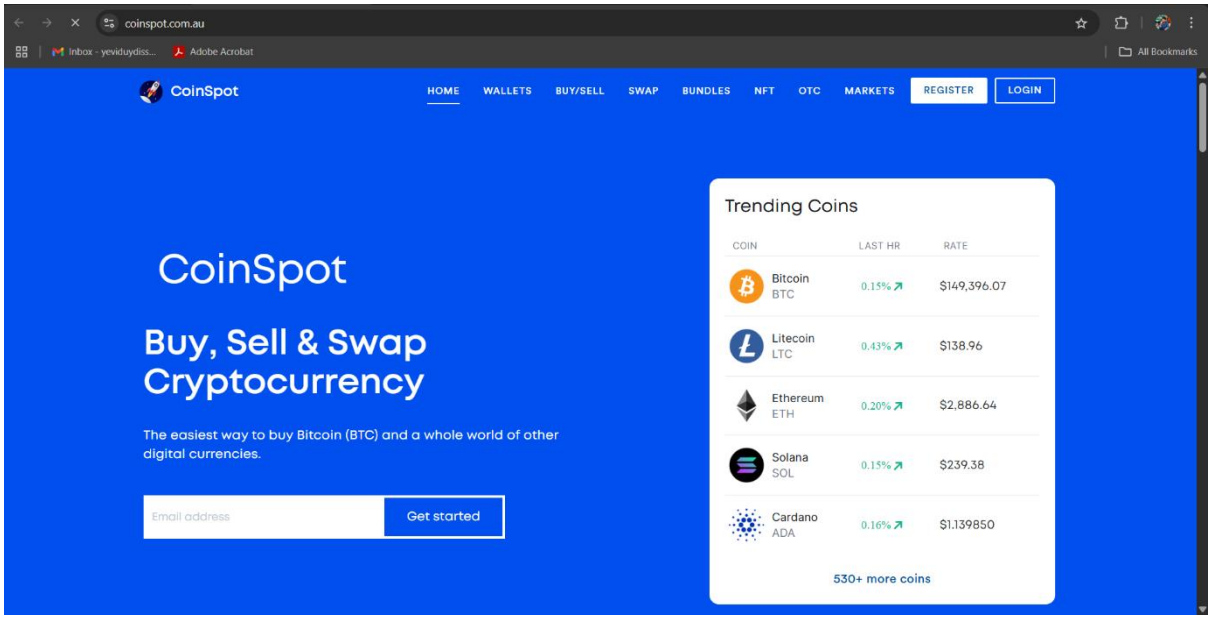
How This Needs to Be Reduced:

- Put in place a robust content security policy that restricts scripts from reliable domains.
- Verify and clean every user entry on the client and server sides.
- Make use of frameworks (such as React and Angular) that automatically escape output.

Report 08.

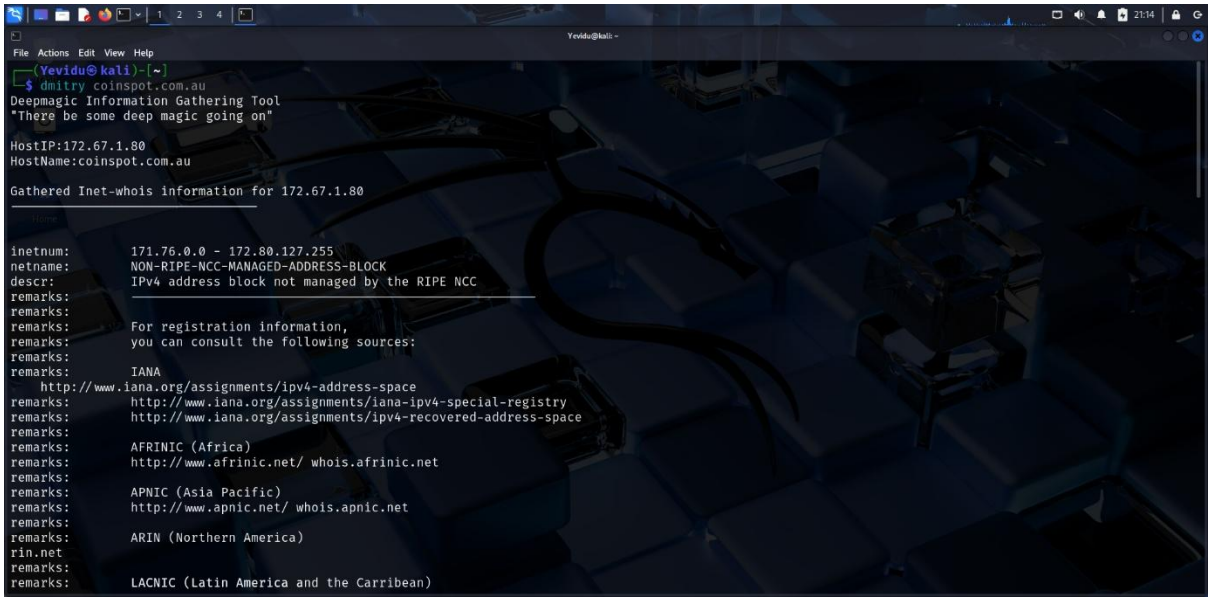
This Bug Bounty report focuses on CoinSpot (https://www.coinspot.com.au/), a well-known cryptocurrency exchange site in Australia. CoinSpot, which was founded in 2013, offers a safe and easy-to-use platform for managing, purchasing, and selling a variety of digital assets, including more than 400 cryptocurrencies. CoinSpot prioritizes security, regulatory compliance, and consumer protection as a Blockchain Australia certified member and an ISO 27001 approved platform. Its features, which are supported by strict security requirements including multi-layered authentication, cold storage options, and sophisticated encryption techniques, include instant buying and selling, staking, multi-coin wallets, and an NFT marketplace. By promoting safe, easy, and regulated digital asset trading for both people and institutions, CoinSpot plays a vital part in the Australian crypto economy.

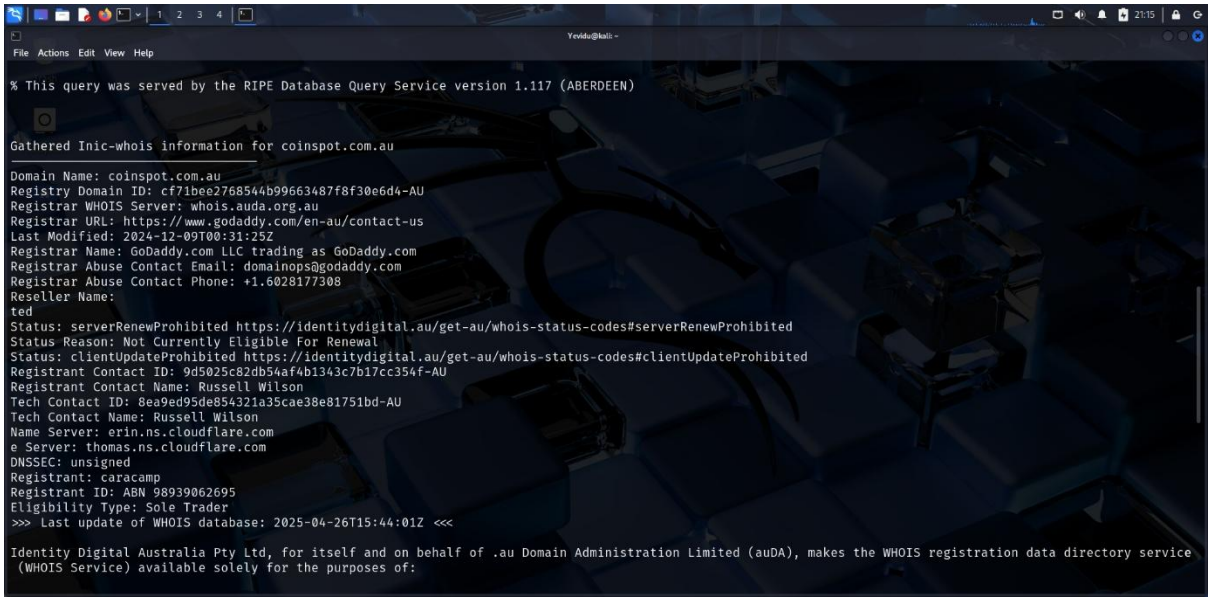


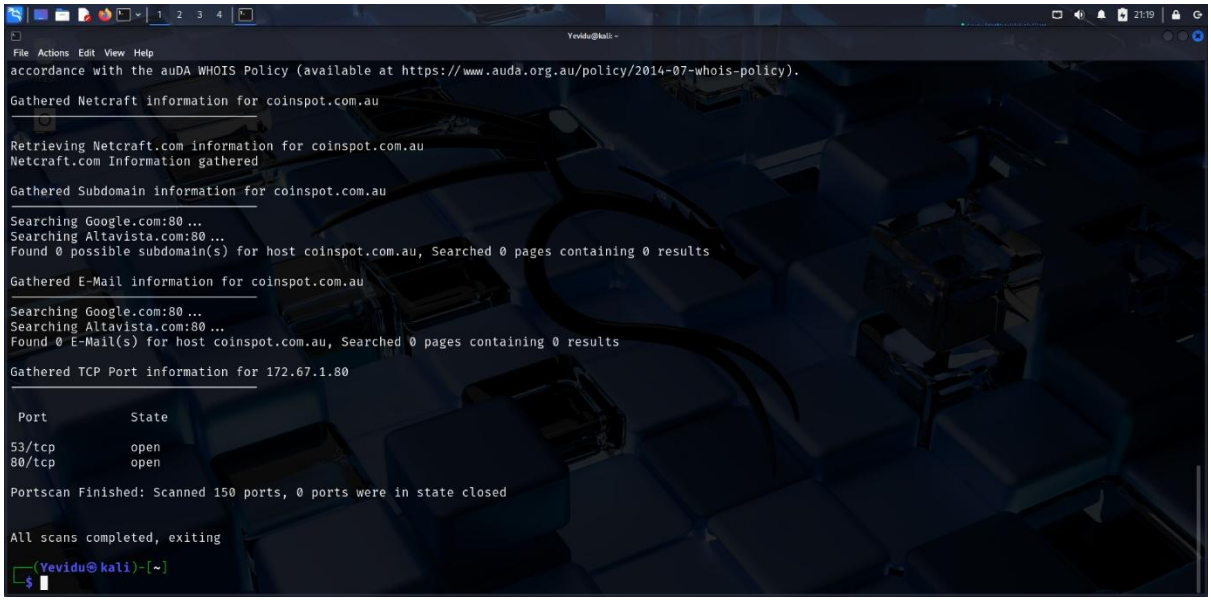


Target Reconnaissance.

Dmitry Scan







IP address of the host: 172.67.1.80

host name: Coinspot.com.au

WHOIS Information (IP):

The IP address 172.67.1.80 is part of a block that is not under the direct control of the RIPE NCC, suggesting that IANA oversees worldwide allocation. Instead, then referring to a particular regional organization, the block is generally connected with global infrastructure.

WHOIS Details (Domain):

GoDaddy.com LLC is the domain registration company for coinspot.com.au.

Registrant: Russell Wilson, a business associate of "caracamp" (ABN 98939062695)

Domain Status: Prohibited Server Renew and Prohibited Client Update (limited from actions related to renewal and update)

Name servers: Erin.ns.cloudflare.com and Thomas.ns.cloudflare.com

DNSSEC: Unsigned or not signed.

Scan of TCP Ports:

Open Port 53/tcp (DNS)

Open port 80/tcp (HTTP)
Only ports 53 and 80 were found to be open out of the 150 ports that were examined.

Whatweb

First Redirects:

HTTP 301 is redirected to https://coinspot.com.au/ from http://coinspot.com.au.

HTTP 301 is further redirected to https://www.coinspot.com.au/ by https://coinspot.com.au/.

Last Stop:

The response from https://www.coinspot.com.au/ is HTTP 200 OK.

Headers and Technologies Found:

Bootstrap is the frontend framework.

Version of HTML is HTML5

Server for the Web is Cloudflare

Features of Security:

Maximum-age=63072000 for Strict-Transport-Security (2 years HTTPS enforcement)

X-Frame-Options: SAMEORIGIN (clickjacking prevention)

X-XSS-Protection: 1; mode=block (defense against XSS attacks that are reflected)

Content Security Policy: Found (this scan does not display all the data).

Only Http Cookies: Found for _csrf

Unusual Headers for Security:

Options for x-content-type

referrer-policy

policy for cross-origin openers

cf-cache-status

cf-ray

Cookies Found:

enhanced defense against Cross-Site Scripting (XSS) by using a _csrf cookie with the HTTP Only flag.

IP Address:

IP address of the final site: 104.20.10.243 (provided via the Cloudflare network).

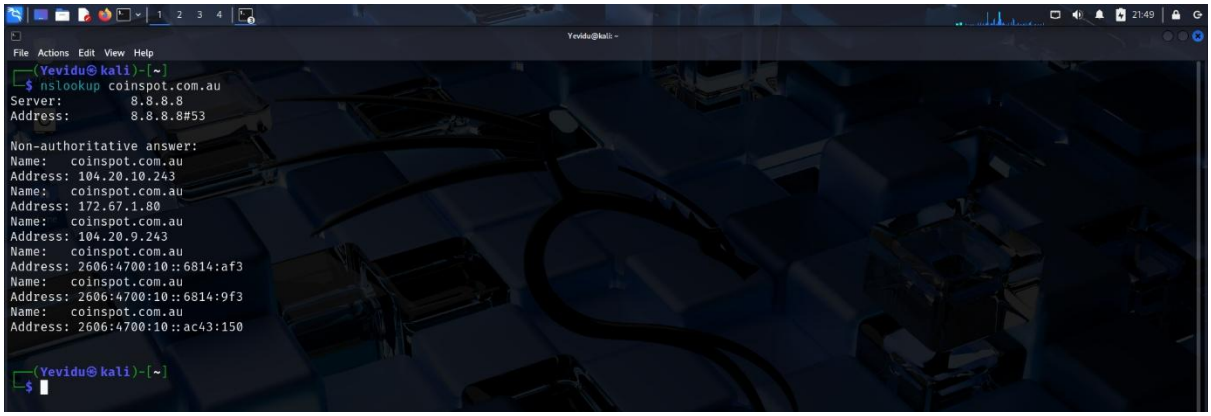
Location:

Despite CoinSpot being an Australian company, it was identified as being hosted in the United States [US] (because of Cloudflare's dispersed CDN architecture).

Title of Page:

"Australian Crypto & Bitcoin Exchange, Crypto Trading | CoinSpot"

Nslookup



IPv4 Addresses:

- 104.20.10.243
- 104.20.9.243
- 172.67.1.80

IPv6 Addresses:

- 2606:4700:10::6814:af3
- 2606:4700:10::6814:9f3
- 2606:4700:10::ac43:150

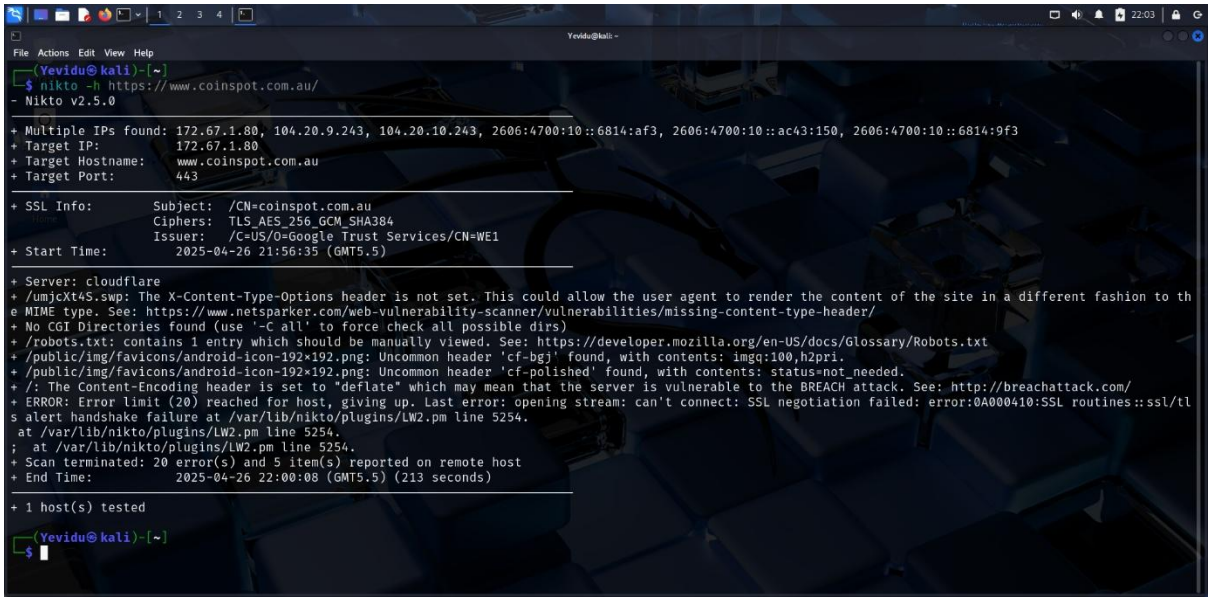
Remarks:

The usage of content delivery networks (CDNs), particularly through Cloudflare, and load balancing is indicated by multiple IP addresses.

Broader accessibility and service future-proofing are ensured by the presence of both IPv4 and IPv6 addresses.

Scanning and vulnerability identification.

Nikto



Vulnerabilities and problems found:

MIME type sniffing attacks are possible since the X-Content-Type-Options header is missing at /umjcXt4S.swp.

found the robots.txt file contains a single entry that needs to be manually examined for leaks of sensitive information**.**

Possible vulnerability for a breach:

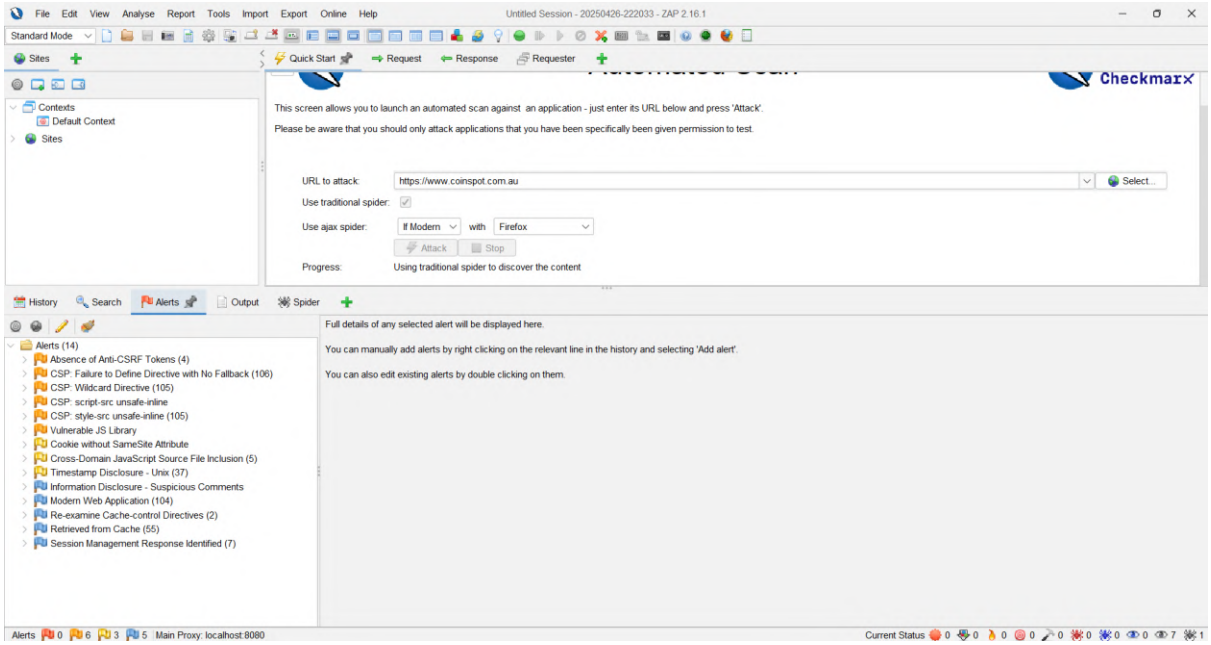
Content-Encoding: deflate is used on the homepage (/). Compression can be used by BREACH attacks to steal information.

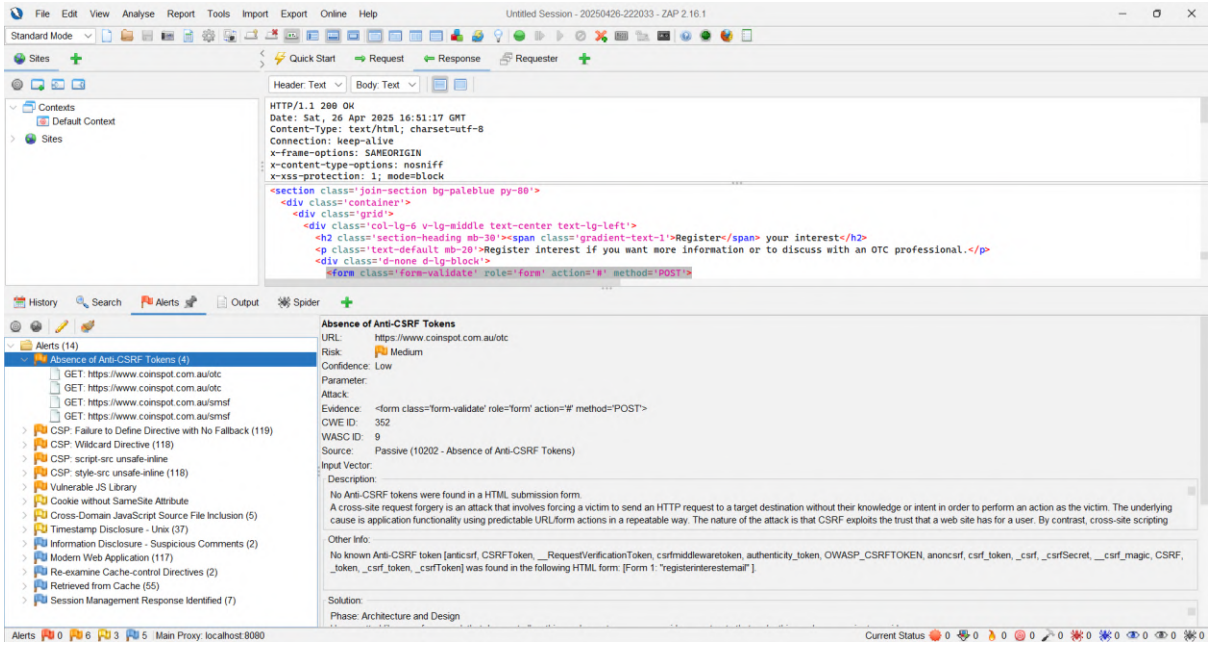
Nmap

Open TCP Ports and Services:

- 53/tcp → domain (likely DNS)
- 80/tcp → http (web traffic)
- 443/tcp → https (secure web traffic)
- 8080/tcp → http-proxy (often used for proxy servers or alternative web interfaces)

OWASP ZAP




File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - 20250426-222033 - ZAP 2.16.1
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Date: Sat, 26 Apr 2025 16:51:17 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
<section class='join-section bg-paleblue py-80'>

<h2 class='section-heading mb-30'>Register your interest</h2>
Register interest if you want more information or to discuss with an OTC professional.

<form class='form-validate' role='form' action='#' method='POST'>
History
Search
Alerts
Output
Spider
Alerts (14)
Absence of Anti-CSRF Tokens (4)
GET: https://www.coinspot.com.au/otc
GET: https://www.coinspot.com.au/otc
GET: https://www.coinspot.com.au/smsf
GET: https://www.coinspot.com.au/smsf
CSP: Failure to Define Directive with No Fallback (119)
CSP: Wildcard Directive (118)
CSP: script-src unsafe-inline
CSP: style-src unsafe-inline (118)
Vulnerable JS Library
Cookie without SameSite Attribute
Cross-Domain JavaScript Source File Inclusion (5)
Timestamp Disclosure - Unix (37)
Information Disclosure - Suspicious Comments (2)
Modern Web Application (117)
Re-examine Cache-control Directives (2)
Retrieved from Cache (55)
Session Management Response Identified (7)
Absence of Anti-CSRF Tokens
URL: https://www.coinspot.com.au/otc
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form class='form-validate' role='form' action='#' method='POST'>
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting
Other Info:
No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "registerinterestemail"].
Solution:
Phase: Architecture and Design
Alerts 0 6 3 5 Main Proxy: localhost:8080
Current Status

Vulnerabilities.

➢ Cryptographic Failures

Found Issues:

- Content-Encoding: deflate (Nikto) is used on the homepage.
- HTTPS communication that has been compressed may be vulnerable to BREACH attacks.

Risk:

Compressed traffic answers could be used by attackers to deduce session IDs or secret tokens.

How This Needs to Be Reduced:

- For sensitive pages (particularly authorized answers), turn off HTTP compression.
- Add padding to responses and use randomized CSRF tokens.

➢ Security Misconfiguration

Found Issues:

- missing crucial security headers, such as Nikto's X-Content-Type-Options.
- failures of the Content Security Policy (CSP) directive (OWASP ZAP).

Risk:

might permit clickjacking, MIME sniffing, and XSS attacks.

How This Needs to Be Reduced:

- Configure the security headers correctly:

  Options for X-Content-Type: nosniff

  Policy for Content Security

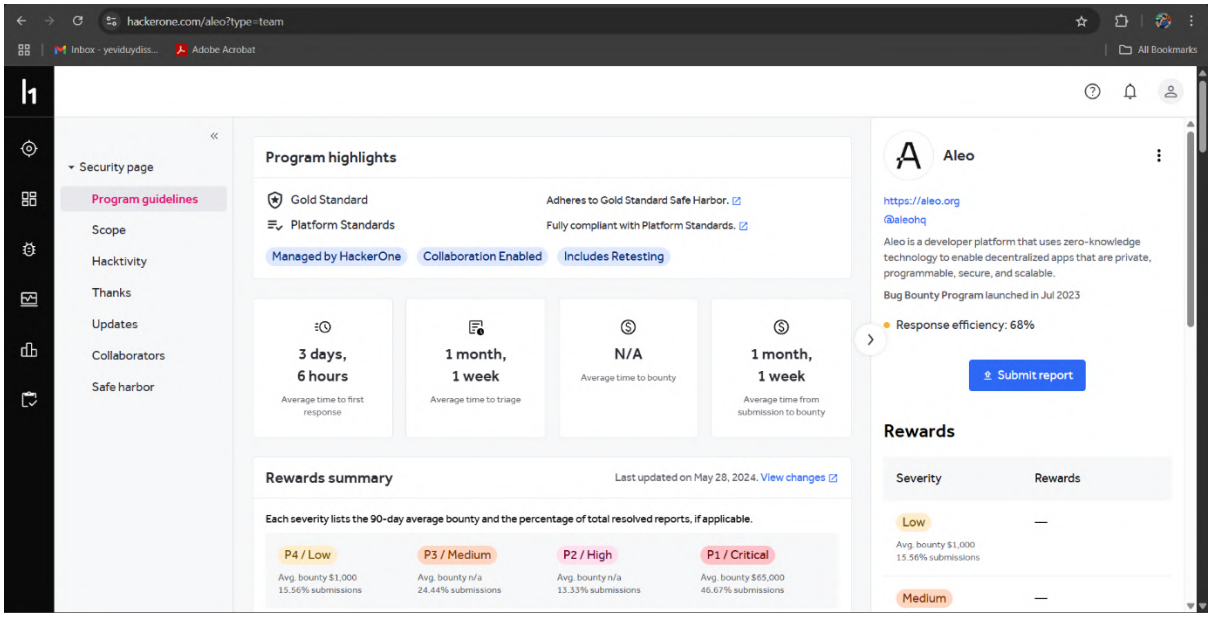
  Transport-Strict Security

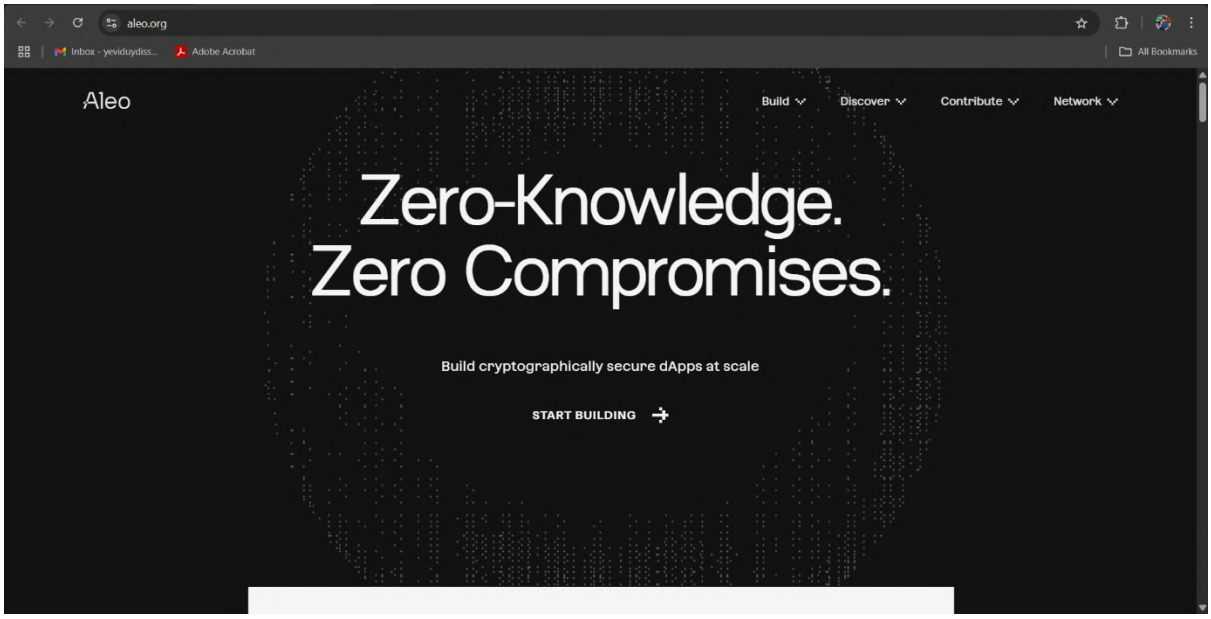
  X-Frame-Options

- Scan and harden server setups on a regular basis.

Report 09.

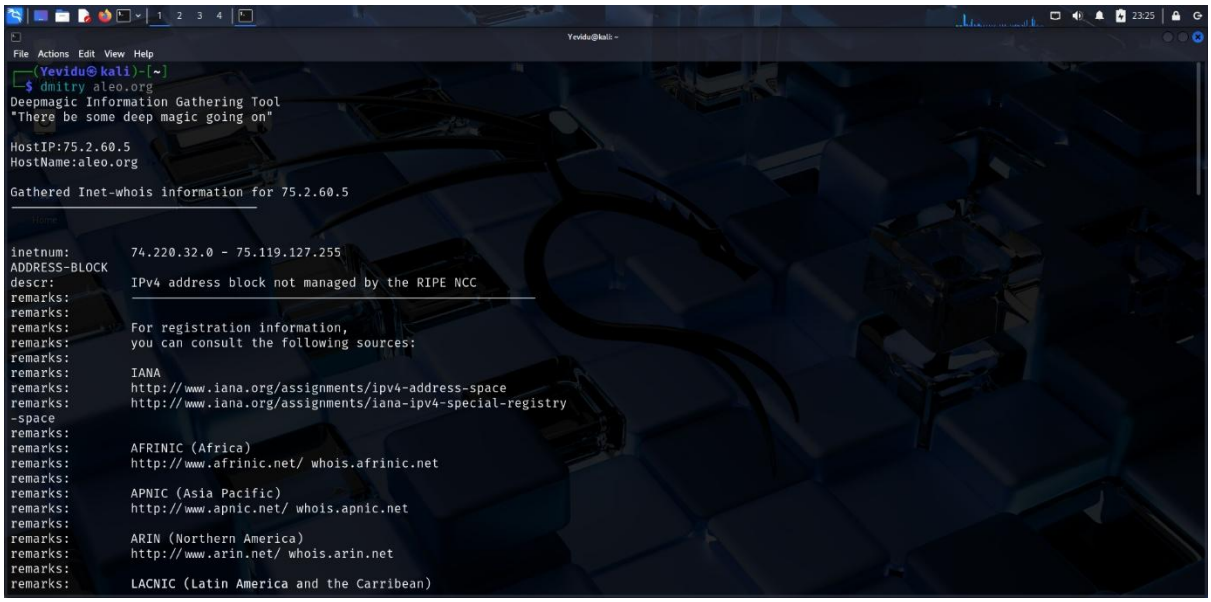
Aleo (https://aleo.org/), a trailblazing platform in the field of decentralized, privacy-preserving applications, is the subject of this Bug Bounty report. Aleo was founded in 2019 and uses zero-knowledge cryptography and blockchain technology to create scalable, completely private smart contracts. Aleo provides a strong platform for building decentralized apps (dApps) where user data is kept private and is designed with developers in mind. Among its features are the Aleo Studio development environment, a secure test net, and a special programming language called Leo. Aleo is influencing the direction of Web3 by prioritizing privacy, scalability, and ease of development. This gives people and companies the means to create private, secure apps without compromising performance or transparency.





Target Reconnaissance.

Dmitry Scan



Host Information

- Host IP: 75.2.60.5
- Host Name: aleo.org

IP Whois Details:

- The IPv4 block 74.220.32.0–75.119.127.255 is not under the direct control of RIPE NCC.
- Country: Although it is internationally allocated, it is listed as EU.
- Internet Assigned Numbers Authority (IANA) is the admin and tech contact.
- Status: UNSPECIFIED ALLOCATED
- RIPE database as a source.

Details of the Domain Whois:

- Name of domain: aleo.org
- Cloudflare, Inc. is the registrar (IANA ID: 1910).
- WHOIS Server for Registrar: whois.cloudflare.com
- Abuse by Registrars Contact information: +1.650.319.8930, registrar-abuse@cloudflare.com
- Date of Domain Creation: September 30, 2009
- Date of Domain Update: October 21, 2024
- Date of Domain Expiration: 2028-09-30
- Aleo Network Foundation is the registrant organization.
- United States (US) (State: Wyoming, WY) is the registrant's country.
- Name servers:

  darl.ns.cloudflare.com

  rosalie.ns.cloudflare.com

- **DNSSEC:** signedDelegation

Whatweb

Details of Servers and Hosting:

Address of IP: 75.2.60.5

United States (US) is the server location.

Netlify is the HTTP server.

Security Headers:

max-age=31536000 (enforces HTTPS for a year) Strict-Transport-Security

Options for the X-Frame: DENY (avoids clickjacking)

Basic XSS protection is enabled with X-XSS-Protection set to 1; mode=block.

Nosniff is an X-Content-Type-Option that stops MIME type sniffing.

(present, adds privacy when navigating away) Referrer-Policy

Technologies Found:

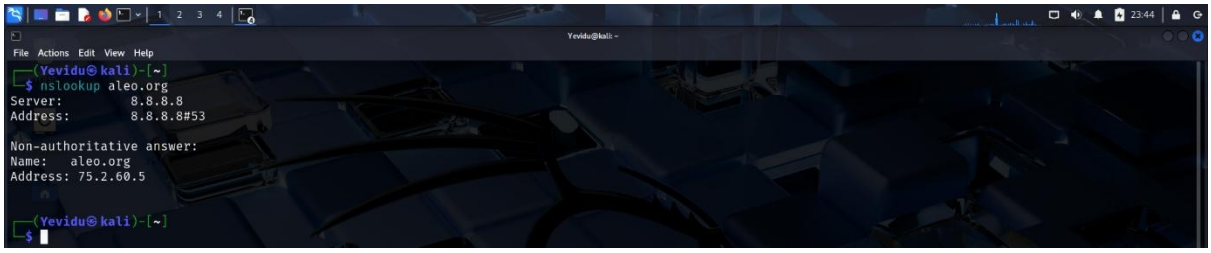
HTML5: HTML5 is used by the website.

Gatsby: Gatsby version 5.13.4 was used to create this static website.

Matomo: An alternative to Google Analytics, this self-hosted web analytics software was found.

The following scripts were found: text/javascript, module, and application/ld+json.

Nslookup



Server: 8.8.8.8

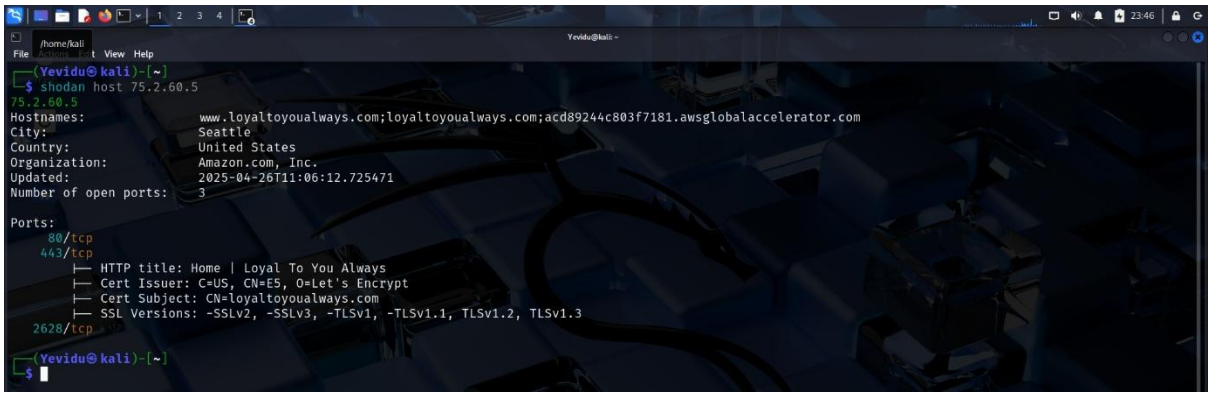
Address: 8.8.8.8#53

Non-authoritative answer:

Name: aleo.org

Address: 75.2.60.5

Shodan



Host Information:

IP address of the host: 75.2.60.5

City: Seattle

Nation: United States

Amazon.com, Inc. is the organization (probably hosted on AWS infrastructure).

Hostnames Associated:

www.loyaltoyoualways.com

loyaltoyoualways.com

acd89244c803f7181.awsglobalaccelerator.com

Ports Open:

80/tcp: HTTP

443/tcp: (HTTPS)

HTTP Title: Home | Always Faithful to You

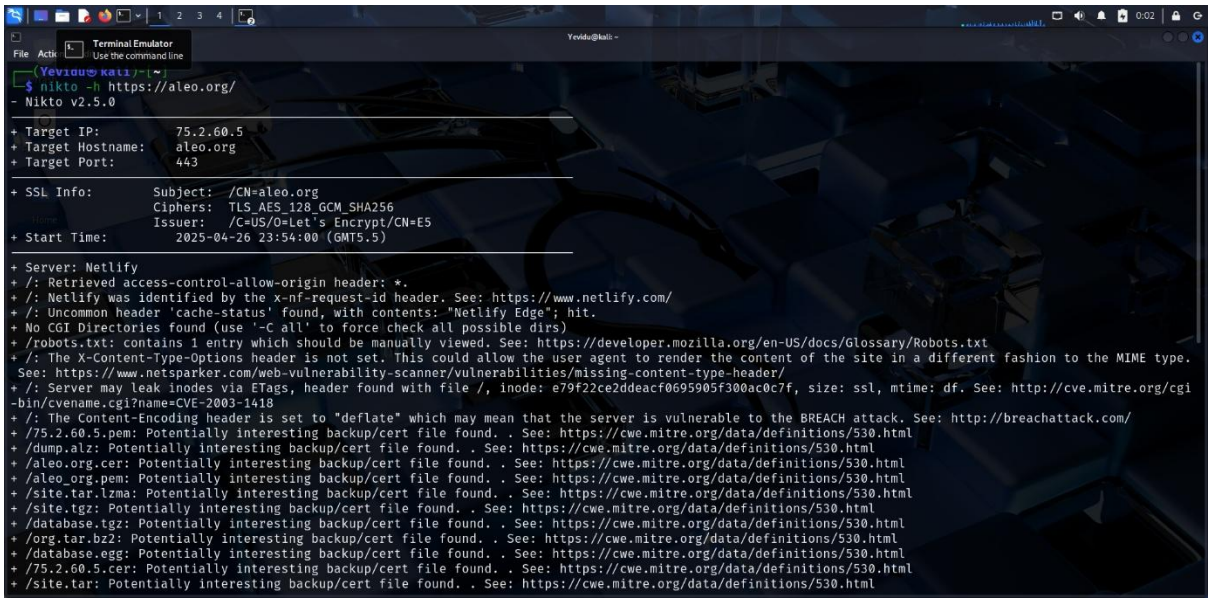
Let's Encrypt is the SSL certificate issuer (CN=E5, O=Let's Encrypt).

Subject of SSL Certificate: CN=loyaltoyoualways.com

TLSv1.2 and TLSv1.3 are supported SSL/TLS versions; previous versions, such as SSLv2, SSLv3, TLSv1, and TLSv1.1, are deactivated for good security.

Scanning and vulnerability identification.

Nikto



Headings:

Access-Control-Allow-Origin: Set to * (if sensitive data is exposed, there may be a CORS misconfiguration).

Cache-status: Netlify Edge; hit is an uncommon header.

Missing X-Content-Type-Options Files may be interpreted differently by the browser than intended (security risk).

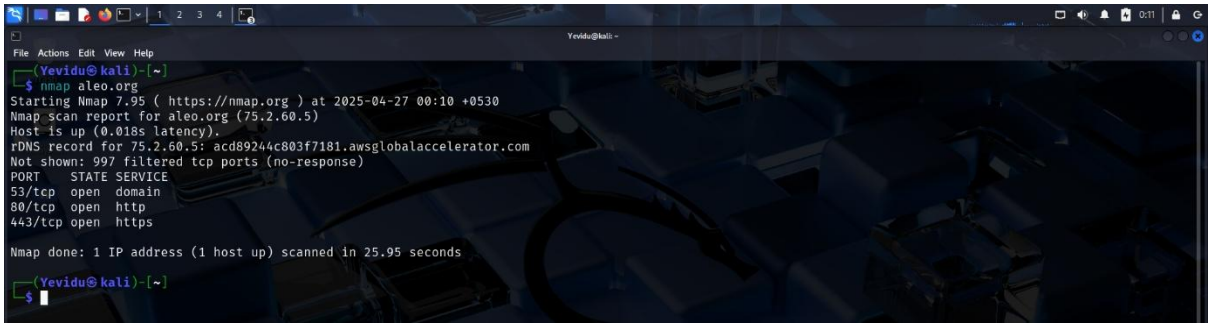
ETag Header: Possible inode leak discovered (associated with CVE-2003-1418).

Possible Vulnerabilities:

Content-Encoding breach: deflate discovered → If HTTPS answers are compressible, they could be susceptible.

CORS Policy: Any origin is permitted by wildcard * → Risk if sensitive data is involved.

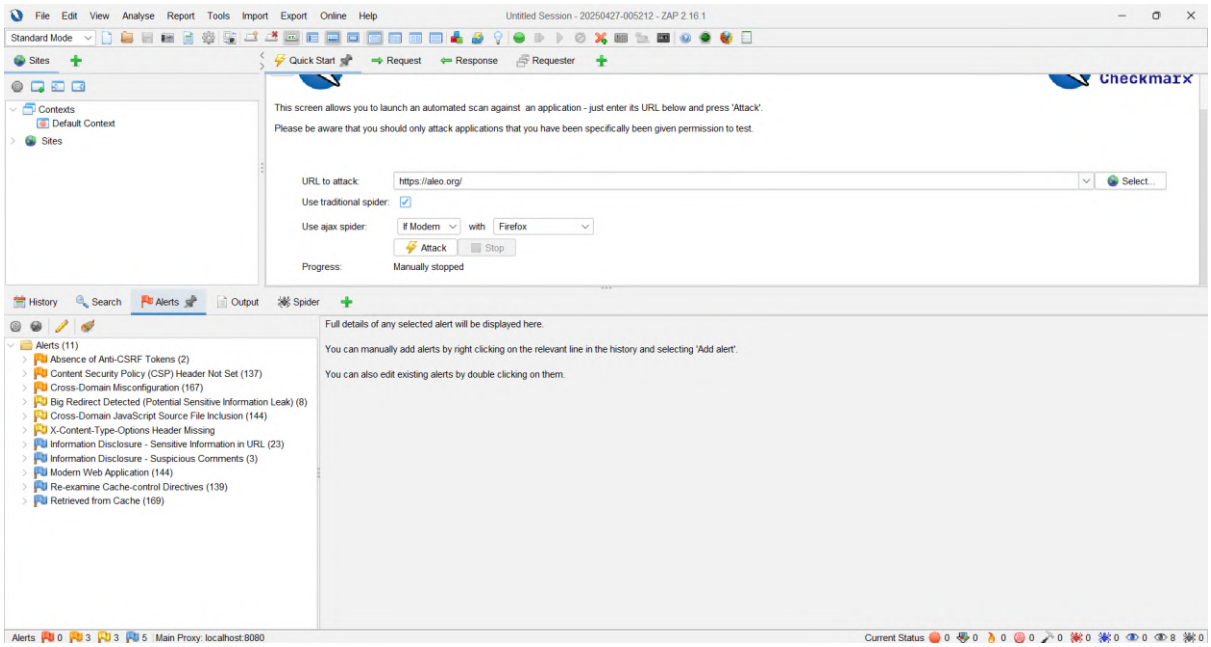
Nmap

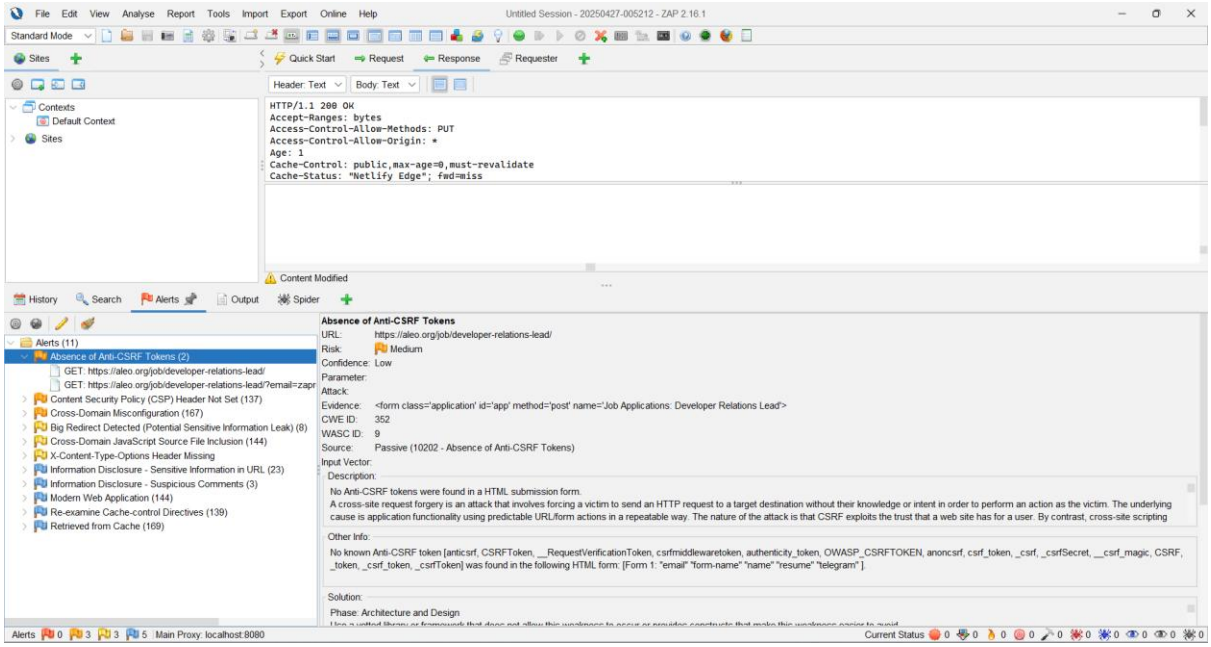


Open Ports

- 53/tcp → Domain Name System (DNS)
- 80/tcp → HTTP (Web traffic)
- 443/tcp → HTTPS (Secure Web traffic)

OWASP ZAP




File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - 20250427-005212 - ZAP 2.16.1
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Methods: PUT
Access-Control-Allow-Origin: *
Age: 1
Cache-Control: public,max-age=0,must-revalidate
Cache-Status: "Netlify Edge"; fwd=miss
Content Modified
History
Search
Alerts
Output
Spider
Alerts (11)
Absence of Anti-CSRF Tokens (2)
GET: https://aleo.org/job/developer-relations-lead/
GET: https://aleo.org/job/developer-relations-lead/?email=zapr
Content Security Policy (CSP) Header Not Set (137)
Cross-Domain Misconfiguration (167)
Big Redirect Detected (Potential Sensitive Information Leak) (8)
Cross-Domain JavaScript Source File Inclusion (144)
X-Content-Type-Options Header Missing
Information Disclosure - Sensitive Information in URL (23)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (144)
Re-examine Cache-control Directives (139)
Retrieved from Cache (169)
Absence of Anti-CSRF Tokens
URL: https://aleo.org/job/developer-relations-lead/
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form class='application' id='app' method='post' name='Job Applications: Developer Relations Lead'>
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting
Other Info:
No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "email" "form-name" "name" "resume" "telegram"].
Solution:
Phase: Architecture and Design
Alerts 0 3 3 5 Main Proxy: localhost:8080
Current Status

Vulnerabilities.

➢ Security Misconfiguration

Missing Security Headers

Found Issues:

- The X-Content-Type-Options header is missing, along with perhaps other headers like X-Frame-Options and Content-Security-Policy.

Risk:

- File interpretation errors by the browser could result in MIME sniffing and XSS attacks.
- increased vulnerability to data theft and clickjacking.

How This Needs to Be Reduced:

- Set important security headers:
  X-Content-Type-Options: nosniff
  X-Frame-Options: DENY
  Content-Security-Policy with strong rules.
  Strict-Transport-Security: max-age=31536000; includeSubDomains.

➢ Cryptographic Failures

Potential BREACH Attack Vulnerability

Found Issues:

- Use of Content-Encoding deflates, leaving it open to attacks based on compression.

Risk:

- Attackers can steal private information from HTTPS traffic by taking advantage of compression side-channels.

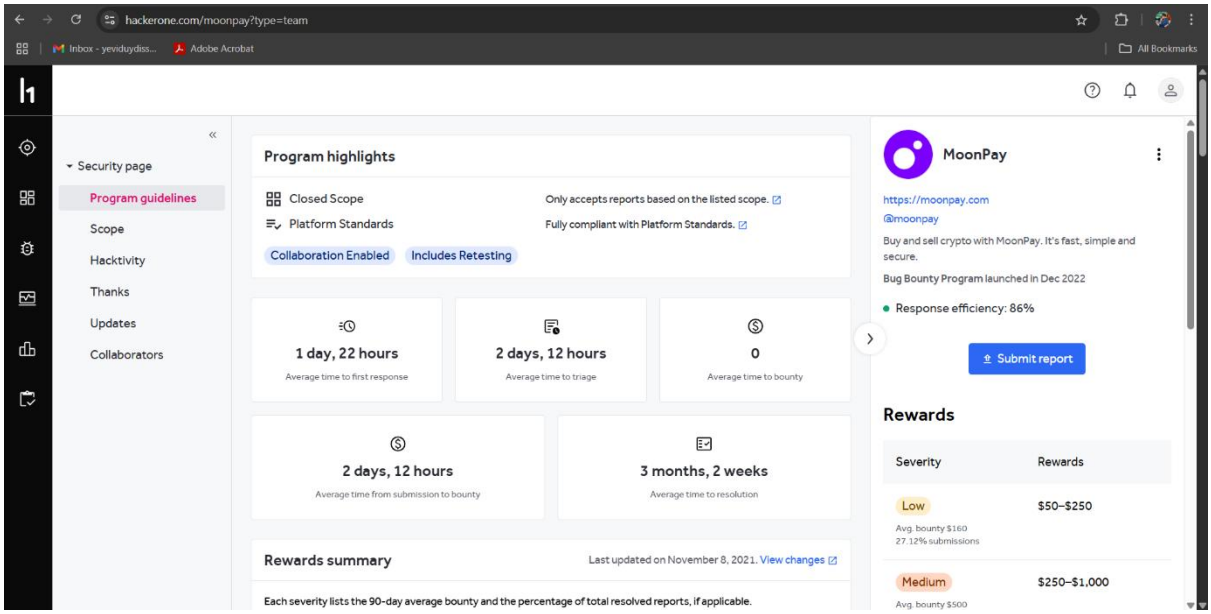
How This Needs to Be Reduced:

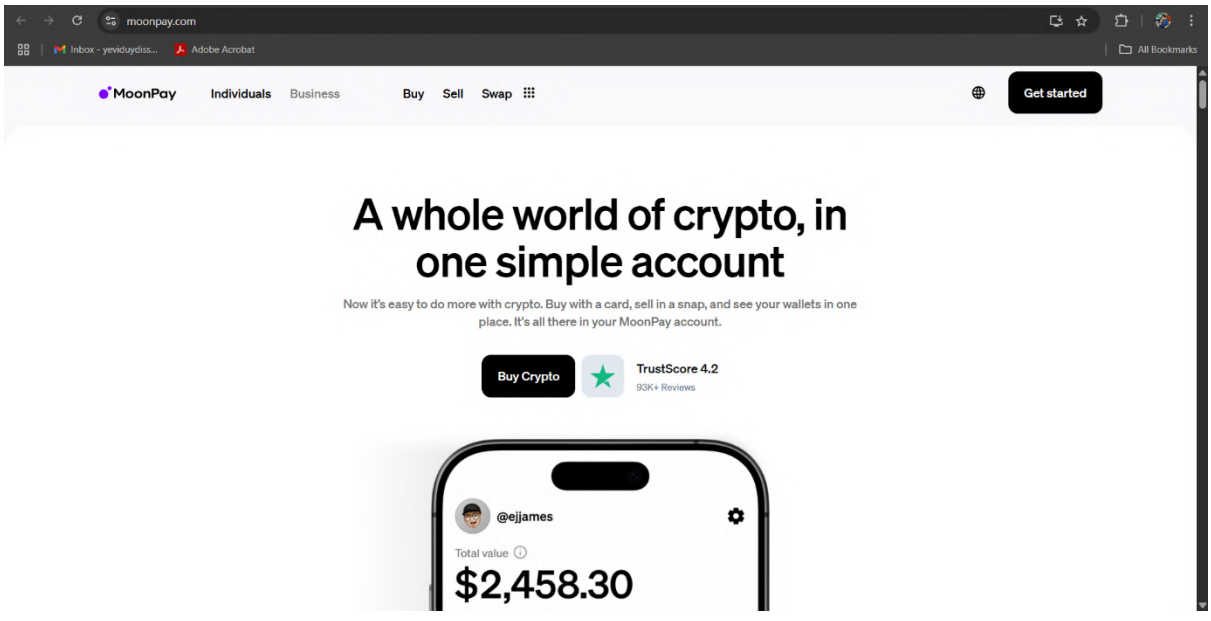
- Turn off HTTP compression (gzip/deflate) for sensitive pages (authenticated sessions, for example).

- Avoid compressing sensitive data and make use of current TLS settings.

Report 10.

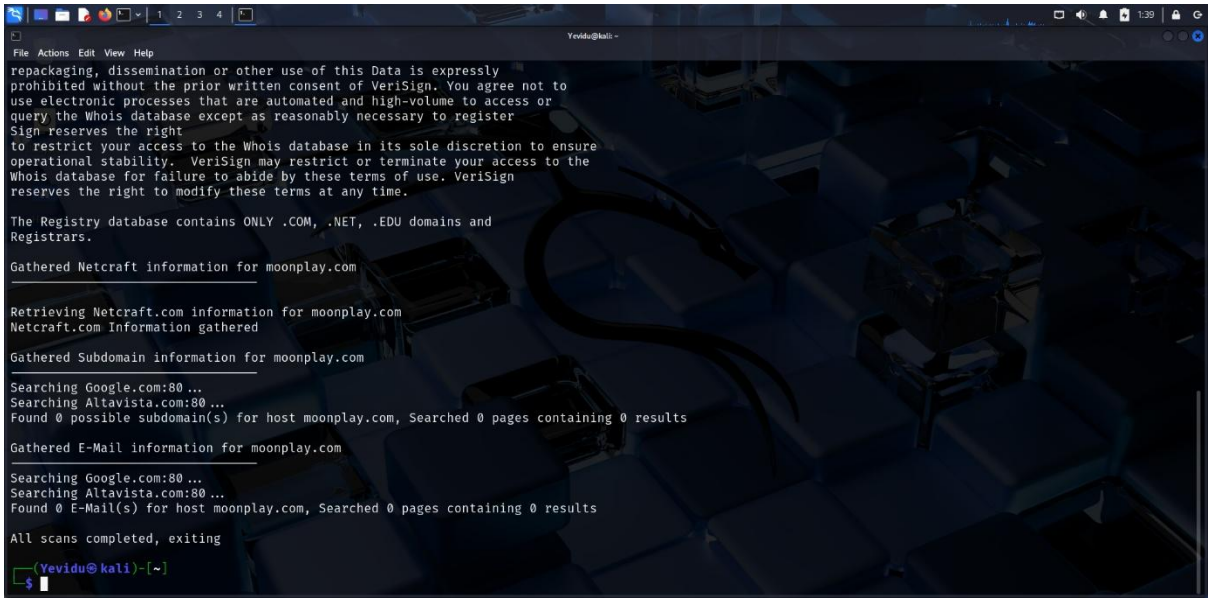
This Bug Bounty report focuses on MoonPay (https://www.moonpay.com/), a prominent platform in the financial technology and cryptocurrency payment space. MoonPay, which was established in 2019, makes it easier for people and businesses to buy and trade cryptocurrencies by offering a user-friendly, secure interface. MoonPay provides services like NFT checkout, on-ramp and off-ramp solutions, and smooth integrations for Web3 apps, in addition to supporting a large variety of digital assets. MoonPay bridges the divide between traditional finance and the decentralized world by designing with user experience and regulatory compliance in mind. MoonPay is influencing the direction of digital transactions and the widespread use of cryptocurrencies by placing a high priority on security, usability, and innovation.





Target Reconnaissance.

Dmitry Scan



WHOIS Domain Information:

Name of domain: moonplay.com

1383748691_DOMAIN_COM is the registry domain ID. -VRSN

Registrar: LLC's GoDaddy

WHOIS Server for Registrar: whois.godaddy.com

Contact information for Registrar Abuse: abuse@godaddy.com | +1 480-624-2505

Date of Creation: January 20, 2008

Current Date of Update: January 21, 2024

Date of Expiration: January 20, 2026

Status of the Domain:

clientRenewProhibited

clientTransferProhibited

clientUpdateProhibited

Name Servers:

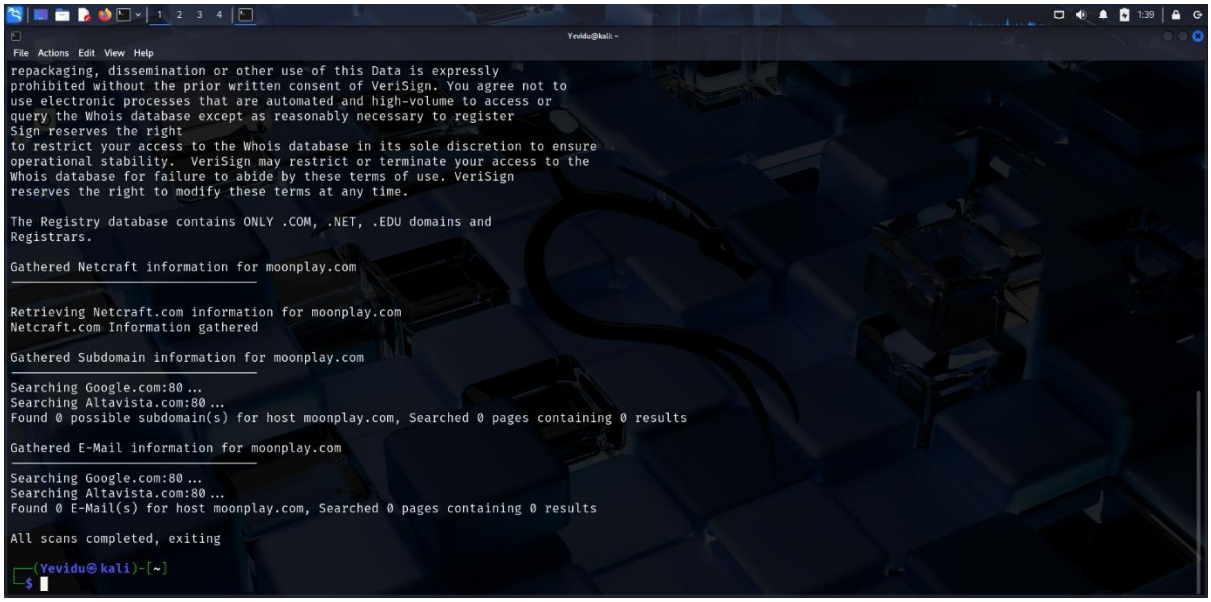
ns1.he.net

ns2.he.net

DNSSEC: Unsigned

Scanning and vulnerability identification.

Nikto



Missing Headers:

Lack of X-Frame options increase the possibility of clickjacking assaults.

Missing X-Content-Type-Options: MIME sniffing attack risk.

Uncommon headers found:

x-vercel-id, x-vercel-cache, content-disposition, x-matched-path, refresh.

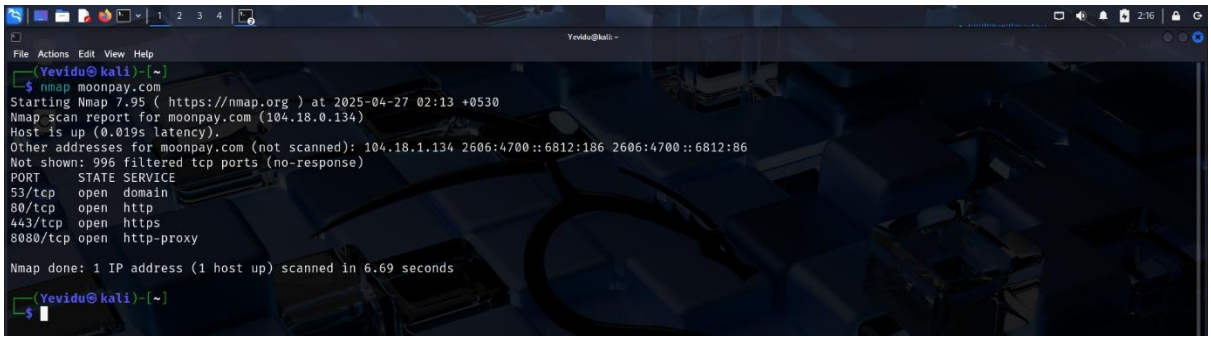
IP addresses exposed in headers and cookies:

located in the report-to, _cfuvid, and __cf_bm headers.

Compression Activated:

Deflate was found in the content-encoding, indicating a possible BREACH attack vulnerability.

Nmap



Services and Ports Open:

- 53/tcp -DNS (Domain):

  shows that a DNS service is being run on the server, which is uncommon for websites that are directly accessible to the public.

- 80/tcp -HTTP:

  standard (unencrypted) web traffic.

- 443/tcp -HTTP:

  Secure web traffic (communication via encryption).

- 8080/tcp- HTTP-Proxy:

  frequently applied to proxies, APIs, and online services. It could be a different administration interface or web application**.**

Vulnerabilities.

➢ Security Misconfiguration

Found Issues:

- X-Frame-Options header missing (risk of clickjacking).
- X-Content-Type-Options header missing (risk of MIME snooping).
- Uncommon headers (such as x-vercel-id and x-powered-by: Next.js) that expose internal operations.
- Open HTTP-proxy port 8080 without doing a thorough investigation.

Risk:

Attackers may sniff MIME types, embed your website in malicious frames, or gain further knowledge about the backend tech stack.

How This Needs to Be Reduced:

Set missing headers:

X-Frame-Options: DENY or SAMEORIGIN

X-Content-Type-Options: nosniff

➢ Cryptographic Failures

Found Issues:

Compression (Content-Encoding: deflate) was found, suggesting a potential breach.

Risk:

If compression and reflection occur, private information (such as session tokens) may be exposed.

How This Needs to Be Reduced:

Turn off HTTP compression in areas where secrets are displayed. Make use of strong CSRF defense.