POC IRDFAS

Presented By:

Crypton Commanders

Sugeng Dwi Hermanto (SMKN 1 Cibinong)

Muhamad Agung (SMKN 1 Cibinong)

[DAFTAR ISI]

[DAFTAR ISI] **1**

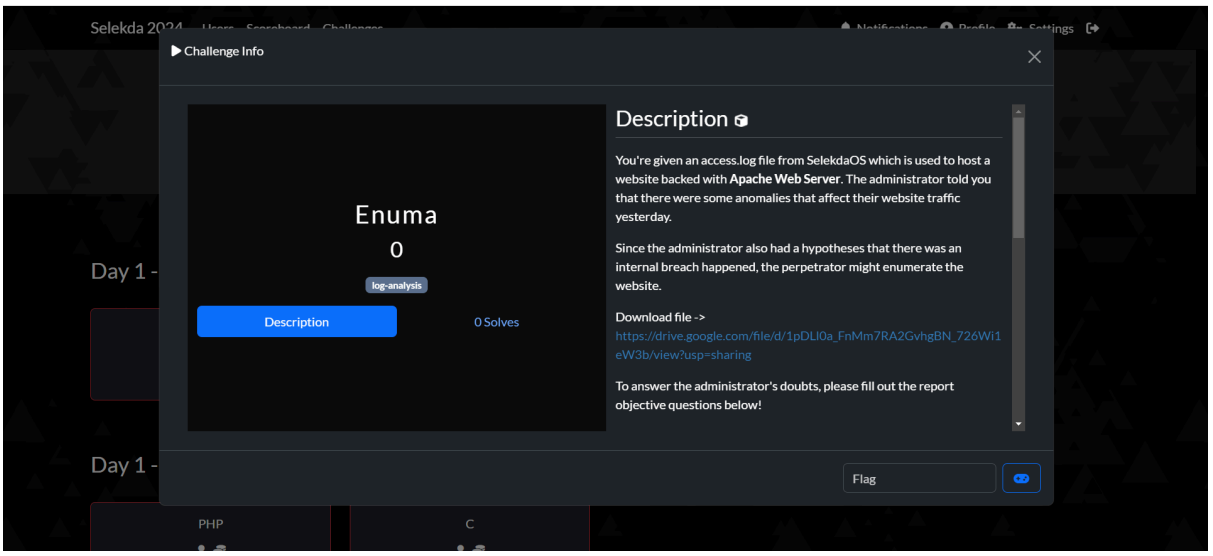
[Log Dump] **3**

- Is there any different external IP that access the website? 3
- How many IP(s) are there? 4
- Any perpetrator's offensive attempt actions involved? If yes, what are they? 4
- Were there any directory brute forcing attempt ? What tool(s) that the perpetrator used? When and HOW MANY TIME(S) did it happen ? 7
- Your IR team told you that there were 2 several specific web attacks happened in the website. One of the attack gave the perpetrator an arbitrary read internal file. When was it happened (first time the payload delivered)? 8
- Continuing from the question above, the other attack let the attacker to possibly extract or fetch some data from important database. What tool(s) that they use to perform it? When did it happen (first time & last time the payload delivered) ? 8

[Memory Dump] **9**
- Mengidentifikasi Proses Pada Sistem Yang Tidak Normal: 9
1. Is/Are there any application(s) downloaded in his device? How many times that they're/it is executed? 9
2. Is/Are there any suspicious URLs/links that Dicky opened in his browser(s)? What are they? 11
3. Is there any activity related to that from Dicky's device? Did he somehow save certain secret information? 12
- Mengumpulkan Bukti Proses Yang Tidak Normal: File Dan Objek Lainnya 12
[Network Traffic] **14**
- Mengidentifikasi & Mengalisis Pola Lalu Lintas Jaringan yang Mencurigakan: 14
1. A port scanning activity is detected in the system. Is it true or false positive? Please do screenshot any kind of proofs including all the port numbers involved and report the open ports 14
2. A PHP CVE Exploitation is detected by our SIEM. Is it true or false positive? Please do screenshot any kind of proofs 16
3. We accidentally exposed some ports due to Firewall misconfiguration. Can you tell me which port that responsible to open up a connection for file transfers? 18
4. What does the attacker download from the file transfer port related? 20
5. Any chance the attacker download an internal file which should not be public? Our developer is pretty clumsy that he puts some kind of confidential hint in the website 21
6. Please answer this question if the previous ones is true. What was the content of the protected file ONLY IF the attacker steal/download the file? Is the password pretty strong? 24
7. (BONUS FOR FUN)There's one FLAG indicating the password disclosure on one of the authenticated ports. Can you find it? 26
- Menilai Dampak Keamanan dari Aktivitas Jaringan 29
[Application Source Code] **30**
PHP: 30
- Attack Method & Proof of the Attacks 30
1. Cross-Site Scripting (XSS) 30
2. SQL Injection (Delete Function) 31
3. Brute Force Login (No Rate Limiting) 31
4. Username Enumeration (Login) 32
5. Weak Username Validation 33
- Patches Approach 34
1. File: home.php (Patched) 34
2. File: login.php (Patched) 35
3. File: register.php (Patched) 35
C: 36
- Attack Method & Proof of the Attacks 37

1. Penggunaan gets()....37
2. Kesalahan Variabel pada removeBook()....37
3. Out-of-bounds Access pada searchBook()....38
4. Potensi Integer Overflow pada book_count (Global Variabel)....39
- Patches Approach....42
1. File:
chall.c (Patched)....42

[Log Dump]



- Is there any different external IP that access the website?

- Pertama unduh terlebih dahulu file yang telah diberikan pada drive dan terdapat file access.log, yang dimana file itu adalah sebuah log dari sebuah web server. Link Download File : https://drive.google.com/file/d/1pDLl0a_FnMm7RA2GvhgBN_726Wi1eW3b/view?usp=sharing .

- Lalu setelah itu pada objective pertama diperintahkan bahwa kita harus mengidentifikasi apakah ada ip eksternal yang mengakses server tersebut. Dan Jawaban nya tidak ada hanya terdapat ip *10.0.2.15,* yang dimana ini adalah sebuah ip private dan karena sudah ada standar internet Rentang IP privat yang ditentukan oleh RFC 1918 adalah:

- **10.0.0.0 - 10.255.255.255 (Class A)**
- **172.16.0.0 - 172.31.255.255 (Class B)**

- **192.168.0.0 - 192.168.255.255 (Class C)**

```
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/indiatimes HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/inf HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/cautari HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/slmdb HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/infocenter HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/slog HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/cave HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/sloggerMDB HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/isp HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/cbb HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/slovakia HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/it_lastminute HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/cblog HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/slow HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/cbs HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/ivillage HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/ccds HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/sluzby HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/joomla15 HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/smallimages HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/ccsearch HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/smallimg HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/jw HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/smart_search HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/ccss HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/smartmoney HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/kanri HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/smarty_plugins HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/cdi HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/smf_scripturl HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/kelloggsie HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/cdr HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/smg HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/cebit HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/kelloggsuk HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/ced HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/smith HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/cell HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/keypublisher_gui HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleton/cem HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/support/sml HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-ui/ui/klmjp HTT^C
```

```
┌──(root㉿kali)-[/home/…/Downloads/worldskill-asean/IRDFAS/logdump]
└─# cat access.log | awk '{print $1}' | grep -vE "^192\.168\.|^10\.|^127\." | sort | uniq -c | sort -nr
    315 ::1
```

315 ::1. "::1" **adalah alamat loopback dari IPv6 sama seperti 127.0.0.1.**

- How many IP(s) are there?

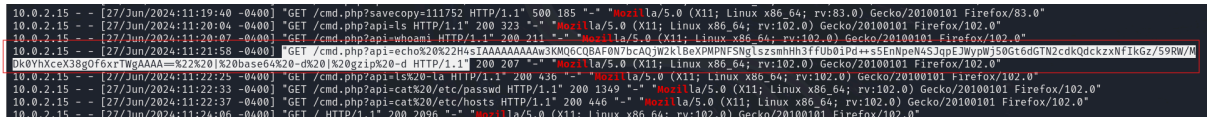
- Seperti yang saya katakan pada objective sebelumnya bahwa ip yang terdapat pada log server tersebut hanya ada satu yaitu *10.0.2.15*.

```
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleto
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/su
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/su
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleto
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/util/su
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/jquery-
10.0.2.15 - - [27/Jun/2024:11:03:29 -0400] "GET /javascript/skeleto
```

- Any perpetrator's offensive attempt actions involved? If yes, what are they?

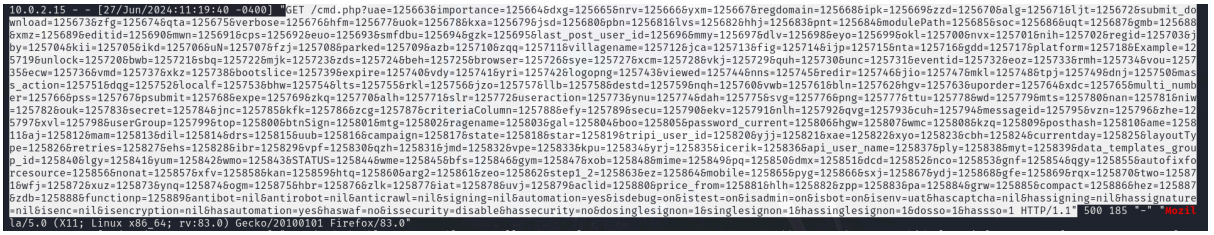
- Terdapat percobaan penyerangan :

- RCE (Remote Code Execution)



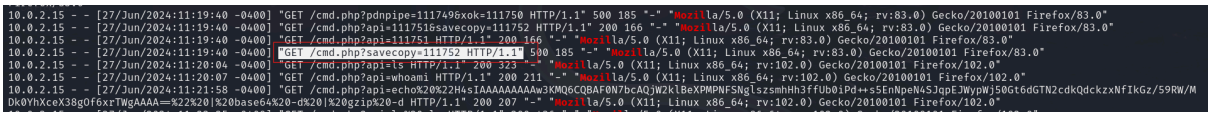
Dalam konteks ini, jika skrip PHP tidak mengelola parameter api dengan baik dan menjalankan perintah sistem menggunakan input tersebut, penyerang bisa mendapatkan informasi sensitif tentang struktur file server.

- Parameter Pollution

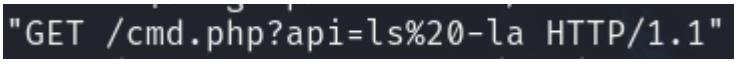


Penyerang mencoba untuk memasukkan berbagai parameter ke dalam permintaan dengan harapan bahwa aplikasi akan mengabaikan validasi input yang diperlukan atau memproses parameter dengan cara yang tidak terduga.

- Command Injection

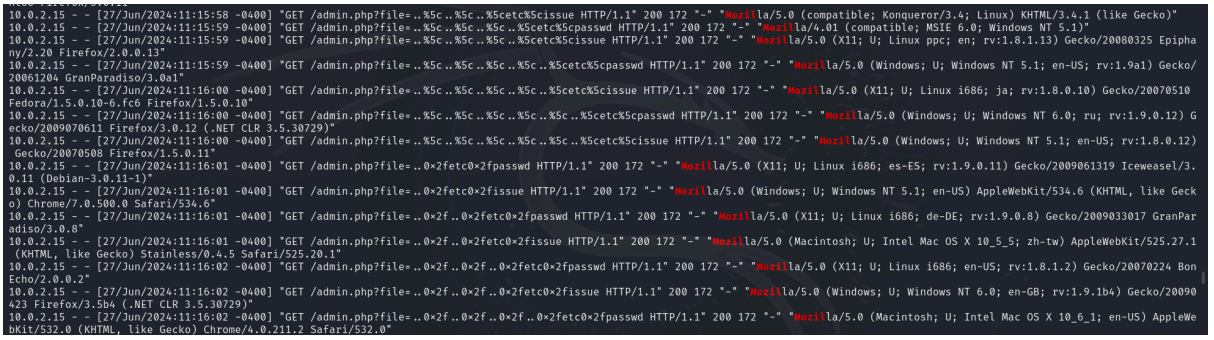


Contoh Lainnya Adalah ini *"GET /cmd.php?api=ls%20-la HTTP/1.1"*



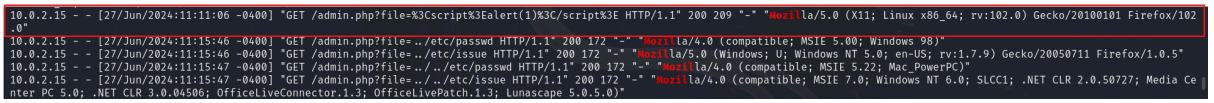
Seperti Pada parameter *"cmd.php?api=ls%20-la"* ls adalah command pada linux untuk menampilkan isi dari directory.

- LFI (Local File Inclusion) Absolute dan Relative Path



penyerangan yang berupaya memanipulasi parameter untuk berpindah directory atau file system pada server dengan command seperti pada linux.

- XSS (Cross Site Scripting)



upaya penyerangan dalam kerentanan input code javascript, seperti

yang bisa kita lihat bahwa terdapat “<script>alert(1)<script>”.

- PHP Wrappers

```
10.0.2.15 - - [27/Jun/2024:11:08:43 -0400] "GET /admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index.php HTTP/1.1" 200 2101 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [27/Jun/2024:11:08:43 -0400] "GET /src/w3.css HTTP/1.1" 200 5593 "http://10.0.2.15/admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [27/Jun/2024:11:08:43 -0400] "GET /src/css HTTP/1.1" 304 248 "http://10.0.2.15/admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [27/Jun/2024:11:08:43 -0400] "GET /src/woods.jpg HTTP/1.1" 304 249 "http://10.0.2.15/admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [27/Jun/2024:11:08:43 -0400] "GET /src/bridge.jpg HTTP/1.1" 304 249 "http://10.0.2.15/admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [27/Jun/2024:11:08:43 -0400] "GET /src/avatar_g.jpg HTTP/1.1" 304 249 "http://10.0.2.15/admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [27/Jun/2024:11:08:43 -0400] "GET /src/workshop.jpg HTTP/1.1" 304 249 "http://10.0.2.15/admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [27/Jun/2024:11:08:43 -0400] "GET /src/gondol.jpg HTTP/1.1" 304 249 "http://10.0.2.15/admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [27/Jun/2024:11:08:43 -0400] "GET /src/skies.jpg HTTP/1.1" 304 249 "http://10.0.2.15/admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [27/Jun/2024:11:08:43 -0400] "GET /src/rock.jpg HTTP/1.1" 304 249 "http://10.0.2.15/admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [27/Jun/2024:11:08:48 -0400] "GET /admin.php?file=php://filter/convert.base64-encode|convert.base64-decode/resource=index HTTP/1.1" 200 208 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
```

terdapat beberapa payload untuk RCE dan LFI menggunakan PHP Wrappers, dimana command dari linux itu dibungkus dengan code php agar tidak terdeteksi oleh server.

- Brutforce dan Ekstraksi Database (SqlMap)

```
http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20baqz HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20bTaB HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20pcez HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20UXJv HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20TeHB HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20jCpf HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20VsKb HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20Urxm HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20qEVO HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%22%29%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20zDbe HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%22%29%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20xuag HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%22%29%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20EsZR HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%22%29%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20FWyO HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%22%29%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20XDaB HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"
```

Beberapa log saat terjadi nya bruteforcing pada server dengan tools sqlmap dengan payload yang disediakan, untuk mencari sebuah credentials pada sql.

- Bruteforce (feroxbuster)

```
10.0.2.15 - - [27/Jun/2024:11:03:11 -0400] "GET /640021d7341c4cb9a225eae215d9b935 HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /category HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /blog HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /install HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /trackback HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /temp HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /logs HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /files HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /aspnet_client HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /inc HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /lib HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /data HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /comments HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /_private HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /help HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /catalog HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /page HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /editor HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /backup HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
10.0.2.15 - - [27/Jun/2024:11:03:12 -0400] "GET /news HTTP/1.1" 404 432 "-" "feroxbuster/2.10.0"
```

Beberapa upaya melakukan bruteforcing terhadap directory dan file sebuah server.

- Bruteforce (gobuster)

Sama seperti tools bruteforce sebelumnya yaitu untuk mencari directory juga file.

- Were there any directory brute forcing attempt ? What tool(s) that the perpetrator used? When and HOW MANY TIME(S) did it happen ?

- Terdapat tindakan penyerangan yang melakukan bruteforcing pada access.log tersebut yaitu menggunakan tools seperti

- **Sqlmap**
- **Feroxbuster**
- **Gobuster**

Lalu Bruteforcing yang pertama kali dilakukan adalah menggunakan feroxbuster pada tanggal *[27/Jun/2024:11:03:11 -0400] "GET / HTTP/1.1" 200 6824 "-" "feroxbuster/2.10.0".* dan untuk jumlah dari melakukan tindakan bruteforcing pada server berjumlah 1403226. Dan cara saya menghitung nya adalah dengan command *“grep -c -E "gobuster|feroxbuster|sqlmap" access.log”*

- Your IR team told you that there were 2 several specific web attacks happened in the website. One of the attack gave the perpetrator an arbitrary read internal file. When was it happened (first time the payload delivered)?

- Saya Mengidentifikasi Kapan pertama kali Jenis Serangan LFI dilakukan menggunakan *cat access.log | grep "Mozil".* dan saya menemukan bahwa pertama kali itu pada tanggal :

[27/Jun/2024:11:07:14 -0400] "GET /admin.php?file=/etc/passwd HTTP/1.1" 200 1355 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"

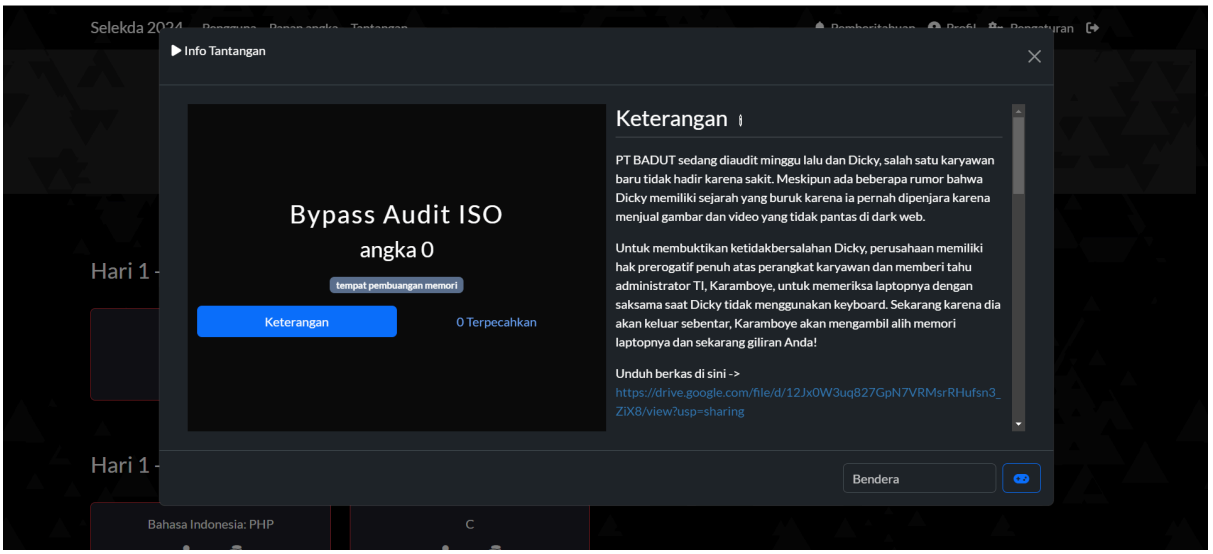
- Continuing from the question above, the other attack let the attacker to possibly extract or fetch some data from important database. What tool(s) that they use to perform it? When did it happen (first time & last time the payload delivered) ?

- Disini dikatakan bahwa saya harus mencari kapan pertama kali dan terakhir kali sebuah bruteforcing yang berupaya mengambil database (SQLMAP TOOLS).

Untuk Pertama Kali Tools Ini Dijalankan adalah :
10.0.2.15 - - [27/Jun/2024:11:06:55 -0400] "GET /?file=1 HTTP/1.1" 200 2059 "-" "sqlmap/1.8.5#stable (https://sqlmap.org)"

Dan Untuk Terakhir Kali Tools Ini Dijalankan adalah :
10.0.2.15 - - [27/Jun/2024:11:23:58 -0400] "GET /?file=1%22%29%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CN
LL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CN
LL--%20XDaB HTTP/1.1" 200 2059 "http://10.0.2.15/" "sqlmap/1.8.5#stable (https://sqlmap.org)"

[Memory Dump]

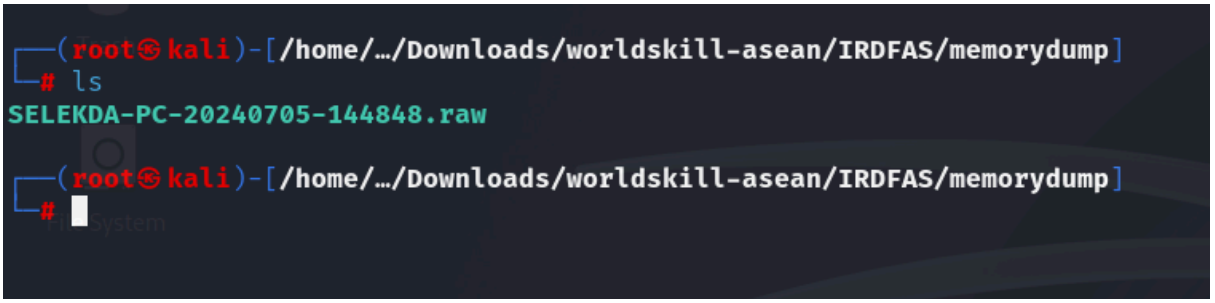


- Mengidentifikasi Proses Pada Sistem Yang Tidak Normal:

1. Is/Are there any application(s) downloaded in his device? How many times that they're/it is executed?

- Pertama-tama install dan extract file zip yang telah di sediakan, dan terdapat file raw.

Untuk Zip password = zip_password_but_not_in_rockyou_lol



- Lalu selanjutnya melakukan Identifikasi Image File (Image Info) menggunakan command “vol -f SELEKDA-PC-20240705-144848.raw imageinfo”.

Disini Saya Menggunakan Tools Volatility v2.6

```
┌──(root㉿kali)-[/home/…/Downloads/worldskill-asean/IRDFAS/memorydump]
└─# vol -f SELEKDA-PC-20240705-144848.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Downloads/worldskill-asean/IRDFAS/memorydump/SELEKDA-PC-20240705-144848.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002c080a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002c09d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2024-07-05 14:48:54 UTC+0000
     Image local date and time : 2024-07-05 14:48:54 +0000

┌──(root㉿kali)-[/home/…/Downloads/worldskill-asean/IRDFAS/memorydump]
└─#
```

- Setelah itu saya melakukan pengidentifikasian file yang sedang berjalan pada saat kejadian ini terjadi, terdapat file yang mencurigakan yaitu "*tor.exe*". Menurut saya ini terdapat hubungannya dengan masa lalu dicky pada saat di dark web.

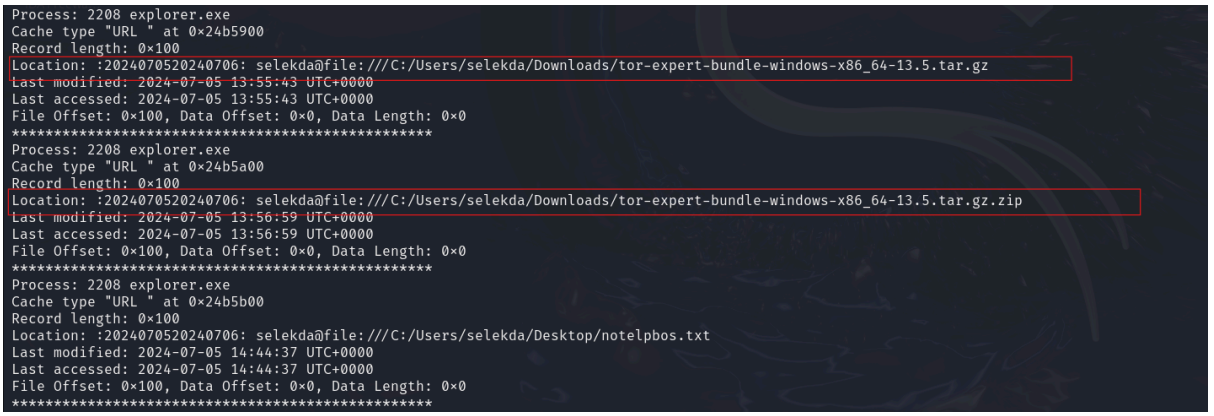
```
0xfffffa8019239210 audiodg.exe           5704    760      6      133      0      0 2024-07-05 14:35:24 UTC+0000
0xfffffa801ad25060 cmd.exe               5452   2208      1       22      1      0 2024-07-05 14:35:46 UTC+0000
0xfffffa801b9fe5b0 conhost.exe           1508    420      2       53      1      0 2024-07-05 14:35:46 UTC+0000
0xfffffa8019d27700 tor.exe               1752   5452      5      106      1      0 2024-07-05 14:36:49 UTC+0000
0xfffffa801bb47320 firefox.exe           5664   1444     48      756      1      0 2024-07-05 14:36:59 UTC+0000
0xfffffa801bf74060 firefox.exe           5808   5664     17      266      1      0 2024-07-05 14:37:01 UTC+0000
0xfffffa8019020b30 tor.exe               5364   5664      5       70      1      0 2024-07-05 14:37:01 UTC+0000
0xfffffa801a6a5b30 conhost.exe           5220    420      1       34      1      0 2024-07-05 14:37:01 UTC+0000
0xfffffa8019436600 firefox.exe           5864   5664     17      220      1      0 2024-07-05 14:37:01 UTC+0000
0xfffffa801be318c0 firefox.exe           6092   5664     17      217      1      0 2024-07-05 14:37:03 UTC+0000
0xfffffa801be1fb30 firefox.exe           4120   5664     17      220      1      0 2024-07-05 14:37:04 UTC+0000
0xfffffa801a199b30 firefox.exe           2956   5664     16      209      1      0 2024-07-05 14:37:18 UTC+0000
```

- Pada Bagian Pengidentifikasian Objective Tentang "*How many times that they're/it is executed?*" Saya menemukan Bahwa tor.exe Dijalankan Sebanyak 2 Kali Pada Saat Itu:

```
0xfffffa80193a8460 firefox.exe           4164    168     18      248      1      1 2024-07-05 13:59:24 UTC+0000
0xfffffa801936b060 firefox.exe           5616    168     17      243      1      1 2024-07-05 14:07:52 UTC+0000
0xfffffa8018e2bb30 firefox.exe           5632    168     22      269      1      1 2024-07-05 14:11:48 UTC+0000
0xfffffa8019ecfb30 httpd.exe             5072   5152      2       81      1      0 2024-07-05 14:31:26 UTC+0000
0xfffffa8019199440 conhost.exe           4980    420      2       47      1      0 2024-07-05 14:31:26 UTC+0000
0xfffffa801b448340 httpd.exe             6000   5072    156      407      1      0 2024-07-05 14:31:26 UTC+0000
0xfffffa801b28f640 notepad.exe           2368   2208      1       61      1      0 2024-07-05 14:31:44 UTC+0000
0xfffffa80193231c0 firefox.exe           1788    168     14      229      1      1 2024-07-05 14:33:04 UTC+0000
0xfffffa8019239210 audiodg.exe           5704    760      6      133      0      0 2024-07-05 14:35:24 UTC+0000
0xfffffa801ad25060 cmd.exe               5452   2208      1       22      1      0 2024-07-05 14:35:46 UTC+0000
0xfffffa801b9fe5b0 conhost.exe           1508    420      2       53      1      0 2024-07-05 14:35:46 UTC+0000
0xfffffa8019d27700 tor.exe               1752   5452      5      106      1      0 2024-07-05 14:36:49 UTC+0000
0xfffffa801bb47320 firefox.exe           5664   1444     48      756      1      0 2024-07-05 14:36:59 UTC+0000
0xfffffa801bf74060 firefox.exe           5808   5664     17      266      1      0 2024-07-05 14:37:01 UTC+0000
0xfffffa8019020b30 tor.exe               5364   5664      5       70      1      0 2024-07-05 14:37:01 UTC+0000
0xfffffa801a6a5b30 conhost.exe           5220    420      1       34      1      0 2024-07-05 14:37:01 UTC+0000
0xfffffa8019436600 firefox.exe           5864   5664     17      220      1      0 2024-07-05 14:37:01 UTC+0000
0xfffffa801be318c0 firefox.exe           6092   5664     17      217      1      0 2024-07-05 14:37:03 UTC+0000
```

- Lalu selanjutnya saya disini melakukan upaya identifikasi file yang diunduh pada sistem tersebut, menggunakan command "vol -f SELEKDA-PC-20240705-144848.raw --profile=Win7SP1x64 iehistory". Dan terdapat bukti bahwa terdapat file yang tidak sesuai ketentuan yang diperbolehkan pada sistem tersebut, yaitu :

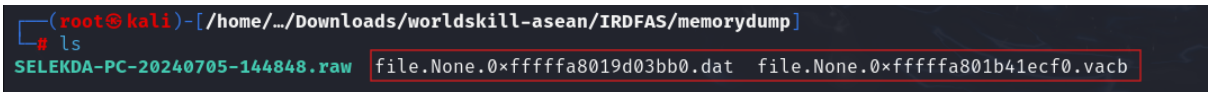
“***Location: :2024070520240706: selekda@file:///C:/Users/selekda/Downloads/tor-expert-bundle-windows-x86_64-13.5.tar.gz***”.



2. Is/Are there any suspicious URLs/links that Dicky opened in his browser(s)? What are they?

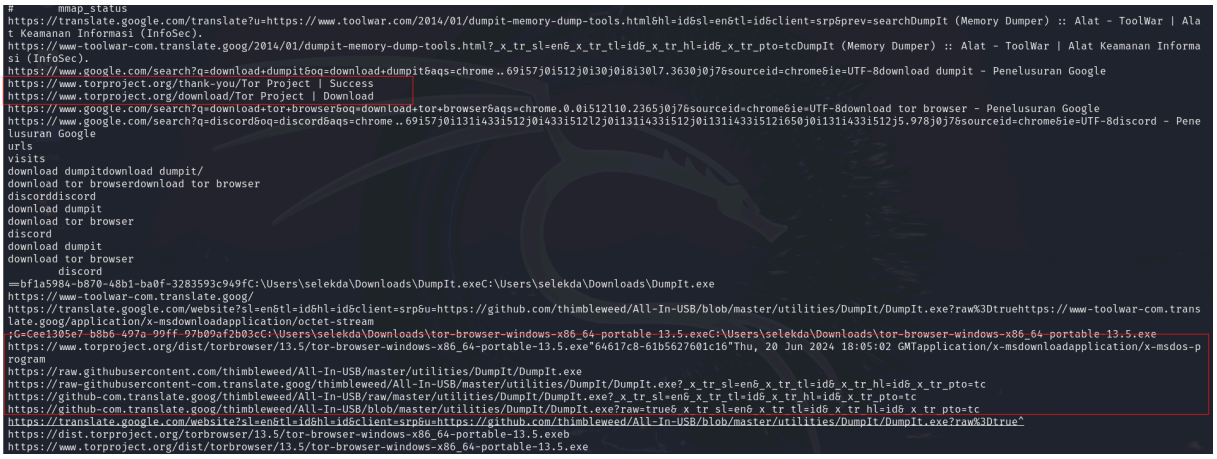
- Pertama Saya mencoba untuk mengidentifikasi file history yang ada pada browser Chrome Dengan command seperti ini *“vol -f SELEKDA-PC-20240705-144848.raw --profile=Win7SP1x64 filescan | grep -ie ‘history$’”* untuk melihat history yang ada pada browser:

- Lalu saya melakukan dumpfiles pada history tersebut dengan command seperti ini *“vol -f SELEKDA-PC-20240705-144848.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000007d5e3d10 -D .”* dan menghasilkan 2 file seperti di bawah ini :



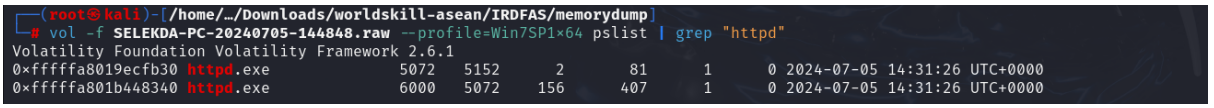
- Selanjutnya disini saya mencoba mengidentifikasi file yang sudah saya dump tadi menggunakan strings dan terdapat beberapa riwayat url yang dikunjungi seperti *“www.torproject.org”* dan *“https://raw.githubusercontent.com/thimbleweed/All-In-USB/master/utilities/DumpIt/DumpIt.exe” untuk Dumpit.exe* juga ada toolwar. lalu untuk *“www.torproject.org”* telah dikunjungi sebanyak 7 kali dan untuk toolwar

sebanyak 3 kali:

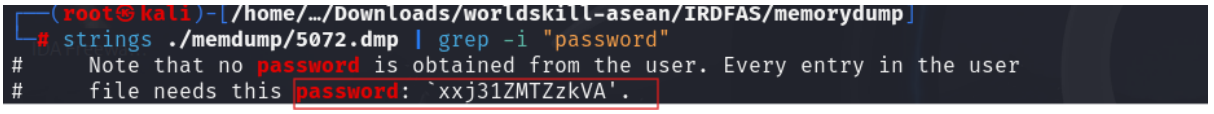


3. Is there any activity related to that from Dicky's device? Did he somehow save certain secret information?

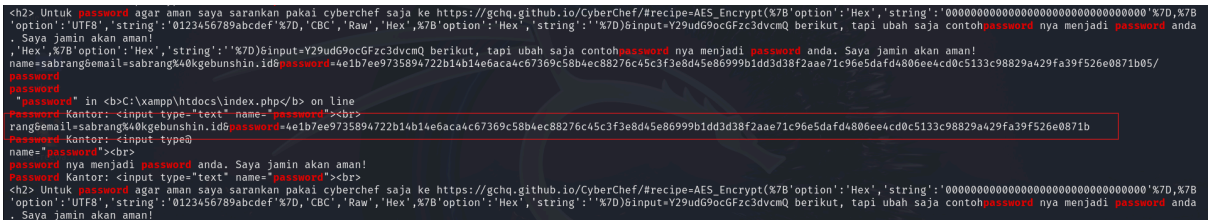
- Pertama disini saya mencoba mengidentifikasi proses yang berjalan pada saat kejadian menggunakan pslist dan di grep "httpd", dan terdapat 2 proses:



- Disini Saya Mencoba Strings pada file yang telah saya dapatkan dari memdump sebelumnya dengan Pid = 5072 yaitu httpd, dan saya grep "password":



- Disini Saya Mencoba Strings pada file yang telah saya dapatkan dari memdump sebelumnya dengan Pid = 6000 yaitu httpd, dan saya grep "password":



- Mengumpulkan Bukti Proses Yang Tidak Normal: File Dan Objek Lainnya

Aplikasi Tidak Resmi yang Diunduh dan Dijalankan:

- **Aplikasi yang Diunduh: tor-expert-bundle-windows-x86_64-13.5.tar.gz ditemukan di direktori Downloads Dicky. Tor adalah software yang sering digunakan untuk mengakses Dark Web, yang mungkin berhubungan dengan masa lalu Dicky.**
- **Eksekusi Aplikasi Mencurigakan:**
    - **File tor.exe ditemukan berjalan pada sistem dan telah dijalankan sebanyak 2 kali.**
    - **Ini menunjukkan kemungkinan akses ke Dark Web yang tidak sesuai dengan kebijakan perusahaan.**

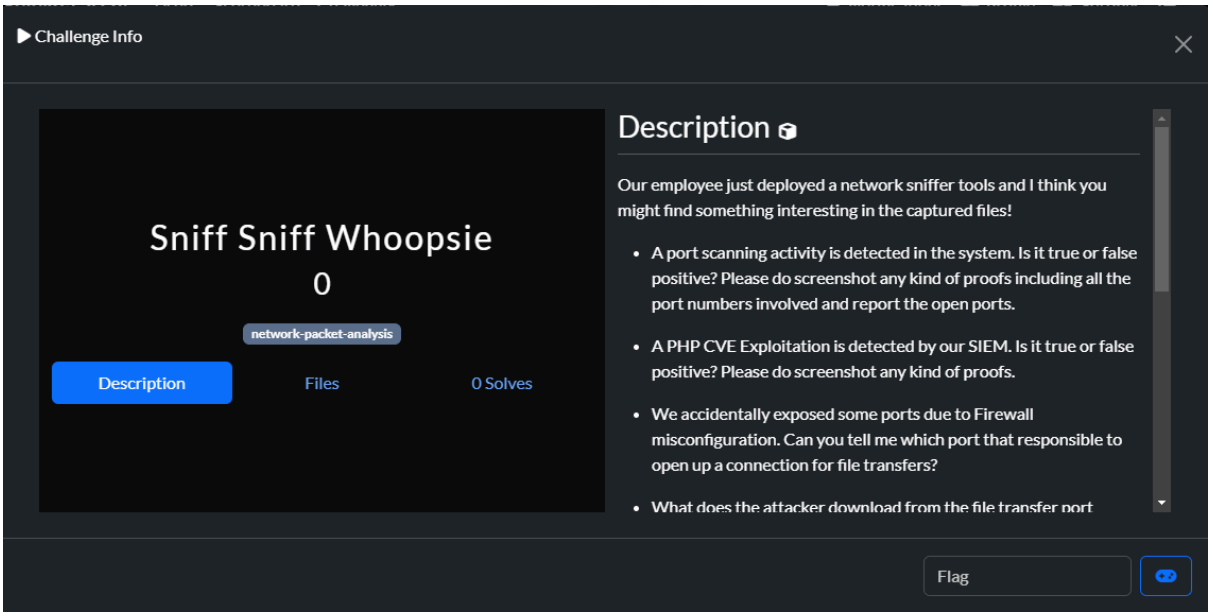
Riwayat URL Mencurigakan yang Dikunjungi Dicky:

- **Dari hasil analisis file history browser, beberapa URL mencurigakan yang dikunjungi oleh Dicky adalah:**
    - **www.torproject.org: Ini adalah situs resmi untuk mendownload Tor Browser, menunjukkan bahwa Dicky mungkin mengakses jaringan Tor untuk mengakses Dark Web.**
    - **https://raw.githubusercontent.com/thimbleweed/All-In-USB/master/utilities/DumpIt/DumpIt.exe: URL ini merujuk pada file DumpIt.exe, yang merupakan alat untuk melakukan dump memory pada sistem Windows. Ini adalah alat yang sering digunakan untuk aktivitas forensic atau bahkan pengintaian.**
- **Jumlah Kunjungan:**
    - **torproject.org: Dikunjungi sebanyak 7 kali.**
    - **DumpIt.exe: Dikunjungi sebanyak 3 kali.**

Aktivitas Terkait Potensi Kebocoran Informasi Rahasia:

- **Dari analisis terhadap proses httpd yang berjalan, ditemukan adanya proses yang terkait dengan server web (HTTP Server) pada sistem. Kedua proses tersebut diidentifikasi memiliki PID 5072 dan 6000.**
- **Saat melakukan pemeriksaan lebih lanjut pada memory dump, ditemukan string yang mengandung kata kunci "password", mengindikasikan adanya informasi sensitif yang mungkin terlibat. Salah satu yang ditemukan adalah potensi password internal atau kredensial yang disimpan dalam file konfigurasi atau dump yang tidak aman.**
- **Ini menunjukkan adanya kemungkinan bahwa Dicky mungkin terlibat dalam aktivitas yang bisa menyebabkan kebocoran informasi internal perusahaan, termasuk password kantor yang mungkin terekspos di file dump atau browser history.**

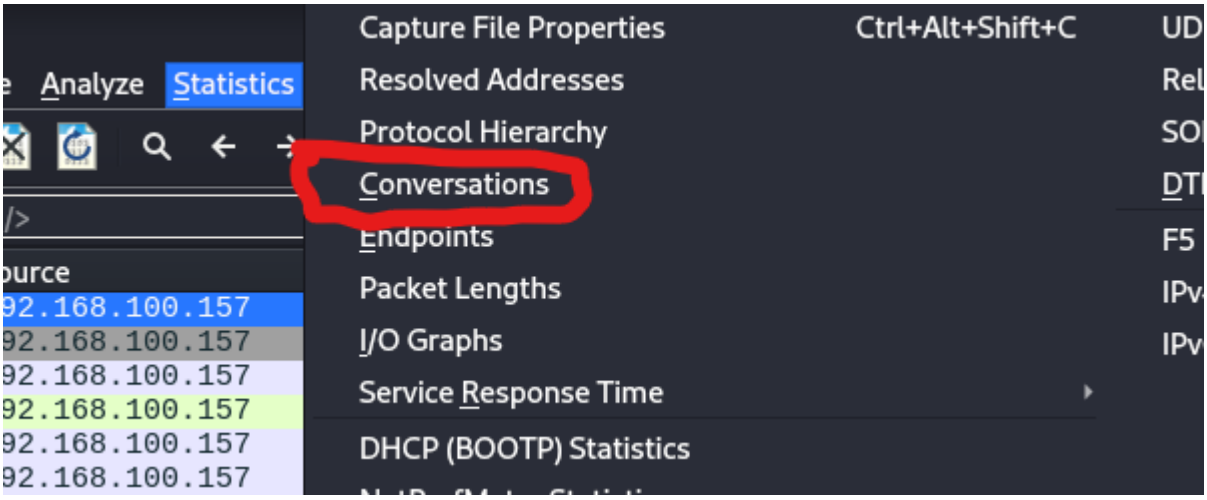
[Network Traffic]



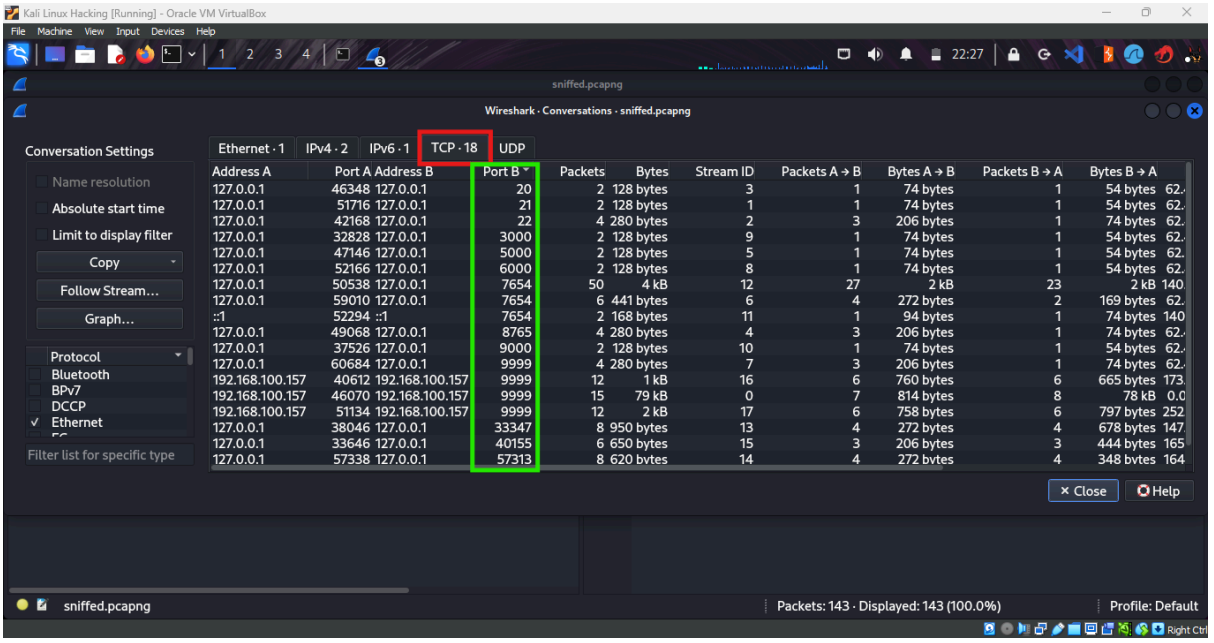
- Mengidentifikasi & Mengalisis Pola Lalu Lintas Jaringan yang Mencurigakan:

1. A port scanning activity is detected in the system. Is it true or false positive? Please do screenshot any kind of proofs including all the port numbers involved and report the open ports.

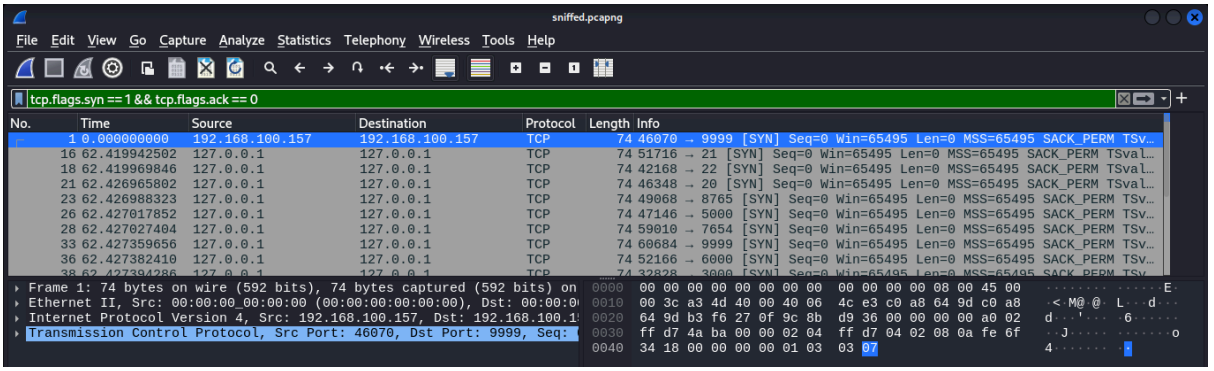
- Pertama-tama install file .pcapng yang telah di sediakan.
- Buka tools wireshark untuk menganalisis & mengidentifikasi file tersebut.
- Untuk menemukan port apa saja yang terlibat,pergi ke menu Statistics > Conversations.



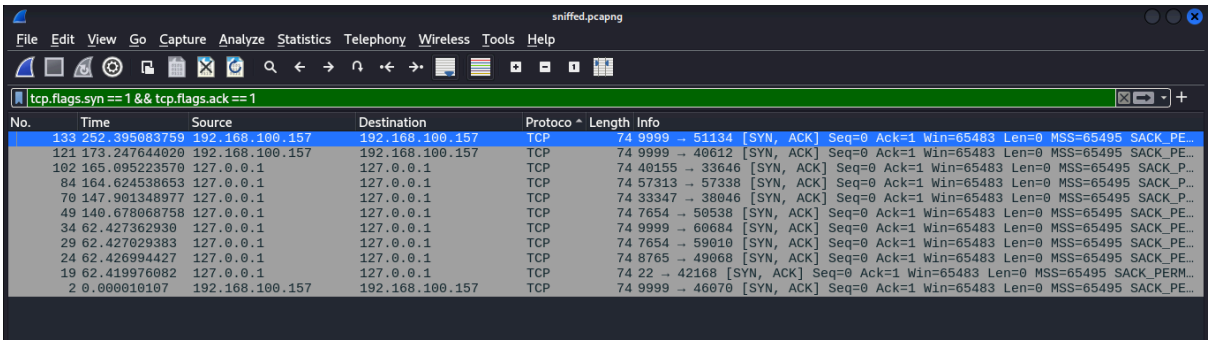
- lalu pergi ke menu TCP-18 > Port B untuk mengecek ada port apa saja.



- lalu ada cara kedua untuk mengecek ada port apa saja dengan cara memfilter paket “tcp.flags.syn == 1 && tcp.flags.ack == 0”.



- lalu untuk mengidentifikasi port apa saja yang terbuka dan terlibat bisa mengunakan command filter paket ini “tcp.flags.syn == 1 && tcp.flags.ack == 1”.



Berikut daftar port yang terbuka berdasarkan informasi SYN-ACK:

1. **Port 9999**
2. **Port 40612**
3. **Port 51134**
4. **Port 40155**
5. **Port 33346**
6. **Port 57313**

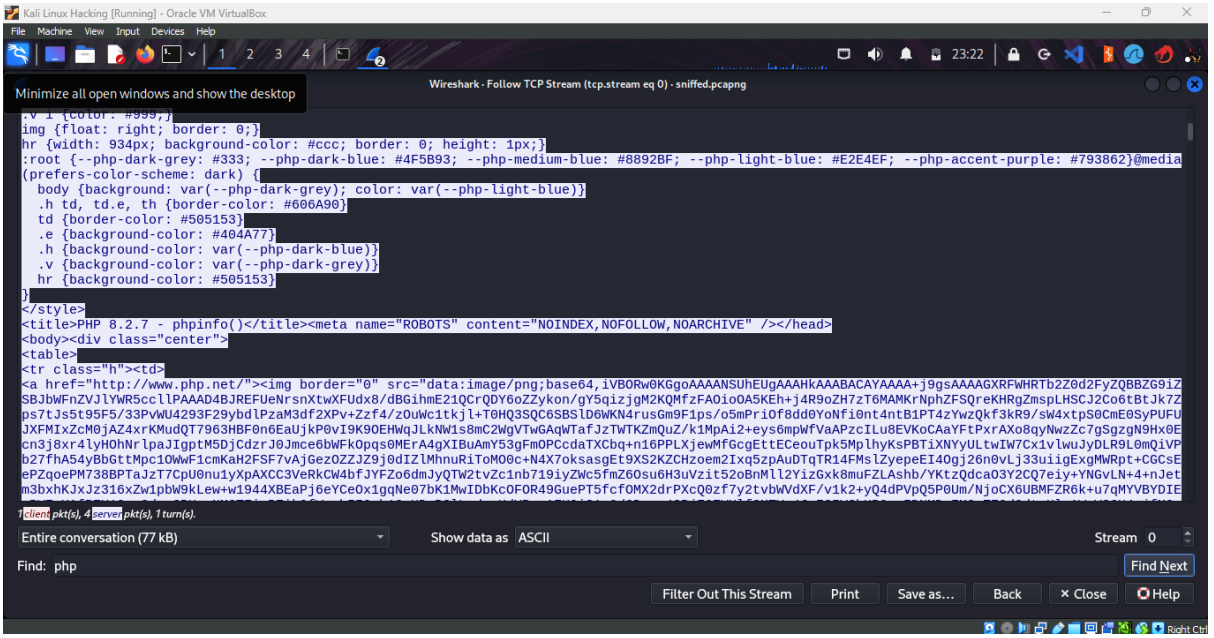
7. **Port 33347**
8. **Port 7654**

Kesimpulan:

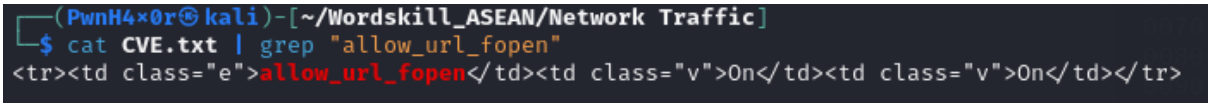
- **192.168.100.157: Port 9999, 40612, 51134**
- **127.0.0.1: Port 40155, 33346, 57313, 33347, 7654**

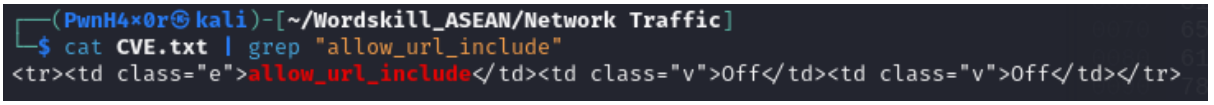
2. A PHP CVE Exploitation is detected by our SIEM. Is it true or false positive? Please do screenshot any kind of proofs.

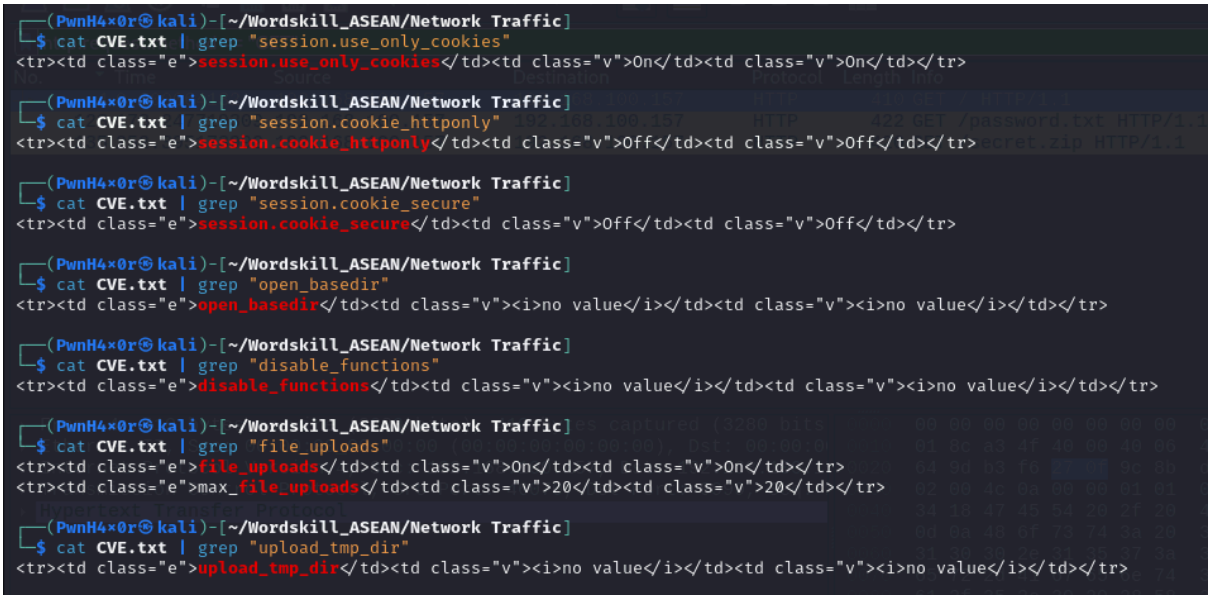
- Jawabannya adalah true, berikut adalah bukti dan deskripsinya:
- Disini terdapat sebuah code dan konfigurasi php yang vuln.



- karena saya kesulitan memfilter nya, lalu saya sari copy semua code nya lalu membuat sebuah file CVE.txt, objective saya adalah konfigurasi php.ini"







- Berdasarkan konfigurasi PHP yang Anda berikan, berikut adalah beberapa poin terkait potensi eksploitasi PHP:

1. Versi PHP

- **Status: PHP versi 8.2.7**
- **Analisis: Periksa apakah ada CVE (Common Vulnerabilities and Exposures) yang terkait dengan versi ini. Secara umum, versi terbaru PHP berupaya memperbaiki banyak kerentanan yang ada di versi sebelumnya.**

2. Pengaturan allow_url_fopen

- **Status: Diaktifkan (On)**
- **Analisis: Fitur ini memungkinkan pengguna untuk mengakses file dari URL, yang dapat dieksploitasi oleh penyerang untuk mengakses file-file sensitif pada server.**

3. Pengaturan allow_url_include

- **Status: Dinonaktifkan (Off)**
- **Analisis: Ini merupakan langkah keamanan yang baik. Jika diaktifkan, fitur ini dapat memungkinkan injeksi file dari URL, meningkatkan risiko eksploitasi melalui pengunggahan file berbahaya.**

4. Pengaturan session.cookie_httponly

- **Status: Dinonaktifkan (Off)**
- **Analisis: Dengan pengaturan ini, cookie sesi dapat diakses oleh skrip JavaScript, meningkatkan risiko serangan XSS (Cross-Site Scripting). Penyerang dapat mencuri ID sesi pengguna jika berhasil menyisipkan skrip jahat ke dalam halaman web.**

5. Pengaturan session.cookie_secure

- **Status: Dinonaktifkan (Off)**
- **Analisis: Jika situs Anda tidak menggunakan HTTPS, cookie sesi akan dikirim melalui koneksi yang tidak aman. Ini membuat cookie rentan terhadap serangan man-in-the-middle (MITM). Mengaktifkan opsi ini memastikan cookie hanya dikirim melalui koneksi yang aman.**

6. Pengaturan open_basedir

- **Status: Tidak ada nilai yang ditentukan**
- **Analisis: Tanpa pembatasan open_basedir, skrip PHP dapat mengakses file di seluruh sistem, yang dapat dieksploitasi untuk membaca file sensitif seperti /etc/passwd atau file konfigurasi aplikasi. Menetapkan direktori yang diizinkan untuk akses file sangat disarankan.**

7. Pengaturan disable_functions

- **Status: Tidak ada fungsi yang dinonaktifkan**
- **Analisis: Tidak menonaktifkan fungsi berbahaya seperti exec(), shell_exec(), dan eval() meningkatkan potensi untuk mengeksekusi perintah sistem. Ini dapat dimanfaatkan oleh penyerang untuk menjalankan kode berbahaya di server.**

8. Pengaturan file_uploads

- **Status: Diaktifkan (On)**
- **Analisis: Mengizinkan unggahan file dapat menjadi risiko jika tidak ada validasi yang ketat terhadap jenis dan ukuran file yang diunggah. Penyerang dapat mencoba mengunggah file berbahaya (misalnya, skrip PHP yang dapat dieksekusi) ke server.**

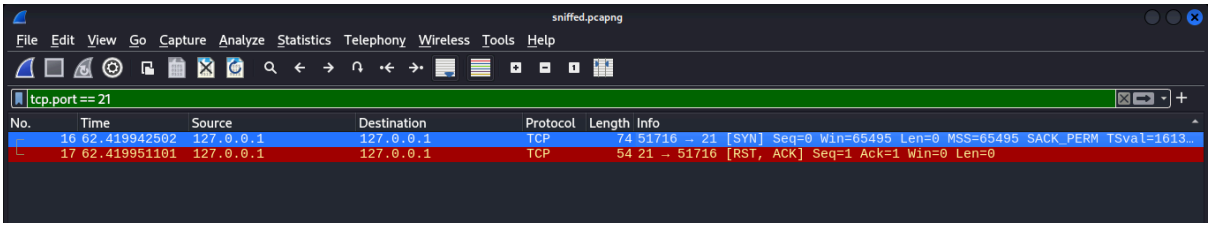
9. Pengaturan upload_tmp_dir

- **Status: Tidak ada nilai yang ditentukan**
- **Analisis: Tanpa direktori sementara yang ditentukan, PHP akan menggunakan direktori default sistem. Jika direktori ini tidak aman, file unggahan dapat diakses oleh pengguna lain, berpotensi mengakibatkan kebocoran data atau eksploitasi.**

3. We accidentally exposed some ports due to Firewall misconfiguration. Can you tell me which port that responsible to open up a connection for file transfers?

- Jawabannya adalah port 21 (ftp), berikut ini adalah bukti dan deskripsinya:
- Di sini terdapat sebuah port 21 (FTP) yang terbuka. Setelah saya cek ke Follow > TCP Stream, saya menemukan informasi lebih lanjut mengenai komunikasi yang terjadi antara klien dan server.
Deskripsi:

- **Port 21 adalah port standar untuk protokol FTP yang digunakan untuk komunikasi kontrol. Dalam analisis lalu lintas, terlihat bahwa klien mengirimkan perintah-perintah FTP seperti USER, PASS, SYST, dan FEAT ke server melalui port ini.**
- **Proses otentikasi berhasil dilakukan dengan mengirimkan username dan password, yang menunjukkan bahwa port ini berfungsi dengan baik untuk menerima dan memproses perintah FTP.**
- **Selanjutnya, port 21 juga digunakan untuk mengatur koneksi data, yang memungkinkan transfer file melalui perintah seperti LIST, NLST, dan RETR.**



4. What does the attacker download from the file transfer port related?

- Penyerang mengunduh file dengan nama secret.zip dari port transfer file yang terkait. Berdasarkan analisis lalu lintas, berikut adalah detail yang relevan:

- Perintah yang Digunakan:

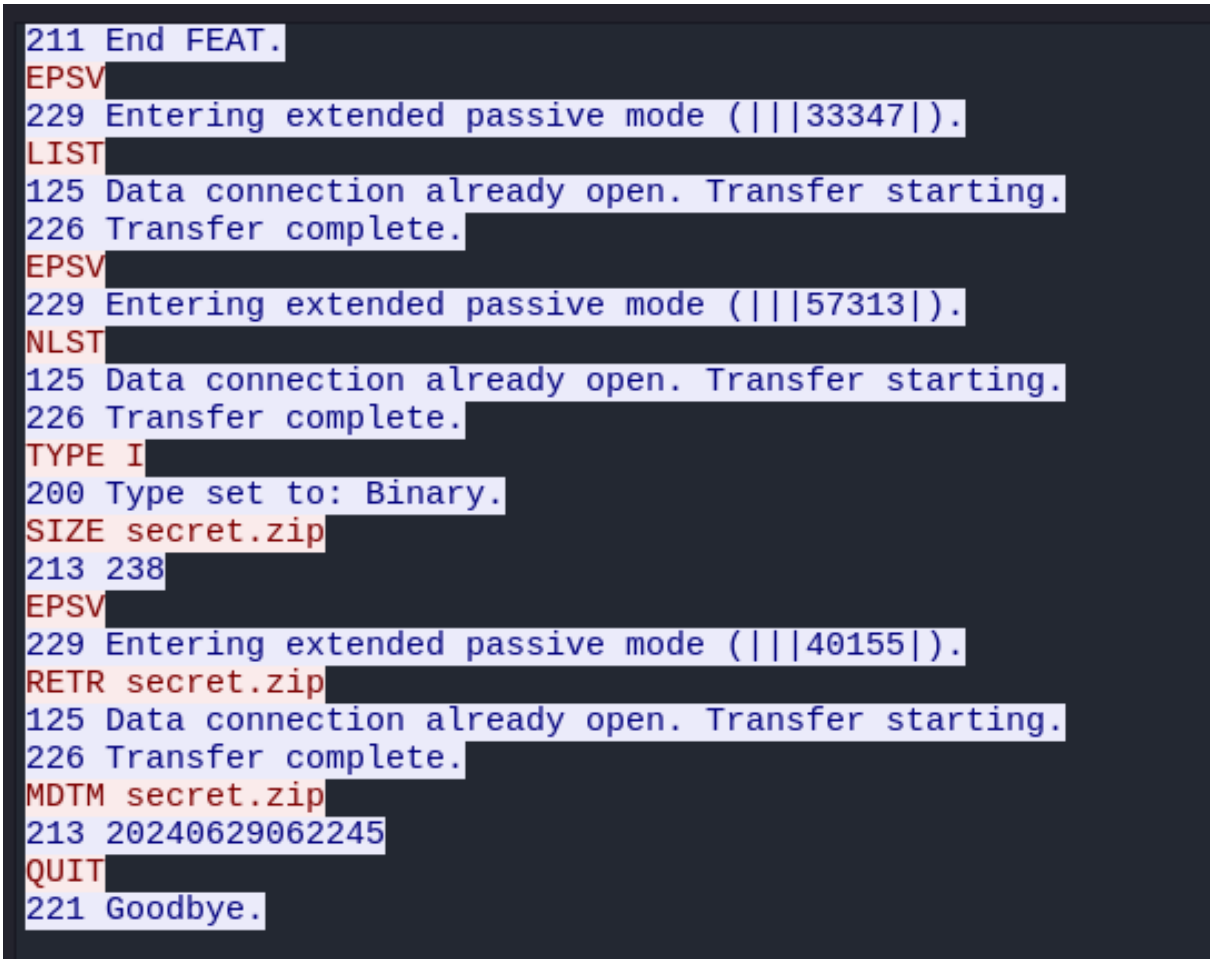
- **Penyerang menggunakan perintah RETR secret.zip untuk meminta pengunduhan file tersebut dari server FTP.**

- Proses Pengunduhan:

- **Setelah perintah RETR dikirim, server memberikan respons 125 Data connection already open. Transfer starting., yang menandakan bahwa koneksi data sudah terbuka dan transfer file akan dimulai.**
- **Setelah proses transfer selesai, server mengonfirmasi dengan respons 226 Transfer complete., menunjukkan bahwa file telah berhasil diunduh oleh penyerang.**

- Ukuran File:

- **Ukuran file yang diunduh adalah 238 bytes, yang diinformasikan melalui perintah SIZE secret.zip dengan respons 213 238.**



5. Any chance the attacker download an internal file which should not be public? Our developer is pretty clumsy that he puts some kind of confidential hint in the website.

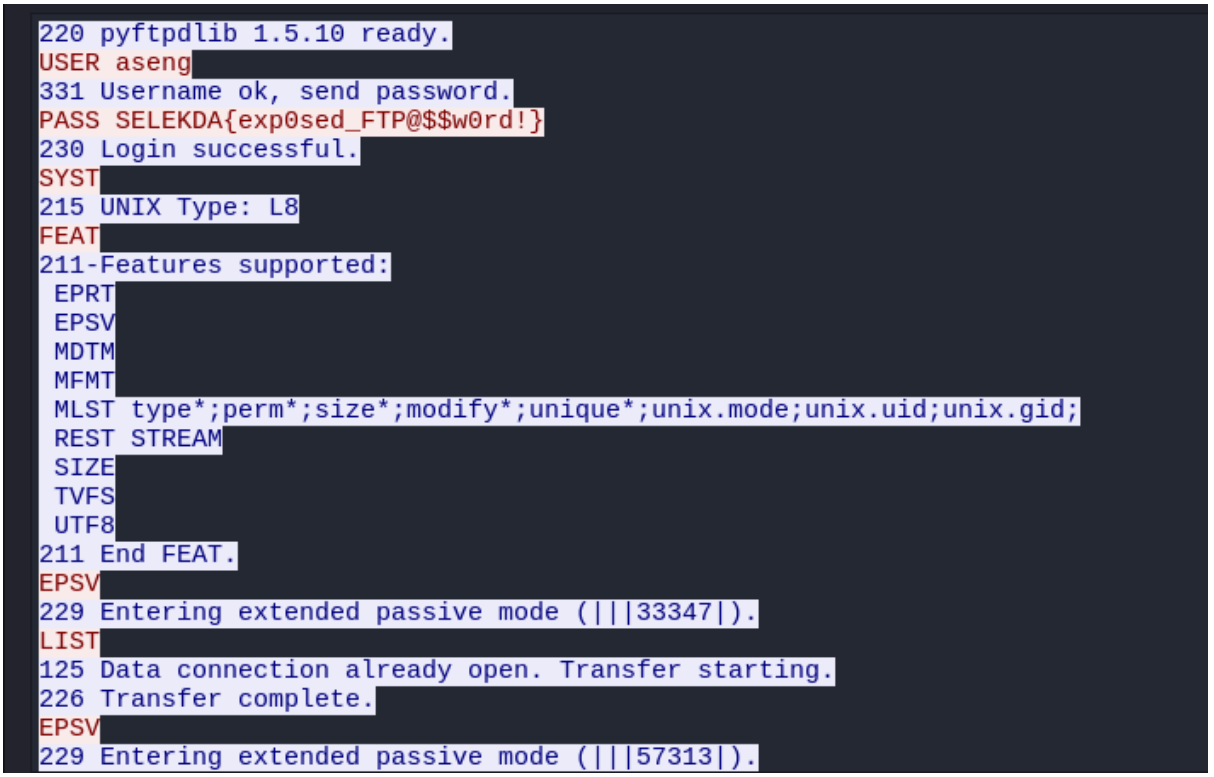
- Ya, terdapat kemungkinan bahwa penyerang dapat mengunduh berkas internal yang seharusnya tidak bersifat publik. Dalam log yang disediakan, penyerang berhasil masuk ke server FTP menggunakan kredensial yang terlihat terbuka, dan melakukan beberapa operasi yang menunjukkan bahwa mereka dapat mengakses berkas yang mungkin bersifat sensitif.

Berikut adalah analisis lebih lanjut terkait hal ini:

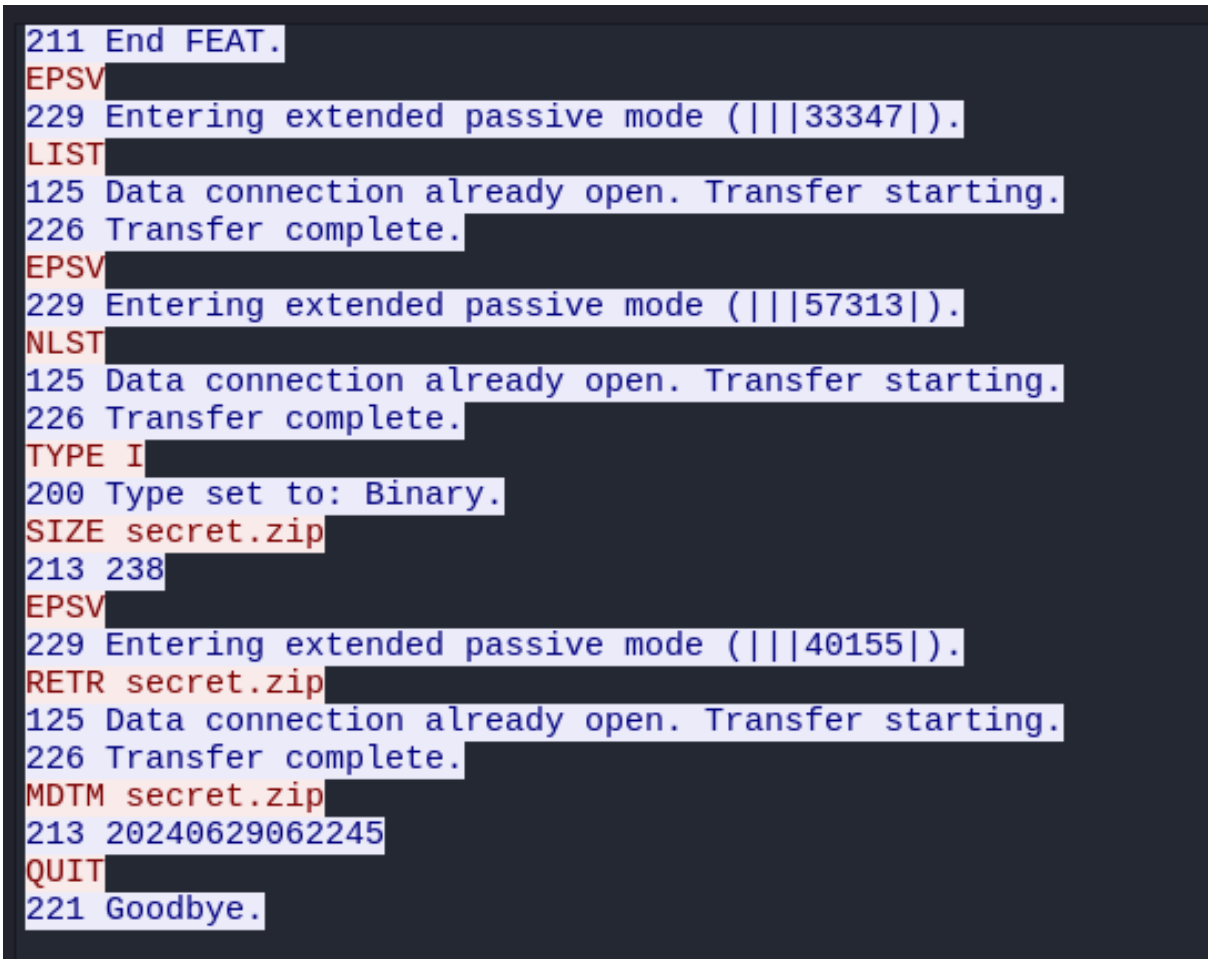
1. **Akses yang Tidak Sah:**
    - **Penyerang berhasil login menggunakan username aseng dan password SELEKDA{exp0sed_FTP@$$w0rd!}. Ini menunjukkan bahwa kredensial yang diekspos digunakan untuk mendapatkan akses ke server FTP.**
2. **Operasi Pengunduhan:**

- **Dalam log, terdapat perintah RETR secret.zip, yang menunjukkan bahwa penyerang berhasil mengunduh berkas dengan nama secret.zip.**
- **Nama berkas ini mengindikasikan bahwa kontennya mungkin bersifat rahasia atau sensitif.**

3. **Transfer Berkas:**
    - **Setelah mengeluarkan perintah RETR, server memberikan respons 226 Transfer complete, yang menandakan bahwa file berhasil diunduh. Ini menunjukkan bahwa penyerang telah mengambil berkas tersebut tanpa izin.**



```
220 pyftpdlib 1.5.10 ready.
USER aseng
331 Username ok, send password.
PASS SELEKDA{exp0sed_FTP@$$w0rd!}
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features supported:
 EPRT
 EPSV
 MDTM
 MFMT
 MLST type*;perm*;size*;modify*;unique*;unix.mode;unix.uid;unix.gid;
 REST STREAM
 SIZE
 TVFS
 UTF8
211 End FEAT.
EPSV
229 Entering extended passive mode (|||33347|).
LIST
125 Data connection already open. Transfer starting.
226 Transfer complete.
EPSV
229 Entering extended passive mode (|||57313|).
```

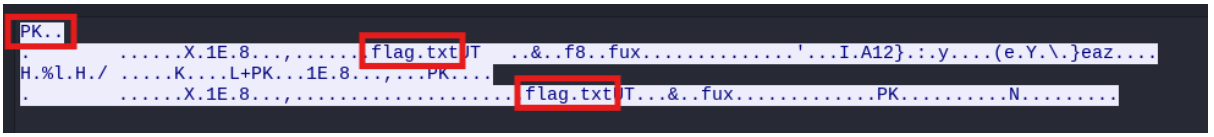


```
211 End FEAT.
EPSV
229 Entering extended passive mode (|||33347|).
LIST
125 Data connection already open. Transfer starting.
226 Transfer complete.
EPSV
229 Entering extended passive mode (|||57313|).
NLST
125 Data connection already open. Transfer starting.
226 Transfer complete.
TYPE I
200 Type set to: Binary.
SIZE secret.zip
213 238
EPSV
229 Entering extended passive mode (|||40155|).
RETR secret.zip
125 Data connection already open. Transfer starting.
226 Transfer complete.
MDTM secret.zip
213 20240629062245
QUIT
221 Goodbye.
```

6. Please answer this question if the previous ones is true. What was the content of the protected file ONLY IF the attacker steal/download the file? Is the password pretty strong?

- Jika penyerang berhasil mengunduh file secret.zip, isi file tersebut berisi:

- **File flag.txt**



- Mengenai kekuatan kata sandi yang digunakan oleh penyerang, kata sandi SELEKDA{exp0sed_FTP@$$w0rd!} memiliki beberapa elemen yang bisa dikategorikan sebagai cukup kompleks:

- **Panjang: Kata sandi ini cukup panjang, yang merupakan faktor positif dalam keamanan.**
- **Karakter Campuran: Terdapat kombinasi huruf besar, huruf kecil, angka, dan karakter khusus (@, $, {, }), yang meningkatkan kompleksitasnya.**

Namun, ada beberapa pertimbangan yang perlu diperhatikan:

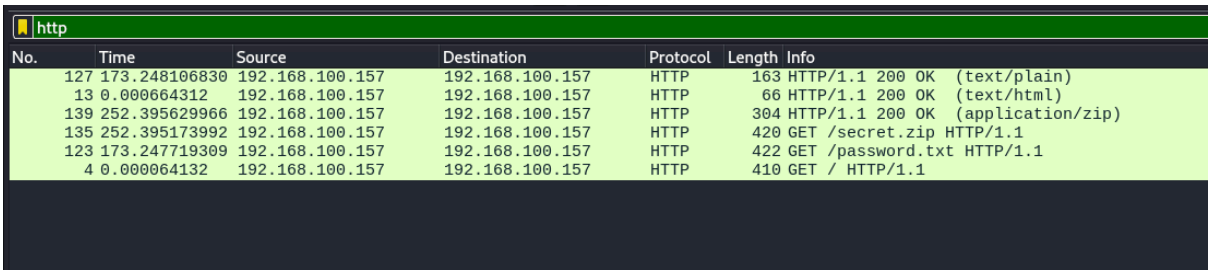
- **Penggunaan Karakter Khusus: Meskipun terdapat karakter khusus, struktur kata sandi ini mengandung pola yang dapat diantisipasi. Penggunaan kata "exposed" di dalamnya mungkin menunjukkan bahwa kata sandi ini bisa saja mudah ditebak jika ada informasi yang relevan tentang konteksnya.**
- **Pola yang Dikenal: Jika penyerang tahu bahwa kata sandi mengikuti pola tertentu, mereka dapat mencoba serangan berbasis pola untuk mendapatkan akses.**

```
220 pyftpdlib 1.5.10 ready.
USER aseng
331 Username ok, send password.
PASS SELEKDA{exp0sed_FTP@$$w0rd!}
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features supported:
 EPRT
 EPSV
 MDTM
 MFMT
 MLST type*;perm*;size*;modify*;unique*;unix.mode;unix.uid;unix.gid;
 REST STREAM
 SIZE
 TVFS
 UTF8
211 End FEAT.
EPSV
229 Entering extended passive mode (|||33347|).
LIST
125 Data connection already open. Transfer starting.
226 Transfer complete.
EPSV
229 Entering extended passive mode (|||57313|).
```

```
211 End FEAT.
EPSV
229 Entering extended passive mode (|||33347|).
LIST
125 Data connection already open. Transfer starting.
226 Transfer complete.
EPSV
229 Entering extended passive mode (|||57313|).
NLST
125 Data connection already open. Transfer starting.
226 Transfer complete.
TYPE I
200 Type set to: Binary.
SIZE secret.zip
213 238
EPSV
229 Entering extended passive mode (|||40155|).
RETR secret.zip
125 Data connection already open. Transfer starting.
226 Transfer complete.
MDTM secret.zip
213 20240629062245
QUIT
221 Goodbye.
```

7. (BONUS FOR FUN)There's one FLAG indicating the password disclosure on one of the authenticated ports. Can you find it?

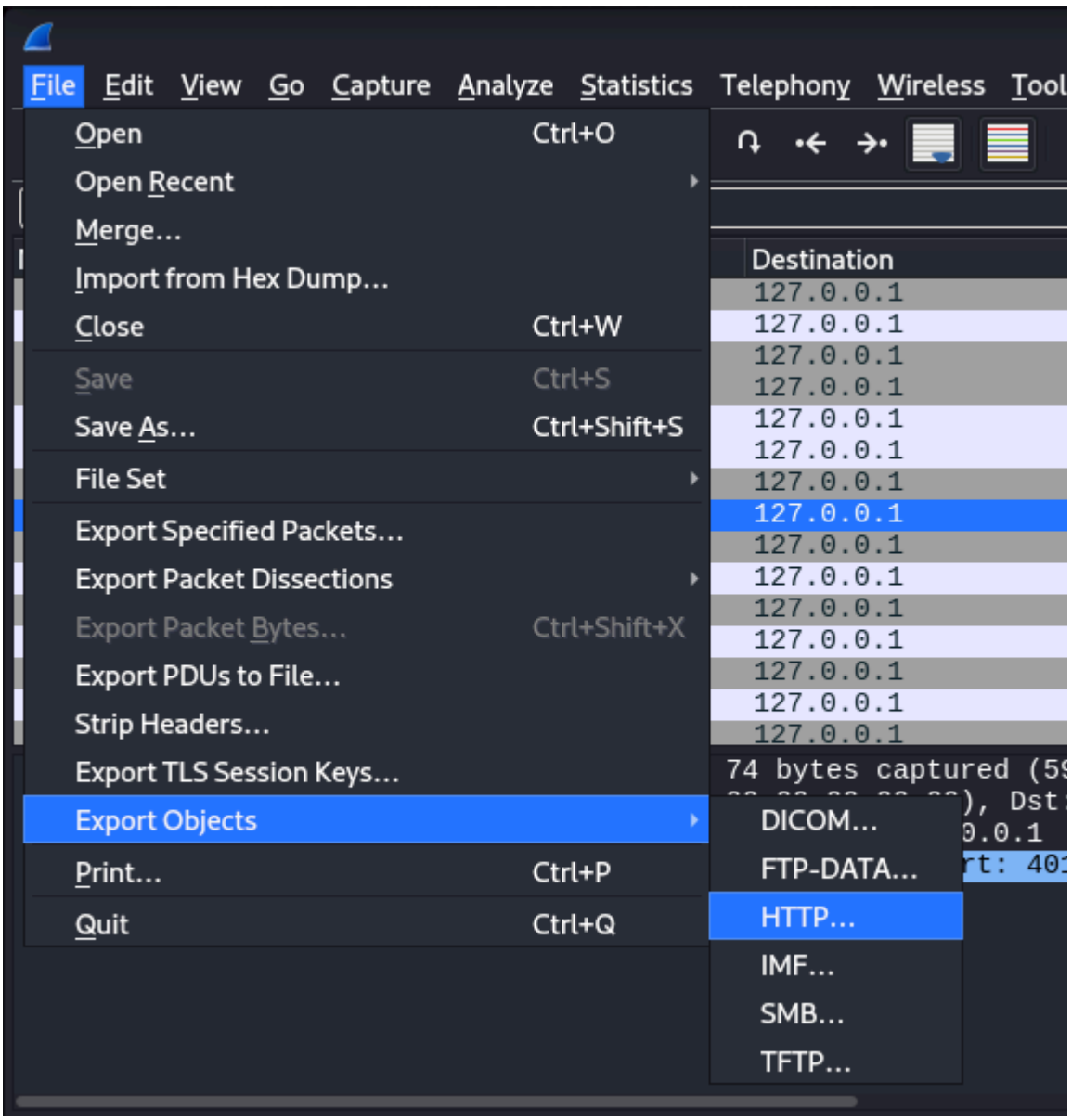
- identifikasi port http.

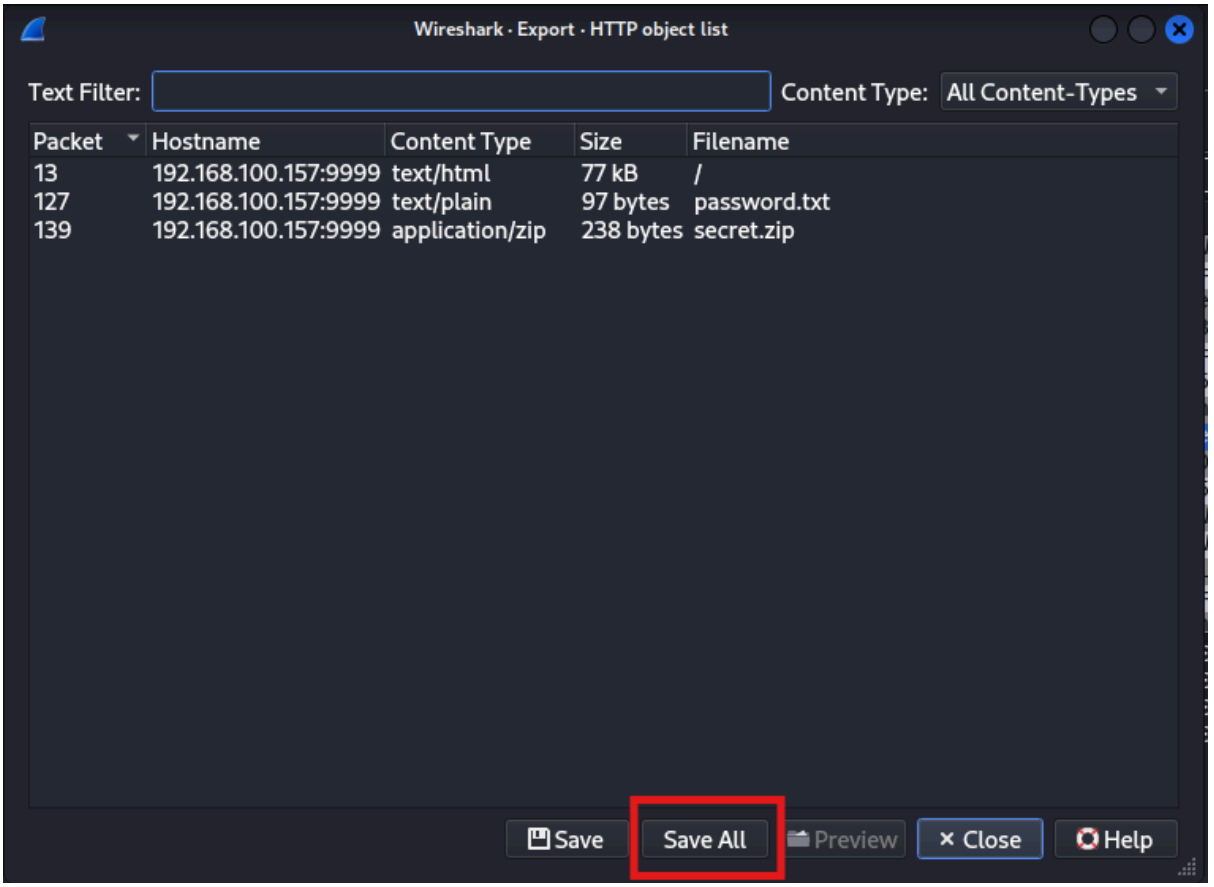


http

No.	Time	Source	Destination	Protocol	Length	Info
127	173.248106830	192.168.100.157	192.168.100.157	HTTP	163	HTTP/1.1 200 OK (text/plain)
13	0.000664312	192.168.100.157	192.168.100.157	HTTP	66	HTTP/1.1 200 OK (text/html)
139	252.395629966	192.168.100.157	192.168.100.157	HTTP	304	HTTP/1.1 200 OK (application/zip)
135	252.395173992	192.168.100.157	192.168.100.157	HTTP	420	GET /secret.zip HTTP/1.1
123	173.247719309	192.168.100.157	192.168.100.157	HTTP	422	GET /password.txt HTTP/1.1
4	0.000064132	192.168.100.157	192.168.100.157	HTTP	410	GET / HTTP/1.1

- extract semua file yang ada di protocol http, dengan pergi ke menu File > Export Objects > HTTP.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tool
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
FTP-DATA...
HTTP...
IMF...
SMB...
TFTP...
Destination
127.0.0.1
74 bytes captured



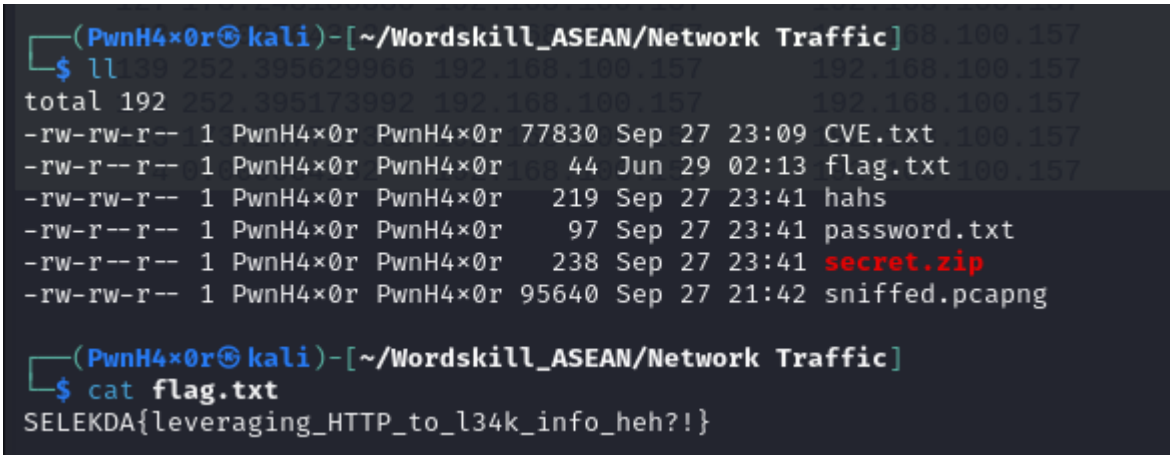
- Ketika saya berusaha mengekstrak file secret.zip, saya dihadapkan pada tantangan karena memerlukan password. Dengan penuh harapan, saya membuka file password.txt, di mana terdapat sebuah petunjuk menarik: "rockyou.txt" Petunjuk ini memicu rasa ingin tahu saya, dan saya segera memutuskan untuk melakukan cracking password menggunakan wordlist yang terkenal, yaitu rockyou.txt.

```
┌──(PwnH4×0r㉿kali)-[~/Wordskill_ASEAN/Network Traffic]
└─$ ll
total 104
-rw-rw-r-- 1 PwnH4×0r PwnH4×0r     0 Sep 28 01:49 CVE.txt
-rw-r--r-- 1 PwnH4×0r PwnH4×0r    97 Sep 28 01:37 password.txt
-rw-r--r-- 1 PwnH4×0r PwnH4×0r   238 Sep 28 01:37 secret.zip
-rw-rw-r-- 1 PwnH4×0r PwnH4×0r 95640 Sep 27 21:42 sniffed.pcapng

┌──(PwnH4×0r㉿kali)-[~/Wordskill_ASEAN/Network Traffic]
└─$ cat password.txt
Whenever you see something compressed, just remember it is a known ones contained in rockyou.txt
```

- dengan menggunakan tools zip2john saya berhasil mendapatkan passwordnya "happybirthday"

```
┌──(PwnH4×0r㉿kali)-[~/Wordskill_ASEAN/Network Traffic]
└─$ zip2john secret.zip > hahs
ver 1.0 efh 5455 efh 7875 secret.zip/flag.txt PKZIP Encr: 2b chk, TS_chk, cmplen=56, decmplen=44, crc=F34531F7 ts=11BD cs=11bd type=0

┌──(PwnH4×0r㉿kali)-[~/Wordskill_ASEAN/Network Traffic]
└─$ john hahs --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
happybirthday    (secret.zip/flag.txt)
1g 0:00:00:00 DONE (2024-09-27 23:42) 25.00g/s 307200p/s 307200c/s 307200C/s iheartyou..henrik
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(PwnH4×0r㉿kali)-[~/Wordskill_ASEAN/Network Traffic]
└─$ unzip secret.zip
Archive:  secret.zip
[secret.zip] flag.txt password:
 extracting: flag.txt
```

Crypton Commanders



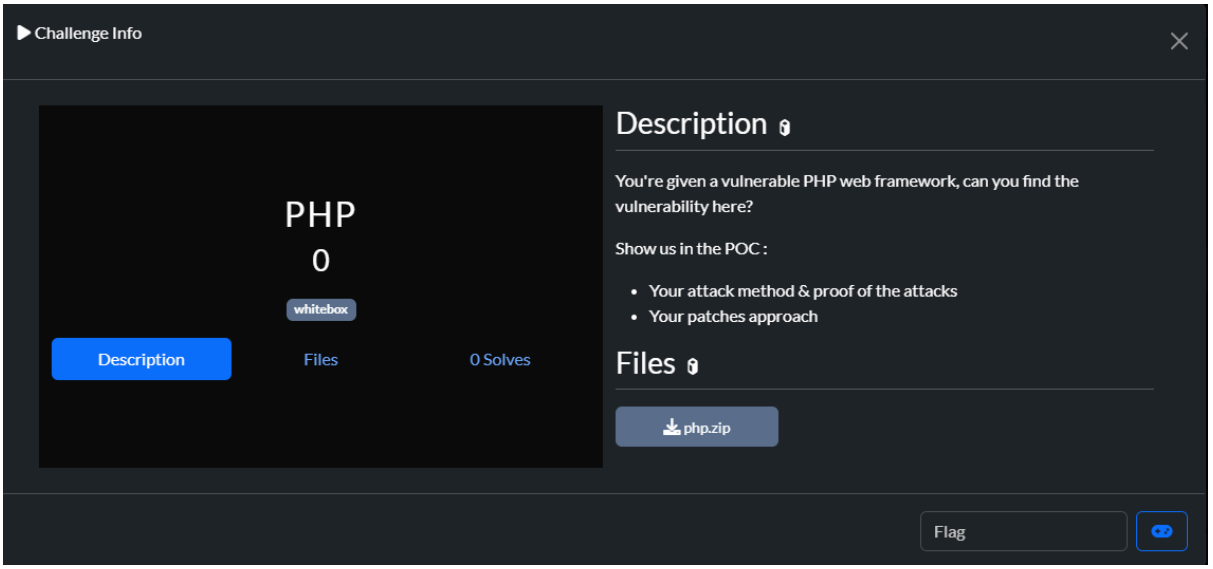
FLAG: SELEKDA{leveraging_HTTP_to_l34k_info_heh?!}

- Menilai Dampak Keamanan dari Aktivitas Jaringan

1. **Ekspos Port FTP (Port 21)**:
   - **Risk**: Port FTP yang terbuka dapat dieksploitasi oleh penyerang untuk mengakses file dan data sensitif yang seharusnya tidak tersedia untuk publik.
   - **Impact**: Potensi pencurian data yang dapat merugikan organisasi, termasuk kebocoran informasi rahasia.
2. **Pengunduhan File Internal**:
   - **Risk**: Penyerang dapat mengunduh file internal, seperti secret.zip, yang mungkin berisi informasi sensitif.
   - **Impact**: Ini dapat menyebabkan kebocoran data, yang dapat mengakibatkan kerugian reputasi dan hukum bagi organisasi.
3. **Kelemahan dalam Autentikasi**:
   - **Risk**: Penggunaan kata sandi yang lemah atau kurang kuat dapat mempermudah penyerang dalam melakukan akses tidak sah.
   - **Impact**: Akses tidak sah dapat mengakibatkan pencurian data atau pengubahan informasi penting.
4. **Koneksi Tanpa Enkripsi**:
   - **Risk**: Jika FTP digunakan tanpa enkripsi, data, termasuk kredensial, dapat ditangkap selama transmisi.
   - **Impact**: Data yang ditangkap dapat digunakan oleh penyerang untuk melakukan akses tidak sah ke sistem dan data lebih lanjut.

[Application Source Code]

PHP:



- Attack Method & Proof of the Attacks

1. Cross-Site Scripting (XSS)

- **File Terpengaruh**: home.php
- **Kerentanan**: Output dari note yang diambil dari database tidak disanitasi sebelum ditampilkan, berpotensi menyebabkan **Stored XSS**.
- **Baris yang Rentan**: **40**

```
37  <ul>
38      <?php foreach ($notes as $note): ?>
39          <li>
40              <?php echo $note['note']; ?>
41              <a href="?delete=<?php echo $note['id']; ?>">Delete</a>
42          </li>
43      <?php endforeach; ?>
44  </ul>
```

- **Dampak**: Jika pengguna menyimpan sebuah catatan yang berisi kode JavaScript berbahaya (misalnya <script>alert('XSS');</script>), kode ini akan dieksekusi ketika catatan tersebut ditampilkan kepada pengguna lain.

- **Patch**: Escape output menggunakan htmlspecialchars() untuk mencegah injeksi JavaScript:

```
37  <ul>
38      <?php foreach ($notes as $note): ?>
39          <li>
40              <?php echo htmlspecialchars($note['note'], ENT_QUOTES, 'UTF-8'); ?>
41              <a href="?delete=<?php echo $note['id']; ?>">Delete</a>
42          </li>
43      <?php endforeach; ?>
44  </ul>
```

2. SQL Injection (Delete Function)

- **File Terpengaruh**: home.php
- **Kerentanan**: Fungsi delete menggunakan nilai yang diambil dari parameter GET tanpa validasi yang memadai, sehingga berpotensi terhadap **SQL Injection**.
- **Baris yang Rentan**: **20**

```
19  if (isset($_GET['delete'])) {
20      $note_id = filter_input(INPUT_GET, 'delete', FILTER_VALIDATE_INT);
21      $stmt = $pdo->prepare('DELETE FROM notes WHERE id = :id AND user_id = :user_id');
22      $stmt->execute(['id' => $note_id, 'user_id' => $user_id]);
23  }
```

- Meskipun FILTER_VALIDATE_INT digunakan, tidak ada pengecekan lebih lanjut apakah parameter tersebut valid. Jika filter_input() gagal, bisa menyebabkan query injection.
- **Dampak**: Penyerang dapat memodifikasi URL dengan parameter yang berbahaya, misalnya ?delete=1' OR 1=1, yang dapat menyebabkan penghapusan seluruh catatan dalam tabel.
- **Patch**: Tambahkan pengecekan lebih ketat setelah filter:

```
19  if (isset($_GET['delete'])) {
20      $note_id = filter_input(INPUT_GET, 'delete', FILTER_VALIDATE_INT);
21      if ($note_id === false || $note_id === null) {
22          exit('Invalid note ID');
23      }
24
25      $stmt = $pdo->prepare('DELETE FROM notes WHERE id = :id AND user_id = :user_id');
26      $stmt->execute(['id' => $note_id, 'user_id' => $user_id]);
27  }
```

3. Brute Force Login (No Rate Limiting)

- **File Terpengaruh**: login.php
- **Kerentanan**: Tidak ada mekanisme rate-limiting atau pembatasan jumlah percobaan login, yang memungkinkan **Brute Force Attack** pada halaman login.

- **Baris yang Rentan: 9**

```php
if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    $username = filter_input(INPUT_POST, 'username', FILTER_SANITIZE_STRING);
    $password = $_POST['password'];

    $stmt = $pdo->prepare('SELECT * FROM users WHERE username = :username');
    $stmt->execute(['username' => $username]);
    $user = $stmt->fetch();
```

- **Dampak**: Penyerang dapat mencoba banyak kombinasi username dan password tanpa batas hingga menemukan kombinasi yang tepat.
- **Patch**: Terapkan rate-limiting atau tambahkan mekanisme delay setelah beberapa percobaan gagal. Sebagai contoh, Anda bisa menghitung percobaan gagal dan memblokir percobaan selanjutnya setelah sejumlah kegagalan:

```php
// Inisialisasi variabel untuk mencatat percobaan login yang gagal
if (!isset($_SESSION['login_attempts'])) {
    $_SESSION['login_attempts'] = 0;
}

if (!isset($_SESSION['last_login_attempt'])) {
    $_SESSION['last_login_attempt'] = 0;
}

// Limit percobaan login
$max_attempts = 5;
// Durasi timeout setelah mencapai limit
$timeout_duration = 60;

if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    // Cek apakah user sedang dalam timeout
    if ($_SESSION['login_attempts'] >= $max_attempts && (time() - $_SESSION['last_login_attempt']) < $timeout_duration) {
        echo "Too many login attempts. Please try again in " . ($timeout_duration - (time() - $_SESSION['last_login_attempt
        exit();
    }

    $username = filter_input(type: INPUT_POST, var_name: 'username', filter: FILTER_SANITIZE_STRING);
    $password = $_POST['password'];

    $stmt = $pdo->prepare('SELECT * FROM users WHERE username = :username');
    $stmt->execute(['username' => $username]);
    $user = $stmt->fetch();
```

4. Username Enumeration (Login)

- **File Terpengaruh**: login.php
- **Kerentanan**: Pesan kesalahan yang spesifik saat login (Invalid username or password) memungkinkan penyerang untuk melakukan **Username Enumeration**.
- **Baris yang Rentan: 13**

```php
    if ($user && password_verify($password, $user['password'])) {
        $_SESSION['user_id'] = $user['id'];
        header('Location: notes.php');
        exit();
    } else {
        echo "Invalid username or password.";
    }
```

Dampak: Penyerang bisa mencoba username yang berbeda-beda dan mendeteksi username yang valid berdasarkan respons spesifik dari aplikasi.

- **Patch**: Ubah pesan kesalahan menjadi lebih generik untuk menyembunyikan apakah username atau password yang salah:

```
13      if ($user && password_verify($password, $user['password'])) {
14          $_SESSION['user_id'] = $user['id'];
15          header('Location: notes.php');
16          exit();
17      } else {
18          echo "Invalid credentials.";
19      }
```

5. Weak Username Validation

- **File Terpengaruh**: register.php
- **Kerentanan**: Validasi username hanya memeriksa karakter alfanumerik tetapi tidak memeriksa panjang username yang masuk akal.
- **Baris yang Rentan**: **8**

```
 8      if (!preg_match("/^[a-zA-Z0-9]*$/", $username)) {
 9          echo "Invalid username.";
10          exit();
11      }
```

- **Dampak**: Pengguna bisa mendaftar dengan username yang sangat panjang atau username yang sangat pendek, yang bisa menyebabkan masalah performa atau membuat identitas pengguna sulit dikenali.
- **Patch**: Tambahkan validasi panjang username:

```
 8      if (!preg_match("/^[a-zA-Z0-9]{3,20}$/", $username)) { // Line 10
 9          echo "Invalid username. It must be between 3 and 20 characters.";
10          exit();
11      }
```

- Patches Approach

1. File: home.php (Patched)

```php
<?php
require 'db.php';
session_start();

if (!isset($_SESSION['user_id'])) {
    header('Location: login.php');
    exit();
}

$user_id = $_SESSION['user_id'];

if ($_SERVER['REQUEST_METHOD'] == 'POST' && isset($_POST['note'])) {
    // Sanitize note input
    $note = filter_input(INPUT_POST, 'note', FILTER_SANITIZE_STRING);

    $stmt = $pdo->prepare('INSERT INTO notes (user_id, note) VALUES (:user_id, :note)');
    $stmt->execute(['user_id' => $user_id, 'note' => $note]);
}

if (isset($_GET['delete'])) {
    // Validate and sanitize delete ID
    $note_id = filter_input(INPUT_GET, 'delete', FILTER_VALIDATE_INT);
    if ($note_id === false || $note_id === null) {
        exit('Invalid note ID');
    }

    $stmt = $pdo->prepare('DELETE FROM notes WHERE id = :id AND user_id = :user_id');
    $stmt->execute(['id' => $note_id, 'user_id' => $user_id]);
}

// Fetch user notes securely
$stmt = $pdo->prepare('SELECT * FROM notes WHERE user_id = :user_id ORDER BY created_at DESC');
$stmt->execute(['user_id' => $user_id]);
$notes = $stmt->fetchAll();
?>

<h2>Your Notes</h2>

<form method="post">
    <textarea name="note" required></textarea><br>
    <input type="submit" value="Add Note">
</form>

<ul>
    <?php foreach ($notes as $note): ?>
        <li>
            <!-- Sanitize output to prevent XSS -->
            <?php echo htmlspecialchars($note['note'], ENT_QUOTES, 'UTF-8'); ?>
            <a href="?delete=<?php echo (int) $note['id']; ?>">Delete</a>
        </li>
    <?php endforeach; ?>
</ul>
```

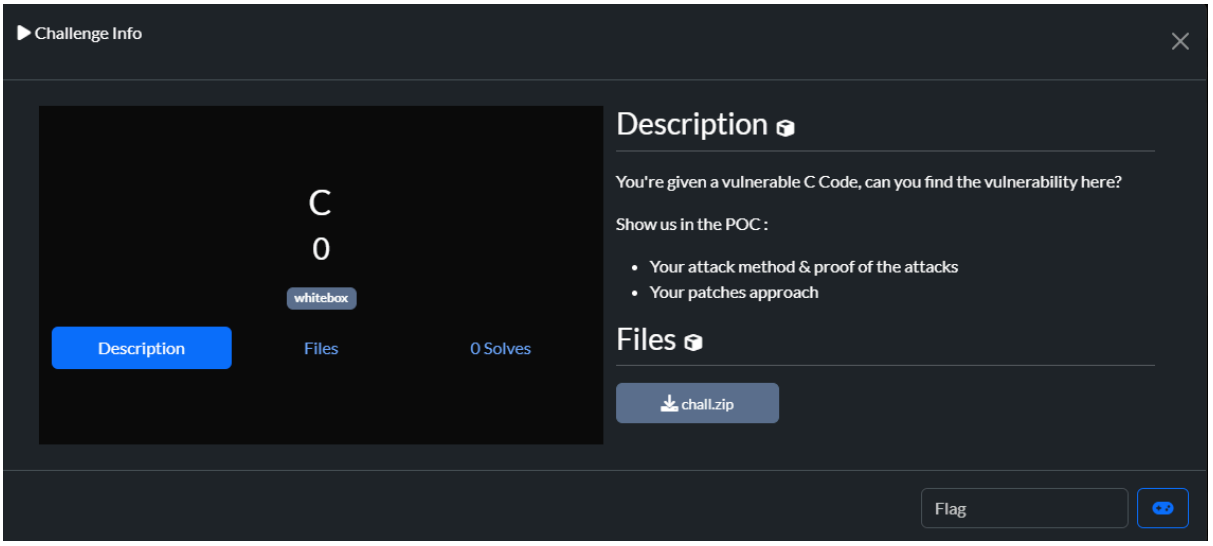
2. File: login.php (Patched)

```php
<?php
require 'db.php';
session_start();

// Inisialisasi variabel untuk mencatat percobaan login yang gagal
if (!isset($_SESSION['login_attempts'])) {
    $_SESSION['login_attempts'] = 0;
}

if (!isset($_SESSION['last_login_attempt'])) {
    $_SESSION['last_login_attempt'] = 0;
}

// Limit percobaan login
$max_attempts = 5;
// Durasi timeout setelah mencapai limit
$timeout_duration = 60;

if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    // Cek apakah user sedang dalam timeout
    if ($_SESSION['login_attempts'] >= $max_attempts && (time() - $_SESSION['last_login_attempt']) < $timeout_duration) {
        echo "Too many login attempts. Please try again in " . ($timeout_duration - (time() - $_SESSION['last_login_attempt'])) . " seconds.";
        exit();
    }

    $username = filter_input(INPUT_POST, 'username', FILTER_SANITIZE_STRING);
    $password = $_POST['password'];

    $stmt = $pdo->prepare('SELECT * FROM users WHERE username = :username');
    $stmt->execute(['username' => $username]);
    $user = $stmt->fetch();

    if ($user && password_verify($password, $user['password'])) {
        $_SESSION['user_id'] = $user['id'];
        // Reset login attempts setelah berhasil login
        $_SESSION['login_attempts'] = 0;
        $_SESSION['last_login_attempt'] = 0;
        header('Location: notes.php');
        exit();
    } else {
        // Tambahkan satu percobaan login yang gagal
        $_SESSION['login_attempts'] += 1;
        $_SESSION['last_login_attempt'] = time();

        if ($_SESSION['login_attempts'] >= $max_attempts) {
            echo "Too many login attempts. Please try again in " . $timeout_duration . " seconds.";
        } else {
            echo "Invalid credentials. You have " . ($max_attempts - $_SESSION['login_attempts']) . " attempts left.";
        }
    }
}
?>

<form method="post">
    Username: <input type="text" name="username" required><br>
    Password: <input type="password" name="password" required><br>
    <input type="submit" value="Login">
</form>

```

3. File: register.php (Patched)

```php
<?php
require 'db.php';

if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    $username = filter_input(INPUT_POST, 'username', FILTER_SANITIZE_STRING);
    $password = $_POST['password'];

    // Validate username length and allowed characters
    if (!preg_match("/^[a-zA-Z0-9]{3,20}$/", $username)) {
        echo "Invalid username. It must be between 3 and 20 characters.";
        exit();
    }

    // Hash the password
    $password_hash = password_hash($password, PASSWORD_BCRYPT);

    $stmt = $pdo->prepare('INSERT INTO users (username, password) VALUES (:username, :password)');
    try {
        $stmt->execute(['username' => $username, 'password' => $password_hash]);
        echo "User registered successfully!";
    } catch (PDOException $e) {
        echo "Error: " . $e->getMessage();
    }
}
?>

<form method="post">
    Username: <input type="text" name="username" required><br>
    Password: <input type="password" name="password" required><br>
    <input type="submit" value="Register">
</form>
```

C:



Crypton Commanders

- Attack Method & Proof of the Attacks

1. Penggunaan gets()

- **Kerentanan**: Fungsi gets() adalah fungsi yang rentan terhadap **buffer overflow** karena tidak membatasi jumlah karakter yang dapat dibaca. Jika pengguna memasukkan lebih banyak karakter daripada ukuran buffer, hal ini dapat menyebabkan overflow dan eksekusi kode berbahaya.
- **Baris yang Rentan:** **30 & 34**

```
29      printf("Enter title: ");
30      gets(new_book.title);
31      new_book.title[strcspn(new_book.title, "\n")] = 0; // Remove newline character
32
33      printf("Enter author: ");
34      gets(new_book.author);
35      new_book.author[strcspn(new_book.author, "\n")] = 0; // Remove newline character
```

- **Dampak**: Potensi buffer overflow dan eksekusi kode berbahaya jika masukan pengguna terlalu besar.
- **Solusi**: Ganti gets() dengan fgets() yang lebih aman karena membatasi jumlah karakter yang dibaca.
- **Patch:**

```
29      printf("Enter title: ");
30      fgets(new_book.title, TITLE_SIZE, stdin);
31      new_book.title[strcspn(new_book.title, "\n")] = 0; // Remove newline character
32
33      printf("Enter author: ");
34      fgets(new_book.author, AUTHOR_SIZE, stdin);
35      new_book.author[strcspn(new_book.author, "\n")] = 0; // Remove newline character
```

2. Kesalahan Variabel pada removeBook()

- **Kesalahan**: Variabel index didefinisikan dua kali dalam fungsi removeBook(), pertama kali untuk menerima input pengguna dan kemudian digunakan kembali sebagai penanda indeks array.
- **Baris yang Rentan:** **48**

```
45  void removeBook() {
46      int index;
47      printf("Enter book ID to remove: ");
48      scanf("%d", &index);
49      getchar(); // Clear newline character from input buffer
50
51      int index = -1;
52      for (int i = 0; i < book_count; i++) {
53          if (bookstore[i].id == index) {
54              index = i;
55              break;
56          }
57      }
```

- **Dampak**: Penggunaan variabel index dua kali menyebabkan kebingungan dalam logika program, yang menyebabkan masalah pada saat mencoba menghapus buku.
- **Solusi**: Gunakan dua variabel yang berbeda, misalnya input_id untuk ID buku dan index untuk indeks di dalam array.
- **Patch:**

```
45  void removeBook() {
46      int input_id;
47      printf("Enter book ID to remove: ");
48      scanf("%d", &input_id);
49      getchar(); // Clear newline character from input buffer
50
51      int index = -1; // Correctly define 'index' here
52      for (int i = 0; i < book_count; i++) {
53          if (bookstore[i].id == input_id) {
54              index = i;
55              break;
56          }
57      }
```

3. Out-of-bounds Access pada searchBook()

- **Kerentanan**: Pada fungsi searchBook(), tidak ada validasi untuk memastikan bahwa indeks yang dimasukkan pengguna berada dalam batas yang valid. Ini bisa menyebabkan **out-of-bounds access** saat mencari buku yang tidak ada.
- **Baris yang Rentan: 73 - 88**

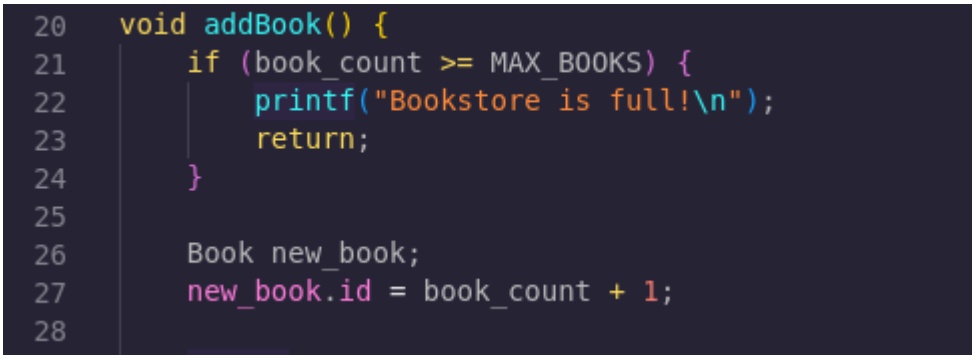
```c
void searchBook() {
    int index;
    printf("Enter book ID to search: ");
    scanf("%d", &index);
    getchar(); // Clear newline character from input buffer
    if (bookstore[index].id) {
        printf("Book found!\n");
        printf("ID: %d\n", bookstore[index].id);
        printf("Title: %s\n", bookstore[index].title);
        printf("Author: %s\n", bookstore[index].author);
        printf("Quantity: %d\n", bookstore[index].quantity);
        return;
    }else{
        printf("Book not found!\n");
    }
}
```

- **Dampak**:Jika pengguna memasukkan ID yang tidak valid atau di luar batas array, hal ini dapat menyebabkan crash atau perilaku yang tidak terduga.
- **Solusi**: Tambahkan validasi untuk memeriksa apakah indeks berada dalam batas array yang benar.
- **Patch:**

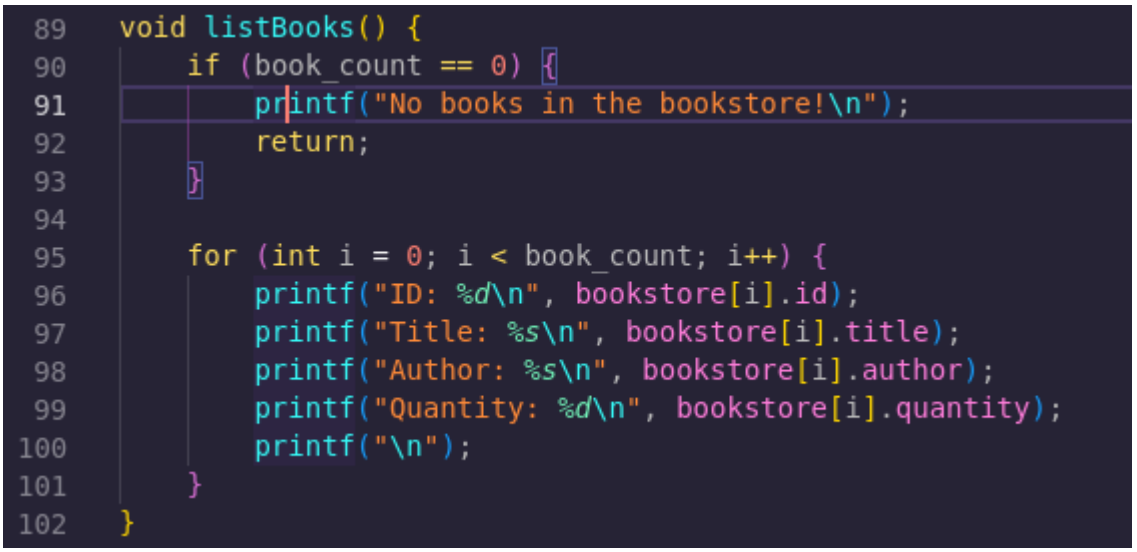
```c
void searchBook() {
    int index;
    printf("Enter book ID to search: ");
    scanf("%d", &index);
    getchar(); // Clear newline character from input buffer

    if (index < 0 || index >= book_count) {
        printf("Invalid book ID!\n");
        return;
    }

    if (bookstore[index].id) {
        printf("Book found!\n");
        printf("ID: %d\n", bookstore[index].id);
        printf("Title: %s\n", bookstore[index].title);
        printf("Author: %s\n", bookstore[index].author);
        printf("Quantity: %d\n", bookstore[index].quantity);
    } else {
        printf("Book not found!\n");
    }
}
```

4. Potensi Integer Overflow pada book_count (Global Variabel)

- **Kerentanan**: Pada saat menambahkan buku baru (addBook()), tidak ada pemeriksaan apakah variabel book_count dapat mengalami **integer overflow** setelah mencapai batas MAX_BOOKS. Ini dapat menyebabkan perilaku tak terduga.
- **Baris yang Rentan: 20 - 27 & 90**



```
20  void addBook() {
21      if (book_count >= MAX_BOOKS) {
22          printf("Bookstore is full!\n");
23          return;
24      }
25
26      Book new_book;
27      new_book.id = book_count + 1;
28
```



```
89  void listBooks() {
90      if (book_count == 0) {
91          printf("No books in the bookstore!\n");
92          return;
93      }
94
95      for (int i = 0; i < book_count; i++) {
96          printf("ID: %d\n", bookstore[i].id);
97          printf("Title: %s\n", bookstore[i].title);
98          printf("Author: %s\n", bookstore[i].author);
99          printf("Quantity: %d\n", bookstore[i].quantity);
100         printf("\n");
101     }
102 }
```

- **Dampak**: Jika buku ditambahkan melebihi batas, bisa menyebabkan data korup atau overwrite data lain.
- **Solusi**: Pastikan tidak ada overflow dengan menambahkan batasan saat increment.
- **Patch:**

```c
void addBook() {
    if (book_count >= MAX_BOOKS) {
        printf("Bookstore is full!\n");
        return;
    }

    if (book_count + 1 < 0) {  // Pastikan tidak terjadi overflow
        printf("Error: Integer overflow detected!\n");
        return;
    }

    Book new_book;
    new_book.id = book_count + 1;

```

```c
void listBooks() {
    if (book_count <= 0 || book_count > MAX_BOOKS) {  // Cegah nilai yang tidak valid
        printf("Error: Invalid book count!\n");
        return;
    }

    for (int i = 0; i < book_count; i++) {
        printf("ID: %d\n", bookstore[i].id);
        printf("Title: %s\n", bookstore[i].title);
        printf("Author: %s\n", bookstore[i].author);
        printf("Quantity: %d\n", bookstore[i].quantity);
        printf("\n");
    }
}
```

- Patches Approach

1. File:

chall.c (Patched)

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <ctype.h>

#define MAX_BOOKS 100
#define TITLE_SIZE 100
#define AUTHOR_SIZE 100

typedef struct {
    int id;
    char title[TITLE_SIZE];
    char author[AUTHOR_SIZE];
    int quantity;
} Book;

Book bookstore[MAX_BOOKS];
int book_count = 0;

void addBook() {
    if (book_count >= MAX_BOOKS) {
        printf("Bookstore is full!\n");
        return;
    }

    Book new_book;
    new_book.id = book_count + 1;

    printf("Enter title: ");
    fgets(new_book.title, TITLE_SIZE, stdin);
    new_book.title[strcspn(new_book.title, "\n")] = 0; // Remove newline character

    printf("Enter author: ");
    fgets(new_book.author, AUTHOR_SIZE, stdin);
    new_book.author[strcspn(new_book.author, "\n")] = 0; // Remove newline character

    printf("Enter quantity: ");
    if (scanf("%d", &new_book.quantity) != 1 || new_book.quantity < 0) {
        printf("Invalid quantity!\n");
        getchar(); // Clear invalid input
        return;
    }
    getchar(); // Clear newline character from input buffer

    bookstore[book_count++] = new_book;
    printf("Book added successfully!\n");
}

```

```c
void removeBook() {
    int input_id;
    printf("Enter book ID to remove: ");
    if (scanf("%d", &input_id) != 1 || input_id <= 0) {
        printf("Invalid book ID!\n");
        getchar(); // Clear any leftover input
        return;
    }
    getchar(); // Clear newline character from input buffer

    int index = -1;
    for (int i = 0; i < book_count; i++) {
        if (bookstore[i].id == input_id) {
            index = i;
            break;
        }
    }

    if (index == -1) {
        printf("Book not found!\n");
        return;
    }

    for (int i = index; i < book_count - 1; i++) {
        bookstore[i] = bookstore[i + 1];
    }

    book_count--;
    printf("Book removed successfully!\n");
}

void searchBook() {
    int index;
    printf("Enter book ID to search: ");
    if (scanf("%d", &index) != 1 || index <= 0 || index > book_count) {
        printf("Invalid book ID!\n");
        getchar(); // Clear any leftover input
        return;
    }
    getchar(); // Clear newline character from input buffer

    if (bookstore[index-1].id) {
        printf("Book found!\n");
        printf("ID: %d\n", bookstore[index-1].id);
        printf("Title: %s\n", bookstore[index-1].title);
        printf("Author: %s\n", bookstore[index-1].author);
        printf("Quantity: %d\n", bookstore[index-1].quantity);
    } else {
        printf("Book not found!\n");
    }
}

```

```c
void listBooks() {
    if (book_count == 0) {
        printf("No books in the bookstore!\n");
        return;
    }

    for (int i = 0; i < book_count; i++) {
        printf("ID: %d\n", bookstore[i].id);
        printf("Title: %s\n", bookstore[i].title);
        printf("Author: %s\n", bookstore[i].author);
        printf("Quantity: %d\n", bookstore[i].quantity);
        printf("\n");
    }
}

void showMenu() {
    printf("1. Add Book\n");
    printf("2. Remove Book\n");
    printf("3. Search Book\n");
    printf("4. List Books\n");
    printf("5. Exit\n");
    printf("Enter your choice: ");
}

int main() {
    int choice;

    while (1) {
        showMenu();
        if (scanf("%d", &choice) != 1) {
            printf("Invalid input! Please enter a number.\n");
            getchar(); // Clear invalid input
            continue;
        }
        getchar(); // Clear newline character from input buffer

        switch (choice)
    }
}
```