

## ***LAPORAN CTF TENESYS***

# **FIT COMPETITION UKSW**

> Dalam event ini kami tidak berhasil menyelesaikan 1 buah tantangan misi yang berkategori web yaitu “Give me your information!” sungguh sangat disayangkan memang, tapi apa boleh buat karena kami masih butuh banyak pengalaman dan masih butuh banyak belajar, berikut adalah hasil writeups yang telah kami susun,

## • Misi 1 (Bonus) Kategori *Example*

Dalam misi ini kami mendapatkan sebuah clue berupa string md5 `03236793d9db0c203656e5c713e2c9d4`. Karena setiap decryptor online berbeda database maka kami mencoba untuk mencari secara bulk dengan pergi ke alamat <http://md5cracker.org/>

**Cracking results:**  
Below you see the cracking results. The engine needs a few seconds to crawl the results from all databases.  
*Don't close the page!*

**03236793d9db0c203656e5c713e2c9d4**


✓ <a href="#">md5cracker.org</a> result: <b>FIT2016{w3lc0me_t0_FIT2016}</b>	✗ <a href="#">TMT0[dot]ORG</a> error: not found	✗ <a href="#">md5.net</a> error: not found
	✗ <a href="#">md5online.net</a> error: not found	✗ <a href="#">MD5.My-Addr.com</a> error: not found
✓ <a href="#">md5decryption.com</a> result: <b>FIT2016{w3lc0me_t0_FIT2016}</b>	✗ <a href="#">md5crack</a> error: timeout	✗ <a href="#">AuthSecu</a> error: not found
	✗ <a href="#">NetMD5Crack</a> error: not found	✗ <a href="#">md5pass</a> error: not found
✗ <a href="#">i337.NET</a> error: timeout		

**Cracked md5 hashes:**  
`03236793d9db0c203656e5c713e2c9d4:FIT2016{w3lc0me_t0_FIT2016}`

Bingo ! Terdapatlah sebuah flag yang kami temukan yaitu `FIT2016{w3lc0me_t0_FIT2016}` Terima kasih ☺

## • Misi 2 (Sudah Tua) Kategori *Cryptography*

Dalam misi ini kami mendapatkan sebuah link clue menuju dropbox, setelah dibuka munculah sebuah string seperti berikut :

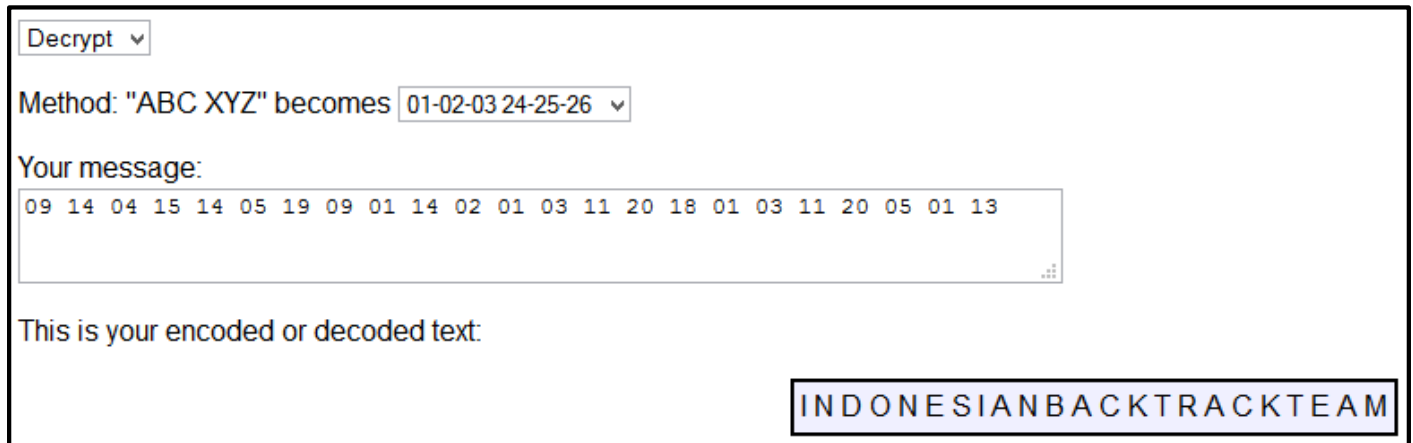
 Crypto1.txt

Vm0wd2QyVzkZOVWhTYmxKWF1URndUMVpzWkc5V2JGbdNXa2M1V0ZadGVibFdNa1ZyVmxVeFYySkVUbGRpVbVaSVZtMXplR115U2tWVWJHaG9UV3N3ZUZadE1UU1RNbEpJm10V1VtSkdXbkJWY1  
hoVlpVWmFjbHBjY0d4U2JHdzFWa2QwVWZsV1NuUmhSemxWVm0xb1JGw1dXbHBsUm1SMFpFW1NUbFpVmtwV2JHUXdWakZhZEZ0c1pHcFNWR3hoV1d4b1UxUkdXWGhYY1hSWFRWaENSbFpYZUZk  
VWJGcFlaSHBDVjJFeVRyaFZha1poVTBaT2MxZHNhR2xoTUhCWVYxZDBZV1F4V1hoVmJHU112bFZhV0Zsc1pGImxWbGw1W1VWT1YwMXJWak5aTUZwVFZqRmFWMk5HVGI1GU1JWcEVWbGQ0UTFeVk  
1VVk5SREE5

String tersebut merupakan encoding Base64 yang telah di encode sebanyak 10 kali, lalu kami coba pula decode sebanyak 10 kali maka akan didapat sebuah flag yaitu `FIT2016{0Ld_cRypto}` Terima kasih ☺

- **Misi 3 (Kids Letter) Kategori *Cryptography***

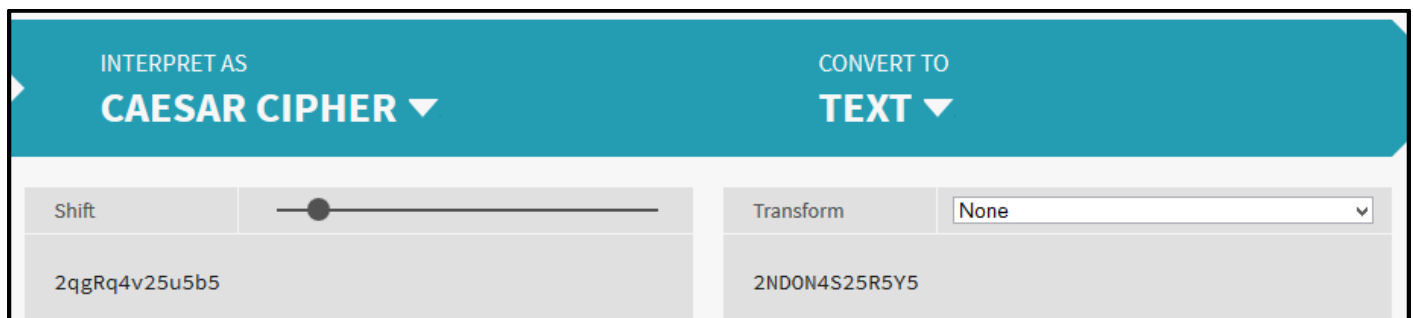
Dalam misi ini kami mendapatkan sebuah clue berupa angka desimal yaitu *09 14 04 15 14 05 19 09 01 14 02 01 03 11 20 18 01 03 11 20 05 01 13* kami menduga itu adalah sebuah urutan huruf alfabet A-Z dan kami coba decode dengan menuju alamat <http://rumkin.com/tools/cipher/numbers.php>



Bingo ! Terdapatlah sebuah flag yang kami temukan yaitu *INDONESIANBACKTRACKTEAM* dan kami submit jawaban tersebut di web score dengan format *FIT2016{indonesianbacktrackteam}* Terima kasih ☺

- **Misi 4 (Decode me!) Kategori *Cryptography***

Dalam misi ini kami mendapatkan sebuah clue berupa string yaitu *2qgRq4v25u5b5* kami mencoba untuk mengubah string tersebut dalam bentuk teks menggunakan chaesar chiper decoder online yang beralamat <http://cryptii.com/caesar/text> seperti gambar berikut :



Terlihat pada geseran ke-4 menghasilkan teks *2NDON4S25R5Y5*, terlihat familiar bukan ? Tidak perlu berfikir panjang karena hanya mengganti angka-angka yang ada pada strings tersebut dengan angka seperti *1NDON3S14R4Y4* dan flag pun kami submit dengan format *FIT2016{1NDON3S14R4Y4}* Terima kasih ☺

- **Misi 5 (Temukan Aku) Kategori Misc**

Dalam misi ini kami mendapatkan sebuah link clue menuju dropbox, setelah dibuka terdapatlah sebuah file yang berekstensi .zip apabila di ekstrak file telah corrupt, maka kami pikir untuk mencoba mengganti ekstensi file tersebut menjadi ekstensi gambar yaitu .png maka terlihat gambar seperti berikut :



Hanya butuh ketelitian saja, apabila pada bagian tengah gambar tersebut kita perbesar maka akan tampak sebuah flag seperti gambar berikut :



Bingo ! Terlihat sebuah flag yang kami temukan yaitu FIT2016{FitUksw} Terima kasih ☺

- **Misi 6 (Fake Account) Kategori Misc**

Dalam misi ini kami diminta untuk mencari sebuah fake account dari FIT KOMPETISI UKSW dan menemukan flagnya, maka langkah awal kami adalah berselancar di google namun tidak menemukan jawaban sampai akhirnya mencoba mencari sebuah nama FIT UKSW pada facebook dan kami temukan sebuah akun seperti gambar berikut :



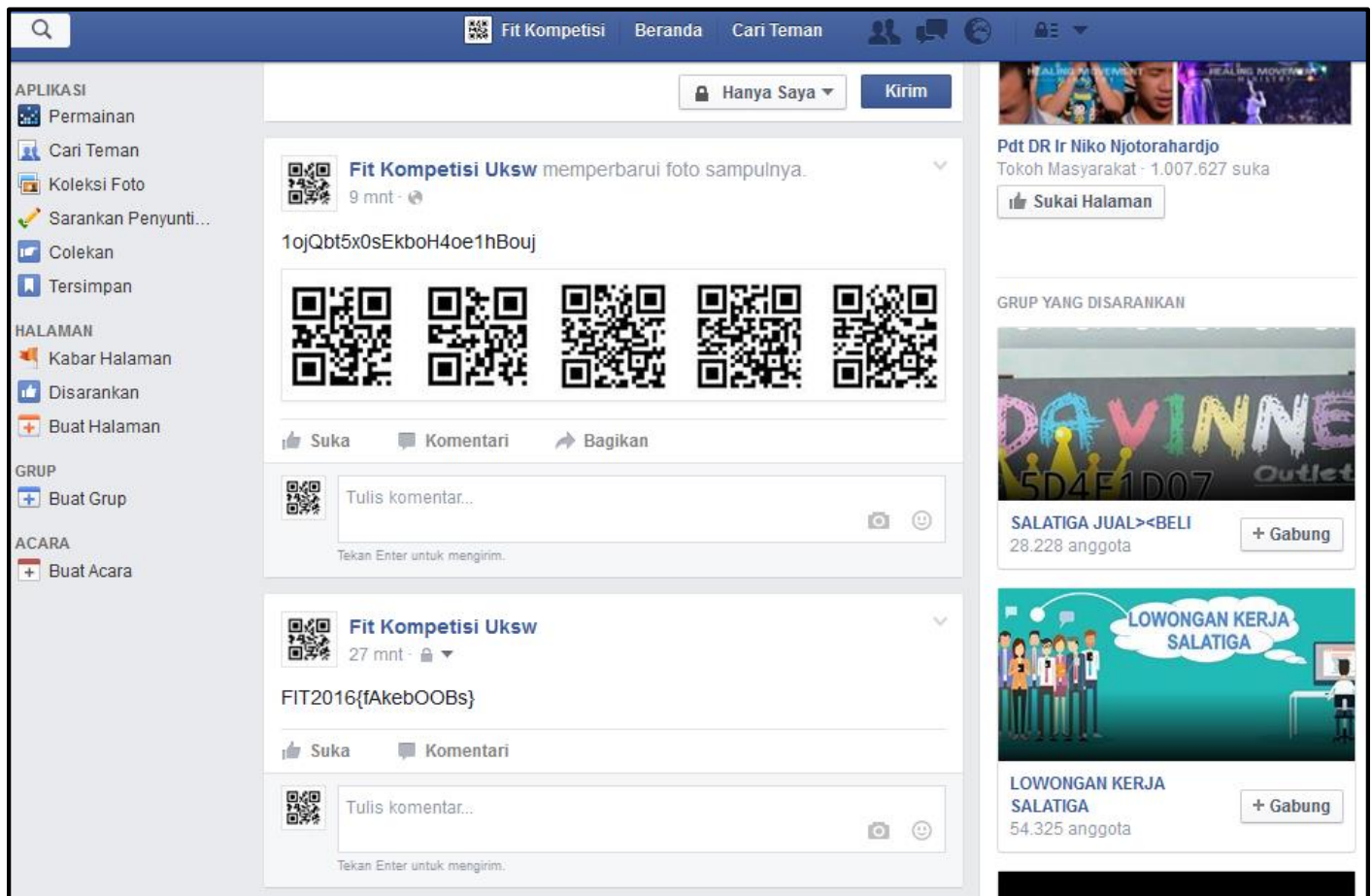
Kami mencoba untuk mencari tahu sesuatu dalam akun tersebut dan menemukan sebuah pemberitahuan status bahwa akun tersebut mengganti gambar dindingnya,



Terdapat sebuah string pada status tersebut apabila di decode menggunakan *Chaesar Chiper* maka didapatkan sebuah teks berupa *1niPas5w0rDjanG4nd1gAnti* kami pikir ini adalah sebuah password dari akun tersebut, maka kami mencoba menelusuri pada bagian *Tentang > Tinjauan* terlihatlah sebuah email seperti gambar berikut :



Lalu kami coba untuk login dengan email dan password yang sudah didapat,



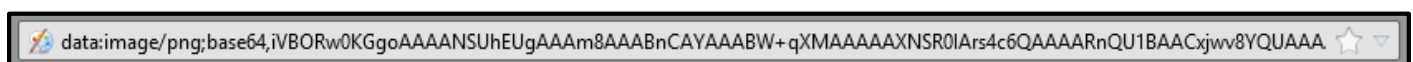
Bingo ! Terlihat sebuah flag yang kami temukan yaitu `FIT2016{fAkebOOBs}` Terima kasih ☺

## • Misi 7 (Lols~) Kategori *Cryptography*

Dalam misi ini kami mendapatkan sebuah link clue menuju dropbox, setelah dibuka munculah sebuah string seperti berikut :

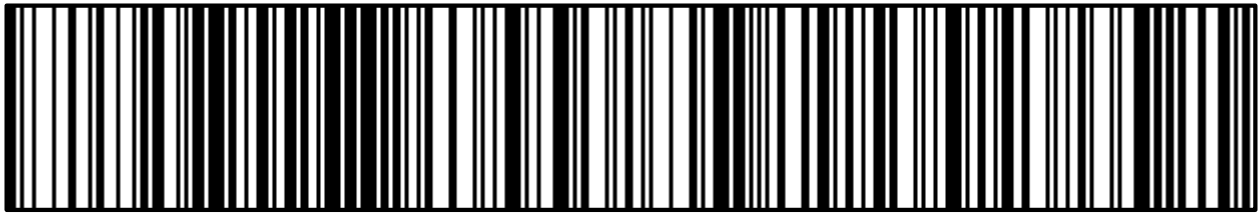


Terlihat sebuah encoding base64 berjenis gambar pada file tersebut, lalu kami coba decode menggunakan address bar di browser kami dengan mengetikkan perintah `data:image/png;base64,`





Setelah itu kami enter maka akan terlihat sebuah gambar seperti berikut :



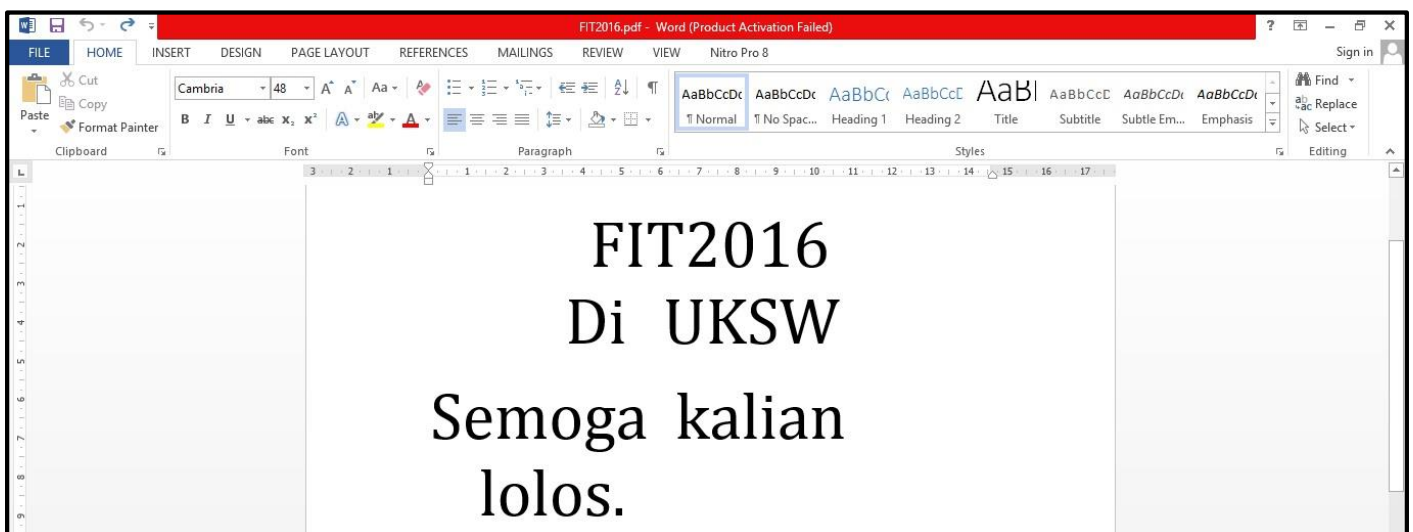
Munculah sebuah gambar berupa barcode, lalu kami coba barcode decoder gambar tersebut menggunakan alamat <https://zxing.org/w/decode.aspx> maka akan terlihat seperti berikut :

Decode Succeeded	
Raw text	<code>FIT2016{antonlim_64nt3ng}</code>
Raw bytes	<code>68 26 29 34 63 14 10 64 5b 41 4e 54 4f 4e 4c 49 4d 3f 16 14 4e 54 13 4e 47 5d 1e 6a</code>
Barcode format	CODE_128
Parsed Result Type	TEXT
Parsed Result	<code>FIT2016{antonlim_64nt3ng}</code>

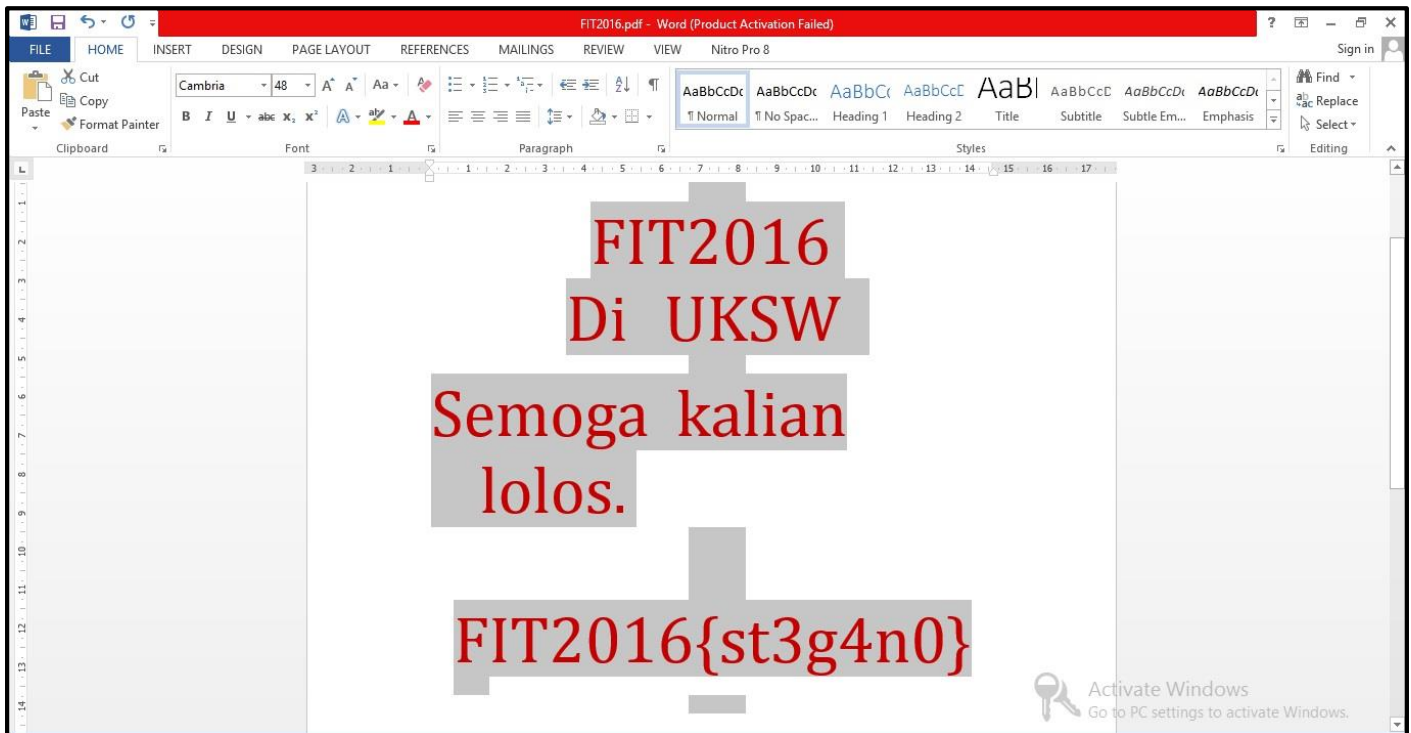
Bingo ! Terlihat sebuah flag yang kami temukan yaitu `FIT2016{antonlim_6ant3ng}` Terima kasih ☺

- **Misi 8 (Selamat Datang) Kategori Stegano**

Dalam misi ini kami mendapatkan sebuah link clue menuju dropbox, setelah dibuka terdapatlah sebuah file pdf yang kami buka menggunakan aplikasi *Ms. Word* seperti berikut :



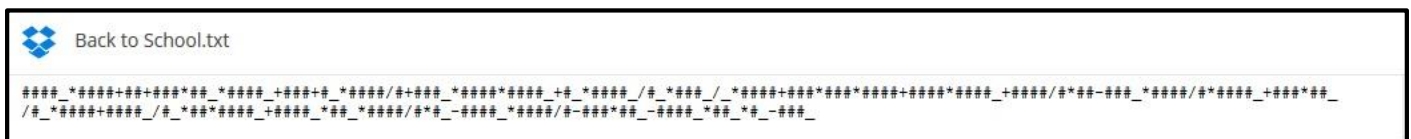
Tidak membutuhkan waktu lama untuk berfikir mengenai flag, kami mencoba untuk block semua kata lalu mengubah warna teks menjadi warna merah maka akan terlihat seperti berikut :



Bingo ! Terlihat sebuah flag yang kami temukan yaitu `FIT2016{st3g4n0}` Terima kasih ☺

- **Misi 9 (Back to School) Kategori *Misc***

Dalam misi ini kami mendapatkan sebuah link clue menuju dropbox, setelah dibuka terdapatlah sebuah strings seperti berikut :



Kami beranggapan bahwa bentuk `#` (*Hastag*) dan `_` (*Underscore*) merupakan dua buah variabel lalu kami membuat sebuah script menggunakan bahasa python seperti berikut :

```
1 for a in range(1,10):
2     for b in range(1,10):
3         c = (a+a+a+a+b)*(a+a+a+a)+(a+a)+(a+a+a)*(a+a+b)*(a+a+a+a+b)+(a+a+a)+(a+b)*(a+a+a+a)/(a)+(a+a
4             +a+b)*(a+a+a+a)*(a+a+a+a+b)+(a+b)*(a+a+a+a+b)/(a+b)*(a+a+a+b)/(b)*(a+a+a+a)+(a+a+a)*(a+a
5             +a)*(a+a+a+a)+(a+a+a+a)*(a+a+a+a+b)+(a+a+a+a)/(a)*(a+a)-(a+a+a+b)*(a+a+a+a)/(a)*(a+a+a+a
6             +b)+(a+a+a)*(a+a+b)/(a+b)*(a+a+a+a)+(a+a+a+a+b)/(a+b)*(a+a)*(a+a+a+a+b)+(a+a+a+a+b)*(a+a
7             +b)*(a+a+a+a)/(a)*(a+b)-(a+a+a+a+b)*(a+a+a+a)/(a)-(a+a+a)*(a+a+b)-(a+a+a+a+b)*(a+a+b)*(a
8             +b)-(a+a+a+b)
9         print (c)
```



Setelah kami running script tersebut, maka akan terlihat output berupa list seperti gambar berikut :

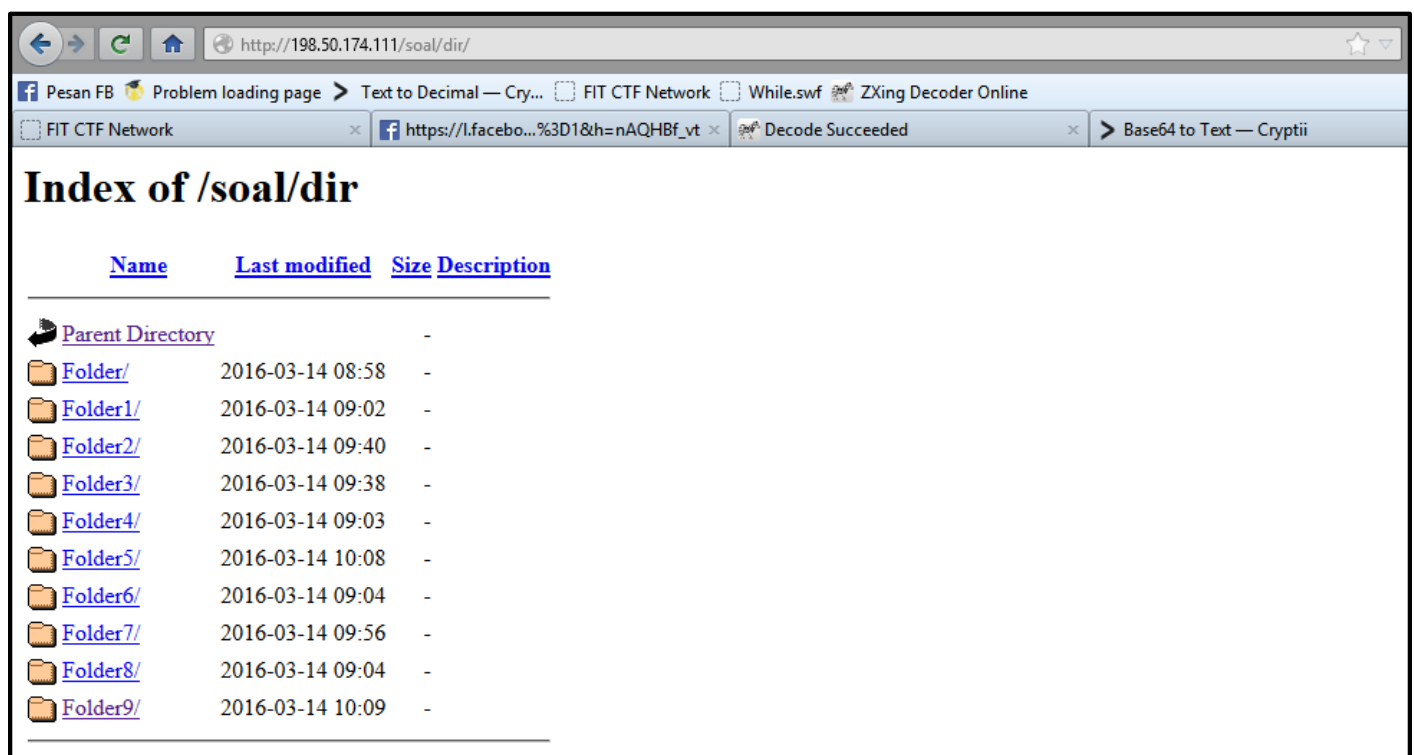
```

C:\Windows\system32\cmd.exe
D:\aaaa>back.py
322.0
456.0
692.5
1036.0
1501.6
2106.285714285714
2867.607142857143
3803.333333333333
4931.333333333333
2016.0
2298.0
2856.0
3608.0
4551.085714285715
5696.0
7057.523809523809
8652.0
10496.4848484848
6167.5
6480.0
7434.0
8717.714285714286
10281.45
12120.0
14241.142857142855
16657.636363636364
```

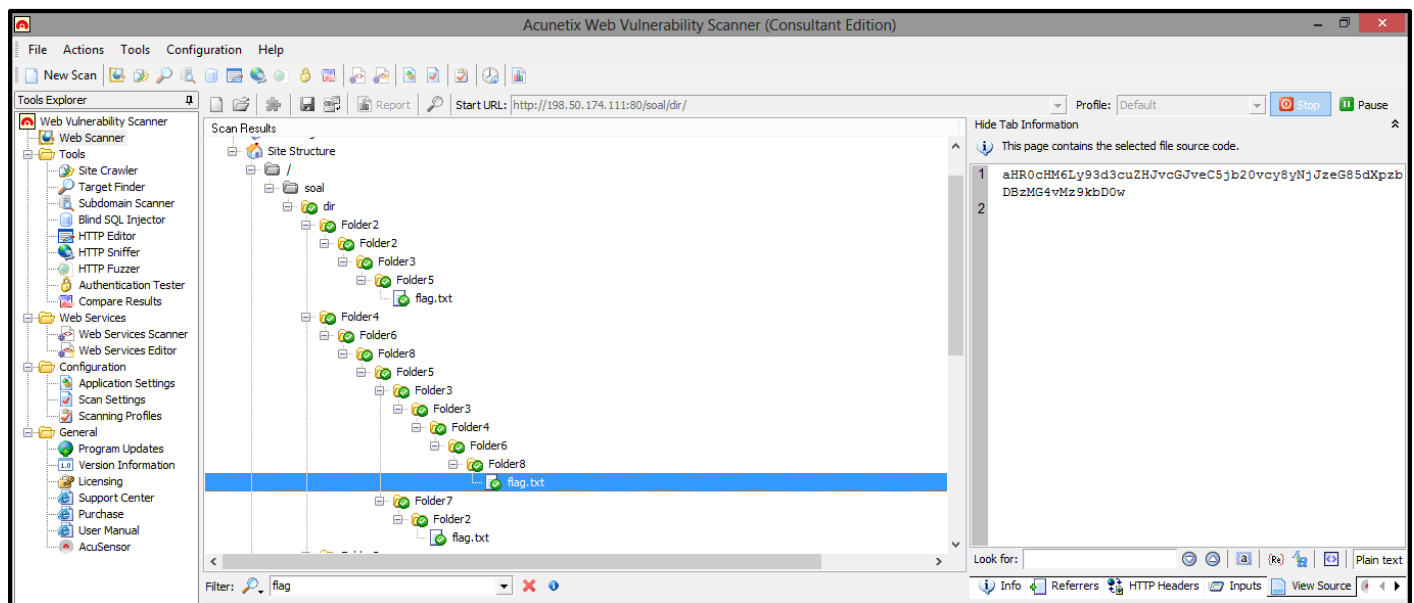
Dari hasil list tersebut, kami memiliki kecurigaan terhadap angka 2016 dan kami pun mencoba untuk mensubmitnya dalam bentuk MD5 yaitu 95192c98732387165bf8e396c0f2dad2 alhasil bingo ! Ternyata benar dugaan kami bahwa flagnya adalah FIT2016{95192c98732387165bf8e396c0f2dad2} Terima kasih ☺

- **Misi 10 (Listing) Kategori Misc**

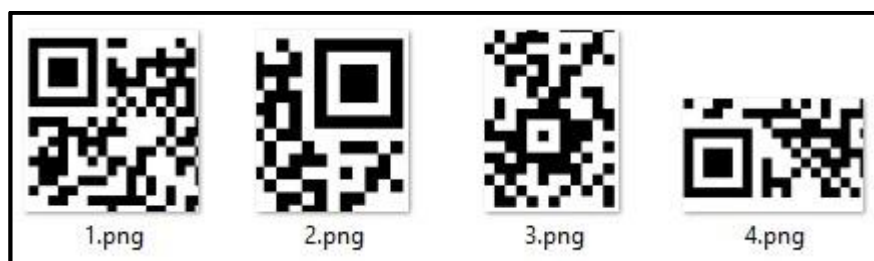
Dalam misi ini kami mendapatkan sebuah link clue menuju ke <http://198.50.174.111/soal/dir/> , setelah dibuka terdapatlah beberapa folder seperti berikut :



Terdapat banyak direktori pada link tersebut apabila dibuka maka akan terdapat direktori lainnya, dan kamipun mencoba cara lain yang sedikit lebih mudah untuk pencarian flag yang terdapat pada masing-masing direktori, aplikasi yang kami gunakan adalah Acunetix Web Vulnerability. Setelah kami scan lalu kami langsung search menggunakan kata kunci “flag” didapatkanlah hasil seperti berikut :



Pada hasil pencarian tersebut ternyata terdapat lebih dari 1 file flag, namun jika dibuka akan ada 4 file berupa gambar potongan dari gambar sebuah barcode,



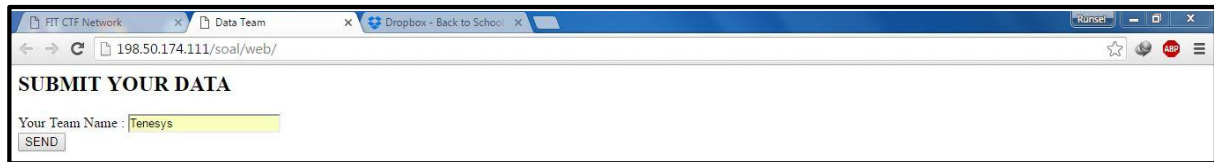
Kamipun menyusun potongan-potongan barcode tersebut hingga menjadi sebuah gambar utuh seperti berikut :



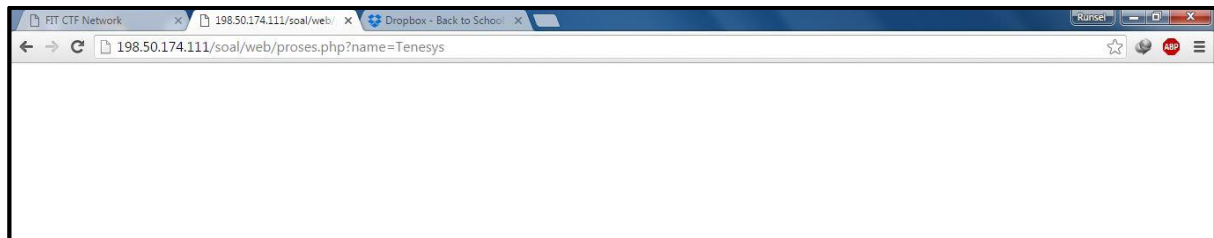
Gambarpun kami scan maka akan terdapat sebuah teks berupa flag yaitu *FIT2016{bArC0d3\_f0r\_y0u}* Terima kasih ☺

## • Misi 11 (Submit Your Team) Kategori Web

Dalam misi ini kami mendapatkan sebuah link clue yang beralamat <http://198.50.174.111/soal/web/> dimana pada link tersebut kita diminta untuk mensubmit teks,



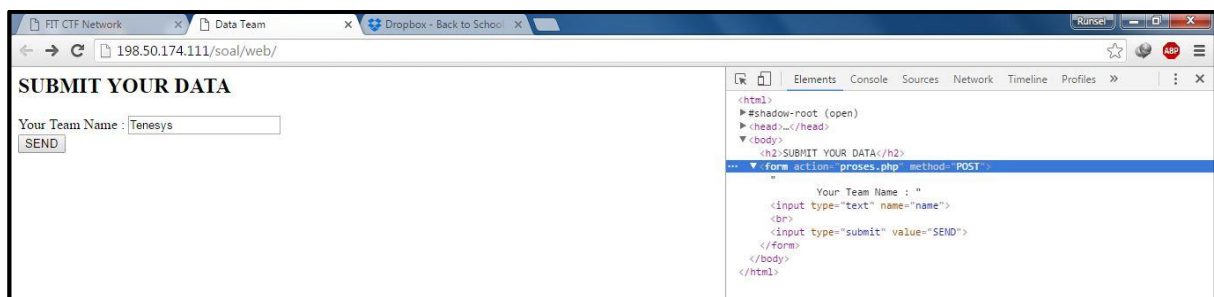
Pada gambar, kami coba memasukkan nama tim dan melakukan submit namun tidak menampilkan hasil apapun.



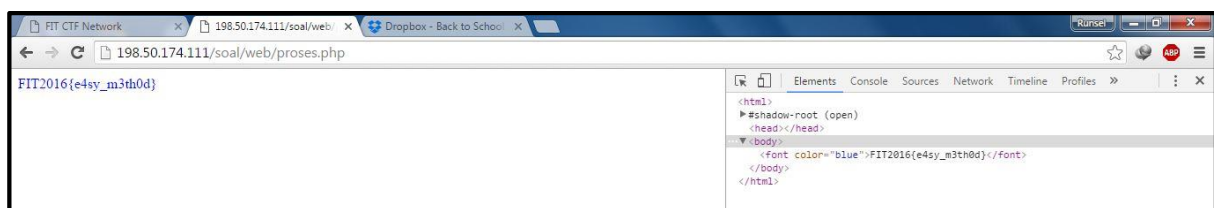
halaman proses.php tidak memberikan hasil apapun, kemudian kami coba untuk melihat Source Code web tersebut,



Terlihat bahwa pada tag form data akan di kirim dengan method "GET" kami curiga bahwa seharusnya menggunakan method "POST" sehingga kami lakukan inspect element dan mengubah method menjadi "POST"



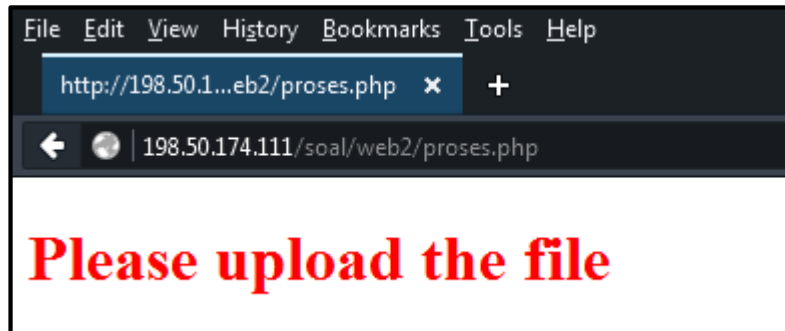
Setelah kami mengubah method menjadi "POST" kami coba submit ulang.



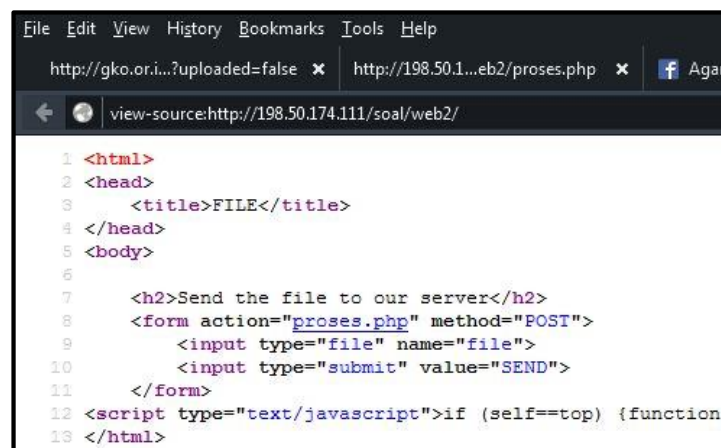
Bingo ! Terlihat sebuah flag yang kami temukan yaitu *FIT2016{e4sy\_m3th0d}* Terima kasih 😊

- **Misi 12 (Encode Your Data) Kategori Web**

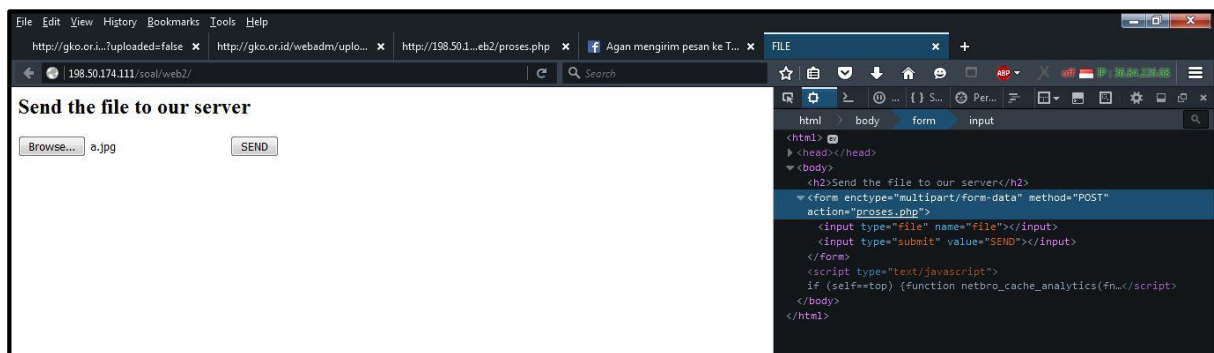
Dalam misi ini kami mendapatkan sebuah link clue yang beralamat <http://198.50.174.111/soal/web2/> Pada web tersebut kami di haruskan mengunggah file melalui form upload, namun saat kami unggah file tersebut, kami mendapatkan pesan bahwa File gagal di unggah,



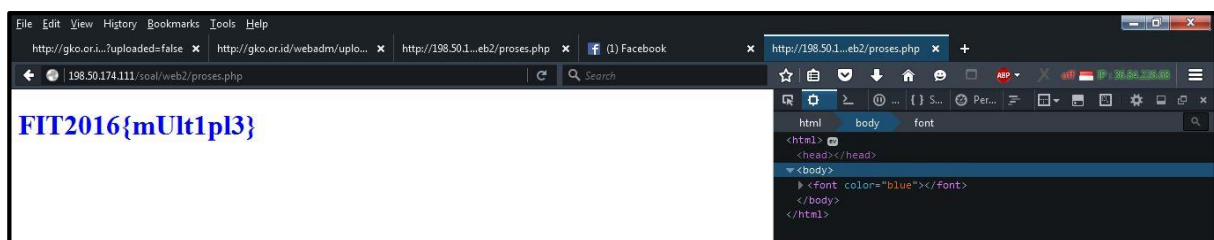
Kemudian kami coba lihat source code halaman utama web tersebut,



Terlihat source code halaman tersebut, namun ada yang aneh dari tag form mengingat ini merupakan upload form seharusnya pada tag form memiliki atribut `enctype="multipart/form-data"`,



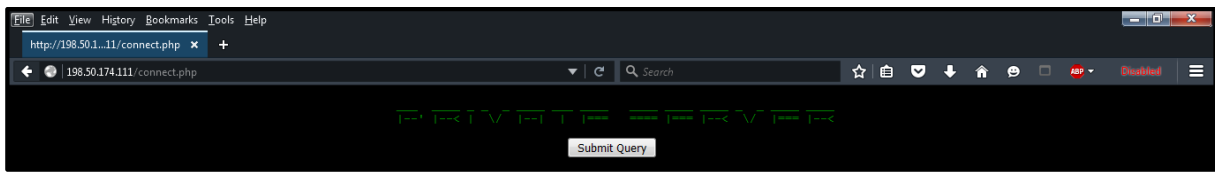
Kami lakukan inspect element dan menambahkan atribut `enctype="multipart/form-data"` kemudian kami coba unggah file gambar ke server.



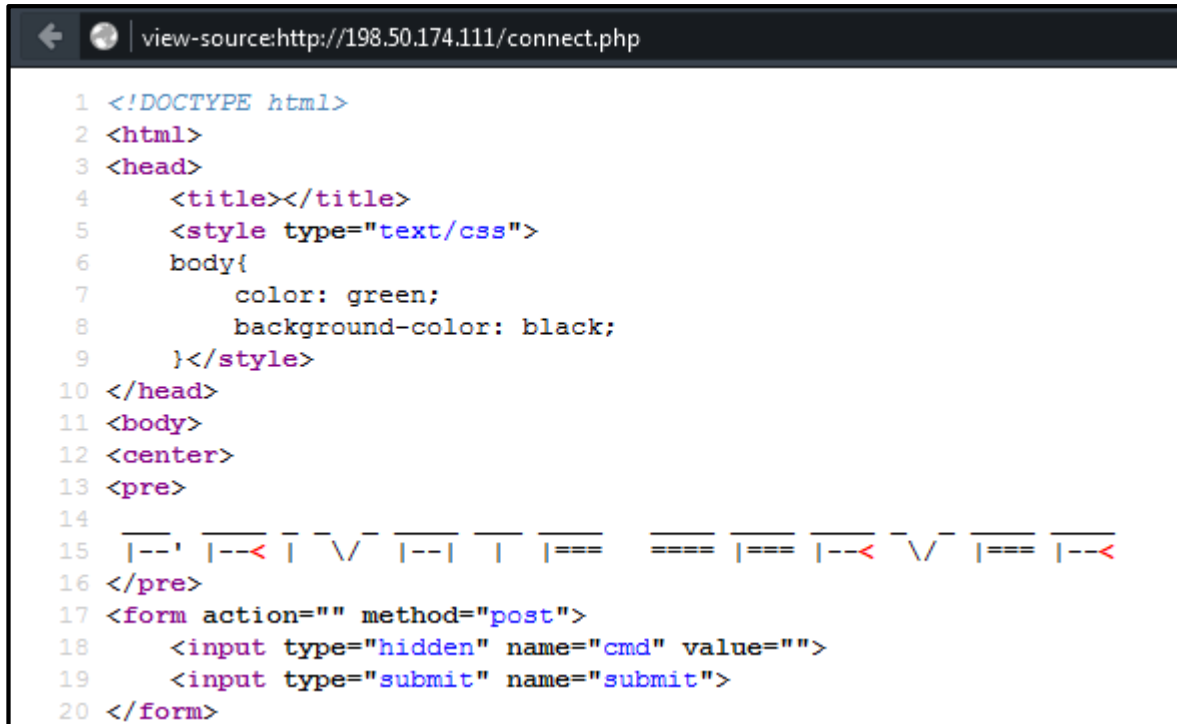
Bingo ! Terlihat sebuah flag yang kami temukan yaitu `FIT2016{mUlt1p13}` Terima kasih ☺

- **Misi 13 (Private!) Kategori Web**

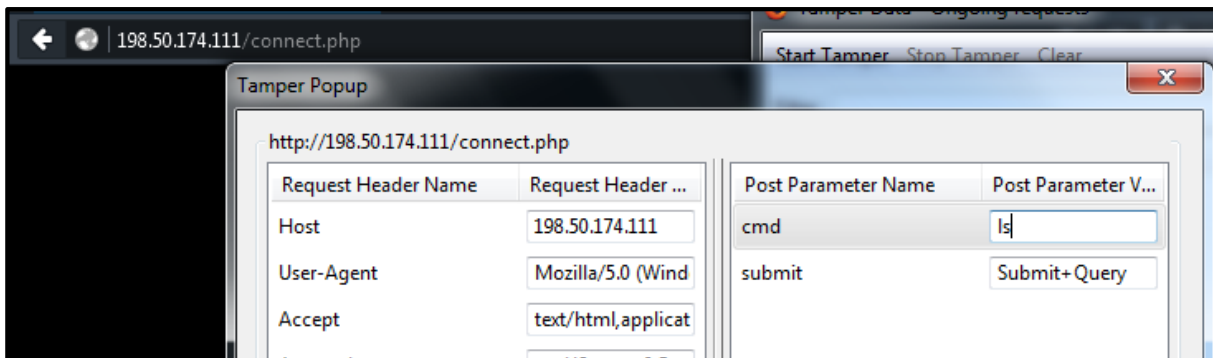
Dalam misi ini kami mendapatkan sebuah link clue yang beralamat *http://198.50.174.111/connect.php*,



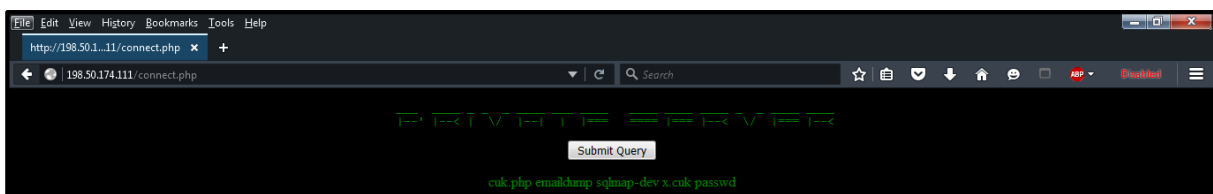
Saat kami mengunjungi alamat tersebut hanya ada sebuah tombol submit, lalu kami coba lihat source code,



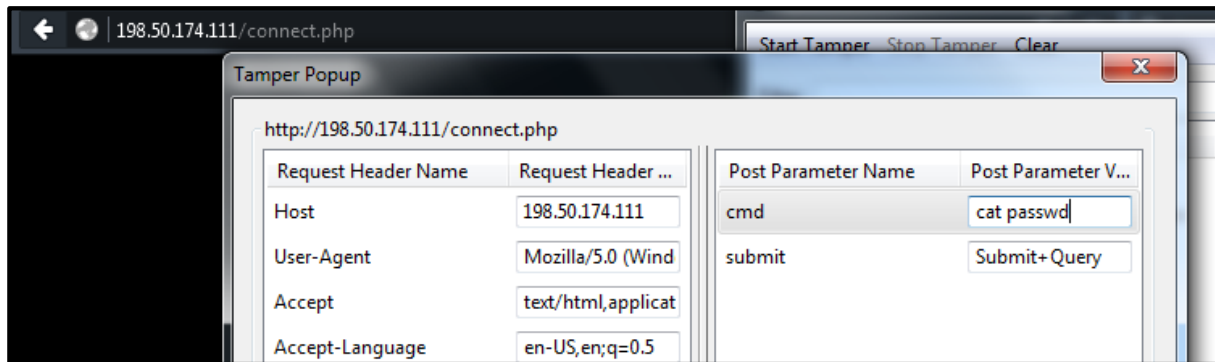
Pada source code terdapat tag input dengan type hidden namun tidak memiliki value, berdasarkan nama pada input tersebut “cmd” kami curigai bahwa web ini memiliki celah code execution,



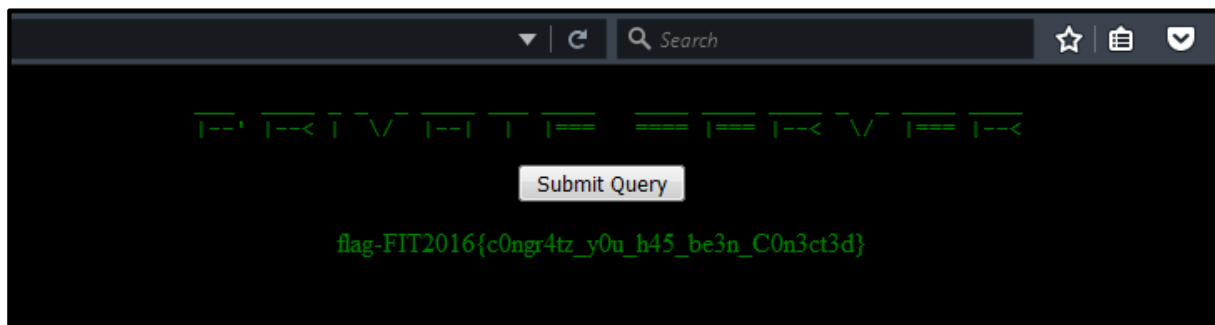
Lalu kami coba klik tombol submit, dan memberikan value pada input *name="cmd"* dengan bantuan temper data. Kami coba dengan perintah *ls* untuk melihat isi dari direktori web,



Terlihat ada beberapa file *cuk.php emaildump sqlmap-dev x.cuk passwd*, kami mencurigai file *passwd* mengandung informasi yang menarik,



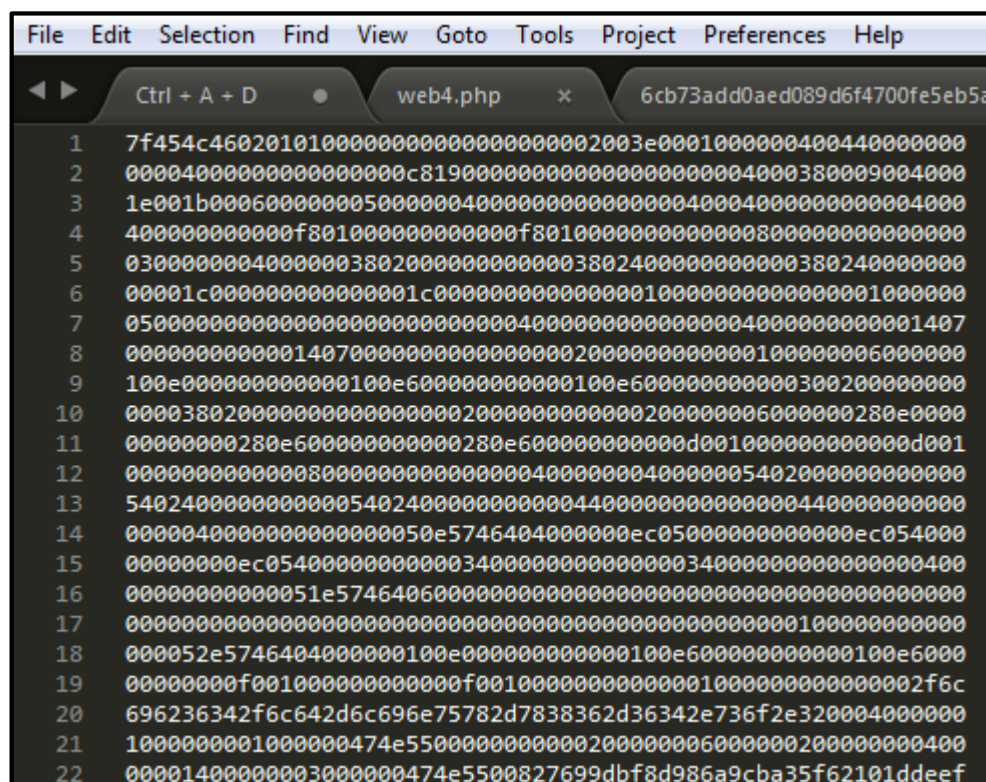
Kami lakukan submit kembali dan menjalankan perintah **cat passwd** untuk melihat isi dari file tersebut.



Bingo ! Terlihat sebuah flag yang kami temukan yaitu *FIT2016{c0ngr4tz\_y0u\_h45\_be3n\_C0n3ct3d}* Terima kasih 😊

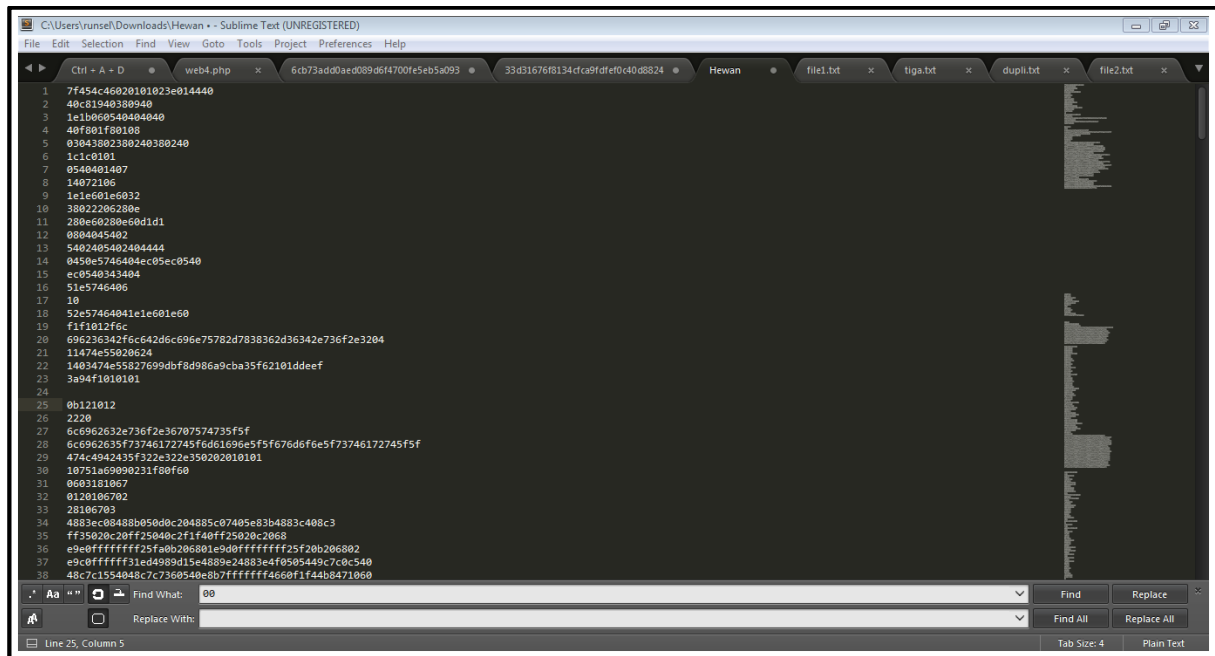
## • Misi 14 (Hewan) Kategori *Reverse*

Dalam misi ini kami mendapatkan sebuah file bernama *Hewan.txt*, terdapat string hex namun sudah dicampur dengan hex 00,

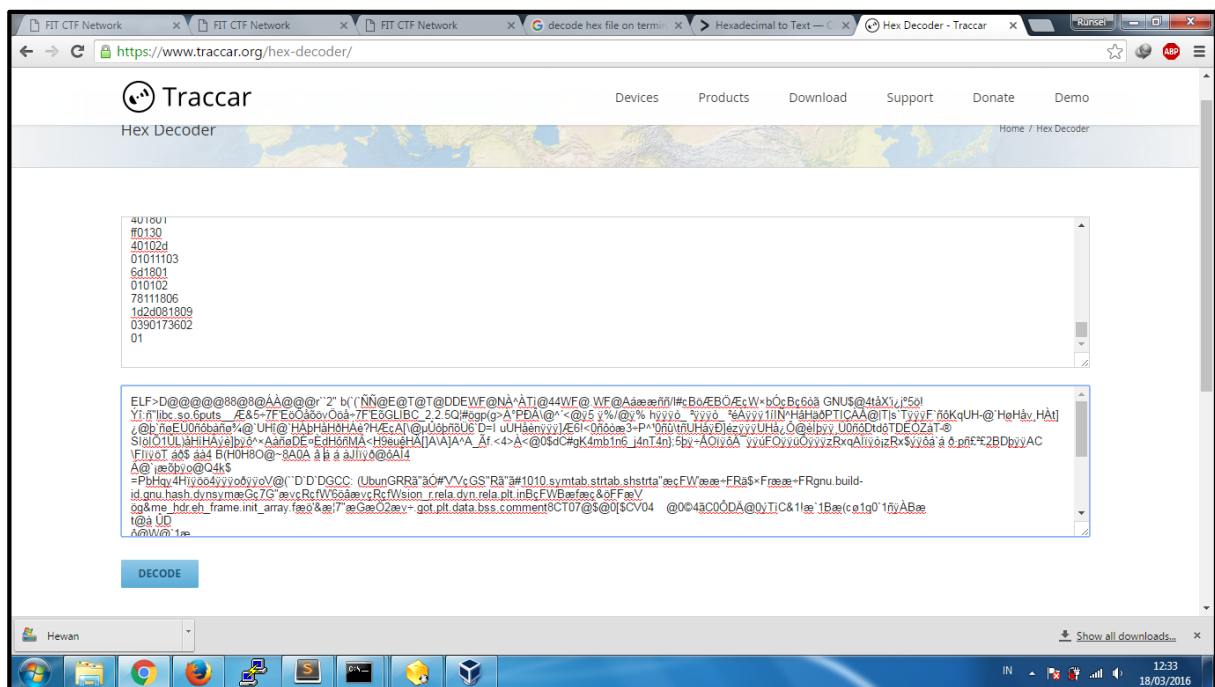




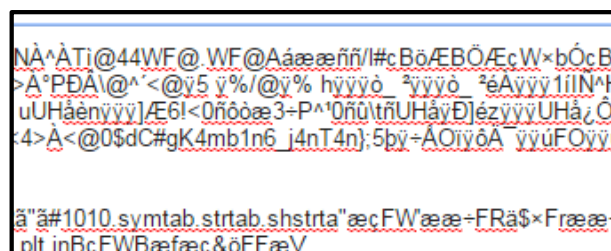
Karena mengganggu saya hapus hex 00 dengan bantuan find and replace hingga didapatlah hasil berikut :



Dengan bantuan situs <https://www.traccar.org/hex-decoder/> kami lakukan decode pada hex tersebut, kemudian mencoba mencari string yang kemungkinan merupakan flag,



Apabila hasil dari decode tersebut di zoom maka akan terlihat,



Bingo ! Terlihat sebuah flag yang kami temukan yaitu *FIT2016{K4mb1n6\_j4nT4n}* Terima kasih ☺

- Misi 15 (JKT48) Kategori *Steganography*



Soal yang di dapat berupa gambar Nabila.

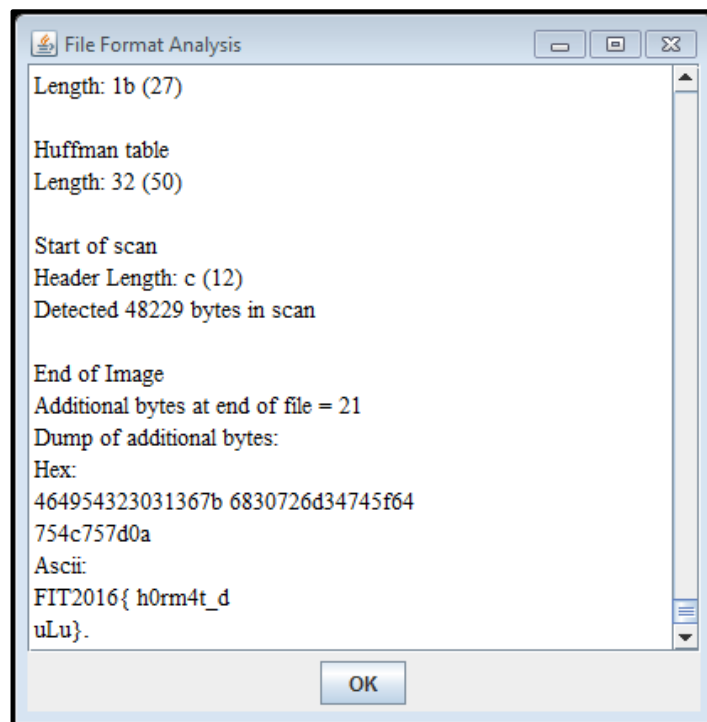
```

C:\Windows\system32\cmd.exe
Artist          : 01100010 01110101 01101011 00110100 01101110 0
1000110 01101100 01100001 00110100 00111001
Copyright       : 19 11-1-12 12-1
ISO             : 100
Exif Version    : 0220
Metering Mode   : Multi-segment
Flash           : On, Red-eye reduction
Exif Image Width      : 600
Exif Image Height     : 600
Focal Length In 35mm Format : 123 mm
XP Title        : da287353e4e008e5212d5d8055346e2e
XP Comment      : 7576fe5c3e5fbf7c2f4c8eb7bb5435bb
XP Author       : 01100010 01110101 01101011 00110100 01101110 0
1000110 01101100 01100001 00110100 00111001
XP Keywords     : aDNoM19jMGi0TGFnaQ==
XP Subject      : 0bbU_GreA14gn_0hx4a
Padding         : <Binary data 2060 bytes, use -b option to extr
act>
About           : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Creator         : 01100010 01110101 01101011 00110100 01101110 0
1000110 01101100 01100001 00110100 00111001
Rights          : 19 11-1-12 12-1
Subject         : aDNoM19jMGi0TGFnaQ==
Title           : da287353e4e008e5212d5d8055346e2e
Description     : da287353e4e008e5212d5d8055346e2e
  
```

Kami coba cek metadata gambar tersebut dengan exiftool, dan di dapatkan beberapa string hex, base64, rot 13, dsb. Namun semua itu hanya mengecoh.



Kemudian kami coba buka dengan tool bernama *StegSolve.jar*



Bingo ! pada bagian File Format Analysis kami temukan flag *FIT2016{h0rm4t\_duLu}* Terima kasih ☺

- Misi 16 (Bunglon) Kategori *Steganography*

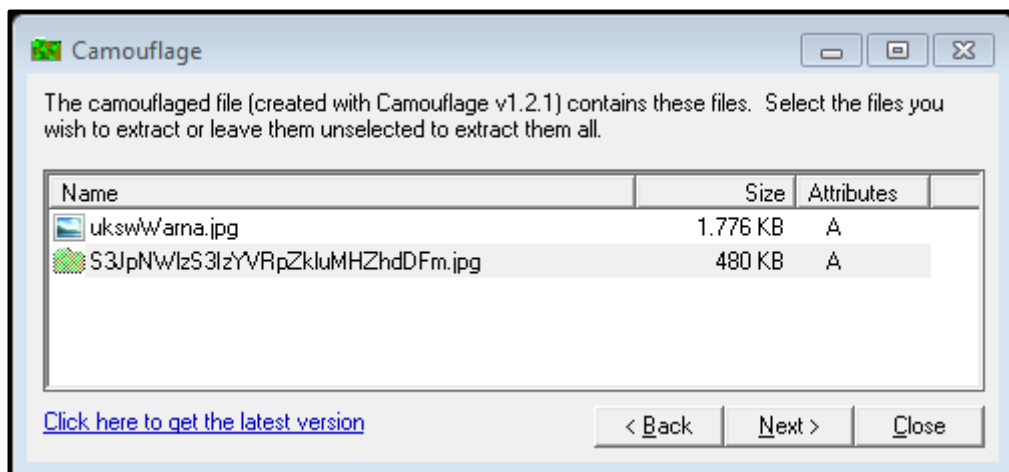


Kami dapatkan filr soal berupa sebuah file gambar, karena clue saosal ini merupakan bunglon, kami curiga ada hal tersembunyi dalam gambar tersebut.

```
C:\Windows\system32\cmd.exe

D:\begal>steghide info UKSW.jpg
"UKSW.jpg":
  format: jpeg
  capacity: 71.9 KB
Try to get information about embedded data ? <y/n> n
```

Saat kami coba cek dnegan steghide terlihat bahwa capacity file sebenarnya hanya 71.9KB namun file size gambar ini sekitar 2MB. Setelah beberapa lama mencari tahu, kami teringat akan program yang disebut *camouflage*.



Setelah mencoba berbagai password kami mendapatkan password untuk membuka steganography-nya adalah admin. Terlihat ada file dengan nama *S3JpNWlZS3lZyVRpZklumHZhdDFm.jpg* saat kami decode nama file tersebut kami mendapatkan Kri5isKr3aTifIn0vat1f, namunsaat kami submit masih salah.



Kami coba cari flag pada gambar dan mencoba submit kata K2I, dan ternyata benar flag adalah FIT2016{K2I} Terima kasih 😊

## • Misi 17 (Kehilangan File) Kategori Misc

Kami diberikan tugas untuk mencari user RouterBoard Mikrotik di alamat 222.124.21.114, melalui clue yang diberikan kami mencoba untuk melakukan bruteforce dengan bantuan hydra dan mencoba beberapa wordlist.

```

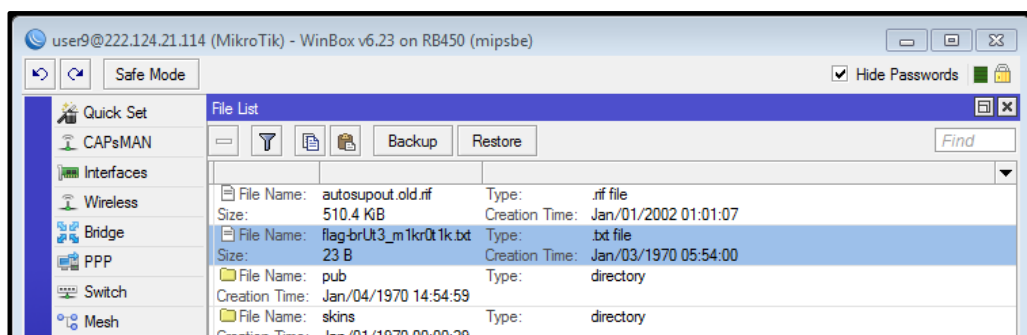
C:\Windows\system32\cmd.exe
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-03-19 17:48:20
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[WARNING] Restorefile (./hydra.restore) from a previous session found, to preven
t overwriting, you have 10 seconds to abort...
[DATA] max 1 task per 1 server, overall 64 tasks, 1 login try (l:1/p:1), ~0 trie
s per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 222.124.21.114 login: user9 password: user9
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-03-19 17:48:40

D:\hegal\hydra>

```

Setelah sekian lama, kami temukan bahwa ada *user9* dan password *user9* pada RB tersebut. Kami coba login dengan winbox.

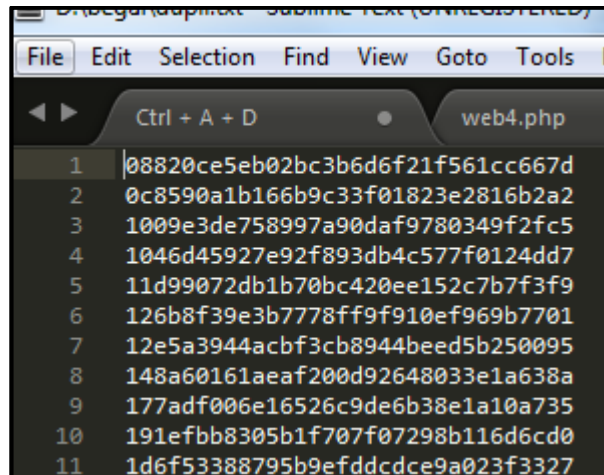


Pada bagian files kami menemukan flag pada challenge ini, FIT2016{flag-brUt3\_m1kr0t1k}



- **Misi 18 (Findme) Kategori Misc**

Kami mendapatkan 2 buah file .txt *file1.txt* dan *file2.txt* kedua file tersebut mengandung 5000 baris hash md5 sehingga total menjadi 10.000 baris.



```
File Edit Selection Find View Goto Tools P
Ctrl + A + D web4.php
1 08820ce5eb02bc3b6d6f21f561cc667d
2 0c8590a1b166b9c33f01823e2816b2a2
3 1009e3de758997a90daf9780349f2fc5
4 1046d45927e92f893db4c577f0124dd7
5 11d99072db1b70bc420ee152c7b7f3f9
6 126b8f39e3b7778ff9f910ef969b7701
7 12e5a3944acbf3cb8944beed5b250095
8 148a60161aeaf200d92648033e1a638a
9 177adf006e16526c9de6b38e1a10a735
10 191efbb8305b1f707f07298b116d6cd0
11 1d6f53388795b9efddcdce9a023f3327
```

Setelah kami selidiki terdapat 100 baris hash yang sama dan 9900 lainnya berbeda, Kami pisahkan keduanya dan mencoba mendecrypt pada 100 baris hash yang telah kami pisahkan.

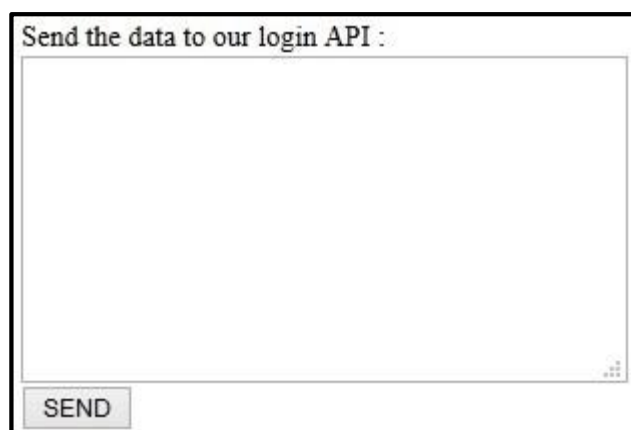
**0c8590a1b166b9c33f01823e2816b2a2**  
✓  
[md5cracker.org](#)  
result:  
FIT2016{Th3\_s4m3\_L1ne}

✗ [TMT0\[dot\]ORG](#)  
error: not found  
✗ [md5online.net](#)  
error: not found  
✗ [md5crack](#)  
error: timeout  
✗ [NetMD5Crack](#)  
error: not found

Kami dapatkan flag pada baris kedua yaitu hash 0c8590a1b166b9c33f01823e2816b2a2, FIT2016{Th3\_s4m3\_L1ne} Terima kasih 😊

- **Misi 19 (JS) Kategori Web**

Dalam misi ini, kami diarahkan menuju link <http://198.50.174.111/soal/web1> terlihat seperti berikut,



Send the data to our login API :

SEND



Lalu kami coba untuk *View source* maka akan terlihat sebuah clue berupa encoding base64,

```
e>  
sets/css/main.css" rel="stylesheet">  
  
I.php" method="POST">  
our login API : <!-- aHR0cDovLzE5OC41MC4xNzQuMTEuL3NvYWwvd2ViMS9qc29uLnR4dA== --> <br/>  
ata" cols="40" rows="10"></textarea>
```

Kami coba decoding kode tersebut maka akan didapat sebuah link yang bertuju ke <http://198.50.174.111/soal/web1/json.txt> dalam file json.txt tersebut akan didapat hasil seperti berikut,

```
<login>  
  <username>FIT2016</username>  
  <password>FTIUKSW</password>  
</login>
```

Lalu kami ubah teks tersebut dalam format json seperti pada link yang kami dapat yaitu <http://json.org/example.html> maka akan menjadi seperti ini,

```
{  
  "login":  
    {  
      "username": "FIT2016",  
      "password": "FTIUKSW"  
    }  
}
```

Lalu kami submit maka akan muncul flag yaitu *FIT2016{JSON\_ex4mpl3}* Terima kasih 😊