CYBER THREAT HUNTING & VULNERABILITY DETECTION (FULLY OPEN SOURCE)

PRESENTED BY
Farras Givari

Farras Givari

CEI, CEH, CTIA, ECIH

Professional Cybersecurity Trainer, Penetration Tester, and Security Engineer with 3 years of experience. Worked on Bug Bounty programs, Pentest/VA/SOC projects, and produced 200+ security research reports (including pentest/bug bounty) and 30+ YouTube videos about Cybersecurity Awareness and Penetration Testing for free to the Community.

Red Team Key Skills

- Penetration Testing
- Vulnerability Assesment
- WebApp Security
- API Security
- Browser Security
- Network / Infra Security
- IoT Security
- Cloud Security
- Attack & Exploit Automation/Dev

Blue Team Key Skills

- Threat Hunting
- Threat Intelligence
- Log Analysis
- SIEM
- WAF
- NGFW
- IDS / IPS
- Detection Engineering
- Server Security Automation

Bug Bounty Experience (250+ Reports)

- Hacked **Google**
- Hacked **Apple**
- Hacked **Microsoft**
- Hacked **Samsung**
- Hacked **Line**
- Hacked **Opera**
- Hacked **Brave**
- Hacked **Snapchat**
- Hacked **Reddit**
- Hacked **MetaMask**
- Hacked **Arc Browser**
- Hacked **Ubiquiti**
- Hacked **Elastic**
- Hacked **Zabbix**
- Hacked **Wazuh**
- **CVE-2024-47770**
- **CVE-2025-3074**
- **CVE-2025-26653**

Cybersecurity?

In today’s world, cyberattacks occur across various industries, often exploiting real-world scenarios like phishing, ransomware, and misconfigured systems to gain unauthorized access to critical assets and disrupt operations.

source: https://www.scworld.com/brief/rise-in-cyberattacks-seen-across-multiple-industries

Threat Hunting

Threat Hunting is the proactive process of searching through networks and systems to detect hidden threats before they cause harm. It focuses on identifying advanced attacks like APT by uncovering suspicious activities that may evade traditional security defenses.

source: https://www.ibm.com/think/topics/threat-intelligence

Tools Used (Open Source):

Subfinder (Subdomain Crawler)
https://github.com/projectdiscovery/subfinder

Dirsearch (Sensitive Information Scanning)
https://github.com/maurosoria/dirsearch

Shodan (IP / Assets Search Engine)
https://shodan.io

Nuclei (Vulnerability Scanning)
https://github.com/projectdiscovery/nuclei

Subfinder Results

```
pentest@sourcecode-host:~/ryakadev$ subfinder -d detik.com -o subdomains.txt -active

                     __    _____           __
   _____  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.7.0 (latest)
[INF] Loading provider config from /home/pentest/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for detik.com
bms.detik.com
git-jenkins.detik.com
blog.detik.com
daerah.detik.com
event.detik.com
kemiri.detik.com
smtpmailer.detik.com
indosatbackstage.detik.com
detikmakassar.lokal.detik.com
adpoint.detik.com
monitoring.detik.com
asset.detik.com
apipay.detik.com
parsley.detik.com
aci.detik.com
preview.detik.com
cmscomm.detik.com
aula.detik.com
```

```
bms.detik.com
surabaya.detik.com
ramadan.detik.com
sgblast.detik.com
ns2.detik.com
comment.detik.com
aumpaperless.detik.com
recg20.detik.com
search.detik.com
newcomment.detik.com
majalah.detik.com
suratbuncit.detik.com
imagesg.detik.com
adimages.detik.com
android.detik.com
map.detik.com
visual.detik.com
reminder.detik.com
smtpmailer.detik.com
apibanner.detik.com
aumpaperless.webs.detik.com
aggregator.detik.com
pentest@sourcecode-host:~/ryakadev$ wc -l subdomains.txt
211 subdomains.txt
```

source: https://shodan.io

Shodan Results

Facet Analysis

ssl.cert.subject.CN:"REDACTED.com" | product

// TOTAL: 88

PT BANK REDACTED	75
Amazon Data Services Jakarta	3
Amazon.com, Inc.	3
Google Asia Pacific Pte. Ltd. (GAPPL)	2
Google LLC	2
01/F, REDACTED 1 (TOWER REDACTED), JalanPr...	1
REDACTED INDONESIA PT	1
PT REDACTED Indonesia	1

Facet Analysis

ssl.cert.subject.CN:"REDACTED.com" | os

// TOTAL: 185

Ubuntu	131
Windows	41
IOS	4
Windows Server 2022 (build 10.0.20348)	6
Windows (build 10.0.17763)	2
Windows (build 10.0.14393)	1

TOTAL RESULTS

268,324

TOP PORTS

80	68,028
443	55,633
8001	8,152
8080	7,240
8443	5,242

More...

TOP ORGANIZATIONS

PT Telekomunikasi Indonesia	10,408
Google Asia Pacific Pte. Ltd. (GAPPL)	8,515
Amazon Data Services Jakarta	8,360
Alibaba Cloud (Singapore) Private Li...	7,261
PT Indonesia Comnets Plus	5,987

More...

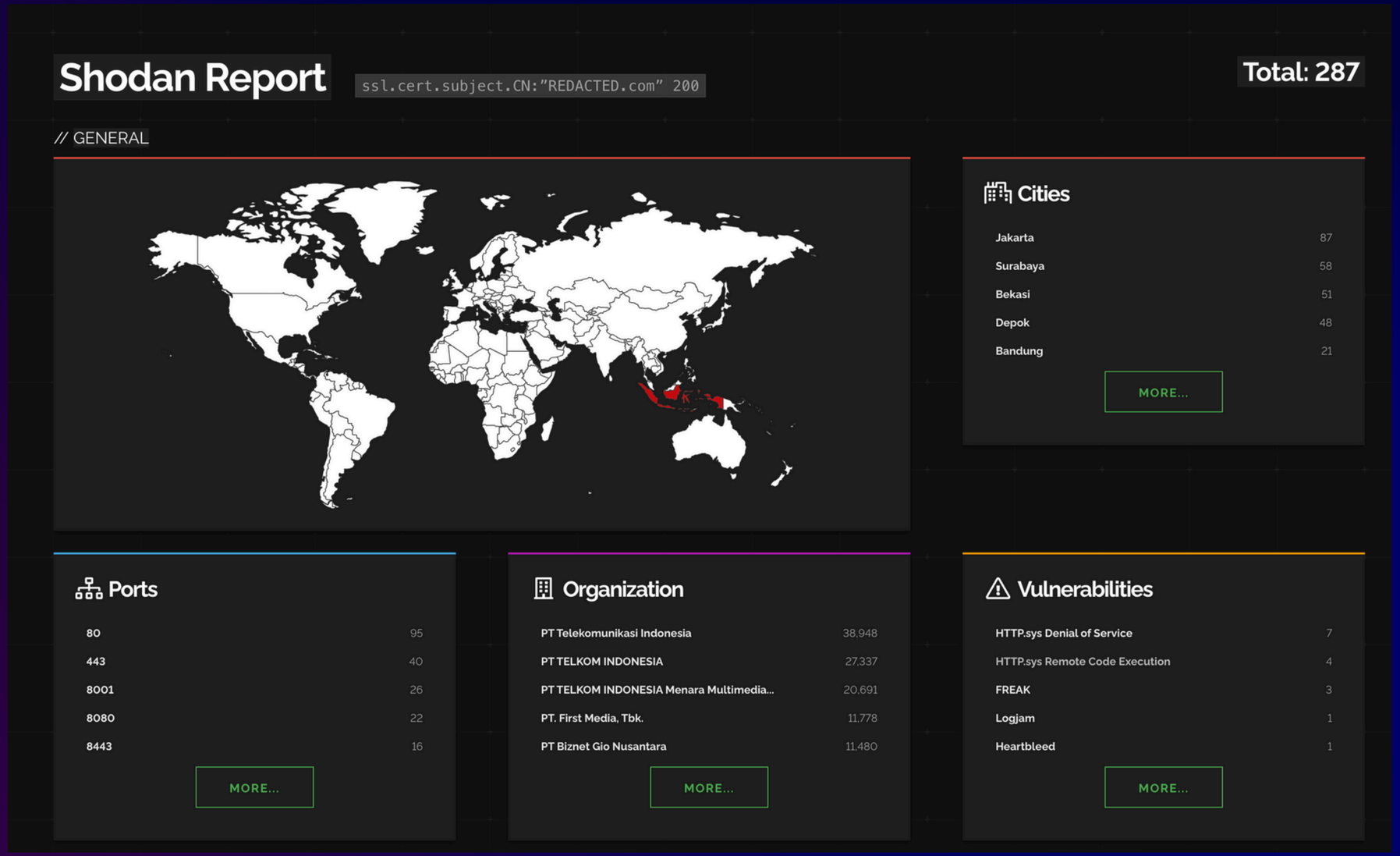
TOP PRODUCTS

nginx	55,548
Apache httpd	41,281
Microsoft IIS httpd	8,863
Hikvision IP Camera	4,237
cPanel	3,145

More...

source: https://shodan.io

Shodan Results



source: https://shodan.io

Shodan Results

SHODAN | Explore | Downloads | Pricing | ssl.cert.subject.CN:"apple.com" 200

TOTAL RESULTS

278

TOP COUNTRIES

United States	161
India	26
China	14
Singapore	11
Japan	10

More...

TOP PORTS

443	269
8443	6
4433	1
8181	1
20000	1

View Report | View on Map | Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

144.178.16.71

xvpn-ft.apple.com
ivpn.apple.com
ivpn-ssl.apple.com
ivpn-vod-ft.apple.com
ivpn-ios-ft.apple.com
Apple Inc
United States, Ashburn

SSL Certificate

Issued By:
|- Common Name:
Apple Public Server RSA CA 11 - G1
|- Organization:
Apple Inc.

Issued To:
|- Common Name:
usqas2-client-vpn.apple.com
|- Organization:
Apple Inc.

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Cache-Control: no-store
Pragma: no-cache
Connection: Keep-Alive
Date: Sat, 26 Apr 2025 08:02:07 GMT
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-...
```

144.178.19.5

xvpn.apple.com
xvpn-ac.apple.com
xvpn-ft.apple.com
ivpn.apple.com
ivpn-ssl.apple.com
Apple Inc
Australia, Sydney

SSL Certificate

Issued By:
|- Common Name:
Apple Public Server RSA CA 11 - G1
|- Organization:
Apple Inc.

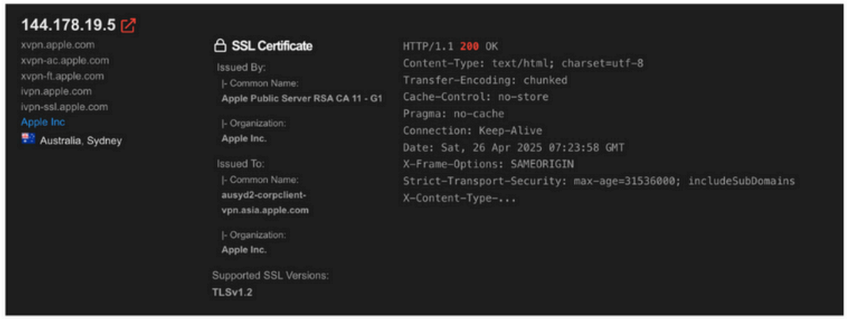
Issued To:
|- Common Name:
ausyd2-corpclient-vpn.asia.apple.com

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Cache-Control: no-store
Pragma: no-cache
Connection: Keep-Alive
Date: Sat, 26 Apr 2025 07:23:58 GMT
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-...
```

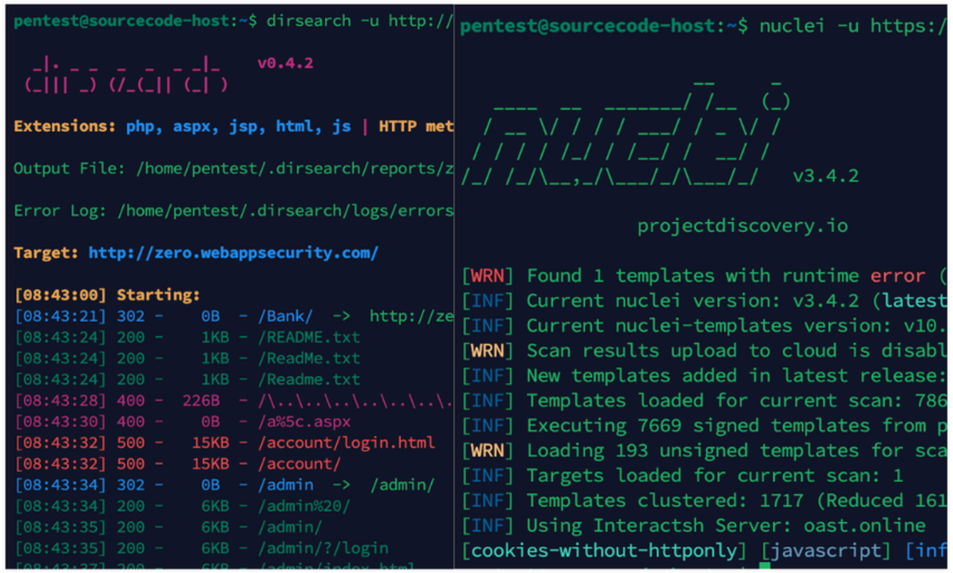
source: https://shodan.io

Threat Hunting + Vulnerability Detection

ssl.cert.subject.CN:”apple.com” 200



144.178.19.5
(target asset)



Scan if there any vulnerability on redacted IP

$ dirsearch -u https://144.178.19.5

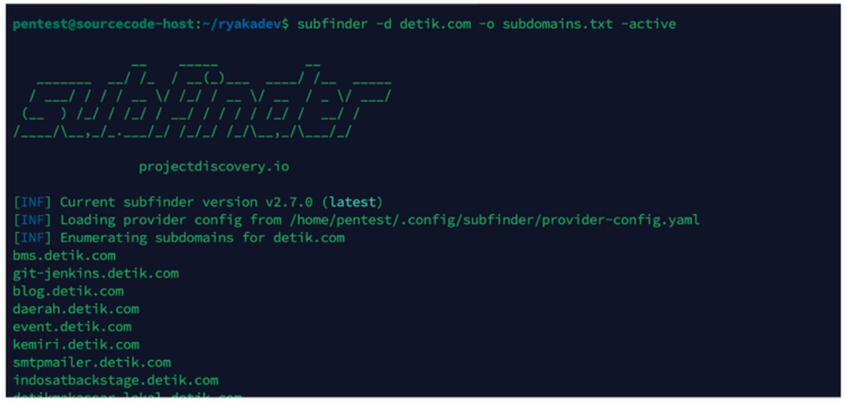
$ nuclei -u https://144.178.19.5

tips: to get an output, add -o output.txt

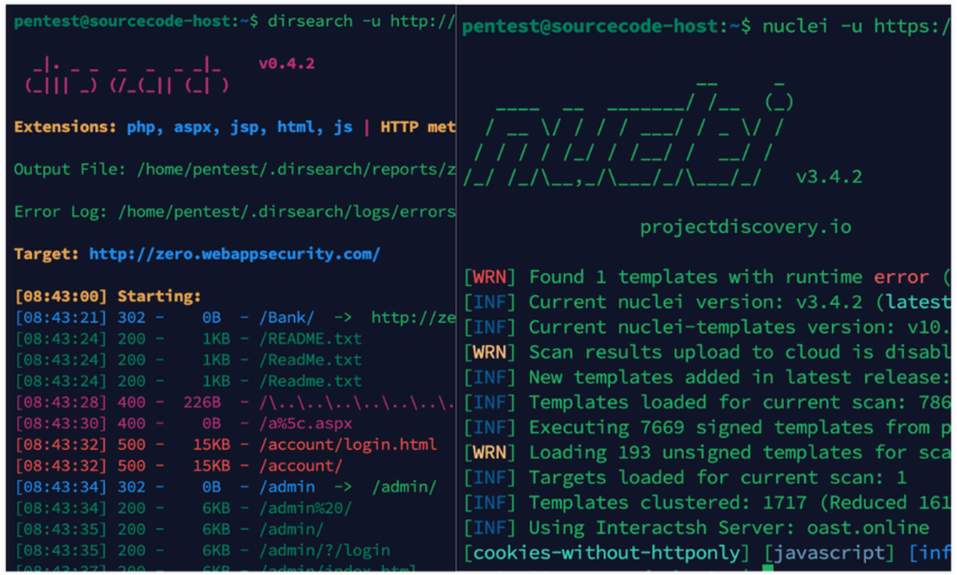
source: https://youtu.be/g0Gdr-RhOG4?si=YRNs7Bx56ZppYBYU

Threat Hunting + Vulnerability Detection

$ subfinder -d apple.com -o subdomains.txt -active



saved to subdomains.txt



Scan if there any vulnerability on redacted subdomains

$ dirsearch -l subdomains.txt

$ nuclei -l subdomains.txt

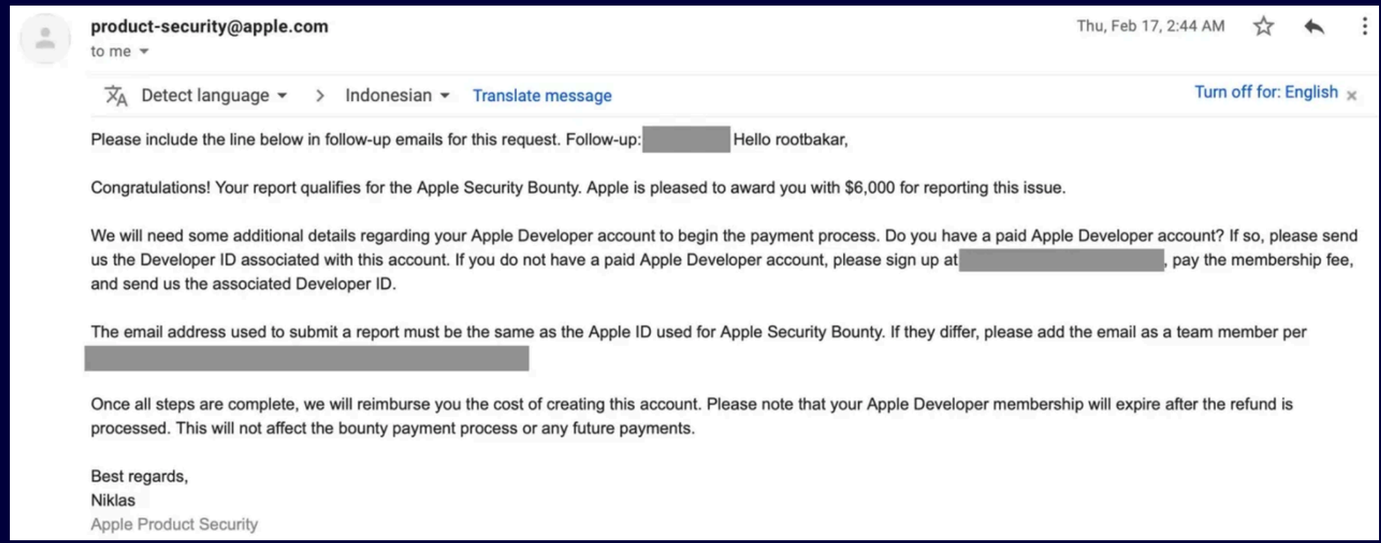
tips: to get an output, add -o output.txt

source: https://youtu.be/g0Gdr-RhOG4?si=YRNs7Bx56ZppYBYU

$6000 Bounty from Apple!

Credits: @rootbakar (https://www.instagram.com/talaohu28)

```
[23:35:39] Starting:
[23:35:44] 200 -    2KB - /.config/karma.conf.js
[23:35:46] 200 -   90KB - /.do
[23:35:58] 200 -   11KB - /.src/app.js
[23:35:58] 200 -  497B  - /.src/index.js
[23:36:01] 200 -  512B  - /.well-known/apple-app-site-association
[23:36:15] 400 -  955B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[23:36:20] 200 -   26KB - /actuator/sso
[23:36:35] 400 -  102B  - /api
[23:36:35] 400 -  102B  - /api/jsonws
[23:36:35] 400 -  102B  - /api/
[23:36:35] 400 -  102B  - /api/2/explore/
[23:36:35] 400 -  102B  - /api/error_log
[23:36:35] 400 -  102B  - /api/package_search/v4/documentation
[23:36:35] 400 -  102B  - /api/jsonws/invoke
[23:36:35] 400 -  102B  - /api/v1
[23:36:35] 400 -  102B  - /api/swagger.yml
[23:36:35] 400 -  102B  - /api/2/issue/createmeta
[23:36:35] 400 -  102B  - /api/v2
[23:36:35] 400 -  102B  - /api/v2/helpdesk/discover
[23:36:36] 400 -  102B  - /api/swagger
[23:36:36] 400 -  102B  - /api/v3
[23:36:36] 200 -   11KB - /app.js
[23:37:01] 200 -   13KB - /favicon.ico
[23:37:09] 200 -    2KB - /karma.conf.js
[23:37:16] 200 -    1KB - /manifest.json
[23:37:32] 200 -    0B  - /proc/sys/kernel/core_pattern
[23:37:34] 200 -   25B  - /public_html/robots.txt
[23:37:37] 200 -   25B  - /robots.txt
[23:37:44] 200 -   11KB - /src/app.js
[23:37:45] 200 -  497B  - /src/index.js
```



product-security@apple.com Thu, Feb 17, 2:44 AM

to me

Detect language › Indonesian Translate message Turn off for: English

Please include the line below in follow-up emails for this request. Follow-up: [redacted] Hello rootbakar,

Congratulations! Your report qualifies for the Apple Security Bounty. Apple is pleased to award you with $6,000 for reporting this issue.

We will need some additional details regarding your Apple Developer account to begin the payment process. Do you have a paid Apple Developer account? If so, please send us the Developer ID associated with this account. If you do not have a paid Apple Developer account, please sign up at [redacted], pay the membership fee, and send us the associated Developer ID.

The email address used to submit a report must be the same as the Apple ID used for Apple Security Bounty. If they differ, please add the email as a team member per [redacted]

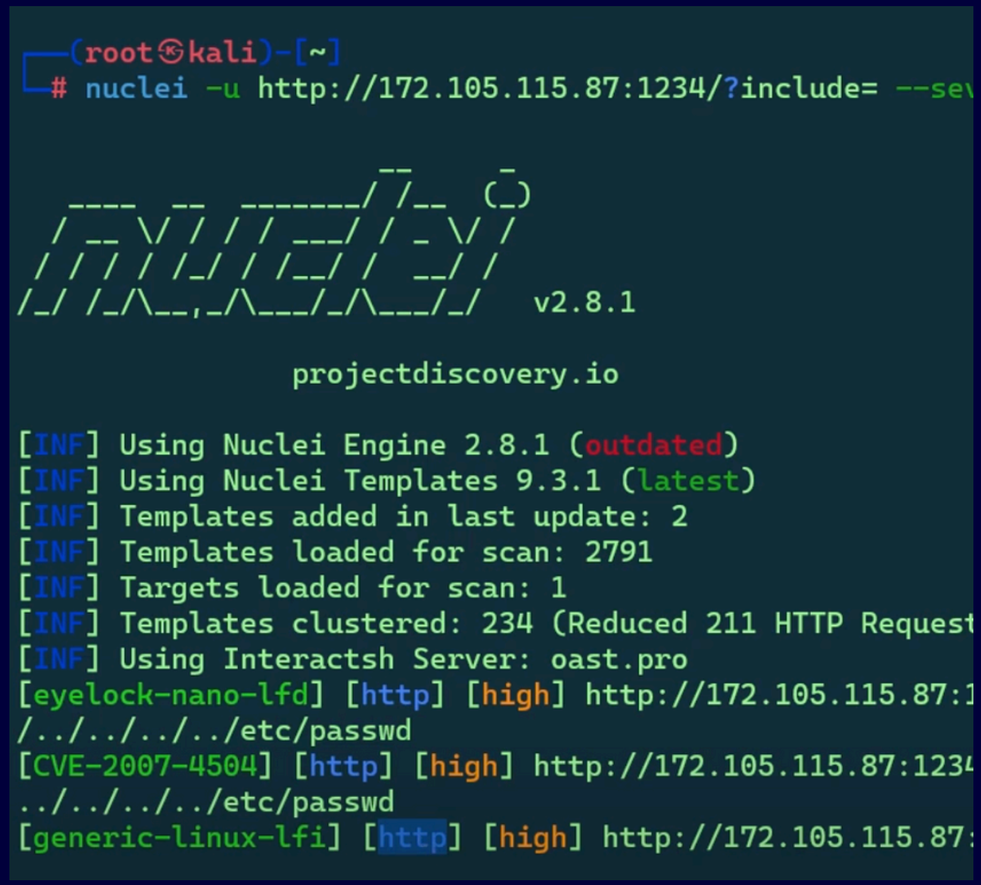
Once all steps are complete, we will reimburse you the cost of creating this account. Please note that your Apple Developer membership will expire after the refund is processed. This will not affect the bounty payment process or any future payments.

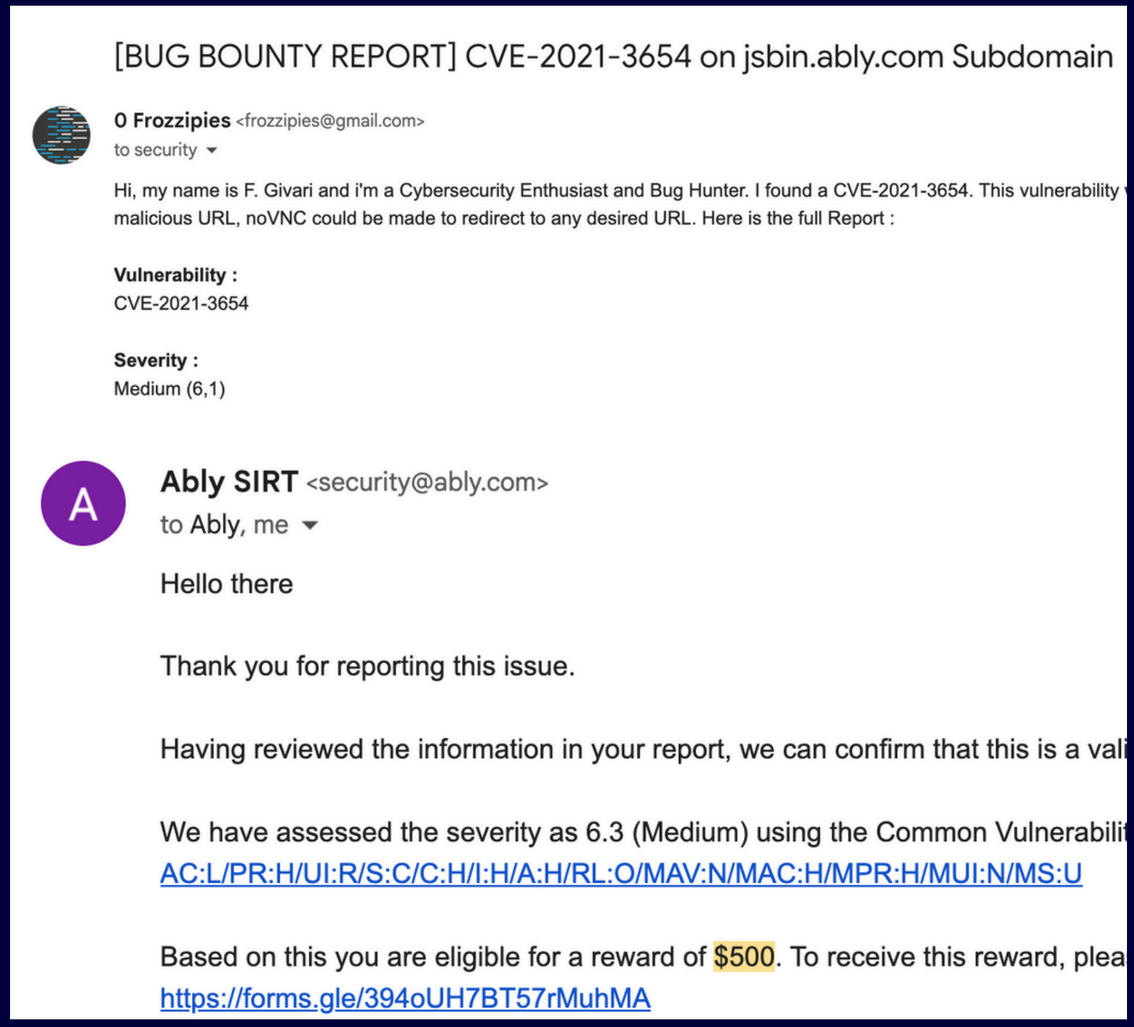
Best regards,
Niklas
Apple Product Security

source: https://milcsirt-tni.mil.id/portal/berita/21

$500 Bounty (Subfinder + Nuclei = Bounty)

Credits: @rootbakar (https://www.instagram.com/talaohu28)

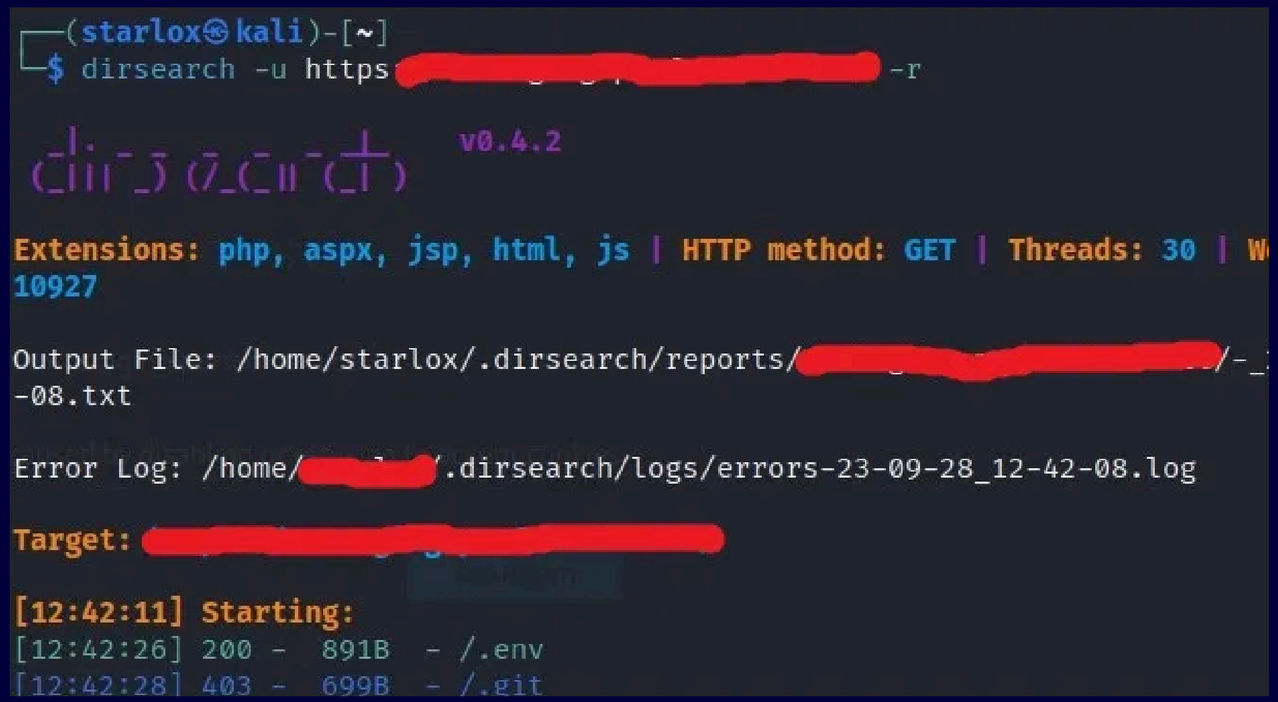


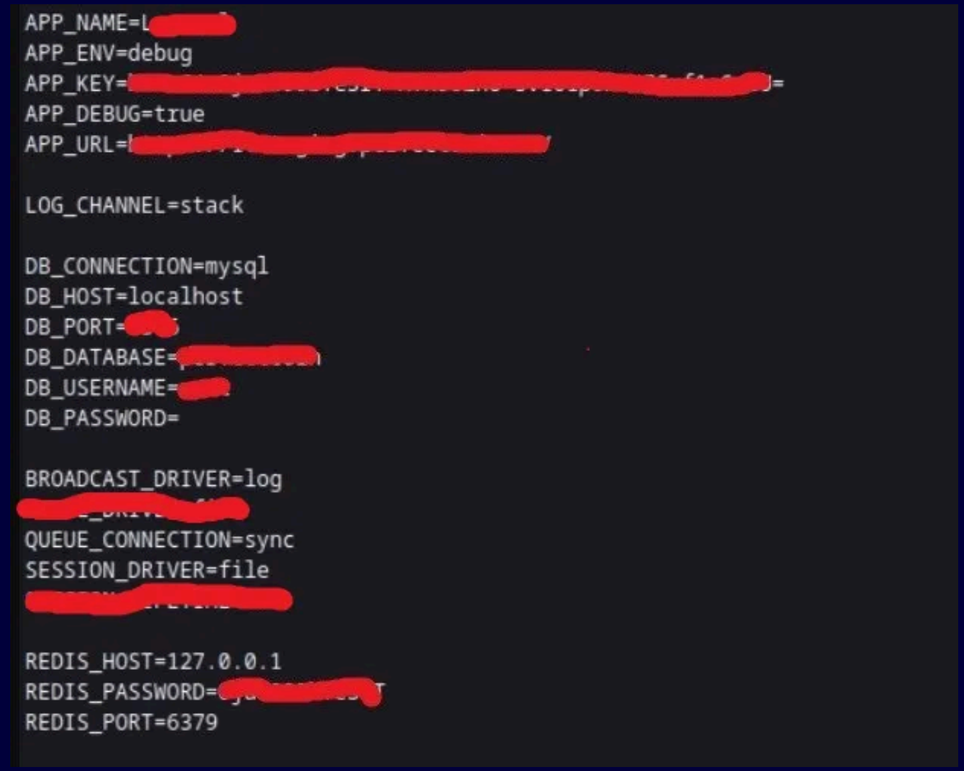


source: Private Documentation

Critical Information Disclosure

Credits: @starlox0 (https://starlox.medium.com/)





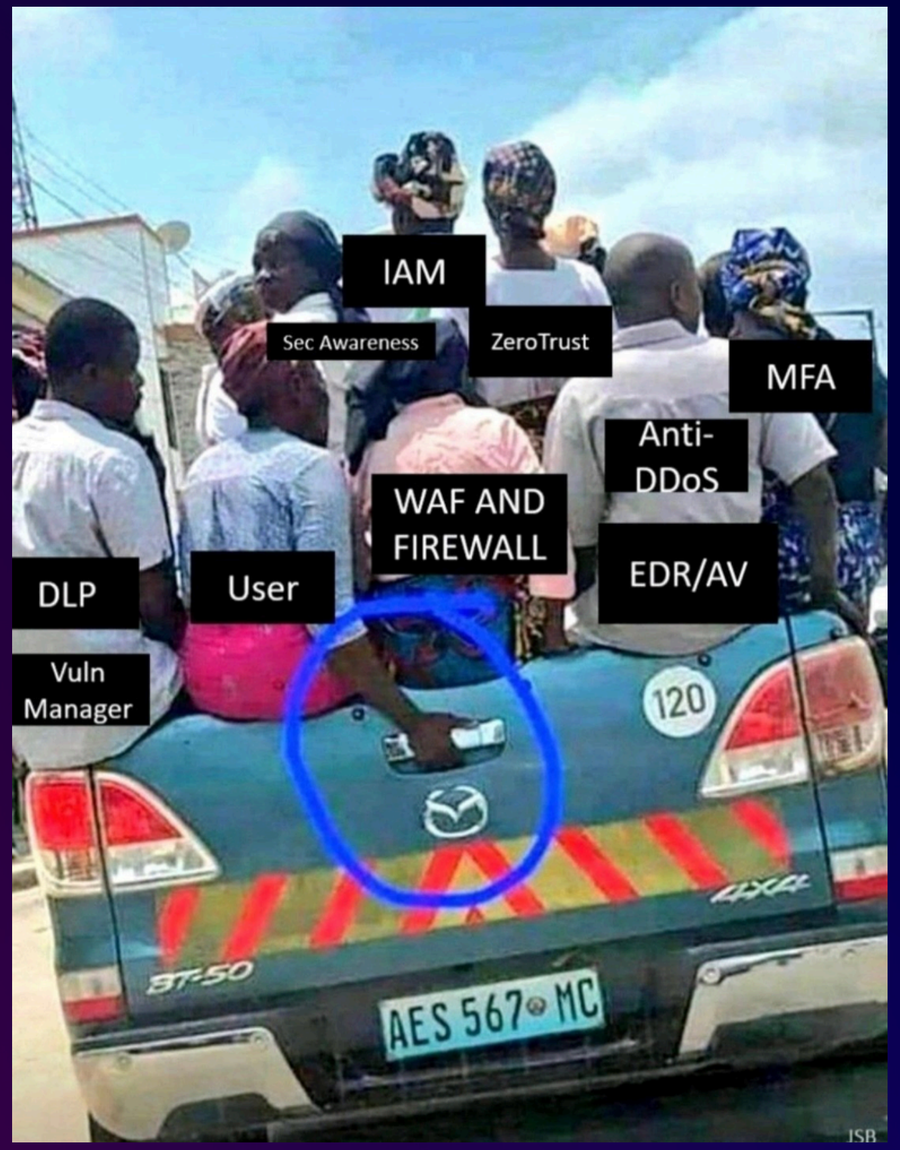
source: https://starlox.medium.com/fuzzing-made-hacking-critical-information-disclose-16701561a4f

Security Remediation & Best Practices

- Implement **SIEM** on Every Assets (Wazuh, Splunk, ELK, etc)
- Implement **enterprise WAF** to secure all your assets (If possible)
- Close **sensitive** directory & endpoint (.env , .git , info.php , etc)
- Don’t use **default credential** on any services (even it is on local)
- Monitor **0-Da**y Vulnerabilities on any third party services
- Always **harden & pentest** servers/web apps before production.
- Keep all system and application always **up-to-date**
- Always perform regular **Threat Hunting, Threat Intelligence, Vulnerability Assesment, and Penetration Testing** session

source: Google, ChatGPT, and based on my experiences :)

The Human Element



Cybersecurity Philosophy

No System is safe
Security need update

THANK YOU!