

# **Sri Lanka Institute of Information Technology**




## **WEB SECURITY (IE2062)**

### **BUG BOUNTY REPORT 1**

**Thilakarathna S.T.D- IT22578914**

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

# Overview of the website



**inDrive**  
inDrive is a global mobility and urban services platform with over 150 million downloads in more than 700 cities across 47 countries.  
<https://indrive.com/> · @indrive

Reports resolved  
95

Assets in scope  
28

Average bounty  
\$150-\$300

[Submit report](#)  
[Give feedback](#)

Bug Bounty Program  
Launched in Feb 2023

Collaboration enabled ⓘ

[Bookmarked](#) [Subscribe](#)

[Overview](#) [Scope](#) [Hacktivity](#) [Thanks](#) [Updates \(3\)](#) [Collaborators](#)

**Rewards**

Last updated on July 17, 2023. [View changes](#)

Low	Medium	High	Critical
Avg. bounty \$106 29.89% submissions	Avg. bounty \$487 47.70% submissions	Avg. bounty \$820 13.79% submissions	Avg. bounty \$1,311 8.62% submissions
\$50	\$150	\$750-\$1,500	\$2,000-\$8,000

The list of vulnerabilities that can be rewarded and their severity are listed in the table at the end of the rules.

**Response Efficiency**

4 hours  
Average time to first response

4 hours  
Average time to triage

6 days, 20 hours  
Average time from triage to bounty

InDrive is a market leader operating in the largest cities in highly competitive marketplaces. Moreover, it functions well in small towns with 7,000–8,000 residents, many of which lack maps and have erratic internet access. Every hamlet, town, or metropolis can have its demands successfully met by us.

# Scope

## • InScope

priority.eu-east-1.indriverapp.com Amazon Web Services IBM Cloud Kubernetes MySQL Nginx Redis	Domain	In scope	Critical	Eligible	Apr 4, 2023	0 (0%)
messenger.eu-east-1.indriverapp.com Go IBM Cloud Kubernetes MySQL Nginx Redis	Domain	In scope	Critical	Eligible	Apr 4, 2023	0 (0%)
external.indrive.dev	Domain	In scope	Critical	Eligible	Dec 14, 2023	0 (0%)
aws.indrive.tech	Domain	In scope	Critical	Eligible	Dec 14, 2023	0 (0%)
debug.clairvoyance.indrive.tech	Domain	In scope	Critical	Eligible	Dec 14, 2023	0 (0%)
ingest.clairvoyance.indrive.tech	Domain	In scope	Critical	Eligible	Dec 14, 2023	0 (0%)
https://*.indriverjob.com	Wildcard	In scope	Critical	Eligible	Sep 26, 2023	0 (0%)
intercity-*.eu-east-1.indriverapp.com Go MySQL Nginx	Wildcard	In scope	Critical	Eligible	May 15, 2023	12 (13%)
watchdocs.indriverapp.com Docker Google Cloud Platform JavaScript MySQL Nginx PHP Redis VUE	Domain	In scope	Critical	Eligible	Apr 4, 2023	24 (25%)
wga.volans.tech	Domain	In scope	Critical	Eligible	Sep 26, 2023	0 (0%)
https://*.indriver.io	Wildcard	In scope	Critical	Eligible	Sep 26, 2023	0 (0%)
super-services.indriverapp.com Go Kubernetes MySQL Nginx	Domain	In scope	Critical	Eligible	Apr 4, 2023	16 (17%)
auth2.indrive.tech	Domain	In scope	Critical	Eligible	Dec 14, 2023	0 (0%)
cargo.indrive.com Go MySQL Redis	Domain	In scope	Critical	Eligible	Jul 19, 2023	15 (16%)
ab-platform-api.eu-east-1.indriverapp.com Amazon Web Services Go IBM Cloud JavaScript MySQL Nginx React	Domain	In scope	Critical	Eligible	Apr 4, 2023	0 (0%)
terra-*.indriverapp.com IBM Cloud MySQL Nginx PHP	Wildcard	In scope	Critical	Eligible	May 15, 2023	196 (206%)

argocd.indrive.dev	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Dec 14, 2023	1 (1%)
file-storage-front.eu-east-1.indriverapp.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Apr 4, 2023	0 (0%)
<div>Amazon Web Services</div> <div>Go</div> <div>MySQL</div> <div>Redis</div>	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Apr 4, 2023	0 (0%)
injob.indriver.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Apr 4, 2023	91 (96%)
<div>Amazon Web Services</div> <div>Docker</div> <div>Elastic Search</div> <div>JavaScript</div> <div>MySQL</div> <div>Nginx</div> <div>React</div>	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Apr 4, 2023	91 (96%)
truck-api.eu-east-1.indriverapp.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Apr 4, 2023	20 (21%)
<div>Go</div> <div>IBM Cloud</div> <div>MySQL</div> <div>Nginx</div>	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Apr 4, 2023	20 (21%)
new-order.eu-east-1.indriverapp.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Apr 4, 2023	150 (158%)
<div>Amazon Web Services</div> <div>Go</div> <div>Kubernetes</div> <div>MySQL</div> <div>Redis</div>	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Apr 4, 2023	150 (158%)
volans.tech	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Sep 26, 2023	4 (4%)
profile-api.eu-east-1.indriverapp.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Apr 4, 2023	3 (3%)
<div>Amazon Web Services</div> <div>Go</div> <div>MySQL</div>	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Apr 4, 2023	3 (3%)
ci.indrive.dev	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Dec 14, 2023	0 (0%)
*.indrive.com	Wildcard	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Jul 11, 2023	28 (29%)
auth.indrive.tech	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	Dec 14, 2023	1 (1%)
*.indriverapp.com	Wildcard	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	May 15, 2023	216 (227%)
<div>Amazon Web Services</div> <div>Elastic Search</div> <div>Go</div> <div>Google Cloud Platform</div> <div>GraphQL</div> <div>IBM Cloud</div> <div>MySQL</div> <div>PHP</div> <div>Redis</div>	Wildcard	In scope	<div><div></div></div> Critical	<div><div></div></div> Eligible	May 15, 2023	216 (227%)
*.indriver.com	Wildcard	In scope	<div><div></div></div> Medium	<div><div></div></div> Eligible	May 15, 2023	6 (6%)

## OutScope

sinet.startup.inDriver	Android: Play Store	Out of scope	<div><div></div></div> None	<div><div></div></div> Ineligible	Feb 27, 2023	0 (0%)
servicos.indrive.com	Domain	Out of scope	<div><div></div></div> None	<div><div></div></div> Ineligible	May 4, 2023	0 (0%)

# Information Gathering

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

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

## Subdomains for Hunting

Subdomain enumeration involves using Kali Linux's robust tools to locate and list subdomains that are linked to a target domain. Through the identification of potential entry points and weak spots, this process helps security experts and ethical hackers assess the company's digital environment. Due to its array of tools, including `Sublist3r` and `Amass` for DNS searches, search engine scraping, and other techniques, Kali Linux is a well-liked platform for security evaluations.

- **Sublist3r**

Sublist3r is an open-source tool used for efficient subdomain enumeration. Penetration testers, security experts, and ethical hackers use Sublist3r to locate subdomains linked to a target website. It accomplishes this by using methods like search engine scraping and DNS queries. Sublist3r only needs the target domain to be input; once that is done, it will look for related subdomains on its own and provide useful data that can be used for vulnerability assessments and security evaluations.

```

(tharusha@kali)-[~]
$ sublist3r -d indrive.com

File System
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for indrive.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 65
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
groupon.indrive.com
ic.indrive.com
id.indrive.com
inapps.indrive.com
inapps2.indrive.com
inapps3.indrive.com
injob.indrive.com

```

```
intercity.indrive.com
www.intercity.indrive.com
job.indrive.com
landing.indrive.com
lp-food.indrive.com
www.lp-food.indrive.com
lp-services.indrive.com
www.lp-services.indrive.com
media.indrive.com
money.indrive.com
movie.indrive.com
promo.indrive.com
promotion.indrive.com
rabota.indrive.com
rd.indrive.com
ref.indrive.com
rideshare.indrive.com
s.indrive.com
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
```





















- **Dnsdumpster**

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

Result of indrive.com





















dns recon & research, find & lookup dns records

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.    	172.253.122.26	GOOGLE United States
10 alt3.aspmx.l.google.com.    	142.250.27.27	GOOGLE United States
10 alt4.aspmx.l.google.com.    	142.250.153.27	GOOGLE United States
5 alt1.aspmx.l.google.com.    	209.85.202.26	GOOGLE United States
5 alt2.aspmx.l.google.com.    	64.233.184.27	GOOGLE United States

TXT Records

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

"MS=ms57223185"
"apple-domain-verification=BWtNCL3NMmnWCp3"
"google-site-verification=Dpiu_uvNLWzSXz0v2lHl_cYjqeNZK4Yf76GfyE5oDVE"
"google-site-verification=00FZN6iYKsmF_TUd93SLa-6yyyi0Cisa7pdbMgBrLiA"
"mandrill_verify.t6QQTxEEpLKIE9FhthHusQ"
"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=MzUwODIzNT05YzY4OGQ3OTNjNDcyYzdjNzhjODY2YjE4NzB1MTViZTE5ZDI1YzdjNjNlNmYwNDE4N2I0NTEzMmI2ZmRlYWQ0"

- **DNSrecon**

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



```

(tharusha@kali)-[~]
$ dnsrecon -d indrive.com
[*] std: Performing General Enumeration against: indrive.com...
[-] DNSSEC is not configured for indrive.com
[*] SOA ns-389.awsdns-48.com 205.251.193.133
[*] SOA ns-389.awsdns-48.com 2600:9000:5301:8500::1
[*] NS ns-694.awsdns-22.net 205.251.194.182
[*] NS ns-694.awsdns-22.net 2600:9000:5302:b600::1
[*] NS ns-1301.awsdns-34.org 205.251.197.21
[*] NS ns-1301.awsdns-34.org 2600:9000:5305:1500::1
[*] NS ns-389.awsdns-48.com 205.251.193.133
[*] NS ns-389.awsdns-48.com 2600:9000:5301:8500::1
[*] NS ns-1831.awsdns-36.co.uk 205.251.199.39
[*] NS ns-1831.awsdns-36.co.uk 2600:9000:5307:2700::1
[*] MX aspmx.l.google.com 74.125.68.27
[*] MX alt4.aspmx.l.google.com 64.233.171.26
[*] MX alt2.aspmx.l.google.com 142.250.141.27
[*] MX alt1.aspmx.l.google.com 173.194.202.27
[*] MX alt3.aspmx.l.google.com 142.250.115.26
[*] MX aspmx.l.google.com 2404:6800:4003:c02::1a
[*] MX alt4.aspmx.l.google.com 2607:f8b0:4003:c15::1b
[*] MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1b
[*] MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1a
[*] MX alt3.aspmx.l.google.com 2607:f8b0:4023:1004::1a
[*] A indrive.com 185.104.210.6
[*] 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

```

- **Wafw00f**


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

We can see that Qrator WAF is protecting indrive.com.

```

(tharusha@kali)-[~/PwnXSS]
$ wafw00f indrive.com

```



```

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

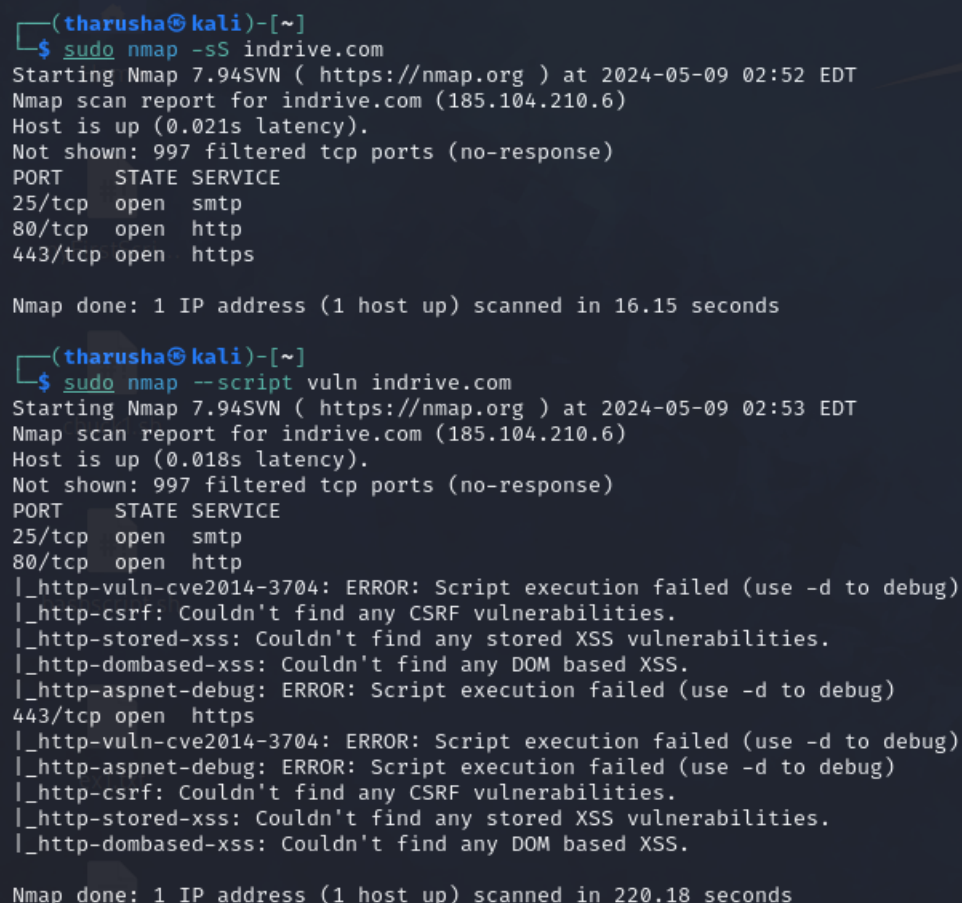
[*] Checking https://indrive.com
[+] The site https://indrive.com is behind Qrator (Qrator) WAF.
[~] Number of requests: 2

```

- **Using nmap, open port enumeration**

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

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



```
(tharusha@kali)-[~]
$ sudo nmap -sS indrive.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 02:52 EDT
Nmap scan report for indrive.com (185.104.210.6)
Host is up (0.021s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 16.15 seconds

(tharusha@kali)-[~]
$ sudo nmap --script vuln indrive.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 02:53 EDT
Nmap scan report for indrive.com (185.104.210.6)
Host is up (0.018s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
443/tcp    open  https
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.

Nmap done: 1 IP address (1 host up) scanned in 220.18 seconds
```

- **Using Nikto to scan for vulnerabilities**

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

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

```
(tharusha@kali)-[~]
$ sudo nikto -h indrive.com
- Nikto v2.5.0

+ Target IP:      185.104.210.6
+ Target Hostname: indrive.com
+ Target Port:    80
+ Start Time:    2024-05-09 03:08:11 (GMT-4)

+ Server: QRATOR
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
sing-content-type-header/
+ Root page / redirects to: https://indrive.com/
^C

(tharusha@kali)-[~]
$ sudo nikto -h 185.104.210.6
- Nikto v2.5.0

+ Target IP:      185.104.210.6
+ Target Hostname: 185.104.210.6
+ Target Port:    80
+ Start Time:    2024-05-09 03:08:24 (GMT-4)

+ Server: QRATOR
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
sing-content-type-header/
+ Root page / redirects to: https://185.104.210.6/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress
+ Scan terminated: 20 error(s) and 2 item(s) reported on remote host
+ End Time:      2024-05-09 03:17:16 (GMT-4) (532 seconds)

+ 1 host(s) tested
```

## Exploitation

I employed PWNXSS and SQLMAP tools to identify cross-site and SQL injection vulnerabilities in the target web application for the exploitations.

PwnXSS is a free and open-source application that may be found on GitHub. This program especially detects cross-site scripting. I execute several payloads in numerous web application directories while testing my target domain for XSS vulnerabilities. After the test, I discovered that indrive.com had no XSS vulnerabilities.

```

[06:12:59] [INFO] Checking connection to: https://indrive.com/id/safety
[06:13:00] [INFO] Connection established 200
[06:13:00] [WARNING] Found link with query: categoryIndex=0&subcategoryId=0 Maybe a vuln XSS point
[06:13:00] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<script>alert(6000/3000)</script>
[06:13:00] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<X3CscriptX3EalertX286000X2F3000X293X2FscriptX3EsubcategoryId=X3CscriptX3EalertX286000X2F3000X293X2FscriptX3E
[06:13:11] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[06:13:12] [INFO] Checking connection to: https://indrive.com/id/safety/
[06:13:13] [INFO] Connection established 200
[06:13:14] [WARNING] Found link with query: categoryIndex=0&subcategoryId=0 Maybe a vuln XSS point
[06:13:14] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<script>alert(6000/3000)</script>
[06:13:14] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<X3CscriptX3EalertX286000X2F3000X293X2FscriptX3EsubcategoryId=X3CscriptX3EalertX286000X2F3000X293X2FscriptX3E
[06:13:14] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<X3CscriptX3EalertX286000X2F3000X293X2FscriptX3EsubcategoryId=X3CscriptX3EalertX286000X2F3000X293X2FscriptX3E
[06:13:28] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[06:13:29] [INFO] Checking connection to: https://indrive.com/ms/safety
[06:13:30] [INFO] Connection established 200
[06:13:31] [WARNING] Found link with query: categoryIndex=0&subcategoryId=0 Maybe a vuln XSS point
[06:13:31] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<script>alert(6000/3000)</script>
[06:13:31] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<X3CscriptX3EalertX286000X2F3000X293X2FscriptX3EsubcategoryId=X3CscriptX3EalertX286000X2F3000X293X2FscriptX3E
[06:13:35] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[06:13:38] [INFO] Checking connection to: https://indrive.com/ms/safety/
[06:13:39] [INFO] Connection established 200
[06:13:39] [WARNING] Found link with query: categoryIndex=0&subcategoryId=0 Maybe a vuln XSS point
[06:13:39] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<script>alert(6000/3000)</script>
[06:13:39] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<X3CscriptX3EalertX286000X2F3000X293X2FscriptX3EsubcategoryId=X3CscriptX3EalertX286000X2F3000X293X2FscriptX3E
[06:13:46] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[06:13:44] [INFO] Checking connection to: https://indrive.com/pt/safety
[06:13:44] [INFO] Connection established 200
[06:13:46] [WARNING] Found link with query: categoryIndex=0&subcategoryId=0 Maybe a vuln XSS point
[06:13:46] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<script>alert(6000/3000)</script>
[06:13:46] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<X3CscriptX3EalertX286000X2F3000X293X2FscriptX3EsubcategoryId=X3CscriptX3EalertX286000X2F3000X293X2FscriptX3E
[06:13:51] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[06:13:54] [INFO] Checking connection to: https://indrive.com/pt/safety/indrive
[06:13:55] [INFO] Connection established 200
[06:13:57] [WARNING] Found link with query: categoryIndex=0&subcategoryId=0 Maybe a vuln XSS point
[06:13:57] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<script>alert(6000/3000)</script>
[06:13:57] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<X3CscriptX3EalertX286000X2F3000X293X2FscriptX3EsubcategoryId=X3CscriptX3EalertX286000X2F3000X293X2FscriptX3E
[06:14:03] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[06:14:03] [INFO] Checking connection to: https://indrive.com/vi/safety
[06:14:05] [INFO] Connection established 200
[06:14:05] [WARNING] Found link with query: categoryIndex=0&subcategoryId=0 Maybe a vuln XSS point
[06:14:05] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<script>alert(6000/3000)</script>
[06:14:05] [INFO] Query (GET): https://indrive.com/en/legal/?categoryIndex=<X3CscriptX3EalertX286000X2F3000X293X2FscriptX3EsubcategoryId=X3CscriptX3EalertX286000X2F3000X293X2FscriptX3E
[06:14:12] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****

```

- **SQLmap**

An open-source penetration testing tool called SQL Map automatically locates and takes advantage of SQL injection vulnerabilities to take over databases.

In an attempt to locate any web application injection points, I experimented with various payloads and parameters. I tested this application and discovered that it is not injectable.

```
tharusha@kali:~$ sqlmap -u 'https://services.indrive.com/auth/'
[!] 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.
sponsible for any misuse or damage caused by this program

[*] starting @ 06:32:01 /2024-05-09/

[06:32:01] [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
[06:32:05] [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=2149644285034642'). Do you want to use those [Y/n] y
[06:33:00] [WARNING] reflective value(s) found and filtering out
[06:33:00] [INFO] testing if the target URL content is stable
[06:33:02] [WARNING] URI parameter '#1*' does not appear to be dynamic
[06:33:04] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[06:33:05] [INFO] testing for SQL injection on URI parameter '#1*'
[06:33:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:33:18] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[06:33:20] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[06:33:25] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[06:33:30] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[06:33:35] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[06:33:40] [INFO] testing 'Generic inline queries'
[06:33:41] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[06:33:45] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[06:33:49] [INFO] testing 'Oracle stacked queries (ODMS_PIPE.RECEIVE_MESSAGE - comment)'
[06:33:53] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[06:33:59] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[06:34:04] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[06:34:09] [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 found. Do you want to reduce the number of requests? [Y/n] y
[06:34:31] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[06:34:35] [WARNING] URI parameter '#1*' does not seem to be injectable
[06:34:35] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there
(e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 06:34:35 /2024-05-09/
```

## Vulnerabilities detect when Scanning

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

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

### 1. Vulnerability Title

Absence of Anti-CSRF Tokens

▼

URL:

https://indrive.com/en/driver/

Risk:

Medium

▼

Confidence:

Low

▼

Parameter:

▼

Attack:

Evidence:

<form class="f1rgtnau">

CWE ID:

352

◇

WASC ID:

9

◇

## Vulnerability Description

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

- \* The victim has an active session on the target site.
- \* The victim is authenticated via HTTP auth on the target site.
- \* The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

## How to mitigate

Phase: Architecture and Design

- Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.  
For example, use anti-CSRF packages such as the OWASP CSRFGuard.
- Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS.
- Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS.

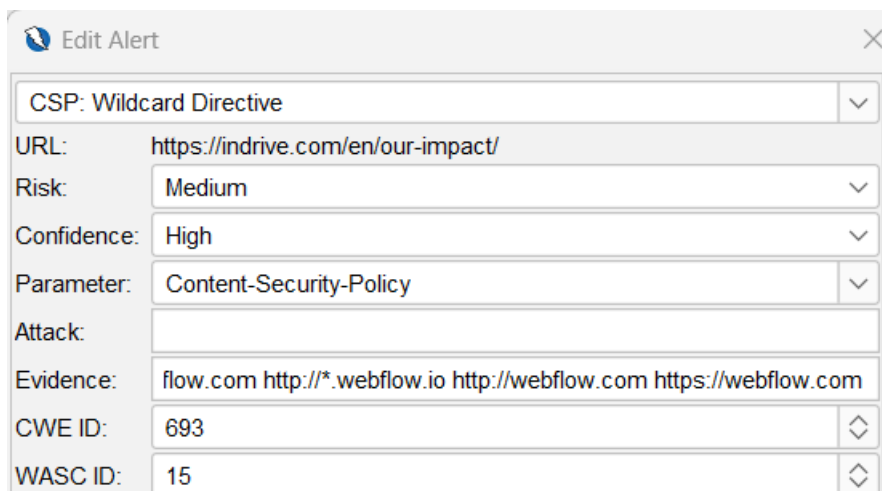


- Use the ESAPI Session Management control. This control includes a component for CSRF.
- Do not use the GET method for any request that triggers a state change.

#### Phase: Implementation

- Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
- Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

## 2. Vulnerability Title



CSP: Wildcard Directive	
URL:	https://indrive.com/en/our-impact/
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	flow.com http://*.webflow.io http://webflow.com https://webflow.com
CWE ID:	693
WASC ID:	15

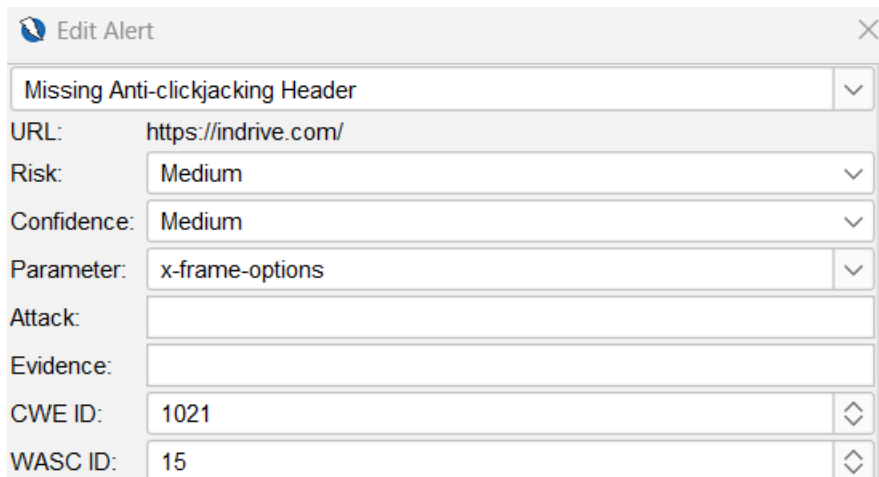
### Vulnerability Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

### How to mitigate

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

### 3. Vulnerability title



The screenshot shows a web application interface for editing a security alert. The title is 'Missing Anti-clickjacking Header'. The URL is 'https://indrive.com/'. The risk is 'Medium', confidence is 'Medium', and the parameter is 'x-frame-options'. The attack, evidence, CWE ID (1021), and WASC ID (15) fields are also visible.

Edit Alert	
Missing Anti-clickjacking Header	
URL:	https://indrive.com/
Risk:	Medium
Confidence:	Medium
Parameter:	x-frame-options
Attack:	
Evidence:	
CWE ID:	1021
WASC ID:	15

#### Vulnerability Description

The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

#### How to Mitigate

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.