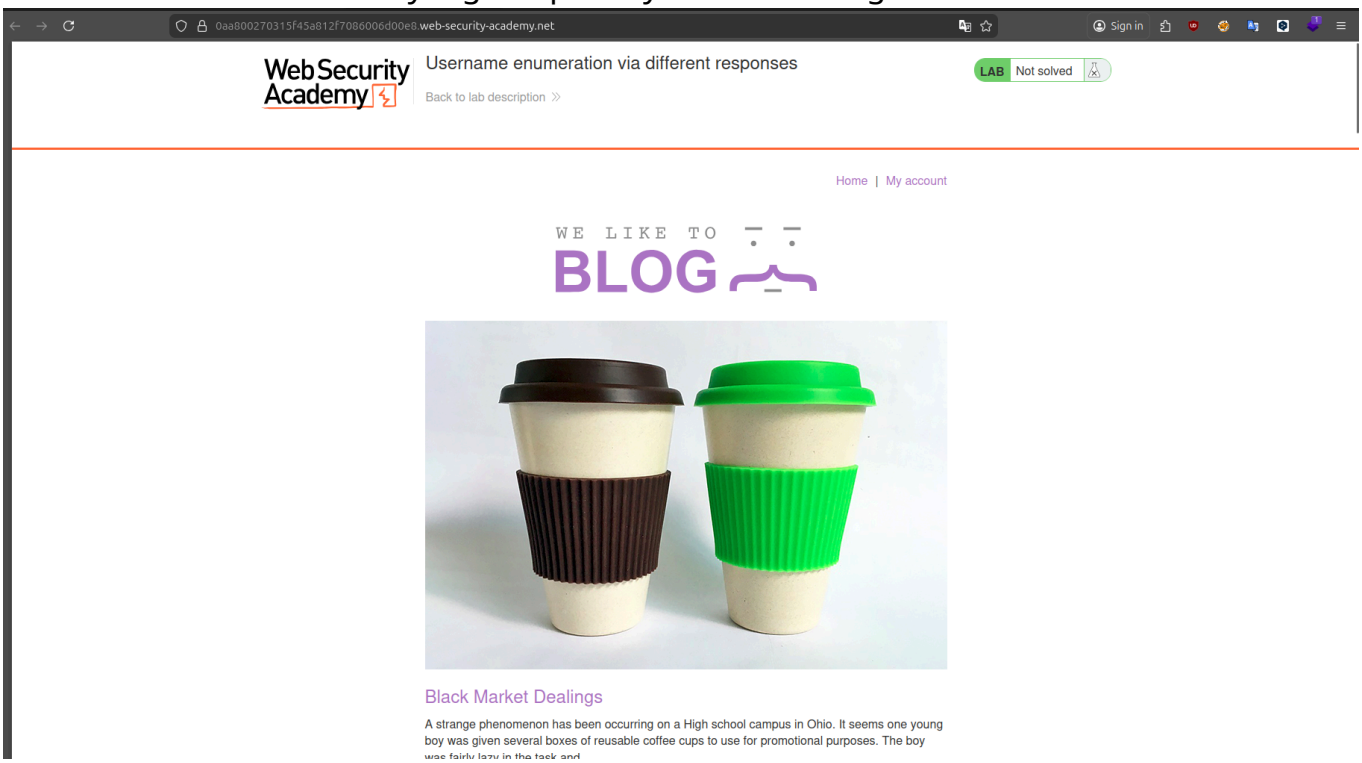
Username enumeration via different responses

Goals : identifikasi nama pengguna yang valid, lakukan serangan brute-force untuk menemukan kata sandi pengguna tersebut, lalu akses halaman akun mereka.

kami diberikan sebuah lab yang tampilannya adalah sebagai berikut

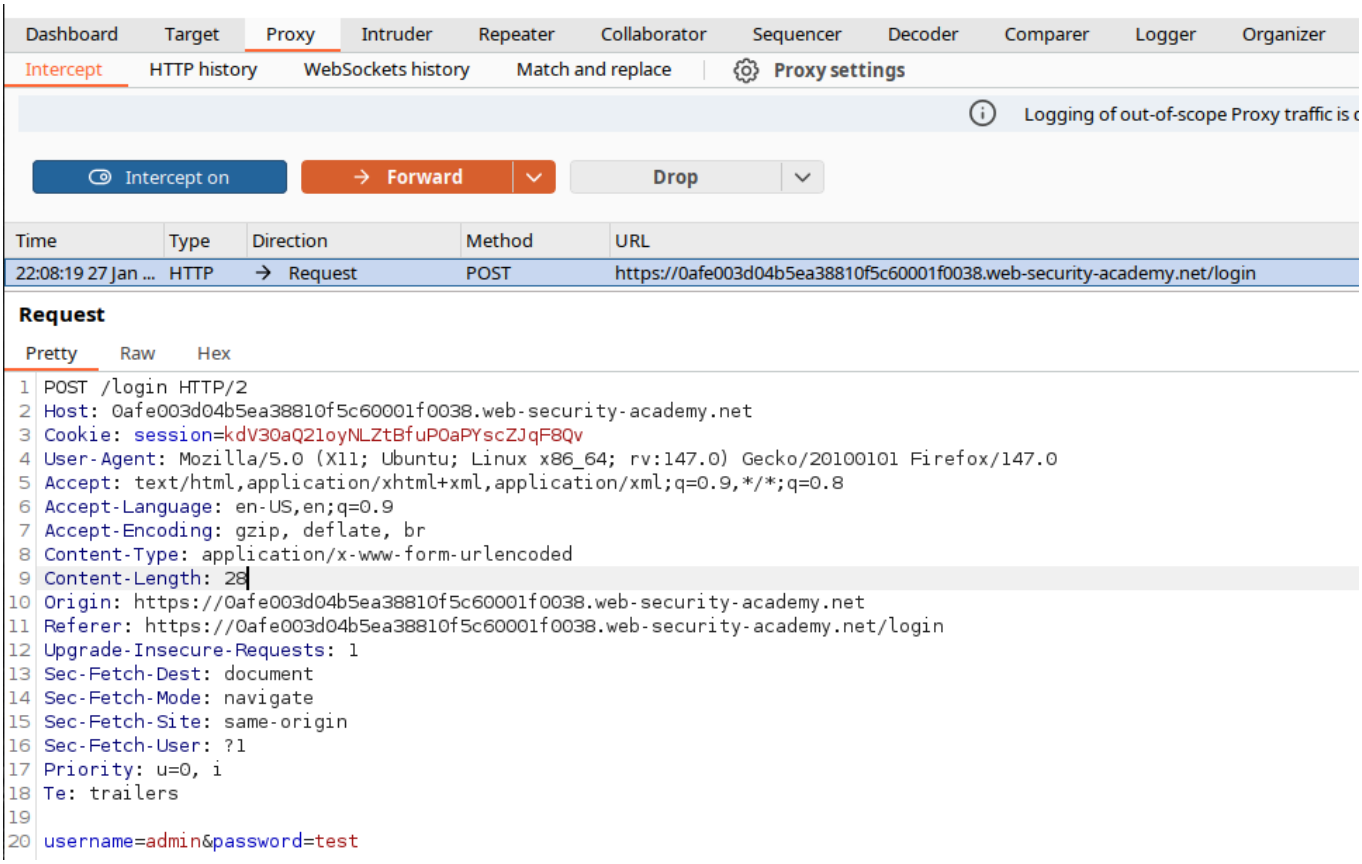


kami diberikan clue untuk menebak user mana yang valid, dan kami di berikan sebuah list user yang akan kami gunakan untuk mencoba melakukan verifikasi bahwa user tersebut valid

https://portswigger.net/web-security/authentication/auth-lab-usernames (untuk username validation)
https://portswigger.net/web-security/authentication/auth-lab-passwords (setelah mendapatkan user yang valid kami gunakan wordlist ini untuk melakukan bruteforce ke dalam kolom katasandi pengguna yang valid)

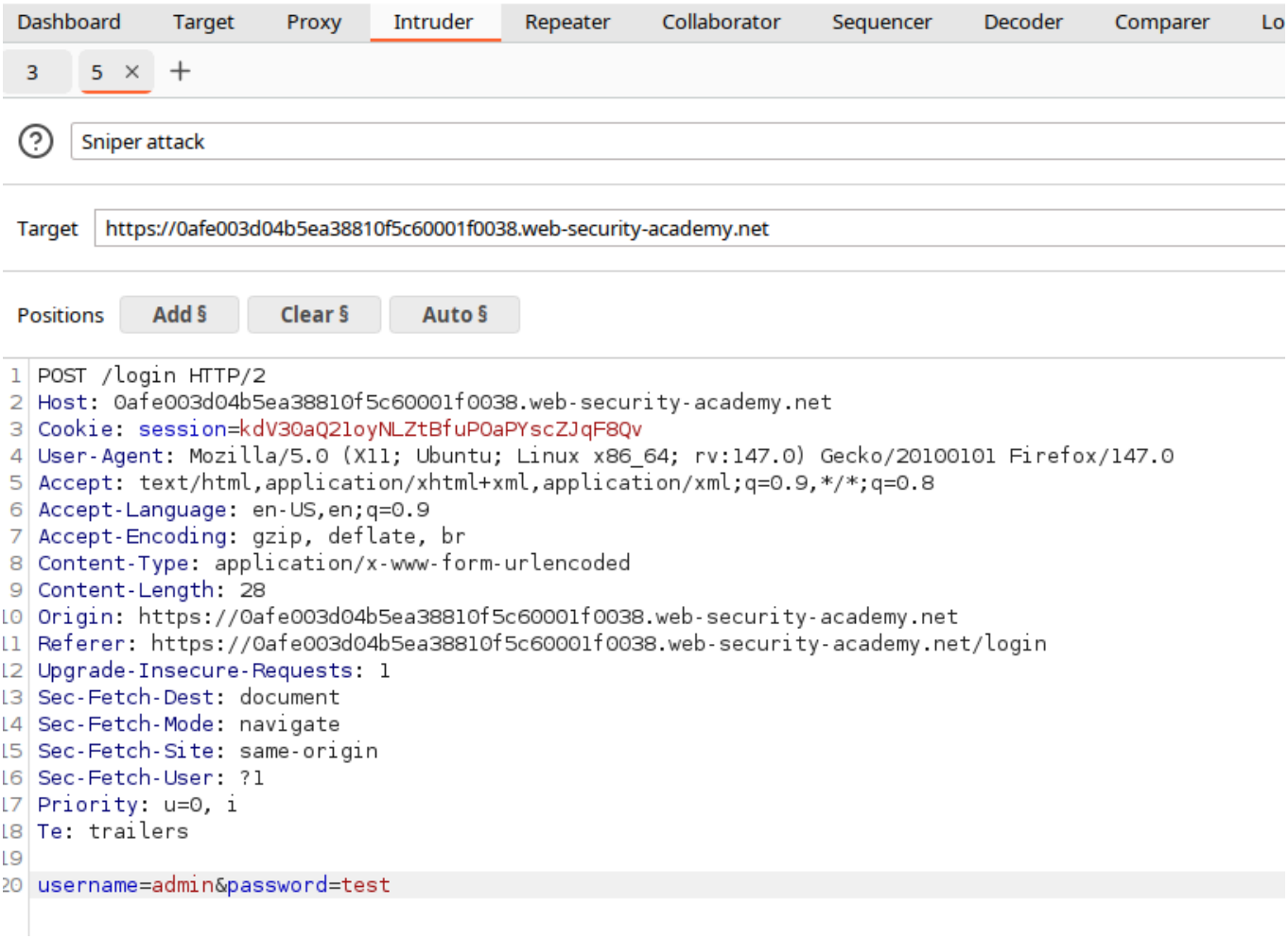
IRC (in real case)
creating wordlist for targeting users -> brute target -> if valid -> creating wordlist for password the valid users -> brute users use the wordlist u make for the valid users -> if found u get bounty.

tugas pertama adalah melakukan intercepting permintaan dari browser yang akan kita attack



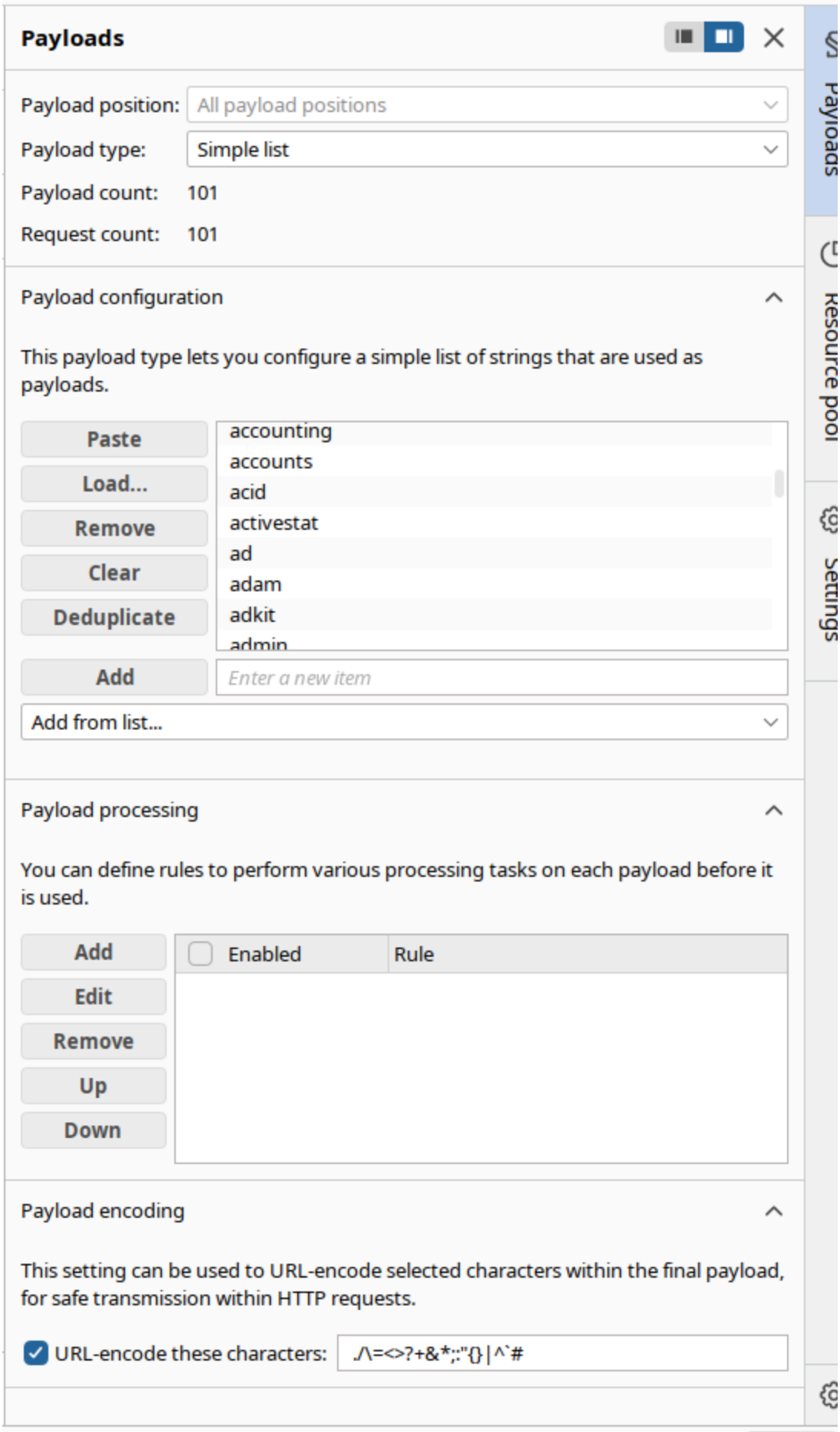
input string apapun kedalam kolom users dan password, untuk melihat request yang di kirim ke server atas permintaan yang kita lakukan.

langkah selanjutnya adalah mengirim request ini sebagai senjata intrusi (brute force) kita ke server, dengan send to intruder.

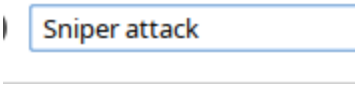


tandai kolom yang ingin di inputkan wordlist.
dengan menggunakan add yang kita gunakan untuk menemukan user yang valid berdasarkan wordlist yang sudah di sediakan.

lakukan setup wordlist pada kolom inputan wordlist



lalu pilih jenis serangan bruteforce yang akan kita lancarkan



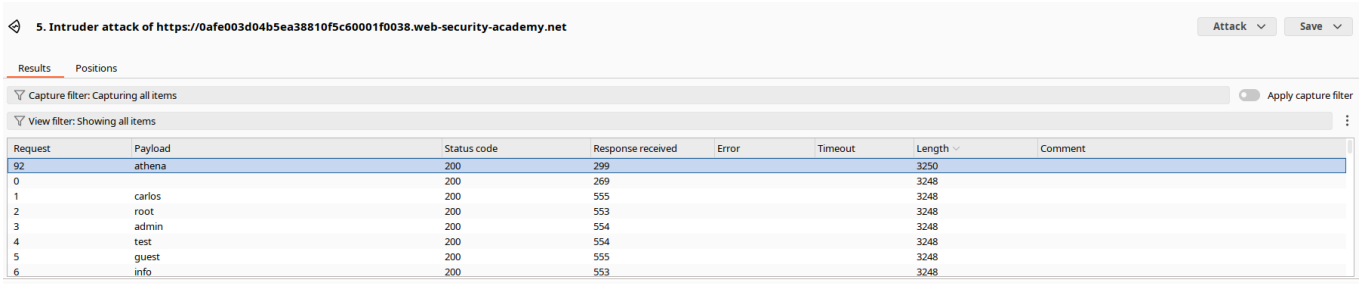
ada 4 jenis serangan yang ada pada bruteforce attack ini.
namun kita hanya menggunakan type serangan sniper, berikut penjelasan singkatnya

Sniper

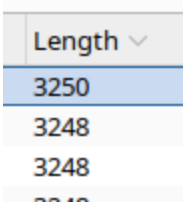
Fungsi: Menggunakan satu payload set dan menguji setiap posisi payload secara bergantian.
Cara kerja: Jika ada 2 posisi payload dan 100 payload, akan ada 200 request (100 untuk posisi 1, kemudian 100 untuk posisi 2).
Kapan digunakan:

- Testing satu parameter dengan banyak nilai (contoh: username enumeration, SQL injection pada satu field)
- Fuzzing parameter individual untuk menemukan vulnerability
- Ketika hanya ingin fokus pada satu titik serangan
  Contoh: Testing berbagai username dengan password yang sama untuk melihat mana yang valid.

kita bisa langsung melakukan eksekusi untuk serangan kali ini.
setelah menunggu kami akhirnya menemukan apa yang kami inginkan

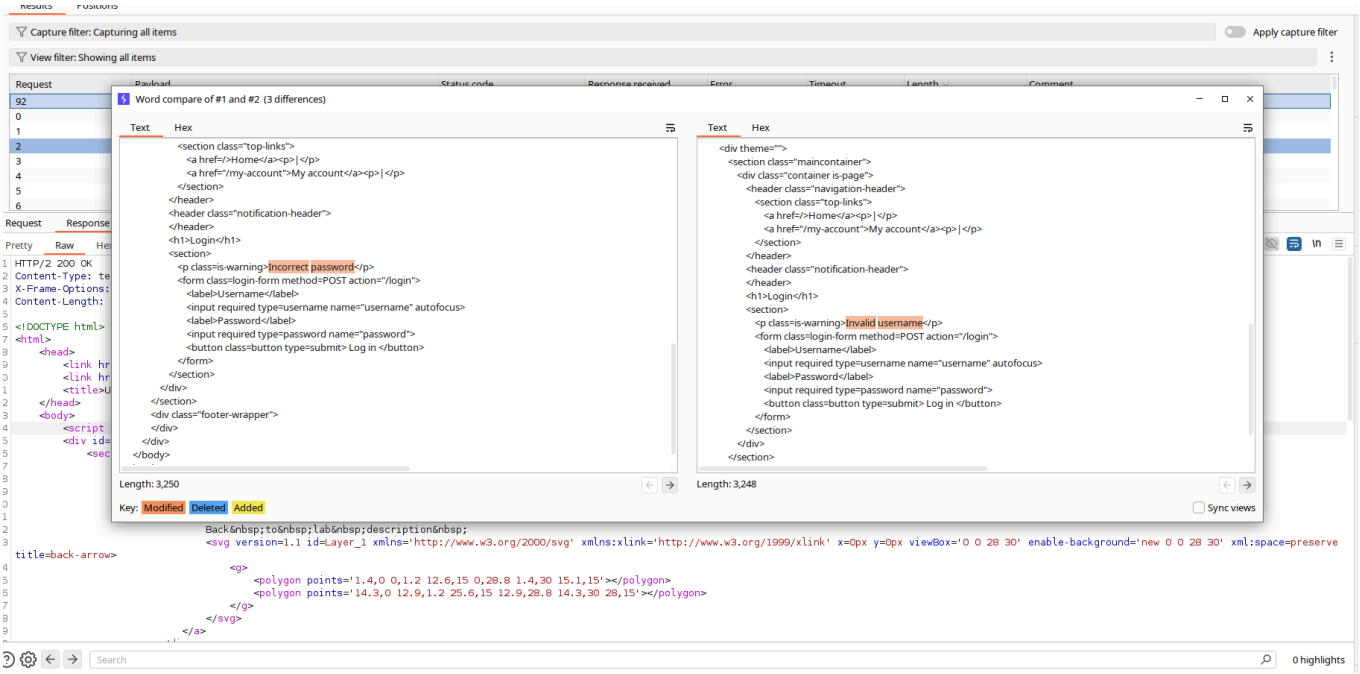


user athena



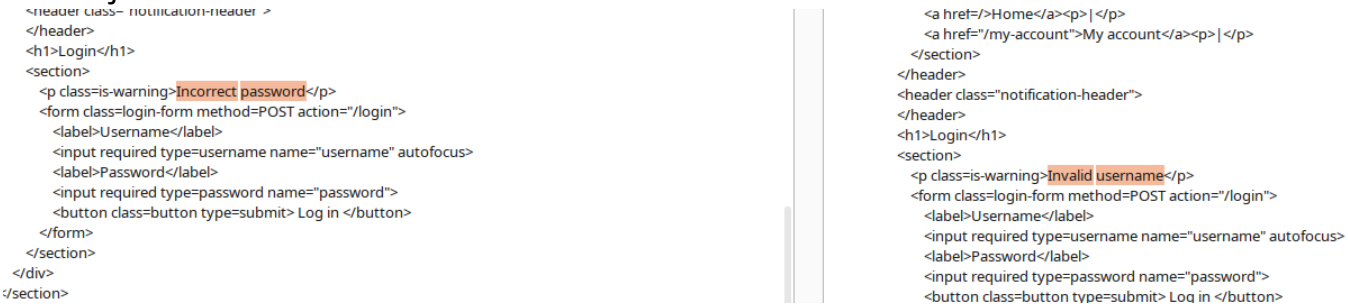
memiliki length yang berbeda dengan users lainya, ini bisa menjadi parameter bahwa user athena adalah user yang valid untuk langkah selnjutnya

bagaimana bisa, berikut saya lakukan komparasi antara users athena dengan length 3250 dengan users lain yang lengthnya adalah 3248

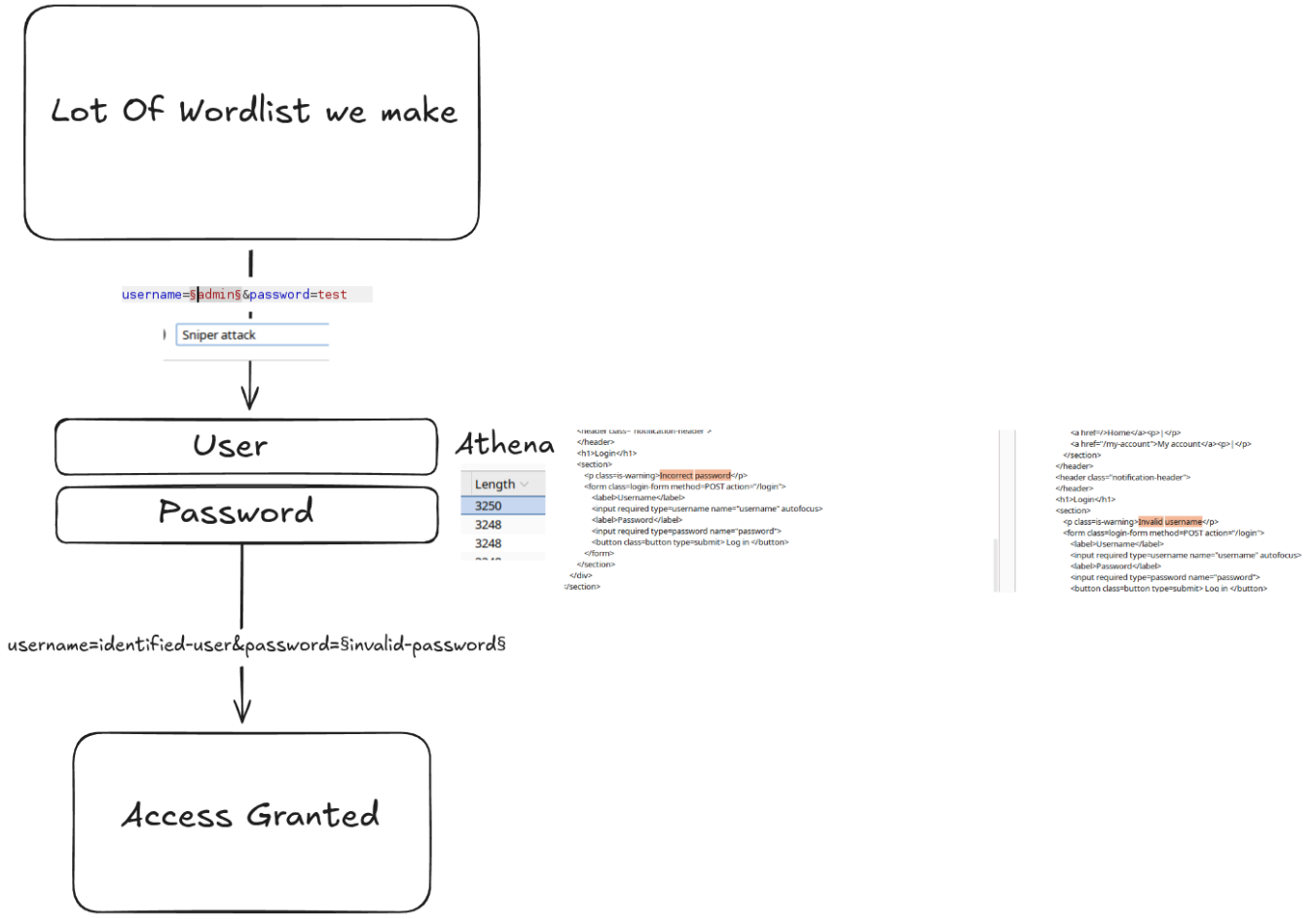


sebelah kiri adalah user athena dan sebelah kanan adalah users lainya.

menunjukan bahwa kata sandi dari user athena salah.



incorrect password, dan invalid username



sekarang kita hanya perlu menebak password dari user athena dengan wordlist password yang sudah di sediakan.

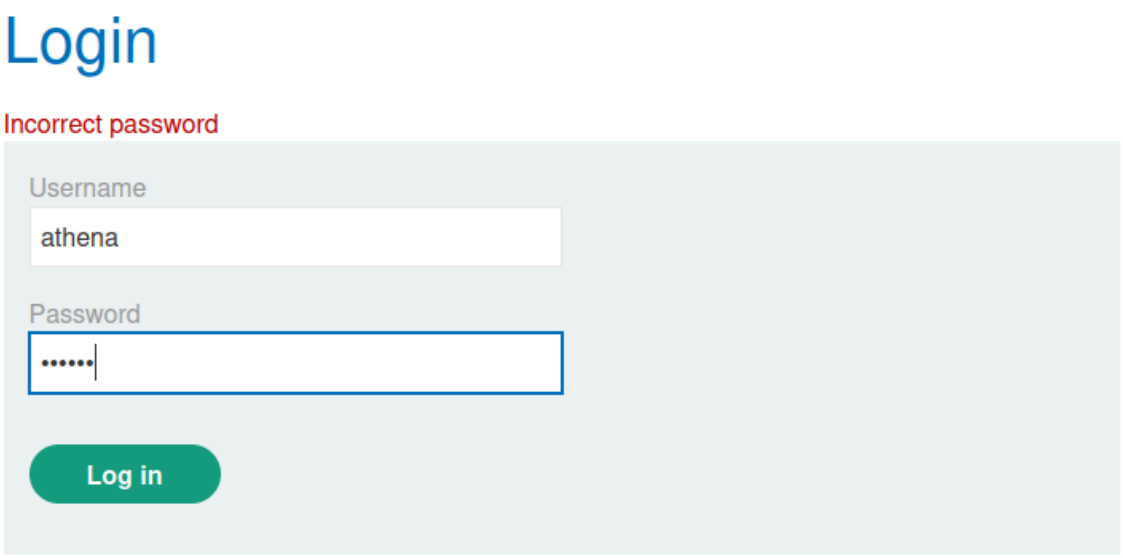
Status code	Response received	Error	Timeout	Length
302	202			188
200	212			3250

dan yap kami berhasil menemukan password yang tepat dan berhasil membuka session untuk user athena

```
username=athena&password=ashley
```

retty Raw Hex Render

```
HTTP/2 302 Found
Location: /my-account?id=athena
Set-Cookie: session=N3dRDXD8KFMIBIRDBG1N35dBry6KrJZq; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```



dan kami mencoba logi ke athena dengan password ashley

dan challenge pun selesai.