Sri Lanka Institute of Information Technology

IE2062-Web Security

IT Number	Name
IT22581402	C.D.Aluthge

Information gathering and reconnaissance phase

a. Subdomain enumeration
    i. Recon-ng

b. Getting alive subdomains
    i. Nslookup
    ii. Sublist3r

c. DNS enumeration
    i. Dnsrecon
    ii. Dnsdumper
    iii. Nikto

d. Public devices enumeration
    i. Censys
    ii. Whois

e. Find WAF (web application firewall) protection.
    i. Wafwoof

f. Find open ports.
    i. Nmap

g. Exploitation
    i. sqlmap

vulnerability analysis phase

1. Target domain: https://indrive.com/

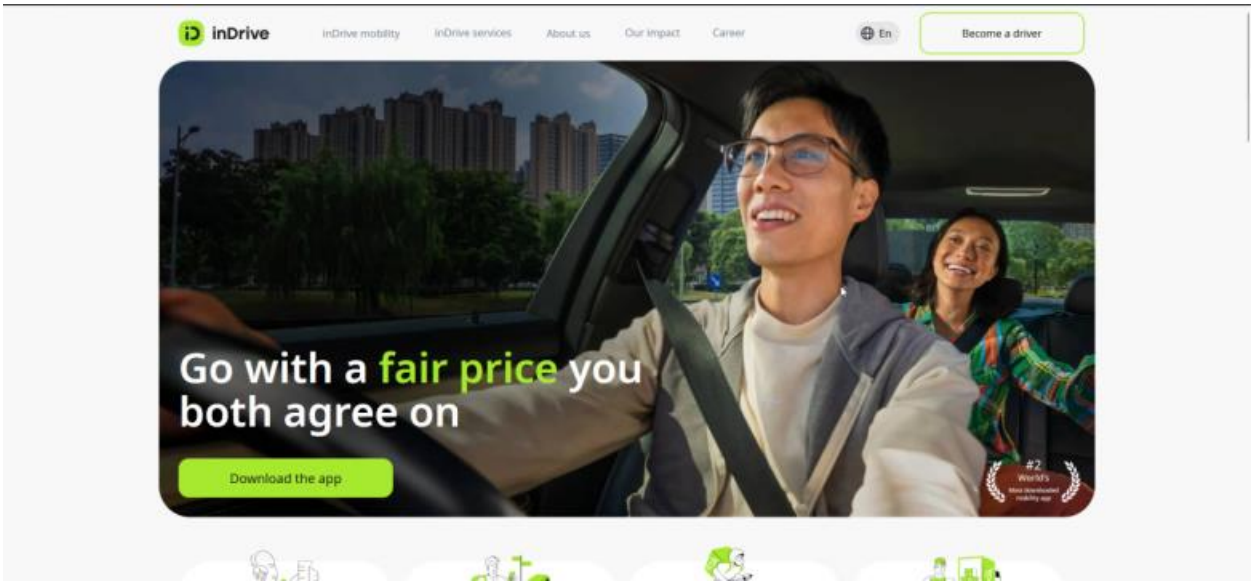
    a. Missing XSS protection header file
    b. CSP (content security policy) not implemented.

Conclusion

Scope:

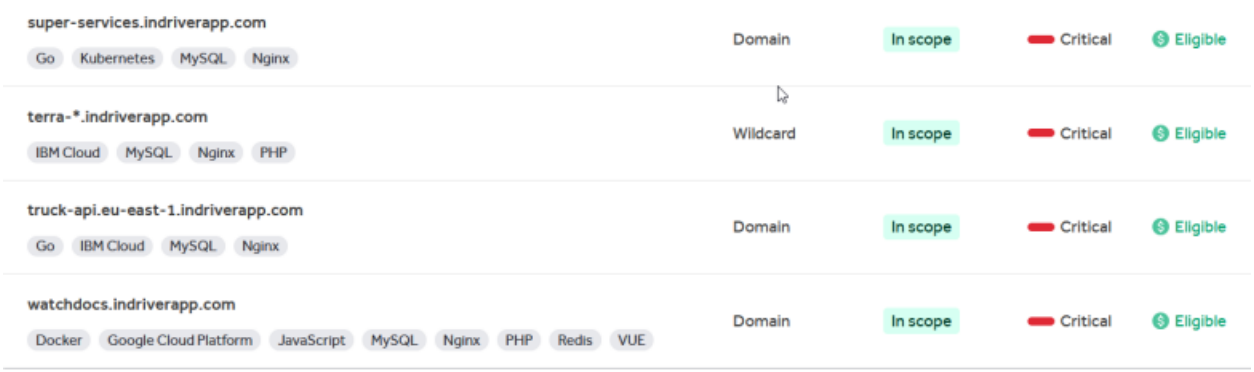
InDrive is a car rental service platform that offers convenient and flexible car rental options to users. It allows individuals to rent cars for

personal use or for business purposes, providing a range of vehicle options from economy cars to luxury vehicles. Users can typically book cars through the InDrive website or mobile app, select rental duration and pick-up/drop-off locations, and manage their bookings seamlessly. The platform often includes features such as insurance options, GPS navigation, and customer support to ensure a smooth rental experience for users.



In Scope:

*.indrive.com	Wildcard	In scope	Medium	Eligible
*.indriver.com	Wildcard	In scope	Medium	Eligible
*.indriverapp.com Amazon Web Services · Elastic Search · Go · Google Cloud Platform · GraphQL · IBM Cloud · MySQL · PHP · Redis	Wildcard	In scope	Critical	Eligible
ab-platform-api.eu-east-1.indriverapp.com Amazon Web Services · Go · IBM Cloud · JavaScript · MySQL · Nginx · React	Domain	In scope	Critical	Eligible
file-storage-front.eu-east-1.indriverapp.com Amazon Web Services · Go · MySQL · Redis	Domain	In scope	Critical	Eligible
injob.indriver.com Amazon Web Services · Docker · Elastic Search · JavaScript · MySQL · Nginx · React	Domain	In scope	Critical	Eligible
intercity-*.eu-east-1.indriverapp.com Go · MySQL · Nginx	Wildcard	In scope	Critical	Eligible



Outscope

OWASP top 10 vulnerabilities

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components

- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

Broken Access Control

When users are unable to adequately impose limitations on what they can access or do within a system, this is known as broken access control. This vulnerability makes it possible for unauthorized individuals to access private data or carry out tasks that shouldn't be permitted. Insecure references to objects, improperly configured permissions, and a lack of authentication checks are the causes of it. Because it can result in illegal data exposure, manipulation, or system penetration, it's a major problem.

Cryptographic Failures

Cryptographic collapses are the result of poor algorithms, incorrect implementations, or improper management of encryption keys, which compromise the security of information encrypted via encryption techniques. Undermining security safeguards and perhaps leading in data breaches, this can lead to unauthorized access to or exposure of sensitive data.

Injection

Injection: it is a type of security vulnerability in which untrusted data is sent to an interpreter as part of a command or query. Most often, attackers use this to inject malicious code into input fields, for example, login forms or search boxes. The interpreter then executes this code, which can give the attacker unauthorized access to data, alter the application's behavior, or gain full control over the system. There are many types of injections, such as SQL injection, where the attackers manipulate database queries, or cross-site scripting, where the malicious script is injected into a web page that other users view.

Insecure Design

Insecure design means the security flaws within the fundamental system or application design born out of insufficient attention to security at the design time. Consequently, systems have vulnerabilities that enable unauthorized system access or breaches. Examples are poor user authentication or no network segmentation. To fix insecure design, significant changes to the architecture are needed to develop the designs securely.

Security Misconfiguration

Imagine you accidentally leave your front door closed but not locked. That's what a security misconfiguration is like. Essentially, it's not properly securing your software systems, servers, or web applications. This can include default settings, shipped insecurely, or unnecessary features. Unauthorized users might target such vulnerabilities to access your info or disrupt the operation. Therefore, one should monitor and update security measures continuously to avoid misconfiguration.

Vulnerable and Outdated Components

Vulnerable components are software elements that are known to contain security flaws that could be exploited by hackers. However, software components that have not received an upgrade in a long time are known as outdated components, and they may not include important security updates and bug fixes. In order to maintain a secure system environment, both sorts of components present security concerns and should be routinely updated and monitored.

Identification and Authentication Failures

When systems are unable to accurately confirm user identities or authenticate their access credentials, identification and authentication failures take place. Whereas authentication failures are caused by an inability to verify user identities, identification failures are the consequence of incorrect user recognition. In order to identify and fix system vulnerabilities, strong authentication procedures and frequent security assessments are essential. These failures might result in unauthorized access and security breaches.

Software and Data Integrity Failures

Software code or data accuracy, consistency, and reliability are jeopardized in software and data integrity issues. Data integrity problems are caused by mistakes, unauthorized access, or cyberattacks, whereas programming errors, malicious code, or unauthorized alterations are the causes of software integrity problems. To reduce risks and guarantee system security and dependability, preventive measures include backups, data encryption, access controls, and regular updates.

Security Logging and Monitoring Failures

Failed security logging and monitoring systems result in a delayed detection of security incidents and higher risks since they are unable to reliably capture and evaluate security-related events. Monitoring failures are caused by insufficient tools

or response protocols, whereas logging failures are caused by misconfigurations or deactivated logging systems. Organizations should establish strong response protocols, use comprehensive logging practices, deploy efficient monitoring tools like SIEM tools, train security teams, and continuously improve logging and monitoring configurations in light of best practices and emerging threats in order to address these failures. By taking these steps, cybersecurity defenses are strengthened, and the effects of security events are lessened.

Server-Side Request Forgery

A security flaw known as server-side request forgery (SSRF) allows attackers to take control of a susceptible server and send unwanted requests, usually to external or internal systems. Unauthorized access, data loss, and more exploitation may result from this. Input validation, whitelisting authorized resources, network segmentation, and access controls are all part of prevention. Frequent security testing improves overall system security by assisting in the identification and mitigation of SSRF threats.

Information gathering and reconnaissance phase.

The objective is to gather as much pertinent data as you can about the intended system or organization. Understanding the target's infrastructure, seeing potential vulnerabilities, and organizing additional security testing operations are all made easier with the aid of this information.

Domain: https://indrive.com/

- **Recon-ng**

Recon-ng is an open-source reconnaissance tool with Python foundation that is used for penetration testing and security evaluations. It collects data from domains, IPs, emails, and social media platforms using a modular framework with different modules. The advantages of recon-ng are its flexibility for scripting and automation, integration with many data sources, and data enrichment capabilities. It is used by security experts to gather and evaluate intelligence, spot possible weaknesses, and improve overall security posture during the first reconnaissance phase. Its vibrant community guarantees continuous upgrades and support, which makes it an invaluable addition to cybersecurity toolkits.

Proof of concept:

```
└─$ recon-ng
[*] Version check disabled.

 _/_/_/    _/_/_/_/    _/_/_/    _/_/_/    _/      _/          _/      _/    _/_/_/
  _/    _/  _/        _/        _/        _/  _/_/    _/        _/_/    _/  _/
 _/_/_/    _/_/_/    _/  _/_/  _/  _/_/  _/  _/  _/  _/_/_/_/  _/  _/  _/  _/  _/_/_/
_/    _/  _/        _/    _/  _/    _/  _/  _/    _/          _/    _/_/  _/      _/
_/    _/  _/_/_/_/    _/_/_/    _/_/_/  _/      _/            _/      _/    _/_/_/

                                  ^
                                 / \\ ^
    Sponsored by ...            ^  /\/  \\V  \/\
                               / \\/ // \\\\\ \\ \/\
                              // // BLACK HILLS \/ \\
                             www.blackhillsinfosec.com

                                www.practisec.com

                       [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.
```

- To get google website give this command.

```
[recon-ng][default] > marketplace search google
[*] Searching module index for 'google' ...

+-----------------------------------------------------------------------------------------+
|                Path                | Version |   Status  |  Updated   | D | K |
+-----------------------------------------------------------------------------------------+
| recon/domains-hosts/google_site_web | 1.0     | installed | 2019-06-24 |   |   |
+-----------------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.
[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
```

- You can see it’s not installed yet. We must download installation path.
- After installing path using show info to see its download or not.

```
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][default] > show info
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports
positories|vulnerabilities>
[recon-ng][default] > marketplace search google
```

- Load the installed module path and use info see options.

```
[recon-ng][default][google_site_web] > info

    Name: Google Hostname Enumerator
  Author: Tim Tomes (@lanmaster53)
 Version: 1.0

Description:
  Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with
  the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  blackrock.com  yes       source of input (see 'info' for details)

Source Options:
  default       SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>      string representing a single input
  <path>        path to a file containing a list of inputs
  query <sql>   database query returning one column of inputs
```

- Go to options and set source to our targeted domain https://indrive.com/ and run it.

```
[recon-ng][default][google_site_web] > options set source indrive.com
SOURCE ⇒ indrive.com
[recon-ng][default][google_site_web] > run
```

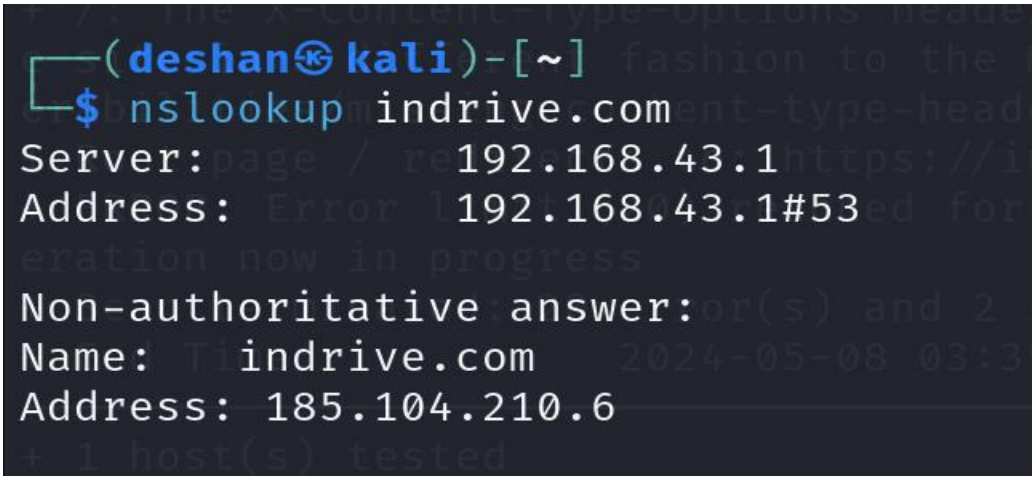
```
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: groupbuy.indrive.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: ventures.indrive.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
```

Getting alive subdomains

- Nslookup

A command-line utility called `nslookup` is used to query DNS (Domain Name System) servers and get DNS-related data. In addition to performing reverse DNS lookups and retrieving other DNS records like A, AAAA, MX, NS, PTR, and TXT records, it resolves domain names to IP addresses. It is flexible for diagnosing DNS problems, validating DNS configurations, and testing DNS servers because it may be used in both interactive and non-interactive modes. Network administrators and cybersecurity experts frequently utilize `nslookup`, which runs on several platforms, for DNS-related activities and diagnostics.

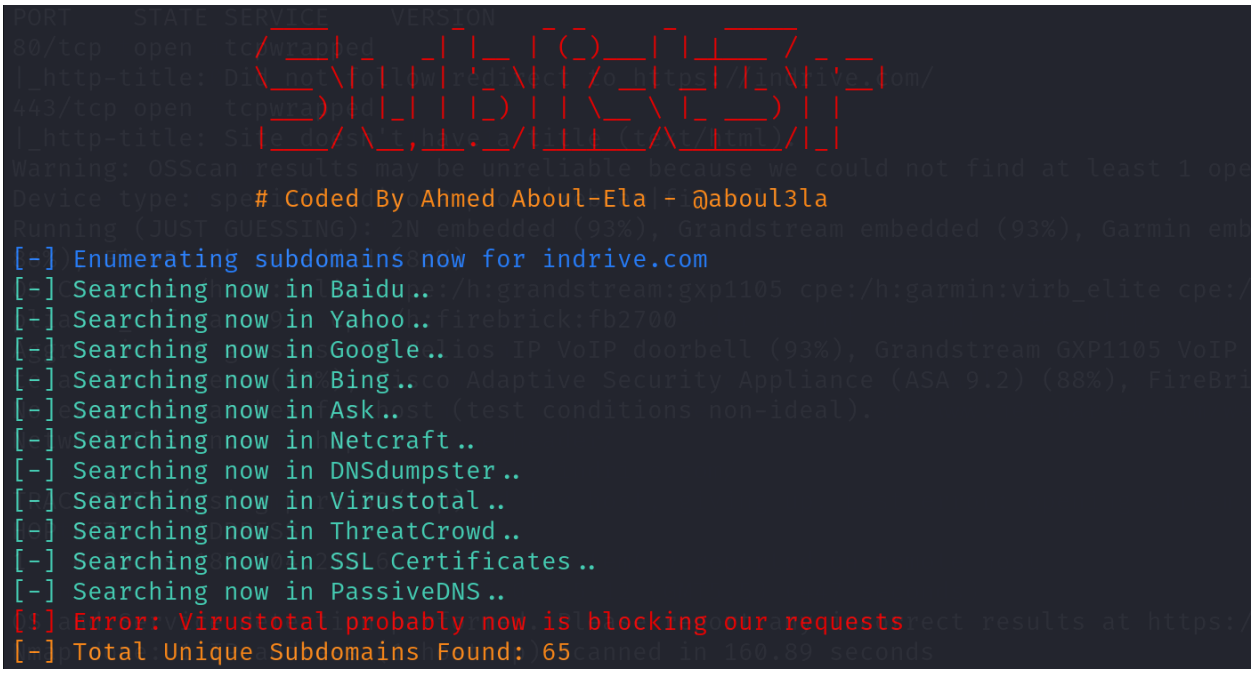
Proof of concept:



- Sublist3r

Sublist3r is an open-source subdomain enumeration tool used in cybersecurity for reconnaissance purposes. It assists security professionals, penetration testers, and researchers in identifying valid subdomains associated with a target domain. The tool employs various methods including passive search through search engine results, active search via DNS queries, and brute-force techniques using wordlists to enumerate subdomains. Sublist3r supports output in multiple formats, making it versatile for integration with other tools and workflows. It is valuable in expanding the attack surface during security assessments but should be used responsibly and with proper authorization.

Proof of concept:



Proof of concept:

```
www.indrive.com
beginit.indrive.com
www.beginit.indrive.com
book.indrive.com
www.book.indrive.com
careers.indrive.com
cargo.indrive.com
catalogue.indrive.com
www.catalogue.indrive.com
classified.indrive.com
compliance.indrive.com
couriers.indrive.com
cr.indrive.com
delivery.indrive.com
dxy.indrive.com
empleo.indrive.com
food.indrive.com
www.food.indrive.com
fr.indrive.com
freight.indrive.com
groupbuy.indrive.com
ic.indrive.com
id.indrive.com
inapps.indrive.com
```

Proof of concept:

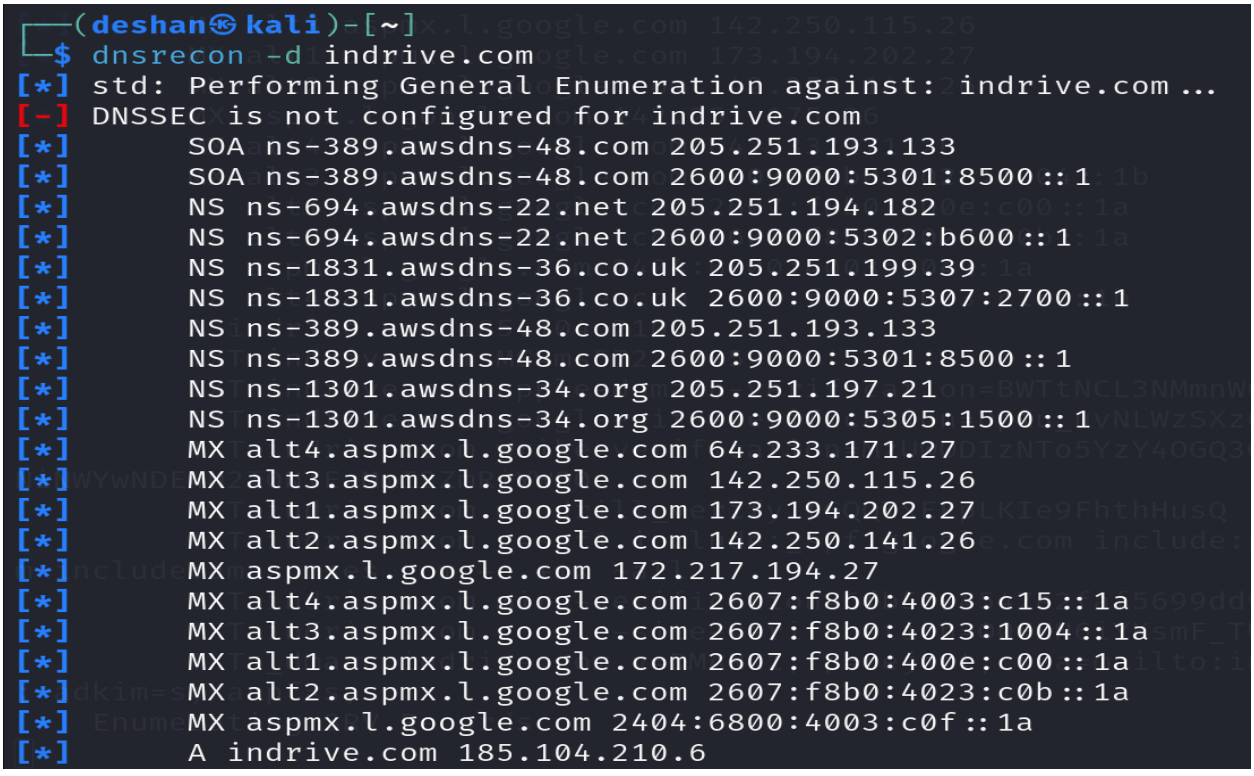
```
sale.indrive.com
www.sale.indrive.com
services.indrive.com
servicos.indrive.com
sgtm.indrive.com
share.indrive.com
sharetrip.indrive.com
sharetrip-origin.indrive.com
sparklab.indrive.com
www.sparklab.indrive.com
supernovas.indrive.com
www.supernovas.indrive.com
updrive.indrive.com
www.updrive.indrive.com
url-checker.indrive.com
us.indrive.com
ventures.indrive.com
wa-auth.indrive.com
yourpace.indrive.com
www.yourpace.indrive.com
```

DNS enumeration

- Dnsrecon

For security evaluations and penetration tests, DNSRecon is a powerful open-source tool for DNS reconnaissance that finds and counts DNS information. It is particularly good at finding subdomains, enumerating DNS records (A, AAAA, MX, NS, SOA, TXT), transferring DNS zones, and it can handle wordlist-based and brute-force attacks. With its automation, customization, and integration features, it's a useful tool for figuring out possible attack points, comprehending target infrastructure, and raising security awareness in general. DNSRecon is still a dependable option for DNS reconnaissance operations because of its community support and frequent updates.

Proof of concept:



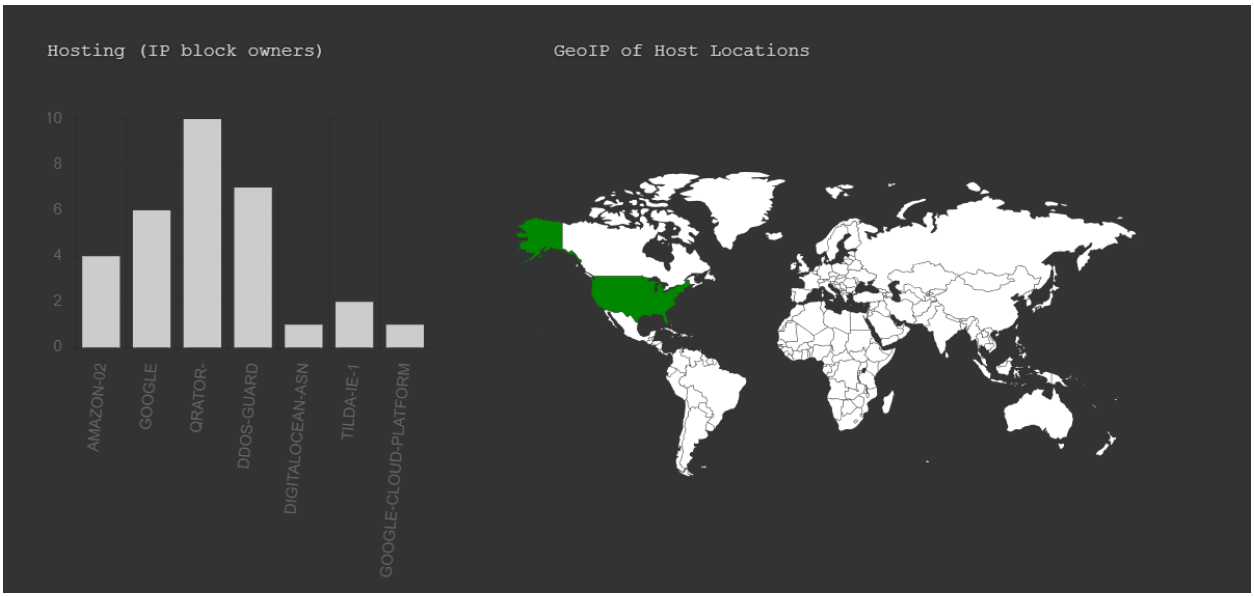
Proof of concept:

```
[*]      MX alt2.aspmx.l.google.com 142.250.141.26
[*]      MX aspmx.l.google.com 172.217.194.27
[*]      MX alt4.aspmx.l.google.com 2607:f8b0:4003:c15::1a
[*]      MX alt3.aspmx.l.google.com 2607:f8b0:4023:1004::1a
[*]      MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1a
[*]      MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*]      MX aspmx.l.google.com 2404:6800:4003:c0f::1a
[*]      A indrive.com 185.104.210.6
[*]      TXT indrive.com google-site-verification=Dpiu_uvNLWzSXz0v2lHl_cYjqeNZK4Yf76GfyE5oDVE
[*]      TXT indrive.com wrike-verification=MzUwODIzNTo5YzY4OGQ3OTNjNDcyYzdjNzhjODY2YjE4NzBlMTViZTE5ZDI1YzdjNj
NiNWYwNDE4N2I0NTEzMmI2ZmRiYWQ0
[*]      TXT indrive.com mandrill_verify.tGQQTxEEpLKIe9FhthHusQ
[*]      TXT indrive.com MS=ms57223185
[*]      TXT indrive.com miro-verification=6fb5d94547e2faf5699dd9b65349835d7a80fec8
[*]      TXT indrive.com apple-domain-verification=BWTtNCL3NMmnWCp3
[*]      TXT indrive.com google-site-verification=O0FZN6iYKsmF_TUd93SLa-Gyyyi0Cisa7pdbMgBrLiA
[*]      TXT indrive.com v=spf1 include:_spf.google.com include:spf.mandrillapp.com include:_spf.salesforce.co
m include:amazonses.com +a +mx ~all
[*]      TXT _dmarc.indrive.com v=DMARC1; p=reject; rua=mailto:indrivepostmaster@gmail.com; sp=reject; pct=100
; adkim=s; aspf=s;
[*] Enumerating SRV Records
[-] No SRV Records Found for indrive.com
```

- Dnsdumper
-

DNSDumpster is an online tool focused on DNS information gathering for a target domain. It assists in discovering subdomains, viewing DNS records (A, AAAA, MX, NS, SOA, TXT), mapping domain names to IP addresses, and providing visual representations of DNS-related data. Security professionals and penetration testers use DNSDumpster during reconnaissance to understand a domain's infrastructure, identify potential vulnerabilities, and aid in security assessments. While it offers valuable insights, users should supplement its findings with other tools for a comprehensive analysis, considering that its data may not always be the most current or complete.

- **Proof of concept:**



DNS Servers

ns-1301.awsdns-34.org.	205.251.197.21	AMAZON-02 United States
ns-1831.awsdns-36.co.uk.	205.251.199.39	AMAZON-02 United States
ns-389.awsdns-48.com.	205.251.193.133	AMAZON-02 United States
ns-694.awsdns-22.net.	205.251.194.182	AMAZON-02 United States

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

1 aspmx.l.google.com.	142.251.167.27	GOOGLE United States
10 alt3.aspmx.l.google.com.	142.250.27.26	GOOGLE United States
10 alt4.aspmx.l.google.com.	142.250.153.26	GOOGLE United States
5 alt1.aspmx.l.google.com.	209.85.202.27	GOOGLE United States
5 alt2.aspmx.l.google.com.	64.233.184.27	GOOGLE United States

- **Proof of concept:**

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

"MS=ms57223185"
"apple-domain-verification=BWTtNCL3NMmnWCp3"
"google-site-verification=Dpiu_uvNLWzSXz0v2lHl_cYjqeNZK4Yf76GfyE5oDVE"
"google-site-verification=O0FZN6iYKsmF_TUd93SLa-Gyyyi0Cisa7pdbMgBrLiA"
"mandrill_verify.tGQQTxEEpLKIe9FhthHusQ"
"miro-verification=6fb5d94547e2faf5699dd9b65349835d7a80fec8"
"v=spf1 include:_spf.google.com include:spf.mandrillapp.com include:_spf.salesforce.com include:amazonses.com +a +mx ~all"
"wrike-verification=MzUwODIzNTo5YzY4OGQ3OTNjNDcyYzdjNzhjODY2YjE4NzBlMTViZTE5ZDI1YzdjNjNiNWYwNDE4N2I0NTEzMmI2ZmRiYWQ0"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

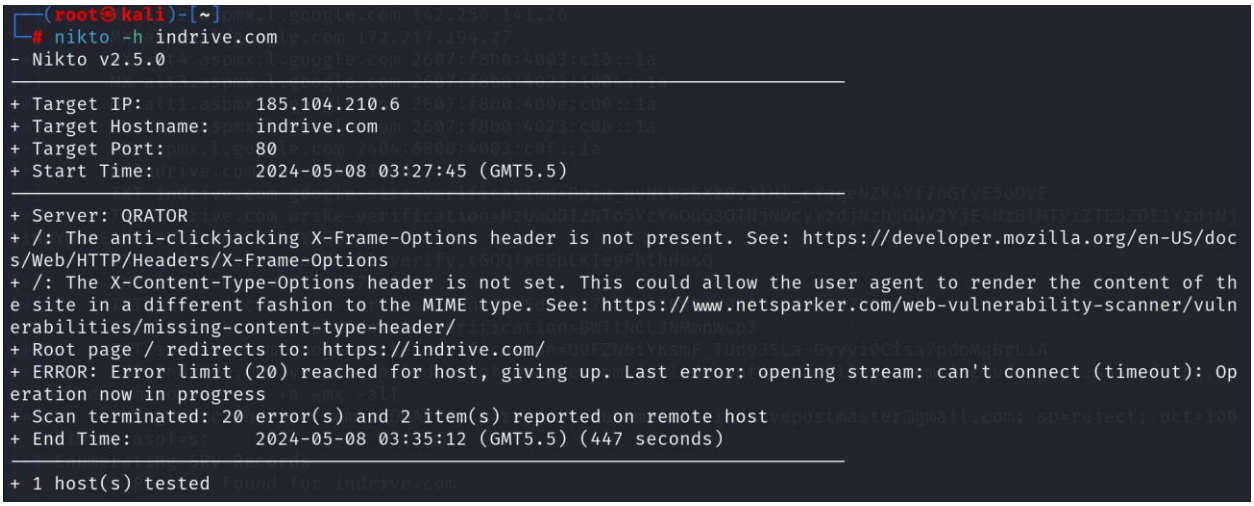
rabota.indrive.com HTTP: QRATOR	185.104.211.6	QRATOR- Czechia
job.indrive.com HTTP: ddos-guard	77.220.207.191	DDOS-GUARD Kazakhstan
injob.indrive.com HTTP: QRATOR	185.104.211.6	QRATOR- Czechia
classified.indrive.com HTTP: QRATOR	185.104.211.6	QRATOR- Czechia
id.indrive.com HTTP: nginx/1.18.0 (Ubuntu) SSH: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3 HTTP TECH: Ubuntu nginx,1.18.0	167.172.86.54	DIGITALOCEAN-ASN Singapore
lp-food.indrive.com	213.130.74.49	TILDA-IE-1 Finland
www.lp-food.indrive.com	213.130.74.49	TILDA-IE-1 Finland
rd.indrive.com HTTP: ddos-guard	185.215.4.20	DDOS-GUARD Russia
rideshare.indrive.com HTTP: QRATOR	185.104.211.6	QRATOR- Czechia

- Nikto

Nikto is an open-source web server scanner made to find possible security holes in applications and web servers. With its extensive scanning capabilities, it may

identify problems including out-of-date software, unsafe configurations, weak scripts, and incorrect SSL/TLS settings. In addition to producing comprehensive results after scanning, Nikto may be customized and scripted, connects with automated workflows, and receives community assistance and frequent database upgrades. For security experts performing web security assessments, it's a useful tool that helps with vulnerability discovery and mitigation to improve overall security posture.

Proof of concept:



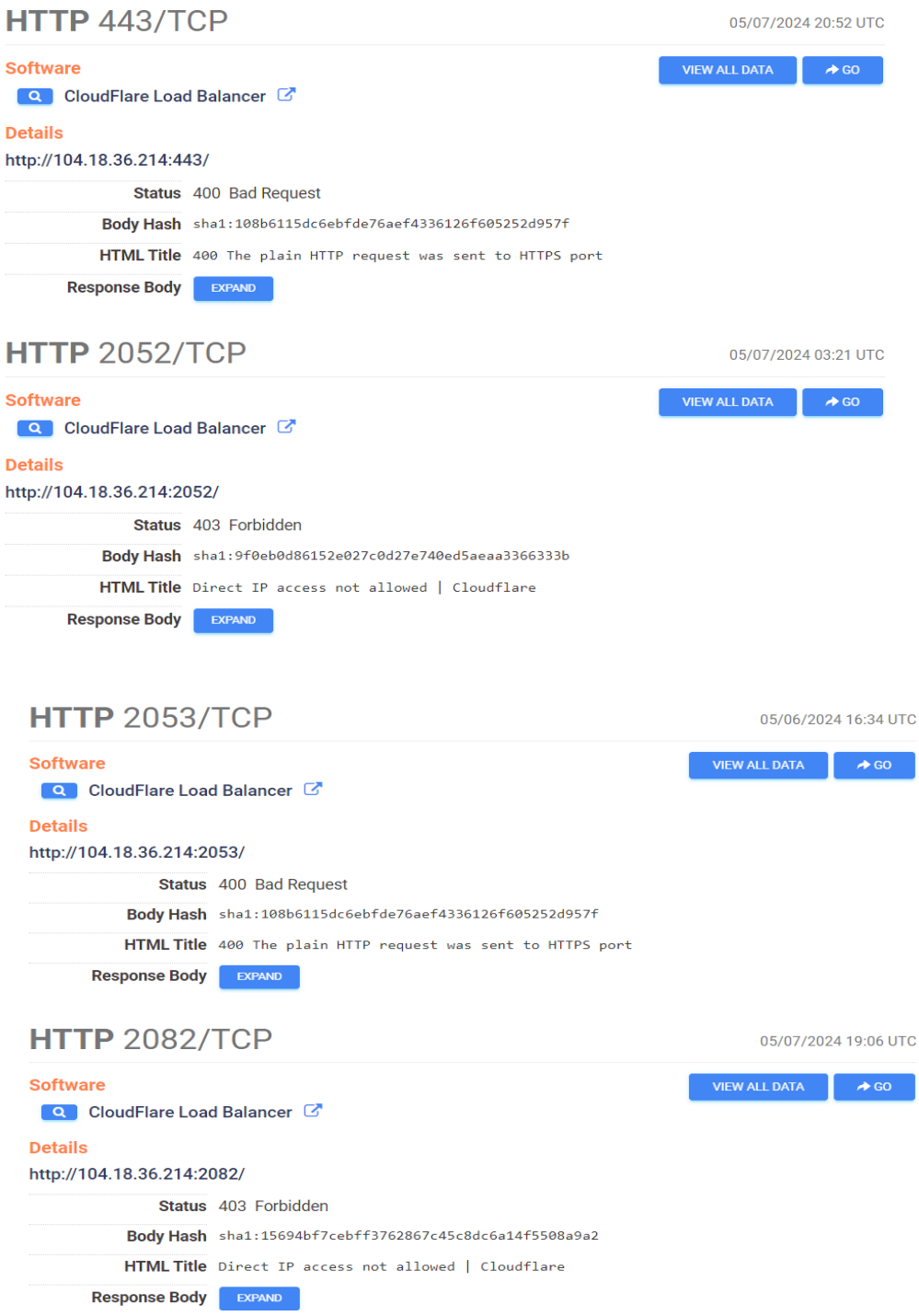
Public devices enumeration

- Censys

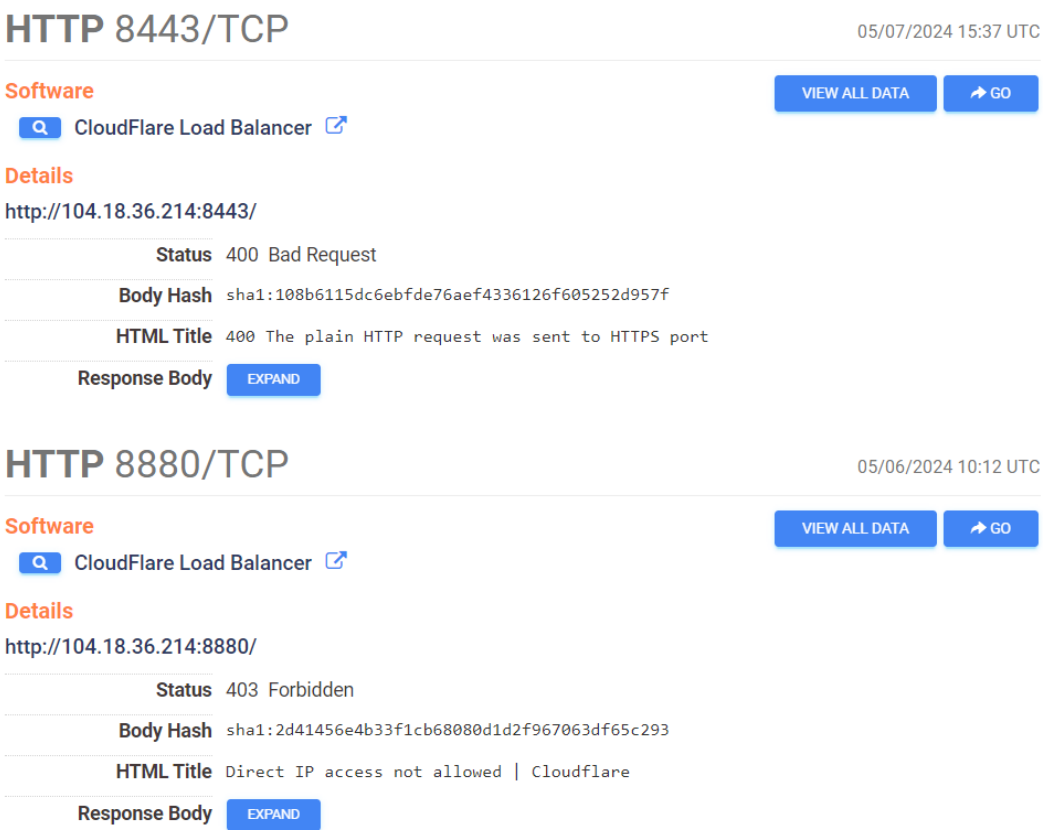
Censys is a potent internet scanning tool that scans and monitors devices, networks, and services online all the time. It performs thorough scans, keeps track of SSL/TLS certificates, keeps an eye on attack surfaces, finds vulnerabilities, and offers threat information. Large volumes of data may be searched and analyzed, processes can be automated with the help of the API, and Censys can be integrated into security workflows. In the connected digital world of today, Censys is useful for asset discovery, vulnerability management, compliance monitoring, and proactive risk reduction.

Proof of concept:

Proof of concept:



Proof of concept:



- Whois

A key networking tool and protocol, whois is used to query databases and obtain data on IP addresses, domain names, and autonomous system numbers (ASNs). It offers information about domain registration, owner contact details, DNS information, IP address allocation, and ASN ownership. Whois is frequently used for domain research, network problems, IP geolocation, abuse investigations, and domain registration questions by network administrators, cybersecurity experts, domain registrars, and law enforcement organizations. Due to privacy concerns, registrars have started offering privacy services that conceal personal information from view in public Whois data. While Whois provides insightful information, users should be aware of potential limits across multiple Whois servers, privacy concerns, and data accuracy.

Proof of concept:

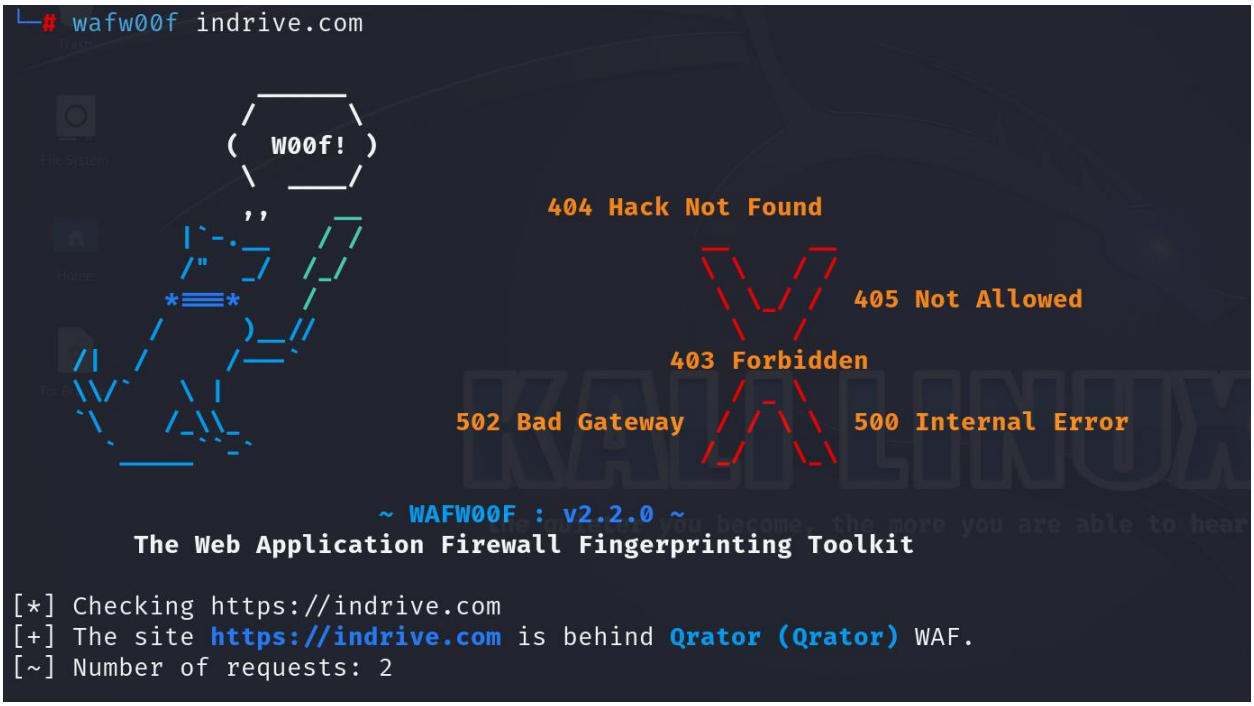
```
┌──(root㉿kali)-[~]
└─# whois indrive.com
   Domain Name: INDRIVE.COM
   Registry Domain ID: 5342839_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://cscdbs.com
   Updated Date: 2023-12-04T14:54:15Z
   Creation Date: 1998-04-08T04:00:00Z
   Registry Expiry Date: 2025-04-07T04:00:00Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS-1301.AWSDNS-34.ORG
   Name Server: NS-1831.AWSDNS-36.CO.UK
   Name Server: NS-389.AWSDNS-48.COM
   Name Server: NS-694.AWSDNS-22.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-05-07T22:37:39Z <<<

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

Domain Name: indrive.com
Registry Domain ID: 5342839_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2023-12-04T09:54:15Z
Creation Date: 1998-04-08T00:00:00Z
Registrar Registration Expiration Date: 2025-04-07T04:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Manager
Registrant Organization: SUOL INNOVATIONS LTD
Registrant Street: 41 Themistokli Dervi, Hawaii Tower, 1ST Floor, Office 106
Registrant City: Nicosia
Registrant State/Province: Nicosia
Registrant Postal Code: 1066
Registrant Country: CY

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

Corporation Service Company(c) (CSC)  The Trusted Partner of More than 50% of the 100 Best Global Brands.

Contact us to learn more about our enterprise solutions for Global Domain Name Registration and Management, Tr
ademark Research and Watching, Brand, Logo and Auction Monitoring, as well SSL Certificate Services and DNS Ho
sting.

NOTICE: You are not authorized to access or query our WHOIS database through the use of high-volume, automated
, electronic processes or for the purpose or purposes of using the data in any manner that violates these term
s of use. The Data in the CSC WHOIS database is provided by CSC for information purposes only, and to assist p
ersons in obtaining information about or related to a domain name registration record. CSC does not guarantee
its accuracy. By submitting a WHOIS query, you agree to abide by the following terms of use: you agree that yo
u may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) al
low, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitation
s via direct mail, e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes
 that apply to CSC (or its computer systems). CSC reserves the right to terminate your access to the WHOIS dat
abase in its sole discretion for any violations by you of these terms of use. CSC reserves the right to modify
 these terms at any time.

Register your domain name at http://www.cscglobal.com
```

Find WAF (web application firewall) protection.

- Wafwoof

Wafw00f is an open-source program that uses content patterns, HTTP responses, and header analysis to detect and fingerprint web application firewalls (WAFs). It gives testers and security experts information about the particular WAF technology or vendor being used as well as assists them in determining whether a web application is protected by a WAF. In addition to being user-friendly and seamlessly integrating with automated testing workflows, Wafw00f also keeps an updated database of WAF signatures and offers community support. It is a useful tool for security assessment and reconnaissance jobs, supporting the creation of efficient testing plans and workarounds.

Proof of concept:



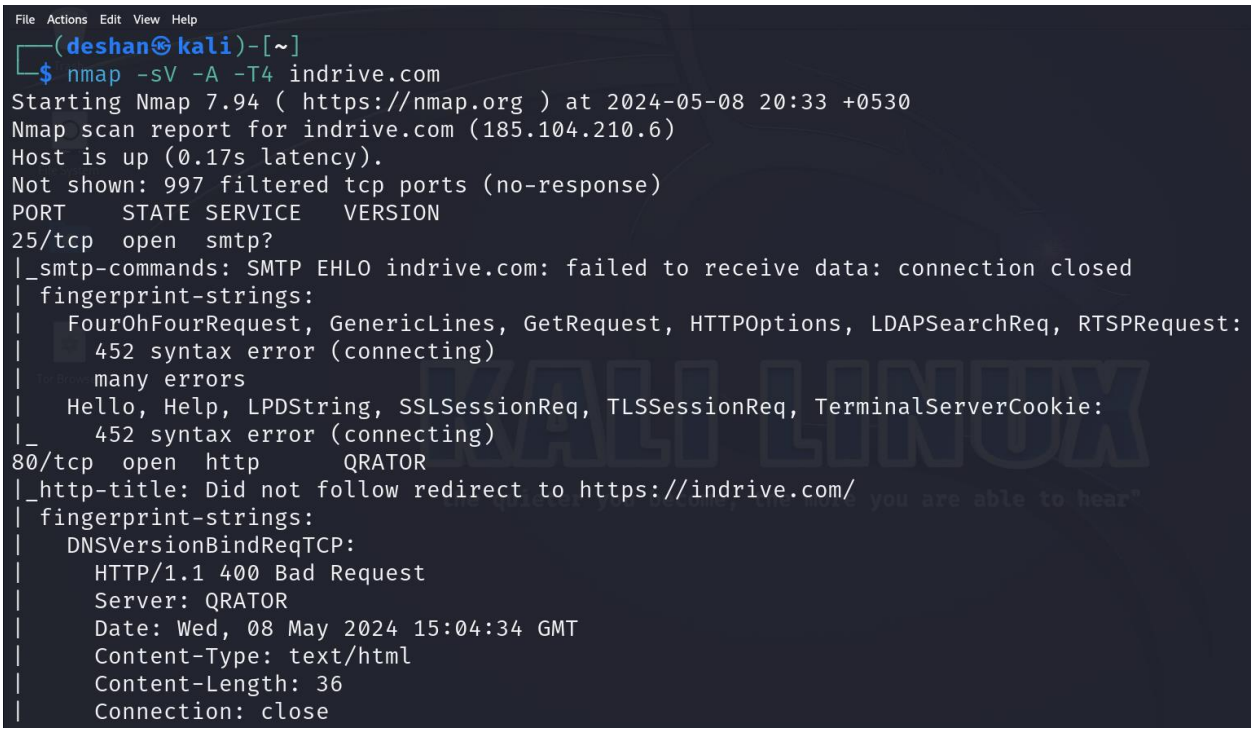
Find open ports.

- Nmap

Nmap, sometimes known as "Network Mapper," is a potent open-source network scanning program used for vulnerability analysis, security audits, and network

discovery. It is particularly good at operating system detection, host discovery, port scanning, and service version detection. Because it supports custom scripting and automation, Nmap's scripting engine (NSE) is adaptable to a wide range of security activities and integration requirements. Because of its dependability, adaptability, and large feature set, network administrators, security experts, and penetration testers frequently use it for network reconnaissance, security audits, and network monitoring.

Proof of concept:



Proof of concept:

```
|     <html>
|     QRATOR HTTP 400
|     </html>
|   FourOhFourRequest:
|     HTTP/1.1 400 Bad Request
|     Server: QRATOR
|     Date: Wed, 08 May 2024 15:04:28 GMT
|     Content-Type: text/html
|     Content-Length: 150
|     Connection: close
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     <hr><center>nginx</center>
|     </body>
|     </html>
|   GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad Request
|     Server: QRATOR
|     Date: Wed, 08 May 2024 15:04:27 GMT
|     Content-Type: text/html
|     Content-Length: 150
|     Connection: close
|     <html>
```

```
443/tcp open  ssl/https QRATOR
|_http-server-header: QRATOR
| http-robots.txt: 55 disallowed entries (15 shown)
| */?shortlink= */?fbclid= */?redirected= */?ref=www
| */?news_id= */s/ /*% /*%20 */blog_driver */?yandex-source
| */?utm_source= */mobile/page */hi/blog/[id] */kz/blog/[id]
|_*/ne/blog/[id]
| http-title: Offer Your Fare With InDrive Service
|_Requested resource was /en/home/
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 400 Bad Request
|     Server: QRATOR
|     Date: Wed, 08 May 2024 15:04:35 GMT
|     Content-Type: text/html
|     Content-Length: 150
|     Connection: close
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     <hr><center>nginx</center>
|     </body>
```

Proof of concept:

Exploitation

- Sqlmap

Web applications with SQL injection vulnerabilities can be automatically found and exploited with SQLMap, an open-source penetration testing tool. It employs a number of detecting methods, supports a number of database management systems, and provides customization choices. Security experts and penetration testers find SQLMap useful as it automates testing, enumeration, data extraction, and reporting procedures during security assessments. It should, therefore, be utilized sensibly, morally, and with the appropriate authorization to test programs and systems.

Proof of concept:

```
┌──(root㉿kali)-[~]
└─# sqlmap -u 'https://services.indrive.com/auth/'
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.9#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
 end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liabilit
y and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:44:03 /2024-05-08/

[20:44:03] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.
php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] Y
[20:44:07] [INFO] testing connection to the target URL
got a 301 redirect to 'https://services.indrive.com/auth'. Do you want to follow? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('abidv0=6013189450435973'). Do you want to
 use those [Y/n] Y
[20:44:16] [INFO] checking if the target is protected by some kind of WAF/IPS
[20:44:20] [WARNING] reflective value(s) found and filtering out
[20:44:20] [INFO] testing if the target URL content is stable
```

```
other non-custom parameters found. Do you want to process them too? [Y/n/q] Y
[20:44:25] [WARNING] URI parameter '#1*' does not appear to be dynamic
[20:44:26] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:44:28] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[20:44:30] [INFO] testing for SQL injection on URI parameter '#1*'
[20:44:30] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[20:44:45] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[20:44:49] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTV
ALUE)'
[20:44:56] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[20:45:02] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[20:45:08] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[20:45:13] [INFO] testing 'Generic inline queries'
[20:45:15] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[20:45:19] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[20:45:23] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[20:45:28] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[20:45:33] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[20:45:38] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[20:45:43] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique f
ound. Do you want to reduce the number of requests? [Y/n] Y
```

```
[20:46:28] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[20:46:34] [WARNING] URI parameter '#1*' does not seem to be injectable
[20:46:34] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--leve
l'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection me
chanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/o
r switch '--random-agent'
[20:46:34] [WARNING] your sqlmap version is outdated

[*] ending @ 20:46:34 /2024-05-08/
```

Vulnerability analysis phase

Targeted Domain: - https://indrive.com/

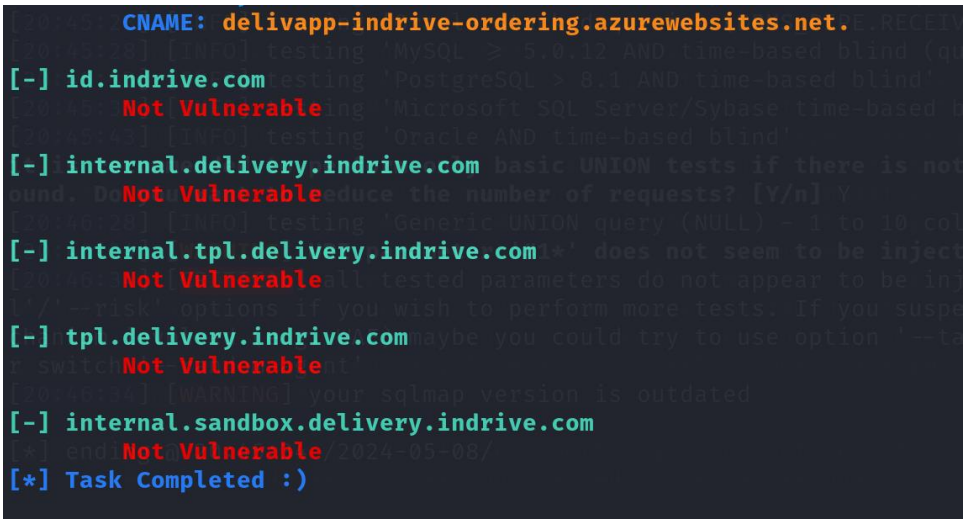
I used tools like sub404 and Netsparker to process and catch bugs and vulnerabilities based on OWASP top 10.

- Sub 404 used to Test any subdomain takeovers that happen.

I’m testing my target domain indrive.com to find any vulnerabilities in their subdomains. After this test no vulnerabilities are found in these subdomains.

Proof of concept:

Proof of concept:



- Netsparker

Netsparker is a web application security scanner used to identify vulnerabilities in web applications and websites. It automates the process of scanning web applications for security issues such as SQL injection, cross-site scripting (XSS), and other vulnerabilities that could be exploited by attackers. Netsparker works by analyzing the web application's source code, identifying potential security flaws, and providing detailed reports to help developers and security professionals mitigate these risks. It’s a valuable tool in the arsenal of cybersecurity professionals to ensure the safety and integrity of web applications.

Vulnerability title

Missing X-Frame-Options Header

- Vulnerability description

The "Missing X-Frame-Options Header" vulnerability refers to a security flaw in web applications where the server fails to include the X-Frame-Options HTTP header in its responses. This header helps prevent clickjacking attacks by controlling whether a web page can be displayed within an iframe on another site. Developers can mitigate this vulnerability by setting the appropriate X-Frame-Options header (e.g., SAMEORIGIN) in their server configurations or web application code.

- Impact assessment

The "Missing X-Frame-Options Header" vulnerability can have significant consequences:

1. Clickjacking Attacks: Allows attackers to embed vulnerable pages on malicious sites, leading to unauthorized actions by users.

2. Data Leakage: Sensitive data on vulnerable pages can be accessed or manipulated without user consent.

3. Spoofing and Phishing: Enables attackers to trick users into providing sensitive information on fake sites.

4. Reputation Damage: Exploitation can harm the trust and reputation of the affected website or application.

5. Regulatory Issues: Non-compliance with data security standards may result in legal consequences.

Mitigation involves setting proper X-Frame-Options headers (e.g., `X-Frame-Options: SAMEORIGIN`), regular security assessments, developer education, and staying updated on security threats.

- Affected components

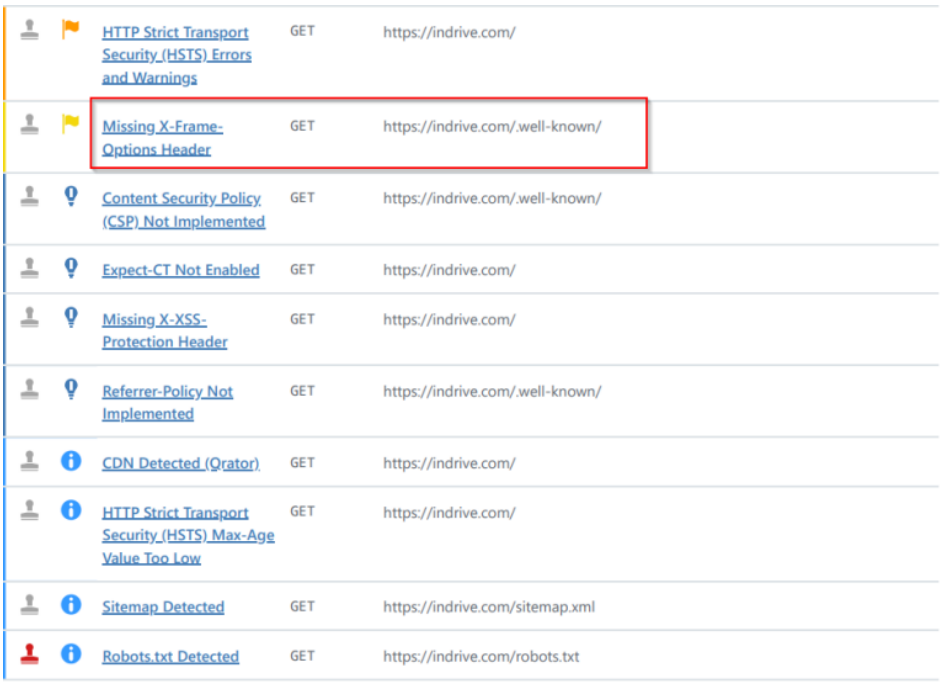
The "Missing X-Frame-Options Header" vulnerability affects various components of web applications, including web pages, web applications themselves, CMS platforms, third-party integrations, API endpoints, authentication pages, and pages containing sensitive data. Attackers exploit this vulnerability through clickjacking attacks, potentially leading to data leakage, spoofing, phishing, reputation damage, and regulatory non-compliance.

- How to mitigate?

There are a few important actions that may be taken to mitigate the "Missing X-Frame-Options Header" vulnerability and stop clickjacking

attacks. First, make sure that the X-Frame-Options HTTP header, which controls framing rights with values like DENY, SAMEORIGIN, or ALLOW-FROM, is included in the answers from your web server or application. Frame-ancestors directives in a Content Security Policy (CSP) can be used to further limit framing to domains that are approved. An additional line of protection against unwanted framing attempts is provided by the inclusion of a frame-busting script in web pages. To find and fix any vulnerabilities or misconfigurations, do routine security audits. Additionally, train your development team on web security best practices. To proactively defend against changing threats and keep your web applications' security posture strong, stay up to current on security updates and industry trends.

Proof of concept:



HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://indrive.com/
Missing X-Frame-Options Header	GET	https://indrive.com/.well-known/
Content Security Policy (CSP) Not Implemented	GET	https://indrive.com/.well-known/
Expect-CT Not Enabled	GET	https://indrive.com/
Missing X-XSS-Protection Header	GET	https://indrive.com/
Referrer-Policy Not Implemented	GET	https://indrive.com/.well-known/
CDN Detected (Qrator)	GET	https://indrive.com/
HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	GET	https://indrive.com/
Sitemap Detected	GET	https://indrive.com/sitemap.xml
Robots.txt Detected	GET	https://indrive.com/robots.txt

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

2.1. https://indrive.com/.well-known/

Certainty

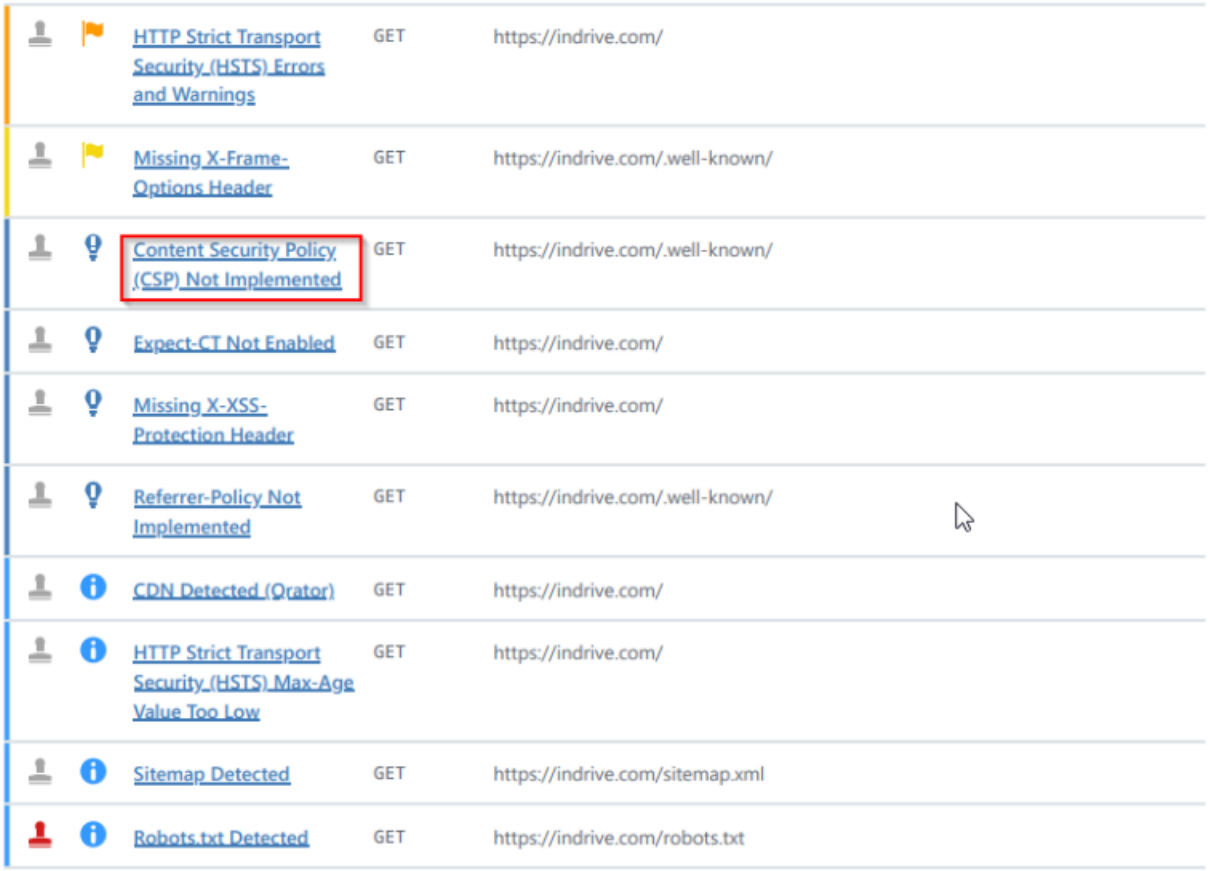
Proof of concept:

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
  - `X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
  - `X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
  - `X-Frame-Options: ALLOW-FROM` *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

Other vulnerabilities were identified during the scan.

- CSP (content security policy) not implemented.



Proof of concept:

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

Vulnerabilities

3.1. https://indrive.com/.well-known/

Certainty

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.

Conclusion

Your reconnaissance phase is comprehensive, utilizing tools like Recon-ng, Nslookup, Sublist3r, Dnsrecon, Dnsdumper, Nikto, Censys, Whois, Wafw00f, and Nmap to gather information about subdomains, DNS information, web application firewalls, open ports, and more. This information provides a foundation for further analysis and testing.

Moving into the vulnerability analysis phase, you've identified specific vulnerabilities like Weak Ciphers Enabled, Phishing Risks, Missing X-XSS-Protection Header, and Forbidden Resource, among others. Each vulnerability is described in detail, including its impact and mitigation strategies.