

WRITE-Ups InfoSec Institute
CTF#1 : Hacking fo n00bz

author : ade Marsekal
Team : iL7Team & Sulawesi IT Security
website : <http://il7team.com> & <http://sulawesi-ITSec.org>

Level 1

soal : may the source be with you !



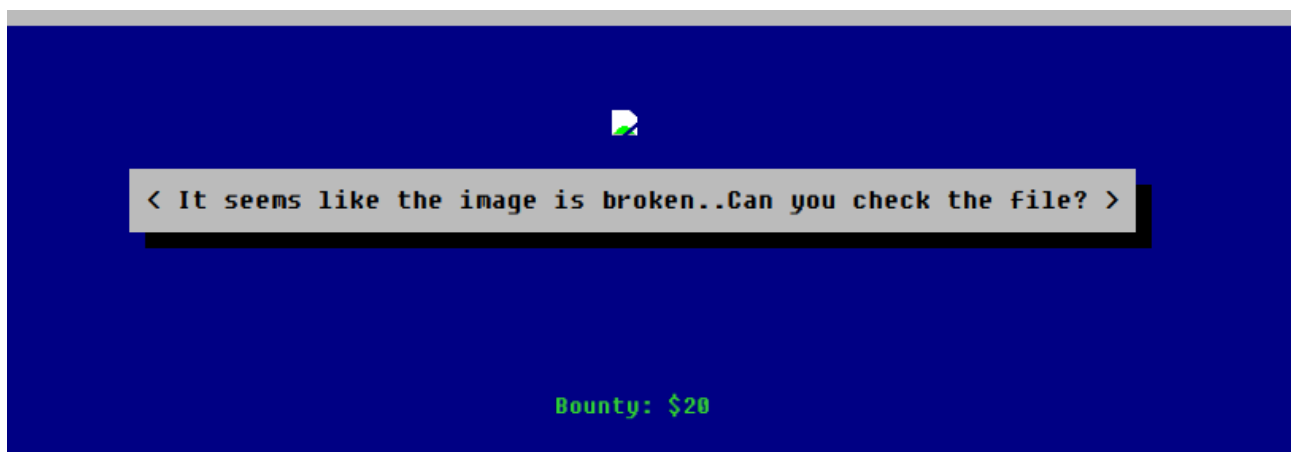
Ketika dibuka source nya, maka di baris pertama kita diberi flag nya

```
1 <!-- infosec flagis welcome -->
2 <!DOCTYPE html>
3 <html lang="en">
4   <head>
5     <meta charset="utf-8">
6     <meta name="viewport" content="width=device-width, initial-scale=1.0">
7     <meta name="description" content="a ctf for newbies">
8     <title>Infosec Institute n00bs CTF Labs</title>
9     <link href="css/bootstrap.css" rel="stylesheet">
10    <link href="css/custom.css" rel="stylesheet">
11  </head>
12
13  <body>
14    <div class="navbar navbar-inverse navbar-fixed-top">
15      <div class="navbar-inner">
16        <div class="container-fluid">
```

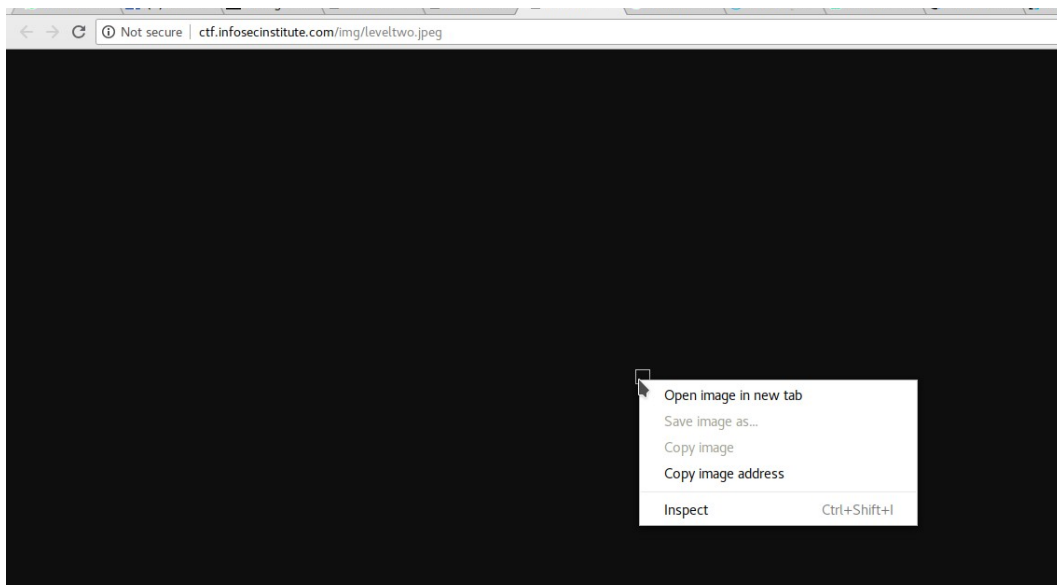
flag : infosec_flagis_welcome

Level 2

soal : kita diberikan file image yang rusak, dan kita disuruh untuk memeriksa file tersebut.



Dan file itu benar” rusak, . Maka untuk menyimpan image itu saya menggunakan wget untuk download image nya.



```
[marsekal@Adeputra]--[~/Downloads/instituteCTF]
→ $wget http://ctf.infosecinstitute.com/img/leveltwo.jpeg
--2018-08-07 14:52:45-- http://ctf.infosecinstitute.com/img/leveltwo.jpeg
Resolving ctf.infosecinstitute.com (ctf.infosecinstitute.com)... 52.27.151.10
Connecting to ctf.infosecinstitute.com (ctf.infosecinstitute.com)|52.27.151.10|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 45 [image/jpeg]
Saving to: 'leveltwo.jpeg'

leveltwo.jpeg      100%[=====>]          45  --.-KB/s   in 0s
2018-08-07 14:52:46 (2.44 MB/s) - 'leveltwo.jpeg' saved [45/45]

[marsekal@Adeputra]--[~/Downloads/instituteCTF]
→ $strings leveltwo.jpeg
aW5mb3NlY19mbGFnaXNfd2VhcmVqdXN0c3RhcnRpbmc=
```

Jika kita telusuri memakai command strings maka akan muncul encode jenis base64

```
[marsekal@Adeputra]--[~]
→ $python3
Python 3.6.6 (default, Jun 27 2018, 14:44:17)
[GCC 8.1.0] on linux
Type "help", "copyright", "credits" or "license" for more information
>>> import base64
>>> ciphertext = 'aW5mb3NlY19mbGFnaXNfd2VhcmVqdXN0c3RhcnRpbmc='
>>> import base64
>>> plaintext = (base64.b64decode(ciphertext))
>>> print (plaintext)
b'infosec_flagis_wearejuststarting'
```

disini saya menggunakan python3 untuk mengdecode code base64 nya.

Flag : infosec_flagis_wearejuststarting

Level 3

soal : kita diberi sebuah image barcode



segera scan online.

onlinebarcode reader.com

WELCOME

With this free online tool you can decode various barcode formats. We support the following ba

1D Point of sale: UPC-A, UPC-E, EAN-8, EAN-13, GS1 DataBar (a.k.a. RSS)

1D Industrial Symbols: Code 39, Code 93, Code 128, GS1-128, Codabar, ITF-14

2D Symbols: QR Code, Data Matrix, Aztec, PDF 417

Upload a file: No file chosen

Or enter a URL:

Max. file size for upload is 6 MB.

Max. height or width for image is 5000 pixel.

Supported file types: png, jpg, jpeg, gif, tiff, tif, pdf, bmp.

Maka code morse nya keluar :

[illegible]

jika kita decode lagi maka hasil nya :

TYPE MORSE CODE

Type any Morse code and it will be translated to alphanumeric code. Characters from Morse code separate by slash "/". The words separate by double slash "//".

Translate to Alphanumeric code

ALPHANUMERIC CODE

Translated Morse code to alphanumeric code.

infosecflagismorsing

flag : infosecflagismorsing

Level 4

soal : page manampilkan image boneka dan text http,...



HTTP means Hypertext Transfer Protocol

Bounty: \$40

X-Powered-By: PHP/5.5.9-1ubuntu4.6
Vary: Accept-Encoding
Content-Type: text/html
Content-Length: 2082
Connection: Keep-Alive
Content-Encoding: gzip
Set-Cookie: fusrodah=vasbfrp_syntvf_jrybirpbbxvrf

saya langsung segera cek header nya, dan menemukan code aneh di cookie.

Langsung decode, dan hasilnya

ROT13

Rumkin.com >> Web-Based Tools >> Ciphers and Codes

This is a JavaScript 1.2 implementation of the "rot13" encoder. If your browser doesn't support JavaScript 1.2, you really algorithm. A becomes N, B becomes O, C changes to P, etc. It is used to obscure spoilers and hints so that the person re the message instead of being able to accidentally read it.

Rot13 is both an encoder and decoder. You can enter plain text or encoded text, and you will be given the other one. Jus encoded or decoded.

I also made a [rotN encoder](#), which is also called a Caesarian Shift, so you can see what your sentence looks like if it is o many you want. Additionally, the [Vigenere](#) cipher is very similar.

fusrodah=vasbfrp_syntvf_jrybirpbbxvrf

This is your encoded or decoded text:

shfebqnu=infosec_flagis_welovecookies

flag : infosec_flagis_welovecookies

Level 5

soal : page menampilkan alert "hacker !" dan ini berulang ulang..

ctf.infosecinstitute.com/levelfive.php

ctf.infosecinstitute.com says

Hacker!!!

OK


dan saya langsung melihat source code nya

→ ↻ ⓘ Not secure | view-source:ctf.infosecinstitute.com/levelfive.php

```
<div class="hero-unit lvlfour">
  <script>
    for(;;){
      alert('Hacker!!!');
    }
  </script>
   <br /> <br />
</div>
```

ternyata terdapat sebuah image dengan nama aliens.jpg

jika di indentifikasi lebih dalam , maka bukan tidak lain lagi ini adalah stegonegraphi.
Saya mengambil alternatif disini, menggunakan web online.



The screenshot shows a web browser window with the address bar displaying "Secure | https://futureboy.us/stegano/decinput.html". The page title is "Steganographic Decoder". Below the title, a paragraph explains the form's purpose: "This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be as may also help you guess at what the payload is and its file type...". The form includes a section "Select a JPEG, WAV, or AU file to decode:" with a "Choose File" button and the filename "aliens.jpg". Below this is a "Password (may be blank):" text input field. There are three radio button options: "View raw output as MIME-type" (selected), "Guess the payload", and "Prompt to save (you must guess the file type yourself.)". The "View raw output as MIME-type" option has a text input field containing "text/plain". At the bottom of the form is a "Submit" button.

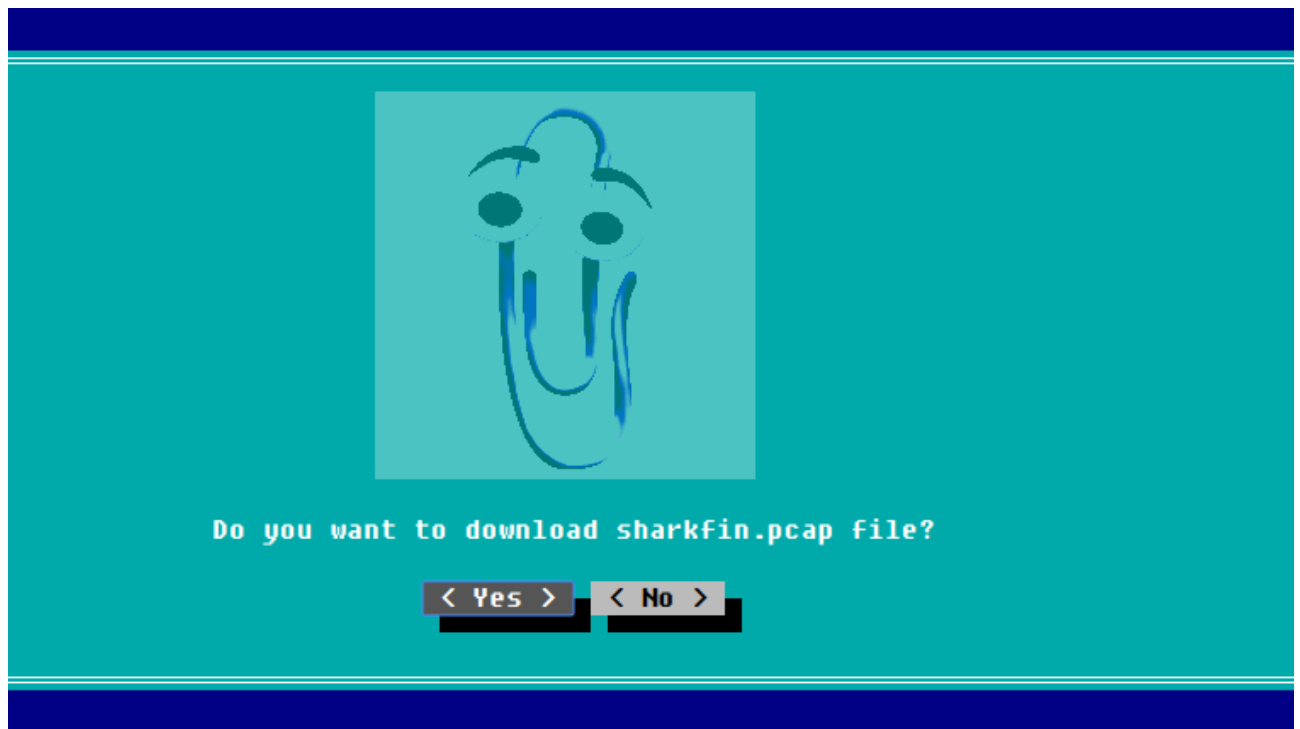
Maka akan keluar code biner :

```
0110100101101110011001100110111101110011011001010110001101011111011001100110110001
100001011001110110100101110011010111110111001101110100011001010110011101100001011
0110001101001011001010110111001110011
```

jika kita decode maka flag nya : infosec_flagis_stegaliens

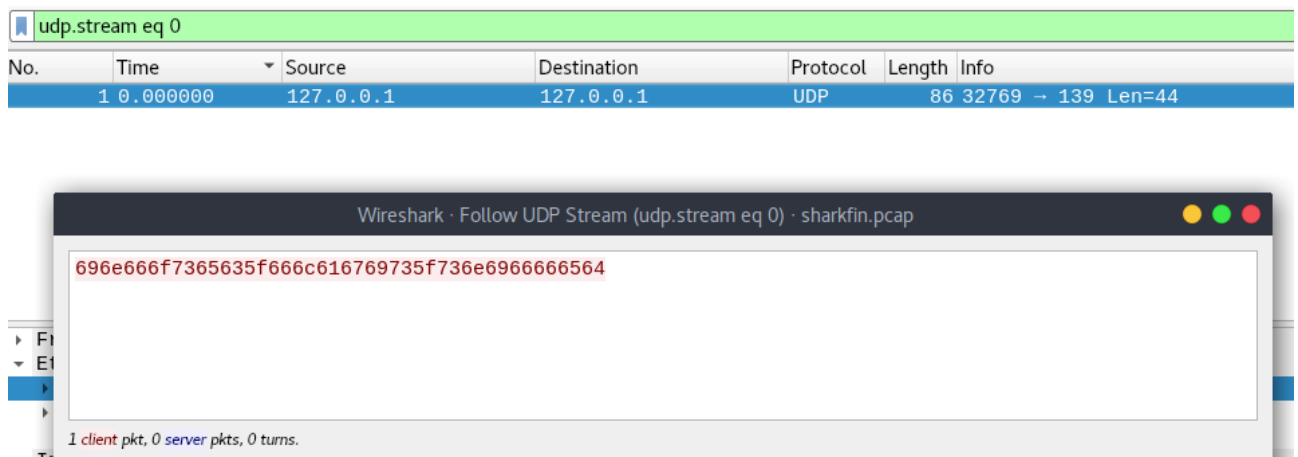
Level 6

soal : diberikan file .pcap



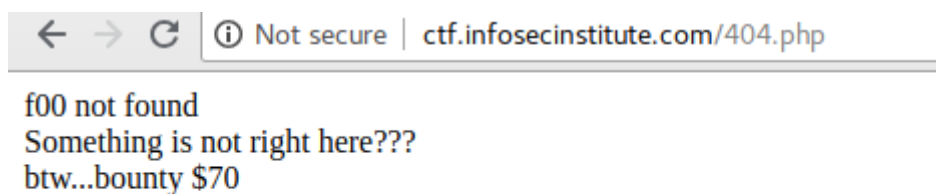
saya langsung buka nomor pertama dengan protocol UDP .

Klik kanan pilih follow > udp stream



ini adalah code hax, jika di decode maka :
flag : infosec_flagis_sniffed

Level 7



saya sudah
memeriksa
header, dll.

Tapi yang aneh nya, nama page kita kali ini 404.php . Yang mana sebelumnya kita selalu memasuki page yang berurutan seperti /levelfive.php atau /levelone.php .

Jika kita menuju /levelseven.php , maka akan menuju page blank.
Tapi mari kita lihat header nya.

```
levelseven.php moz-extension://3c738b44-aed2-4bfe-9cc0-51e14d6648fa - HTTP Header Live Main - Mozilla Firefox
pentest
GET: HTTP/1.1 404 Not Found
Date: Tue, 07 Aug 2018 09:52:13 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Type: text/html; charset=iso-8859-1
Content-Length: 298
Connection: Keep-Alive

http://ctf.infosecinstitute.com/levelseven.php
Host: ctf.infosecinstitute.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/1.0 200 aw5mb3NlY19mbGFnaXNfeW91Zm91bmRpdA==
Date: Tue, 07 Aug 2018 09:52:11 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.6
Content-Type: text/html
Content-Length: 0
Connection: Keep-Alive
```

Jika kita decode maka hasil nya :

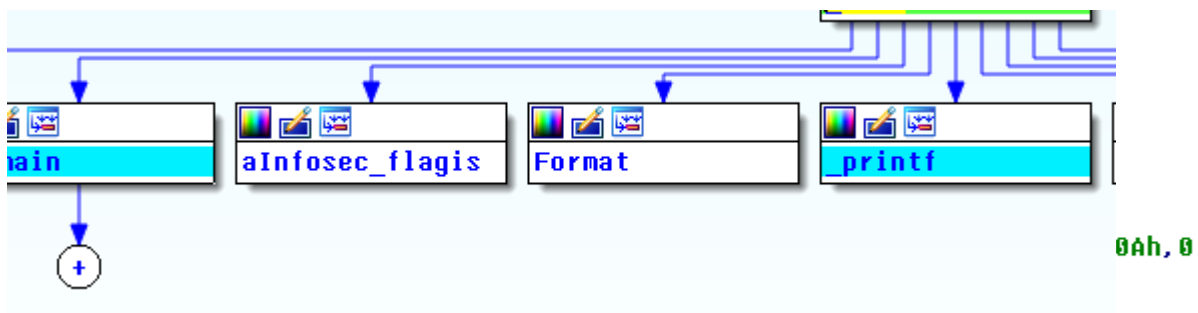
```
>>> import base64
>>> base64.b64decode('aw5mb3NlY19mbGFnaXNfeW91Zm91bmRpdA==')
b'infosec_flagis_youfoundit'
>>>
```

flag : 'infosec_flagis_youfoundit'

Level 8



jika kita buka di
ida dengan melihat graphic nya maka akan terlihat flag nya.



align 4

```

3000 _rdata          segment para public DATA use32
3000                assume cs:_rdata
3000                ;org 403000h
3000 aInfosec_flagis db 'infosec_flagis_0x1a',0 ; DATA XREF: _r
3014 ; char Format[]
3014 Format           db '#####'
3014                ; DATA XREF: _main
3014                ; _main+4Afo

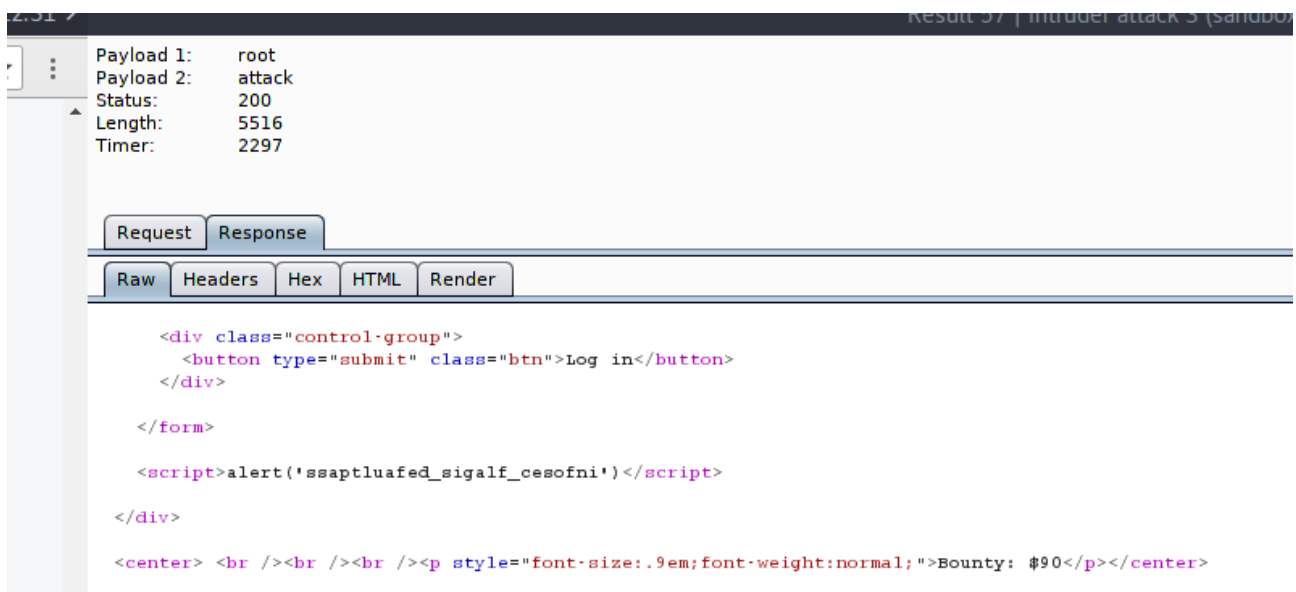
```

Flag : 'infosec_flagis_0x1a'

Level 9

saya sudah mencoba melihat header, cookie, dll.

Dan saya mencoba untuk brute force menggunakan burpsuite dengan list yang saya punya.



Terlihat status code nya 200. dan ada alert dengan notifikasi yang sangat aneh.



Alert : ssaptluafed_sigalf_cesofni

saya kira ini rot13 dan substitution.. ternyata ini huruf nya terbalik
untuk reverse nya saya menggunakan python


```

[marsekal@Adeputra]~$ python3
Python 3.6.6 (default, Jun 27 2018, 14:44:17)
[GCC 8.1.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> aneh = 'ssaptluafeed_sigalf_cesofni'
>>> aneh[::-1]
'infosec_flagis_defaultpass'
>>>

```

flag : infosec_flagis_defaultpass

Level 11



```

$strings php-logo-virus.jpg
JFIF
Exif
infosec_flagis_aHR0cDovL3d3dy5yb2xsZXJza2kuY28udWsvaW1hZ2VzYi9wb3dlcnNsaWRlX2xvZ29fbGFyZ2UuZ2lm
Photoshop ICC profile
XICC_PROFILE
HLino

```

infosec_flagis_aHR0cDovL3d3dy5yb2xsZXJza2kuY28udWsvaW1hZ2VzYi9wb3dlcnNsaWRlX2xvZ29fbGFyZ2UuZ2lm

```

Python 3.6.6 (default, Jun 27 2018, 14:44:17)
[GCC 8.1.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import base64
>>> base64.b64decode('aHR0cDovL3d3dy5yb2xsZXJza2kuY28udWsvaW1hZ2VzYi9wb3dlcnNsaWRlX2xvZ29fbGFyZ2UuZ2lm')
'http://www.rollerski.co.uk/imagesb/powerslide_logo_large.gif'

```

ini ada jenis encode base64.

http://www.rollerski.co.uk/imagesb/powerslide_logo_large.gif

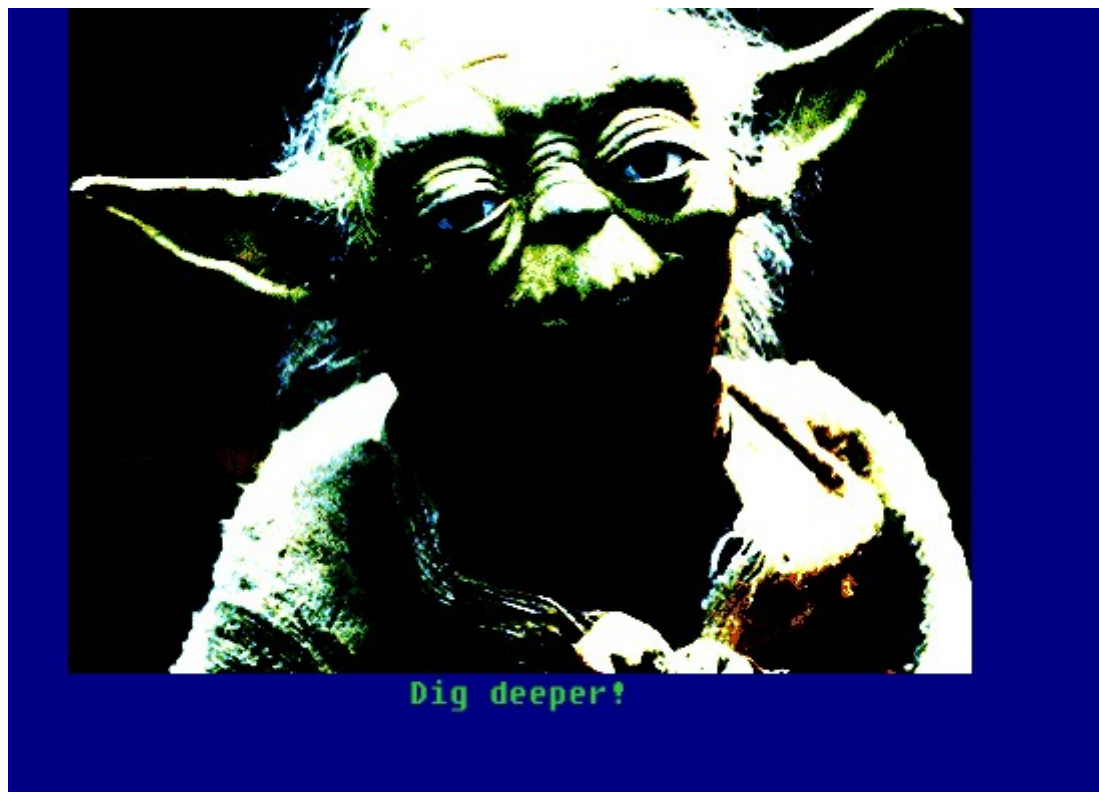
The logo for Powerslide, featuring the word "POWERSLIDE" in a bold, italicized, blue sans-serif font. Below the text is a stylized blue graphic consisting of a series of horizontal lines that curve upwards and to the right, resembling a checkered flag or a speed line.

jika kita identifikasi maka tidak ada info lainnya, tapi ini adalah flag nya

flag : infosec_flagis_POWERSLIDE

Level 12

soal : ada image yoda.png dan text dig deeper.



Pergi ke source code dan lihat di file design.css, terdapat kode hex yang diletakkan di class .thisloveis.

```
< > ↻ ⓘ Not secure | ctf.infosecinstitute.com/css/design.css

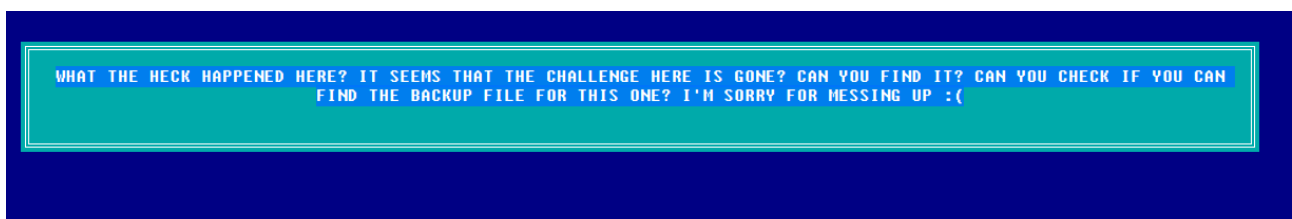
.thisloveis{
    color: #696e666f7365635f666c616769735f686579696d6e6f7461636f6c6f72;
}
```

Jika kita decode maka flag nya muncul

```
[marsekal@Adeputra]-(~/Downloads/instituteCTF)
→ $python
Python 2.7.15 (default, Jul 28 2018, 11:29:29)
[GCC 8.1.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> '696e666f7365635f666c616769735f686579696d6e6f7461636f6c6f72'.decode('hex')
'infosec_flagis_heyimnotacolor'
>>>
```

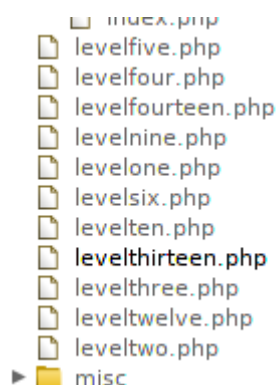
Level 13

SS soal : APA YANG TERJADI DI SINI? ITU TAMPAKNYA BAHWA TANTANGAN DI SINI ADALAH PERGI? BISA ANDA MENEMUKANNYA? BISA ANDA PERIKSA JIKA ANDA DAPAT Mencari FILE BACKUP UNTUK SATU INI? AKU MAAF UNTUK MESSING UP :(



clue nya disuruh mencari file backup,.

Saya mulai spidering menggunakan burpsuite, dan tidak menemukan apapun.



Saya mulai mencari nya dengan menambahkan extensi nya.

/levelthirteen-old.php . /13backup.php . Dll.

Terakhir saya mendapatkan pencerahan yaitu /levelthirteen.php.old

jika kita identifikasi maka ini adalah file berbentuk ascii.

Dan saya menemukan yang menarik, yaitu

```
<h1>
What the heck happened here? It seems that the challenge here is gone?
Can you find it? Can you check if you can find the backup file for this one?
I'm sorry for messing up :(

</h1>
<?php

/*  <br /> <br />

<p>Do you want to download this mysterious file?</p>

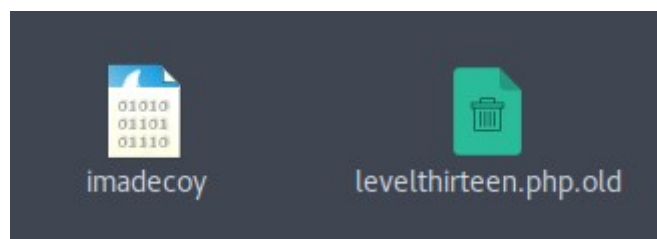
<a href="misc/imadecoy">
  <button class="btn">Yes</button>
</a>

<a href="index.php">
  <button class="btn">No</button>
</a>
*/

?>
```

ada file image bernama clippy1.jpg dan ada sebuah options dimana ketika memilih yes maka pergi ke /misc/imadecoy .. jika tidak maka ke /index.php

jadi mari kita telusuri



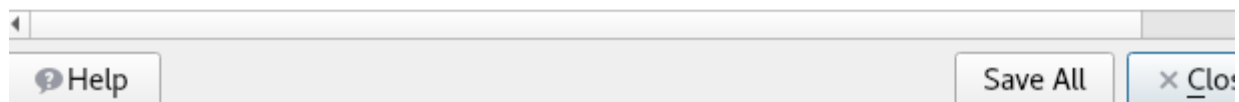
mari kita buka dengan wireshark.

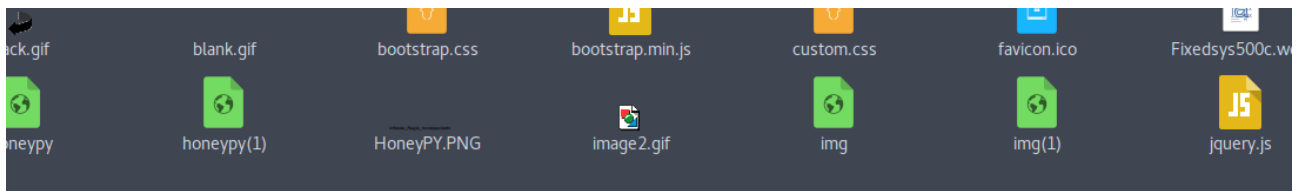
Ada banyak protocol http yang tampil, maka saya langsung filter .

Protocol	Length	Info
HTTP	434	GET /honeypy HTTP/1.1
HTTP	435	GET /honeypy/ HTTP/1.1
HTTP	432	GET /honeypy/css/bootstrap.css HTTP/1.1
HTTP	429	GET /honeypy/css/custom.css HTTP/1.1
HTTP	412	GET /honeypy/js/jquery.js HTTP/1.1
HTTP	419	GET /honeypy/js/bootstrap.min.js HTTP/1.1
HTTP	444	GET /honeypy/css/fonts/Fixedsys500c.woff HTTP/1.1
HTTP	367	GET /favicon.ico HTTP/1.1
HTTP	438	GET /honeypy/img HTTP/1.1
HTTP	439	GET /honeypy/img/ HTTP/1.1
HTTP	428	GET /icons/blank.gif HTTP/1.1
HTTP	427	GET /icons/back.gif HTTP/1.1
HTTP	429	GET /icons/image2.gif HTTP/1.1
HTTP	490	GET /honeypy/img/HoneyPY.PNG HTTP/1.1
HTTP	609	GET /honeypy/img/HoneyPY.PNG HTTP/1.1
HTTP	609	GET /honeypy/img/HoneyPY.PNG HTTP/1.1
HTTP	154	OPTIONS * HTTP/1.0
HTTP	154	OPTIONS * HTTP/1.0

Mari kita save semua file misterius ini .

Packet	Hostname	Content Type	Size	Filename
486	localhost	text/html	308 bytes	honeypy
489	localhost	text/html	1,703 bytes	honeypy
507	localhost	text/css	30 bytes	custom.css
509	localhost	application/javascript	29 kB	bootstrap.min.js
513	localhost	text/css	109 kB	bootstrap.css
516	localhost	application/javascript	93 kB	jquery.js
520	localhost		13 kB	Fixedsys500c.woff
524	localhost	text/html	284 bytes	favicon.ico
599	localhost	text/html	312 bytes	img
614	localhost	text/html	1,397 bytes	img
621	localhost	image/gif	216 bytes	back.gif
623	localhost	image/gif	148 bytes	blank.gif
624	localhost	image/gif	309 bytes	image2.gif
633	localhost	image/png	1,595 bytes	HoneyPY.PNG





Jika kita buka file image HoneyPY.PNG ., maka kita akan menemukan flag nya

flag : infosec_flagis_morepackets

Level 14

SS soal :



jika kita klik
yes maka kita
diarahkan ke
file
phpmyadmin.

```
-- phpMyAdmin SQL Dump
-- version 3.4.10.1deb1
-- http://www.phpmyadmin.net
--
-- Host: localhost
-- Generation Time: Dec 14, 2014 at 02:06 PM
-- Server version: 5.5.34
-- PHP Version: 5.3.10-1ubuntu3.9

SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;

--
-- Database: `level14`
--
```

Tapi ada sesuatu yang aneh disini.

```
INSERT INTO `friends` (`id`, `name`, `address`, `status`) VALUES
(102, 'Sasha Grey', 'Vatican City', 'Active'),
(101, 'Andres Bonifacio', 'Tondo, Manila', 'Active'),
(103, 'lol', 'what the???' , 'Inactive'),
(104, '\\u0069\\u006e\\u0066\\u006f\\u0073\\u0065\\u0063\\u005f\\u0066\\u006c\\u0061\\u0067\\u0069\\u0073\\u005f\\u0077\\u0068\\u0061\\u0074\\u0073\\u006f\\u0072\\u0063\\u0065\\u0072\\u0079\\u0069\\u0073\\u0074\\u0068\\u0069\\u0073',
'annoying', '0x0a')
```

setelah cukup lama untuk browsing mengenai code diatas, maka saya mendapatkan web yang menyediakan decode jenis encode diatas. <http://ddecode.com/hexdecoder/>

Decode

Original code:

```
\\u0069\\u006e\\u0066\\u006f\\u0073\\u0065\\u0063\\u005f\\u0066\\u006c\\u0061\\u0067\\u0069\\u0073\\u005f\\u0077\\u0068\\u0061\\u0074\\u0073\\u006f\\u0072\\u0063\\u0065\\u0072\\u0079\\u0069\\u0073\\u0074\\u0068\\u0069\\u0073
```

Decoded results:

```
infosec_flagis_whatsorceryisthis
```

flag : infosec_flagis_whatsorceryisthis