

**Sri Lanka Institute of Information Technology**  
**Specializing in Cyber Security.**



**IE2062 - Web Security**

**Bug Bounty Assignment**

**IT23238794 – DISSANAYAKE YY**

## Table of Contents

Report 01 .....	4
Target Reconnaissance.....	5
Scanning and vulnerability identification. ....	10
Vulnerabilities. ....	14
Report 02 .....	15
Target Reconnaissance.....	16
Scanning and vulnerability identification. ....	23
Vulnerabilities. ....	26
Report 03.....	28
Target Reconnaissance. ....	29
Scanning and vulnerability identification. ....	34
Vulnerabilities. ....	41
Report 04.....	42
Target Reconnaissance. ....	43
Scanning and vulnerability identification. ....	46
Vulnerabilities. ....	50
Report 05.....	50
Target Reconnaissance. ....	53
Scanning and vulnerability identification. ....	58
Vulnerabilities. ....	64
Report 06.....	65
Target Reconnaissance. ....	67
Scanning and vulnerability identification. ....	73
Vulnerabilities. ....	76
Report 07.....	78
Target Reconnaissance. ....	79
Scanning and vulnerability identification. ....	83
Vulnerabilities. ....	86
Report 08.....	87
Target Reconnaissance. ....	88
Scanning and vulnerability identification. ....	93
Vulnerabilities. ....	96
Report 09.....	98
Target Reconnaissance. ....	99
Scanning and vulnerability identification. ....	104

Vulnerabilities .....	107
Report 10.....	109
Target Reconnaissance.....	110
Scanning and vulnerability identification. ....	112
Vulnerabilities. ....	115

# 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.

The screenshot shows the HackerOne interface for the Booking.com bug bounty program. It includes sections for Program highlights, Rewards summary, and Rewards. Key data points shown include:

- Program highlights:** Fully compliant with Platform Standards, Managed by HackerOne, Collaboration Enabled, Includes Retesting.
- Rewards summary:** Last updated on November 2, 2022. Shows average bounty per severity: Low (\$150) and Medium (\$500).
- Rewards:** Severity (Low/Medium) vs. Rewards (\$150/\$500).

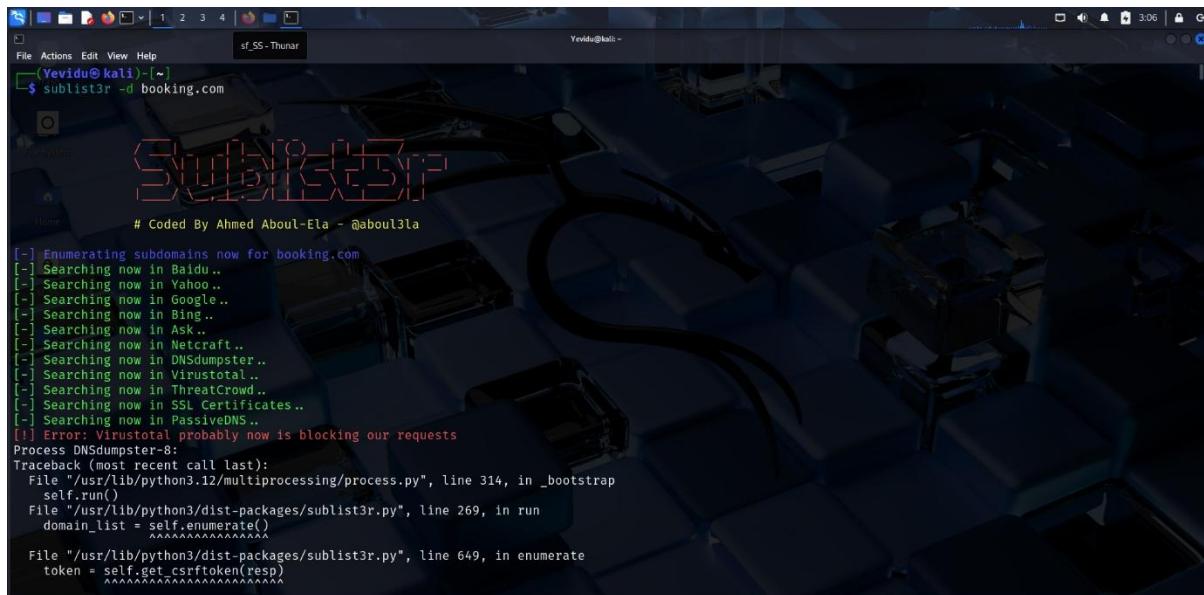
The screenshot shows the Booking.com homepage. Key features include:

- Header:** Booking.com logo, LKR, USA flag, List your property, Register, Sign in.
- Search Bar:** Where are you going? (highlighted with a yellow border), Check-in date — Check-out date, 2 adults · 0 children · 1 room, Search button.
- Offers:** Promotions, deals, and special offers for you. One offer highlighted: "Quick escape, quality time" (Save up to 20% with a Getaway Deal, Save on stays).

# Target Reconnaissance.

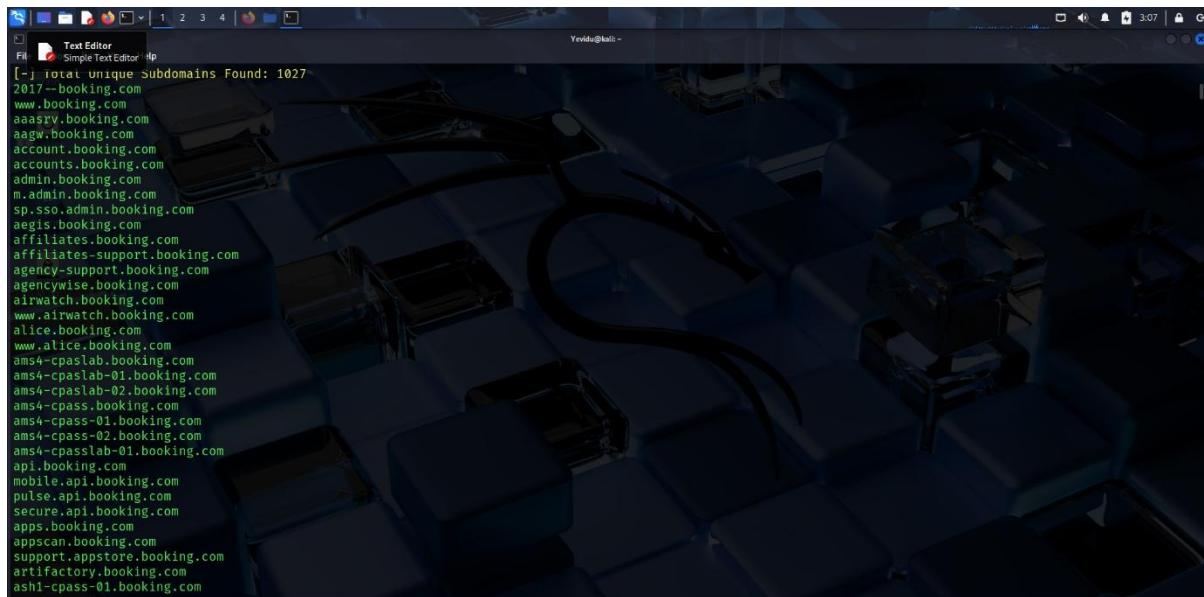
## Sublist3r

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



```
(Yevidu㉿kali)-[~] $ sublist3r -d booking.com
# Coded By Ahmed Aboul-Ela - @aboul3la

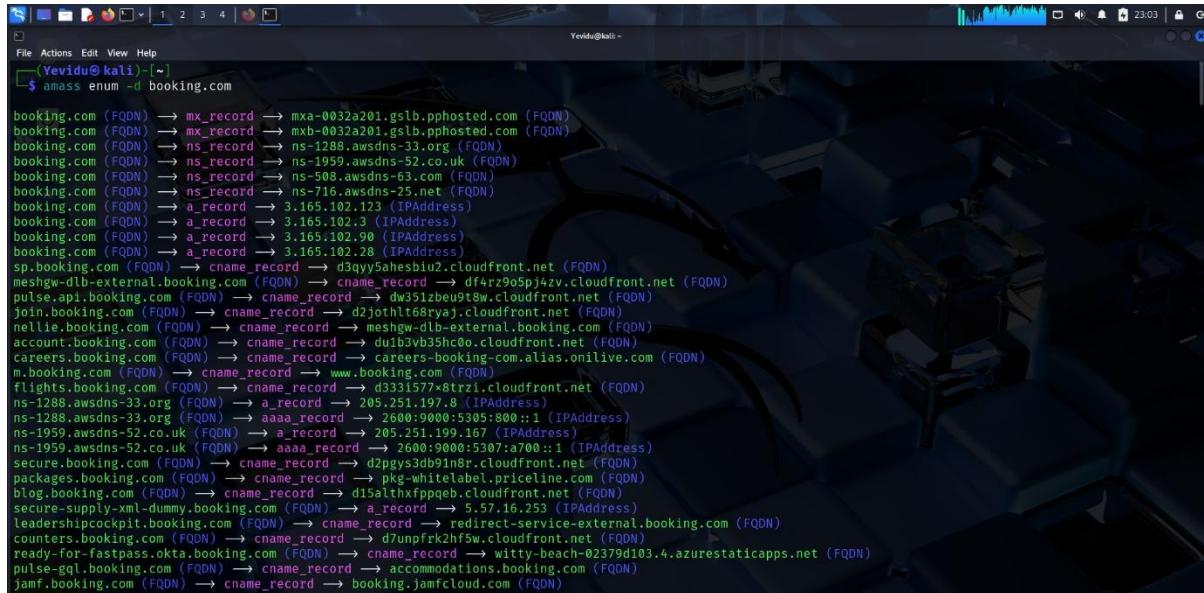
[-] Enumerating subdomains now for booking.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.12/multiprocessing/process.py", line 314, in _bootstrap
    self.run()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
                  ^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
    token = self.get_csrfToken(resp)
            ^^^^^^^^^^
```



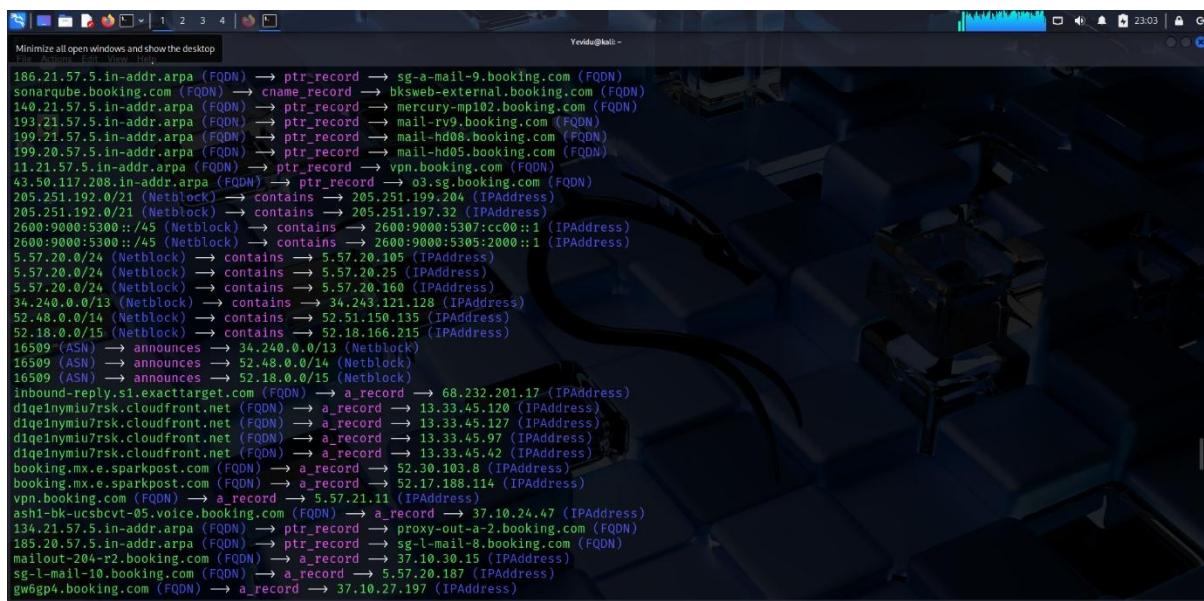
```
[+] Total Unique Subdomains Found: 1027
2017-booking.com
www.booking.com
aaa$rv.booking.com
aagw.booking.com
account.booking.com
accounts.booking.com
admin.booking.com
m.admin.booking.com
sp.sso.admin.booking.com
aegis.booking.com
affiliates.booking.com
affiliates-support.booking.com
agency-support.booking.com
agencywise.booking.com
airwatch.booking.com
www.airwatch.booking.com
alice.booking.com
www.alice.booking.com
ams4-cpaslab.booking.com
ams4-cpaslab-01.booking.com
ams4-cpaslab-02.booking.com
ams4-cpass.booking.com
ams4-cpass-01.booking.com
ams4-cpass-02.booking.com
ams4-cpasslab-01.booking.com
api.booking.com
mobile.api.booking.com
pulse.api.booking.com
secure.api.booking.com
apps.booking.com
appscan.booking.com
support.appstore.booking.com
artifactory.booking.com
ashl-cpass-01.booking.com
```

## 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.



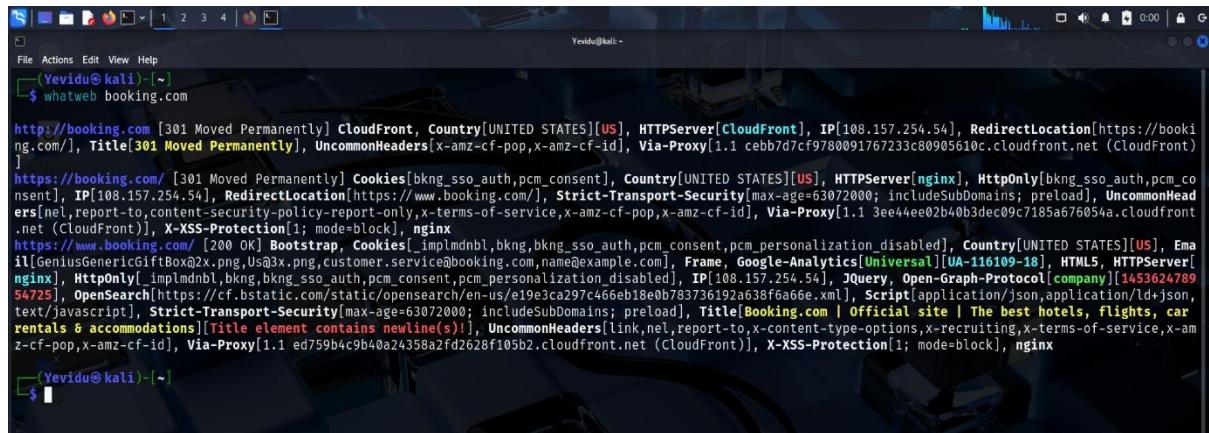
```
Yevidu@kali:~$ amass enum -d booking.com
booking.com (FQDN) --> mx_record --> mx-0032a201.gslb.phhosted.com (FQDN)
booking.com (FQDN) --> mx_record --> mxb-0032a201.gslb.phhosted.com (FQDN)
booking.com (FQDN) --> ns_record --> ns-1288.awsdns-33.org (FQDN)
booking.com (FQDN) --> ns_record --> ns-1959.awsdns-52.co.uk (FQDN)
booking.com (FQDN) --> ns_record --> ns-508.awsdns-63.com (FQDN)
booking.com (FQDN) --> ns_record --> ns-716.awsdns-25.net (FQDN)
booking.com (FQDN) --> a_record --> 3.165.102.123 (IPAddress)
booking.com (FQDN) --> a_record --> 3.165.102.3 (IPAddress)
booking.com (FQDN) --> a_record --> 3.165.102.90 (IPAddress)
booking.com (FQDN) --> a_record --> 3.165.102.28 (IPAddress)
sp.booking.com (FQDN) --> cname_record --> d3qyy5ahesbiu2.cloudfront.net (FQDN)
meshgw-dlb-external.booking.com (FQDN) --> cname_record --> dfarz905pj4zv.cloudfront.net (FQDN)
pulse.api.booking.com (FQDN) --> cname_record --> dw35lzebe9t8w.cloudfront.net (FQDN)
join.booking.com (FQDN) --> cname_record --> d2j0thlt68ryej.cloudfront.net (FQDN)
nelli.booking.com (FQDN) --> cname_record --> meshgw-dlb-external.booking.com (FQDN)
account.booking.com (FQDN) --> cname_record --> du1b3vb35hc0o.cloudfront.net (FQDN)
careers.booking.com (FQDN) --> cname_record --> careers-booking-com.alias.onlive.com (FQDN)
m.booking.com (FQDN) --> cname_record --> www.booking.com (FQDN)
flights.booking.com (FQDN) --> cname_record --> d333157x8trzi.cloudfront.net (FQDN)
ns-1288.awsdns-33.org (FQDN) --> a_record --> 205.251.197.8 (IPAddress)
ns-1959.awsdns-52.co.uk (FQDN) --> aaaa_record --> 2600:9000:5305::800::1 (IPAddress)
ns-1959.awsdns-52.co.uk (FQDN) --> aaaa_record --> 2600:9000:5307:a700::1 (IPAddress)
secure.booking.com (FQDN) --> cname_record --> d2pgys3db91n8r.cloudfront.net (FQDN)
packages.booking.com (FQDN) --> cname_record --> pkg-whiteLabel.priceline.com (FQDN)
blog.booking.com (FQDN) --> cname_record --> d15alhxfpqeb.cloudfront.net (FQDN)
secure-supply-xml-dummy.booking.com (FQDN) --> a_record --> 5.57.16.253 (IPAddress)
leadershipcockpit.booking.com (FQDN) --> cname_record --> redirect-service-external.booking.com (FQDN)
counters.booking.com (FQDN) --> cname_record --> d7unopfrk2hf5w.cloudfront.net (FQDN)
ready-for-fastpass.okta.booking.com (FQDN) --> cname_record --> witty-beach-02379d103.4.azurestaticapps.net (FQDN)
pulse-gql.booking.com (FQDN) --> cname_record --> accommodations.booking.com (FQDN)
jamf.booking.com (FQDN) --> cname_record --> booking.JamfCloud.com (FQDN)
```



```
Yevidu@kali:~$ amass enum -d booking.com
186.21.57.5.in-addr.arpa (FQDN) --> ptr_record --> sg-a-mail-9.booking.com (FQDN)
sonarqube.booking.com (FQDN) --> cname_record --> bksweb-external.booking.com (FQDN)
140.21.57.5.in-addr.arpa (FQDN) --> ptr_record --> mercury-mp102.booking.com (FQDN)
193.21.57.5.in-addr.arpa (FQDN) --> ptr_record --> mail-rv9.booking.com (FQDN)
199.21.57.5.in-addr.arpa (FQDN) --> ptr_record --> mail-hd08.booking.com (FQDN)
199.20.57.5.in-addr.arpa (FQDN) --> ptr_record --> mail-hd05.booking.com (FQDN)
11.21.57.5.in-addr.arpa (FQDN) --> ptr_record --> vpn.booking.com (FQDN)
43.50.117.208.in-addr.arpa (FQDN) --> ptr_record --> o3.sg.booking.com (FQDN)
205.251.192.0/21 (Netblock) --> contains --> 205.251.199.204 (IPAddress)
205.251.192.0/21 (Netblock) --> contains --> 205.251.197.32 (IPAddress)
2600:9000:5300::/45 (Netblock) --> contains --> 2600:9000:5307:cc00::1 (IPAddress)
2600:9000:5300::/45 (Netblock) --> contains --> 2600:9000:5305:2000::1 (IPAddress)
5.57.20.0/24 (Netblock) --> contains --> 5.57.20.105 (IPAddress)
5.57.20.0/24 (Netblock) --> contains --> 5.57.20.25 (IPAddress)
5.57.20.0/24 (Netblock) --> contains --> 5.57.20.160 (IPAddress)
34.240.0.0/13 (Netblock) --> contains --> 34.243.121.128 (IPAddress)
52.48.0.0/14 (Netblock) --> contains --> 52.51.150.135 (IPAddress)
52.18.0.0/15 (Netblock) --> contains --> 52.18.166.215 (IPAddress)
16509 (ASN) --> announces --> 34.240.0.0/13 (Netblock)
16509 (ASN) --> announces --> 52.48.0.0/14 (Netblock)
16509 (ASN) --> announces --> 52.18.0.0/15 (Netblock)
inbound-reply.s1.exacttarget.com (FQDN) --> a_record --> 68.232.201.17 (IPAddress)
diquenymiu7rsk.cloudfront.net (FQDN) --> a_record --> 13.33.45.120 (IPAddress)
diquenymiu7rsk.cloudfront.net (FQDN) --> a_record --> 13.33.45.127 (IPAddress)
diquenymiu7rsk.cloudfront.net (FQDN) --> a_record --> 13.33.45.97 (IPAddress)
diquenymiu7rsk.cloudfront.net (FQDN) --> a_record --> 13.33.45.42 (IPAddress)
booking.mx.e.sparkpost.com (FQDN) --> a_record --> 52.30.103.8 (IPAddress)
booking.mx.e.sparkpost.com (FQDN) --> a_record --> 52.17.188.114 (IPAddress)
vpn.booking.com (FQDN) --> a_record --> 5.57.21.11 (IPAddress)
ash1-bk-ucsbcvt-95.voice.booking.com (FQDN) --> a_record --> 37.10.24.47 (IPAddress)
134.21.57.5.in-addr.arpa (FQDN) --> ptr_record --> proxy-out-a-2.booking.com (FQDN)
185.20.57.5.in-addr.arpa (FQDN) --> ptr_record --> sg-l-mail-8.booking.com (FQDN)
mailout-204-r2.booking.com (FQDN) --> a_record --> 37.10.30.15 (IPAddress)
SG-l-mail-10.booking.com (FQDN) --> a_record --> 5.57.20.187 (IPAddress)
gw6gp4.booking.com (FQDN) --> a_record --> 37.10.27.197 (IPAddress)
```

## 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.



```
Yevidu@kali:~$ whatweb booking.com
http://booking.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[108.157.254.54], RedirectLocation[https://booki
ng.com/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 cebb7d7cf9780091767233c80905610c.cloudfront.net (CloudFront)
]
https://booking.com/ [301 Moved Permanently] Cookies[bkng_sso_auth,pcm_consent], Country[UNITED STATES][US], HTTPServer[nginx], HttpOnly[bkng_sso_auth,pcm_co
nsent], IP[108.157.254.54], RedirectLocation[https://www.booking.com/], Strict-Transport-Security[max-age=63072000; includeSubDomains; preload], UncommonHead
ers[nel,report-to,content-security-policy-report-only,x-terms-of-service,x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 3ee44ee02b40b3dec09c7185a676054a.cloudfront
.net (CloudFront)], X-XSS-Protection[1; mode=block], nginx
https://www.booking.com/ [200 OK] Bootstrap, Cookies[_implrndbl,bkng,bkng_sso_auth,pcm_consent,pcm_personalization_disabled], Country[UNITED STATES][US], Ema
il[GeniusGenericGiftBox@2x.png,Us@3x.png,customer.service@booking.com,name@example.com], Frame, Google-Analytics[Universal][UA-116109-18], HTML5, HTTPServer[
nginx], HttpOnly[_implrndbl,bkng,bkng_sso_auth,pcm_consent,pcm_personalization_disabled], IP[108.157.254.54], JQuery, Open-Graph-Protocol[company][1453624789
54725], OpenSearch[https://cf.bstatic.com/static/opensearch/en-us/e19e3ca297c466eb18e0b783736192a38f6a66e.xml], Script[application/json,application/ld+json,
text/javascript], Strict-Transport-Security[max-age=63072000; includeSubDomains; preload], Title[Booking.com | Official site | The best hotels, flights, car
rentals & accommodations][Title element contains newline(s)!], UncommonHeaders[link,nel,report-to,x-content-type-options,x-recruiting,x-terms-of-service,x-am
z-cf-pop,x-amz-cf-id], Via-Proxy[1.1 ed759b4c9b40a24358a2fd2628f105b2.cloudfront.net (CloudFront)], X-XSS-Protection[1; mode=block], nginx
Yevidu@kali:~$
```

## 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.



```
Yevide@kali:~$ nslookup booking.com
Server: 192.168.43.2
Address: 192.168.43.1#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

Yevide@kali:~$
```

Server: 192.168.43.2

Address: 192.168.43.1#53

Non-authoritative answer:

Name: booking.com

Address: 100.157.254.54

Name: booking.com

Address: 100.157.254.89

Name: booking.com

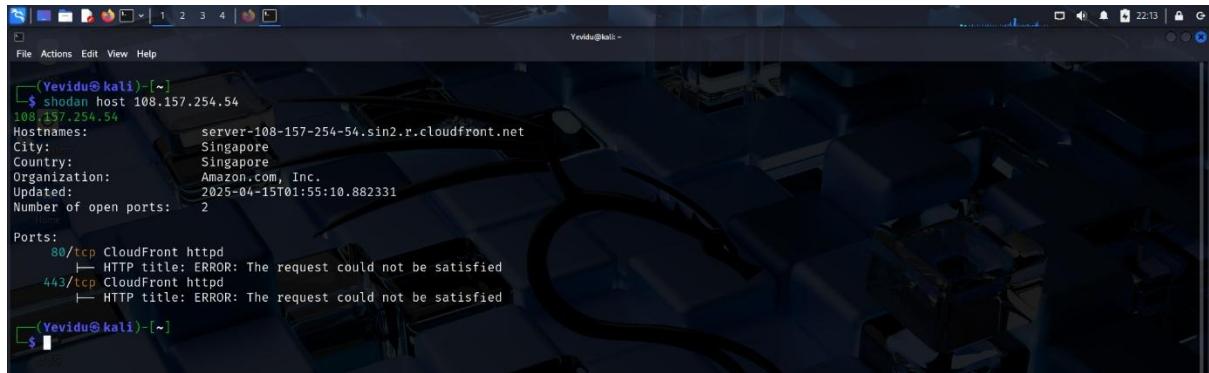
Address: 100.157.254.31

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.



The screenshot shows a terminal window on a Kali Linux system. The user has run the command `$ shodan host 108.157.254.54`. The output provides detailed information about the host:

```
(Yevidu@kali)-[~]
$ shodan host 108.157.254.54
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
```

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

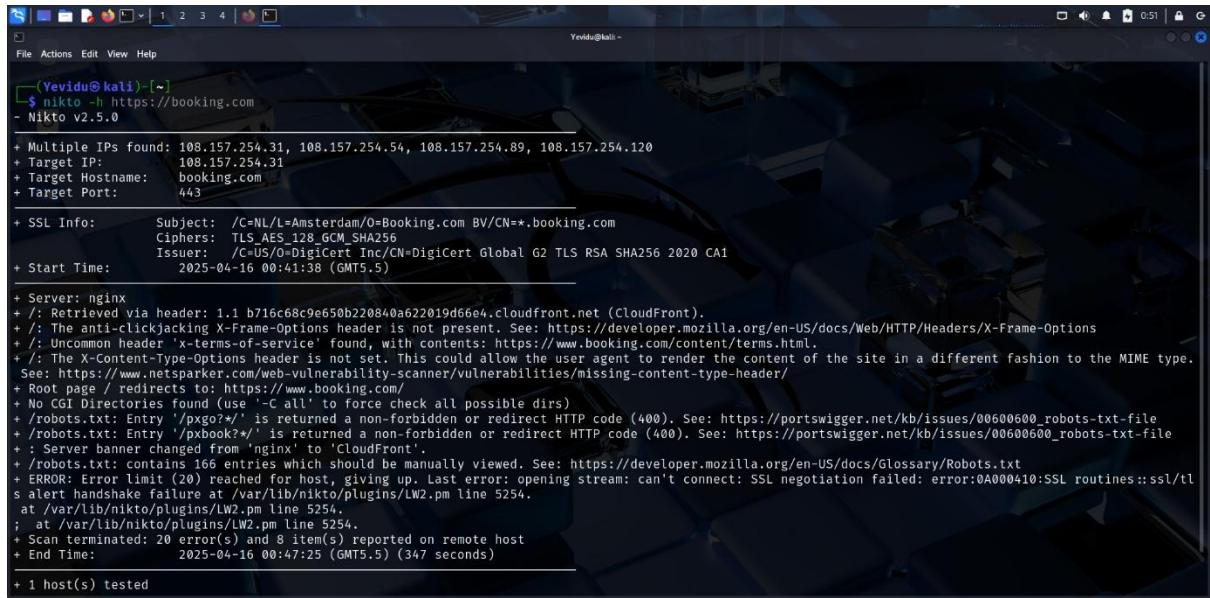
443/tcp CloudFront httpd

  └─ 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.



```
Yevidu@kali: ~
$ nikto -h https://booking.com
- Nikto v2.5.0

+ Multiple IPs found: 108.157.254.31, 108.157.254.54, 108.157.254.89, 108.157.254.120
+ Target IP: 108.157.254.31
+ Target Hostname: booking.com
+ Target Port: 443

+ SSL Info: Subject: /C=NL/L=Amsterdam/O=Booking.com BV/CN=*.booking.com
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1

+ Start Time: 2025-04-16 00:41:38 (GMT5.5)

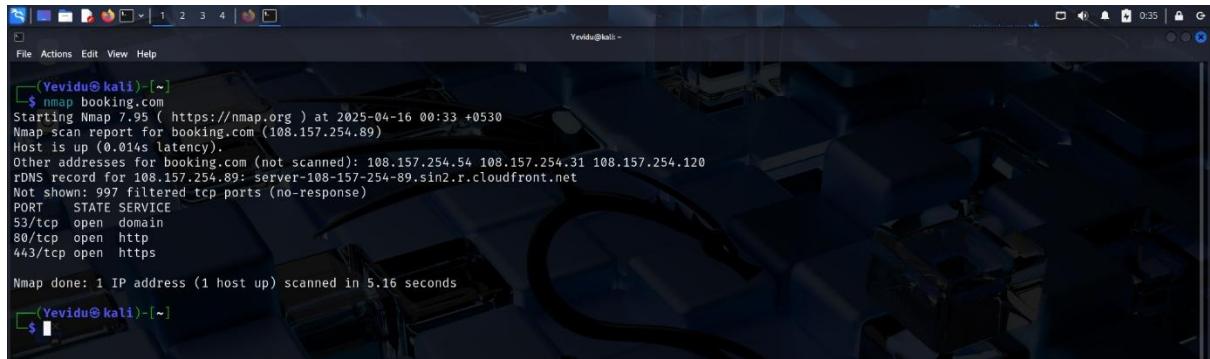
+ Server: nginx
+ /: Retrieved via header: 1.1 b716c68c9e650b220840a622019d66e4.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-terms-of-service' found, with contents: https://www.booking.com/content/terms.html.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.booking.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/pxgo?*' is returned a non-forbidden or redirect HTTP code (400). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /roots.txt: Entry '/pxbook?*' is returned a non-forbidden or redirect HTTP code (400). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ : Server banner changed from 'nginx' to 'CloudFront'.
+ /robots.txt: contains 166 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/tl
s alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 8 item(s) reported on remote host
+ End Time: 2025-04-16 00:47:25 (GMT5.5) (347 seconds)

+ 1 host(s) tested
```

- 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.



```
Yevidu@kali:~$ nmap booking.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-16 00:33 +0530
Nmap scan report for booking.com (108.157.254.89)
Host is up (0.014s latency).
Other addresses for booking.com (not scanned): 108.157.254.54 108.157.254.31 108.157.254.120
DNS record for 108.157.254.89: server-108-157-254-89.s1n2.r.cloudfront.net
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

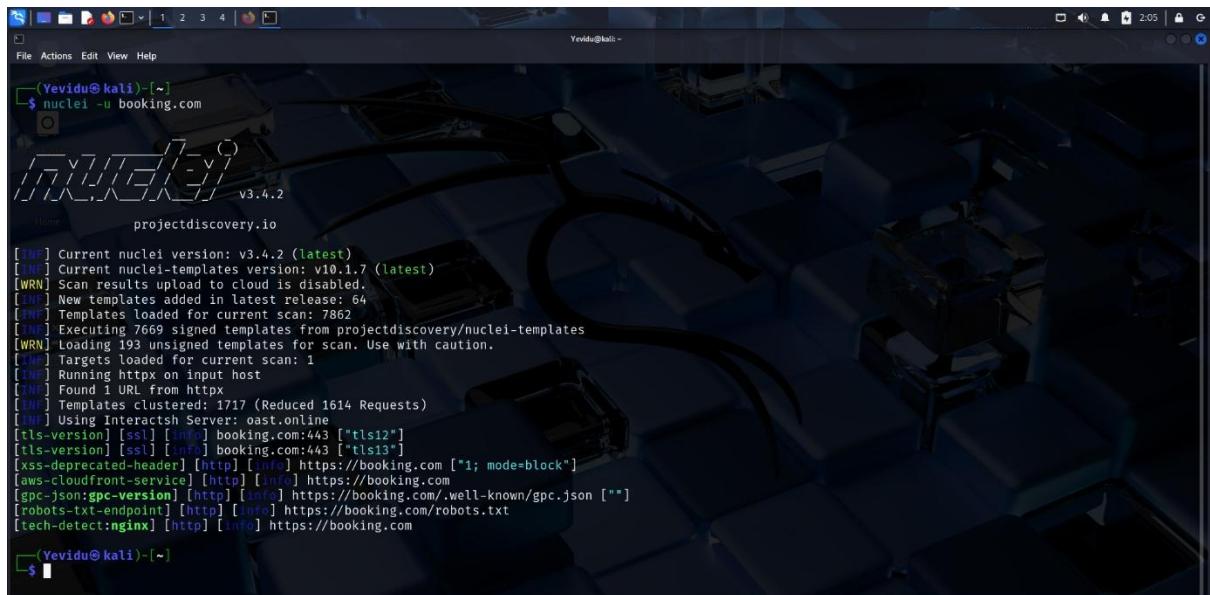
Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds
Yevidu@kali:~$
```

- 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.



```
Yevidu@kali:~$ nuclei -u booking.com
v3.4.2
projectdiscovery.io

[INI] Current nuclei version: v3.4.2 (latest)
[INI] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[... ] New templates added in latest release: 64
[... ] Templates loaded for current scan: 7862
[... ] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[... ] Targets loaded for current scan: 1
[... ] Running httpx on input host
[... ] Found 1 URL from httpx
[... ] Templates clustered: 1717 (Reduced 1614 Requests)
[... ] Using Interactsh Server: oast.online
[tls-version] [ssl] [info] booking.com:443 ["tls12"]
[tls-version] [ssl] [info] booking.com:443 ["tls13"]
[xss-deprecated-header] [http] [info] https://booking.com [*; mode=block*]
[aws-cloudfront-service] [http] [info] https://booking.com
[gpc-json:gpc-version] [http] [info] https://booking.com/.well-known/gpc.json [*]
[robots-txt-endpoint] [http] [info] https://booking.com/robots.txt
[tech-detect:nginx] [http] [info] https://booking.com

Yevidu@kali:~$
```

- 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.

The screenshot shows the OWASP ZAP 2.16.1 interface. The main window displays a scan for 'HTTP to HTTPS Insecure Transition in Form Post' on the URL <http://www.booking.com>. The alert details pane shows the following information:

- Attack:** Evidence: <https://www.booking.com/searchresults.html>; CWE ID: 319; WASC ID: 15; Source: Passive (10041 - HTTP to HTTPS Insecure Transition in Form Post)
- Description:** This check looks for insecure HTTP pages that host HTTPS forms. The issue is that an insecure HTTP page can easily be hijacked through MITM and the secure HTTPS form can be replaced or spoofed.
- Solution:** Use HTTPS for landing pages that host secure forms.

The bottom right corner of the alert details pane shows a modal dialog titled 'Edit Alert' for the 'Content Modified' alert. The dialog contains fields for 'Key' (OWASP\_2021\_A02) and 'Value' ([https://owasp.org/Top10/A02\\_2021-Cryptographic\\_Failures/](https://owasp.org/Top10/A02_2021-Cryptographic_Failures/)). Buttons for 'Cancel' and 'Save' are visible.

### **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.

The top screenshot displays the HackerOne security page for Shopify. Key highlights include:

- Program highlights:**
  - Gold Standard: Adheres to Gold Standard Safe Harbor.
  - Platform Standards: Fully compliant with Platform Standards.
  - Top Response Efficiency: This program's response efficiency is above 90%.
- Response times:**
  - Average time to first response: 15 hours
  - Average time to triage: 4 days
  - Average time to bounty: 4 days, 5 hours
  - Average time from submission to bounty: 1 week, 1 day
  - Average time to resolution: 3 weeks, 4 days
- Rewards:**

Severity	Rewards
Low	\$500-\$1,000
Medium	\$1,000-\$10,000

The bottom screenshot shows the main Shopify homepage with a large banner featuring a man wearing glasses and a hoodie with the text "RUNAWAY". The banner text reads: "Be the next one to watch" and "Dream big, build fast, and grow far on Shopify." Buttons for "Start free trial" and "Why we build Shopify" are visible.

# Target Reconnaissance.

## Sublist3r

```
File Actions Edit View Help
upcoming11.shopify.com
upcoming12.shopify.com
upcoming13.shopify.com
upcoming14.shopify.com
upcoming15.shopify.com
upcoming16.shopify.com
upcoming17.shopify.com
upcoming18.shopify.com
upcoming19.shopify.com
upcoming2.shopify.com
upcoming20.shopify.com
upcoming3.shopify.com
upcoming4.shopify.com
upcoming5.shopify.com
upcoming6.shopify.com
upcoming7.shopify.com
upcoming8.shopify.com
upcoming9.shopify.com
ux.shopify.com
www.ux.shopify.com
v.shopify.com
v-ca.shopify.com
vault.shopify.com
vision.shopify.com
weareopen.shopify.com
webdav.shopify.com
webinar-sept-30.shopify.com
wholesale.shopify.com
wiki.shopify.com
win.shopify.com
windsor.shopify.com
ww.shopify.com

(Yevidu@ kali) - [~]
```

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

```
(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 → dmärcreject.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)
```

```
(Yevidu㉿kali)-[~]
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:f0fe:: (IPAddress)
o22.mailer.shopify.com (FQDN) → a_record → 168.245.113.14 (IPAddress)
s1.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 → 149.72.45.101 (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 → 34.135.140.14 (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-PLATFOR, 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:f0fe:: (IPAddress)
```

```
(Yevidu㉿kali)-[~]
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 → o32.ptr265.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**

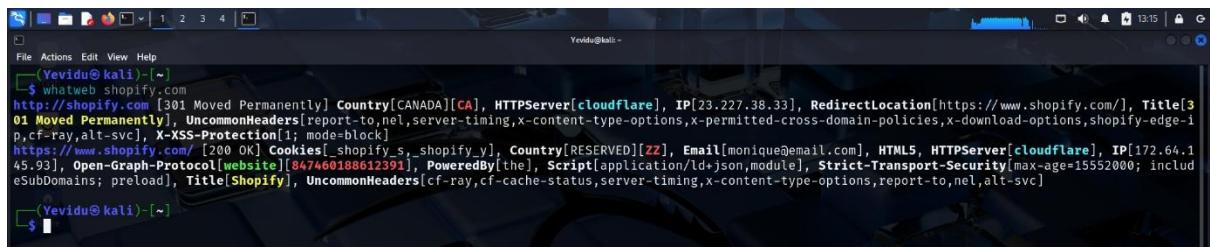
customer.login.shopify.com; A record → Login system (potential target for auth-related bugs)

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



```
Yevidu@kali:~$ whatweb shopify.com
http://shopify.com [301 Moved Permanently] Country[CANADA][CA], HTTPServer[cloudflare], IP[23.227.38.33], RedirectLocation[https://www.shopify.com/], Title[301 Moved Permanently], UncommonHeaders[report-to, net, server-timing, x-content-type-options, x-permitted-cross-domain-policies, x-download-options, shopify-edge-ip, cf-ray, alt-svc], X-XSS-Protection[1; mode=block]
https://www.shopify.com/ [200 OK] Cookies[_shopify_s, _shopify_y], Country[RESERVED][ZZ], Email[monique@email.com], HTML5, HTTPServer[cloudflare], IP[172.64.145.93], Open-Graph-Protocol[website][847460188612391], PoweredBy[theL], Script[application/json, module], Strict-Transport-Security[max-age=15552000; includeSubDomains, preload], Title[Shopify], UncommonHeaders[cf-ray, cf-cache-status, server-timing, x-content-type-options, report-to, net, alt-svc]
Yevidu@kali:~$
```

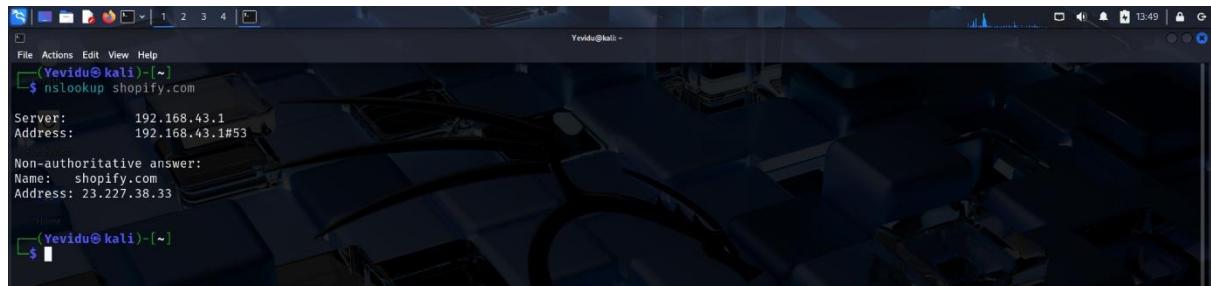
### **Initial Request:**

- **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



```
(Yevidu@kali)-[~]$ nslookup shopify.com
Server:      192.168.43.1
Address:     192.168.43.1#53

Non-authoritative answer:
Name:  shopify.com
Address: 23.227.38.33

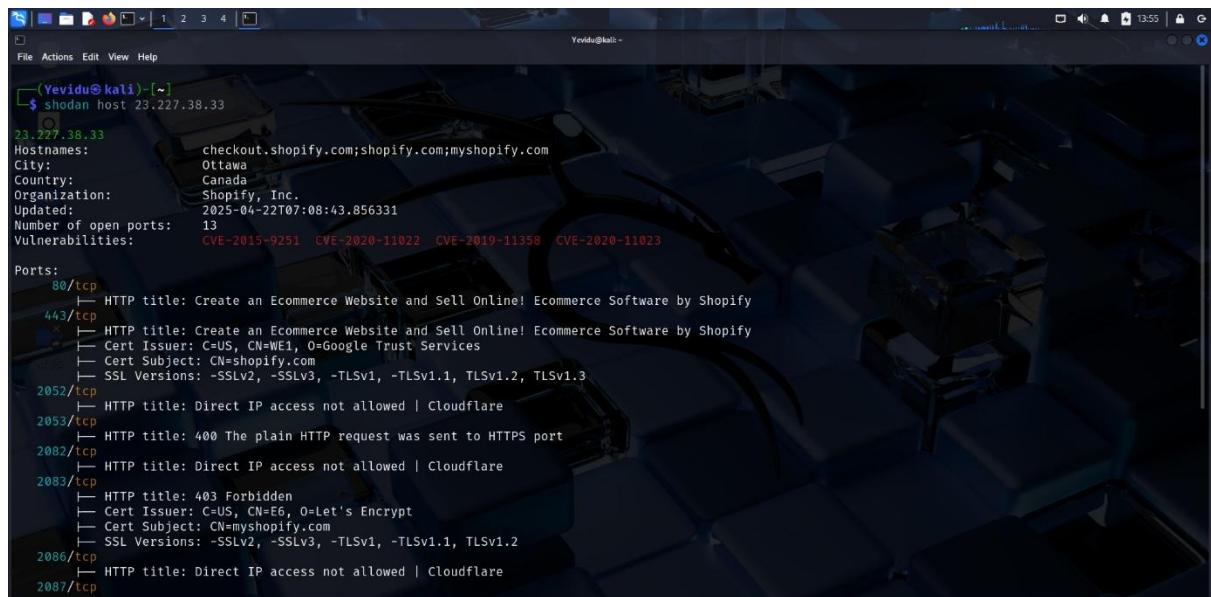
(Yevidu@kali)-[~]$
```

Server: 192.168.43.1  
Address: 192.168.43.1#53

Non-authoritative answer:

Name: shopify.com  
Address: 23.227.38.33

## Shodan



```
(Yevidu@kali)-[~]$ shodan host 23.227.38.33
23.227.38.33
Hostnames:
City: Ottawa
Country: Canada
Organization: Shopify, Inc.
Updated: 2025-04-22T07:08:43.856331
Number of open ports: 13
Vulnerabilities: CVE-2015-9251 CVE-2020-11022 CVE-2019-11358 CVE-2020-11023

Ports:
  80/tcp
    HTTP title: Create an Ecommerce Website and Sell Online! Ecommerce Software by Shopify
  443/tcp
    HTTP title: Create an Ecommerce Website and Sell Online! Ecommerce Software by Shopify
    Cert Issuer: C=US, CN=WEl, O=Google Trust Services
    Cert Subject: CN=shopify.com
    SSL Versions: -SSLv2, -SSLv3, -TLSv1, TLSv1.2, TLSv1.3
  2052/tcp
    HTTP title: Direct IP access not allowed | Cloudflare
  2053/tcp
    HTTP title: 400 The plain HTTP request was sent to HTTPS port
  2082/tcp
    HTTP title: Direct IP access not allowed | Cloudflare
  2083/tcp
    HTTP title: 403 Forbidden
    Cert Issuer: C=US, CN=E6, O=Let's Encrypt
    Cert Subject: CN=myshopify.com
    SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
  2086/tcp
    HTTP title: Direct IP access not allowed | Cloudflare
  2087/tcp
```

The terminal window displays a Shodan search query for Shopify hosts. The results show various ports (2052, 2053, 2082, 2083, 2086, 2087, 2095, 2096, 8080, 8443, 8880) and their corresponding details, such as SSL versions (SSLv2, SSLv3, TLSv1.1, TLSv1.2, TLSv1.3) and Cloudflare proxy information. The terminal prompt shows the user is on a Kali Linux system.

```
File Actions Edit View Help
  Cert Subject: CN=shopify.com
  Cert Issuer: C=US, CN=E6, O=Let's Encrypt
  SSL Versions: -SSLv2, -SSLv3, -TLSv1, TLSv1.2, TLSv1.3
2052/tcp
  HTTP title: Direct IP access not allowed | Cloudflare
2053/tcp
  HTTP title: 400 The plain HTTP request was sent to HTTPS port
2082/tcp
  HTTP title: Direct IP access not allowed | Cloudflare
2083/tcp
  HTTP title: 403 Forbidden
  Cert Issuer: C=US, CN=E6, O=Let's Encrypt
  Cert Subject: CN=myshopify.com
  SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
2086/tcp
  HTTP title: Direct IP access not allowed | Cloudflare
2087/tcp
  HTTP title: 403 Forbidden
  Cert Issuer: C=US, CN=E6, O=Let's Encrypt
  Cert Subject: CN=myshopify.com
  SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
2095/tcp
  HTTP title: Direct IP access not allowed | Cloudflare
2096/tcp
  HTTP title: 400 The plain HTTP request was sent to HTTPS port
8080/tcp
  Cloudflare
  HTTP title: Direct IP access not allowed | Cloudflare
8443/tcp
  Cloudflare
  HTTP title: 403 Forbidden
  Cert Issuer: C=US, CN=E6, O=Let's Encrypt
  Cert Subject: CN=myshopify.com
  SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
8880/tcp
  (Yevidu@kali)-[~]
$
```

- 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

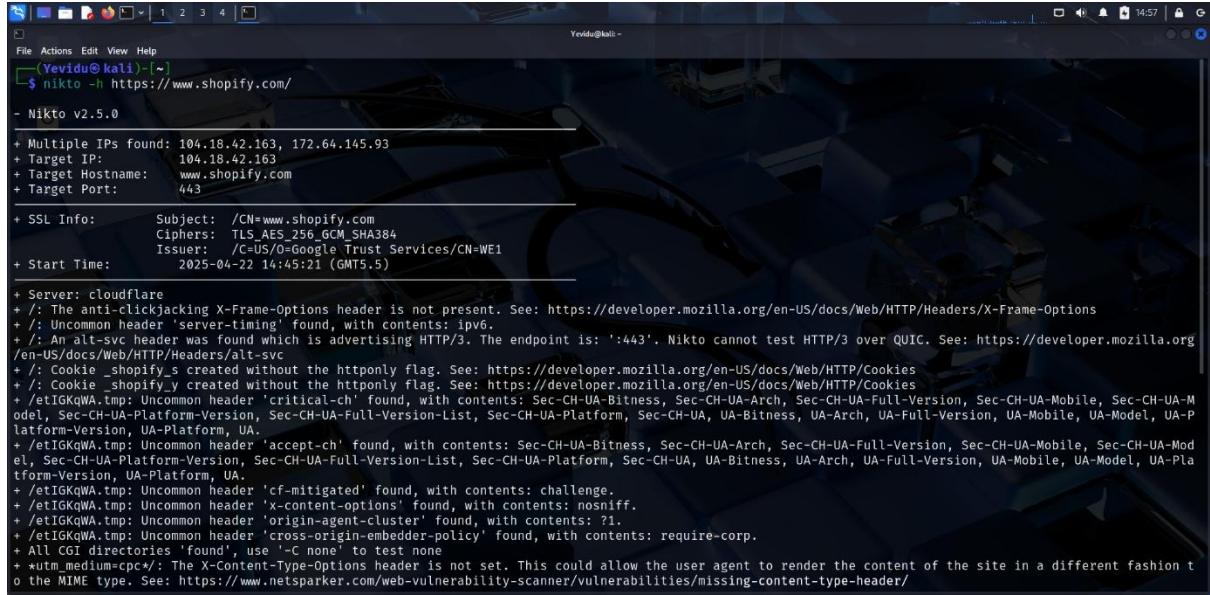
CVE-2020-11023 – Improper input sanitization in jQuery

CVE-2019-11358 – jQuery prototype pollution

<b>Port</b>	<b>Service</b>	<b>Notes</b>
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



```
Yevidu@kali:~$ nikto -h https://www.shopify.com/
[+] Nikto v2.5.0
[+] Multiple IPs found: 104.18.42.163, 172.64.145.93
[+] Target IP: 104.18.42.163
[+] Target Hostname: www.Shopify.com
[+] Target Port: 443
[+] SSL Info: Subject: /CN=www.shopify.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=Google Trust Services/CN=WE1
[+] Start Time: 2025-04-22 14:45:21 (GMT5.5)

[+] Server: cloudflare
[+] The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
[+] Uncommon header 'server-timing' found, with contents: ipv6.
[+] An alt-svc header was found which is advertising HTTP/3. The endpoint is ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
[+] Cookie _shopify_s created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
[+] Cookie _shopify_y created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
[+] setIGKqWA.tmp: Uncommon header 'critical-ch' found, with contents: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-M
odel, Sec-CH-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platform, Sec-CH-UA, UA-Bitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-P
latform-Version, UA-Platform, UA.
[+] etIGKqWA.tmp: Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-M
odel, Sec-CH-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platform, Sec-CH-UA, UA-Bitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-P
latform-Version, UA-Platform, UA.
[+] etIGKqWA.tmp: Uncommon header 'cf-mitigated' found, with contents: challenge.
[+] etIGKqWA.tmp: Uncommon header 'x-content-options' found, with contents: nosniff.
[+] etIGKqWA.tmp: Uncommon header 'origin-agent-cluster' found, with contents: ?1.
[+] etIGKqWA.tmp: Uncommon header 'cross-origin-embedder-policy' found, with contents: require-corp.
[+] All CGI directories 'found', use '-C none' to test none
[+] *utm_medium=cpc*: The X-Content-Type-Options header is not set. This could allow the user agent to render the content in a different fashion t
o the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
[+] utm_medium=cpc*: The X-Content-Type-Options header is not set. This could allow the user agent to render the content in a different fashion t
o the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
[+] robots.txt: Entry '/_pb/mm/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
[+] /*enterprise/blog/search?/: Uncommon header 'x-remix-error' found, with contents: yes.
[+] robots.txt: Entry '/enterprise/blog/search?/' is returned a non-forbidden or redirect HTTP code (404). See: https://portswigger.net/kb/issues/00600600_r
obots-txt-file
[+] robots.txt: Entry '/__dux/' is returned a non-forbidden or redirect HTTP code (405). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
[+] robots.txt: Entry '/cdn-cgi/challenge-platform/' is returned a non-forbidden or redirect HTTP code (404). See: https://portswigger.net/kb/issues/00600600_
cdn-cgi-challenge-platform
[+] robots.txt: contains 103 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
[+] favicon.ico: Retrieved access-control-allow-origin header: *
[+] favicon.ico: Drupal Link header found with value: <https://cdn.shopify.com/static/images/favicon.ico>; rel="canonical". See: https://www.drupal.org/
[+] favicon.ico: Uncommon header 'x-request-id' found, with contents: dfe74284-c3bc-44d6-b301-429ea7c82ef2-1738721591.
[+] favicon.ico: Uncommon header 'x-dc' found, with contents: gcp-us-east1,gcp-us-east1.
[+] : The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
[+] ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/tl
s alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
[+] Scan terminated: 19 error(s) and 23 item(s) reported on remote host
[+] End Time: 2025-04-22 14:56:52 (GMT5.5) (691 seconds)

[+] 1 host(s) tested
```

## 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

The screenshot shows the OWASP ZAP interface during an automated scan of <http://www.shopify.com>. The main window displays the 'Automated Scan' configuration, including the URL, spider type (set to 'Use traditional spider'), and attack settings. The progress bar indicates the scan is 'Manually stopped'. The bottom pane lists various security issues (Alerts) found, such as PII Disclosure, Absence of Anti-CSRF Tokens, and Cross-Domain JavaScript Source File Inclusion. One specific alert is highlighted as 'Content Modified'.

```

HTTP/1.1 200 OK
Date: Wed, 23 Apr 2015 18:19:32 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
CF-Ray: 934fSe9e2b6f92f5-CNB
CF-Cache-Status: EXPIRED
Cache-Control: no-store, s-maxage=0
ETag: W/"e0d455f27afaf778c7a1f7c7d1d4a0"
if (enableGtm) loadGtm(window);
DO
</script>
script src="https://cdn.shopify.com/shopifycloud/growth_tools/assets/manifests/index-8ed72b7ea060fe4da4c39449900ef733cf0cd84316133318b459ac10a12674e.js"></script>

```

**Alerts (19)**

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

**Alerts** 1 8 4 6 Main Proxy: localhost:8080 Current Status

### **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.

The screenshot shows the HackerOne interface for the GitLab program. On the left sidebar, there's a 'Program guidelines' section with links to 'Scope', 'Hacktivity', 'Thanks', 'Updates', 'Collaborators', and 'Safe harbor'. The main content area has a 'Program highlights' section with two items: 'Gold Standard' (Adheres to Gold Standard Safe Harbor) and 'Top Response Efficiency' (This program's response efficiency is above 90%). Below this are four boxes showing average times: 14 hours (average time to first response), 1 month, 2 weeks (average time to bounty), 1 month, 2 weeks (average time from submission to bounty), and 3 months, 6 days (average time to resolution). A 'Rewards summary' table follows, last updated on November 22, 2021. It shows the 90-day average bounty and percentage of total resolved reports for four severity levels: Low, Medium, High, and Critical. The table includes columns for Severity, Rewards, and the breakdown of submissions. A sidebar on the right shows the GitLab logo, URL, and a note about being a single application for the entire software development lifecycle, launched in Feb 2016, with a 95% response efficiency.

The screenshot shows the GitLab website homepage. At the top, there's a navigation bar with links to 'Platform', 'Product', 'Pricing', 'Resources', 'Company', 'Contact us', 'Talk to sales', 'Get free trial', and 'Sign in'. The main headline is 'Software. Faster.' Below it, a sub-headline says 'GitLab is the most comprehensive AI-powered DevSecOps Platform.' There's a 'Get free trial' button. To the right, there's a section titled 'Ship more secure software faster with AI throughout the entire software development lifecycle' with a link 'Discover GitLab Duo >'. Another section features a graphic of a cat inside a hexagonal pattern with text: 'GitLab named a Leader in the 2020 Gartner® Magic Quadrant™ for AI Assistants' and a link 'Read the report >'. The footer contains a link to 'https://about.gitlab.com/partners/technology-partners/aws/#interest'.

# Target Reconnaissance.

### Sublist3r

```
File Actions Edit View Help
registry.gke.staging.gitlab.com
kas.staging.gitlab.com
www.kas.staging.gitlab.com
next.staging.gitlab.com
www.next.staging.gitlab.com
observe.staging.gitlab.com
registry.staging.gitlab.com
www.registry.staging.gitlab.com
cdn.registry.staging.gitlab.com
static-objects.staging.gitlab.com
staging-ref.gitlab.com
customers.staging-ref.gitlab.com
geo.staging-ref.gitlab.com
registry.geo.staging-ref.gitlab.com
prometheus.staging-ref.gitlab.com
registry.staging-ref.gitlab.com
status.gitlab.com
www.status.gitlab.com
customers.stg.gitlab.com
www.customers.stg.gitlab.com
support.gitlab.com
www.support.gitlab.com
support-mw.gitlab.com
www.support-mw.gitlab.com
translate.gitlab.com
triage-ops.gitlab.com
triage-serverless.gitlab.com
www.triage-serverless.gitlab.com
university.gitlab.com
www.university.gitlab.com
version.gitlab.com
www.version.gitlab.com

(Yevidu@kali:~)
$
```

### ○ **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

```
(Yevido@kali:~) → a_record → 104.18.43.134 (IPAddress)
$ amass enum -d gitlab.com main_record → 2606:4700:4400::6812:2b86 ([IPAddress])
gitlab.com (FQDN) → mx_record → aspmx1.google.com (FQDN) → 40.907a ([IPAddress])
gitlab.com (FQDN) → mx_record → alt2.aspmx1.google.com (FQDN) → 40.907a ([IPAddress])
gitlab.com (FQDN) → mx_record → alt3.aspmx1.google.com (FQDN) → 40.907a ([IPAddress])
gitlab.com (FQDN) → mx_record → alt4.aspmx1.google.com (FQDN) → 40.907a ([IPAddress])
gitlab.com (FQDN) → ns_record → jermaine.ns.cloudflare.com (FQDN) → 1.2.1.100 ([IPAddress])
gitlab.com (FQDN) → ns_record → diva.ns.cloudflare.com (FQDN) → 1.2.1.100 ([IPAddress])
about.gitlab.com (FQDN) → a_record → 172.64.144.122 (IPAddress)
about.gitlab.com (FQDN) → a_record → 104.18.43.134 (IPAddress)
about.gitlab.com (FQDN) → aaaa_record → 2606:4700:4400::6812:2b86 ([IPAddress])
about.gitlab.com (FQDN) → aaaa_record → 2606:4700:4400::ac40:907a ([IPAddress])
email.gitlab.com (FQDN) → cname_record → mktc-ab130188.com (FQDN)
www.gitlab.com (FQDN) → cname_record → gitlab.com (FQDN)
forum.gitlab.com (FQDN) → cname_record → gitlab.hosted-by-discourse.com (FQDN)
support.gitlab.com (FQDN) → cname_record → gitlab.zendesk.com (FQDN)
internal.gitlab.com (FQDN) → cname_record → internal-handbook.gitlab.io (FQDN)
handbook.gitlab.com (FQDN) → cname_record → gitlab-com.gitlab.io (FQDN) → 1.2.1.100 ([IPAddress])
slippers.gitlab.com (FQDN) → cname_record → gitlab-com.gitlab.io (FQDN) → 1.2.1.100 ([IPAddress])
email.mg.gitlab.com (FQDN) → cname_record → mailgun.org (FQDN) → 1.2.1.100 ([IPAddress])
104.16.0.0/14 ([Netblock]) → contains → 104.18.43.134 (IPAddress) → 1.2.1.100 ([IPAddress])
172.64.144.0/20 ([Netblock]) → contains → 172.64.144.122 (IPAddress) → 1.2.1.100 ([IPAddress])
13335 (ASN) → managed_by → CLOUDFLARENET - Cloudflare, Inc. (RIROrganization)
13335 (ASN) → announces → 104.16.0.0/14 ([Netblock])
13335 (ASN) → announces → 172.64.144.0/20 ([Netblock])
links.gitlab.com (FQDN) → cname_record → d223t7pq0u0pac.cloudflare.net (FQDN)
status.staging.gitlab.com (FQDN) → cname_record → 46864463.hostedstatus.com (FQDN)
mg.gitlab.com (FQDN) → mx_record → mx.a.mailgun.org (FQDN)
mg.gitlab.com (FQDN) → mx_record → mx.b.mailgun.org (FQDN)
staging.gitlab.com (FQDN) → ns_record → arya.ns.cloudflare.com (FQDN)
staging.gitlab.com (FQDN) → ns_record → hat.ns.cloudflare.com (FQDN)
us-east1.cell-c01j2gdw0zfdafxr6.cells.gitlab.com (FQDN) → cname_record → bc5a1e6d8574a748dc3fe0e09740474.pacloudflare.com (FQDN)
marketplace.gitlab.com (FQDN) → cname_record → lb.gitlab.cloudblue.io (FQDN)
2606:4700:4400::/48 ([Netblock]) → contains → 2606:4700:4400::6812:2b86 ([IPAddress])

File Actions Edit View Help
File Actions Edit View Help
grafana.cell-c01j2gdw0zfdafxr6.cells.gitlab.com (FQDN) → a_record → 104.18.40.9 (IPAddress)
grafana.cell-c01j2gdw0zfdafxr6.cells.gitlab.com (FQDN) → a_record → 172.64.147.247 (IPAddress)
www.shop.gitlab.com (FQDN) → cname_record → shop.gitlab.com (FQDN)
kas.cell-c01j2gdw0zfdafxr6.cells.gitlab.com (FQDN) → a_record → 172.64.147.247 (IPAddress)
kas.cell-c01j2gdw0zfdafxr6.cells.gitlab.com (FQDN) → a_record → 104.18.40.9 (IPAddress)
registry.cell-c01j2gdw0zfdafxr6.cells.gitlab.com (FQDN) → a_record → 104.18.40.9 (IPAddress)
registry.cell-c01j2gdw0zfdafxr6.cells.gitlab.com (FQDN) → a_record → 172.64.147.247 (IPAddress)
cloud.gitlab.com (FQDN) → a_record → 104.18.42.65 (IPAddress)
cloud.gitlab.com (FQDN) → a_record → 172.64.145.191 (IPAddress)
cloud.gitlab.com (FQDN) → aaaa_record → 2606:4700:4400::ac40:91bf (IPAddress)
cloud.gitlab.com (FQDN) → aaaa_record → 2606:4700:4400::6812:2a41 (IPAddress)
new.docs.gitlab.com (FQDN) → a_record → 172.64.148.245 (IPAddress)
new.docs.gitlab.com (FQDN) → a_record → 104.18.39.11 (IPAddress)
new.docs.gitlab.com (FQDN) → aaaa_record → 2606:4700:4400::ac40:94f5 (IPAddress)
new.docs.gitlab.com (FQDN) → aaaa_record → 2606:4700:4400::6812:270b (IPAddress)
registry.getstaging-ref.gitlab.com (FQDN) → a_record → 34.65.51.8 (IPAddress)
104.16.0.0/14 ([Netblock]) → contains → 104.18.35.3 (IPAddress)
172.64.144.0/20 ([Netblock]) → contains → 172.64.152.253 (IPAddress)
2606:4700:4400::/48 ([Netblock]) → contains → 2606:4700:4400::6812:2303 (IPAddress)
2606:4700:4400::/48 ([Netblock]) → contains → 2606:4700:4400::ac40:98fd (IPAddress)
34.108.0.0/14 ([Netblock]) → contains → 34.110.199.161 (IPAddress)
172.65.240.0/20 ([Netblock]) → contains → 172.65.255.193 (IPAddress)
2606:4700:90::/44 ([Netblock]) → contains → 2606:4700:90::d91:b84e:71b:899 (IPAddress)
13.33.176.0/21 ([Netblock]) → contains → 13.33.183.92 (IPAddress)
13.33.176.0/21 ([Netblock]) → contains → 13.33.183.82 (IPAddress)
13.33.176.0/21 ([Netblock]) → contains → 13.33.183.38 (IPAddress)
13.33.176.0/21 ([Netblock]) → contains → 13.33.183.91 (IPAddress)
16509 (ASN) → announces → 13.33.176.0/21 (Netblock)
396982 (ASN) → announces → 34.108.0.0/14 (Netblock)
alt2.aspmx1.google.com (FQDN) → a_record → 173.194.202.26 (IPAddress)
alt2.aspmx1.google.com (FQDN) → aaaa_record → 2607:f8b0:400e::c01:1a (IPAddress)
gitlab.hosted-by-discourse.com (FQDN) → a_record → 184.105.99.75 (IPAddress)
gitlab.hosted-by-discourse.com (FQDN) → aaaa_record → 2602:fd3f:3:f02::4b (IPAddress)
registry.gitlab.com (FQDN) → a_record → 35.227.35.254 (IPAddress)
prometheus.staging-ref.gitlab.com (FQDN) → a_record → 35.237.45.16 (IPAddress)
```

```

Yevidu@Kali: ~
File Actions Edit View Help
2606:4700:4400::/48 (Netblock) → contains → 2606:4700:4400::ac40:9bb9 (IPAddress)
2606:4700:4400::/48 (Netblock) → contains → 2606:4700:4400::6812:2047 (IPAddress)
2606:4700:90::/44 (Netblock) → contains → 2606:4700:90::0:f0ff:e6a3:2ac:f7ef (IPAddress)
216.239.32.0/20 (Netblock) → contains → 216.239.32.106 (IPAddress)
216.239.32.0/20 (Netblock) → contains → 216.239.38.106 (IPAddress)
2001:4860::/32 (Netblock) → contains → 2001:4860:4802:36::6a (IPAddress)
2001:4860::/32 (Netblock) → contains → 2001:4860:4802:34::6a (IPAddress)
2001:4860::/32 (Netblock) → contains → 2001:4860:4802:38::6a (IPAddress)
15169 (ASN) → announces → 108.177.104.0/24 (Netblock)
15169 (ASN) → announces → 2001:4860::/32 (Netblock)
2607:f8b0:4003::/48 (Netblock) → contains → 2607:f8b0:4003:c04::1a (IPAddress)
2001:4860::/32 (Netblock) → contains → 2001:4860:4802:32::6a (IPAddress)
2a06:98c1:3122::/48 (Netblock) → contains → 2a06:98c1:3122:e000::4 (IPAddress)
2a06:98c1:3123::/48 (Netblock) → contains → 2a06:98c1:3123:e000::4 (IPAddress)
13335 (ASN) → announces → 2a06:98c1:3122::/48 (Netblock)
13335 (ASN) → announces → 2a06:98c1:3123::/48 (Netblock)
15169 (ASN) → announces → 2607:f8b0:4003::/48 (Netblock)
2607:f8b0:400e::/48 (Netblock) → contains → 2607:f8b0:400e:c00::1a (IPAddress)
173.194.202.0/24 (Netblock) → contains → 173.194.202.26 (IPAddress)
2600:9000:2816::/48 (Netblock) → contains → 2600:9000:2816:dc00::b:43f:a0:93a1 (IPAddress)
2600:9000:2816::/48 (Netblock) → contains → 2600:9000:2816:2a00::b:43f:a0:93a1 (IPAddress)
2600:9000:2816::/48 (Netblock) → contains → 2600:9000:2816:ea00::b:43f:a0:93a1 (IPAddress)
2600:9000:2816::/48 (Netblock) → contains → 2600:9000:2816:b400::b:43f:a0:93a1 (IPAddress)
2600:9000:2816::/48 (Netblock) → contains → 2600:9000:2816:c800::b:43f:a0:93a1 (IPAddress)
2600:9000:2816::/48 (Netblock) → contains → 2600:9000:2816:1400::b:43f:a0:93a1 (IPAddress)
13.225.0.0/21 (Netblock) → contains → 13.225.5.107 (IPAddress)
13.225.0.0/21 (Netblock) → contains → 13.225.5.117 (IPAddress)
13.225.0.0/21 (Netblock) → contains → 13.225.5.30 (IPAddress)
108.159.80.0/23 (Netblock) → contains → 108.159.80.88 (IPAddress)
2600:9000:238c::/48 (Netblock) → contains → 2600:9000:238c:5c00::1a:leef:6c40:93a1 (IPAddress)
2600:9000:238c::/48 (Netblock) → contains → 2600:9000:238c:3c00::1a:leef:6c40:93a1 (IPAddress)
2600:9000:238c::/48 (Netblock) → contains → 2600:9000:238c:4200::1a:leef:6c40:93a1 (IPAddress)
2600:9000:238c::/48 (Netblock) → contains → 2600:9000:238c:fa00::1a:leef:6c40:93a1 (IPAddress)
2600:9000:238c::/48 (Netblock) → contains → 2600:9000:238c::0::1a:leef:6c40:93a1 (IPAddress)
2600:9000:238c::/48 (Netblock) → contains → 2600:9000:238c:2200::1a:leef:6c40:93a1 (IPAddress)

```

## 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

```

Yevidu@Kali: ~
File Actions Edit View Help
[Yevidu@Kali: ~]
$ nslookup gitlab.com
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::f22e:fbec:5bed:a9b9

[Yevidu@Kali: ~]
$ 

```

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

```
(Yevidu@kali)-[~]$ shodan host 172.65.251.78
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 CloudFlare
 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

(Yevidu@kali)-[~]$
```

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

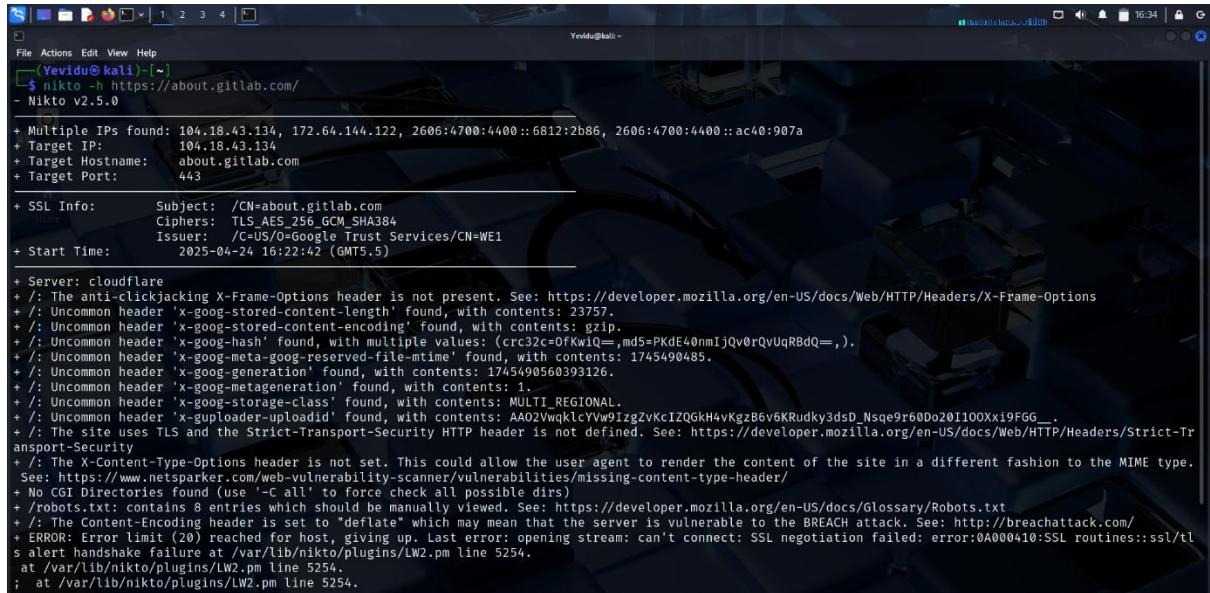
  └ HTTP title: 400 The plain HTTP request was sent to HTTPS port

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

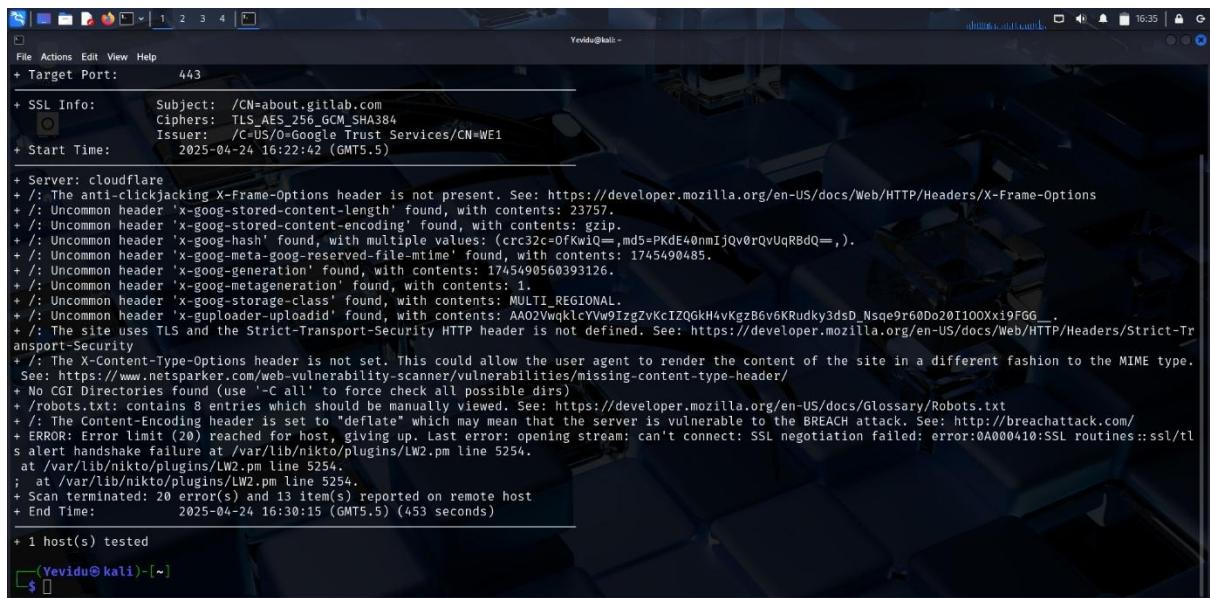


```
Yevidu@kali:~]$ nikto -h https://about.gitlab.com/
- Nikto v2.5.0

+ Multiple IPs found: 104.18.43.134, 172.64.144.122, 2606:4700:4400::6812:2b86, 2606:4700:4400::ac40:907a
+ Target IP: 104.18.43.134
+ Target Hostname: about.gitlab.com
+ Target Port: 443

+ SSL Info: Subject: /CN=about.gitlab.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=Google Trust Services/CN=WE1
+ Start Time: 2025-04-24 16:22:42 (GMT5.5)

+ Server: cloudflare
+/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+/: Uncommon header 'x-goog-stored-content-length' found, with contents: 23757.
+/: Uncommon header 'x-goog-stored-content-encoding' found, with contents: gzip.
+/: Uncommon header 'x-goog-hash' found, with multiple values: (crc32c=OfKwiQ==,md5=PKdE40nmIjQv0rQvUqRBdQ==,).
+/: Uncommon header 'x-goog-meta-goog-reserved-file-mtime' found, with contents: 1745490485.
+/: Uncommon header 'x-goog-generation' found, with contents: 1745490560393126.
+/: Uncommon header 'x-goog-metageneration' found, with contents: 1.
+/: Uncommon header 'x-goog-storage-class' found, with contents: MULTI REGIONAL.
+/: Uncommon header 'x-uploader-uploadid' found, with contents: AA02VwqklcYw91zgZvKcIZQGkH4vKgzb6v6KRudy3dsD.Nsqe9r60D0o20I100Xx19FG6.
+/: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 8 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+/: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/tl
s alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
```



```
Yevidu@kali:~]$ nikto -h https://about.gitlab.com/
+ Target Port: 443

+ SSL Info: Subject: /CN=about.gitlab.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=Google Trust Services/CN=WE1
+ Start Time: 2025-04-24 16:22:42 (GMT5.5)

+ Server: cloudflare
+/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+/: Uncommon header 'x-goog-stored-content-length' found, with contents: 23757.
+/: Uncommon header 'x-goog-stored-content-encoding' found, with contents: gzip.
+/: Uncommon header 'x-goog-hash' found, with multiple values: (crc32c=OfKwiQ==,md5=PKdE40nmIjQv0rQvUqRBdQ==,).
+/: Uncommon header 'x-goog-meta-goog-reserved-file-mtime' found, with contents: 1745490485.
+/: Uncommon header 'x-goog-generation' found, with contents: 1745490560393126.
+/: Uncommon header 'x-goog-metageneration' found, with contents: 1.
+/: Uncommon header 'x-goog-storage-class' found, with contents: MULTI REGIONAL.
+/: Uncommon header 'x-uploader-uploadid' found, with contents: AA02VwqklcYw91zgZvKcIZQGkH4vKgzb6v6KRudy3dsD.Nsqe9r60D0o20I100Xx19FG6.
+/: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 8 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+/: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/tls alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 13 item(s) reported on remote host
+ End Time: 2025-04-24 16:30:15 (GMT5.5) (453 seconds)

+ 1 host(s) tested
```

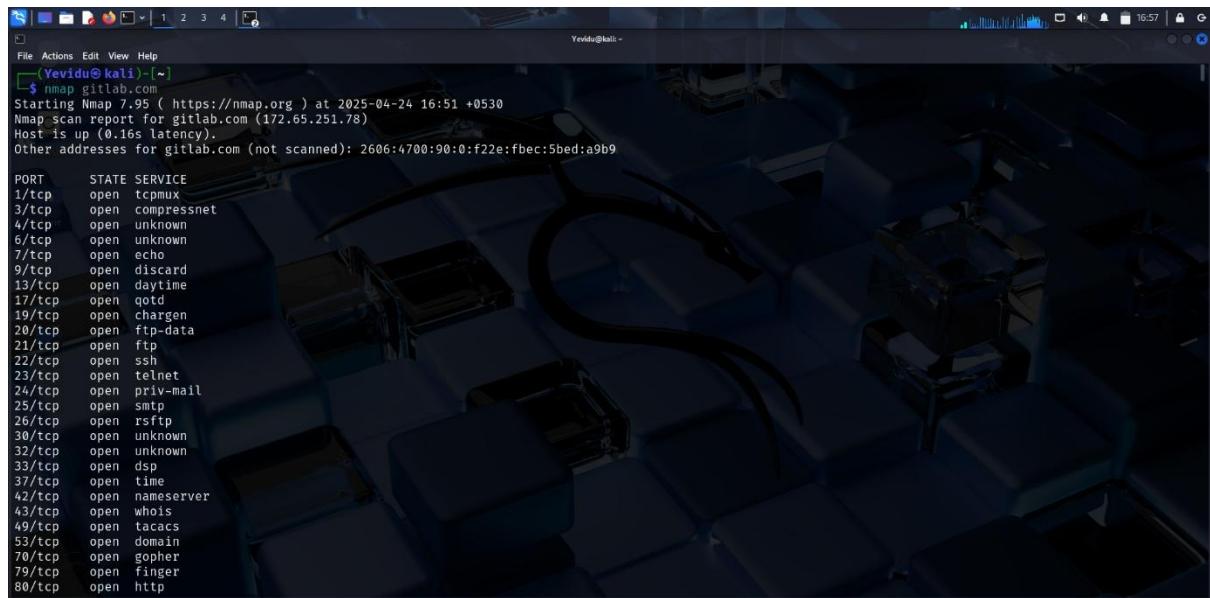
## Security Headers Missing

- 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



```
Yevidu@kali: ~]$ nmap gitlab.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 16:51 +0530
Nmap scan report for gitlab.com (172.65.251.78)
Host is up (0.16s latency).
Other addresses for gitlab.com (not scanned): 2606:4700:90:0:f22e:5bed:a9b9

PORT      STATE SERVICE
1/tcp      open  tcpmux
3/tcp      open  compressnet
4/tcp      open  unknown
6/tcp      open  unknown
7/tcp      open  echo
9/tcp      open  discard
13/tcp     open  daytime
17/tcp     open  qotd
19/tcp     open  chargen
20/tcp     open  ftp-data
21/tcp     open  ftp
22/tcp     open  ssh
23/tcp     open  telnet
24/tcp     open  priv-mail
25/tcp     open  smtp
26/tcp     open  rsftp
30/tcp     open  unknown
32/tcp     open  unknown
33/tcp     open  dsp
37/tcp     open  time
42/tcp     open  nameserver
43/tcp     open  whois
49/tcp     open  tacacs
53/tcp     open  domain
70/tcp     open  gopher
79/tcp     open  finger
80/tcp     open  http
```

```
File Actions Edit View Help
50636/tcp open  unknown
50800/tcp open  unknown
51103/tcp open  unknown
51493/tcp open  unknown
52673/tcp open  unknown
52822/tcp open  unknown
52848/tcp open  unknown
52869/tcp open  unknown
54045/tcp open  unknown
54328/tcp open  unknown
55055/tcp open  unknown
55056/tcp open  unknown
55555/tcp open  unknown
55600/tcp open  unknown
56737/tcp open  unknown
56738/tcp open  unknown
57294/tcp open  unknown
57797/tcp open  unknown
58080/tcp open  unknown
60020/tcp open  unknown
60443/tcp open  unknown
61532/tcp open  unknown
61900/tcp open  unknown
62078/tcp open  iphone-sync
63331/tcp open  unknown
64623/tcp open  unknown
64680/tcp open  unknown
65000/tcp open  unknown
65129/tcp open  unknown
65389/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 16.92 seconds
[Yevidu@kali] ~]$
```

## 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

```
Yevidiu@kali:~$ nuclei -U gitlab.com
[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 64
[INF] Templates loaded for current scan: 7862
[INF] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from https
[INF] Templates clustered: 1717 (Reduced 1614 Requests)
[dns-waf-detect:cloudflare] [dns] [info] gitlab.com
    Using Interactx Server: oast.pro
[azure-domain-tenant] [http] [ ] https://login.microsoftonline.com/v2.0/.well-known/openid-configuration ["7cc60e3a-c2c5-43d6-b426-1d8c9e8e7ad1"]
[graphql-alias-batching] [http] [info] https://gitlab.com/api/graphql
[graphql-field-suggestion] [http] [info] https://gitlab.com/api/graphql
[graphql-detect] [http] [info] https://gitlab.com/api/graphql [paths="/api/graphql"]
[oauth2-detect] [http] [info] https://gitlab.com/oauth/token
[waf-detect:cloudflare] [http] [ ] https://gitlab.com
[ssh-auth-methods] [javascript] [info] gitlab.com:22 ["[publickey]"]
[ssh-server-enumeration] [javascript] [info] gitlab.com:22 ["SSH-2.0-GitLab-SSHD"]
[ssh-sha1-hmac-algo] [javascript] [info] gitlab.com:22
[tls-version] [ssl] [info] gitlab.com:443 ["tls12"]
```

```
Yevidiu@kali:~$ gitlab-explore:gitlab-community
[ssh-server-enumeration] [javascript] [info] gitlab.com:22 ["SSH-2.0-GitLab-SSHD"]
[ssh-sha1-hmac-algo] [javascript] [info] gitlab.com:22
[tls-version] [ssl] [info] gitlab.com:443 ["tls12"]
[tls-version] [ssl] [info] gitlab.com:443 ["tls13"]
[oidc-detect] [http] [info] https://gitlab.com/.well-known/openid-configuration
[tech-detect:cloudflare] [http] [info] https://gitlab.com
[gitlab-explore:gitlab-community] [http] [info] https://gitlab.com/api/v4/projects
[robots-txt] [http] [info] https://gitlab.com/robots.txt
[robots-txt-endpoint] [http] [info] https://gitlab.com/robots.txt
[gitlab-public-repos] [http] [info] https://gitlab.com/api/v4/projects
[dmarc-detect] [dns] [info] dmrc.gitlab.com ["v=DMARC1; p=reject; pct=100%"]
[mx-fingerprint] [dns] [info] gitlab.com ["alt4.aspmx.l.google.com.", "10 alt3.aspmx.l.google.com.", "1 aspmx.l.google.com.", "5 alt1.aspmx.l.google.com."]
[mx-service-detector:google Apps] [dns] [info] gitlab.com
[ca-fingerprint] [dns] [info] gitlab.com ["globalsign.com", "ssl.com", "awstrust.com", "mailto:security@gitlab.com", "sectigo.com", "amazonaws.com", "comodoca.com", "pki.goog; cansignhtpxchanges=yes", "digicert.com; cansignhtpxchanges=yes", "amazontrust.com", "letsencrypt.org", "amazon.com"]
[ssl-issuer] [ssl] [info] gitlab.com:443 ["Sectigo Limited"]
[ssl-dns-names] [ssl] [info] gitlab.com:443 ["gitlab.com", "auth.gitlab.com", "customers.gitlab.com", "email.customers.gitlab.com", "gprd.gitlab.com", "www.gitlab.com"]
[nameserver-fingerprint] [dns] [info] gitlab.com ["jermine.ns.cloudflare.com", "diva.ns.cloudflare.com"]
[spf-record-detect] [dns] [info] gitlab.com ["v=spf1 include:mail.zendesk.com include:_spf.google.com include:mktomail.com include:_spf.salesforce.com includ
e:_spf.ip.gitlab.com a:@gateway.zuora.com include:mailgun.org -all"]
[txt-fingerprint] [dns] [info] gitlab.com ["google-site-verification=6cb3PPomp6-xRavXf2HZz037pplQeG5MiiuaPGiu_Q", "mgverify=9549a9644bc9886fb483bcd56872eaf2b5b9e690d26402401cf446644cb114", "google-site-verification=lnPj0x5EAxmESH8FSn4colWVMaxe1K4ZlOpD81IEDY", "docsign=1a7d6818-2cf5-4956-a9fb-c3d2e9a578dd", "MS0196128", "google-site-verification=XRDr7LE0qv60V0RF0Fh7G2XgpzdycygJBQde334q4", "v=spf1 include:mail.zendesk.com include:_spf.google.com includ
e:mktomail.com include:_spf.ip.gitlab.com a:@gateway.zuora.com include:mailgun.org -all", "onetrust-domain-verification=84b59aa2659244d486bb86f5db073dd", "globalsign-domain-verification=a2HJ7gl04Dr8r2VR0tXu7Orwg7uzp06v7LOHWVp1b3", "google-site-verification=t99AMja1lnkbCOvnN5fIWFp085ze/ZH0BWj2WkD2pe", "asv=3763643512ad5b0dc0d42caeab3951", "onetrust-domain-verification=a5b5fd1be45a9b4c4b0c09e571923", "mgverify=2dd945066758840fe3bfbd9ccf9062c6000458f13345baa576338880dc86658", "google-site-verification=Q167NT1WpedorF171mnN70Ve2Fo_yA6Rclsx08St0a8", "google-site-verification=1W2U6Qb3MvV83zy47ZFrGFVL6ADfpjqch1Qjok", "google-site-verification=PPG6D0lgvt5vhZqg5zG1SLao6-07-VzzpqvmCf5Y", "Ms=ms83893381", "drift-domain-verification=nfa583cff88c496bcc6265105750656a98ab3e689c314255a1a6ae848e3e56d", "uber-domain-verification=38ba2b7b-5ae3-4694-9701-086b20ea3d36", "adobe-idp-site-verification=5a5e001556a2c0595ed571d2a17f58a749a00742853e035eb909bdd31622b8"]
```

## 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

The screenshot shows two instances of the OWASP ZAP application interface.

**Top Window (Untitled Session - 20250424-172800 - ZAP 2.16.1):**

- Toolbar:** File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help.
- Left Sidebar:** Standard Mode, Sites, Contexts (Default Context), and a tree view for Sites.
- Central Panel:** Title: "Automated Scan". Subtitle: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'." A note: "Please be aware that you should only attack applications that you have been specifically given permission to test." Input fields: "URL to attack" (http://about.gitlab.com), "Use traditional spider" (checked), "Use ajax spider" (dropdown: If Modem, with: Firefox), and buttons: "Attack" and "Stop". Status: "Progress: Using traditional spider to discover the content".
- Bottom Panel:** History, Search, Alerts, Output, Spider tab (selected), and a progress bar at 2%.
- Alerts Panel:** Shows 0 alerts.
- URIs Panel:** A table listing URLs processed by the spider, all of which are GET requests to various pages on http://about.gitlab.com.
- Flags Panel:** Shows current status with 0 critical, 0 high, 0 medium, 0 low, 0 info, and 0 debug.

**Bottom Window (Untitled Session - 20250424-172800 - ZAP 2.16.1):**

- Toolbar:** File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help.
- Left Sidebar:** Standard Mode, Sites, Contexts (Default Context), and a tree view for Sites.
- Central Panel:** Title: "Please be aware that you should only attack applications that you have been specifically given permission to test." Input fields: "URL to attack" (http://about.gitlab.com), "Use traditional spider" (checked), "Use ajax spider" (dropdown: If Modem, with: Firefox), and buttons: "Attack" and "Stop". Status: "Progress: Manually stopped".
- Bottom Panel:** History, Search, Alerts tab (selected), and a progress bar at 0%.
- Alerts Panel:** Shows 17 alerts, including:

  - 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)
  - Modem Web Application (86)
  - Re-examine Cache-control Directives (233)

- Flags Panel:** Shows current status with 0 critical, 0 high, 0 medium, 0 low, 0 info, and 0 debug.

**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.

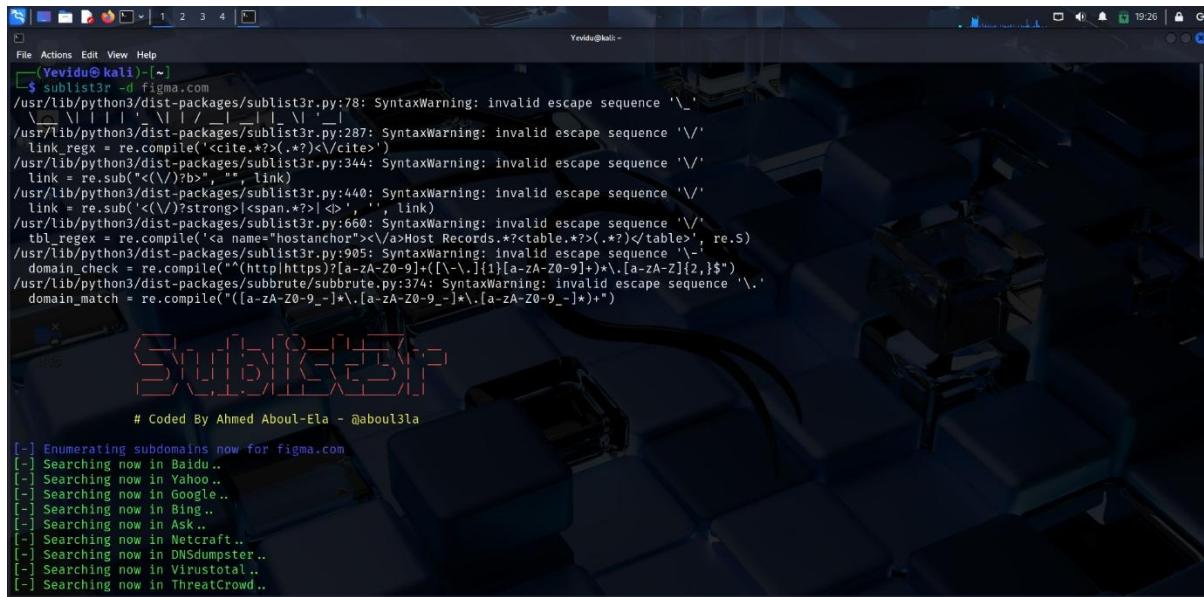
## Report 04.

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.

The image contains two screenshots of the Figma bug bounty program. The top screenshot is from the HackerOne platform, showing the 'Program highlights' section with metrics: Average time to first response (3 days, 19 hours), Average time to triage (6 days, 3 hours), Average time to bounty (8 hours), Average time from submission to bounty (6 days, 11 hours), and Average time to resolution (7 months, 2 days). It also shows the 'Rewards' section with severity levels: Low (\$1-\$300), Medium (\$300-\$2,000), and High (\$2,000-\$5,000). The bottom screenshot is from the official Figma website, featuring a large 'Think bigger. Build faster.' headline, a sub-headline 'Figma helps design and development teams build great products, together.', and a 'Get started for free' button. A promotional banner at the bottom for 'Config 25' includes the text 'Figma's newest product announcements coming May 7. Join Config 25 virtually for free.' and a 'Register' button.

## Target Reconnaissance.

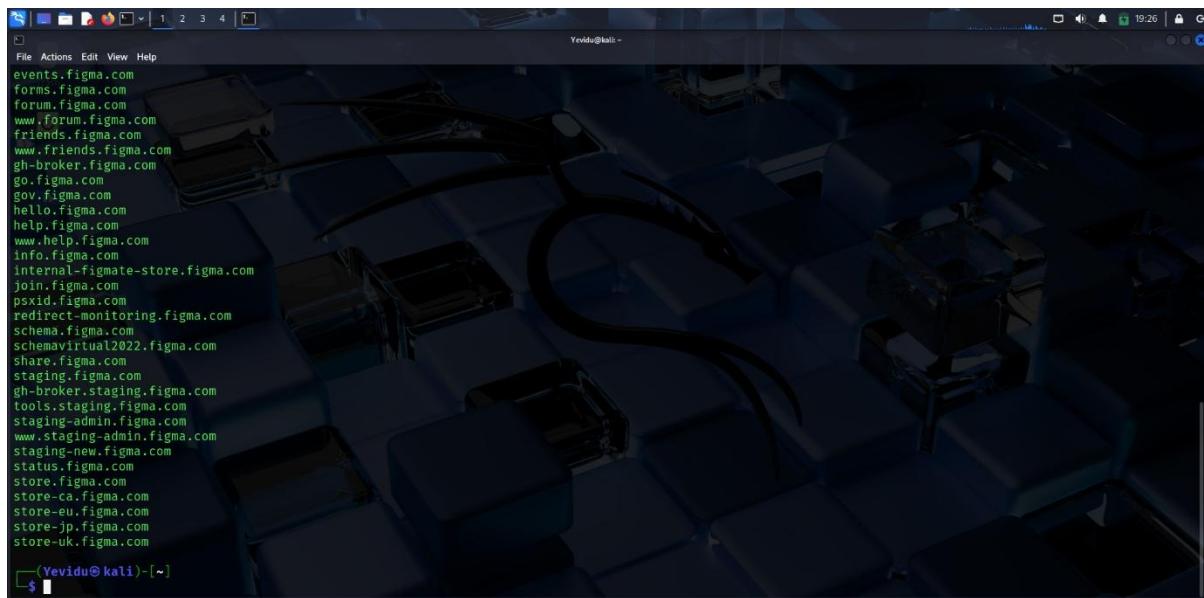
### Sublist3r



```
Yevidu@kali:~$ sublist3r -d figma.com
/usr/lib/python3/dist-packages/sublist3r.py:78: SyntaxWarning: invalid escape sequence '\_'
  \_\_|\_| |\_|\_|\_|\_|\_|\_|\_
/usr/lib/python3/dist-packages/sublist3r.py:287: SyntaxWarning: invalid escape sequence '\\''
  line_regex = re.compile('<cite.*?>(.*)</cite>')
/usr/lib/python3/dist-packages/sublist3r.py:344: SyntaxWarning: invalid escape sequence '\\''
  line = re.sub("<(</>)b>", "", link)
/usr/lib/python3/dist-packages/sublist3r.py:440: SyntaxWarning: invalid escape sequence '\\''
  line = re.sub('<(</>)?strong>|<span.*?>|<>', '', link)
/usr/lib/python3/dist-packages/sublist3r.py:660: SyntaxWarning: invalid escape sequence '\\''
  tbl_regex = re.compile('<a name="hostanchor"></a>Host Records.*?<table.*?></table>', re.S)
/usr/lib/python3/dist-packages/sublist3r.py:905: SyntaxWarning: invalid escape sequence '\\''
  domain_check = re.compile("^(http|https)?[a-zA-Z0-9]+([\\_.][a-zA-Z0-9]+)*.[a-zA-Z]{2,}$")
/usr/lib/python3/dist-packages/subbrute/subbrute.py:374: SyntaxWarning: invalid escape sequence '\\''
  domain_match = re.compile("([a-zA-Z0-9_-]*.[a-zA-Z0-9_-]*\.[a-zA-Z0-9_-]*)$")

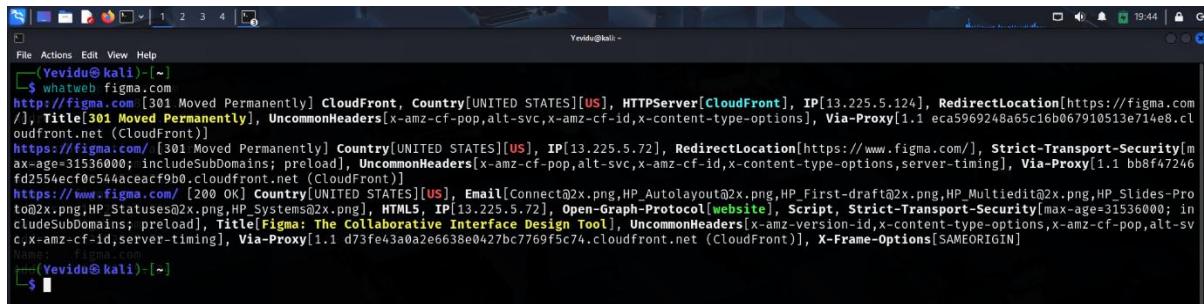
# Coded By Ahmed Aboul-Ela - @abou3la

[-] Enumerating subdomains now for figma.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in VirusTotal..
[-] Searching now in ThreatCrowd..
```



```
Yevidu@kali:~$ sublist3r -d figma.com
events.figma.com
forms.figma.com
forum.figma.com
www.forum.figma.com
friends.figma.com
www.friends.figma.com
gh-broker.figma.com
go.figma.com
gov.figma.com
hello.figma.com
help.figma.com
www.help.figma.com
info.figma.com
internal-figate-store.figma.com
join.figma.com
pscid.figma.com
redirect-monitoring.figma.com
schema.figma.com
schemavirtual2022.figma.com
share.figma.com
staging.figma.com
gh-broker.staging.figma.com
tools.staging.figma.com
staging-admin.figma.com
www.staging-admin.figma.com
staging-new.figma.com
status.figma.com
store.figma.com
store-ca.figma.com
store-eu.figma.com
store-jp.figma.com
store-uk.figma.com
```

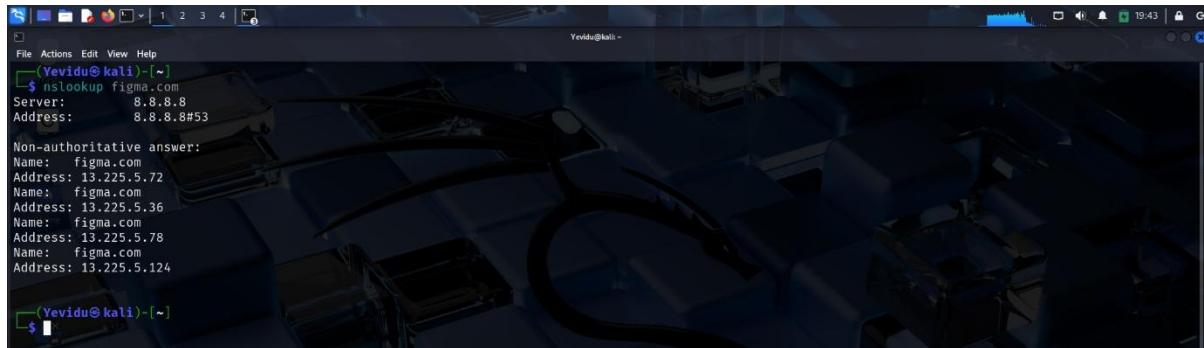
## Whatweb



```
Yevidu@kali:~$ whatweb figma.com
http://figma.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[13.225.5.124], RedirectLocation[https://figma.com/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf-id,x-content-type-options], Via-Proxy[1.1 eca5969248a65c16b067910513e714e8.cloudfront.net (CloudFront)]
https://figma.com/ [301 Moved Permanently] Country[UNITED STATES][US], IP[13.225.5.72], RedirectLocation[https://www.figma.com/], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf-id,x-content-type-options,server-timing], Via-Proxy[1.1 bb8f47246fd2554ecf0c544aceacf9b0.cloudfront.net (CloudFront)]
https://www.figma.com/ [200 OK] Country[UNITED STATES][US], Email[Connect@2x.png,HP_AutoLayout@2x.png,HP_First-draft@2x.png,HP_MultiEdit@2x.png,HP_Slides-Proto@2x.png,HP_Statuses@2x.png,HP_Systems@2x.png], HTML5, IP[13.225.5.72], Open-Graph-Protocol[website], Script, Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Figma: The Collaborative Interface Design Tool], UncommonHeaders[x-amz-version-id,x-content-type-options,x-amz-cf-pop,alt-svc,x-amz-cf-id,server-timing], Via-Proxy[1.1 d73fe43a0a2e6638e0427bc7769f5c74.cloudfront.net (CloudFront)], X-Frame-Options[SAMEORIGIN]
Yevidu@kali:~$
```

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



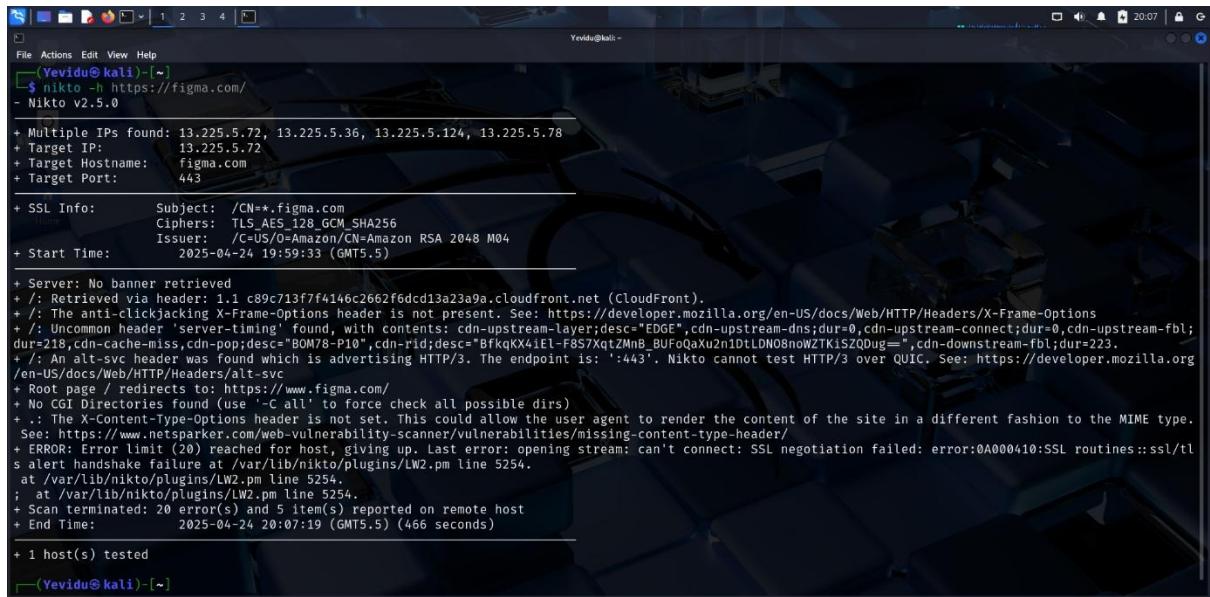
```
Yevidu@kali:~$ nslookup figma.com
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: figma.com
Address: 13.225.5.72
Name: figma.com
Address: 13.225.5.36
Name: figma.com
Address: 13.225.5.78
Name: figma.com
Address: 13.225.5.124
Yevidu@kali:~$
```

<b>Query</b>	<b>Result</b>
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



```
Yevidu@kali:~$ nikto -h https://figma.com/
- Nikto v2.5.0

+ Multiple IPs found: 13.225.5.72, 13.225.5.36, 13.225.5.124, 13.225.5.78
+ Target IP: 13.225.5.72
+ Target Hostname: figma.com
+ Target Port: 443

+ SSL Info: Subject: /CN=*.figma.com
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M04
+ Start Time: 2025-04-24 19:59:33 (GMT5.5)

+ Server: No banner retrieved
+ Retrieved via header: 1.1 c89c713f7ff146c2662f6dc13a23a9a.cloudfront.net (CloudFront).
+ : The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ : Uncommon header 'server-timing' found, with contents: cdn-upstream-layer;desc="EDGE",cdn-upstream-dns;dur=0,cdn-upstream-connect;dur=0,cdn-upstream-fbl;
dur=218,cdn-cache-miss,cdn-pop;desc="BOM78-P10",cdn-rid;desc="BfkqKX41El-F857XqtZMnB_BUFOQaXu2n1DtLDNO8nwZTK15ZQdug=",cdn-downstream-fbl;dur=223.
+ : An alt-svc header was found which is advertising HTTP/3. The endpoint is ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ Root page / redirects to: https://www.figma.com/
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ : The X-Content-type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/tl
s alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time: 2025-04-24 20:07:19 (GMT5.5) (466 seconds)

+ 1 host(s) tested

Yevidu@kali:~$
```

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



```

File Actions Edit View Help
(Yevidu@kali)-[~]
$ nmap figma.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 20:17 +0530
Nmap scan report for figma.com (13.225.5.78)
Host is up (0.022s latency).
Other addresses for figma.com (not scanned): 13.225.5.124 13.225.5.36 13.225.5.72
rDNS record for 13.225.5.78: server-13-225-5-78.bom78.r.cloudfront.net
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 8.38 seconds
$ 

```

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

## OWASP ZAP

The screenshot shows the OWASP ZAP interface in Standard Mode. The main window displays an 'Automated Scan' configuration panel. The 'URL to attack' field contains 'http://figma.com'. The 'Attack' button is highlighted in yellow. Below the panel, the status bar shows 'Progress: 0 http://figma.com' and 'Current Scans 0 URLs Found 9 Nodes Added 5'. The bottom section of the interface shows a table of processed requests with columns for Method, URI, and Flags. Most requests are marked as 'Seed', while two are labeled 'Out of Scope'.

Method	URI	Flags
GET	http://figma.com	Seed
GET	http://figma.com/robots.txt	Seed
GET	http://figma.com/sitemap.xml	Seed
GET	https://figma.com/	
GET	https://figma.com/robots.txt	
GET	https://figma.com/sitemap.xml	
GET	https://www.figma.com/	
GET	https://www.figma.com/robots.txt	Out of Scope Out of Scope

The screenshot shows a complex interface for web application security testing. At the top, there's a standard menu bar (File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help) and a session header (Untitled Session - 20260424-204942 - ZAP 2.16.1). Below the menu is a toolbar with icons for Standard Mode, Sites, Quick Start, Request, Response, and Requester.

The main area has tabs for Header Text, Body Text, and a dropdown for Requester. On the left, there's a sidebar with sections for Contexts, Default Context, and Sites. The main content area displays a Figma page with several audit results overlaid:

- A large red box highlights a critical issue: "HTTP/1.1 200 OK Content-type: text/html; charset=utf-8 Content-length: 77829 Connection: keep-alive Date: Thu, 24 Apr 2023 15:19:46 GMT".
- An "Inspect" tool is open, showing detailed code analysis for the page.
- A "Content Modified" section is present.
- The "Alerts" section lists several findings:
  - CSP: Failure to Define Directive with No Fallback (severity: Critical)
  - script-src unsafe-eval
  - CSP: script-src unsafe-inline
  - CSP: style-src unsafe-inline
  - Timestamp Disclosure - Unix
  - Information Disclosure - Suspicious Comments (2)
  - Retrieved from Cache
  - User Agent Fuzzer (18)
- At the bottom, there are "Alerts" and "Current Status" buttons.

## 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.

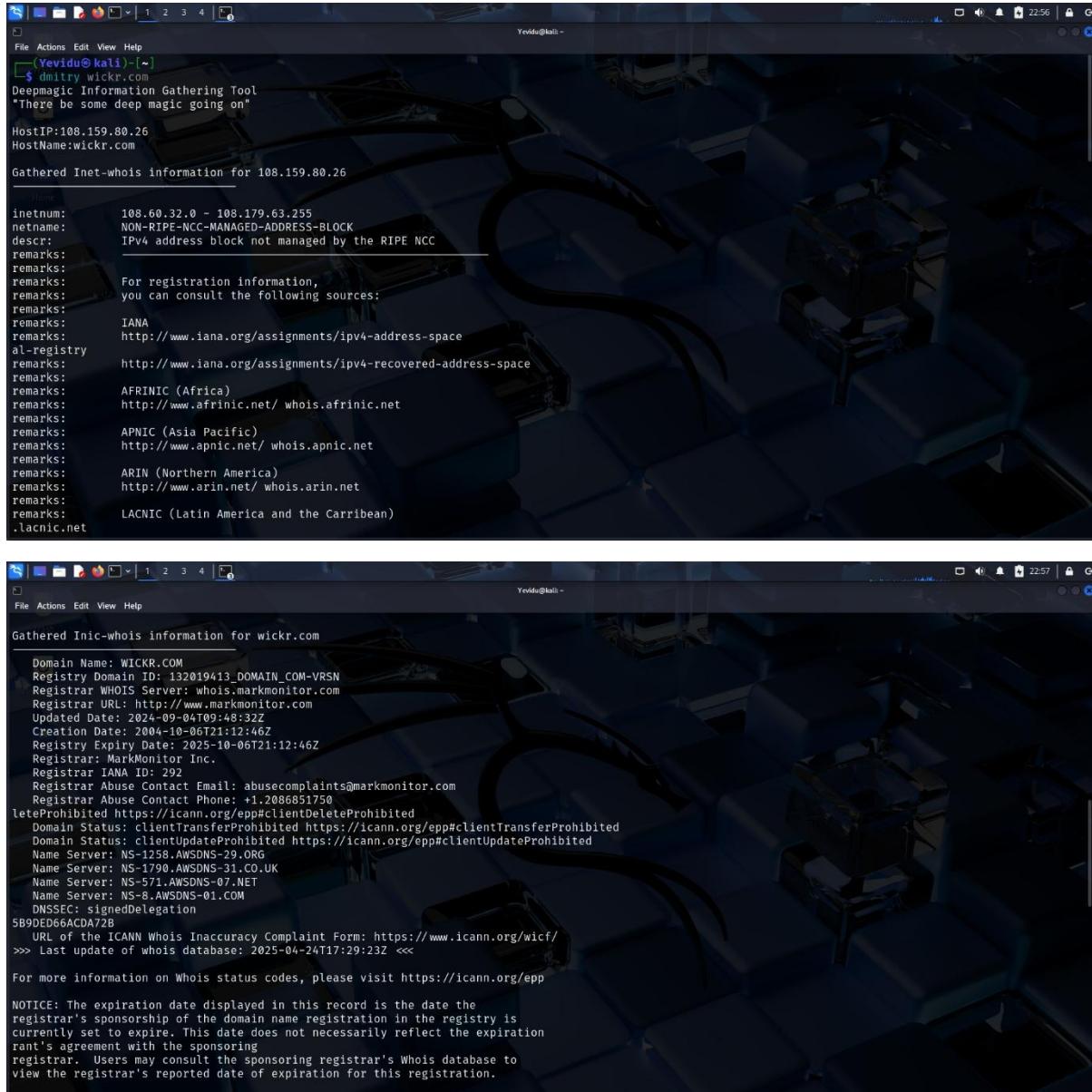
The top screenshot shows the 'Program guidelines' section of the hackerone.com/wickr?type=team page. It displays various performance metrics:

Metric	Value
Average time to first response	7 hours
Average time to triage	1 day, 20 hours
Average time to bounty	N/A
Average time from submission to bounty	1 day, 20 hours
Average time to resolution	N/A

The bottom screenshot shows the main wickr.com website. It features a banner about protecting communications with end-to-end encryption and secure collaboration across messaging, calling, file sharing, and screen sharing. It includes download and contact sales buttons.

# Target Reconnaissance.

## Dmitry Scan



```
Yevidu@kali: ~]$ dmitry wickr.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:108.159.80.26
HostName:wickr.com

Gathered Inet-whois information for 108.159.80.26

inetnum: 108.60.32.0 - 108.179.63.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
For registration information,
you can consult the following sources:
Remarks: IANA
http://www.iana.org/assignments/ipv4-address-space
al-registry
http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
AFRINIC (Africa)
http://www.afrinic.net/ whois.afrinic.net
remarks:
APNIC (Asia Pacific)
http://www.apnic.net/ whois.apnic.net
remarks:
ARIN (Northern America)
http://www.arin.net/ whois.arin.net
remarks:
LACNIC (Latin America and the Caribbean)
.lacnic.net

Gathered Inic-whois information for wickr.com

Domain Name: WICKR.COM
Registry Domain ID: 132019413_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-09-04T09:48:32Z
Creation Date: 2004-10-06T21:12:46Z
Registry Expiry Date: 2025-10-06T21:12:46Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
let'sProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS-1258.AWSDNS-29.ORG
Name Server: NS-1790.AWSDNS-31.CO.UK
Name Server: NS-571.AWSDNS-07.NET
Name Server: NS-8.AWSDNS-01.COM
DNSSEC: signedDelegation
5B90ED66ACDA72B
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-24T17:29:23Z <<

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

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
of the registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

The screenshot shows a terminal window with the following output:

```
mains and Registrars.

Gathered Netcraft information for wickr.com

Retrieving Netcraft.com information for wickr.com
Netcraft.com Information gathered

Gathered Subdomain information for wickr.com
_____
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host wickr.com, Searched 0 pages containing 0 results

Gathered E-Mail information for wickr.com
_____
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host wickr.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 108.159.80.26
_____
Port      State
21/tcp    open
80/tcp    open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting
```

**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).

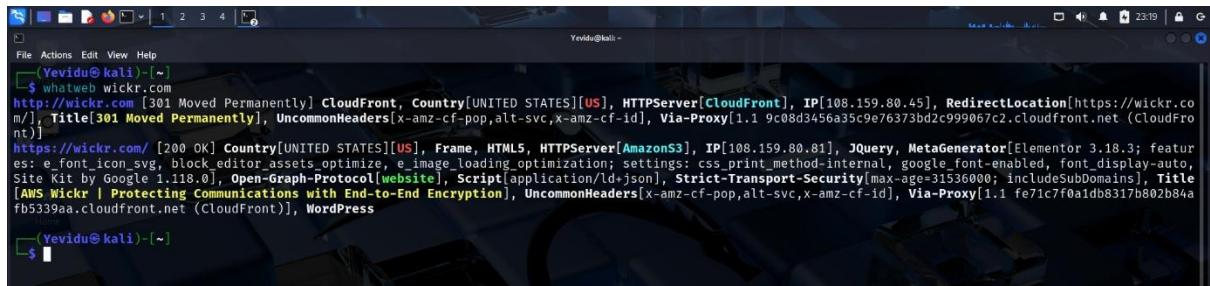
## Domain WHOIS

- **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



```
Yevidu@kali: ~
$ whatweb wickr.com
http://wickr.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[108.159.80.45], RedirectLocation[https://wickr.com], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 9c08d3456a35c9e76373bd2c999067c2.cloudfront.net (CloudFront)]
https://wickr.com/ [200 OK] Country[UNITED STATES][US], Frame, HTML5, HTTPServer[AmazonS3], IP[108.159.80.81], JQuery, MetaGenerator[Elementor 3.18.3; features: e_font_icon_svg, block_editor_assets_optimize, e_image_loading_optimization; settings: css_print_method=internal, google_font-enabled, font_display-auto, Site Kit by Google 1.118.0], Open-Graph-Protocol[website], Script[application/ld+json], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[AWS Wickr | Protecting Communications with End-to-End Encryption], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 fe71c7f0a1db8317b802b84a fb5339aa.cloudfront.net (CloudFront)], WordPress
$
```

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

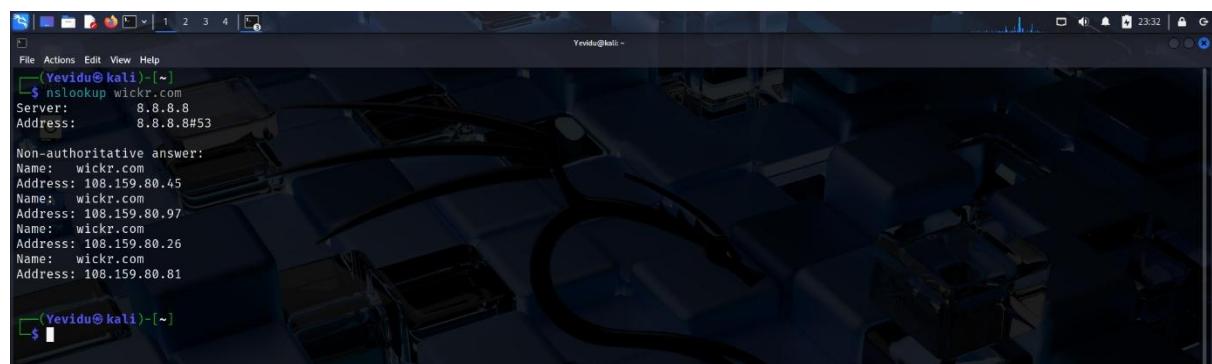
Scripts: Make use of structured data (ld+json) and jQuery

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



```
(Yevidu@kali)-[~]$ nslookup wickr.com
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: wickr.com
Address: 108.159.80.45
Name: wickr.com
Address: 108.159.80.97
Name: wickr.com
Address: 108.159.80.26
Name: wickr.com
Address: 108.159.80.81

(Yevidu@kali)-[~]$
```

- Domain: wickr.com
- IP Addresses:

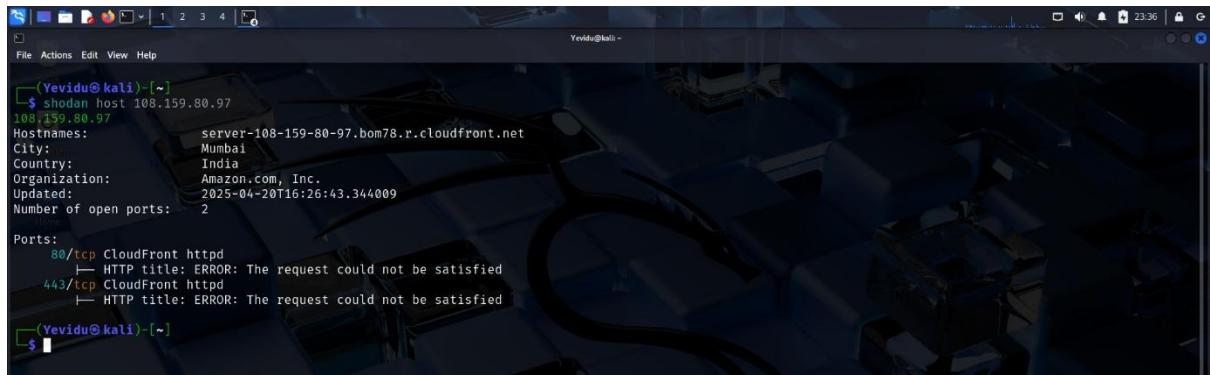
108.159.80.26

108.159.80.45

108.159.80.81

108.159.80.97

## Shodan



```
[Yevidu@kali)-[~]$ shodan host 108.159.80.97
108.159.80.97
Hostnames: server-108-159-80-97.bom78.r.cloudfront.net
City: Mumbai
Country: India
Organization: Amazon.com, Inc.
Updated: 2025-04-20T16:26:43.344009
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
[Yevidu@kali)-[~]$
```

IP Address: 108.159.80.97

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

Location: Mumbai, India IN

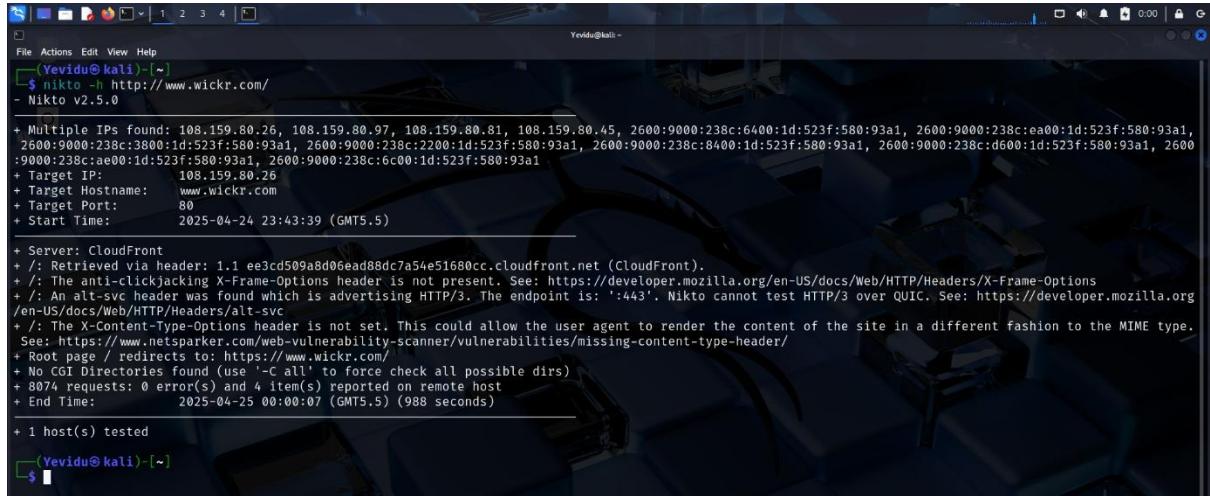
Organization: Amazon.com, Inc. (CloudFront CDN)

Last Updated: April 20, 2025

Port	Protocol	Service
80	TCP	HTTP
443	TCP	HTTPS

## Scanning and vulnerability identification.

### Nikto



```
Yevidu@kali:~]$ nikto -h http://www.wickr.com/
- Nikto v2.5.0

+ Multiple IPs found: 108.159.80.26, 108.159.80.97, 108.159.80.81, 108.159.80.45, 2600:9000:238c:6400:1d:523f:580:93a1, 2600:9000:238c:ea00:1d:523f:580:93a1, 2600:9000:238c:ea00:1d:523f:580:93a1, 2600:9000:238c:8400:1d:523f:580:93a1, 2600:9000:238c:d600:1d:523f:580:93a1, 2600:9000:238c:a000:1d:523f:580:93a1, 2600:9000:238c:c000:1d:523f:580:93a1
+ Target IP: 108.159.80.26
+ Target Hostname: www.wickr.com
+ Target Port: 80
+ Start Time: 2025-04-24 23:43:39 (GMT5.5)

+ Server: CloudFront
+ /: Retrieved via header: 1.1 ee3cd509a0d06ead88dc7a54e51680cc.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.wickr.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8074 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2025-04-25 00:00:07 (GMT5.5) (988 seconds)

+ 1 host(s) tested

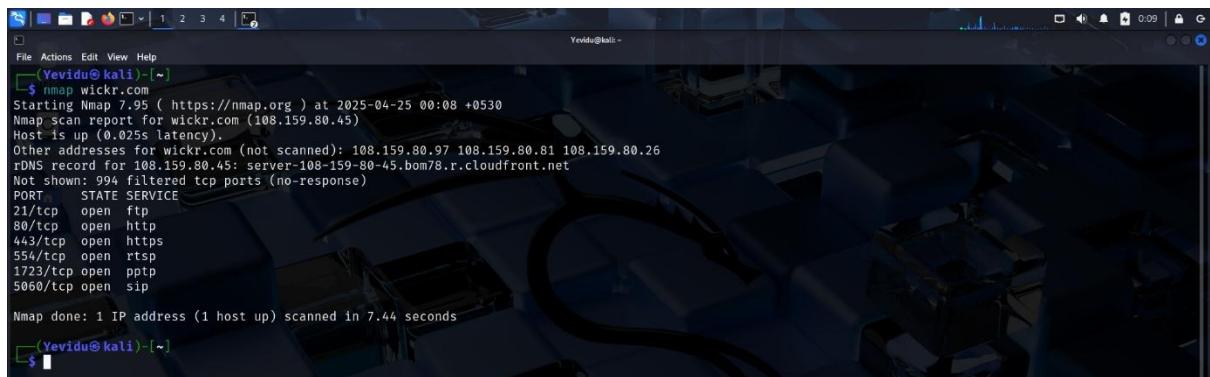
Yevidu@kali:~]$
```

- Site to target: [www.wickr.com](http://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



```
File Actions Edit View Help
[Yevidu@kali: ~]
$ nmap wickr.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 00:08 +0530
Nmap scan report for wickr.com (108.159.80.45)
Host is up (0.025s latency).
Other addresses for wickr.com (not scanned): 108.159.80.97 108.159.80.81 108.159.80.26
rDNS record for 108.159.80.45: server-108-159-80-45.bom78.r.cloudfront.net
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp
5060/tcp  open  sip

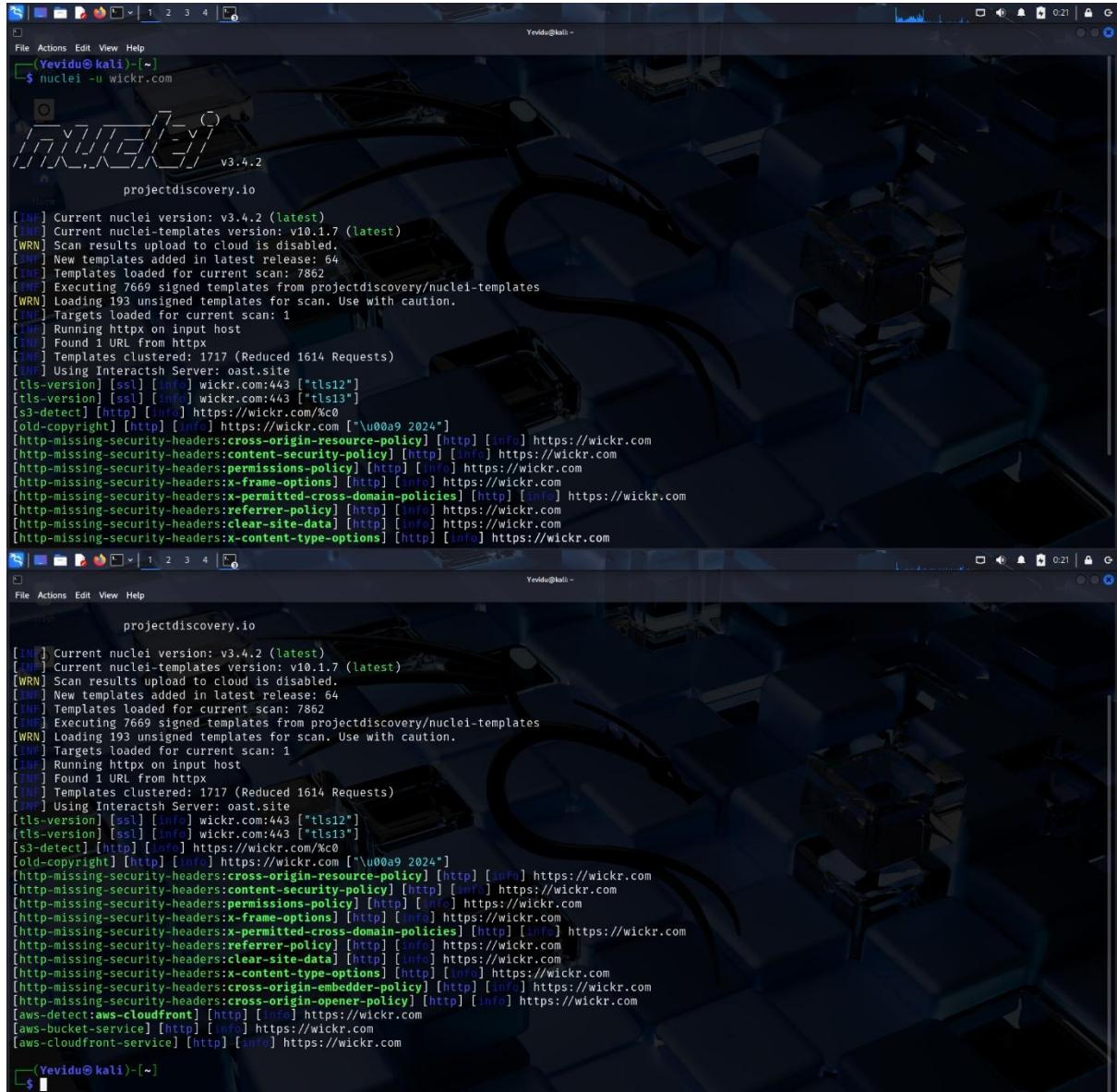
Nmap done: 1 IP address (1 host up) scanned in 7.44 seconds
[Yevidu@kali: ~]
```

- 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



```
Yevidu@kali:~$ nuclei -u wickr.com
[✓] (Yevidu@kali)-~] $ nuclei -u wickr.com
v3.4.2
projectdiscovery.io

[!] Current nuclei version: v3.4.2 (latest)
[!] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[!] New templates added in latest release: 64
[!] Templates loaded for current scan: 7862
[!] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[!] Targets loaded for current scan: 1
[!] Running httpx on input host
[!] Found 1 URL from httpx
[!] Templates clustered: 1717 (Reduced 1614 Requests)
[!] Using Interactsh Server: oast.site
[tls-version] [ssl] [info] wickr.com:443 ["tls12"]
[tls-version] [ssl] [info] wickr.com:443 ["tls13"]
[s3-detect] [http] [info] https://wickr.com/%c0
[old-copyright] [http] [info] https://wickr.com ["\u00a9 2024"]
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://wickr.com
[http-missing-security-headers:content-security-policy] [http] [info] https://wickr.com
[http-missing-security-headers:permissions-policy] [http] [info] https://wickr.com
[http-missing-security-headers:x-frame-options] [http] [info] https://wickr.com
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://wickr.com
[http-missing-security-headers:referrer-policy] [http] [info] https://wickr.com
[http-missing-security-headers:clear-site-data] [http] [info] https://wickr.com
[http-missing-security-headers:x-content-type-options] [http] [info] https://wickr.com
[http-missing-security-headers:x-content-type-options] [http] [info] https://wickr.com

Yevidu@kali:~$ nuclei -u wickr.com
[✓] (Yevidu@kali)-~] $ nuclei -u wickr.com
v3.4.2
projectdiscovery.io

[!] Current nuclei version: v3.4.2 (latest)
[!] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[!] New templates added in latest release: 64
[!] Templates loaded for current scan: 7862
[!] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[!] Targets loaded for current scan: 1
[!] Running httpx on input host
[!] Found 1 URL from httpx
[!] Templates clustered: 1717 (Reduced 1614 Requests)
[!] Using Interactsh Server: oast.site
[tls-version] [ssl] [info] wickr.com:443 ["tls12"]
[tls-version] [ssl] [info] wickr.com:443 ["tls13"]
[s3-detect] [http] [info] https://wickr.com/%c0
[old-copyright] [http] [info] https://wickr.com ["\u00a9 2024"]
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://wickr.com
[http-missing-security-headers:content-security-policy] [http] [info] https://wickr.com
[http-missing-security-headers:permissions-policy] [http] [info] https://wickr.com
[http-missing-security-headers:x-frame-options] [http] [info] https://wickr.com
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://wickr.com
[http-missing-security-headers:referrer-policy] [http] [info] https://wickr.com
[http-missing-security-headers:clear-site-data] [http] [info] https://wickr.com
[http-missing-security-headers:x-content-type-options] [http] [info] https://wickr.com
[http-missing-security-headers:x-content-type-options] [http] [info] https://wickr.com
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://wickr.com
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://wickr.com
[aws-detect:aws-cloudfront] [http] [info] https://wickr.com
[aws-bucket-service] [http] [info] https://wickr.com
[aws-cloudfront-service] [http] [info] https://wickr.com
```

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

<b>Missing Header</b>	<b>Risk</b>
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

The screenshot displays two instances of the OWASP ZAP application interface.

**Top Window (Automated Scan):**

- Header:** File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help. Untitled Session - 20250425-002615 - ZAP 2.16.1.
- Left Sidebar:** Standard Mode, Sites, Contexts (Default Context), and a tree view for Sites.
- Middle Panel:** "Automated Scan" section. It shows the URL to attack as <http://wickr.com>, with "Use traditional spider" checked. Below it are options for "Use ajax spider" (If Modem with Firefox) and "Attack" (button). Progress is shown as "Manually stopped".
- Bottom Panel:** Alerts tab (13 alerts), showing a list of findings including PII Disclosure, Content Security Policy (CSP) Header Not Set, and Vulnerable JS Library.
- Footer:** Alerts (13), Main Proxy: localhost:8080, Current Status (multiple icons).

**Bottom Window (Detailed Alert View):**

- Header:** File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help. Untitled Session - 20250425-002615 - ZAP 2.16.1.
- Left Sidebar:** Standard Mode, Sites, Contexts (Default Context), and a tree view for Sites.
- Middle Panel:** "Header Text" and "Body Text" tabs are open. The Body Text tab shows a large amount of raw HTTP response code for a request to <https://wickr.com/wp-content/plugins/elementor-pro/assets/js/preloaded-elements-handlers.min.js>.
- Bottom Panel:** Alerts tab (13 alerts), showing a list of findings including PII Disclosure, Content Security Policy (CSP) Header Not Set, and Vulnerable JS Library. A specific alert for the Vulnerable JS Library is expanded, showing details like URL (<https://wickr.com/wp-content/plugins/elementor-pro/assets/js/preloaded-elements-handlers.min.js>), Risk (High), Confidence (Medium), and Source (Passive (10003 - Vulnerable JS Library (Powered by Retire.js))).
- Footer:** Alerts (13), Main Proxy: localhost:8080, Current Status (multiple icons).

## 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.

The screenshot shows the 'Program highlights' section of the Plaid bug bounty program on HackerOne. It includes metrics like average response time (8 hours), average time to bounty (0), and average time from submission to bounty (0). The 'Rewards' section lists bounties for Low, Medium, High, and Critical severity levels, with amounts of \$1,000, \$2,500, \$5,000, and \$10,000 respectively. A sidebar on the right provides general information about Plaid, including its logo, website, and launch date.

The screenshot shows the Plaid homepage. The main headline reads 'Turn data into revolutionary financial products'. Below it, a sub-headline says 'Connect to real-time insights on the Plaid Network to create fast, safe, and smart financial experiences.' A large illustration of a person's face is visible on the right side of the page. At the bottom, there is a cookie consent banner.

# Target Reconnaissance.

## Dmitry Scan

```
(Yevidu@kali)-[~]$ dmitry plaid.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:52.84.45.42
HostName:plaid.com

Gathered Inet-whois information for 52.84.45.42

inetnum:      52.0.0.0 - 52.144.63.255
K
descr:        IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks:      For registration information,
remarks:      you can consult the following sources:
remarks:      IANA
remarks:      http://www.iana.org/assignments/ipv4-address-space
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
ks:
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:      APNIC (Asia Pacific)
remarks:      http://www.apnic.net/ whois.apnic.net
remarks:
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
remarks:
```

```
(Yevidu@kali)-[~]$ dmitry plaid.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

% This query was Served by the RIPE Database Query Service version 1.117 (SHETLAND)

Gathered Inic-whois information for plaid.com

Domain Name: PLAID.COM
Registry Domain ID: 1418247_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2024-07-12T01:44:55Z
Creation Date: 1995-08-16T04:00:00Z
Registry Expiry Date: 2025-08-15T04:00:00Z
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
.org/eppclientTransferProhibited
Name Server: NS-1123.AWSDNS-12.ORG
Name Server: NS-1688.AWSDNS-19.CO.UK
Name Server: NS-309.AWSDNS-38.COM
Name Server: NS-967.AWSDNS-56.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-25T14:53:01Z <<<

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

The domain name registration is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.
```

```
Yevidu@kali: ~
```

File Actions Edit View Help

Retrieving Netcraft.com information for plaid.com  
Netcraft.com Information gathered

Gathered Subdomain information for plaid.com

Searching Google.com:80 ...  
HostName:my.plaid.com  
HostIP:3.164.85.57  
HostName:sandbox.plaid.com  
HostIP:52.7.212.85  
HostName:dashboard.plaid.com  
HostIP:3.164.85.127  
HostName:support-my.plaid.com  
HostIP:216.198.54.1  
HostName:www.plaid.com  
HostIP:108.156.144.5  
HostName:production.plaid.com  
HostIP:52.21.52.166  
Searching Altavista.com:80 ...  
Found 6 possible subdomain(s) for host plaid.com, Searched 0 pages containing 0 results

Gathered E-Mail information for plaid.com

Searching Google.com:80 ...  
Searching Altavista.com:80 ...  
Found 0 E-Mail(s) for host plaid.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 52.84.45.42

Port	State

Yevidu@kali: ~

```
Yevidu@kali: ~
```

File Actions Edit View Help

HostIP:3.164.85.114  
HostName:sandbox.plaid.com  
HostIP:3.234.14.107  
HostName:dashboard.plaid.com  
HostIP:3.164.85.95  
HostName:support-my.plaid.com  
HostIP:216.198.53.1  
HostName:www.plaid.com  
HostIP:108.156.144.5  
HostName:production.plaid.com  
HostIP:54.163.163.171  
Searching Altavista.com:80 ...  
Found 6 possible subdomain(s) for host plaid.com, Searched 0 pages containing 0 results

Gathered E-Mail information for plaid.com

Searching Google.com:80 ...  
Searching Altavista.com:80 ...  
Found 0 E-Mail(s) for host plaid.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 52.84.45.79

Port	State
53/tcp	open
80/tcp	open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting

[Yevidu@kali: ~]

## 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

```
File Actions Edit View Help
(Yevidu@kali)-[~]
$ whatweb https://plaid.com/
https://plaid.com/ [200 OK] Cookies[locale], Country[UNITED STATES][us], HTML5, HTTPServer[AmazonS3], IP[52.84.45.24], Open-Graph-Protocol[website], PoweredBy[Plaid], Script[application/json,application/ld+json,text/javascript], Strict-Transport-Security[max-age=63072000; includeSubDomains; preload], Title[Plaid: Enabling all companies to build fintech solutions | Plaid], UncommonHeaders[x-amz-version-id,x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 19a730cc6a36iccbf99b2c18fe3d654.cloudfront.net (CloudFront)], X-UA-Compatible[ie=edge]
(Yevidu@kali)-[~]
$ 
```

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:

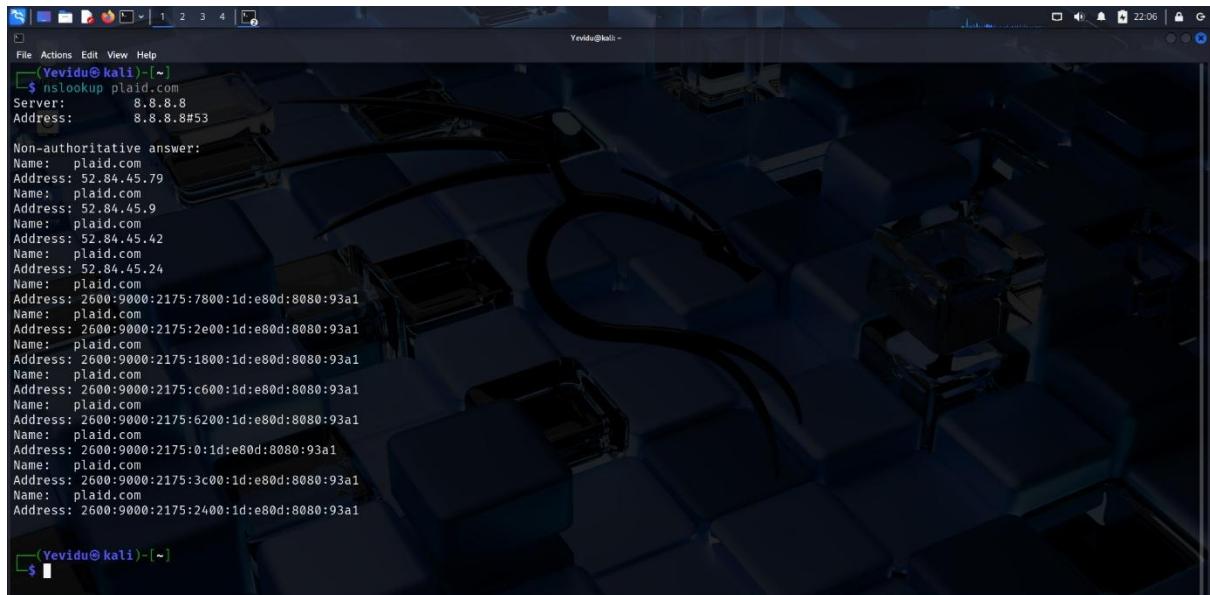
Strict-Transport-Security

Cookies: location

Driven by: Plaid

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

## Nslookup



```
(Yevidu@kali)-[~]$ nslookup plaid.com
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: plaid.com
Address: 52.84.45.79
Name: plaid.com
Address: 52.84.45.9
Name: plaid.com
Address: 52.84.45.42
Name: plaid.com
Address: 52.84.45.24
Name: plaid.com
Address: 2600:9000:2175:7800:1d:e80d:8080:93a1
Name: plaid.com
Address: 2600:9000:2175:2e00:1d:e80d:8080:93a1
Name: plaid.com
Address: 2600:9000:2175:1800:1d:e80d:8080:93a1
Name: plaid.com
Address: 2600:9000:2175:c600:1d:e80d:8080:93a1
Name: plaid.com
Address: 2600:9000:2175:6200:1d:e80d:8080:93a1
Name: plaid.com
Address: 2600:9000:2175:0:1d:e80d:8080:93a1
Name: plaid.com
Address: 2600:9000:2175:3c00:1d:e80d:8080:93a1
Name: plaid.com
Address: 2600:9000:2175:2400:1d:e80d:8080:93a1

(Yevidu@kali)-[~]$
```

### 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

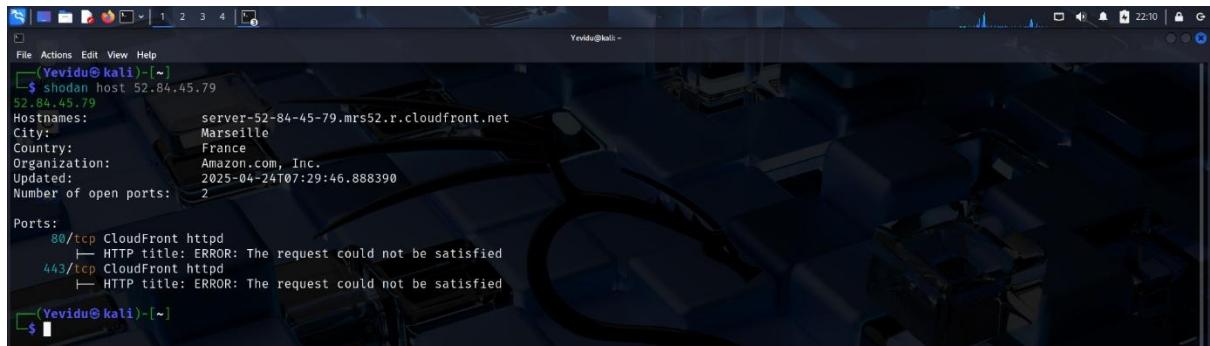
2600:9000:2175: 1800:1d: e80d: 8080:93a1

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



```
File Actions Edit View Help
[Yevidu@kali:~] $ shodan host 52.84.45.79
52.84.45.79
Hostnames: server-52-84-45-79.mrs52.r.cloudfront.net
City: Marseille
Country: France
Organization: Amazon.com, Inc.
Updated: 2025-04-24T07:29:46.888390
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

[Yevidu@kali:~] $
```

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

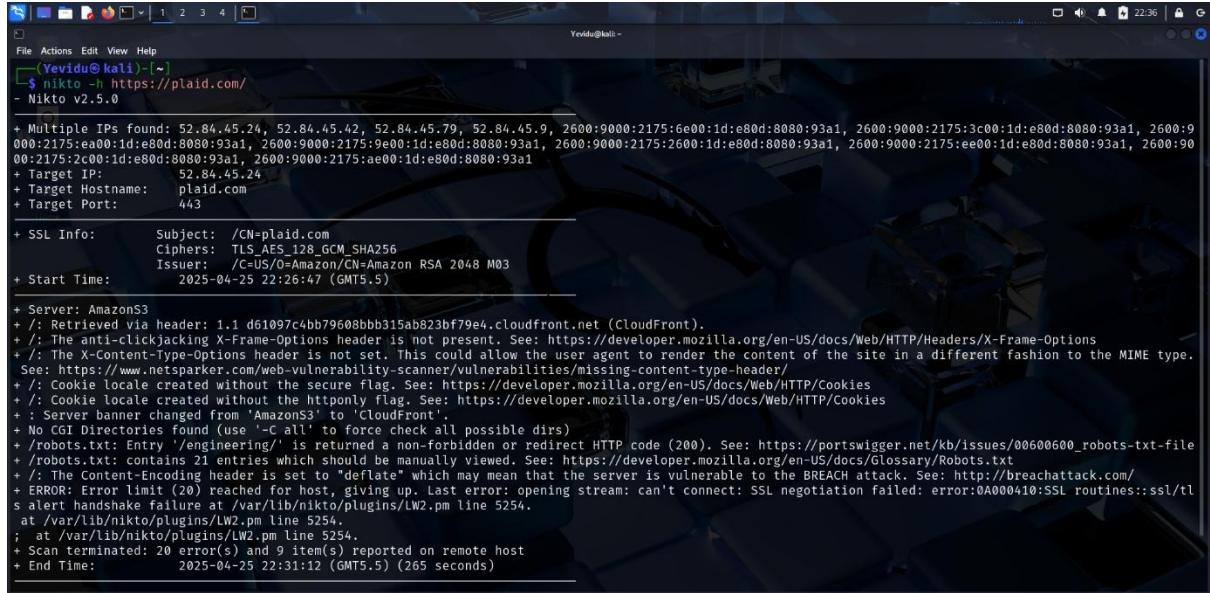
HTTPS (CloudFront) at 443/tcp

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



```
Yevivid@kali: ~]$ nikto -h https://plaid.com/
- Nikto v2.5.0

+ Multiple IPs found: 52.84.45.24, 52.84.45.42, 52.84.45.79, 52.84.45.9, 2600:9000:2175:6e00:1d:e80d:8080:93a1, 2600:9000:2175:3c00:1d:e80d:8080:93a1, 2600:9000:2175:2c00:1d:e80d:8080:93a1, 2600:9000:2175:2600:1d:e80d:8080:93a1, 2600:9000:2175:ee00:1d:e80d:8080:93a1, 2600:9000:2175:2c00:1d:e80d:8080:93a1, 2600:9000:2175:2600:1d:e80d:8080:93a1, 2600:9000:2175:ee00:1d:e80d:8080:93a1, 2600:9000:2175:2c00:1d:e80d:8080:93a1, 2600:9000:2175:2600:1d:e80d:8080:93a1, 2600:9000:2175:ee00:1d:e80d:8080:93a1, 2600:9000:2175:2c00:1d:e80d:8080:93a1, 2600:9000:2175:2600:1d:e80d:8080:93a1, 2600:9000:2175:ee00:1d:e80d:8080:93a1
+ Target IP: 52.84.45.24
+ Target Hostname: plaid.com
+ Target Port: 443

+ SSL Info:
  Subject: /CN=plaid.com
  Ciphers: TLS_AES_128_GCM_SHA256
  Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M03
+ Start Time: 2025-04-25 22:26:47 (GMT5.5)

+ Server: AmazonS3
+ : Retrieved via header: 1.1 d61097c4bb79608bbb315ab823bf79ea.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie locale created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie locale created without the httpOnly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ : Server banner changed from 'AmazonS3' to 'CloudFront'.
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ /robots.txt: Entry '/engineering/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 21 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A00410:SSL routines::ssl/tl
s alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 9 item(s) reported on remote host
+ End Time: 2025-04-25 22:31:12 (GMT5.5) (265 seconds)
```

## 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



The screenshot shows a terminal window on a Kali Linux desktop environment. The user has run the command `nmap plaid.com`. The output of the scan is displayed, showing the host is up with 0.023s latency. It lists other addresses for plaid.com and a CloudFront DNS record. Services found include port 53 (DNS), 80 (HTTP), and 443 (HTTPS). The scan took 8.83 seconds.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 23:02 +0530
Nmap scan report for plaid.com (52.84.45.42)
Host is up (0.023s latency).

Other addresses for plaid.com (not scanned):
 52.84.45.79 52.84.45.24 52.84.45.9 2600:9000:2175:3400:1d:e80d:8080:93a1
 2600:9000:2175:8e00:1d:e80d:8080:93a1
 2600:9000:2175:bao0:1d:e80d:8080:93a1
 2600:9000:2175:3600:1d:e80d:8080:93a1
 2600:9000:2175:4e00:1d:e80d:8080:93a1
 2600:9000:2175:1c00:1d:e80d:8080:93a1
 2600:9000:2175:8600:1d:e80d:8080:93a1

rDNS record for 52.84.45.42: server-52-84-45-42.mrs52.r.cloudfront.net
Not shown: 997 filtered tcp ports (no-response)

PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 8.83 seconds
```

- 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

## 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.

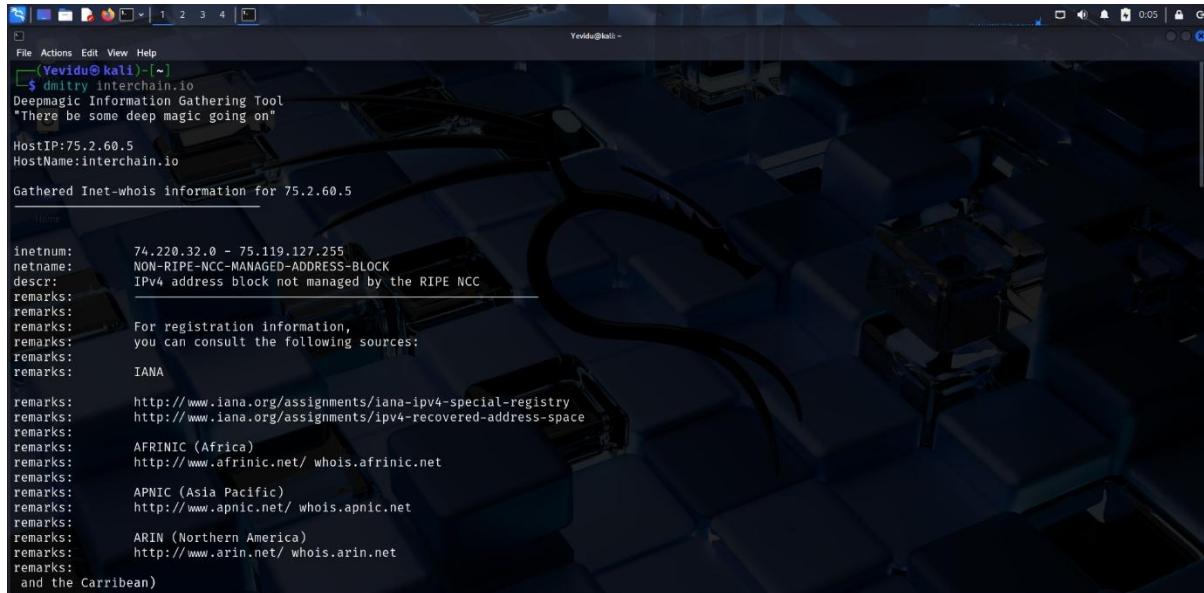
Interchain (<https://interchain.io/>), an open-source ecosystem devoted to facilitating safe communication and interoperability between separate blockchains, is the subject of this Bug Bounty report. The Inter-Blockchain Communication (IBC) protocol, which is the foundation of Interchain's design, enables 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.

The screenshot shows the 'Program highlights' section of the HackerOne platform. It includes contact information (security@interchain.io), adherence to Gold Standard Safe Harbor (fully compliant), response efficiency (above 90%), and a 'Collaboration Enabled' badge. Below this are performance metrics: average time to first response (17 hours), average time to triage (1 day, 19 hours), average time to bounty (2 weeks, 4 days), average time from submission to bounty (2 weeks, 5 days), and average time to resolution (2 weeks, 5 days). To the right, there is a summary for the 'Cosmos' program, showing its URL (https://interchain.io/), social media handles (@cosmos), launch date (May 2018), and response efficiency (97%). A 'Submit report' button is visible.

The screenshot shows the Interchain Foundation website. The top navigation bar includes links for About, Ecosystem, Investments, Advocacy, Technology, and Builders. The 'About' section features the 'INTERCHAIN FOUNDATION' logo. The 'Ecosystem' section contains a large call-to-action banner with the text 'Responsibly shaping a new technological paradigm.' and a 'Work with us' button. The 'News' section below it discusses the ICF's acquisition of Skip and creation of Interchain Labs. The bottom of the page includes a cookie consent banner with 'Accept' and 'Reject' buttons.

# Target Reconnaissance.

## Dmitry Scan

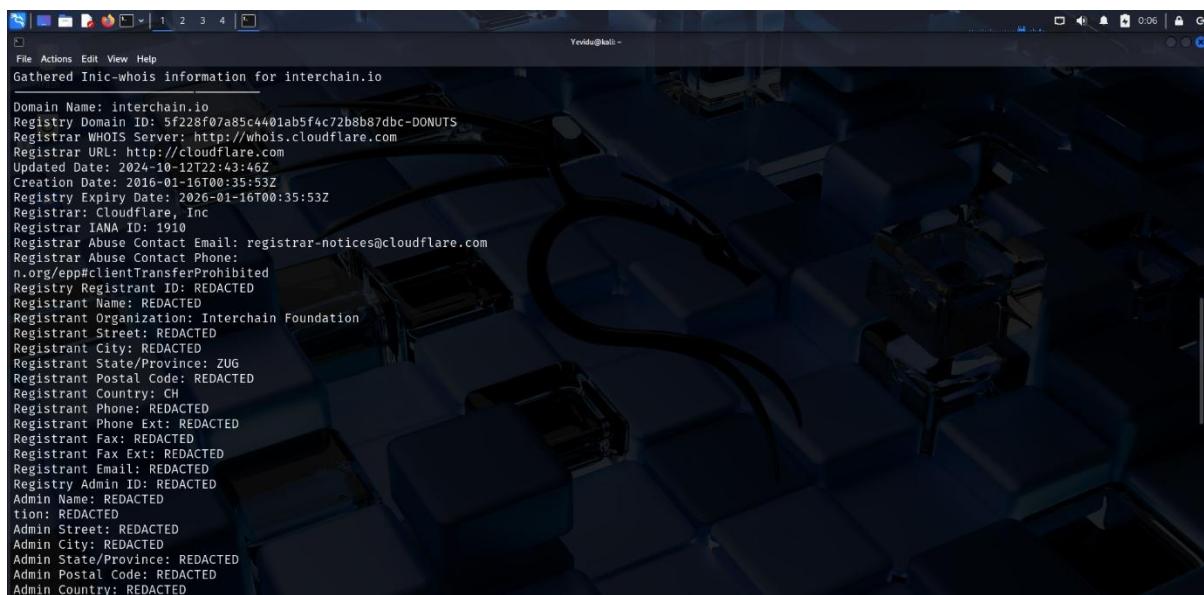


```
(Yevivid@kali)-[~]$ dmitry interchain.io
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:75.2.60.5
HostName:interchain.io

Gathered Inet-whois information for 75.2.60.5

inetnum: 74.220.32.0 - 75.119.127.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks:
remarks: IANA
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks: and the Caribbean)
```



```
(Yevivid@kali)-[~]$ dmitry interchain.io
Gathered Inic-whois information for interchain.io

Domain Name: interchain.io
Registry Domain ID: 5f228f07a85c4401ab5f4c72b8b87dbc-DONUTS
Registrar WHOIS Server: http://whois.cloudflare.com
Registrar URL: http://cloudflare.com
Updated Date: 2024-10-12T22:43:46Z
Creation Date: 2016-01-16T00:35:53Z
Registry Expiry Date: 2026-01-16T00:35:53Z
Registrar: Cloudflare, Inc
Registrar IANA ID: 1910
Registrar Abuse Contact Email: registrar-notices@cloudflare.com
Registrar Abuse Contact Phone: +41 44 506 57 77
n.org/epp#clientTransferProhibited
Registrar Registrant ID: REDACTED
Registrant Name: REDACTED
Registrant Organization: Interchain Foundation
Registrant Street: REDACTED
Registrant City: REDACTED
Registrant State/Province: ZUG
Registrant Postal Code: REDACTED
Registrant Country: CH
Registrant Phone: REDACTED
Registrant Phone Ext: REDACTED
Registrant Fax: REDACTED
Registrant Fax Ext: REDACTED
Registrant Email: REDACTED
Registry Admin ID: REDACTED
Admin Name: REDACTED
Admin Title: REDACTED
Admin Street: REDACTED
Admin City: REDACTED
Admin State/Province: REDACTED
Admin Postal Code: REDACTED
Admin Country: REDACTED
```

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



```
(Yevidu@kali)-[~] $ whatweb interchain.io
http://interchain.io [301 Moved Permanently] Country[UNITED STATES][us], HTTPServer[Netlify], IP[75.2.60.5], RedirectLocation[https://interchain.io/], Uncomm
onHeaders[x-nf-request-id]
https://interchain.io/ [200 OK] Country[UNITED STATES][us], Email[hello@interchain.io], HTML5, HTTPServer[Netlify], IP[75.2.60.5], Open-Graph-Protocol[websit
e], Script[application/json], Strict-Transport-Security[max-age=31536000], Title[Stewarding The Interchain Ecosystem - Interchain Foundation], UncommonHeader
s[cache-status,netlify-vary,x-nf-request-id]
(Yevidu@kali)-[~] $
```

IP: 75.2.60.5 (United States)

Redirect: HTTP (interchain.io) redirects to HTTPS

Web Server: Netlify

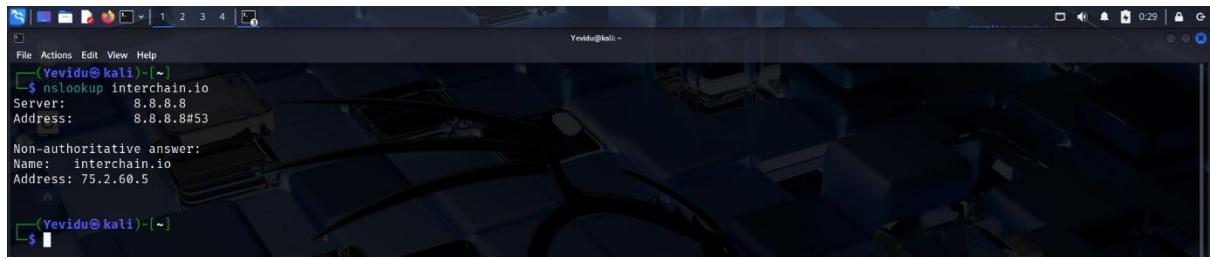
Security Header: Strict-Transport-Security enabled

Email Found: hello@interchain.io

Tech Found: HTML5, Open Graph Protocol

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

## Nslookup

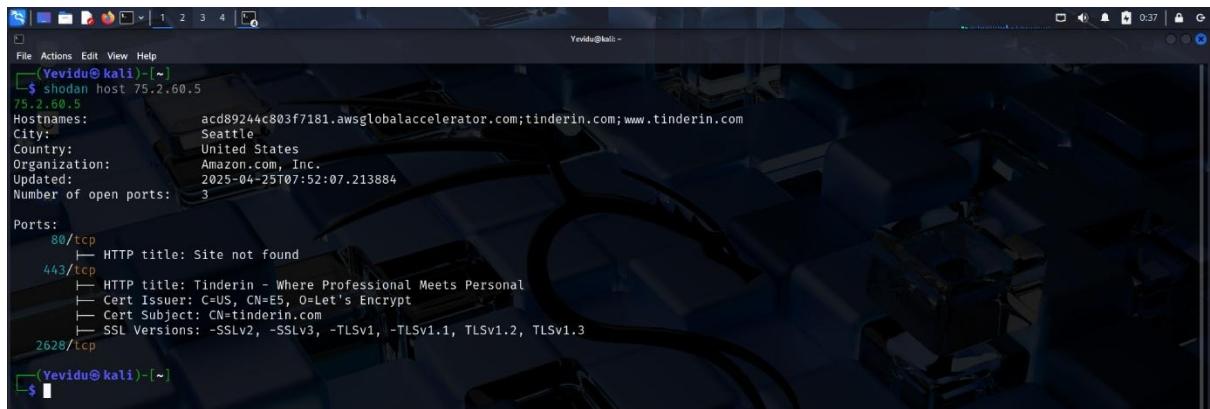


```
(Yevidu@kali)-[~]
$ nslookup interchain.io
Server:     8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
Name:  interchain.io
Address: 75.2.60.5

(Yevidu@kali)-[~]
```

## Shodan



```
(Yevidu@kali)-[~]
$ shodan host 75.2.60.5
75.2.60.5
Hostnames: acd89244c803f7181.awsglobalaccelerator.com;tinderin.com;www.tinderin.com
City: Seattle
Country: United States
Organization: Amazon.com, Inc.
Updated: 2025-04-25T07:52:07.213884
Number of open ports: 3

Ports:
  80/tcp
    └── HTTP title: Site not found
  443/tcp
    └── HTTP title: Tinderin - Where Professional Meets Personal
        └── Cert Issuer: C=US, CN=E5, O=Let's Encrypt
        └── Cert Subject: CN=tinderin.com
        └── SSL Versions: -SSLv2, -SSLv3, -TLSv1.1, TLSv1.2, TLSv1.3
  2628/tcp

(Yevidu@kali)-[~]
```

Location: Seattle, USA

The company is Amazon.com, Inc.

Hostnames:

[www.awsglobalaccelerator.com/acd89244c803f7181](http://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"

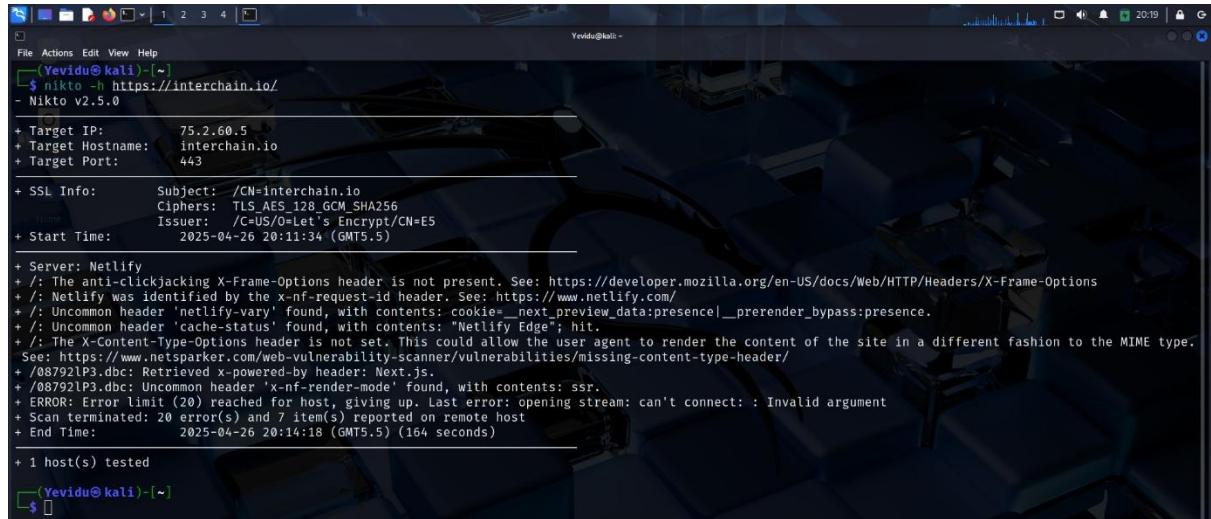
Certificate: Issued by Let's Encrypt for tinderin.com

SSL Support: TLS 1.2 and TLS 1.3 only

Updated on April 25, 2025

## Scanning and vulnerability identification.

### Nikto



```
(Yevidu㉿kali)-[~]$ nikto -h https://interchain.io/
- Nikto v2.5.0
+ Target IP: 75.2.60.5
+ Target Hostname: interchain.io
+ Target Port: 443
+ SSL Info: Subject: /CN=interchain.io
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=Let's Encrypt/CN=E5
+ Start Time: 2025-04-26 20:11:34 (GMT5.5)

+ Server: Netlify
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Netlify was identified by the x-nf-request-id header. See: https://www.netlify.com/
+ /: Uncommon header 'netlify-vary' found, with contents: cookie=_next_preview_data:presence:_prerender_bypass:presence.
+ /: Uncommon header 'cache-status' found, with contents: "Netlify Edge"; hit.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /08792lP3.dbc: Retrieved x-powered-by header: Next.js.
+ /08792lP3.dbc: Uncommon header 'x-nf-render-mode' found, with contents: ssr.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: : Invalid argument
+ Scan terminated: 20 error(s) and 7 item(s) reported on remote host
+ End Time: 2025-04-26 20:14:18 (GMT5.5) (164 seconds)

+ 1 host(s) tested
(Yevidu㉿kali)-[~]$
```

- SSL Certificate:

Subject: CN=interchain.io

Issuer: Let's Encrypt

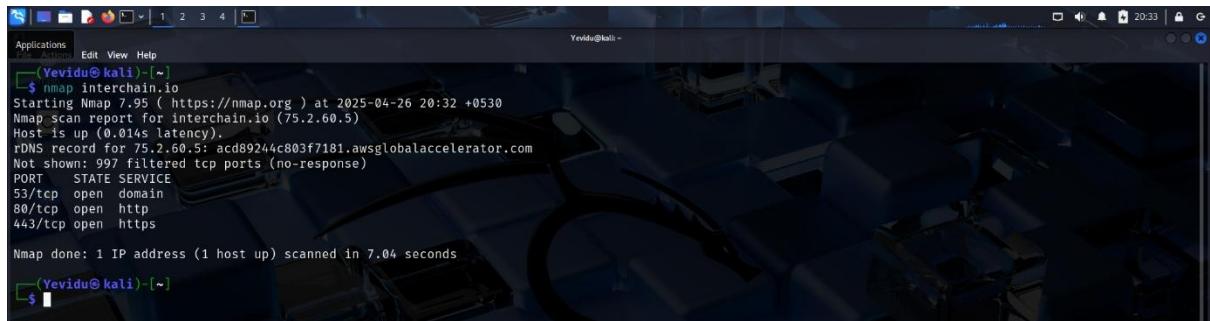
Cipher: TLS\_AES\_128\_GCM\_SHA256

- 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



```
(Yevidu@kali)-[~]$ nmap interchain.io
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 20:32 +0530
Nmap scan report for interchain.io (75.2.60.5)
Host is up (0.014s latency).
rDNS record for 75.2.60.5: acd89244c803f7181.awsglobalaccelerator.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 7.04 seconds
(Yevidu@kali)-[~]$
```

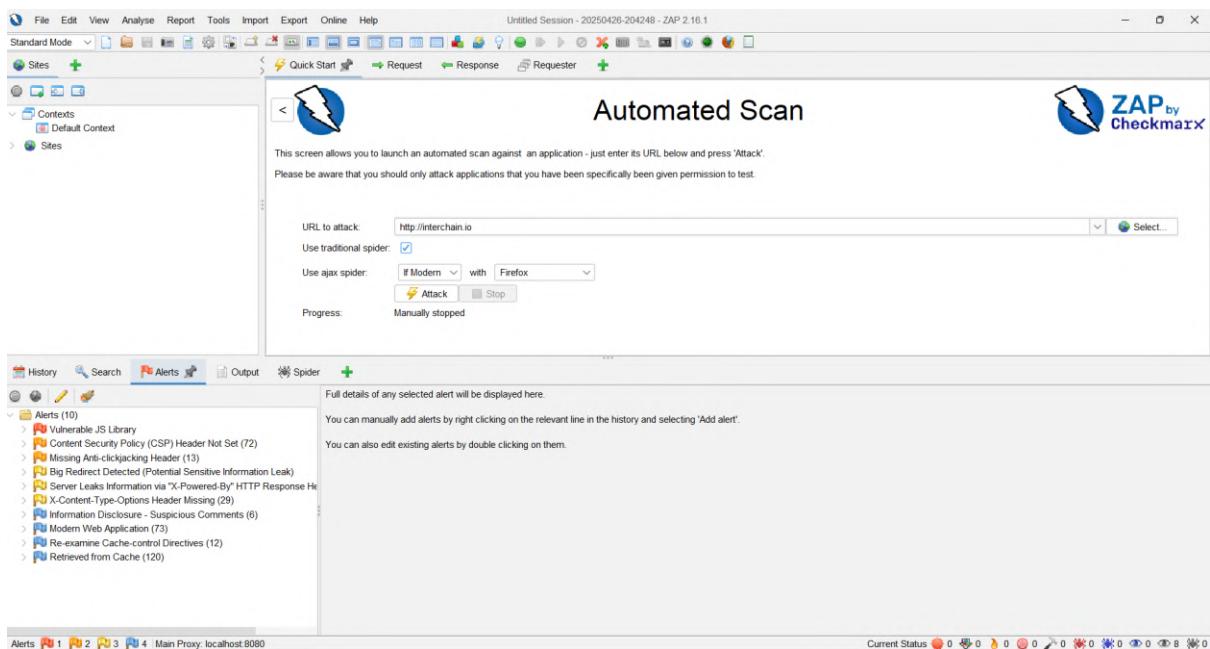
Ports Open:

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



The screenshot shows the OWASP ZAP interface with an "Automated Scan" dialog open. The URL to attack is set to `http://interchain.io`. The "Attack" button is highlighted. On the left, the "Alerts" panel lists 10 vulnerabilities, including "Vulnerable JS Library", "Content Security Policy (CSP) Header Not Set", and "Missing Anti-clickjacking Header". The bottom status bar shows "Current Status" with various icons.

The screenshot shows the ZAP 2.16.1 interface with an 'Automated Scan' in progress. The 'Alerts' tab is active, showing 10 vulnerabilities. One specific alert is expanded, detailing a 'Content Security Policy (CSP) Header Not Set' issue. The alert includes parameters, evidence (CWE ID 693, WASC ID 15), source (Passive (10038 - Content Security Policy (CSP) Header Not Set)), and an alert reference (10038-1). The expanded alert also shows a detailed description of CSP and its purpose.

## 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.

The top screenshot shows the Bug Bounty program page on HackerOne. It includes sections for Introduction, Program highlights, and Rewards. Key highlights from the program highlights section include:

- Gold Standard: Adheres to Gold Standard Safe Harbor.
- Platform Standards: Fully compliant with Platform Standards.
- Top Response Efficiency: This program's response efficiency is above 90%.

The rewards section shows two levels: Low (\$1,000) and Medium (\$2,000). The bottom screenshot shows the main homepage of coinspot.com.au. It features a navigation bar with links to HOME, WALLETS, BUY/SELL, SWAP, BUNDLES, NFT, OTC, MARKETS, REGISTER, and LOGIN. The main content area includes a 'CoinSpot' logo, a call-to-action 'Buy, Sell & Swap Cryptocurrency', and a 'Trending Coins' section displaying the following data:

COIN	LAST HR	RATE
Bitcoin (BTC)	0.15%	\$149,396.07
Litecoin (LTC)	0.43%	\$138.96
Ethereum (ETH)	0.20%	\$2,886.64
Solana (SOL)	0.15%	\$239.38
Cardano (ADA)	0.16%	\$1,139.850

A note at the bottom of the trending coins section states: "530+ more coins".

# Target Reconnaissance.

## Dmitry Scan

```
$ dmitry coinspot.com.au
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:172.67.1.80
HostName:coinspot.com.au

Gathered Inet-whois information for 172.67.1.80

inetnum: 171.76.0.0 - 172.80.127.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks:
remarks: ARIN (Northern America)
rin.net
remarks:
remarks: LACNIC (Latin America and the Caribbean)
```

```
% This query was served by the RIPE Database Query Service version 1.117 (ABERDEEN)

Gathered Inic-whois information for coinspot.com.au

Domain Name: coinspot.com.au
Registry Domain ID: cf71be02768544b99663487f8f30e6d4-AU
Registrar WHOIS Server: whois.auda.org.au
Registrar URL: https://www.godaddy.com/en-au/contact-us
Last Modified: 2024-12-09T00:31:25Z
Registrar Name: GoDaddy.com LLC trading as GoDaddy.com
Registrar Abuse Contact Email: domainops@godaddy.com
Registrar Abuse Contact Phone: +61.6028177308
Reseller Name:
ted
Status: serverRenewProhibited https://identitydigital.au/get-au/whois-status-codes#serverRenewProhibited
Status Reason: Not Currently Eligible For Renewal
Status: clientUpdateProhibited https://identitydigital.au/get-au/whois-status-codes#clientUpdateProhibited
Registrant Contact ID: 9d5025c82db54af4b1343cb17cc354f-AU
Registrant Contact Name: Russell Wilson
Tech Contact ID: 8ea9ed95de854321a35cae38e81751bd-AU
Tech Contact Name: Russell Wilson
Name Server: erin.ns.cloudflare.com
Name Server: thomas.ns.cloudflare.com
DNSSEC: unsigned
Registrant: caracamp
Registrant ID: ABN 98939062695
Eligibility Type: Sole Trader
>>> Last update of WHOIS database: 2025-04-26T15:44:01Z <<
```

Identity Digital Australia Pty Ltd, for itself and on behalf of .au Domain Administration Limited (auDA), makes the WHOIS registration data directory service (WHOIS Service) available solely for the purposes of:

The terminal window shows the following output:

```
Yevidu@Kali: ~
File Actions Edit View Help
accordance with the auDA WHOIS Policy (available at https://www.audac.org.au/policy/2014-07-whois-policy).

Gathered Netcraft information for coinspot.com.au

Retrieving Netcraft.com information for coinspot.com.au
Netcraft.com Information gathered

Gathered Subdomain information for coinspot.com.au

Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host coinspot.com.au, Searched 0 pages containing 0 results

Gathered E-Mail information for coinspot.com.au

Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host coinspot.com.au, Searched 0 pages containing 0 results

Gathered TCP Port information for 172.67.1.80

Port      State
53/tcp    open
80/tcp    open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting
[Yevidu@Kali: ~]
```

**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.

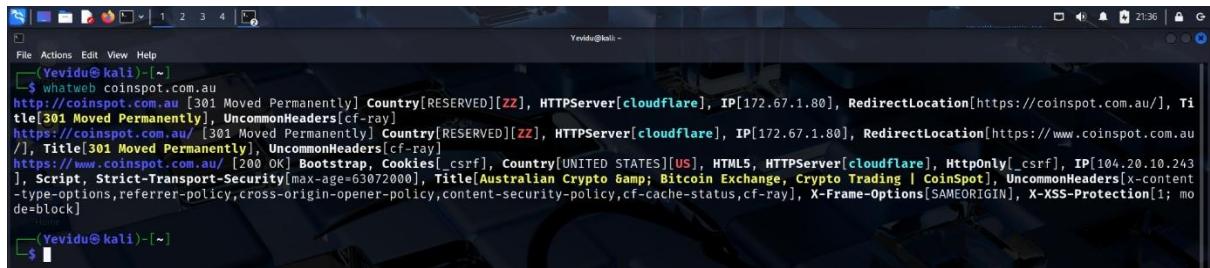
#### **Scan of TCP Ports:**

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



```
Yevidu@kali:~$ whatweb coinspot.com.au
http://coinspot.com.au [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[cloudflare], IP[172.67.1.80], RedirectLocation[https://coinspot.com.au/], Title[301 Moved Permanently], UncommonHeaders[cf-ray]
https://coinspot.com.au/ [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[cloudflare], IP[172.67.1.80], RedirectLocation[https://www.coinspot.com.au/], Title[301 Moved Permanently], UncommonHeaders[cf-ray]
https://www.coinspot.com.au/ [200 OK] Bootstrap, Cookies[_csrf], Country[UNITED STATES][US], HTML5, HTTPServer[cloudflare], HttpOnly[_csrf], IP[104.20.10.243], Script, Strict-Transport-Security[max-age=63072000], Title[Australian Crypto & Bitcoin Exchange, Crypto Trading | CoinSpot], UncommonHeaders[x-content-type-options,referrer-policy,cross-origin-opener-policy,content-security-policy,cf-cache-status,cf-ray], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]
Yevidu@kali:~$
```

## 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).

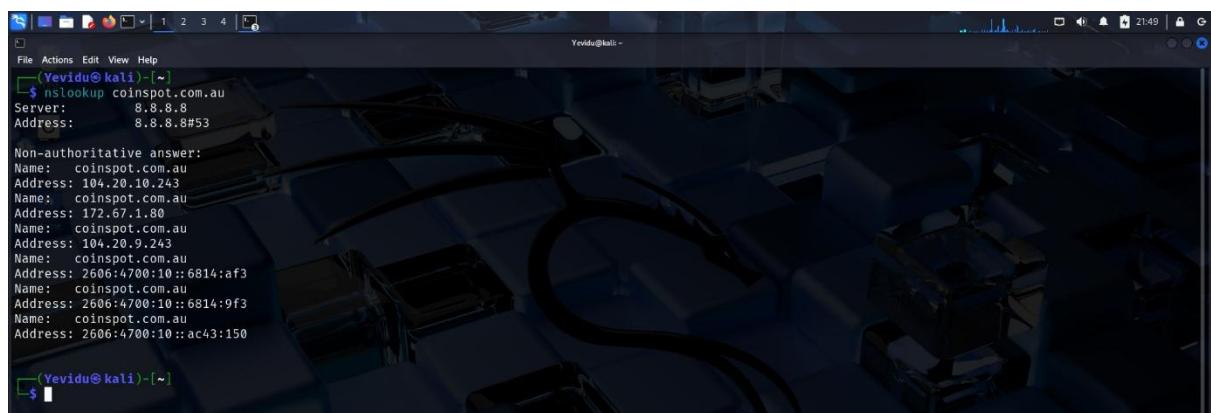
## Location:

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



```
Yevidu@kali:~]$ nslookup coinspot.com.au
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: coinspot.com.au
Address: 104.20.10.243
Name: coinspot.com.au
Address: 172.67.1.80
Name: coinspot.com.au
Address: 104.20.9.243
Name: coinspot.com.au
Address: 2606:4700:10::6814:af3
Name: coinspot.com.au
Address: 2606:4700:10::6814:9f3
Name: coinspot.com.au
Address: 2606:4700:10::ac43:150

Yevidu@kali:~]$
```

**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

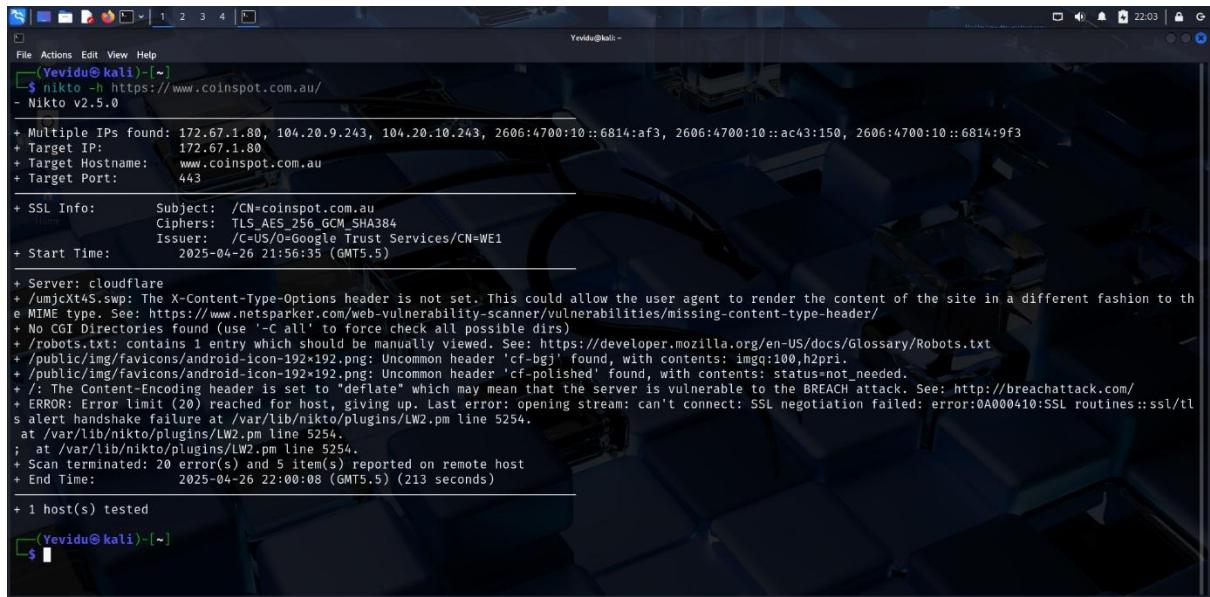
**Remarks:**

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



```
Yevidu@kali:~$ nikto -h https://www.coinspot.com.au/
- Nikto v2.5.0

+ Multiple IPs found: 172.67.1.80, 104.20.9.243, 104.20.10.243, 2606:4700:10::6814:af3, 2606:4700:10::ac43:150, 2606:4700:10::6814:9f3
+ Target IP: 172.67.1.80
+ Target Hostname: www.coinspot.com.au
+ Target Port: 443

+ SSL Info: Subject: /CN=coinspot.com.au
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=Google Trust Services/CN=WE1
+ Start Time: 2025-04-26 21:56:35 (GMT+5.5)

+ Server: cloudflare
+ /umjcXt4S.swp: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /public/img/favicons/android-icon-192x192.png: Uncommon header 'cf-bgi' found, with contents: imgg:100,h2pri.
+ /public/img/favicons/android-icon-192x192.png: Uncommon header 'cf-polished' found, with contents: status:not_needed.
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/tl
s alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time: 2025-04-26 22:00:08 (GMT+5.5) (213 seconds)

+ 1 host(s) tested

Yevidu@kali:~$
```

### 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

```
Yevidu@kali:~$ nmap coinspot.com.au
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 22:07 +0530
Nmap scan report for coinspot.com.au (104.20.9.243)
Host is up (0.017s latency).
Other addresses for coinspot.com.au (not scanned): 172.67.1.80 104.20.10.243 2606:4700:10::6814:9f3 2606:4700:10::6814:af3 2606:4700:10::ac43:150
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.49 seconds
```

## 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

The screenshot shows the OWASP ZAP interface with a session titled "Untitled Session - 20250426-222033 - ZAP 2.16.1". The main pane displays a spidering configuration for "https://www.coinspot.com.au". The "Spider" tab is active, showing a progress bar at 100% completion. The "Alerts" tab on the left shows 14 alerts, including "Absence of Anti-CSRF Tokens (4)", "CSP Failure to Define Directive with No Fallback (106)", and "Vulnerable JS Library". The bottom status bar indicates "Current Status" with various icons.

Screenshot of ZAP 2.16.1 showing an alert for 'Absence of Anti-CSRF Tokens'.

**Header Text**

```
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">
  <div class="grid">
    <div class="col-lg-6 v-lg-middle text-center text-lg-left">
      <h2 class="section-heading mb-30"><span class="gradient-text-1">Register</span> your interest</h2>
      <p class="text-default mb-20">Register interest if you want more information or to discuss with an OTC professional.</p>
    </div>
    <div class="o-hidden o-lg-block">
      <form class="form-validate" role="form" action="#" method="POST">
```

**Alerts (14)**

- Absence of Anti-CSRF Tokens (4)
  - GET: https://www.comspot.com.au/otc
  - GET: https://www.comspot.com.au/otc
  - GET: https://www.comspot.com.au/msf
  - GET: https://www.comspot.com.au/msf
- 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)
- Modem Web Application (117)
- Re-examine Cache-control Directives (2)
- Retrieved from Cache (65)
- Session Management Response Identified (7)

**Absence of Anti-CSRF Tokens**

URL: https://www.comspot.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 (XSS) is an attack that injects malicious code into a web page viewed by a user, allowing the attacker to steal sensitive information or manipulate the user's session.  
 Other Info:  
 No known Anti-CSRF token [anticarf, CSRFToken, \_RequestVerificationToken, carfmiddlewareToken, authenticity\_token, OWASP\_CSRFTOKEN, anoncarf, 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

## 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-Secure Headers
  - 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.

The screenshot shows the Aleo bug bounty program page on the HackerOne platform. The left sidebar includes links for Security page, Program guidelines (which is selected), Scope, Hacktivity, Thanks, Updates, Collaborators, and Safe harbor. The main content area displays 'Program highlights' with two sections: 'Gold Standard' (Adheres to Gold Standard Safe Harbor) and 'Platform Standards' (Fully compliant with Platform Standards). It also shows that the program is 'Managed by HackerOne', 'Collaboration Enabled', and 'Includes Retesting'. Below this are four boxes showing response times: '3 days, 6 hours' (Average time to first response), '1 month, 1 week' (Average time to triage), 'N/A' (Average time to bounty), and '1 month, 1 week' (Average time from submission to bounty). A 'Rewards summary' section indicates that last updated on May 28, 2024, with changes. It lists severities: P4 / Low (Avg. bounty \$1,000, 15.56% submissions), P3 / Medium (Avg. bounty n/a, 24.44% submissions), P2 / High (Avg. bounty n/a, 13.33% submissions), and P1 / Critical (Avg. bounty \$65,000, 46.67% submissions). To the right, there's a sidebar for Aleo, which includes its logo, URL (<https://aleo.org>), handle (@aleohq), a brief description (Aleo is a developer platform that uses zero-knowledge technology to enable decentralized apps that are private, programmable, secure, and scalable.), and a note about the bug bounty program launching in July 2023. It also shows a response efficiency of 68%. A 'Submit report' button is located at the bottom of the sidebar.

The screenshot shows the Aleo homepage. The top navigation bar includes 'Build', 'Discover', 'Contribute', and 'Network'. The main headline reads 'Zero-Knowledge. Zero Compromises.' Below it is the subtext 'Build cryptographically secure dApps at scale'. A 'START BUILDING' button with a plus sign is centered. The background features a dark, abstract pattern of dots.

# Target Reconnaissance.

## Dmitry Scan

```
(Yevivid@kali)-[~]$ dmitry aleo.org
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:75.2.60.5
HostName:aleo.org

Gathered Inet-whois information for 75.2.60.5

inetnum: 74.220.32.0 - 75.119.127.255
ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
-space
remarks:
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks:
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks:
remarks: LACNIC (Latin America and the Caribbean)
```

```
(Yevivid@kali)-[~]$ dmitry aleo.org
Registrant Phone Ext: REDACTED
Registrant Fax: REDACTED
Registrant Fax Ext: REDACTED
Registrant Email: REDACTED
Registry Admin ID: REDACTED
Admin Name: REDACTED
n Organization: REDACTED
Admin Street: REDACTED
Admin City: REDACTED
Admin State/Province: REDACTED
Admin Postal Code: REDACTED
Admin Country: REDACTED
Admin Phone: REDACTED
Admin Phone Ext: REDACTED
Admin Fax: REDACTED
Admin Fax Ext: REDACTED
Admin Email: REDACTED
Registry Tech ID: REDACTED
Tech Name: REDACTED
Tech Organization: REDACTED
Tech Street: REDACTED
Tech City: REDACTED
Tech State/Province: REDACTED
REDACTED
Tech Country: REDACTED
Tech Phone: REDACTED
Tech Phone Ext: REDACTED
Tech Fax: REDACTED
Tech Fax Ext: REDACTED
Tech Email: REDACTED
Name Server: darl.ns.cloudflare.com
Name Server: rosalie.ns.cloudflare.com
DNSSEC: signedDelegation
URL of the ICANN Whois Inaccuracy Complaint Form: https://icann.org/wicf/
>>> Last update of WHOIS database: 2025-04-26T17:54:54Z <<
```

## 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



```
File Actions Edit View Help
[Yevidu@kali:~]$ whatweb aleo.org
http://aleo.org [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Netlify], IP[75.2.60.5], RedirectLocation[https://aleo.org/], UncommonHeaders[x-nf-request-id]
https://aleo.org/ [200 OK] Access-Control-Allow-Methods[PUT], Country[UNITED STATES][US], HTML5, HTTPServer[Netlify], IP[75.2.60.5], Matomo, MetaGenerator[Gatsby 5.13.4], Script[application/ld+json,module,text/javascript], Strict-Transport-Security[max-age=31536000], UncommonHeaders[access-control-allow-methods,access-control-allow-origin,cache-status,referrer-policy,x-content-type-options,x-nf-request-id], X-Frame-Options[DENY], X-UA-Compatible[ie=edge], X-XSS-Protection[1; mode=block]
[Yevidu@kali:~]$
```

## 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:

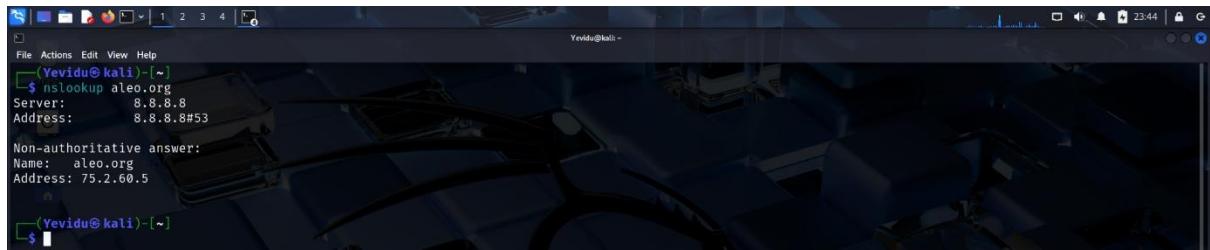
HTML5: HTML5 is used by the website.

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



```
(Yevidu㉿kali)-[~]$ nslookup aleo.org
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:  aleo.org
Address: 75.2.60.5

(Yevidu㉿kali)-[~]$
```

Server: 8.8.8.8

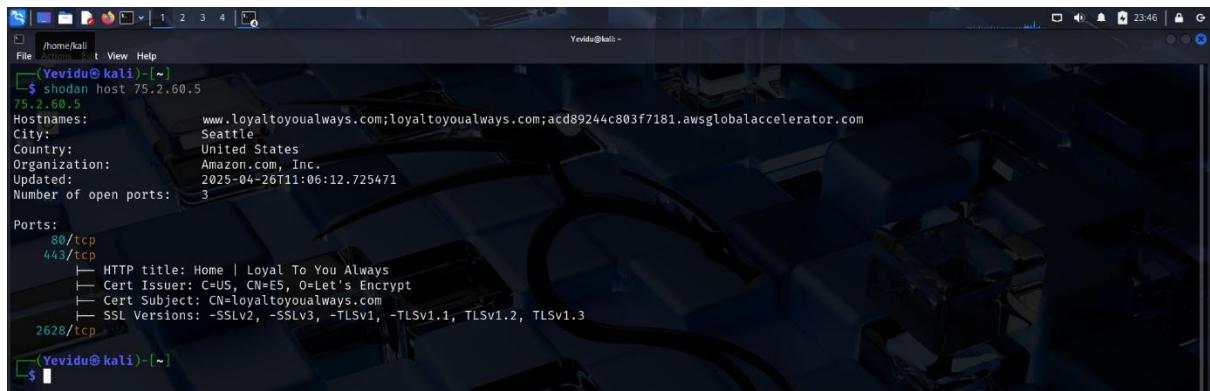
Address: 8.8.8.8#53

Non-authoritative answer:

Name: aleo.org

Address: 75.2.60.5

## Shodan



```
(Yevidu㉿kali)-[~]$ shodan host 75.2.60.5
75.2.60.5
Hostnames: www.loyaltoyoualways.com;loyaltoyoualways.com;acd89244c803f7181.awsglobalaccelerator.com
City: Seattle
Country: United States
Organization: Amazon.com, Inc.
Updated: 2025-04-26T11:06:12.725471
Number of open ports: 3

Ports:
  80/tcp
  443/tcp
    HTTP title: Home | Loyal To You Always
    Cert Issuer: C=US, CN=E5, O=Let's Encrypt
    Cert Subject: CN=loyaltoyoualways.com
    SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2, TLSv1.3
  2628/tcp

(Yevidu㉿kali)-[~]$
```

### 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

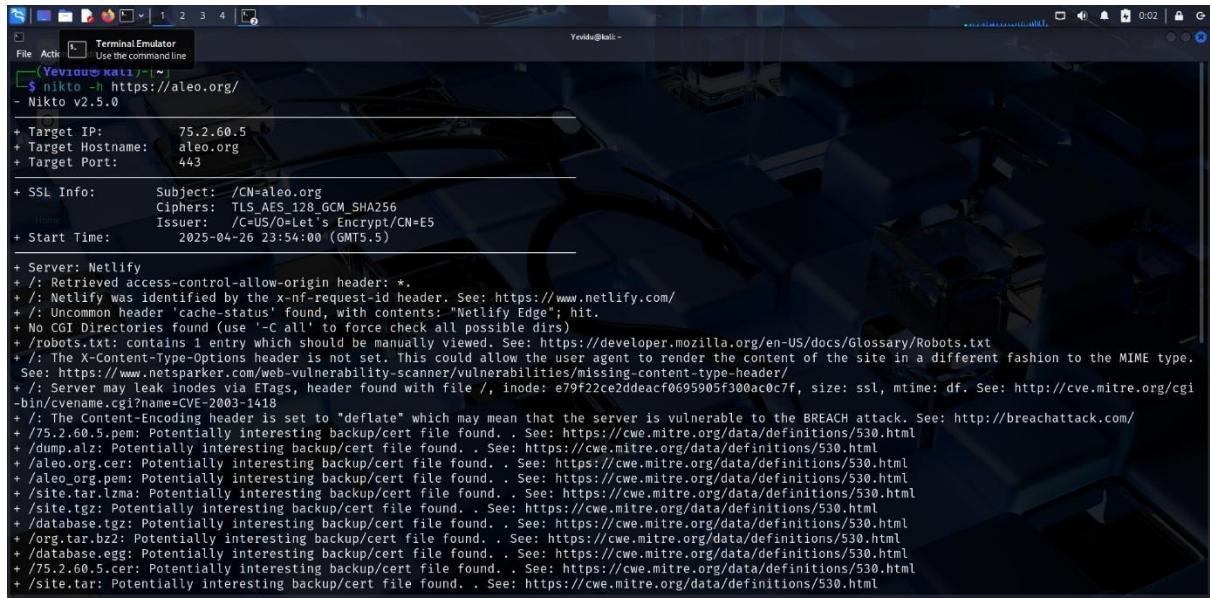
Let's Encrypt is the SSL certificate issuer (CN=E5, O=Let's Encrypt).

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



```
(Yevdus@Kali)-~]$ nikto -h https://aleo.org/
- Nikto v2.5.0
+ Target IP: 75.2.60.5
+ Target Hostname: aleo.org
+ Target Port: 443
+ SSL Info: Subject: /CN=aleo.org
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=Let's Encrypt/CN=E5
+ Start Time: 2025-04-26 23:54:00 (GMT5.5)

+ Server: Netlify
+ /: Retrieved access-control-allow-origin header: *.
+ /: Netlify was identified by the x-nf-request-id header. See: https://www.netlify.com/
+ /: Uncommon header 'cache-status' found, with contents: "Netlify Edge"; hit.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Server may leak inodes via ETags, header found with file /, inode: e79f22ce2ddeacf0f695905f300ac0c7f, size: ssl, mtime: df. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ /75.2.60.5.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /aleo.org.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /aleo.org.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /org.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /75.2.60.5.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
```

## 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



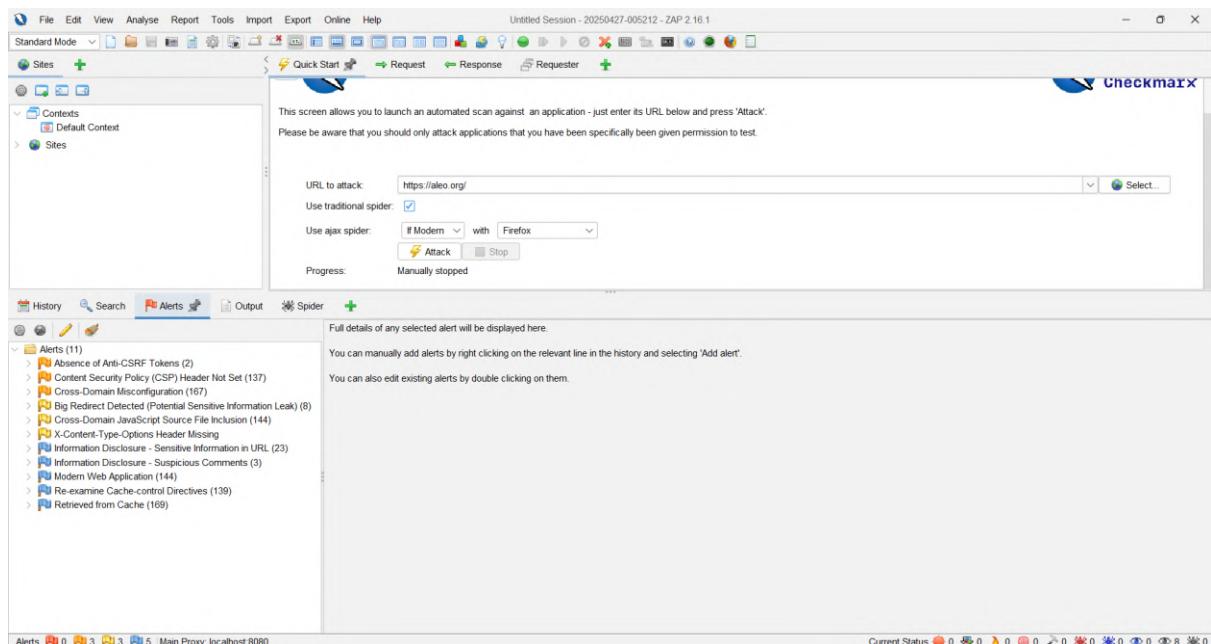
```
(Yevidu@kali)-[~]
$ nmap aleo.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 00:10 +0530
Nmap scan report for aleo.org (75.2.60.5)
Host is up (0.018s latency).
rDNS record for 75.2.60.5: acd89244c803f7181.awsglobalaccelerator.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 25.95 seconds
(Yevidu@kali)-[~]
```

## Open Ports

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

## OWASP ZAP



The screenshot shows the OWASP ZAP interface in Standard Mode. The main panel displays a configuration for an automated scan against the URL <https://aleo.org/>. The "Attack" button is highlighted. The left sidebar shows a tree view of contexts and sites, with "Alerts" expanded to show 11 items. The bottom status bar indicates "Current Status" with various icons.

The screenshot shows the ZAP 2.16.1 interface. At the top, the menu bar includes File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help, and Standard Mode. Below the menu is a toolbar with icons for various functions like Site Scan, Request, Response, and Spider. The main window has tabs for Header Text and Body Text. On the left, there's a tree view under Contexts with a Default Context node. The right side displays a detailed alert message:

**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 (XSS) attacks exploit the trust that a web site has for a user.  
Other Info:  
No known Anti-CSRF token [anticsrf, CSRFToken, \_RequestVerificationToken, csrfmiddlewaretoken, authenticity\_token, OWASP\_CSRFTOKEN, antoncsrf, 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  
This is a critical flaw or framework that does not allow this weakness to occur or provides protection that makes this weakness easier to avoid.

At the bottom, there are buttons for Alerts, History, Search, Output, and Spider. The status bar shows 'Current Status' with various icons and counts (e.g., 0 errors, 0 warnings, 0 info).

## 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:**

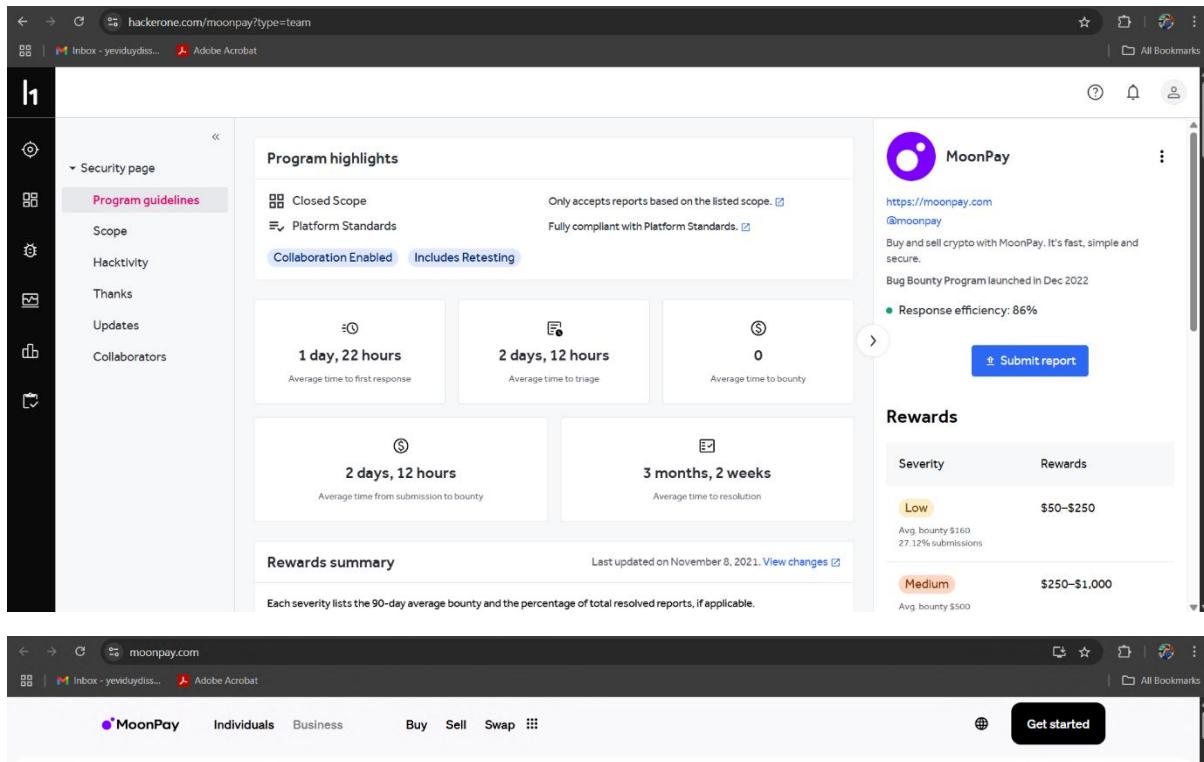
- Attackers can steal private information from HTTPS traffic by taking advantage of compression side-channels.

**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.



The screenshot shows the 'Program guidelines' section of the MoonPay bug bounty program on the HackerOne platform. It highlights the following key metrics:

- Closed Scope: Only accepts reports based on the listed scope.
- Platform Standards: Fully compliant with Platform Standards.
- Collaboration Enabled: Includes Retesting.

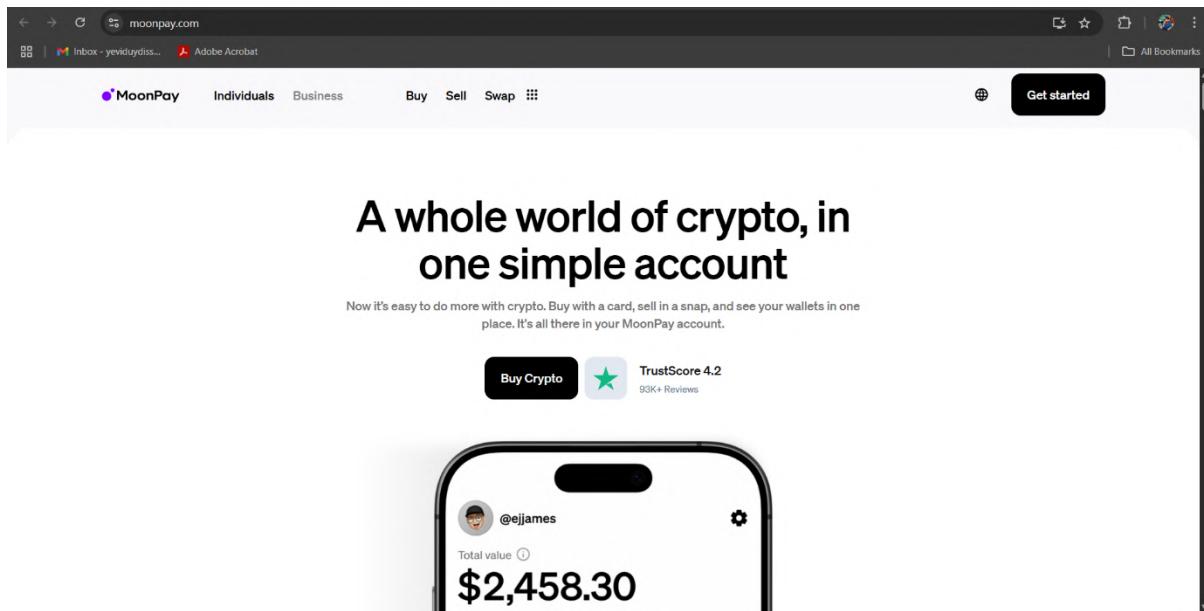
Performance metrics include:

- Average time to first response: 1 day, 22 hours.
- Average time to triage: 2 days, 12 hours.
- Average time to bounty: 0.
- Average time from submission to bounty: 2 days, 12 hours.
- Average time to resolution: 3 months, 2 weeks.

Rewards summary table:

Severity	Rewards
Low	\$50-\$250 Avg. bounty \$160 27.12% submissions
Medium	\$250-\$1,000 Avg. bounty \$500

A 'Submit report' button is visible on the right.

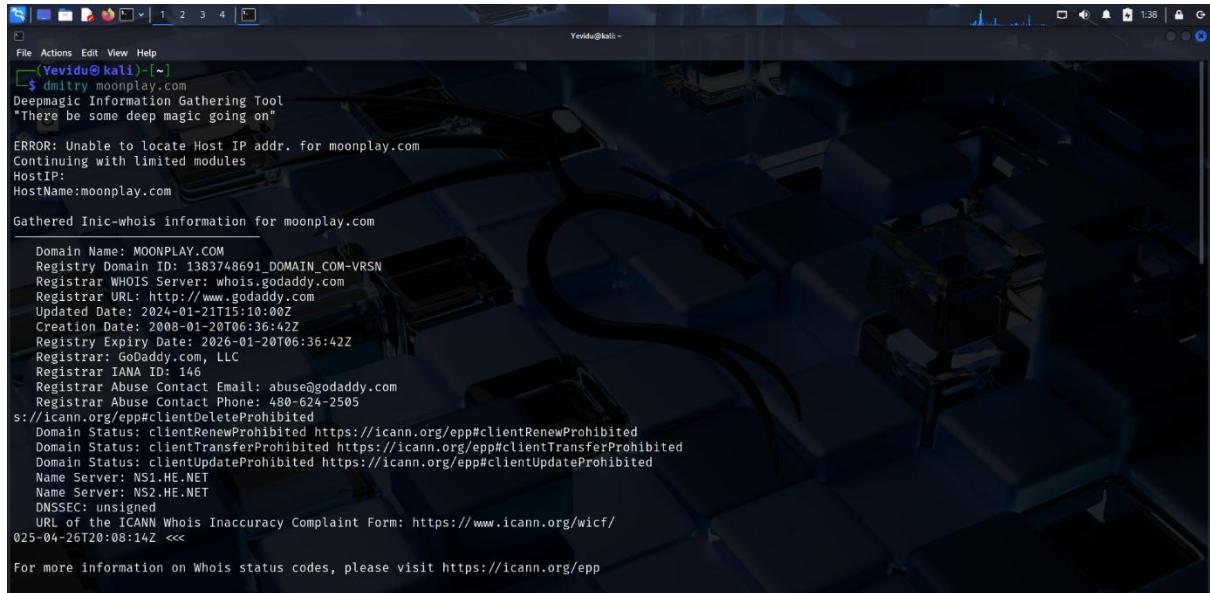


The screenshot shows the MoonPay website homepage. The main headline reads: "A whole world of crypto, in one simple account". Below the headline, a subtext states: "Now it's easy to do more with crypto. Buy with a card, sell in a snap, and see your wallets in one place. It's all there in your MoonPay account." A "Get started" button is located on the right.

Below the headline, there are three buttons: "Buy Crypto", "TrustScore 4.2", and "93K+ Reviews". A smartphone icon displays a profile picture (@ejjames) and a total value of "\$2,458.30".

# Target Reconnaissance.

## Dmitry Scan

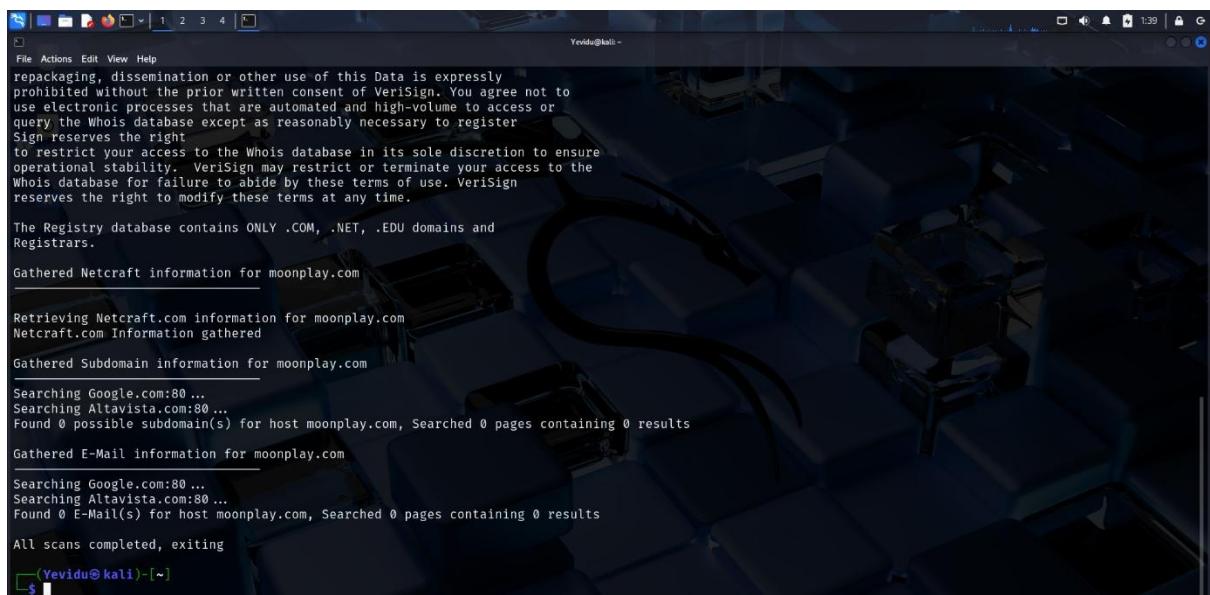


```
(Yevidu㉿kali)-[~]
$ dmitry moonplay.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host IP addr. for moonplay.com
Continuing with limited modules
HostIP:
HostName:moonplay.com

Gathered Inic-whois information for moonplay.com
Domain Name: MOONPLAY.COM
Registry Domain ID: 1383748691_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2024-01-21T15:10:00Z
Creation Date: 2008-01-20T06:36:42Z
Registry Expiry Date: 2026-01-20T06:36:42Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
s://icann.org/epp#clientRenewProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS1.HE.NET
Name Server: NS2.HE.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
025-04-26T20:08:14Z <<

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



```
(Yevidu㉿kali)-[~]
File Actions Edit View Help
Yevidu㉿kali ~
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
Sign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

Gathered Netcraft information for moonplay.com

Retrieving Netcraft.com information for moonplay.com
Netcraft.com Information gathered

Gathered Subdomain information for moonplay.com
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host moonplay.com, Searched 0 pages containing 0 results

Gathered E-Mail information for moonplay.com
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host moonplay.com, Searched 0 pages containing 0 results

All scans completed, exiting
(Yevidu㉿kali)-[~]
$
```

**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

```
(Yevidu@kali)-[~]$ dmitry moonplay.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host IP addr. for moonplay.com
Continuing with limited modules
HostIP:
HostName:moonplay.com

Gathered Inic-whois information for moonplay.com
Domain Name: MOONPLAY.COM
Registry Domain ID: 1383748691_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2024-01-21T15:10:00Z
Creation Date: 2008-01-20T06:36:42Z
Registry Expiry Date: 2026-01-20T06:36:42Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
s://icann.org/epp#clientRenewProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS1.HE.NET
Name Server: NS2.HE.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
025-04-26T20:08:14Z <<

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

```
(Yevidu@kali)-[~]$ dmitry moonplay.com
Deepmagic Information Gathering Tool
There be some deep magic going on

repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register
Sign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Gathered Netcraft information for moonplay.com
_____
Retrieving Netcraft.com information for moonplay.com
Netcraft.com Information gathered

Gathered Subdomain information for moonplay.com
_____
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host moonplay.com, Searched 0 pages containing 0 results

Gathered E-Mail information for moonplay.com
_____
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host moonplay.com, Searched 0 pages containing 0 results

All scans completed, exiting

(Yevidu@kali)-[~]$
```

## 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, \_cfuvild, and \_\_cf\_bm headers.

### **Compression Activated:**

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

## **Nmap**

```
Yevidu@kali:~$ nmap moonpay.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 02:13 +0530
Nmap scan report for moonpay.com (104.18.0.134)
Host is up (0.019s latency).
Other addresses for moonpay.com (not scanned): 104.18.1.134 2606:4700::6812:186 2606:4700::6812:86
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.69 seconds
```

### **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.



