4. Brute Force Attack dengan Burp Suite

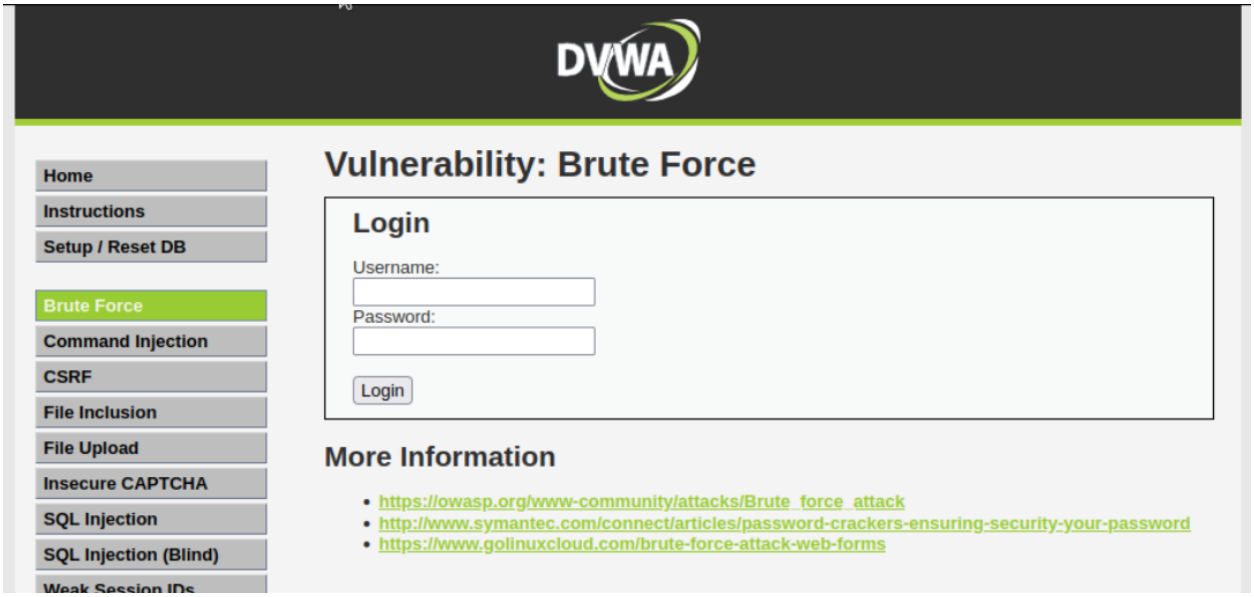
Disusun oleh :

Chaerul Umam, M.Kom (chaerul@dsn.dinus.ac.id)

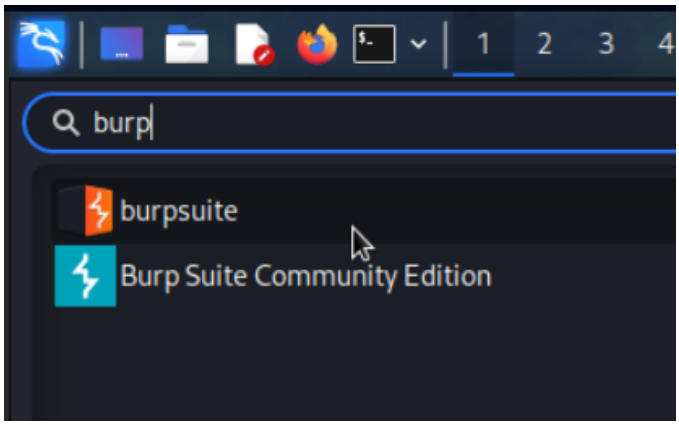
Hafiidh Akbar Sya'bani (akbar@dinustek.com)

☠️ Brute Force dengan Burp Suite

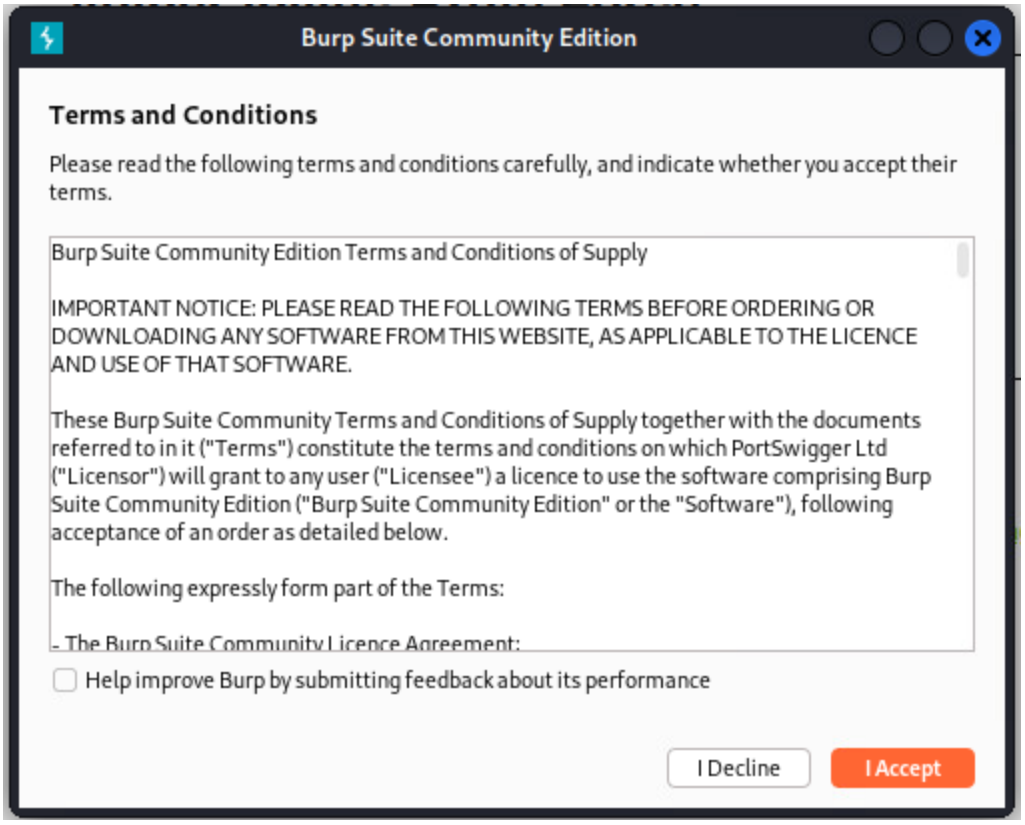
Pada tampilan awal DVWA klik bagian Brute Force



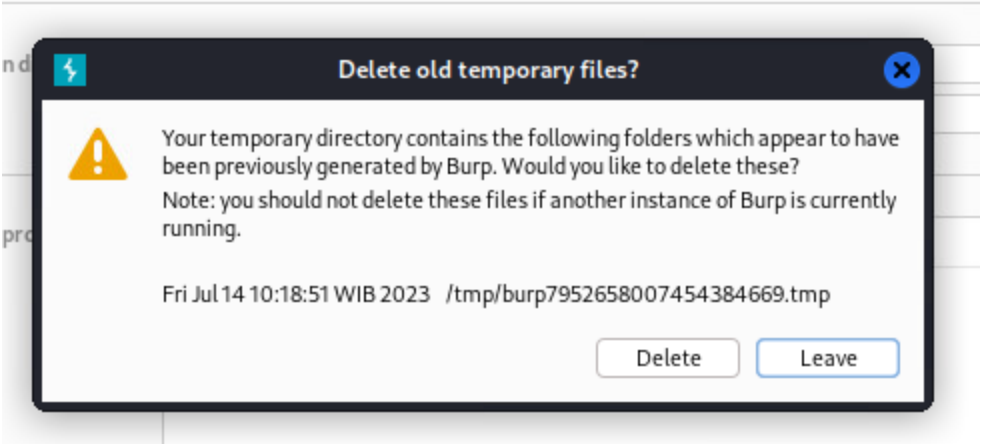
Buka Burp Suite



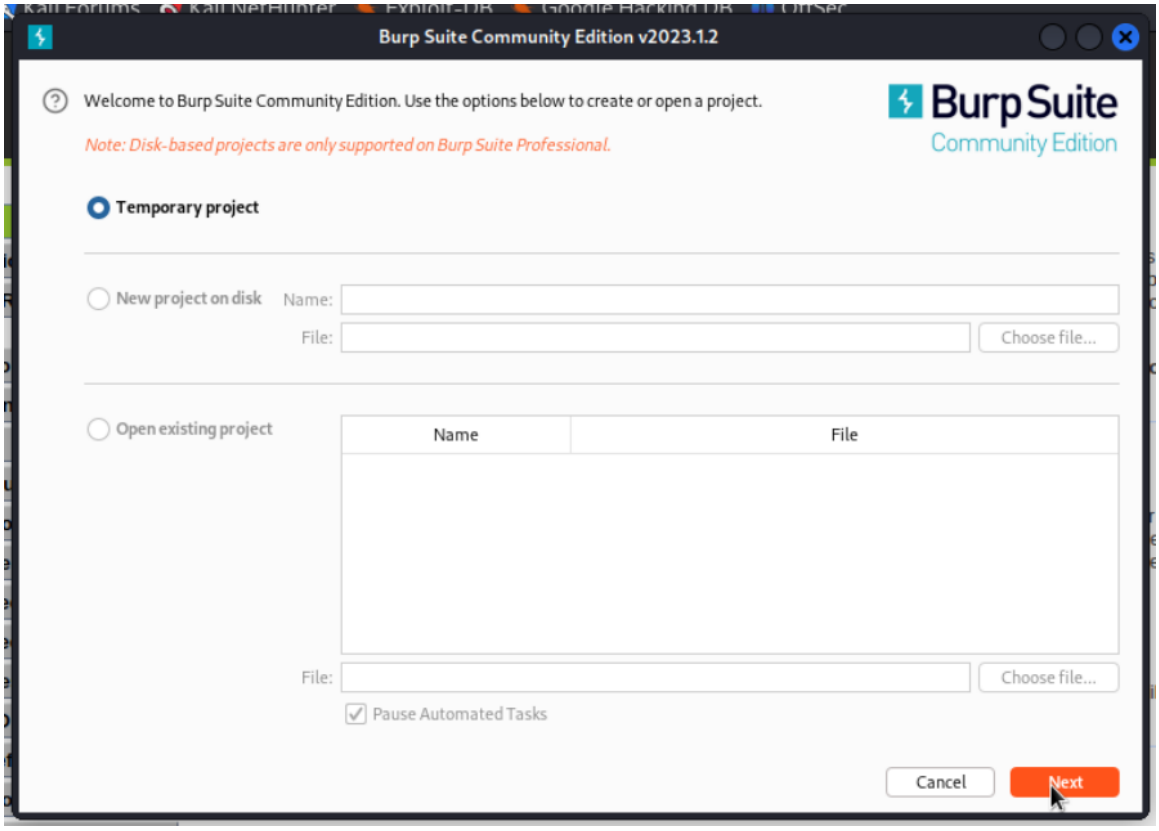
Klik I Accept



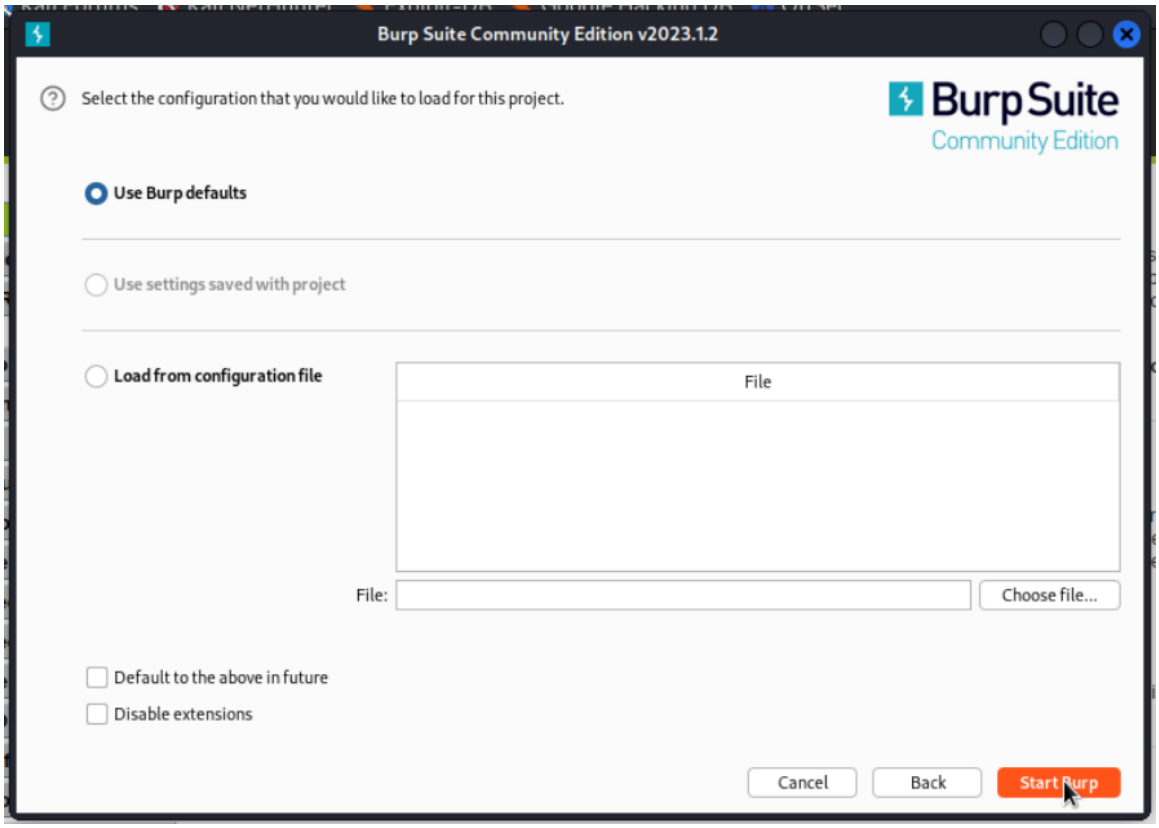
Klik Leave



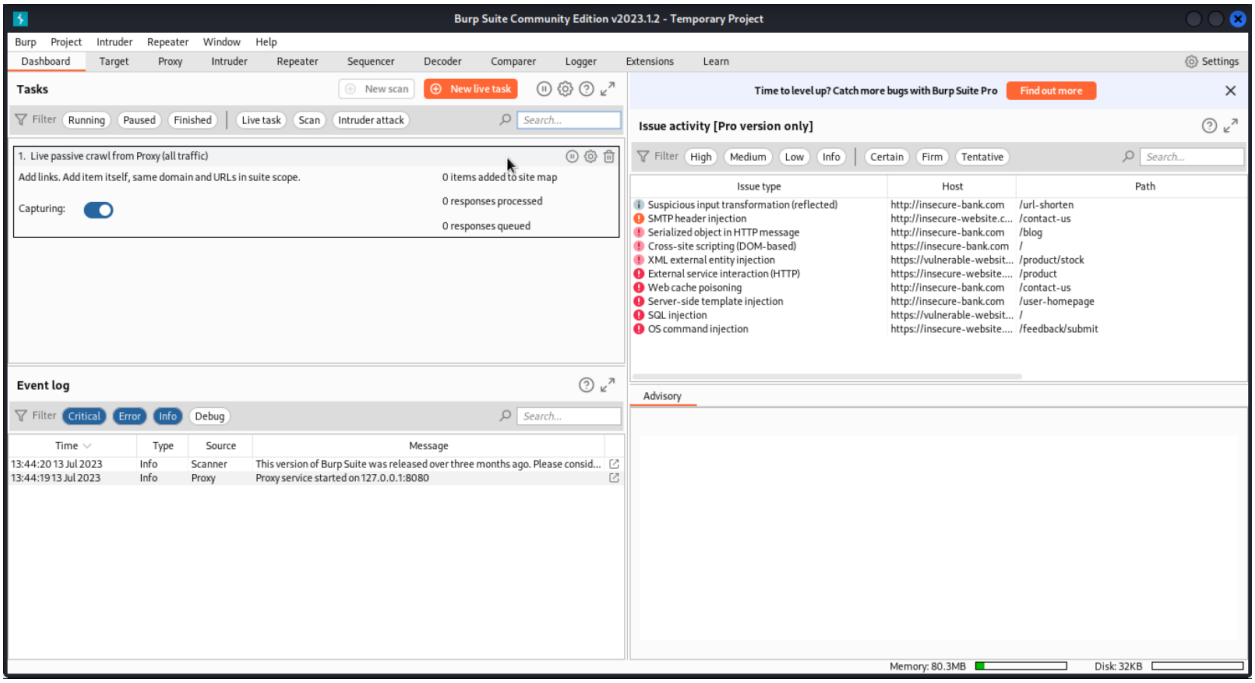
Klik next



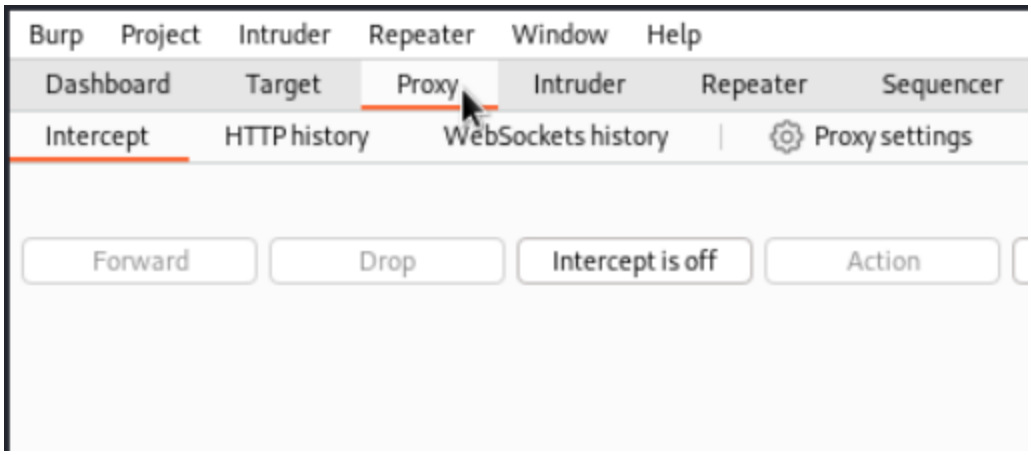
Klik Start Burp



Tampilan Burp Suite

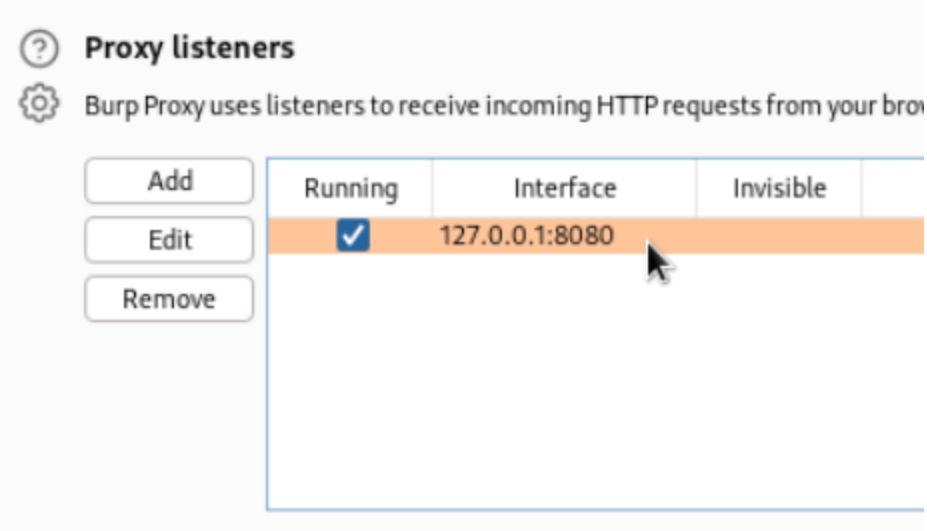


Klik tab Proxy

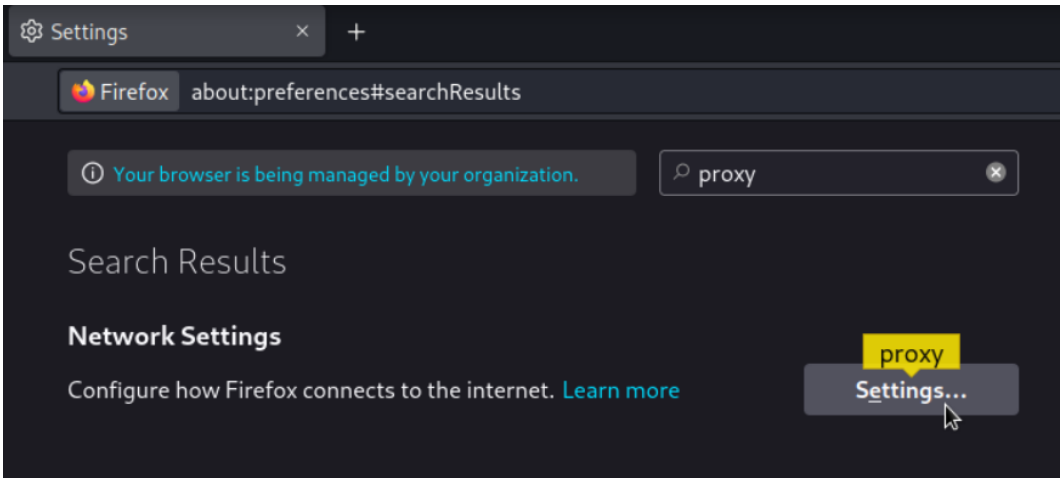


Klik Proxy settings dan pastikan pada Proxy listeners terdapat alamat IP dan port yang running

IP dan port ini yang nanti akan dijadikan proxy oleh browser

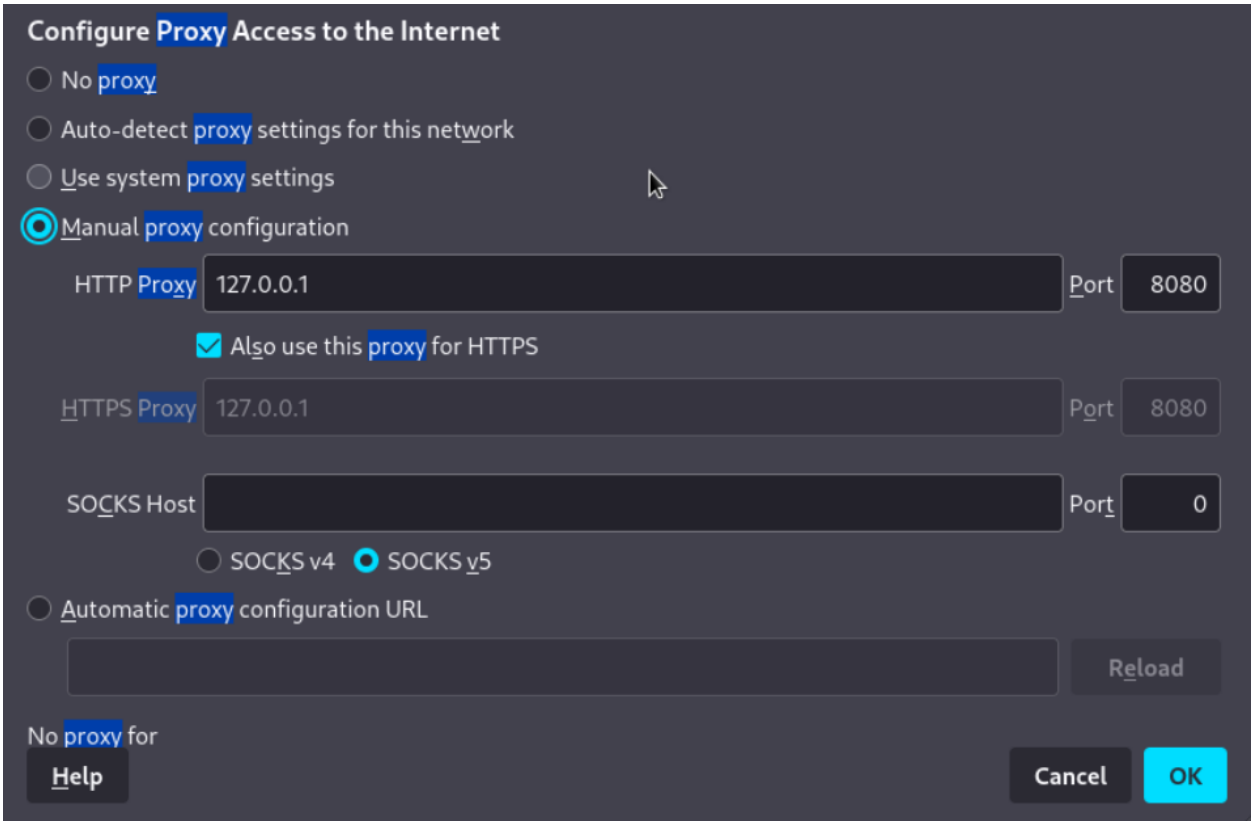


Kembali ke browser, pada Firefox masuk ke settings dan pada kolom pencarian ketikkan proxy

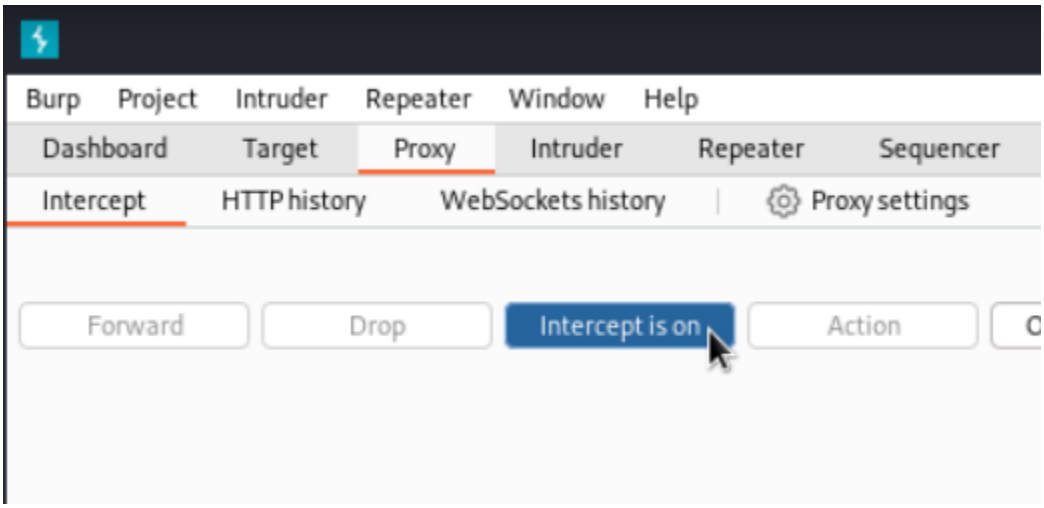


Didalamnya ganti “Use system proxy settings” menjadi “Manual proxy configuration”

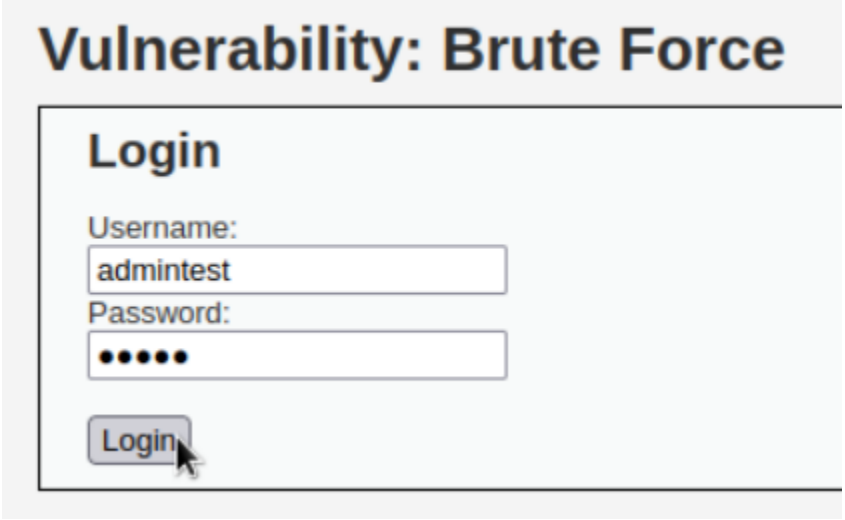
Pada HTTP Proxy masukkan IP dan Port yang sebelumnya didapat dari Burp Suite lalu klik OK



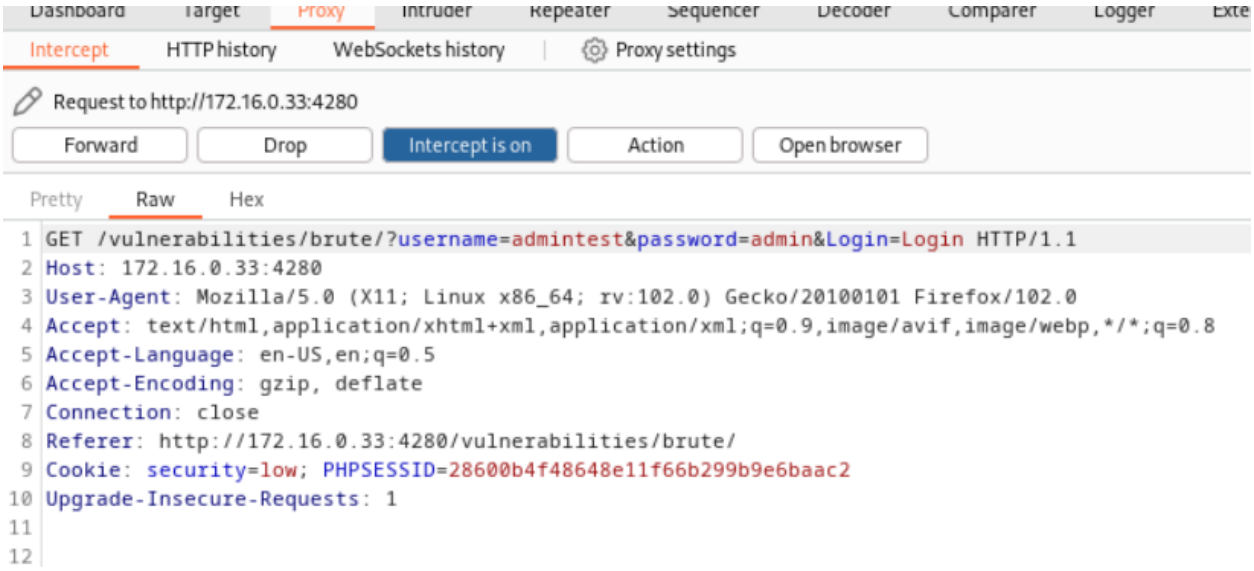
Buka Burp Suite, aktifkan intercept dengan klik tombol “Intercept is off”



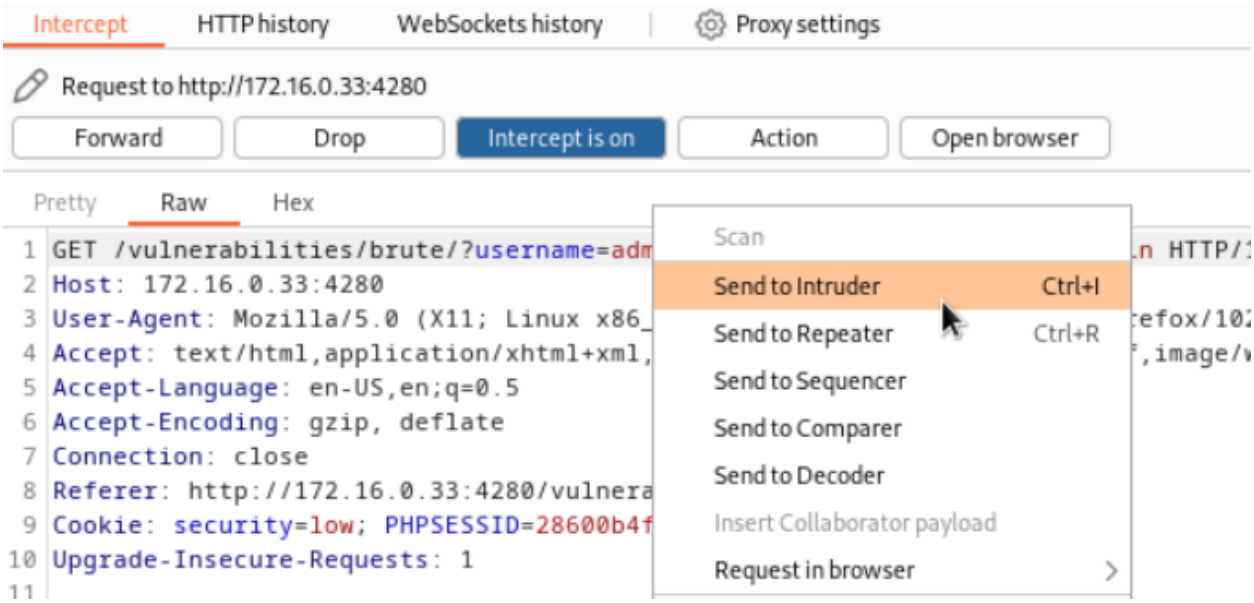
Kembali ke tab Brute Force DVWA, pada field username dan password isikan data apa saja lalu klik Login, ini hanya akan digunakan agar burp suite dapat melakukan intercept



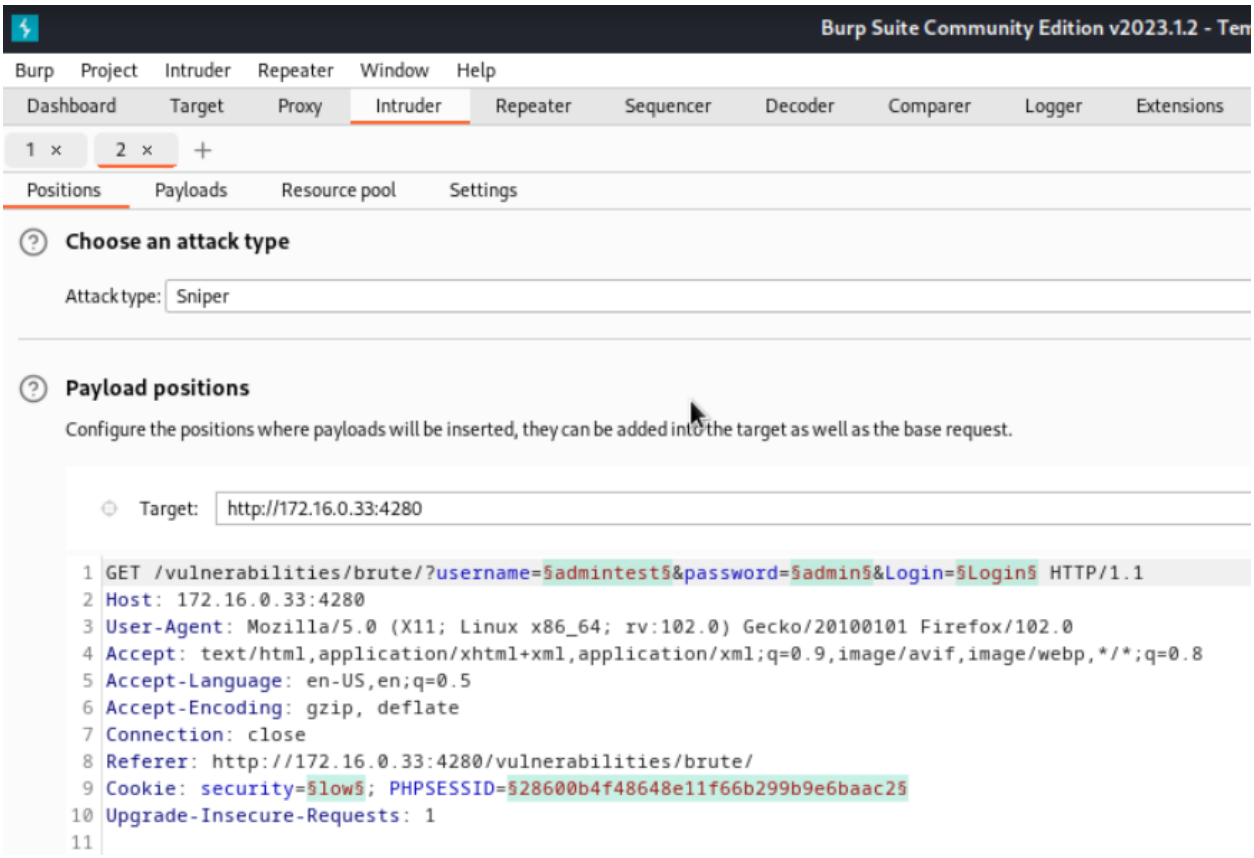
Saat tombol Login ditekan akan muncul pop up dari Burp Suite yang menampilkan hasil intercept. Di dalamnya pada baris 1 akan tampak data yang telah diinputkan pada field username dan password



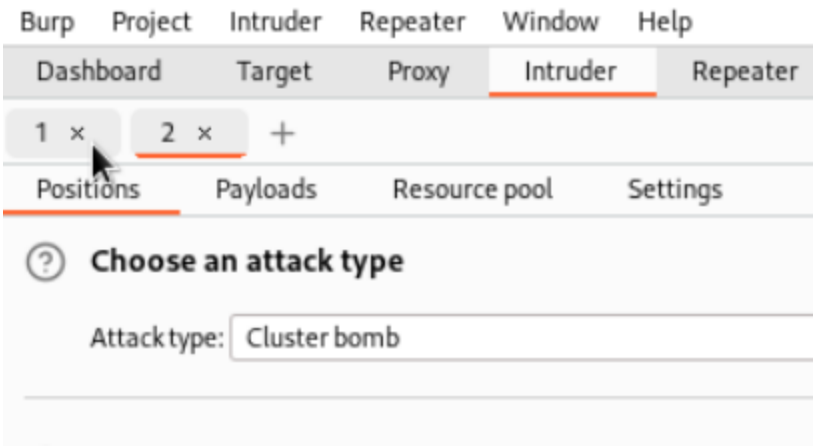
Klik kanan pada hasil intercept lalu pilih “Send to Intruder”



Pada tahap ini proses Intercept dapat dimatikan dan beralih ke tab Intruder



Ganti Attack type dari Sniper menjadi Cluster bomb



Ada beberapa yang harus di edit pada bagian Payload positions, jika diperhatikan ada text yang memiliki block hijau dan diawali dengan karakter ‘§’ pada awal dan akhir text.

```
GET /vulnerabilities/brute/?username=§admintest§&password=§admin§&Login=§Login§ HTTP/1.1
Host: 172.16.0.33:4280
```

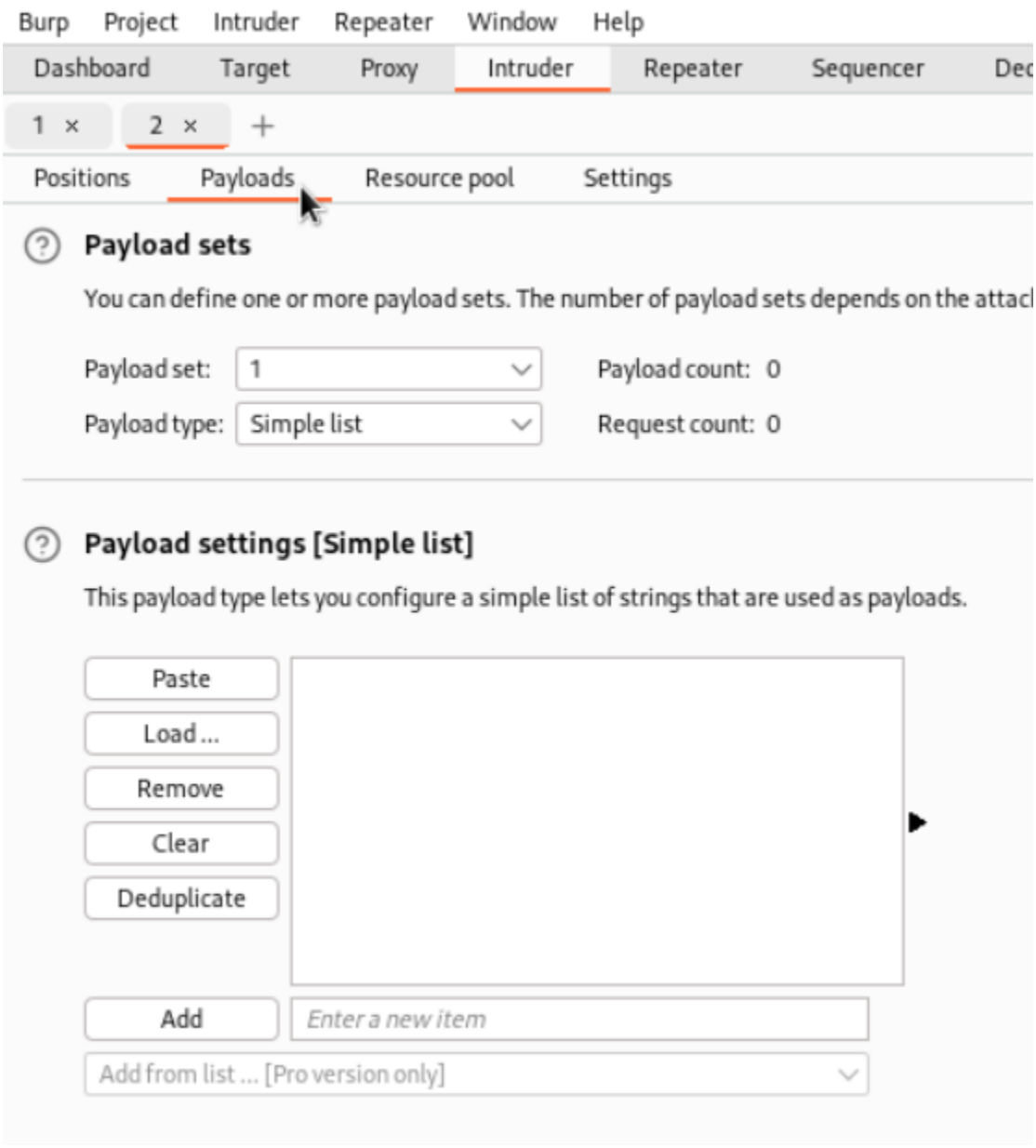
```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.0.33:4280/vulnerabilities/brute/
Cookie: security=§low§; PHPSESSID=§28600b4f48648e11f66b299b9e6baac2§
Upgrade-Insecure-Requests: 1
```

Burp suite membedakan text biasa dengan payload menggunakan karakter ‘§’, maka text yang memiliki awal dan akhiran karakter ‘§’ akan dianggap payload oleh Burp suite. Payload ini yang akan digunakan Burp suite sebagai target untuk dilakukannya brute force.

Karena fokus utama saat ini adalah untuk mendapatkan username dan password, maka hapus payload lain yang tidak diperlukan hingga hanya menyisakan payload username dan password.

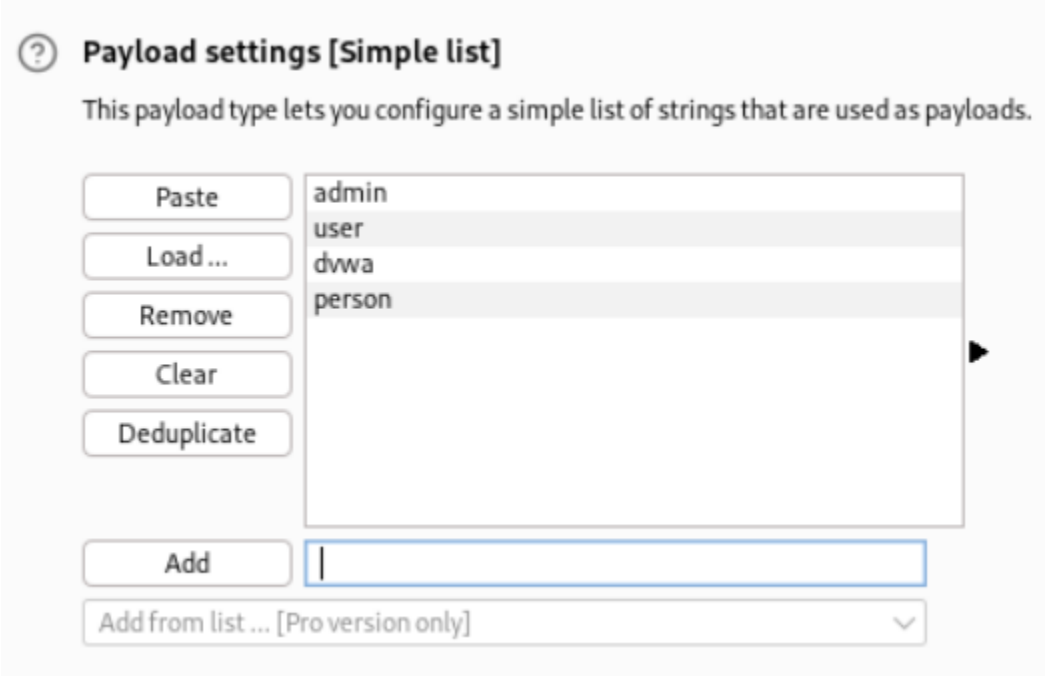
```
GET /vulnerabilities/brute/?username=§admintest§&password=§admin§&Login=Login HTTP/1.1
Host: 172.16.0.33:4280
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.0.33:4280/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=28600b4f48648e11f66b299b9e6baac2
Upgrade-Insecure-Requests: 1
```

Masuk ke tab Payloads

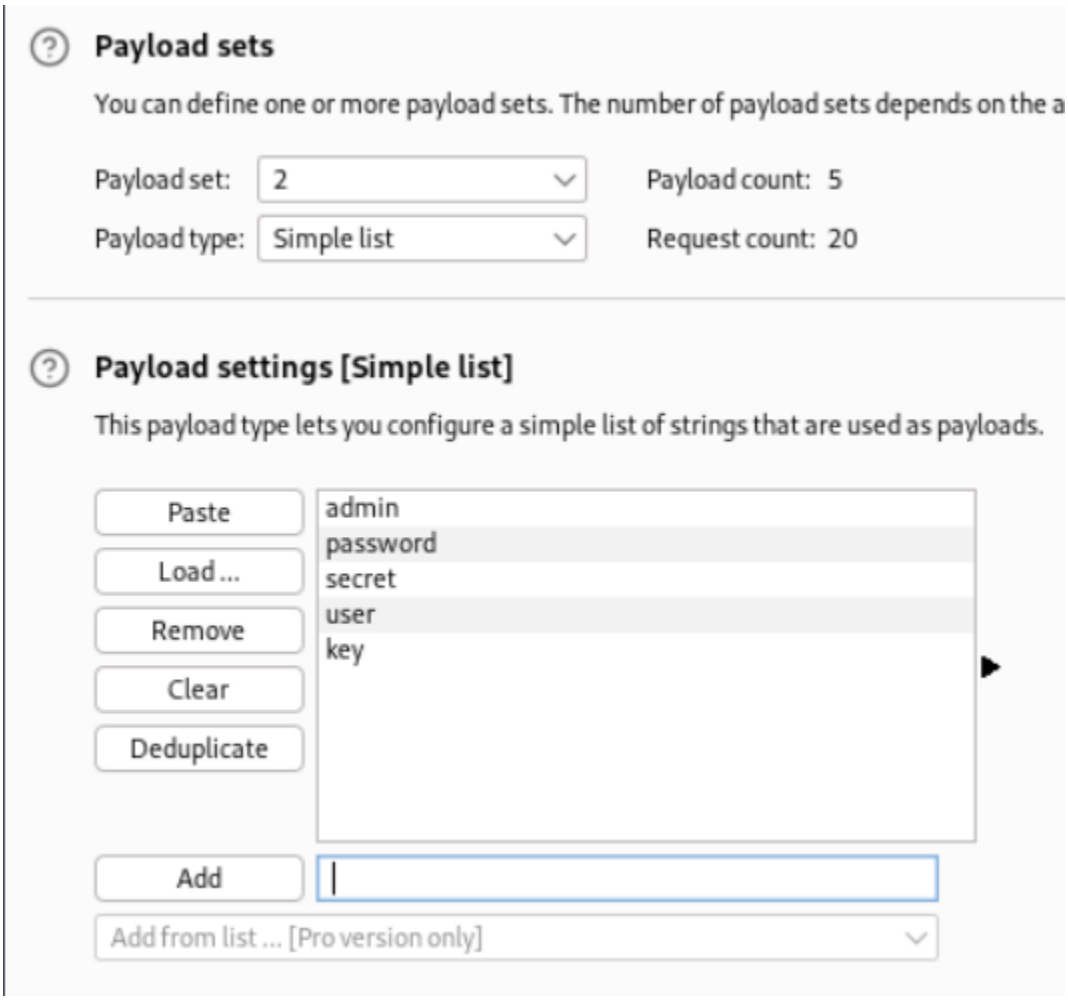


Pada Payload sets terdapat dropdown dengan value 1 dan 2, payload set 1 mewakili username dan 2 sebagai password. Untuk saat ini pilih payload set 1 untuk username.

Pada payload settings dapat diisikan dengan mengimport file word list atau daftar kata yang akan digunakan, atau bisa dibuat secara satu persatu dengan mengetikkan kata lalu klik Add.

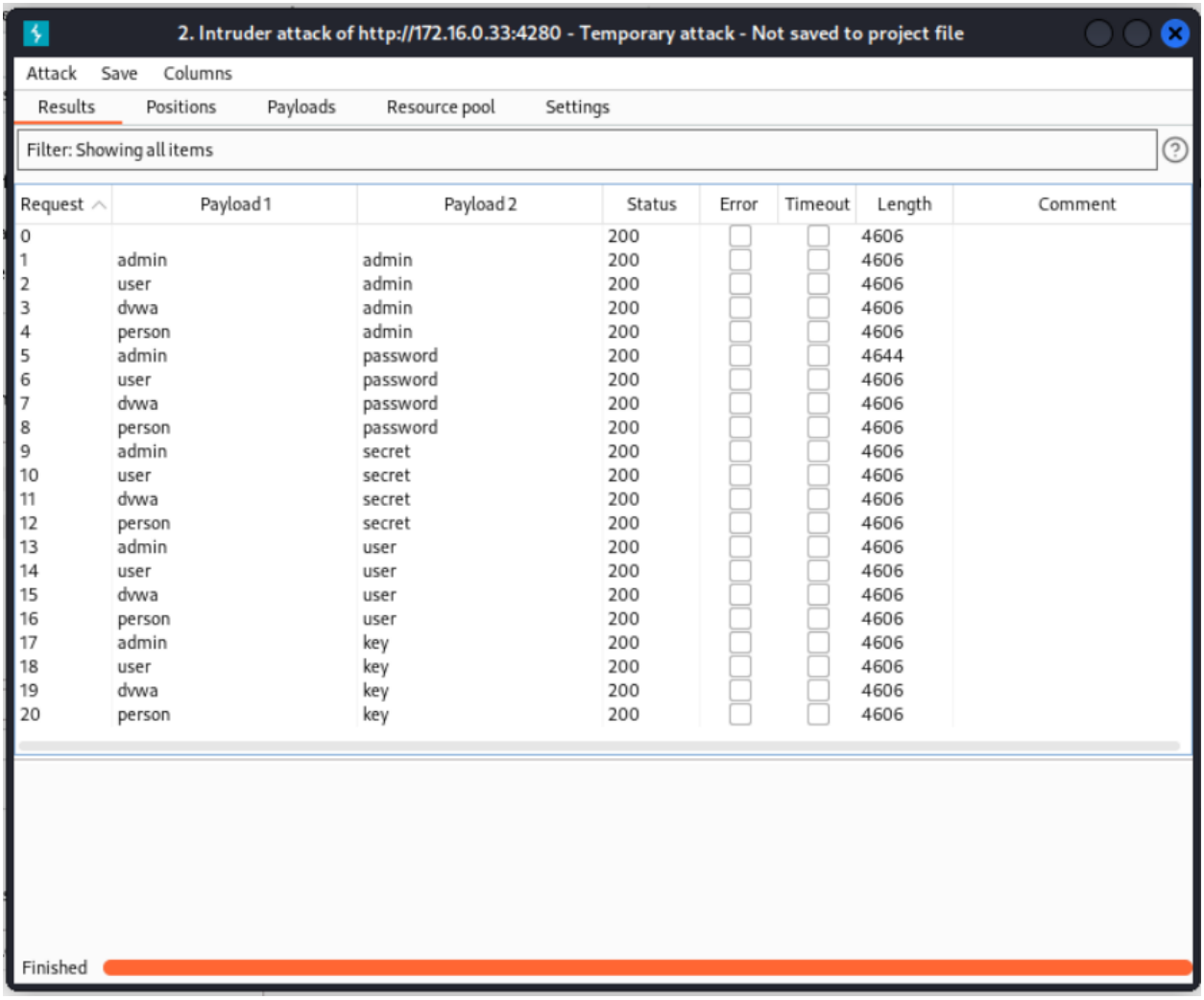


Setelah semua word list dimasukkan, selanjutnya beralih ke payload set 2 untuk menambahkan word list password. Sama seperti sebelumnya, word list dapat ditambahkan dengan mengimport file word list atau dengan diketik satu persatu.

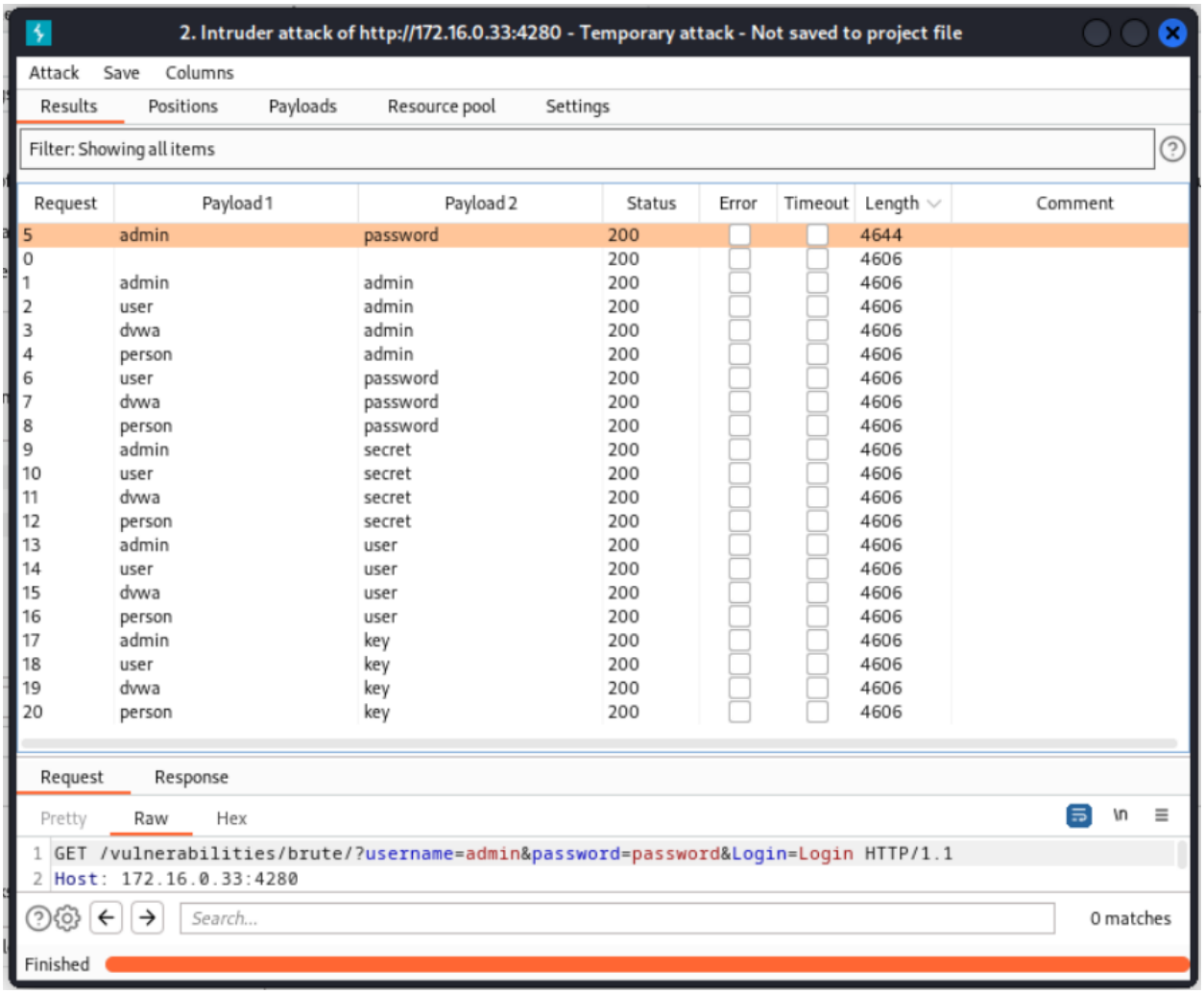


Jika semua payload sudah memiliki word list, maka selanjutnya lakukan brute force dengan klik tombol Start attack

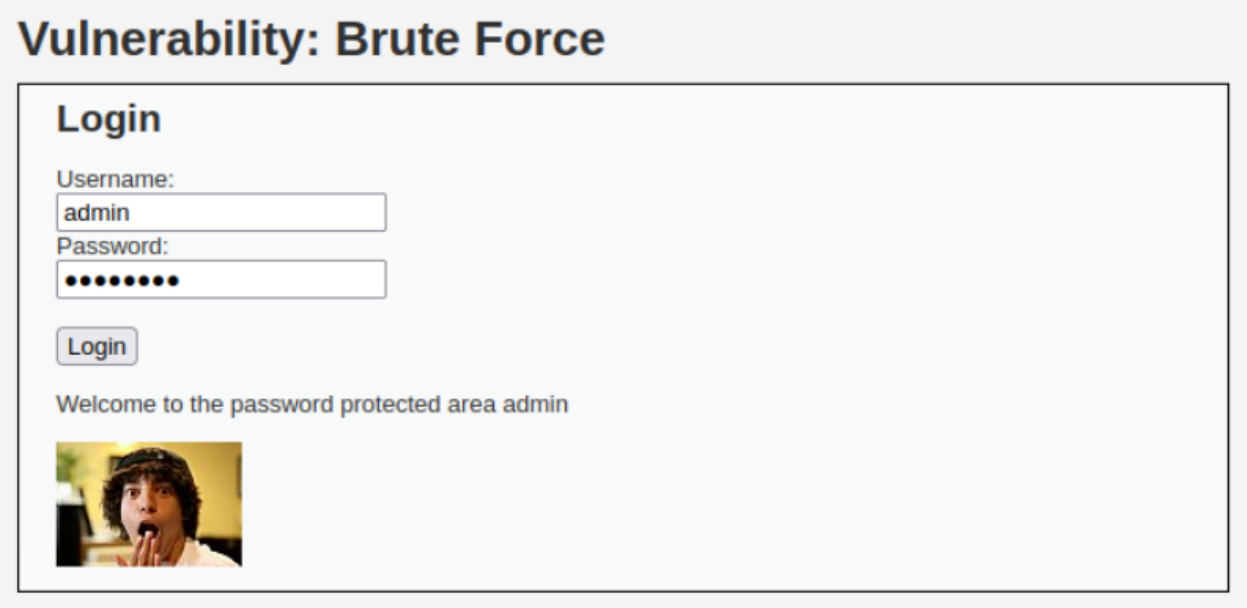
Selanjutnya Burp suite akan mencoba satu persatu kombinasi word list sebelumnya untuk diinputkan ke dalam field username dan password



Setelah proses brute force selesai untuk mengetahui username dan password yang benar dapat dilihat dari nilai “Length”, nilai yang berbeda dari yang lain merupakan kombinasi username dan password yang benar. Untuk mempermudah dalam pencarian, nilai Length dapat diurutkan dari yang terkecil ke terbesar atau sebaliknya.



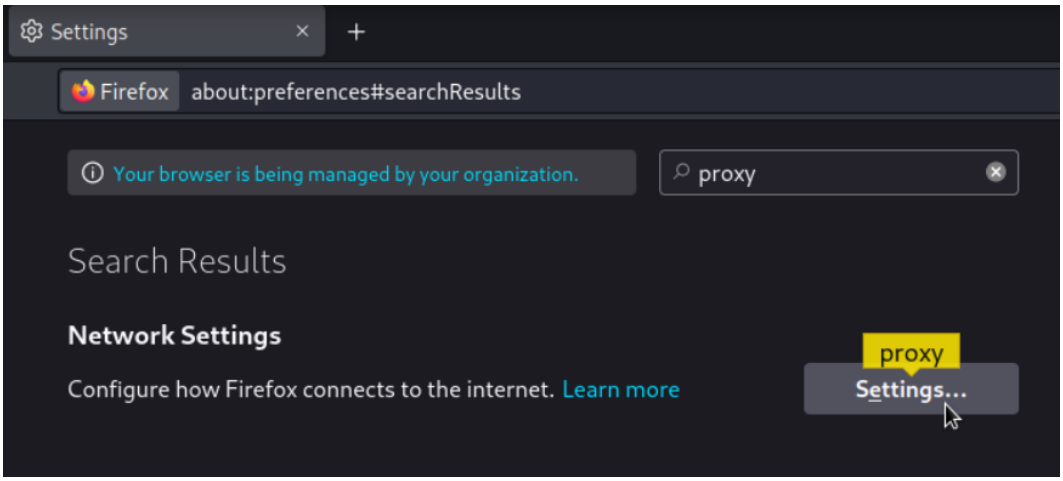
Lakukan pengujian dengan login ke halaman DVWA-Brute Force menggunakan kombinasi username dan password yang telah ditemukan



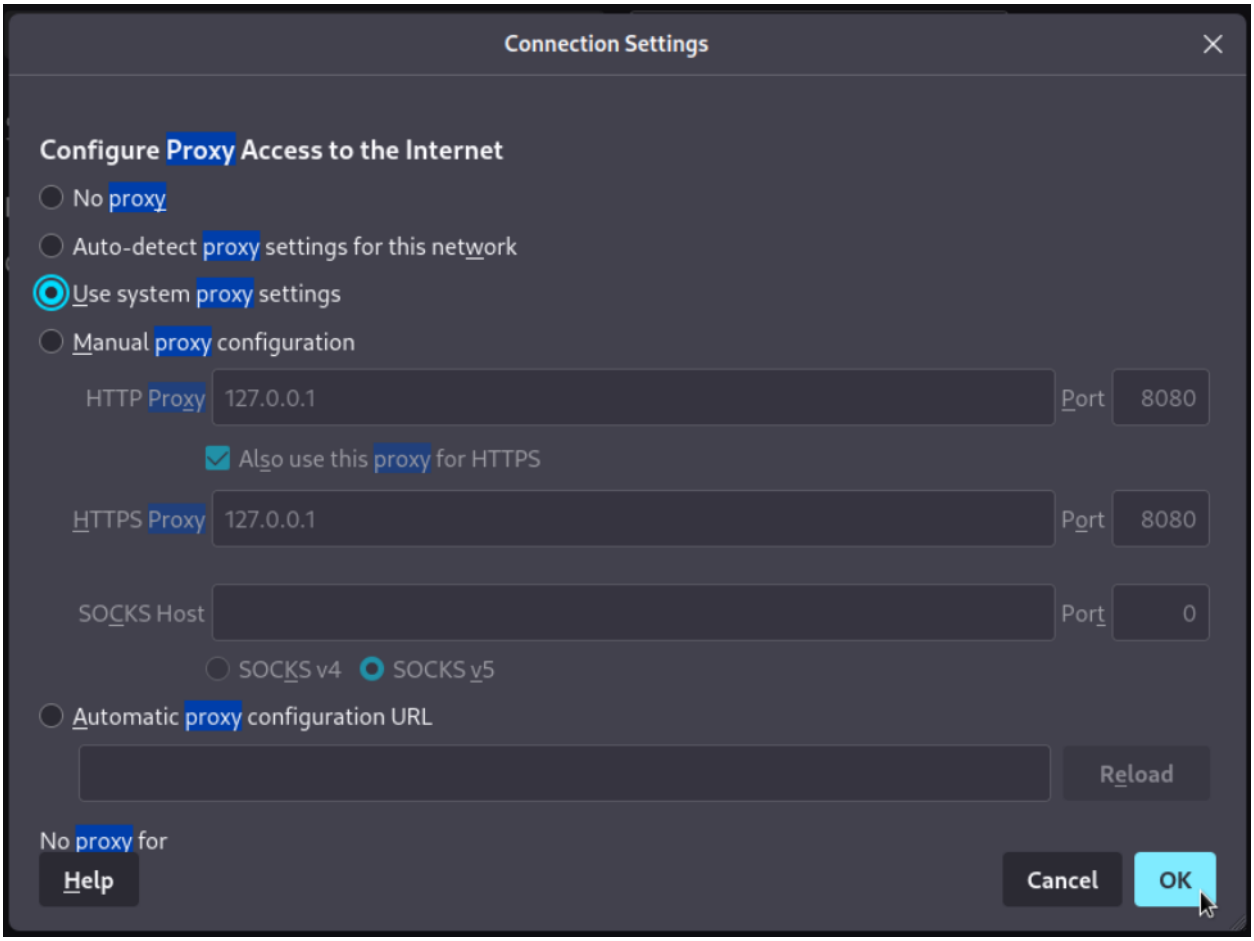
🧹 Clean up

Kembalikan setting proxy seperti semula pada browser

Masuk ke browser, pada Firefox masuk ke settings dan pada kolom pencarian ketikkan proxy



Didalamnya ganti “Manual proxy configuration” menjadi “Use system proxy settings” lalu klik OK



Note

- Metode Brute Force sangat bergantung pada word list
- Proses Brute Force akan semakin lama jika word list atau daftar kata yang digunakan semakin banyak
- Sebanyak apapun word list jika username dan password yang benar tidak terdapat dalam word list tersebut, maka metode brute force tidak akan berhasil