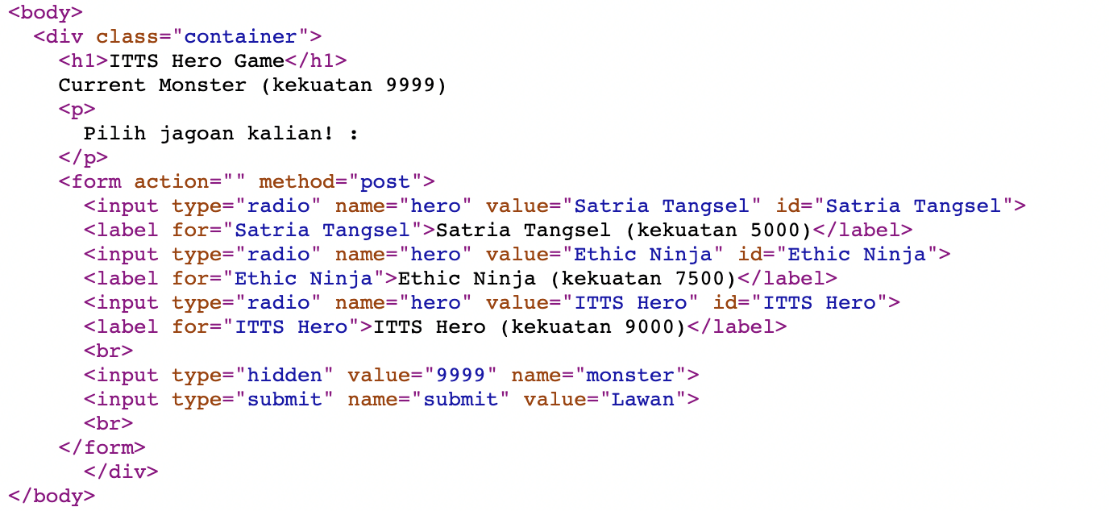
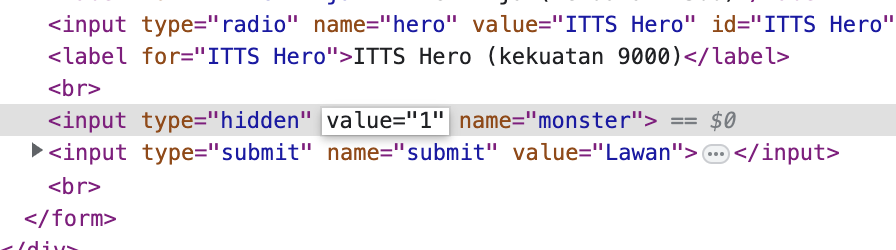
Penyelesaian soal Not too Easy

* Lihat source code di bawah ini. 

Terlihat inputan yang hidden adalah monster, maka soal ini bisa diselesaikan cara:

Edit melalui inspect element, ubah value 9999 menjadi 1, kemudian pilih jagoan apapun. Maka akan terlihat flagnya seperti di bawah ini.

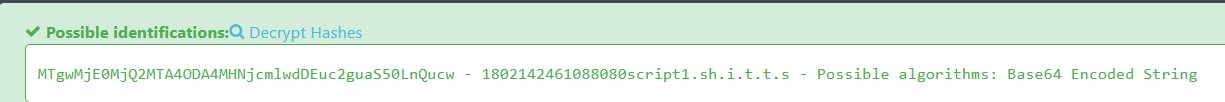


Untuk flag, kemarin memang sengaja tidak kita tampilkan di halaman flag.php. Kami berharap ada beberapa dari kalian yang masuk langsung ke server…(beberapa dari kalian melakukan hal itu di week 1, jadi sengaja kami tes kembali…hehehehe)

Di bawah ini adalah halaman endpoint jika kalian sudah berhasil melakukan web tampering



Karakter “MTgwMjE0MjQ2MTA4ODA4MHNjcmlwdDEuc2guaS50LnQucw” akan kita cek di [https://hashes.com/en/tools/hash\_identifier](https://hashes.com/en/tools/hash_identifier%20) untuk mengetahui hash apa yang digunakan. Hasilnya sebagai berikut :



Ternyata di-encode menggunakan Base64. Sekarang cermati :“1802142461088080script1.sh.i.t.t.s” Kita bisa memisah menjadi 3 bagian

1802142461088080 = ini seperti alamat IP dan port (180.214.246.108:8080)

script1.sh = ini seperti program bash shell yang harus kita download ?

i.t.t.s = dibaca ITTS. Institut Teknologi Tangerang Selatan, penyelenggara kompetisi ini. bisa jadi ini hanya dummy teks yang ditambahkan oleh panitia. Bisa kita abaikan

coba masukkan di browser kalian <http://180.214.246.108:8080/script1.sh.i.t.t.s> jika berhasil kalian akan mendapatkan program bash shell untuk dianalisa.

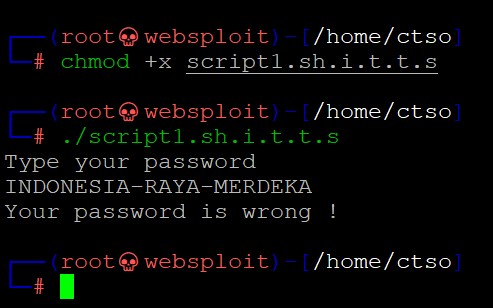
Banyak pertanyaan yang datang ke panita…apakah soal ini Reverse Engineering. Kami sudah menulis di awal bahwa kategori soal ini adalah Web Hacking dan materi reverse engineering kami rasa belum pantas jadi soal CTF tingkat SMK. Jadi focus saja jalankan program script1.sh

Periksa atribut file



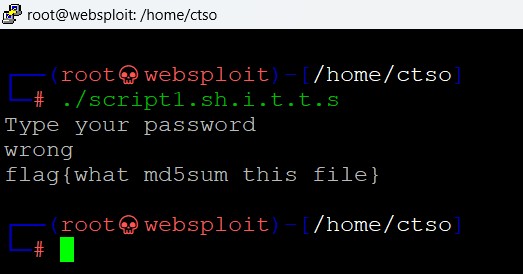
Sudah jelas di atas bahwa program di-compile di lingkungan GNU/Linux. Abaikan reverse engineering

Jadikan executable dan jalankan programnya



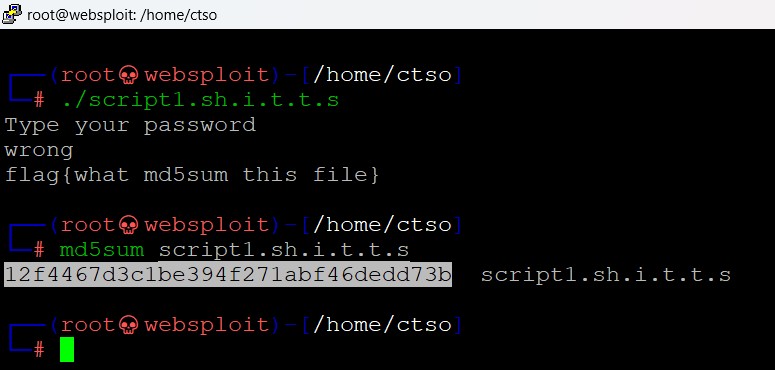
Jika dijalankan, program akan minta input password. Disinilah pentingnya kita belajar pengalaman apa dan bagaimana budaya CTF. Sejak awal, CTF itu dibentuk sebagai game problem solving. Beberapa kasus mengambil apa yang terjadi di dunia nyata dan sebagian dimaksudkan untuk bersenang-senang (game mode). Kami yakin beberapa peserta ada yang sudah familiar dengan dunia CTF.

Kembali ke soal, apapun password yang kalian masukkan, “Your password is wrong !” Itulah kata kuncinya teman-teman…“Your password is wrong !”



Sekali lagi dibutuhkan konsentrasi dan ketelitian…Di dalam dunia CTF, tidak pernah flag disertai spasi. Jadi apakah flag di asli atau fake flag ???

flag{what m5sum this file} kalau dibahasa indonesiakan artinya {berapa md5sum file ini}. Jadi challenge sebetulnya kalian hanya disuruh validasi berapa md5sum file script1.sh.i.t.t.s !!! kalian bahkan tidak perlu sampai reverse engineering…



Moral story soal di atas :

* Kalian harus menguasai serangan web berupa web tampering
* Kalian memahamai program di linux seperti apa dan bisa menganalisanya
* Md5sum sering digunakan untuk memeriksa keaslian/integritas suatu file
* Jadikan ini sebagai pengalaman dalam bermain CTF. Butuh konsentrasi dan ketelitian. Di beberapa event terkadang panitia suka jahil seperti kami 😊…awas kena gocek… :p
* Program script1.sh..i.t.t.s dicompile dengan software shc <https://neurobin.org/projects/softwares/unix/shc/> yang katanya mustahil untuk di-decode/reverse engineering. Tapi coba lihat artikel disini https://www.hexacorn.com/blog/2023/01/13/decrypting-shell-compiled-shc-elf-files/

Sepertinya bisa dilakukan reverse engineering…cukup menarik bukan…hehehe. Mungkin tahun depan akan ada soal reverse engineering 😊