

FootPrinting & Scanning

Bug Bounty

Úvod

Táto dokumentácia popisuje postup, výsledky a zistenia z vykonanej fázy Footprintingu a Scanningu v rámci testovania bezpečnosti domény truck-api.eu-east-1.indriverapp.com (Bug Bounty - HackerOne).

Cieľom bolo zhromaždiť verejne dostupné informácie o cieľovej doméne a identifikovať otvorené porty, služby a potenciálne prístupné endpointy, ktoré by mohli byť využité v ďalších fázach penetračného testovania.

Testovanie prebehlo podľa pravidiel (Program Guidelines) portálu HackerOne pričom sa rešpektoval rozsah a zakázané aktivity definované zadávateľom. Doména patrí do kategórie "**In Scope**" a je označená ako "**Critical**", čo umožňuje jej podrobnú bezpečnostnú analýzu v rozsahu povolenom pravidlami.

Použité nástroje:

1. **Burp Suite** (od HackerOne v rámci Bug Bounty, ktorý upozorní ak náhodou prekročím hranicu tolerancie)
2. **FootPrinting: Pasívny & Aktívny** (**WHOIS**, **DIG**, **NSLOOKUP**, **HOST**, **theHarvester**, **WHATWEB**, **WAFW00F**)
3. **Scanningu** (**Nmap**, **Curl**, **FFUF**)

Cieľ → truck-api.eu-east-1.indriverapp.com:

volans.tech	Domain	In scope	Critical	Eligible	Sep 26, 2023	7
truck-api.eu-east-1.indriverapp.com	Domain	In scope	Critical	Eligible	Apr 4, 2023	2
Go IBM Cloud MySQL Nginx						
terra-*.indriverapp.com	Wildcard	In scope	Critical	Eligible	May 15, 2023	4 (2
IBM Cloud MySQL Nginx PHP						
super-services.indriverapp.com	Domain	In scope	Critical	Eligible	Apr 4, 2023	3
Go Kubernetes MySQL Nginx						

Cieľom útoku je doména truck-api.eu-east-1.indriverapp.com, ktorá je typu „In Scope“, čo znamená, že mám povolenie ju testovať v rámci Bug Bounty programu, „Critical“ vraví, že prijímajú reporty aj o najzávažnejších „dierach“.

Pravidlá testovania (útoku), ktoré ako pentester musím striktne dodržiavať:

▼ Security page

Program guidelines

Scope

Hacktivity

Thanks

Updates

Collaborators

We will not pay a reward (and we will be really upset) if we detect:

- Social engineering directed at the company's employees
- Attempt to access arbitrary user's account or data or another vulnerability post- exploitation not required to demonstrate the bug presence
- Distributed network/request flooding and other resource exhaustion attacks. Automated scanning tools must be limited to 5 request per second (300 requests per minute) to one target host summing up all tools and threads running in parallel and must not exceed 5 parallel requests at the same time (5 threads).

Please use your own accounts, phone numbers, etc to conduct your research. Do not try to gain access to others' accounts or any confidential information. When testing the feedback functionality, sending a message to technical support, etc., be sure to specify the subject `Test` and use [hacker email alias](#)

We do not initiate security investigations regarding:

- Messages from security scanners and other automated systems without clear PoC and impact;
- Vulnerability reports based on software/protocol versions not indicating the actual usage/exploitation;
- Reports about the absence of a protection mechanism or non-compliance with recommendations (for example, the absence of a CSRF token) without indicating real negative consequences;
- Self-XSS;
- Framing;
- Social engineering;
- Clickjacking;
- SPF/DKIM/DMARC issues;
- Man-in-the-Middle attacks
- Vulnerabilities in partner services and products that do not directly affect the security of the company's services.
- Infrastructure vulnerabilities, including:
 - Server configuration issues (e.g. open ports, TLS versions, etc.)
 - Issues related to SSL certificates

We do not initiate security investigations regarding:

- Messages from security scanners and other automated systems without clear PoC and impact;
- Vulnerability reports based on software/protocol versions not indicating the actual usage/exploitation;
- Reports about the absence of a protection mechanism or non-compliance with recommendations (for example, the absence of a CSRF token) without indicating real negative consequences;
- Self-XSS;
- Framing;
- Social engineering;
- Clickjacking;
- SPF/DKIM/DMARC issues;
- Man-in-the-Middle attacks
- Vulnerabilities in partner services and products that do not directly affect the security of the company's services.
- Infrastructure vulnerabilities, including:
 - Server configuration issues (e.g. open ports, TLS versions, etc.)
 - Issues related to SSL certificates
 - DNS configuration issues
- Google API key(for google maps)

Strictly prohibited actions:

- DoS / DDoS attacks;
- Threats/harm to company employees.

Ako vidíme, pravidlá jasne hovoria, že nesmiem vykonávať: **Sociálne inžinierstvo; prístupy k cudzím účtom či dátam; DoS & DDoS útoky; automatizovaný Brute-Scanning (viac ako 300 requestov/min); Exploitovanie portov; Shell prístup či Telnet (hoci vedia, že niektoré porty sú otvorené).**

Pasívny FootPrinting

WHOIS dotaz na doménu indriverapp.com:

```
File Actions Edit View Help
(root@kali)-[~]
# whois indriverapp.com
Domain Name: INDRIVERAPP.COM
Registry Domain ID: 2001082186_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2025-02-04T06:22:20Z
Creation Date: 2016-02-08T03:06:32Z
Registry Expiry Date: 2026-02-08T03:06:32Z
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-CLOUD-A1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-A4.GOOGLEDOMAINS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-05-26T21:41:43Z <<<

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

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

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

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

Domain Name: indriverapp.com
Registry Domain ID: 2001082186_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2025-02-04T01:22:20Z
Creation Date: 2016-02-07T22:06:32Z
Registrar Registration Expiration Date: 2026-02-08T03:06:32Z
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
```

Domain Name: indriverapp.com
Registry Domain ID: 2001082186_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2025-02-04T01:22:20Z
Creation Date: 2016-02-07T22:06:32Z
Registrar Registration Expiration Date: 2026-02-08T03:06:32Z
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
Registrant Phone: +357.22667730
Registrant Phone Ext:
Registrant Fax: +357.22667740
Registrant Fax Ext:
Registrant Email: domainmaster@indriver.com
Registry Admin ID:
Admin Name: Domain Manager
Admin Organization: SUOL INNOVATIONS LTD
Admin Street: 41 Themistokli Dervi, Hawaii Tower, 1ST Floor, Office 106
Admin City: Nicosia
Admin State/Province: Nicosia
Admin Postal Code: 1066
Admin Country: CY
Admin Phone: +357.22667730
Admin Phone Ext:
Admin Fax: +357.22667740
Admin Fax Ext:
Admin Email: domainmaster@indriver.com
Registry Tech ID:
Tech Name: Domain Manager
Tech Organization: SUOL INNOVATIONS LTD
Tech Street: 41 Themistokli Dervi, Hawaii Tower, 1ST Floor, Office 106
Tech City: Nicosia
Tech State/Province: Nicosia
Tech Postal Code: 1066
Tech Country: CY
Tech Phone: +357.22667730
Tech Phone Ext:
Tech Fax: +357.22667740
Tech Fax Ext:
Tech Email: domainmaster@indriver.com
Name Server: ns-cloud-a3.googledomains.com
Name Server: ns-cloud-a4.googledomains.com
Name Server: ns-cloud-a1.googledomains.com
Name Server: ns-cloud-a2.googledomains.com
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>
>>> Last update of WHOIS database: 2025-02-04T01:22:20Z <<<

WHOIS výsledky:

Príkaz: **whois** indriverapp.com

Základné informácie:

Doména (Domain Name): INDRIVERAPP.COM

Registrar: CSC CORPORATE DOMAINS, INC.

Založenie od (Creation Date): 8.2.2016

Platnosť do (Registry Expiry Date): 8.2.2026

Posledná aktualizácia (Updated Date): 4.2.2025

Tieto základné informácie hovoria o tom, či je doména stabilná & dôveryhodná, a či je pravidelne udržiavaná alebo sa blíži k expirácii.

Registrátor a WHOIS Server:

Registrar WHOIS Server: whois.corporatedomains.com

Registrar URL: <http://cscdbs.com>

Registrar IANA ID: 299

Registrar Abuse Contact Email: domainabuse@cscglobal.com

Tieto informácie slúžia pre prípad, ak by som našiel kritickú zraniteľnosť, a potreboval ich o tom informovať

Majiteľ a organizácia:

Názov spoločností (Registrant Corporation): SUOL INNOVATIONS LTD

Kontaktná osoba (Registrant Name): Domain Manager

Adresa (Registrant Street): 41 Themistokli Dervii, Hawaii Tower, 1st Floor, Office 106

Mesto (Registrant City): Nicosia,

Krajina (Registrant Country): CY (Cyprus)

Poštové smerovacie číslo (Registrant Postal Code): 1066

Kontaktný email (Registrant Email): domaimaster@indriver.com

Telefón (Phone): +357 226 677 30

Toto sú geografické údaje organizácie, čo sa obvykle zíše pre mapovanie cieľa alebo OSINT techniky

DNS Servery:

Name Server (DNS): NS-CLOUD-A1.GOOGLEDOMAINS.COM

NS-CLOUD-A2.GOOGLEDOMAINS.COM

NS-CLOUD-A3.GOOGLEDOMAINS.COM

NS-CLOUD-A4.GOOGLEDOMAINS.COM

Využívajú Google DNS, čo naznačuje, že využívajú pravdepodobne Google Cloud infraštruktúru.

Súhrn informácií:

1. Doménu vlastní a spravuje InDriver
2. InDriver pochádza z Cyprusu
3. Využíva Google ako infraštruktúru na DNS úrovni
4. Doménu bola zaregistrovaná 8.2.2016 a končí 8.2.2026 pričom naposledy bola updatovaná 4.2.2025, čo znamená, že je udržiavaná, dôveryhodná a stabilná

Zneužitie pre útočníka:

Informácie o registrátorovi, geografickej polohe a kontaktoch umožňujú lepšie cielené OSINT techniky, alebo sociálne inžinierstvo (napr. phishing emaily, falošné ponuky)

DNS & OSINT analýza

DIG → DNS dotaz typu ANY:

Príkaz: **dig** truck-api.eu-east-1.indriverapp.com ANY

```
(root@kali)-[~]
# dig truck-api.eu-east-1.indriverapp.com ANY

; <<>> DiG 9.20.0-Debian <<>> truck-api.eu-east-1.indriverapp.com ANY
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 38212
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;truck-api.eu-east-1.indriverapp.com. IN      ANY

;; ANSWER SECTION:
truck-api.eu-east-1.indriverapp.com. 287 IN CNAME d2dyammkel2gvr.cloudfront.net.

;; Query time: 8 msec
;; SERVER: 192.168.217.2#53(192.168.217.2) (TCP)
;; WHEN: Mon May 26 17:51:41 EDT 2025
;; MSG SIZE rcvd: 96
```

Odpoveď: **287** IN **CNAME** **d2dyammkel2gvr**.cloudfront.net.

Význam odpovede:

- a.) **CNAME** je alias subdomény pre CloudFront (Amazon CDN → AWS)
- b.) **D2dyammkel2gvr** → náhodné distribučné ID typické pre CloudFront
- c.) **287** → TTL (287 sekúnd), to znamená, že odpoveď sa bude 287 sekúnd cacheovať. Po uplynutí TTL sa vykoná DNS dotaz, aby sa zistili, či sa niečo nezmenilo (napr. IP adresa)

Vo všeobecnosti tento výsledok hovorí, že server je za CDN, čo môže sťažiť priamy sken v Scanning fáze

CNAME (zneužitie): Skutočný backend je ukrytý za CDN. Ak útočník objaví pôvodnú IP (napr. cez leaks), môže CDN obísť a útočiť priamo (napr. pomocou Brute-Force techník)

NSLOOKUP → Reverzný DNS dotaz:

Príkaz: **nslookup** truck-api.eu-east-1.indriverapp.com

```
(root@kali)-[~]
# nslookup truck-api.eu-east-1.indriverapp.com
Server:      192.168.217.2
Address:     192.168.217.2#53

Non-authoritative answer:
truck-api.eu-east-1.indriverapp.com    canonical name = d2dyammkel2gvr.cloudfront.net.
Name:   d2dyammkel2gvr.cloudfront.net
Address: 18.66.27.51
Name:   d2dyammkel2gvr.cloudfront.net
Address: 18.66.27.108
Name:   d2dyammkel2gvr.cloudfront.net
Address: 18.66.27.94
Name:   d2dyammkel2gvr.cloudfront.net
Address: 18.66.27.128
```

Výsledky:

1. Server vracia **d2dyammkel2gvr.cloudfront.net**.
2. DNS vrátilo IP adresy: **18.66.27.51**
18.66.27.108
18.66.27.94
18.66.27.128

HOST → DNS lookup:

Príkaz: **host** truck-api.eu-east-1.indriverapp.com

```
(root@kali)-[~]
# host truck-api.eu-east-1.indriverapp.com
truck-api.eu-east-1.indriverapp.com is an alias for d2dyammkel2gvr.cloudfront.net.
d2dyammkel2gvr.cloudfront.net has address 18.66.27.51
d2dyammkel2gvr.cloudfront.net has address 18.66.27.108
d2dyammkel2gvr.cloudfront.net has address 18.66.27.128
d2dyammkel2gvr.cloudfront.net has address 18.66.27.94
```

Výsledky:

1. HOST potvrdzuje, že doména, **truck-api.eu-east-1.indriverapp.com**, je alias pre **d2dyammkel2gvr.cloudfront.net**
2. **HOST** vrátil **tie isté IP adresy** čo **NSLOOKUP**

HOST potvrdzuje, že subdoména je obsluhovaná Amazon CloudFrontom (CDN)

THE HARVESTER → OSINT zo služby crt.sh (SSL certifikáty)

Príkaz: theHarvester -d truck-api.eu-east-1.indriverapp.com -b crtsh

```
(root@kali)-[~]
# theHarvester -d truck-api.eu-east-1.indriverapp.com -b crtsh
Read proxies.yaml from /root/.theHarvester/proxies.yaml
*****
*
* [TheHarvester]
*
* theHarvester 4.6.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: truck-api.eu-east-1.indriverapp.com

[*] Searching CRTsh.

[*] No IPs found.

[*] No emails found.
```

Cieľom Harvesteru je nájsť **SSL certifikáty**, a ďalšie **subdomény**, **emaily** alebo **IP adresy**

Výsledok:

1. No IPs found
2. No emails found
3. No hosts found

Nenašiel ani žiadne ďalšie záznamy o subdoménach v CRT.SH (Certificate Transparency Log Database)

TheHarvester (zneužitie): Neúspešný Harvester poukazuje na dobré nastavenú ochranu, ale núti útočníka prejsť na aktívnejšie techniky (DNS brute force napr.)

Záver Pasívneho FootPrintingu:

1. Cieľ je chránený CDN CloudFrontom, čo znamená, že pri aktívnom skene budem narážať na ochranu Amazonu
2. Nulové výsledky záznamov v CRT.SH znamená, že endpointy sú dobré skryté
3. IP adresy patria Amazon, kde treba byť v rámci legislatívy útoku opatrný

Aktívny FootPrinting

Cieľ: truck-api.eu-east-1.indriverapp.com

PING → Overenie cieľa, či je ONLINE a DOSTUPNÝ:

Príkaz: **ping -c 4** truck-api.eu-east-1.indriverapp.com

```
(root@kali)~[~]
# ping -c 4 truck-api.eu-east-1.indriverapp.com
PING d2dyammkel2gvr.cloudfront.net (18.66.27.128) 56(84) bytes of data.
64 bytes from server-18-66-27-128.vie50.r.cloudfront.net (18.66.27.128): icmp_seq=1 ttl=128 time=13.4 ms
64 bytes from server-18-66-27-128.vie50.r.cloudfront.net (18.66.27.128): icmp_seq=2 ttl=128 time=16.8 ms
64 bytes from server-18-66-27-128.vie50.r.cloudfront.net (18.66.27.128): icmp_seq=3 ttl=128 time=16.3 ms
64 bytes from server-18-66-27-128.vie50.r.cloudfront.net (18.66.27.128): icmp_seq=4 ttl=128 time=14.3 ms

— d2dyammkel2gvr.cloudfront.net ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 13.447/15.232/16.835/1.400 ms
```

Výsledok:

1. Služba je online a dostupná → Cieľ odpovedá na ICMP požiadavky
2. Rýchlosť spojenia = 13.4 – 16.8ms, najpravdepodobnejšie EU
3. TTL = 128 (sekúnd)

WHATWEB → Identifikácia technológií webservera

Príkaz: **whatweb** <https://truck-api.eu-east-1.indriverapp.com>

```
(root@kali)~[~]
# whatweb https://truck-api.eu-east-1.indriverapp.com
https://truck-api.eu-east-1.indriverapp.com/ [410 Gone] CloudFront, Country[UNITED STATES][us],
HTTPServer[CloudFront], IP[18.66.27.128], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 f0aabb4cf746d4b45640e8d63e2aaf1c.cloudfront.net (CloudFront)]
```

Výsledok:

1. **[410 Gone]** CloudFront → Stránka bola natrvalo odstránená
2. Server beží cez CloudFront (Amazon → AWS)
3. IP adresa: 18.66.27.128 (tá istá čo pri NSLOOKUP (Amazon))
4. Country[UNITED STATES] → fyzická IP adresa Web Servera je lokalizovaná v USA

WAFW00F → DETEKCIA Web Application Firewall (WAF)

Príkaz: wafw00f <https://truck-api.eu-east-1.indriverapp.com>

```
(root@kali)-[~]
# wafw00f https://truck-api.eu-east-1.indriverapp.com

  W00f!

  404 Hack Not Found
  405 Not Allowed
  403 Forbidden
  502 Bad Gateway
  500 Internal Error

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

[*] Checking https://truck-api.eu-east-1.indriverapp.com
[+] The site https://truck-api.eu-east-1.indriverapp.com is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2

(root@kali)-[~]
#
```

Odpoved: „The site <https://truck-api.eu-east-1.indriverapp.com> is behind CloudFront (Amazon) WAF“

Táto odpoveď znamená, že server je chránený Amazon CloudFront WAF, teda firewall, ktorý:

- a.) Filtruje HTTP a HTTPS požiadavky
b.) Pravdepodobne detekuje a blokuje skenery, Brute-Force útoky či iné neštandardné požiadavky

Detekovaný WAF (zneužitie): Útočník vie, že potrebuje použiť slow-rate útoky, obfuskácie payloadov, aby sa vyhol detekcii

Záver Aktívneho FootPrintingu:

1. Cieľ je živý a odpovedá
2. Prítomnosť WAF od Amazon znamená, že je potrebné byť veľmi opatrný s brute-force metódami, agresívnymi skenmi ako masscan, wordlistami či payloadmi, ktoré pravdepodobne budú detekované alebo filtrované (alebo zablokuje IP adresu útočníka)

SCANNING

Ciel: truck-api.eu-east-1.indriverapp.com

Full TCP SYN Scan všetkých portov (65 532):

Príkaz: `nmap -sS -p- -T4 -Pn truck-api.eu-east-1.indriverapp.com -oN ports-truckapi.txt`

-sS → SYN scan (stealth TCP handshake)

-p- → všetky porty (65 532 portov)

-T4 → agresivita/rýchlosť skenu (T1 najpomalejší ale menej detekovateľný, T4 najrýchlejší ale väčšia šanca byť detekovaným)

-Pn → Nmap nebude čakať, či je port dostupný, proste ho rovno oskenuje (preskočí ICMP ping - detekciu hostu)

-oN ports-truckapi.txt → výstup do textového súboru

```
(root@kali)-[~]
└─$ nmap -sS -p- -T4 -Pn truck-api.eu-east-1.indriverapp.com -oN ports-truckapi.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 18:33 EDT
Nmap scan report for truck-api.eu-east-1.indriverapp.com (18.66.27.128)
Host is up (0.016s latency).
Other addresses for truck-api.eu-east-1.indriverapp.com (not scanned): 18.66.27.94 18.66.27.51 18.66.27.108
rDNS record for 18.66.27.128: server-18-66-27-128.vie50.r.cloudfront.net
Not shown: 65532 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 8938.74 seconds

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

Výsledok (po viac ako 2 hodinách čakania...):

1. **Porty 80 a 443 sú otvorené**
2. Zvyšné sú „**filtered**“ (pravdepodobne WAF či iného firewall-u)

80 & 443 otvorené porty (zneužitie): Táto vedomosť, že beží na CDN a žiadne iné porty sú otvorené umožňuje útočníkovi sa sústrediť len na web aplikačnú vrstvu.

Scan 1000 najbežnejších TCP portov:

Tento sken je rýchlejší, skúša iba najbežnejších 1000 portov

Príkaz: `nmap -sS --top-ports 1000 -T4 -Pn truck-api.eu-east-1.indriverapp.com`

```
(root@kali)-[~]
# nmap -sS --top-ports 1000 -T4 -Pn truck-api.eu-east-1.indriverapp.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 21:03 EDT
Nmap scan report for truck-api.eu-east-1.indriverapp.com (18.66.27.108)
Host is up.
Other addresses for truck-api.eu-east-1.indriverapp.com (not scanned): 18.66.27.128 18.66.27.94 18.66.27.51
rDNS record for 18.66.27.108: server-18-66-27-108.vie50.r.cloudfront.net
All 1000 scanned ports on truck-api.eu-east-1.indriverapp.com (18.66.27.108) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 106.38 seconds

(root@kali)-[~]
#
```

Výsledok: Ten istý čo pri **FULL TCP SYN Scan**

Nmap → Detekcia služieb a ich verzii:

Príkaz: `nmap -sV -sC -p 80, 443 truck-api.eu-east-1.indriverapp.com`

-sV → skenuje verziu služby

-sC → stealth scanning

-p 80, 443 → skenuje konkrétne otvorené porty (80, 443)

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# nmap -sV -sC -p 80,443 truck-api.eu-east-1.indriverapp.com -oN truckapi-services.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 21:10 EDT
Nmap scan report for truck-api.eu-east-1.indriverapp.com (18.66.27.108)
Host is up (0.0032s latency).
Other addresses for truck-api.eu-east-1.indriverapp.com (not scanned): 18.66.27.51 18.66.27.94 18.66.27.128
rDNS record for 18.66.27.108: server-18-66-27-108.vie50.r.cloudfront.net

PORT      STATE SERVICE VERSION
80/tcp    open  http   Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://truck-api.eu-east-1.indriverapp.com/
|_http-server-header: CloudFront
443/tcp    open  ssl/http Amazon CloudFront httpd
|_http-title: Site doesn't have a title.
|_http-server-header: CloudFront
|_ssl-cert: Subject: commonName=*.eu-east-1.indriverapp.com
| Subject Alternative Name: DNS:*.eu-east-1.indriverapp.com
| Not valid before: 2024-10-08T00:00:00
|_Not valid after: 2025-11-06T23:59:59

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.60 seconds
```

Výsledky:

PORT	STATE	SERVICE	VERSION
80/TCP	Open	HTTP	Amazon CloudFront httpd
443/TCP	Open	SSL/HTTP	Amazon CloudFront httpd

truck-api.eu-east-1.indriverapp.com má otvorené porty **80 (HTTP)** a **443 (HTTPS)**, pričom oba sú chránené Amazon CloudFront – teda ide o CDN vrstvu, ktorá zabezpečuje distribúciu obsahu a zároveň poskytuje určitú mieru ochrany

Na porte 80 server odpovedal presmerovaním na HTTPS, čo je bežné správanie pri zabezpečených webových službách.

Na porte 443 beží HTTPS služba, ale nezobrazila žiadny titulok stránky, čo znamená, že nie je verejne dostupné alebo vyžaduje špecifické požiadavky ako napríklad API token pre overenie.

SSL certifikát je platný a je vystavený pre wildcard doménu *.eu-east-1.indriverapp.com

CURL → Čítanie HTTP hlavičiek (HEAD) zo servera

Príkaz: `curl -I https://truck-api.eu-east-1.indriverapp.com`

`curl -I` → načíta hlavičky (HEAD požiadavka namiesto GET) z cieľového servera (CloudFront)

```
(root@kali)-[~]
# curl -I https://truck-api.eu-east-1.indriverapp.com
HTTP/2 410
server: CloudFront
date: Tue, 27 May 2025 01:12:33 GMT
content-length: 0
x-cache: Error from cloudfront
via: 1.1 dcbc01ed47e0218a59f0fec8e1b9aa18.cloudfront.net (CloudFront)
x-amz-cf-pop: VIE50-P1
alt-svc: h3=":443"; ma=86400
x-amz-cf-id: 2y4AFf2yt-OuvV4C4cs8VWif4uymvfbXD48QXU7RUNzle7f1skhyPA=

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

Výsledok:

1. **HTTP/2 410 (Gone)** → Server (CloudFront) odpovedal, že zdroj už natrvalo neexistuje
2. **Serverom je CloudFront**
3. **Hlavičky (headers):**
 - a.) **x-cache (error from cloudfront)** → požiadavka zablokovaná
 - b.) **alt-svc: 443** → Server podporuje HTTP3
 - c.) **x-amz-cf-id** → jedinečné ID požiadavky cez CloudFront
 - d.) **via: 1.1 dcbc.... (Cloudfront)** → požiadavka prešla cez CloudFront uzol

CURL & HTTP 410 GONE (zneužitie): „410 gone“ môže znamenať zmazané API, ktoré mohlo byť archivované alebo stále je dostupné cez iný subdoménový endpoint

FUZZ → Rýchle testovanie URL ciest, súborov a adresárov

Príkaz: **ffuf** -u <https://truck-api.eu-east-1.indriverapp.com/FUZZ> -w </usr/share/wordlists/dirb/common.txt> -t 5 -p 0.2 -o truckapi-ffuf.txt

ffuf → „Fuzz faster you fool“ (rýchly test)

-u → URL s parametrom FUZZ, ktorý ffuf nahradím každým slovom zo slovníka

-w /usr/share/wordlists/dirb/common.txt → cesta k slovníku (wordlist), ktorý predstavuje zoznam najčastejších adresárov a súborov

-t 5 → 5 paralelných vlákien (threadov) v súlade s Bug Bounty pravidlami (max 5 threadov)

-p 0.2 → oneskorenie (delay) na 0.2 sekundy medzi požiadavkami (zníženie šance na blokovanie)

-o truckapi-ffuf.txt → výstup do súboru

```
(root@kali)~# ffuf -u https://truck-api.eu-east-1.indriverapp.com/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 5 -p 0.2 -o truckapi-ffuf.txt

v2.1.0-dev

:: Method      : GET
:: URL         : https://truck-api.eu-east-1.indriverapp.com/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Output file : truckapi-ffuf.txt
:: File format : json
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 5
:: Delay      : 0.20 seconds
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500

:: Progress: [4614/4614] :: Job [1/1] :: 23 req/sec :: Duration: [0:03:23] :: Errors: 0 ::

(root@kali)~#
```

Výsledok (1.obrázok):

1. FFUF skúsil 4614 kombinácii (riadkov zo slovníka)
2. FFUF vykonal rýchly test bez chýb
3. Results[]: → Neobjavil žiadne platné endpointy

```
File Actions Edit View Help
{
  "commandline": "ffuf -u https://truck-api.eu-east-1.indriverapp.com/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 5 -p 0.2 -o truckapi-ffuf.txt",
  "time": "2025-05-26T21:19:23-04:00",
  "results": [],
  "config": {
    "autocalibration": false,
    "autocalibration_keyword": "FUZZ",
    "autocalibration_perhost": false,
    "autocalibration_strategies": [
      "basic"
    ],
    "autocalibration_strings": [],
    "colors": false,
    "cmdline": "ffuf -u https://truck-api.eu-east-1.indriverapp.com/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 5 -p 0.2 -o truckapi-ffuf.txt",
    "configfile": "",
    "postdata": "",
    "debuglog": "",
    "delay": {
      "value": "0.20-0.00"
    },
    "dirsearch_compatibility": false,
    "encoders": [],
    "extensions": [],
    "fmode": "or",
    "follow_redirects": false,
    "headers": {},
    "ignorebody": false,
    "ignore_wordlist_comments": false,
    "inputmode": "clusterbomb",
    "cmd_inputnum": 100,
    "inputproviders": [
      {
        "name": "wordlist",
        "keyword": "FUZZ",
        "value": "/usr/share/wordlists/dirb/common.txt",
        "encoders": "",
        "template": ""
      }
    ],
    "inputshell": "",
    "json": false,
    "matchers": {
      "IsCalibrated": false,
      "Mutex": {},
      "Matchers": {
        "status": {
          "value": "200-299,301,302,307,401,403,405,500"
        }
      }
    },
    "filters": {},
    "PerDomainFilters": {}
  },
  "mmode": "or",
  "maxtime": 0,
  "maxtime_job": 0,
  "method": "GET",
  "noninteractive": false,
  "outputdirectory": "",
  "outputfile": "truckapi-ffuf.txt",
  "outputformat": "json",
  "OutputSkipEmptyFile": false,
  "proxyurl": "",
  "quiet": false,
  "rate": 0,
  "raw": false,
  "recursion": false,
  "recursion_depth": 0,
  "recursion_strategy": "default",
  "replayproxyurl": "",
  "requestfile": "",
  "requestproto": "https",
  "scraperfile": ""
}
```

Výsledok (2.obrázok):

4. Výstupný súbor → obsahuje všetky použité parametre ako URL, slovník, počet threadov, matcher status codes, atď.
5. results[]: vo výstupnom súbore → Potvrdenie, že nenašiel žiadne platné endpointy

FFUF bez endpointov (zneužitie): Hoci výsledky FFUF ukázali, že žiadne end-points nie sú, útočník môže skúsiť vlastné wordlisty, rôzne obfuskácie alebo známe endpointy z verejných repozitárov (SecLists)

Záver **SCANNING-u**:

1. **2 bežne služby** → HTTP a HTTPS hostovaných cez CDN službu Amazon CloudFront, **ich porty 80 a 443 sú otvorené**
2. **CloudFront zároveň poskytuje WAF ochranu (Web Application Firewall)**
3. **FFUF** neodhalilo žiadne verejne dostupné API endpointy alebo citlivé adresáre, čo znamená, že **pokus o útok je obmedzený a pravdepodobne dobre chránený**