Sri Lanka Institute of Information Technology

WEB SECURITY

(IE2062)

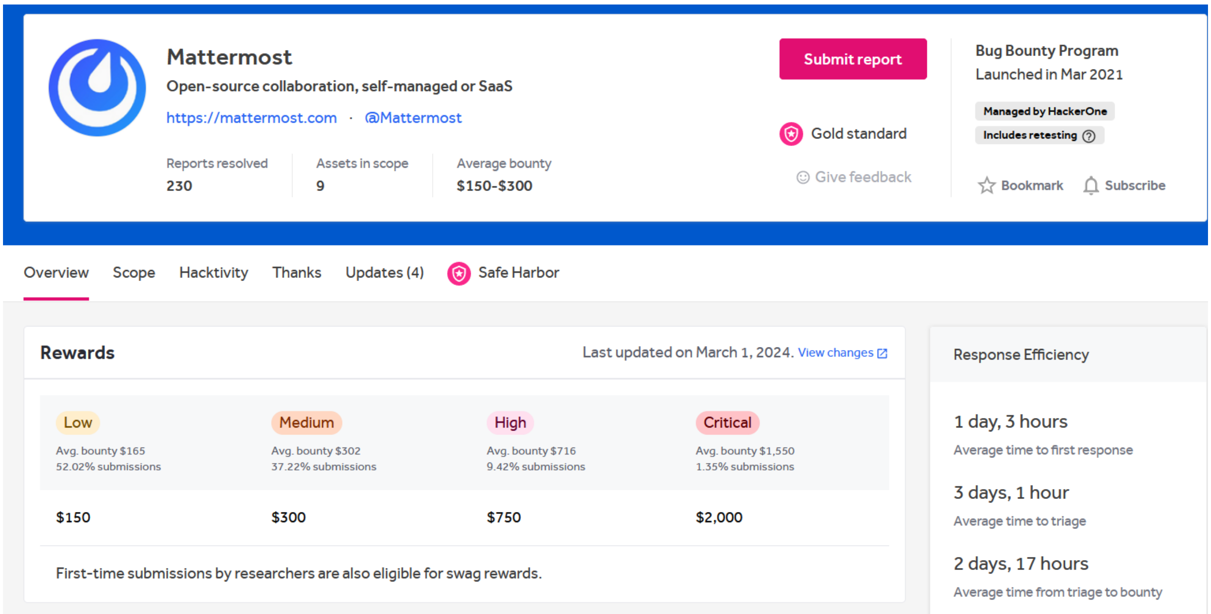
BUG BOUNTY

REPORT 7

Thilakarathna S.T.D- IT22578914

B.Sc. (Hons) in Information Technology Specializing in cyber security

Overview of the website



Mattermost

Open-source collaboration, self-managed or SaaS

https://mattermost.com · @Mattermost

Reports resolved	Assets in scope	Average bounty
230	9	$150-$300

Gold standard

Bug Bounty Program
Launched in Mar 2021

Managed by HackerOne

Includes retesting

Rewards

Last updated on March 1, 2024.

Low	Medium	High	Critical
Avg. bounty $165 52.02% submissions	Avg. bounty $302 37.22% submissions	Avg. bounty $716 9.42% submissions	Avg. bounty $1,550 1.35% submissions
$150	$300	$750	$2,000

First-time submissions by researchers are also eligible for swag rewards.

Response Efficiency

1 day, 3 hours
Average time to first response

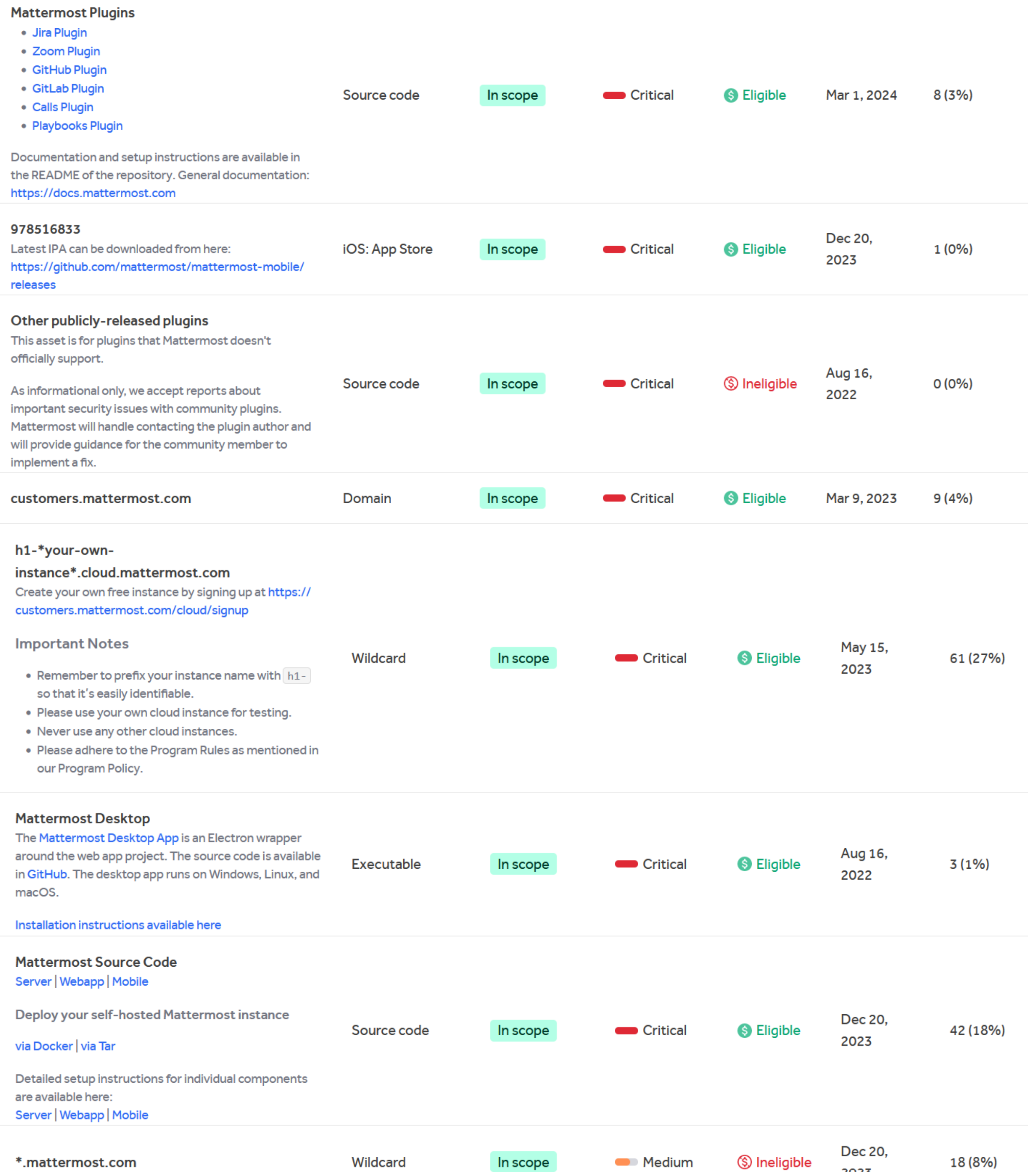
3 days, 1 hour
Average time to triage

2 days, 17 hours
Average time from triage to bounty

Mattermost is an open-source substitute for proprietary communication systems. It is a flexible and safe messaging platform made for contemporary teams. Mattermost facilitates successful collaboration among organizations while upholding data sovereignty, all while emphasizing privacy and control. Teams may improve productivity and optimize communication by integrating it seamlessly with current workflows and systems thanks to its flexible architecture. With the greatest levels of security and compliance guaranteed, Mattermost offers a central hub for teams to connect and interact, whether it is for project management, file sharing, or real-time chat.

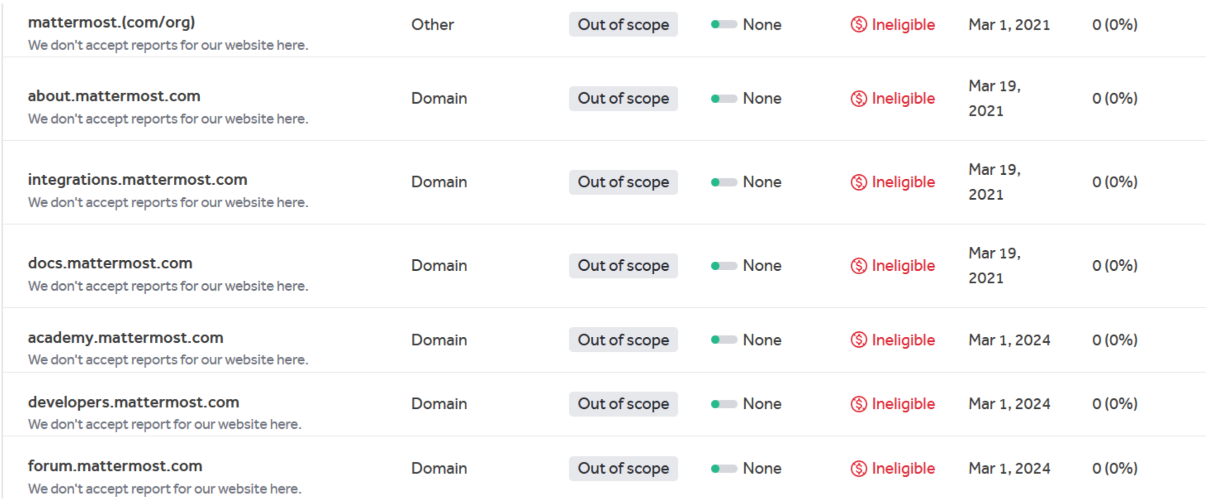
Scope

• InScope



Mattermost Plugins • Jira Plugin • Zoom Plugin • GitHub Plugin • GitLab Plugin • Calls Plugin • Playbooks Plugin Documentation and setup instructions are available in the README of the repository. General documentation: https://docs.mattermost.com	Source code	In scope	Critical	Eligible	Mar 1, 2024	8 (3%)
978516833 Latest IPA can be downloaded from here: https://github.com/mattermost/mattermost-mobile/releases	iOS: App Store	In scope	Critical	Eligible	Dec 20, 2023	1 (0%)
Other publicly-released plugins This asset is for plugins that Mattermost doesn't officially support. As informational only, we accept reports about important security issues with community plugins. Mattermost will handle contacting the plugin author and will provide guidance for the community member to implement a fix.	Source code	In scope	Critical	Ineligible	Aug 16, 2022	0 (0%)
customers.mattermost.com	Domain	In scope	Critical	Eligible	Mar 9, 2023	9 (4%)
h1-*your-own-instance*.cloud.mattermost.com Create your own free instance by signing up at https://customers.mattermost.com/cloud/signup Important Notes • Remember to prefix your instance name with `h1-` so that it's easily identifiable. • Please use your own cloud instance for testing. • Never use any other cloud instances. • Please adhere to the Program Rules as mentioned in our Program Policy.	Wildcard	In scope	Critical	Eligible	May 15, 2023	61 (27%)
Mattermost Desktop The Mattermost Desktop App is an Electron wrapper around the web app project. The source code is available in GitHub. The desktop app runs on Windows, Linux, and macOS. Installation instructions available here	Executable	In scope	Critical	Eligible	Aug 16, 2022	3 (1%)
Mattermost Source Code Server | Webapp | Mobile Deploy your self-hosted Mattermost instance via Docker | via Tar Detailed setup instructions for individual components are available here: Server | Webapp | Mobile	Source code	In scope	Critical	Eligible	Dec 20, 2023	42 (18%)
***.mattermost.com**	Wildcard	In scope	Medium	Ineligible	Dec 20, 2023	18 (8%)

- ## OutScope



mattermost.(com/org) We don't accept reports for our website here.	Other	Out of scope	None	Ineligible	Mar 1, 2021	0 (0%)
about.mattermost.com We don't accept reports for our website here.	Domain	Out of scope	None	Ineligible	Mar 19, 2021	0 (0%)
integrations.mattermost.com We don't accept reports for our website here.	Domain	Out of scope	None	Ineligible	Mar 19, 2021	0 (0%)
docs.mattermost.com We don't accept reports for our website here.	Domain	Out of scope	None	Ineligible	Mar 19, 2021	0 (0%)
academy.mattermost.com We don't accept reports for our website here.	Domain	Out of scope	None	Ineligible	Mar 1, 2024	0 (0%)
developers.mattermost.com We don't accept report for our website here.	Domain	Out of scope	None	Ineligible	Mar 1, 2024	0 (0%)
forum.mattermost.com We don't accept report for our website here.	Domain	Out of scope	None	Ineligible	Mar 1, 2024	0 (0%)

Information Gathering

Security researchers and ethical hackers must first gather data through bug bounty programs in order to identify vulnerabilities in a target system or application. This step's objective is to learn as much as you can about the target, including its technologies, architecture, known vulnerabilities, and potential weak points. Open-source intelligence gathering (OSINT), network scanning, fingerprinting, and asset enumeration are typically required to give a complete view of the target's attack surface.

Since it enables ethical hackers to identify potential points of entry and focus their search for system security flaws, efficient information gathering is the cornerstone of a successful bug hunting operation.

Subdomains for Hunting

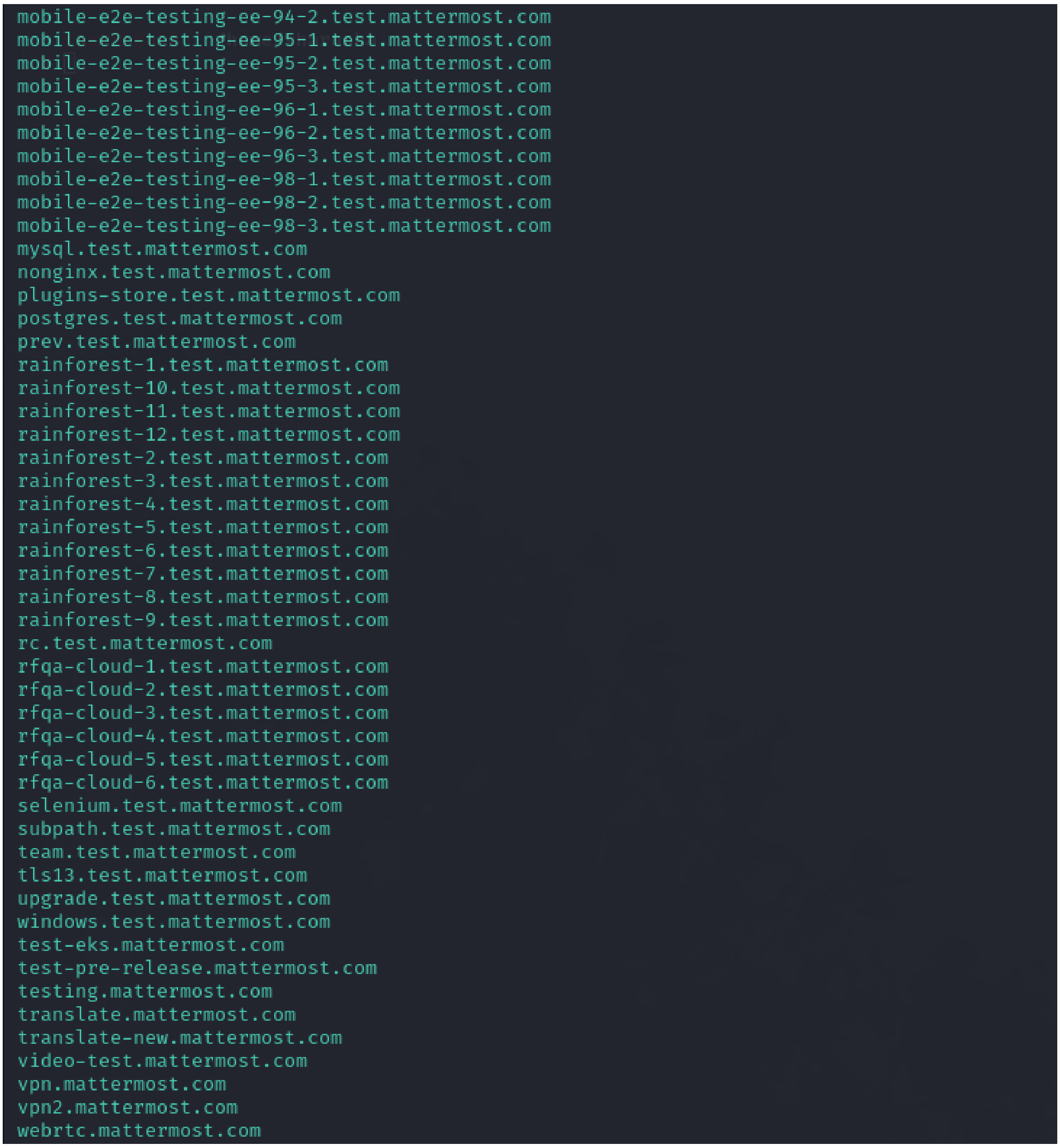
The process of listing sub-domains for one or more domains is called sub-domain enumeration. This is a critical stage in the reconnaissance process. Finding vulnerabilities is made more likely by sub-domain enumeration, which can identify several domains and sub-domains that are part of a security assessment.

Seen through cryptic, abandoned sub-domains, programs may have dangerous bugs.

The same weaknesses are frequently found throughout numerous domains and applications within a single organization.

- **Sublist3r**

Sublist3r is an open-source program used for efficient subdomain enumeration. Penetration testers, security experts, and ethical hackers utilize Sublist3r to locate subdomains linked to a target website. It accomplishes this by using methods like search engine scraping and DNS requests. Sublist3r only needs to know the target domain to begin searching for relevant subdomains. It then provides useful information that can be utilized for vulnerability discovery and security assessments.



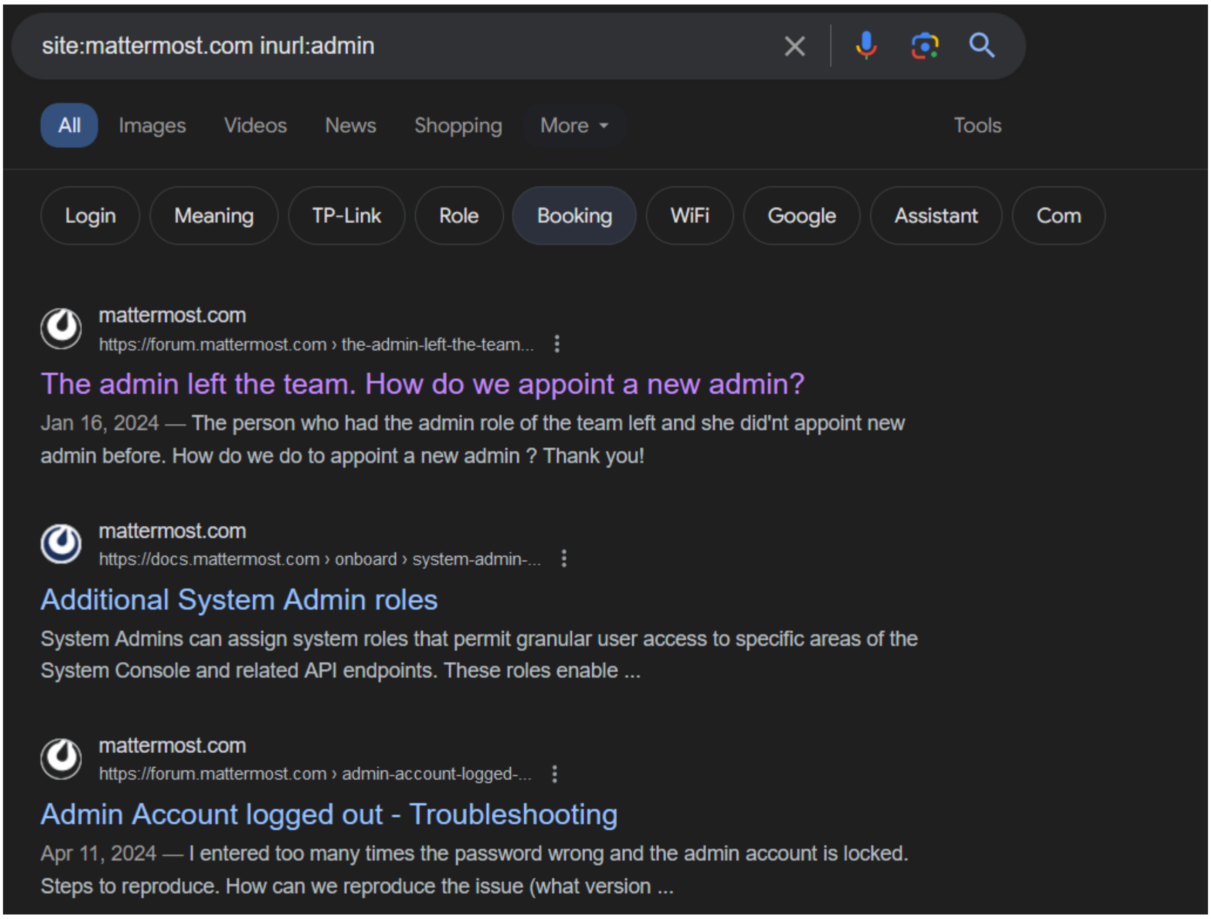
```
mobile-e2e-testing-ee-94-2.test.mattermost.com
mobile-e2e-testing-ee-95-1.test.mattermost.com
mobile-e2e-testing-ee-95-2.test.mattermost.com
mobile-e2e-testing-ee-95-3.test.mattermost.com
mobile-e2e-testing-ee-96-1.test.mattermost.com
mobile-e2e-testing-ee-96-2.test.mattermost.com
mobile-e2e-testing-ee-96-3.test.mattermost.com
mobile-e2e-testing-ee-98-1.test.mattermost.com
mobile-e2e-testing-ee-98-2.test.mattermost.com
mobile-e2e-testing-ee-98-3.test.mattermost.com
mysql.test.mattermost.com
nonginx.test.mattermost.com
plugins-store.test.mattermost.com
postgres.test.mattermost.com
prev.test.mattermost.com
rainforest-1.test.mattermost.com
rainforest-10.test.mattermost.com
rainforest-11.test.mattermost.com
rainforest-12.test.mattermost.com
rainforest-2.test.mattermost.com
rainforest-3.test.mattermost.com
rainforest-4.test.mattermost.com
rainforest-5.test.mattermost.com
rainforest-6.test.mattermost.com
rainforest-7.test.mattermost.com
rainforest-8.test.mattermost.com
rainforest-9.test.mattermost.com
rc.test.mattermost.com
rfqa-cloud-1.test.mattermost.com
rfqa-cloud-2.test.mattermost.com
rfqa-cloud-3.test.mattermost.com
rfqa-cloud-4.test.mattermost.com
rfqa-cloud-5.test.mattermost.com
rfqa-cloud-6.test.mattermost.com
selenium.test.mattermost.com
subpath.test.mattermost.com
team.test.mattermost.com
tls13.test.mattermost.com
upgrade.test.mattermost.com
windows.test.mattermost.com
test-eks.mattermost.com
test-pre-release.mattermost.com
testing.mattermost.com
translate.mattermost.com
translate-new.mattermost.com
video-test.mattermost.com
vpn.mattermost.com
vpn2.mattermost.com
webrtc.mattermost.com
```

- **Google dorking**

Use this search method to help the search engine find sensitive and significant website information.

Site refers to the request that Google show only results from a particular website. By doing this, you'll be able to find the most trustworthy source on the topic with ease.

Inurl: This is a useful technique for locating vulnerable pages on a certain website. For example, we could look up admin, email, password, login, etc. It will provide us with private information.



mattermost.com
https://forum.mattermost.com › the-admin-left-the-team...

The admin left the team. How do we appoint a new admin?

Jan 16, 2024 — The person who had the admin role of the team left and she did'nt appoint new admin before. How do we do to appoint a new admin ? Thank you!

mattermost.com
https://docs.mattermost.com › onboard › system-admin-...

Additional System Admin roles

System Admins can assign system roles that permit granular user access to specific areas of the System Console and related API endpoints. These roles enable ...

mattermost.com
https://forum.mattermost.com › admin-account-logged-...

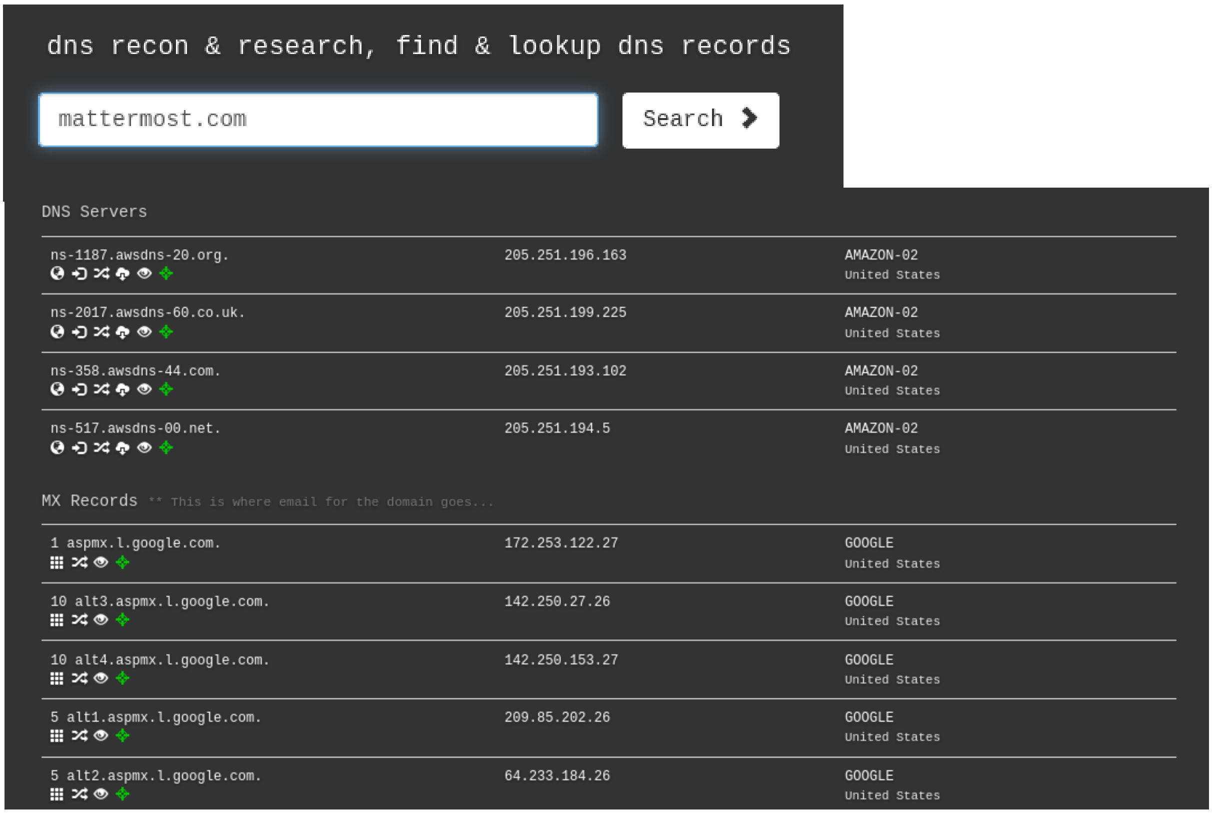
Admin Account logged out - Troubleshooting

Apr 11, 2024 — I entered too many times the password wrong and the admin account is locked. Steps to reproduce. How can we reproduce the issue (what version ...

- **Dnsdumpster**

Block addresses, emails, domain names, and other kinds of DNS-related data can be gathered using an online passive scanning tool called DNSdumpster.

Result of mattermost.com



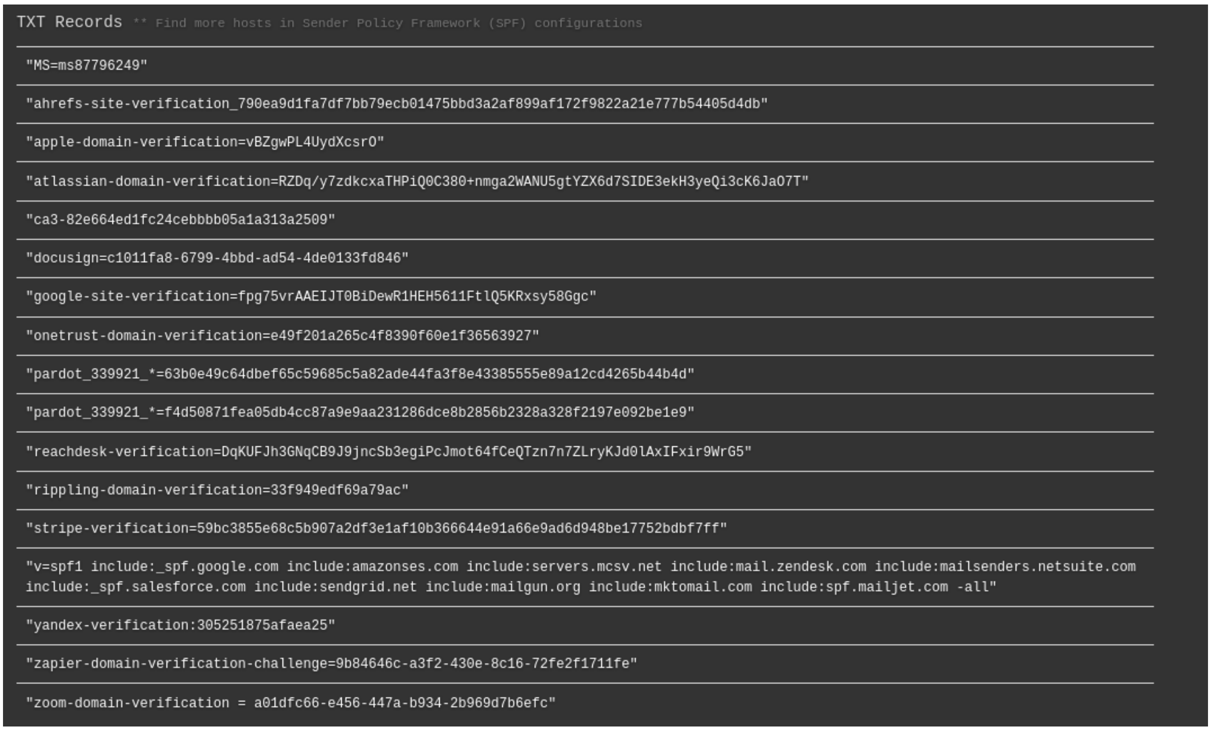
dns recon & research, find & lookup dns records

DNS Servers

ns-1187.awsdns-20.org.	205.251.196.163	AMAZON-02 United States
ns-2017.awsdns-60.co.uk.	205.251.199.225	AMAZON-02 United States
ns-358.awsdns-44.com.	205.251.193.102	AMAZON-02 United States
ns-517.awsdns-00.net.	205.251.194.5	AMAZON-02 United States

MX Records ** This is where email for the domain goes...

1 aspmx.l.google.com.	172.253.122.27	GOOGLE United States
10 alt3.aspmx.l.google.com.	142.250.27.26	GOOGLE United States
10 alt4.aspmx.l.google.com.	142.250.153.27	GOOGLE United States
5 alt1.aspmx.l.google.com.	209.85.202.26	GOOGLE United States
5 alt2.aspmx.l.google.com.	64.233.184.26	GOOGLE United States

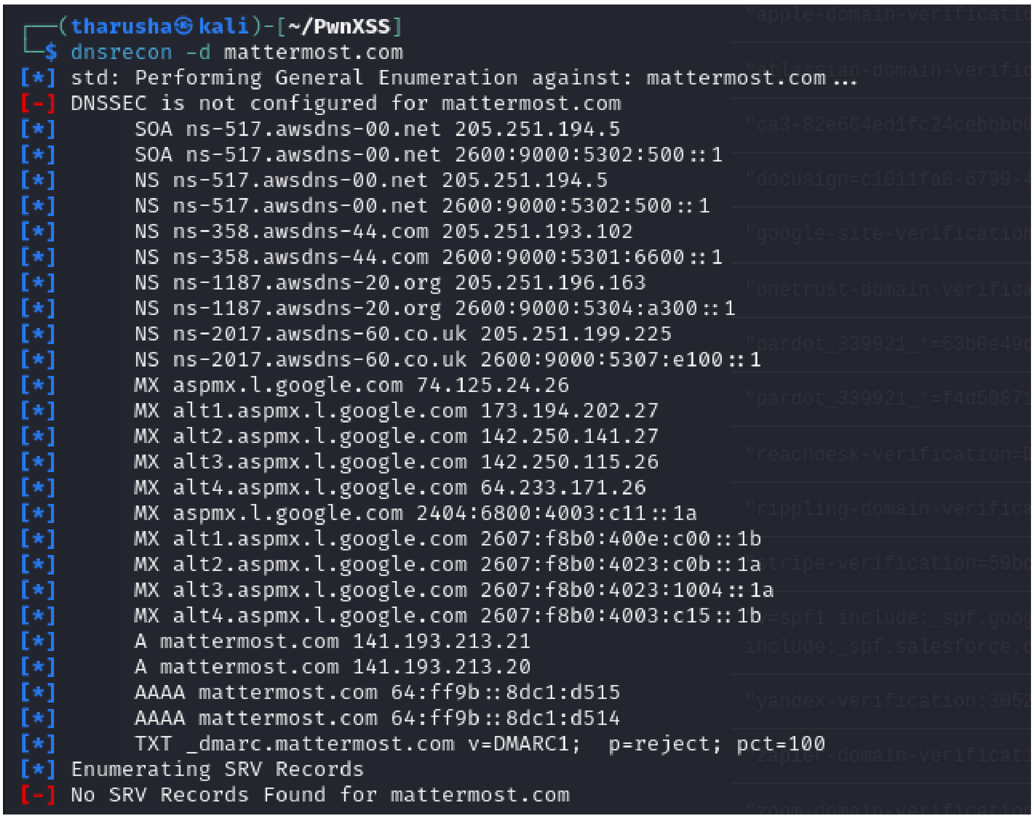


TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

```
"MS=ms87796249"
"ahrefs-site-verification_790ea9d1fa7df7bb79ecb01475bbd3a2af899af172f9822a21e777b54405d4db"
"apple-domain-verification=vBZgwPL4UydXcsrO"
"atlassian-domain-verification=RZDq/y7zdkcxaTHPiQ0C380+nmga2WANU5gtYZX6d7SIDE3ekH3yeQi3cK6Ja07T"
"ca3-82e664ed1fc24cebbbb05a1a313a2509"
"docusign=c1011fa8-6799-4bbd-ad54-4de0133fd846"
"google-site-verification=fpg75vrAAEIJT0BiDewR1HEH5611FtlQ5KRxsy58Ggc"
"onetrust-domain-verification=e49f201a265c4f8390f60e1f36563927"
"pardot_339921_*=63b0e49c64dbef65c59685c5a82ade44fa3f8e43385555e89a12cd4265b44b4d"
"pardot_339921_*=f4d50871fea05db4cc87a9e9aa231286dce8b2856b2328a328f2197e092be1e9"
"reachdesk-verification=DqKUFJh3GNqCB9J9jncSb3egiPcJmot64fCeQTzn7n7ZLryKJd0lAxIFxir9WrG5"
"rippling-domain-verification=33f949edf69a79ac"
"stripe-verification=59bc3855e68c5b907a2df3e1af10b366644e91a66e9ad6d948be17752bdbf7ff"
"v=spf1 include:_spf.google.com include:amazonses.com include:servers.mcsv.net include:mail.zendesk.com include:mailsenders.netsuite.com
include:_spf.salesforce.com include:sendgrid.net include:mailgun.org include:mktomail.com include:spf.mailjet.com -all"
"yandex-verification:305251875afaea25"
"zapier-domain-verification-challenge=9b84646c-a3f2-430e-8c16-72fe2f1711fe"
"zoom-domain-verification = a01dfc66-e456-447a-b934-2b969d7b6efc"
```

- **DNSrecon**

For DNS enumeration and reconnaissance, an open-source tool named DNSRecon is utilized. The purpose of gathering information is to assist with penetration testing and security evaluations by providing details on DNS servers, domains, subdomains, and DNS records.

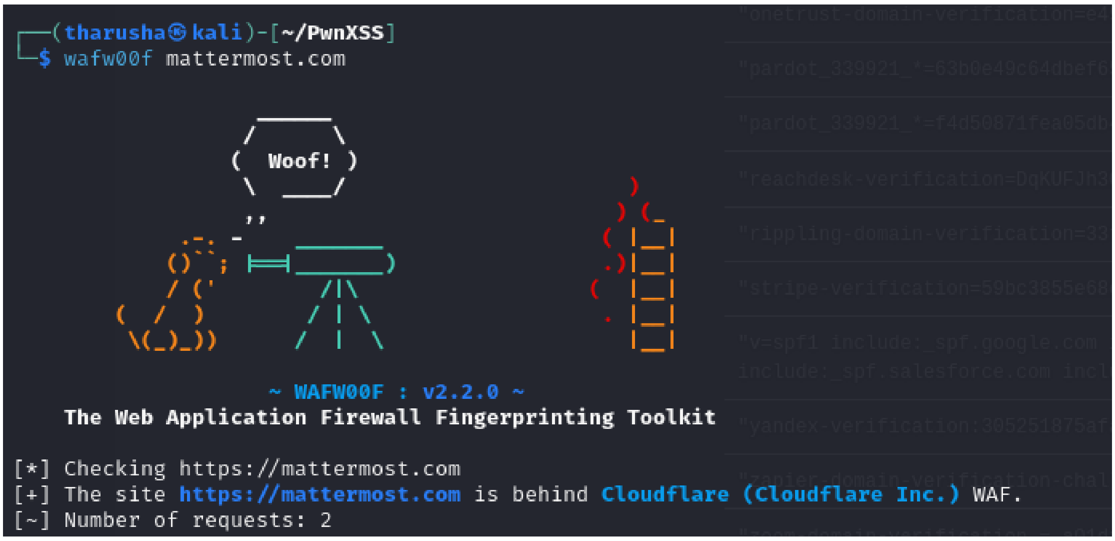


```
┌──(tharusha㉿kali)-[~/PwnXSS]
└─$ dnsrecon -d mattermost.com
[*] std: Performing General Enumeration against: mattermost.com...
[-] DNSSEC is not configured for mattermost.com
[*]      SOA ns-517.awsdns-00.net 205.251.194.5
[*]      SOA ns-517.awsdns-00.net 2600:9000:5302:500::1
[*]      NS ns-517.awsdns-00.net 205.251.194.5
[*]      NS ns-517.awsdns-00.net 2600:9000:5302:500::1
[*]      NS ns-358.awsdns-44.com 205.251.193.102
[*]      NS ns-358.awsdns-44.com 2600:9000:5301:6600::1
[*]      NS ns-1187.awsdns-20.org 205.251.196.163
[*]      NS ns-1187.awsdns-20.org 2600:9000:5304:a300::1
[*]      NS ns-2017.awsdns-60.co.uk 205.251.199.225
[*]      NS ns-2017.awsdns-60.co.uk 2600:9000:5307:e100::1
[*]      MX aspmx.l.google.com 74.125.24.26
[*]      MX alt1.aspmx.l.google.com 173.194.202.27
[*]      MX alt2.aspmx.l.google.com 142.250.141.27
[*]      MX alt3.aspmx.l.google.com 142.250.115.26
[*]      MX alt4.aspmx.l.google.com 64.233.171.26
[*]      MX aspmx.l.google.com 2404:6800:4003:c11::1a
[*]      MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1b
[*]      MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*]      MX alt3.aspmx.l.google.com 2607:f8b0:4023:1004::1a
[*]      MX alt4.aspmx.l.google.com 2607:f8b0:4003:c15::1b
[*]      A mattermost.com 141.193.213.21
[*]      A mattermost.com 141.193.213.20
[*]      AAAA mattermost.com 64:ff9b::8dc1:d515
[*]      AAAA mattermost.com 64:ff9b::8dc1:d514
[*]      TXT _dmarc.mattermost.com v=DMARC1;  p=reject; pct=100
[*] Enumerating SRV Records
[-] No SRV Records Found for mattermost.com
```

- **Wafw00f**

An open-source program called Wafw00f is used to identify and fingerprint Web application firewalls (WAFs). Web application firewalls (WAFs), security solutions, defend against SQL injection, cross-site scripting (XSS), and other attacks.

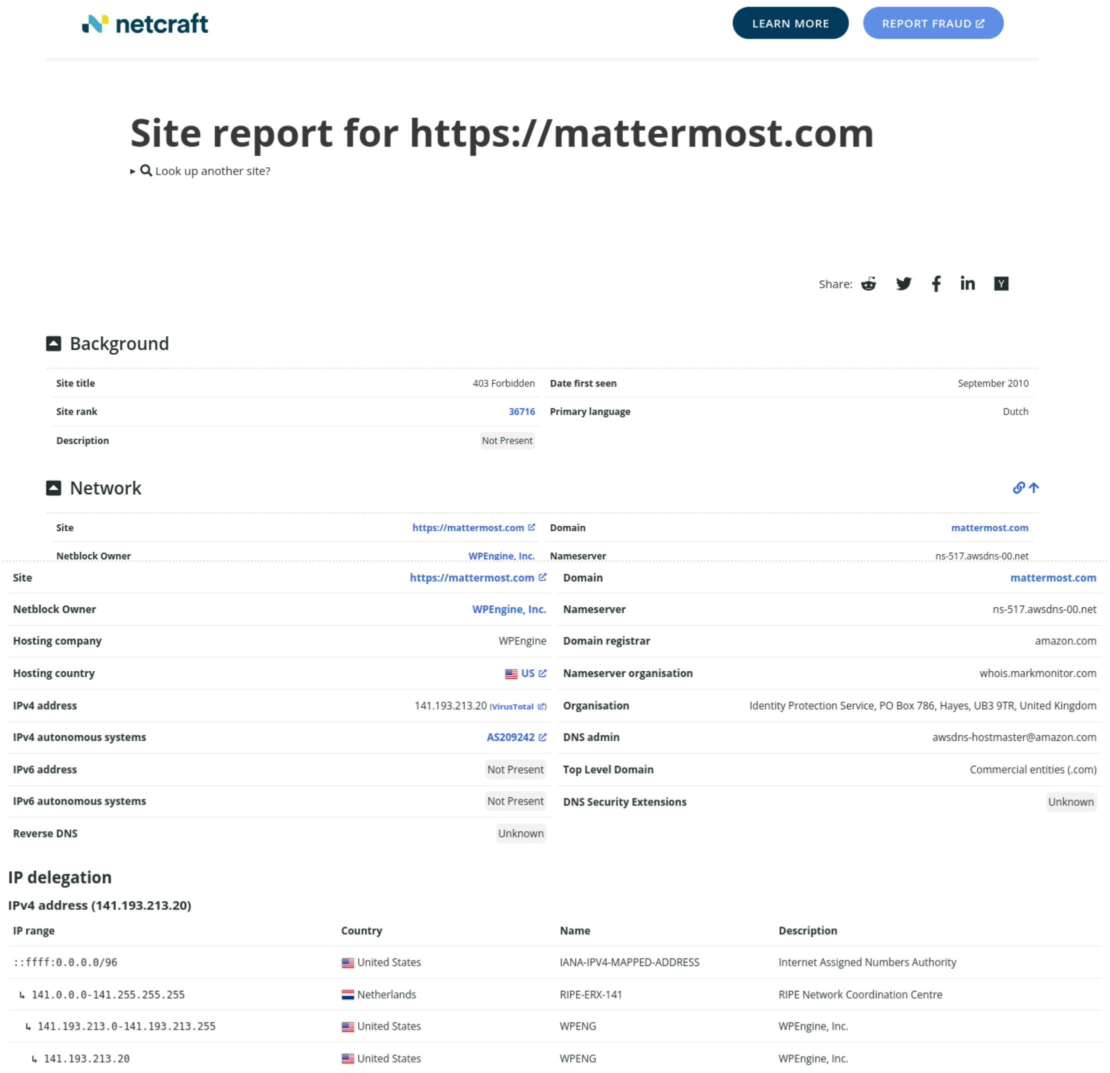
We can see that Cloudfront WAF is protecting mattermost.com.



```
┌──(tharusha㉿kali)-[~/PwnXSS]
└─$ wafw00f mattermost.com

                   ______
                  /      \
                 (  Woof! )
                  \  ____/                      )
                  ,,                          ) (_
             .-. -    _______               ( |__|
            ()``; |==|_______)             .)|__|
            / ('      /|\                  (  |__|
        (  /  )      / | \                  . |__|
         \(_)_))    /  |  \                   |__|

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

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

- **Netcraft**

Based in Bath, Somerset, England, Netcraft provides internet services. A variety of industries are served by the company's cybercrime disruption services. I learned useful knowledge from this website. Like backdrop, IP delegation, SSL/TLS, Network, and Transparency of Certificates.



Site report for https://mattermost.com

▸ Look up another site?

Background

Site title	403 Forbidden	Date first seen	September 2010
Site rank	36716	Primary language	Dutch
Description	Not Present		

Network

Site	https://mattermost.com	Domain	mattermost.com
Netblock Owner	WPEngine, Inc.	Nameserver	ns-517.awsdns-00.net

Site	https://mattermost.com	Domain	mattermost.com
Netblock Owner	WPEngine, Inc.	Nameserver	ns-517.awsdns-00.net
Hosting company	WPEngine	Domain registrar	amazon.com
Hosting country	US	Nameserver organisation	whois.markmonitor.com
IPv4 address	141.193.213.20 (VirusTotal)	Organisation	Identity Protection Service, PO Box 786, Hayes, UB3 9TR, United Kingdom
IPv4 autonomous systems	AS209242	DNS admin	awsdns-hostmaster@amazon.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Unknown
Reverse DNS	Unknown		

IP delegation

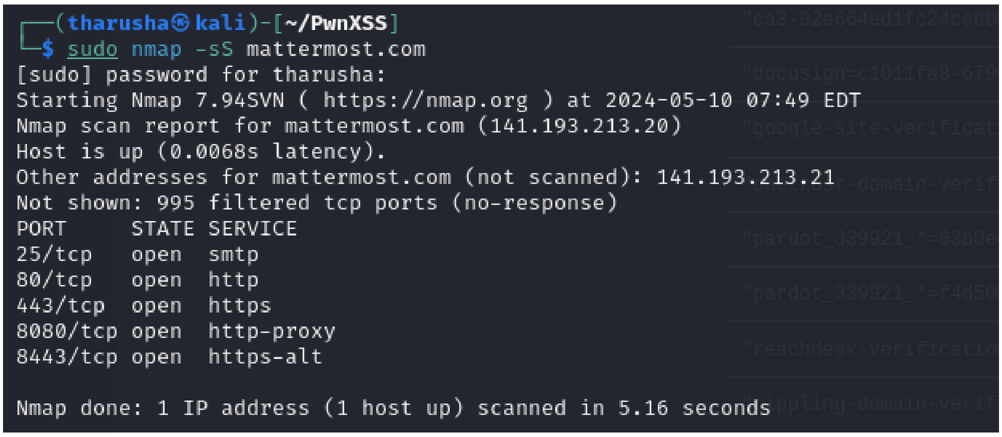
IPv4 address (141.193.213.20)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 141.0.0.0-141.255.255.255	Netherlands	RIPE-ERX-141	RIPE Network Coordination Centre
↳ 141.193.213.0-141.193.213.255	United States	WPENG	WPEngine, Inc.
↳ 141.193.213.20	United States	WPENG	WPEngine, Inc.

- ## Using nmap, open port enumeration

Open port enumeration is a method for locating and classifying the open network ports on a target machine or network using the Nmap (Network Mapper) program. Nmap is an effective open-source tool for network scanning and host discovery that provides extensive information on the services and statuses that are running on various ports. This process involves sending specially made packets to a target system and analyzing the responses in order to determine which ports are open and what services are using them.

Nmap is a popular tool for network administrators and security specialists to assess system security, identify potential security flaws, and enhance network configurations due to its abundance of features and versatility. It's a helpful tool for enhancing security and computer network administration in general.

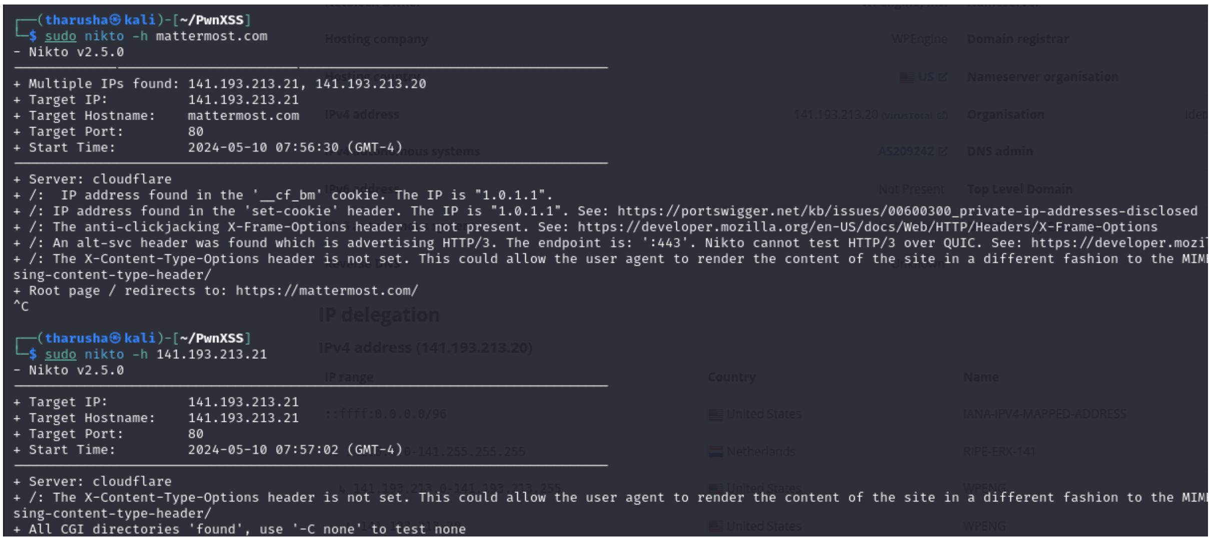


```
┌──(tharusha㉿kali)-[~/PwnXSS]
└─$ sudo nmap -sS mattermost.com
[sudo] password for tharusha:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 07:49 EDT
Nmap scan report for mattermost.com (141.193.213.20)
Host is up (0.0068s latency).
Other addresses for mattermost.com (not scanned): 141.193.213.21
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds
```

- ## Using Nikto to scan for vulnerabilities

One method to check for vulnerabilities in Kali Linux is to use the powerful open-source tool Nikto web scanner, which is part of the popular operating system for penetration testing and ethical hacking. Nikto is specifically designed to identify and assess server and web application vulnerabilities.

When checking target web servers for known vulnerabilities, common security issues, and misconfigurations, Nikto can be used from the Kali Linux command line. Nikto searches for issues including outdated software, possibly unsafe scripts, security headers, and other online vulnerabilities. It helps ethical hackers and security professionals understand and reduce such threats by providing comprehensive information on the vulnerabilities discovered.



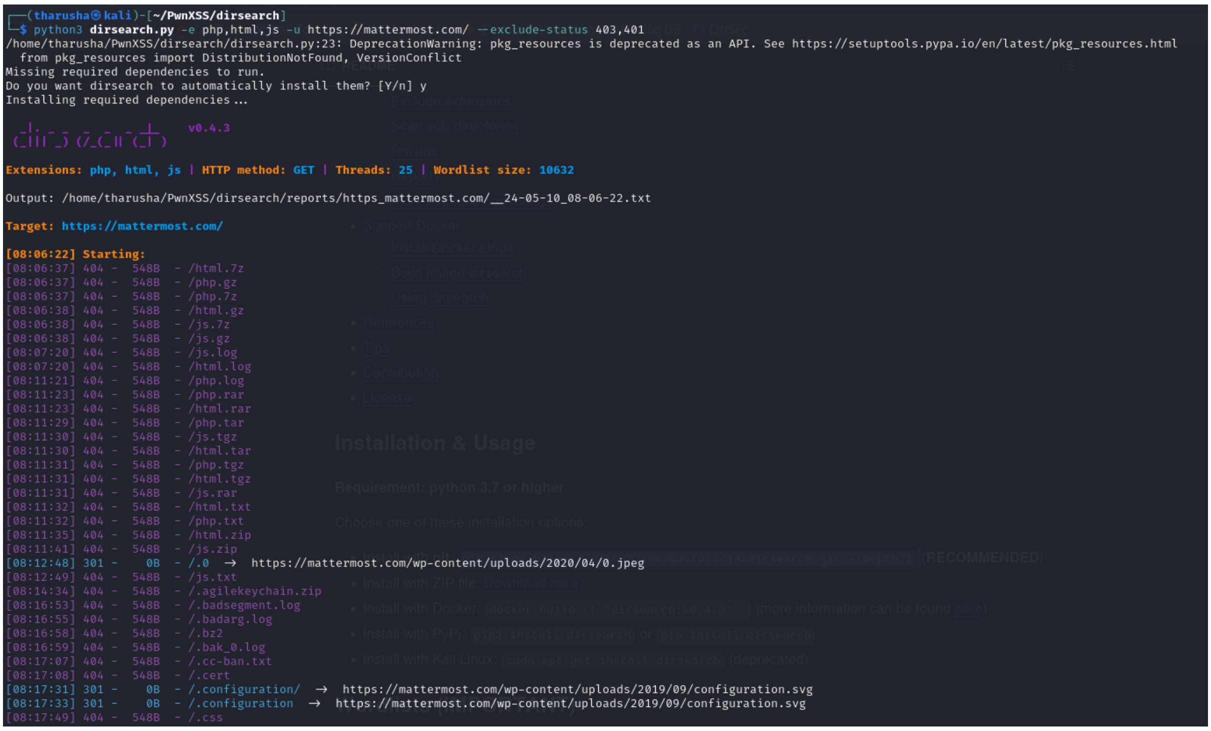
```
┌──(tharusha㉿kali)-[~/PwnXSS]
└─$ sudo nikto -h mattermost.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 141.193.213.21, 141.193.213.20
+ Target IP:          141.193.213.21
+ Target Hostname:    mattermost.com
+ Target Port:        80
+ Start Time:         2024-05-10 07:56:30 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /:  IP address found in the '__cf_bm' cookie. The IP is "1.0.1.1".
+ /: IP address found in the 'set-cookie' header. The IP is "1.0.1.1". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: 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.mozi
+ /: 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 MIM
sing-content-type-header/
+ Root page / redirects to: https://mattermost.com/
^C

┌──(tharusha㉿kali)-[~/PwnXSS]
└─$ sudo nikto -h 141.193.213.21
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          141.193.213.21
+ Target Hostname:    141.193.213.21
+ Target Port:        80
+ Start Time:         2024-05-10 07:57:02 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: 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 MIM
sing-content-type-header/
+ All CGI directories 'found', use '-C none' to test none
```

- ## Dirsearch

open-source program that gives users the ability to execute advanced web content discovery using a variety of wordlist vectors, excellent performance, high accuracy, complex connection/request settings, and state-of-the-art brute-force techniques.

There are a few "blacklist files" in the folder or database. These files will not appear in the scan results if the paths within them have the same status as the filename indicates.

For example, if the admin.php file is added to the database or blacklist of files, it will be screened during each scan and produce a 400 status code.Derrfefd

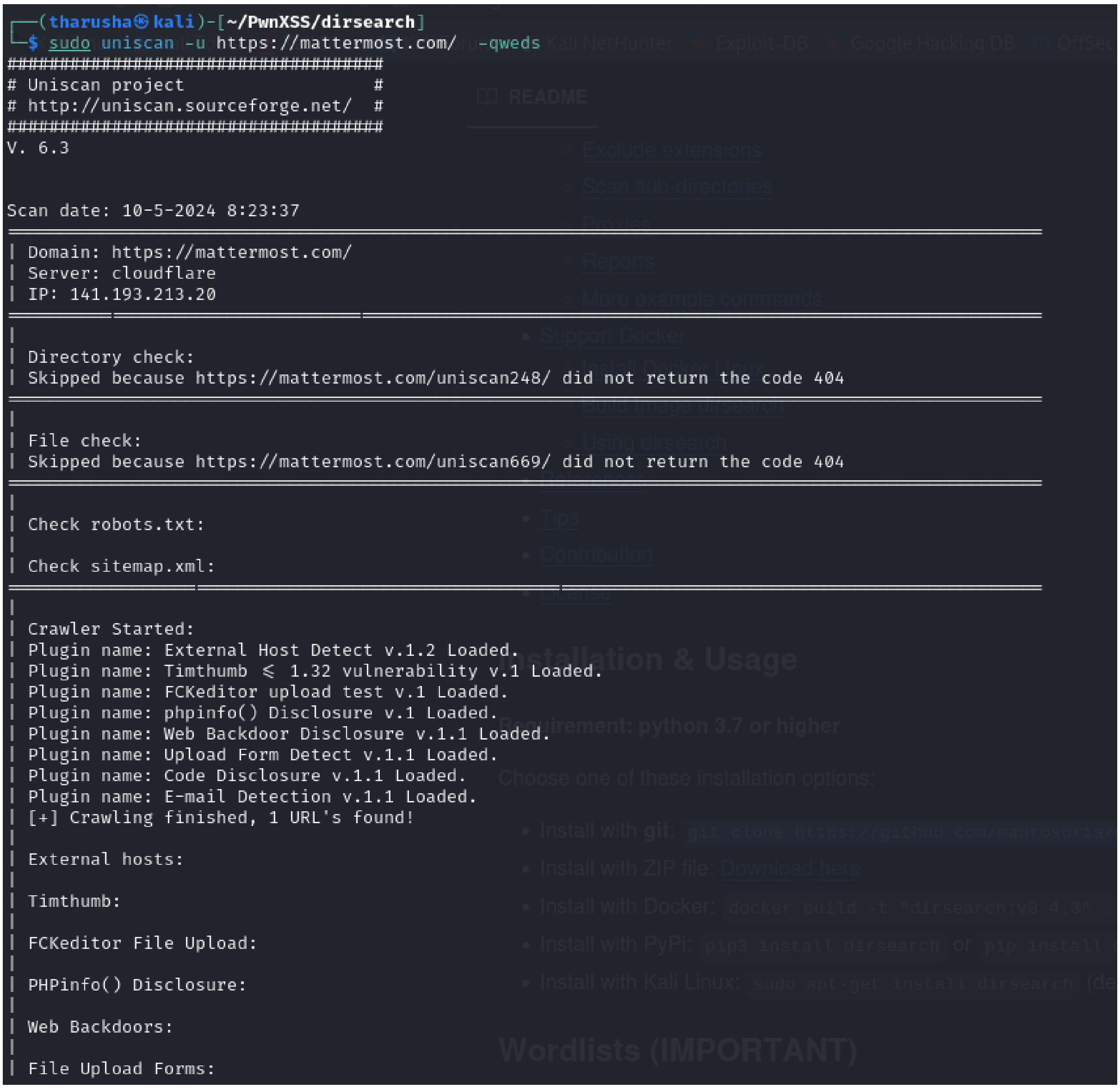


```
┌──(tharusha㉿kali)-[~/PwnXSS/dirsearch]
└─$ python3 dirsearch.py -e php,html,js -u https://mattermost.com/ --exclude-status 403,401
/home/tharusha/PwnXSS/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
Missing required dependencies to run.
Do you want dirsearch to automatically install them? [Y/n] y
Installing required dependencies ...

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 10632

Output: /home/tharusha/PwnXSS/dirsearch/reports/https_mattermost.com/__24-05-10_08-06-22.txt

Target: https://mattermost.com/

[08:06:22] Starting:
[08:06:37] 404 -  548B  - /html.7z
[08:06:37] 404 -  548B  - /php.gz
[08:06:37] 404 -  548B  - /php.7z
[08:06:38] 404 -  548B  - /html.gz
[08:06:38] 404 -  548B  - /js.7z
[08:06:38] 404 -  548B  - /js.gz
[08:07:20] 404 -  548B  - /js.log
[08:07:20] 404 -  548B  - /html.log
[08:11:21] 404 -  548B  - /php.log
[08:11:23] 404 -  548B  - /php.rar
[08:11:23] 404 -  548B  - /html.rar
[08:11:29] 404 -  548B  - /php.tar
[08:11:30] 404 -  548B  - /js.tgz
[08:11:30] 404 -  548B  - /html.tar
[08:11:31] 404 -  548B  - /php.tgz
[08:11:31] 404 -  548B  - /html.tgz
[08:11:31] 404 -  548B  - /js.rar
[08:11:32] 404 -  548B  - /html.txt
[08:11:32] 404 -  548B  - /php.txt
[08:11:35] 404 -  548B  - /html.zip
[08:11:41] 404 -  548B  - /js.zip
[08:12:48] 301 -    0B  - /.0  ->  https://mattermost.com/wp-content/uploads/2020/04/0.jpeg
[08:12:49] 404 -  548B  - /js.txt
[08:14:34] 404 -  548B  - /.agilekeychain.zip
[08:16:53] 404 -  548B  - /.badsegment.log
[08:16:55] 404 -  548B  - /.badarg.log
[08:16:58] 404 -  548B  - /.bz2
[08:16:59] 404 -  548B  - /.bak_0.log
[08:17:07] 404 -  548B  - /.cc-ban.txt
[08:17:08] 404 -  548B  - /.cert
[08:17:31] 301 -    0B  - /.configuration/  ->  https://mattermost.com/wp-content/uploads/2019/09/configuration.svg
[08:17:33] 301 -    0B  - /.configuration  ->  https://mattermost.com/wp-content/uploads/2019/09/configuration.svg
[08:17:49] 404 -  548B  - /.css
```

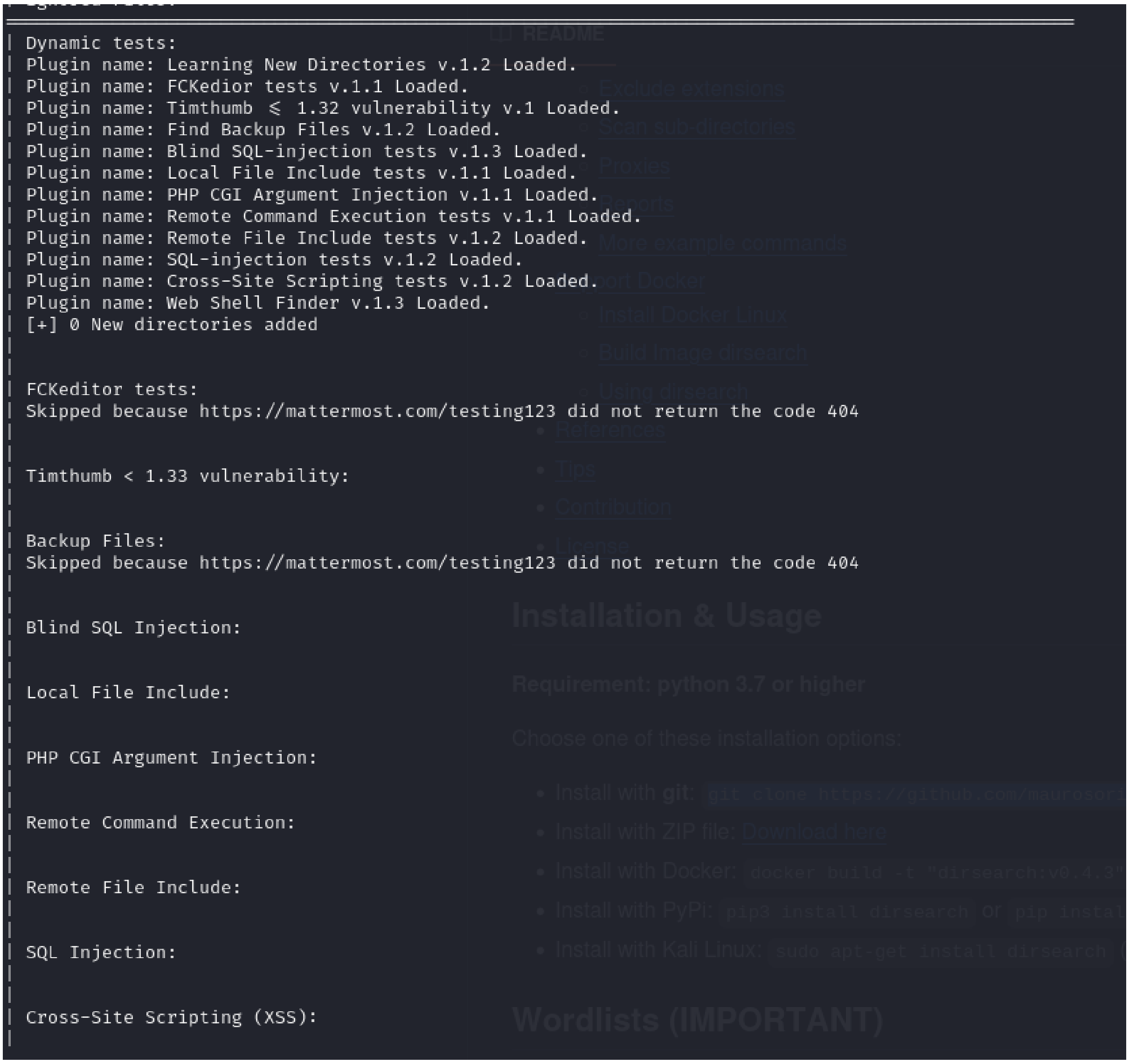
- ## Uniscan

Uniscan is a free penetration testing program. This application is used to scan web applications for vulnerabilities. This scan allows us to examine the target online application for vulnerabilities related to web shells, SQL injection, PHP injection, remote file inclusion (LFI), remote command execution, and backup files.

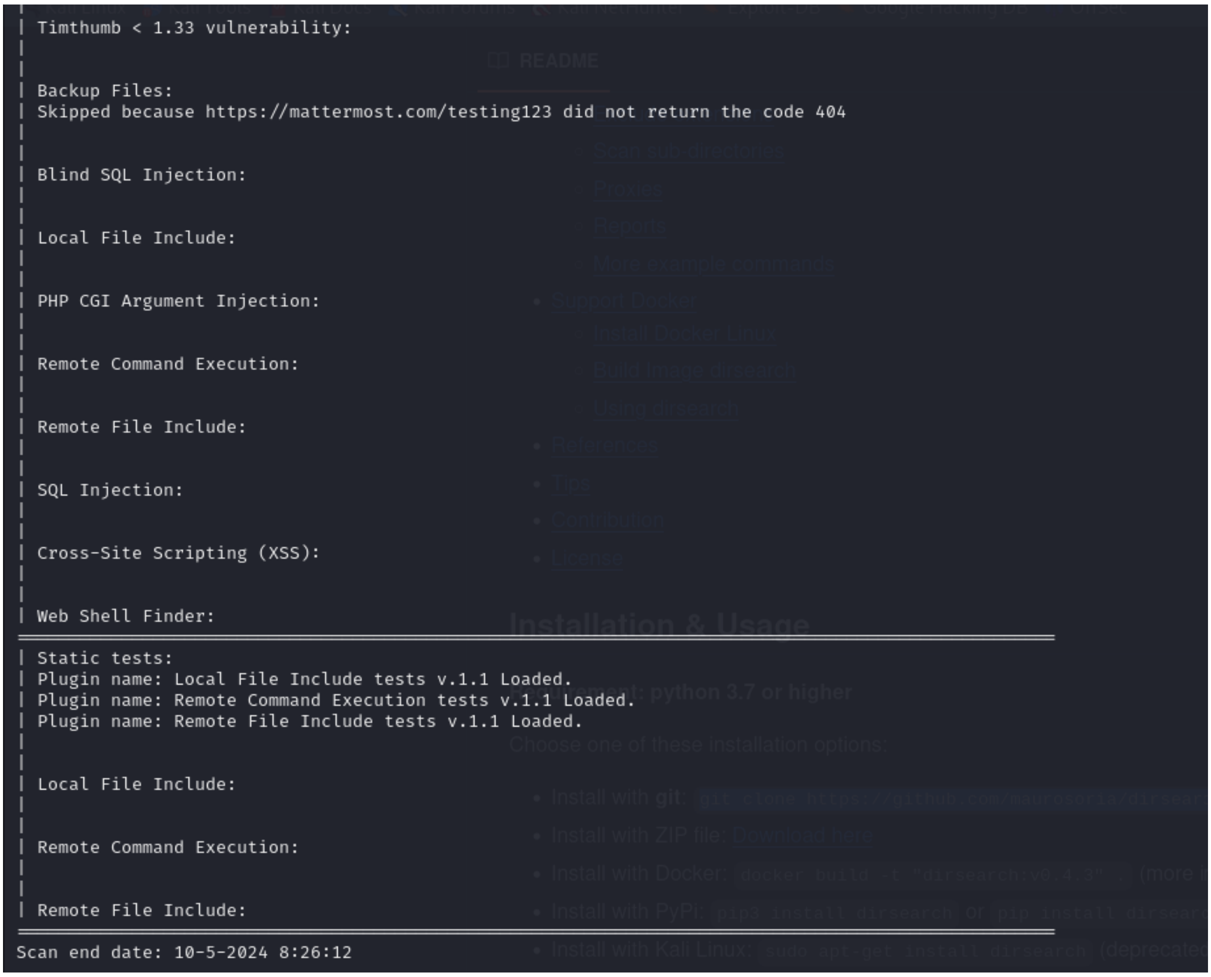
These are mattermost.com's scan findings.



```
┌──(tharusha㉿kali)-[~/PwnXSS/dirsearch]
└─$ sudo uniscan -u https://mattermost.com/ -qweds
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


Scan date: 10-5-2024 8:23:37
═══════════════════════════════════════════════════════════════════════════════════════════════
| Domain: https://mattermost.com/
| Server: cloudflare
| IP: 141.193.213.20
═══════════════════════════════════════════════════════════════════════════════════════════════
|
| Directory check:
| Skipped because https://mattermost.com/uniscan248/ did not return the code 404
═══════════════════════════════════════════════════════════════════════════════════════════════
|
| File check:
| Skipped because https://mattermost.com/uniscan669/ did not return the code 404
═══════════════════════════════════════════════════════════════════════════════════════════════
|
| Check robots.txt:
|
| Check sitemap.xml:
═══════════════════════════════════════════════════════════════════════════════════════════════
|
| Crawler Started:
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: Timthumb ≤ 1.32 vulnerability v.1 Loaded.
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: E-mail Detection v.1.1 Loaded.
| [+] Crawling finished, 1 URL's found!
|
| External hosts:
|
| Timthumb:
|
| FCKeditor File Upload:
|
| PHPinfo() Disclosure:
|
| Web Backdoors:
|
| File Upload Forms:
```



```
| Ignored Files:
═══════════════════════════════════════════════════════════════════════════════════════════════
| Dynamic tests:
| Plugin name: Learning New Directories v.1.2 Loaded.
| Plugin name: FCKedior tests v.1.1 Loaded.
| Plugin name: Timthumb ⩽ 1.32 vulnerability v.1 Loaded.
| Plugin name: Find Backup Files v.1.2 Loaded.
| Plugin name: Blind SQL-injection tests v.1.3 Loaded.
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.2 Loaded.
| Plugin name: SQL-injection tests v.1.2 Loaded.
| Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
| Plugin name: Web Shell Finder v.1.3 Loaded.
| [+] 0 New directories added
|
|
| FCKeditor tests:
| Skipped because https://mattermost.com/testing123 did not return the code 404
|
|
| Timthumb < 1.33 vulnerability:
|
|
| Backup Files:
| Skipped because https://mattermost.com/testing123 did not return the code 404
|
|
| Blind SQL Injection:
|
|
| Local File Include:
|
|
| PHP CGI Argument Injection:
|
|
| Remote Command Execution:
|
|
| Remote File Include:
|
|
| SQL Injection:
|
|
| Cross-Site Scripting (XSS):
|
```



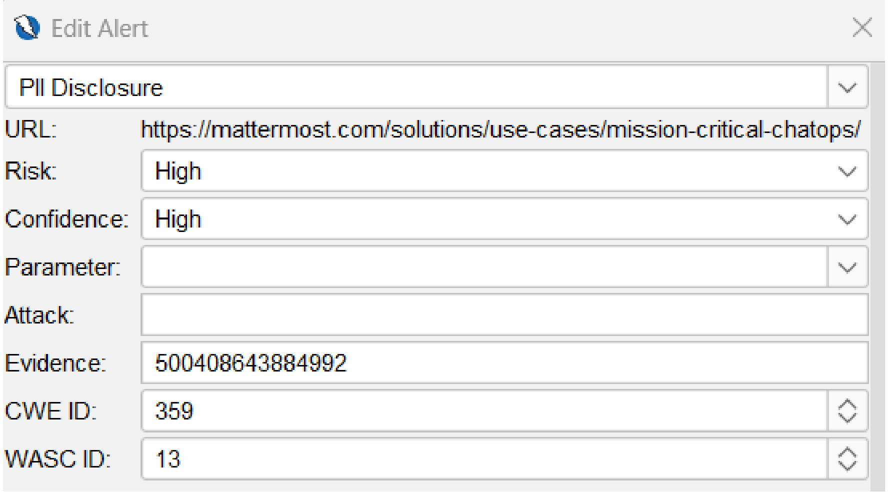
```
| Timthumb < 1.33 vulnerability:
|
|
| Backup Files:
| Skipped because https://mattermost.com/testing123 did not return the code 404
|
|
| Blind SQL Injection:
|
|
| Local File Include:
|
|
| PHP CGI Argument Injection:
|
|
| Remote Command Execution:
|
|
| Remote File Include:
|
|
| SQL Injection:
|
|
| Cross-Site Scripting (XSS):
|
|
| Web Shell Finder:
===============================================================================
| Static tests:
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.1 Loaded.
|
|
| Local File Include:
|
|
| Remote Command Execution:
|
|
| Remote File Include:
===============================================================================
Scan end date: 10-5-2024 8:26:12
```

Vulnerabilities detect when Scanning

In order to process and find problems and vulnerabilities that are based on the OWASP top 10, I used tool like OWASP ZAP.

OWASP ZAP is a testing tool that may be used to identify potential security gaps in internet applications. OWASP ZAP can be used to find common vulnerabilities such as SQL injection and cross-site scripting (XSS).

1. Vulnerability Title



PII Disclosure	
URL:	https://mattermost.com/solutions/use-cases/mission-critical-chatops/
Risk:	High
Confidence:	High
Parameter:	
Attack:	
Evidence:	500408643884992
CWE ID:	359
WASC ID:	13

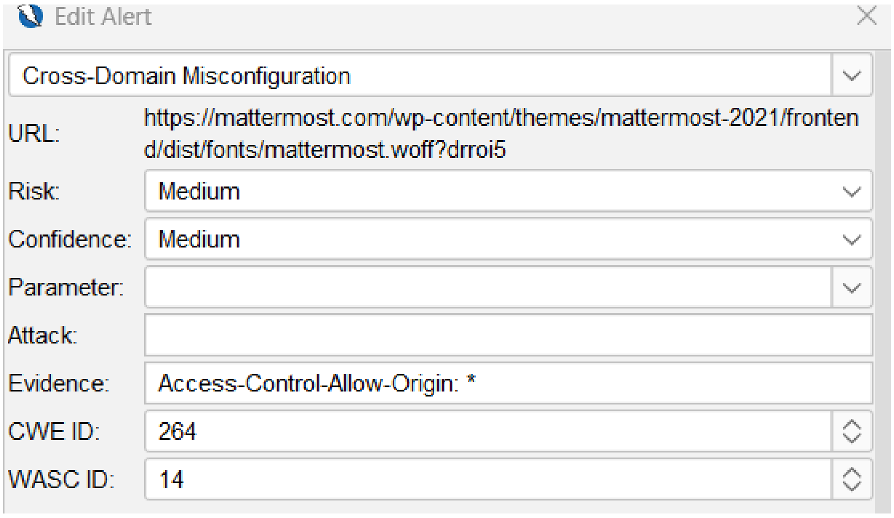
Vulnerability Description

The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

How to mitigate

Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

2. Vulnerability Title



Cross-Domain Misconfiguration	
URL:	https://mattermost.com/wp-content/themes/mattermost-2021/frontend/dist/fonts/mattermost.woff?drroi5
Risk:	Medium
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	Access-Control-Allow-Origin: *
CWE ID:	264
WASC ID:	14

Vulnerability Description

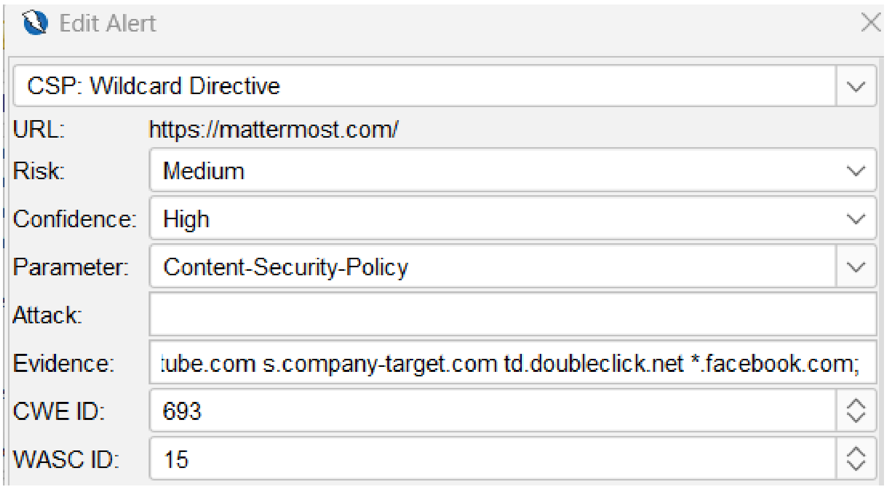
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server

How to mitigate

Make sure that no unauthenticated access to sensitive data exists (for example, by employing IP address white-listing).

To enable the web browser to enforce the Same Origin Policy (SOP) more strictly, configure the "Access-Control-Allow-Origin" HTTP header to a more restricted set of domains, or delete all CORS headers altogether.

3. Vulnerability Title



CSP: Wildcard Directive

URL:	https://mattermost.com/
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	ube.com s.company-target.com td.doubleclick.net *.facebook.com;
CWE ID:	693
WASC ID:	15

Vulnerability Description

One additional security layer that aids in the detection and mitigation of specific attack types is Content Security Policy (CSP). include, but not restricted to, data injection and Cross Site Scripting (XSS). Data theft, malware dissemination, and site defacement are just a few of the uses for these attacks. Website owners can specify which content sources, such as JavaScript, CSS, HTML frames, fonts, images, and embeddable objects like Java applets, ActiveX, audio, and video files, are acceptable for browsers to load on their page by using the standard HTTP headers provided by CSP.

How to mitigate

Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.