Final OWWI CTF 2019 Writeup

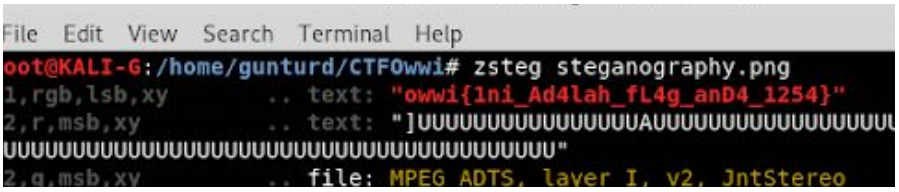
By : We Have Hazboy

Steganography 1

Flag terlihat pada header langsung menggunakan default image opener dari browser googlechrome, menampilkan flag dengan format **owwi{Y0ur_g3t_fl4g_0ww1i}**

Steganography 5

Menggunakan library zsteg dari Ruby , file tersebut dieksekusi dengan zsteg [namafile] dan flag didapatkan dengan format **owwi{1ni_Ad4lah_fL4g_anD4_1254}**



SQL Injection 1

Terdapat sebuah form dengan input username dan password. Kami langsung melakukan injeksi dasar dengan teknik SQL Injection dengan payload
Username : ‘ or ‘1’ = ‘1
Password : ‘ or ‘1’ = ‘1

Flag : **owwi{selamat_ini_flag_anda_2207}**

SQL Injection 2

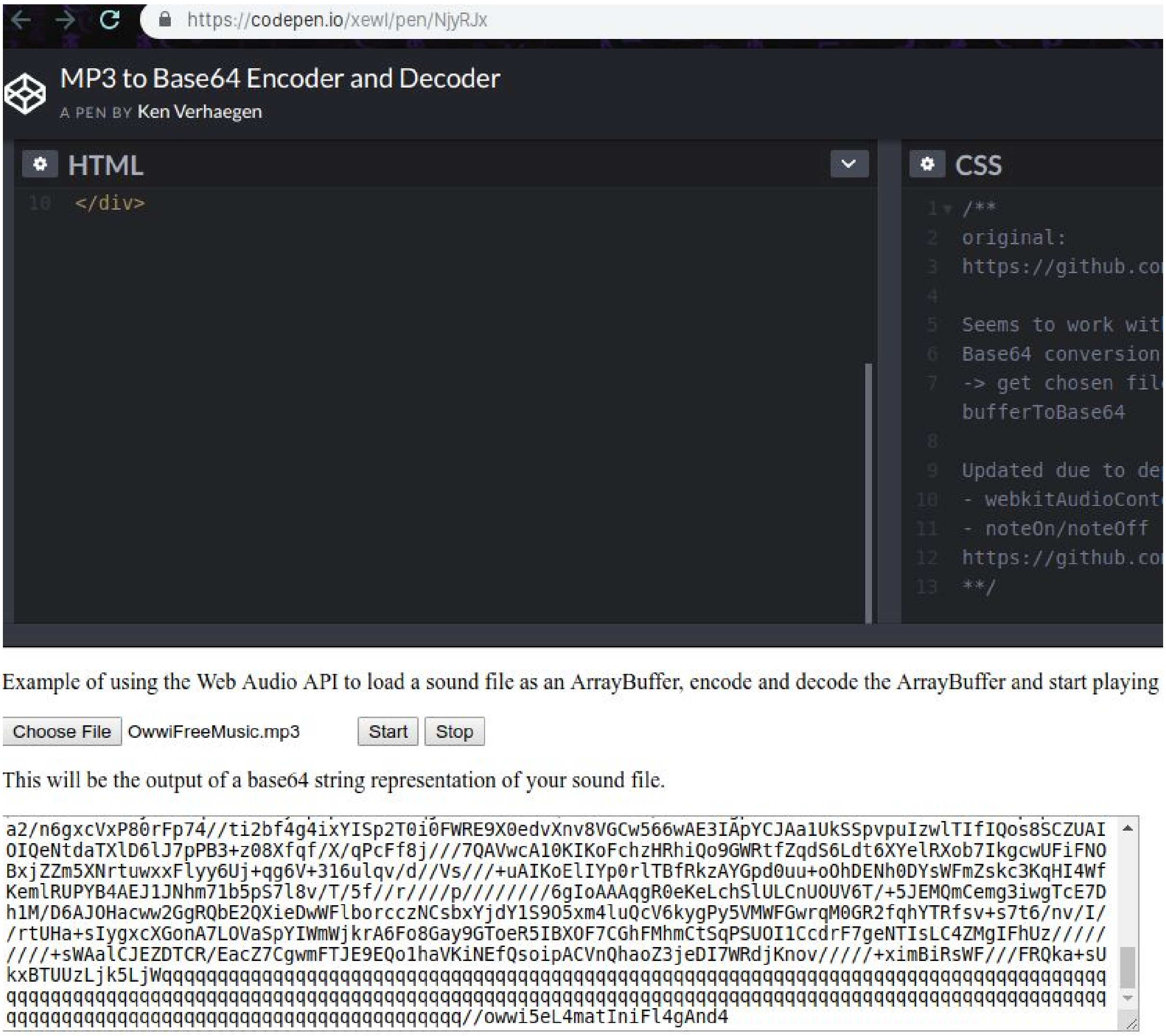
Dari challenge ini diberikan link menuju http://172.2.5.1/login2/login.php. Pada halaman ini terdapat 2 buah input yaitu username dan password. Ketika kami mencoba melakukan SQL Injection dengan cara seperti yang sebelumnya ternyata gagal.

Setelah dilakukan injeksi dengan beberapa input dan masih gagal, kami iseng mengakses halaman http://172.2.5.1/login2/index.php dan disitu sudah tertera flag dengan jelas.

Flag : **owwi{selamat_ini_flag_anda_2102}**

Encryption

Diberikan sebuah file bernama OwwiFreeMusic.mp3. Pada soal terdapat *hint* yaitu file ini telah terenkripsi dengan teknik base64.
Sehingga dapat digunakan *tools online* yang dapat diakses melalui link berikut:
https://codepen.io/xewl/pen/NjyRJx
File tersebut dapat didekripsi dengan *tool* ini, yang menghasilkan flag :



Flag : **owwi5eL4matIniFl4gAnd4**