Write up CTF Foresty 2019



By : lonteeam

“Maaf baru pertama kali mengikuti CTF”

Nama : Bayu Muhammad Iqbal

NIM : 1301184241

Program Study : S1 Informatika angkatan 2018 ======================================

NAMA : Ganjar Gingin T

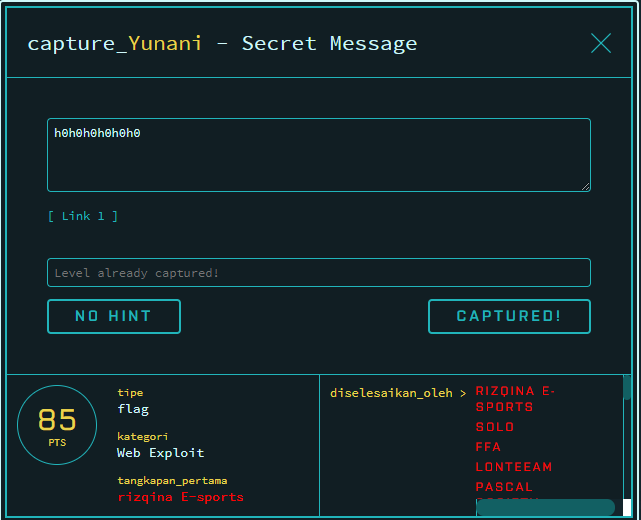
NIM : 1301180237

program study : S1 informatika angkatan 2018 =======================================

NAMA : Putranto Octa Adika

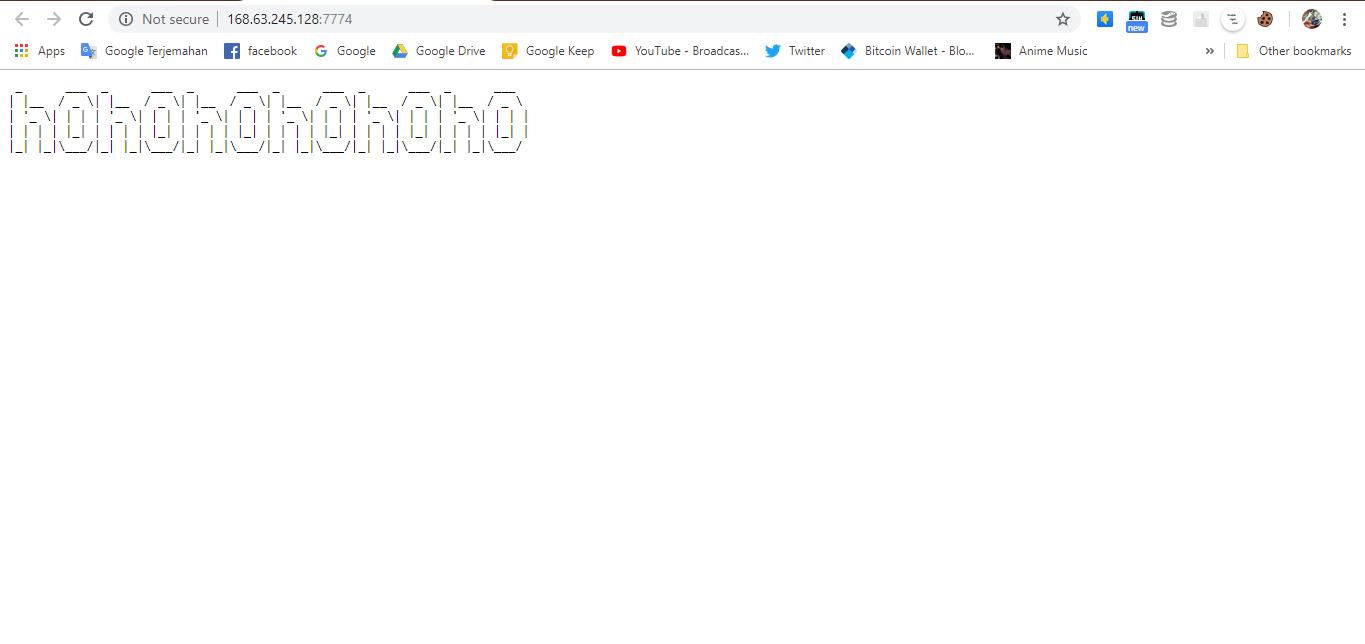
NIM : 1103184086

program study : S1 Teknik Komputer angkatan 2018

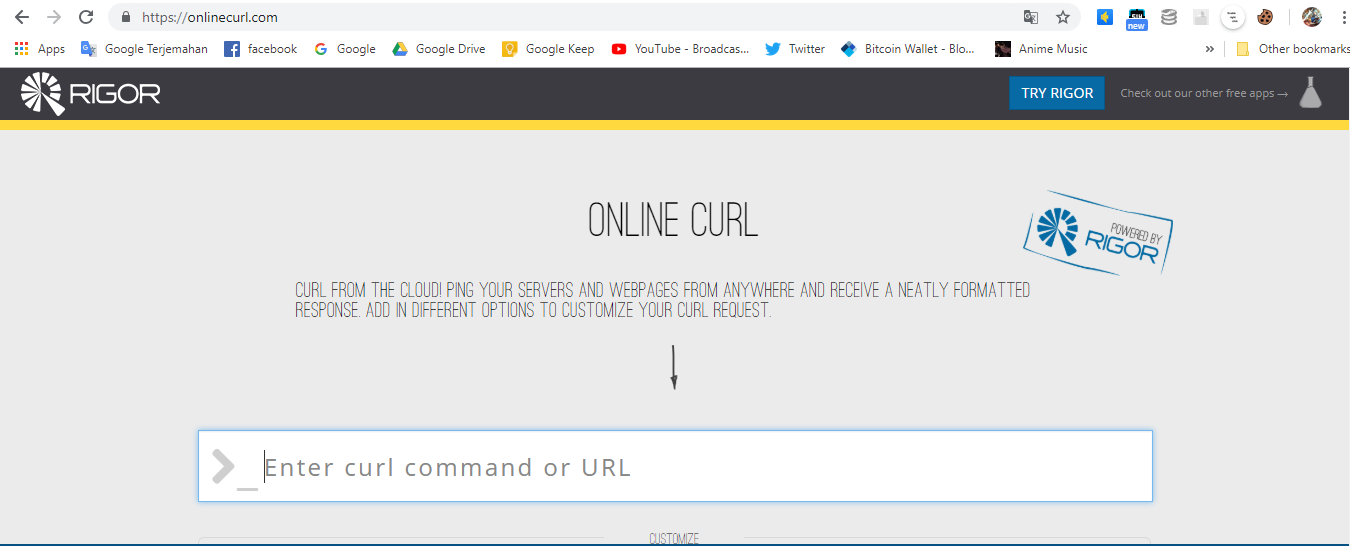
1. Soal Yunani

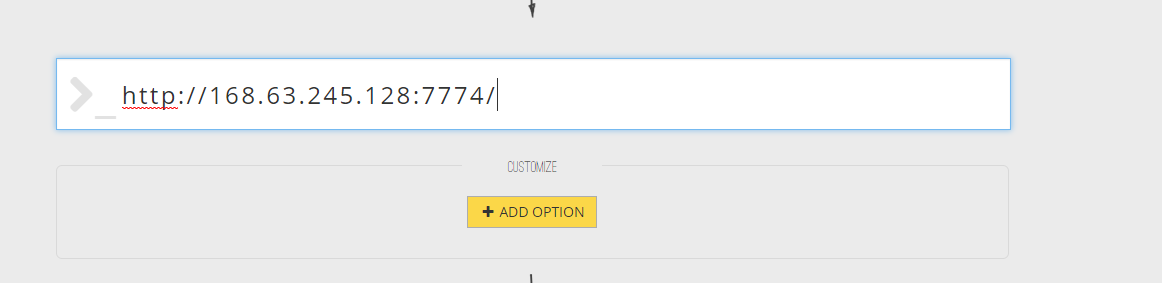
1.Buka Link yang telah disediakan

2.Tampilan Web akan seperti ini

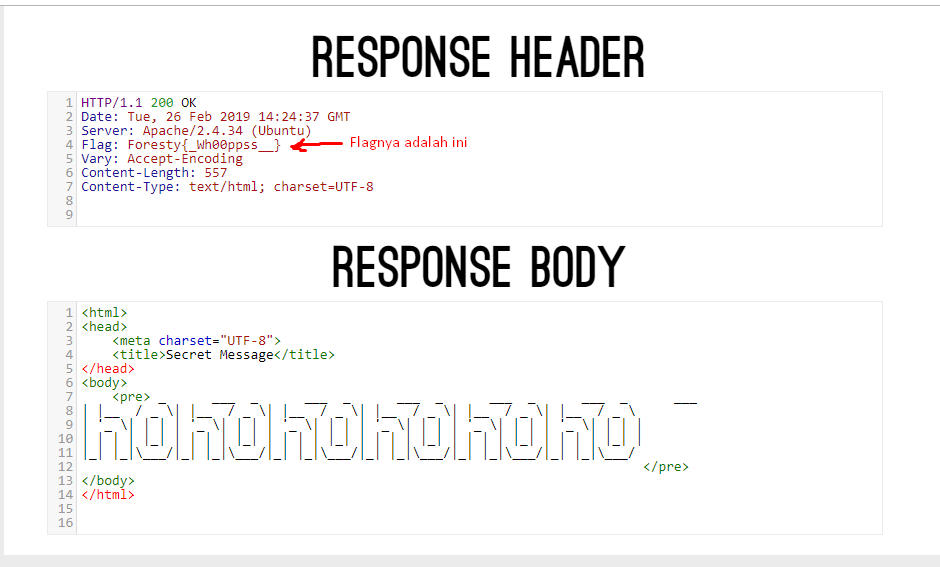


3.Buka Web onlinecurl.com

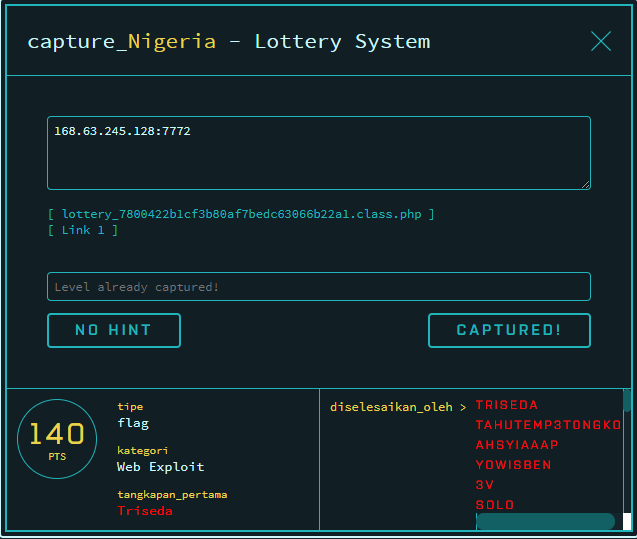


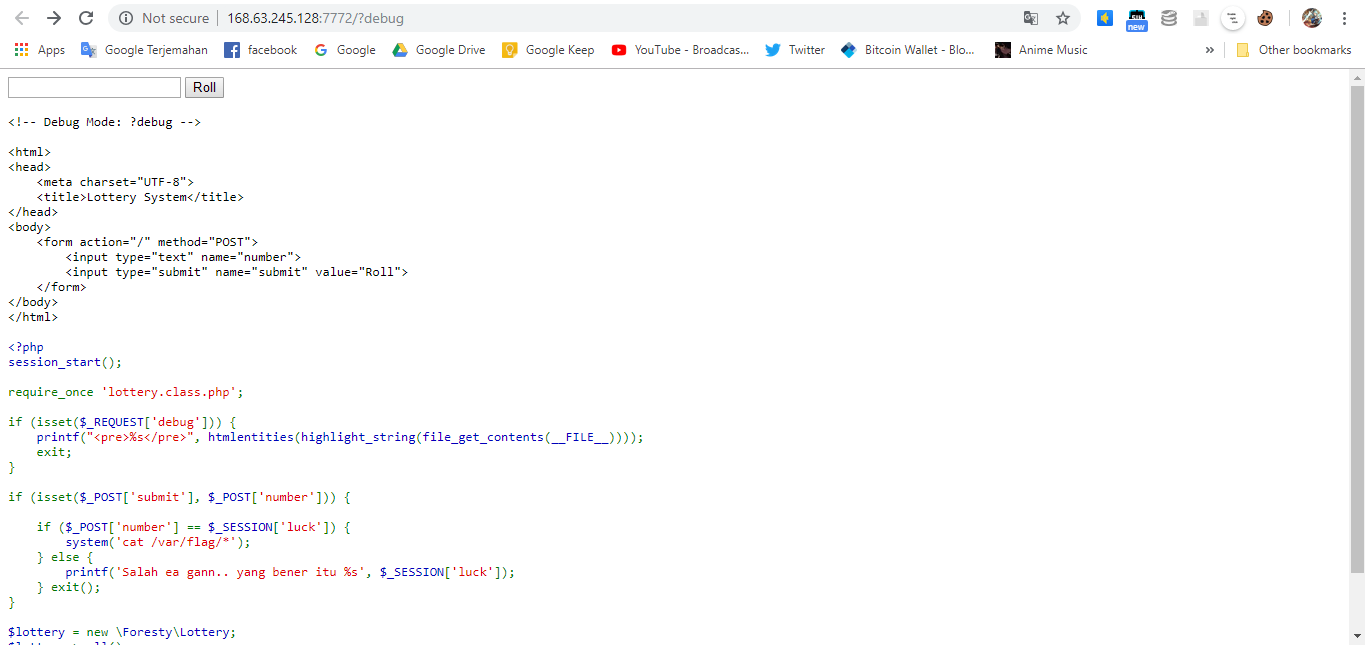
4.Copy URL Foresty ke onlinecurl.com lalu tekan enter

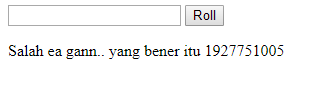
5.Hasilnya akan seperti ini dan jawaban ada pada Flag

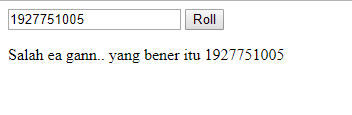


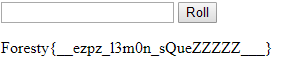
Cara Menjawab soal Nigeria

1.Buka URL yang disediakan

2.Tampilan Web seperti ini

3.Tekan Tombol ROLL lalu akan muncul angka

4.Masukan angka ke dalam Form lalu tekan roll

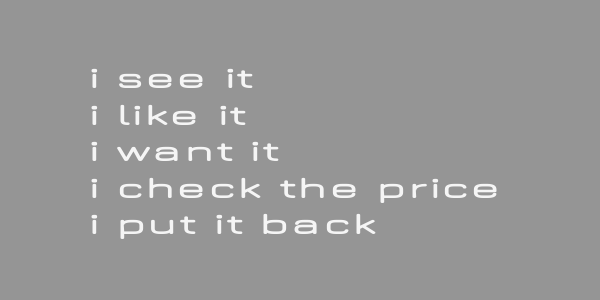
5.Flag Telah Ditemukan

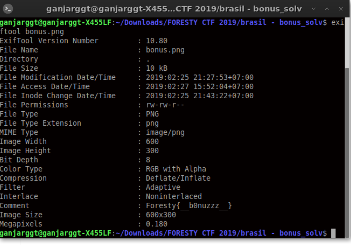
Cara menjawab soal bonus(miscellaneous)



Didapat file berformat .png sebagai berikut :

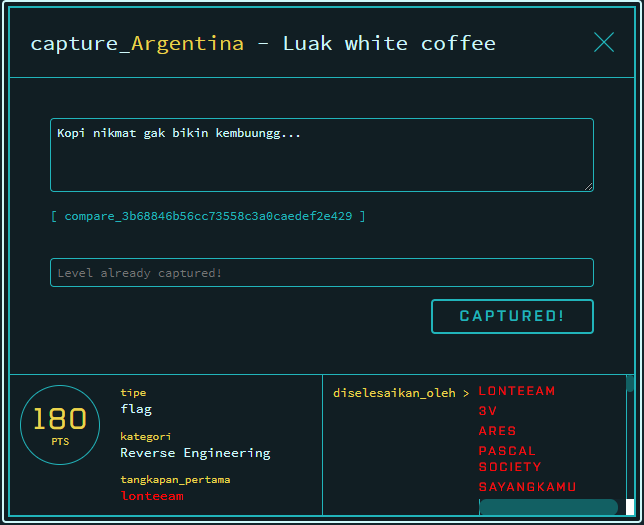
dengan bantuan tool exiftool didapat flag :



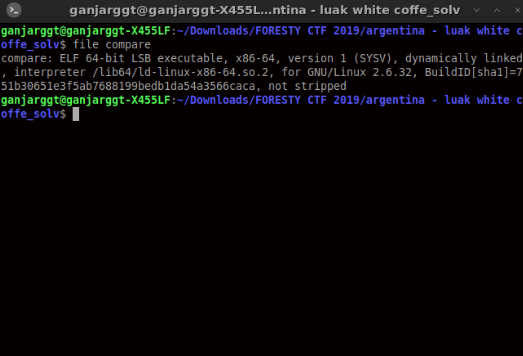


Flag : Foresty{\_\_b0nuzzz\_\_}

Menjawab soal Luak white coffe ( Reverse engineering )

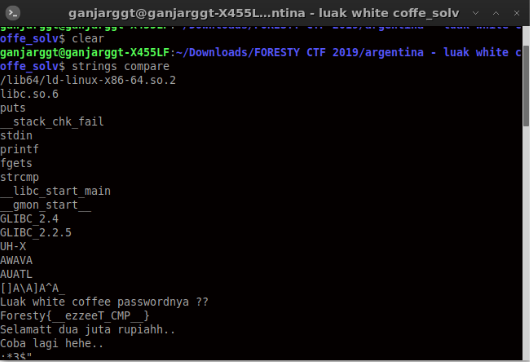


Didapat file dengan format ELF executable dengan arsitektur 32 bit, dengan bantuan tool file pada unix didapat informasi :



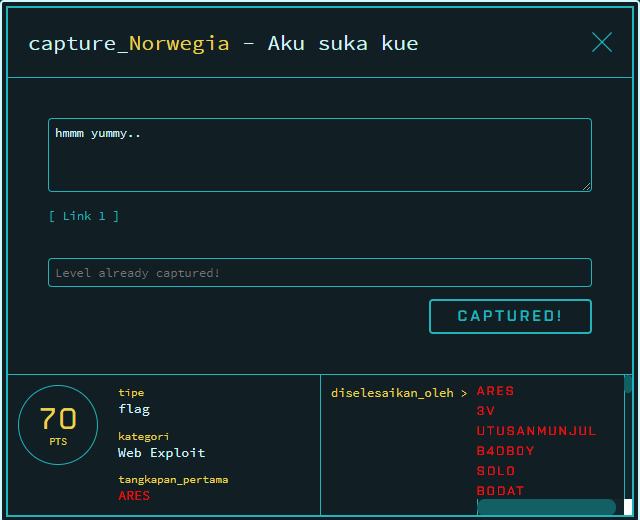
File elf 32 bit tidak stripped dan dynamic linked .

Sebenarnya kami menggunakan tools IDA untuk identifikasi, namun ternyata dengan memanfaat tool strings, flag sudah didapat

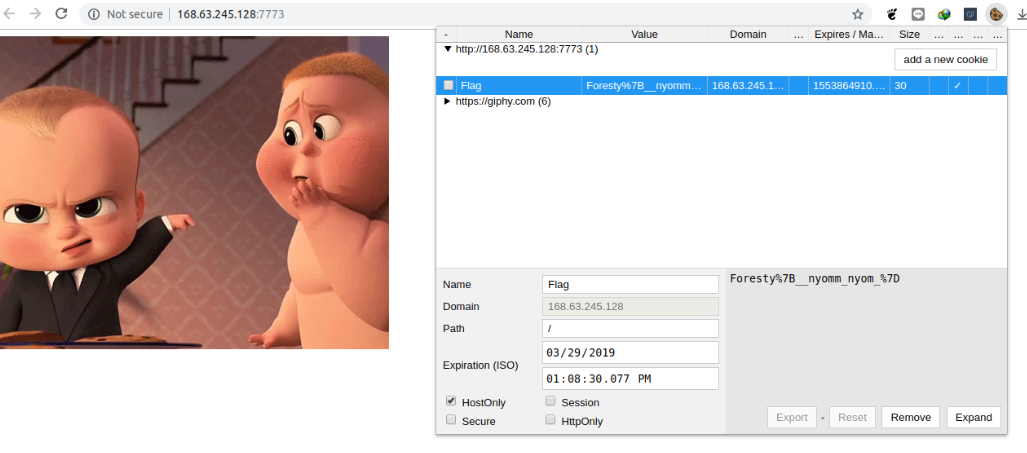


Flag : Foresty{\_\_ezzeeT\_CMP\_\_}

Soal Aku suka kue ( Web exploitation )



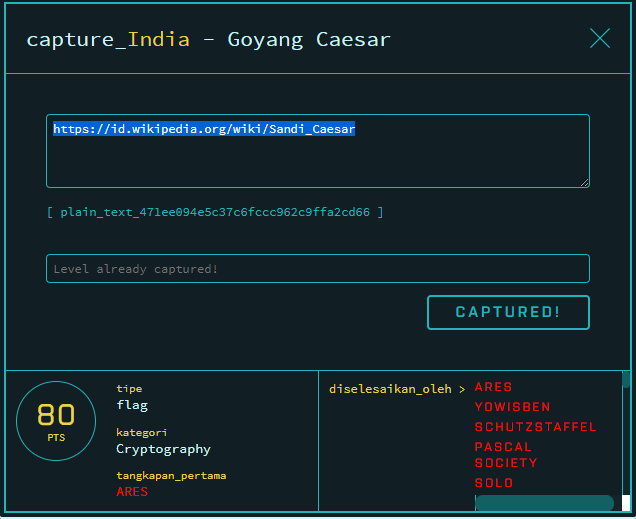
Pertama, dari soal sudah dicurigai flag berada di cookies, langsung saja mengunjungi website nya :



Ternyata benar, flag ada di cookie.

Flag : Foresty{\_\_nyomm\_nyom\_}

Soal Goyang Caesar (Cryptography )



Didapat file sebagai berikut

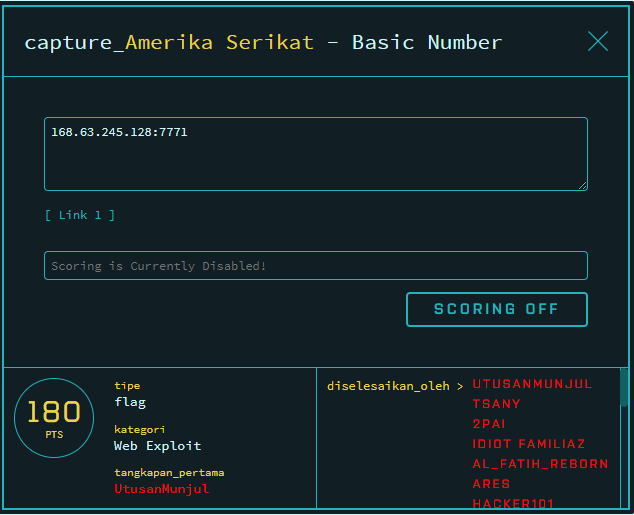


Sesuai namanya, sandi tersebut ter-enkripsi dengan teknik chaesar dengan n = -9.

Flag : Foresty{\_oke\_s1app\_\_}

==============SOAL YANG BELUM TUNTAS==================

BASIC NUMBER ( Web Exploitation )



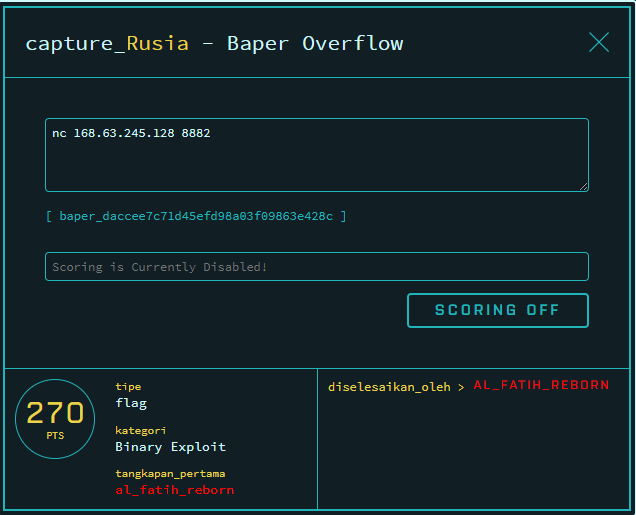
Setelah mengunjungi link yang tersedia, dan membuka

url/index.php?debug , didapat script php sebagai berikut :



Mungkin, flag didapat dari memasukkan angka integer dengan maksimal 5 digit dan harus lebih dari variable PHP\_INT\_MAX pada script PHP di server, namun kami belum berhasil, karena tim kami kekurangan orang yang berpengalaman dalam web exploitation.

Baper Overflow ( Binary exploitation )

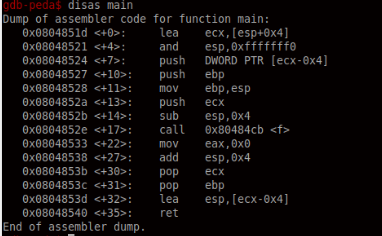


Setelah file di download, dengan menggunakan perintah file, didapat informasi sebagai berikut



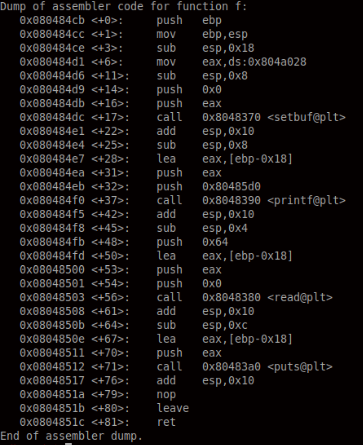
File executable, dengan arsitektur 32 bit, dynamic linked, dan not stripped

Kemudian, dengan bantuan command gdb dan proses disassembly, di dapat informasi sebagai berikut



Terdapat pemanggilan fungsi <f>, substitusi antara data di esp,0x4.

Kemudian didapat informasi dari fungsi <f> sebagai berikut :

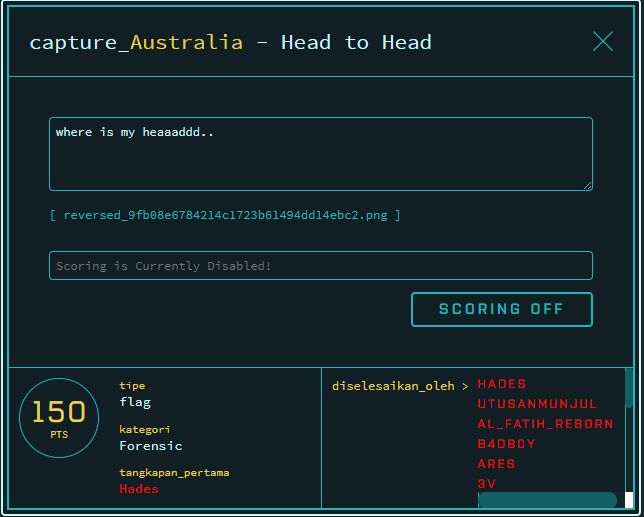


Terdapat pemanggilan fungsi \_setbuf.

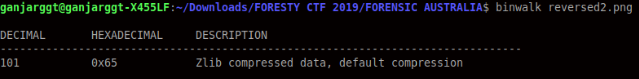
Karena ini adalah soal tipe buffer overflow, maka disana haruslah terdapat variable char/array untuk menyimpan deretan hexadimal.

Lagi-lagi, karena pengalaman yang kurang terhadap soal buffer overflow, soal tersebut belum dapat kami selesaikan.

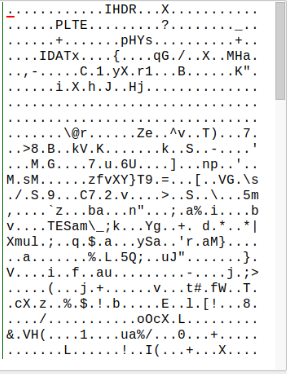
Soal Head\_to\_Head ( File forensic )



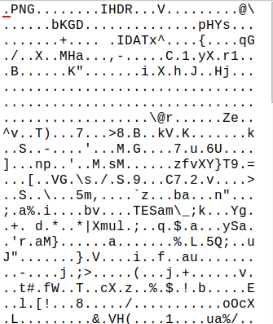
Setelah file di download, kemudian dilakukan identifikasi file dengan tools binwalk didapat informasi berikut :



Kami mencurigai file tersebut adalah file .png , sehingga dilakukan identifikasi menggunakan tools hex editor dan didapat informasi sebagai berikut



Karena, apabila file tersebut adalah file berformat .png, maka seharusnya terdapat data .PNG pada header data, namun dalam file ini tidak ada, sehingga kami mencoba menambahnya manual, sehingga berubah menjadi

  
namun, ternyata file .png tersebut tetap teridentifikasi corrupt.

Sehingga untuk saat ini kami belum menyelesaikan soal ini.