

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)

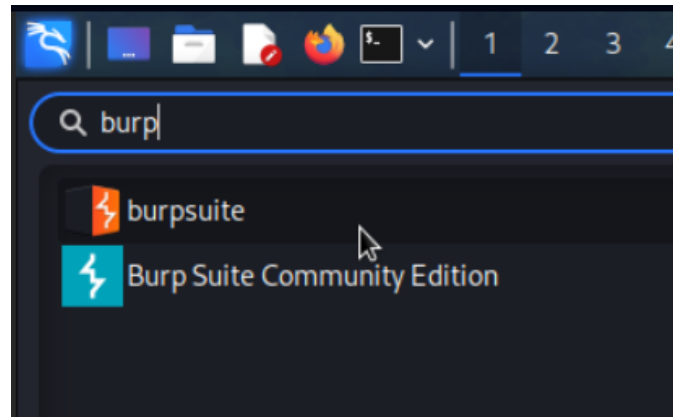


Brute Force dengan Burp Suite

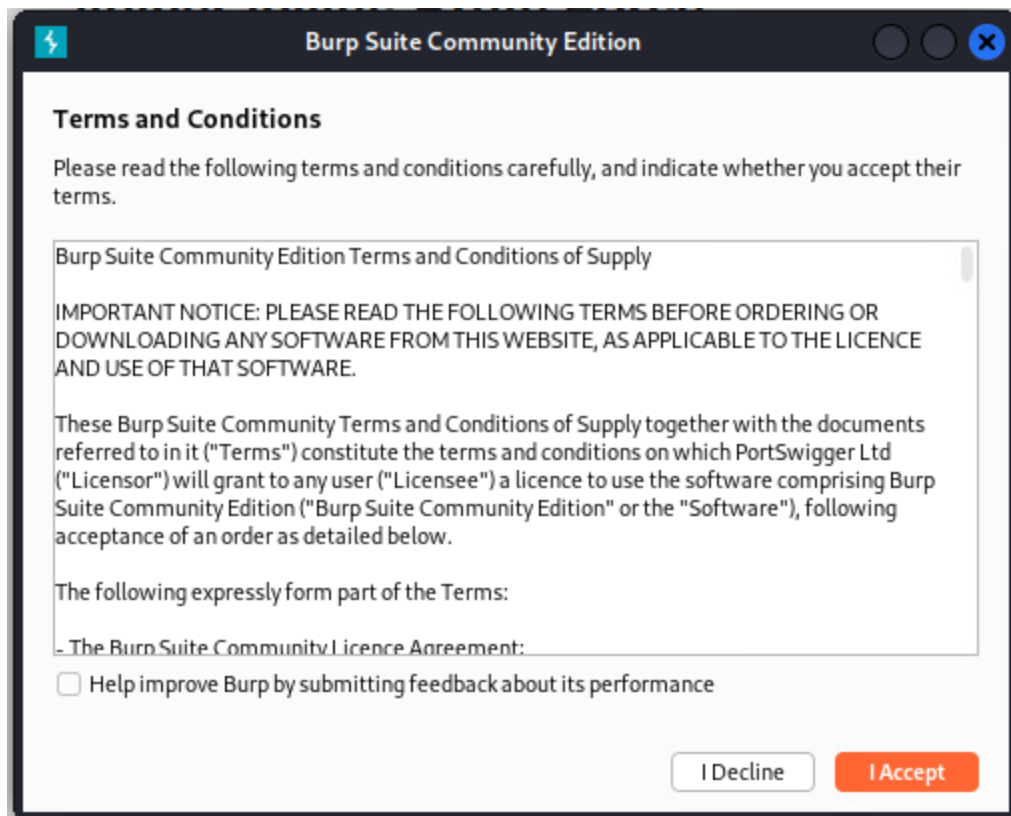
Pada tampilan awal DVWA klik bagian Brute Force

The screenshot shows the DVWA web application interface. At the top, there is a dark header with the DVWA logo. Below the header, on the left, is a sidebar menu with buttons for 'Home', 'Instructions', 'Setup / Reset DB', 'Brute Force' (which is highlighted in green), 'Command Injection', 'CSRF', 'File Inclusion', 'File Upload', 'Insecure CAPTCHA', 'SQL Injection', 'SQL Injection (Blind)', and 'Weak Session IDs'. The main content area is titled 'Vulnerability: Brute Force'. It contains a 'Login' form with fields for 'Username:' and 'Password:', and a 'Login' button. Below the form, there is a section titled 'More Information' with three links: https://owasp.org/www-community/attacks/Brute_force_attack, <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>, and <https://www.golinuxcloud.com/brute-force-attack-web-forms>.

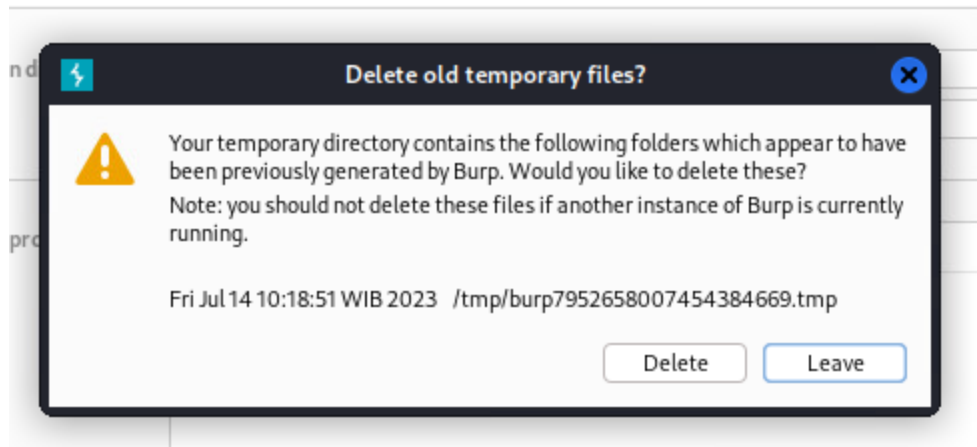
Buka Burp Suite



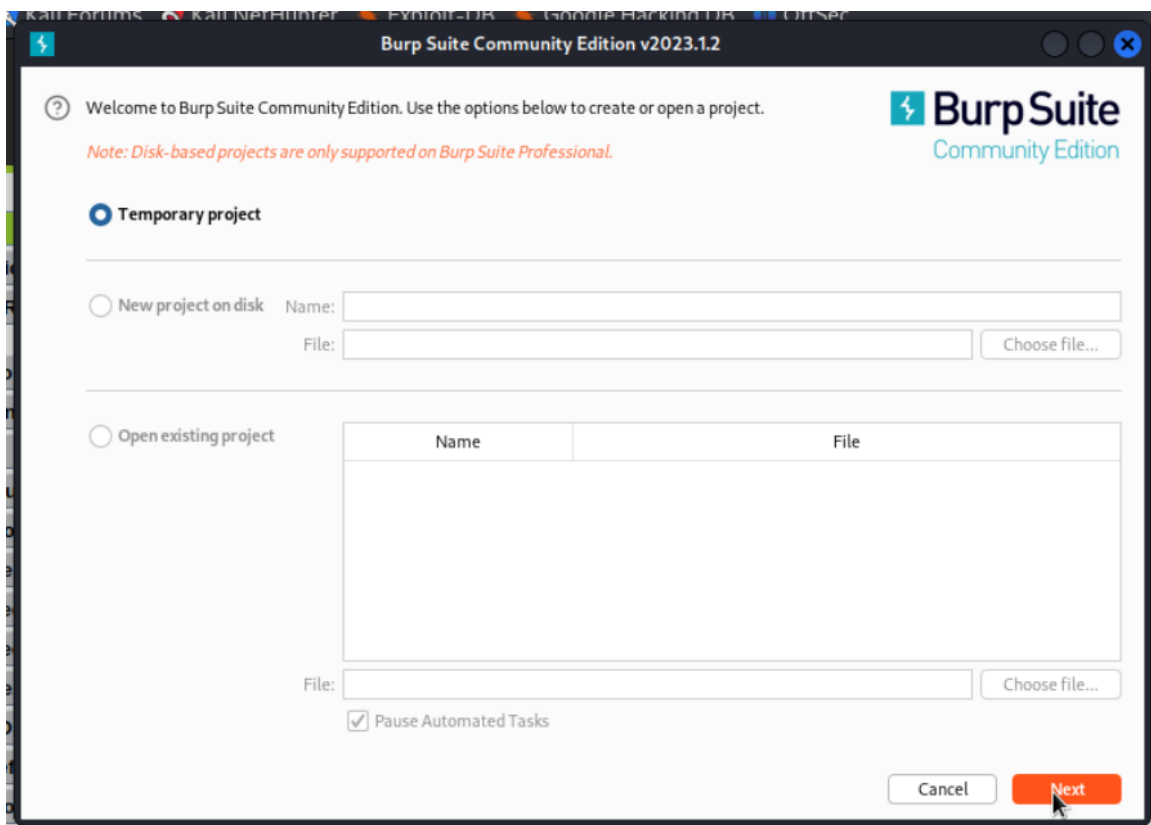
Klik I Accept



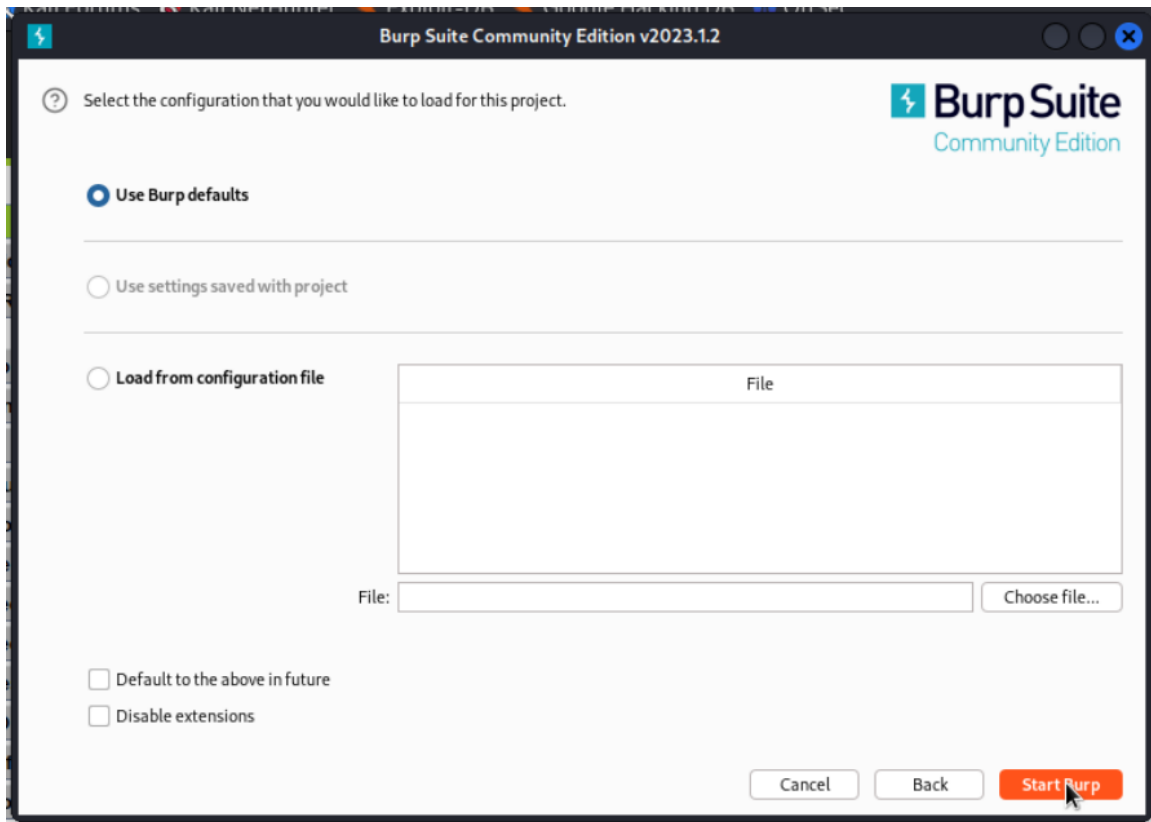
Klik Leave



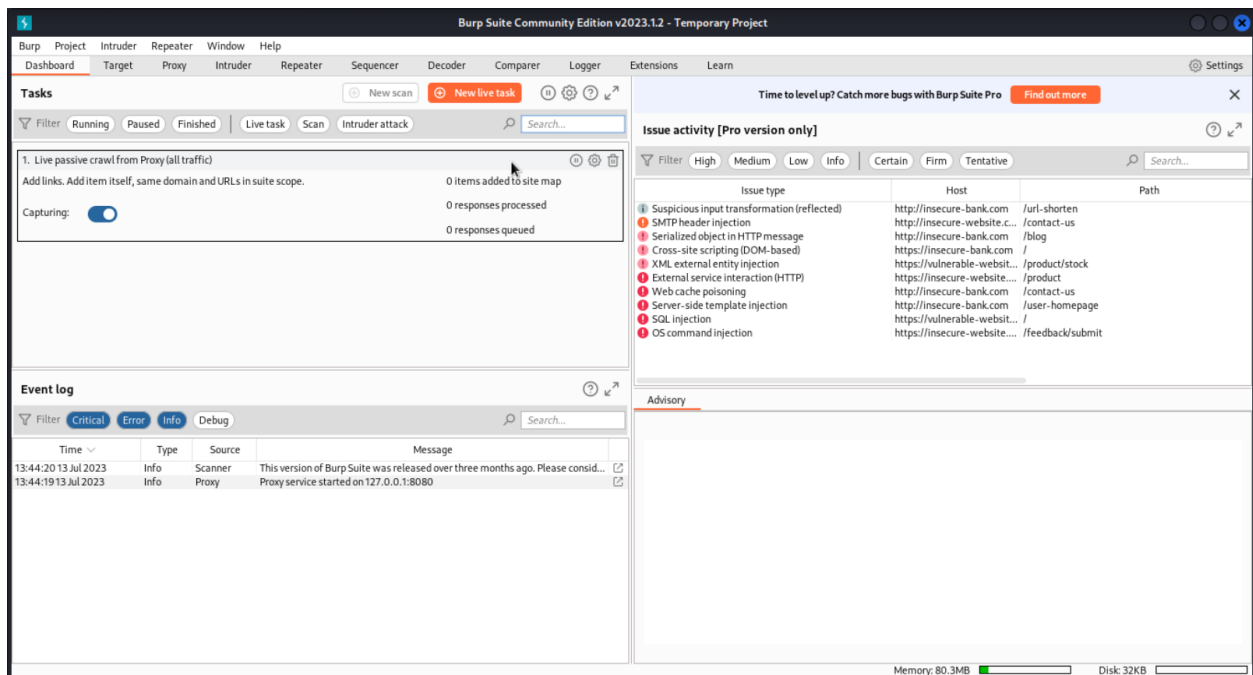
Klik next



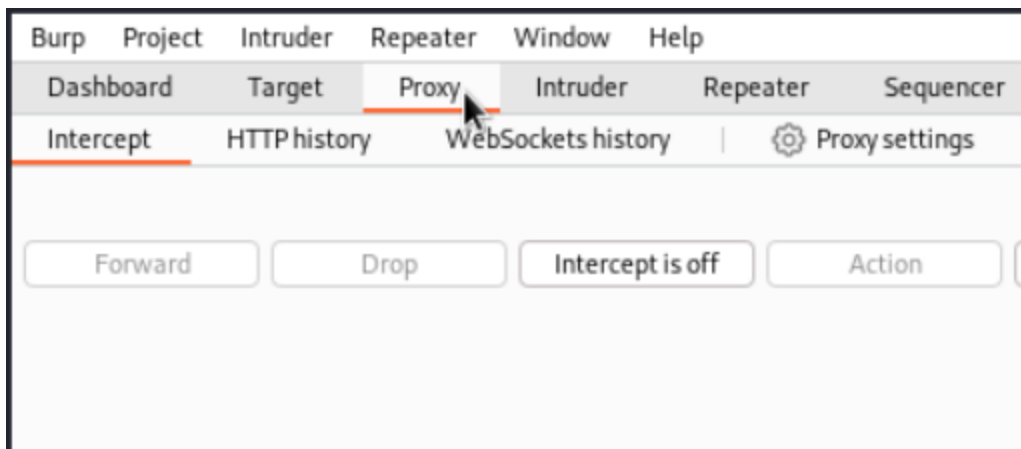
Klik Start Burp



Tampilan Burp Suite

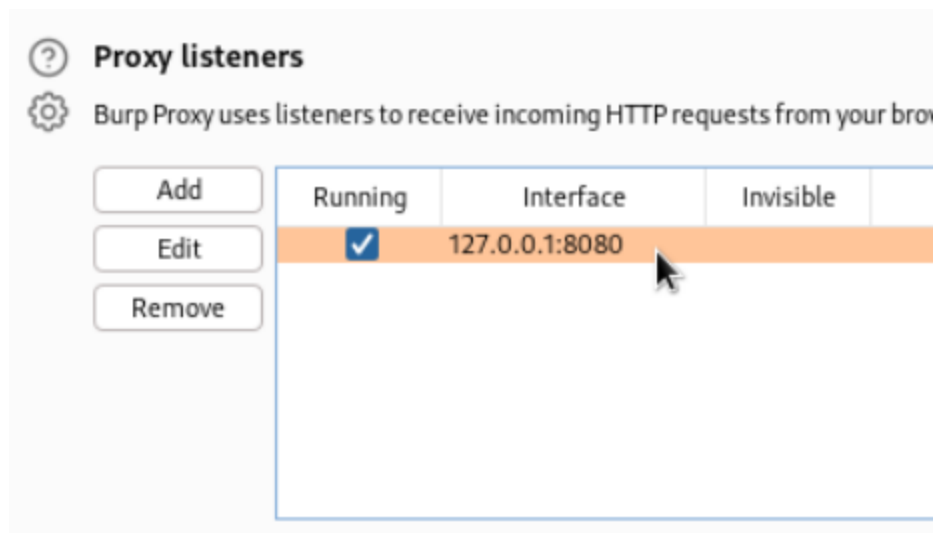


Klik tab Proxy

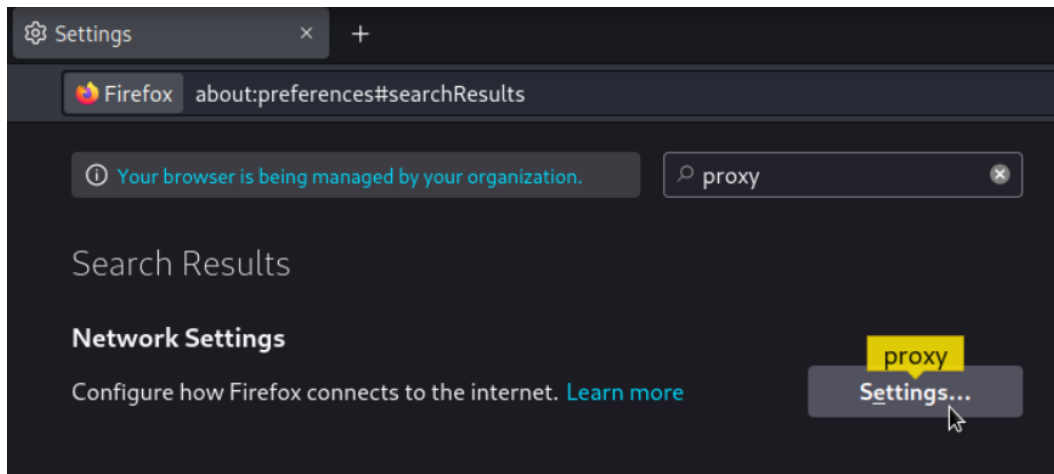


Klik Proxy settings and pastikan pada Proxy listeners terdapat alamat IP dan port yang running

IP dan port ini yang nanti akan dijadikan proxy oleh browser

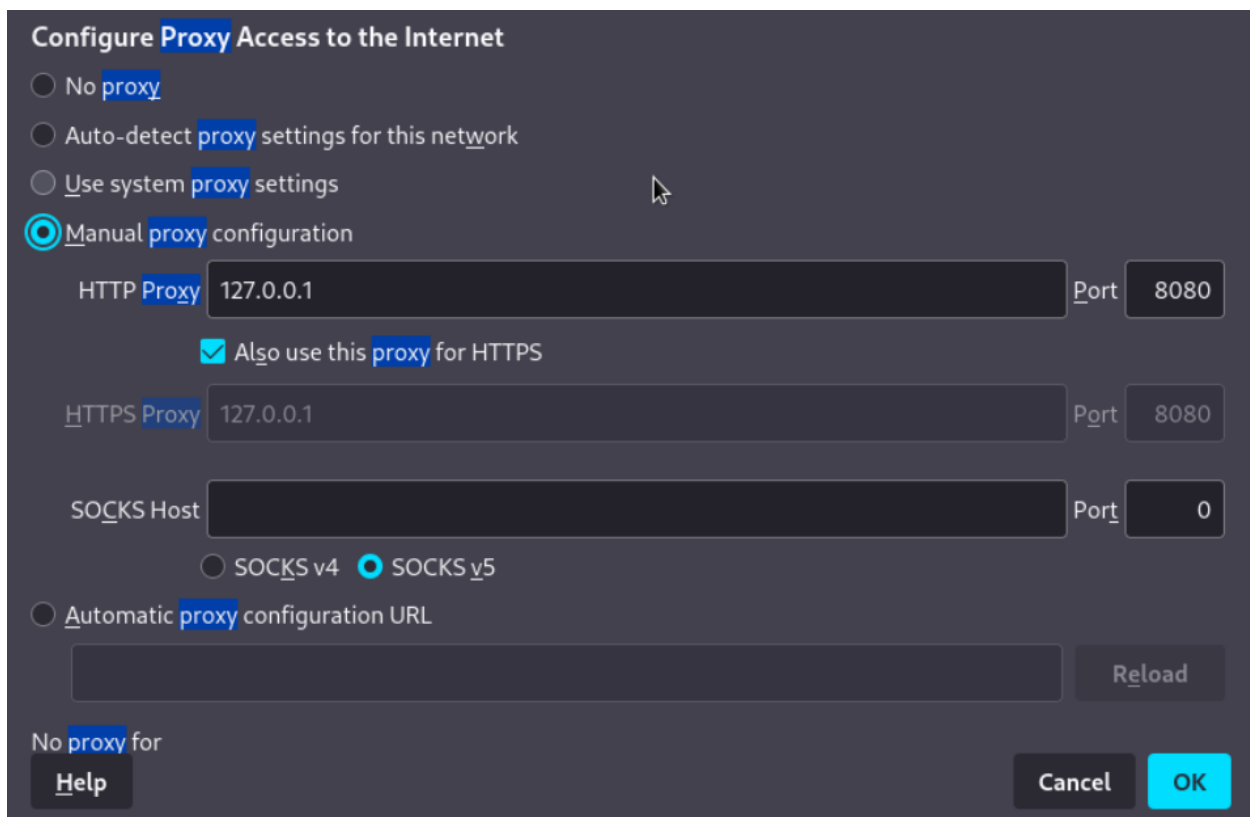


Kembali ke browser, pada Firefox masuk ke settings dan pada kolom pencarian ketikkan proxy

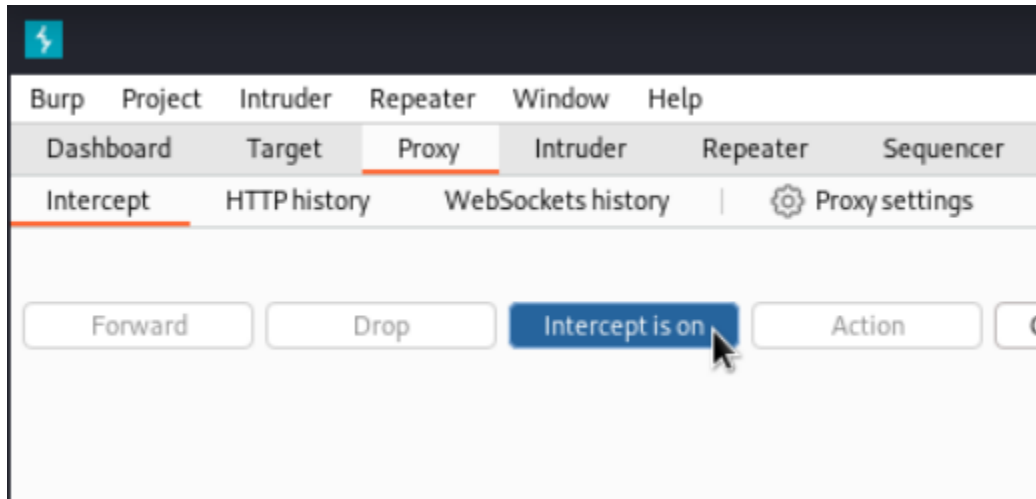


Didalamnya ganti “Use system proxy settings” menjadi “Manual proxy configuration”

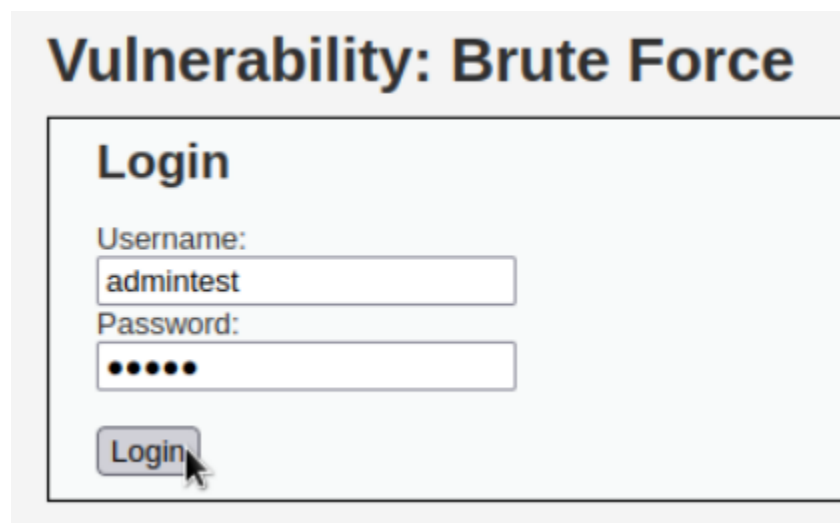
Pada HTTP Proxy masukkan IP dan Port yang sebelumnya didapat dari Burp Suite lalu klik OK



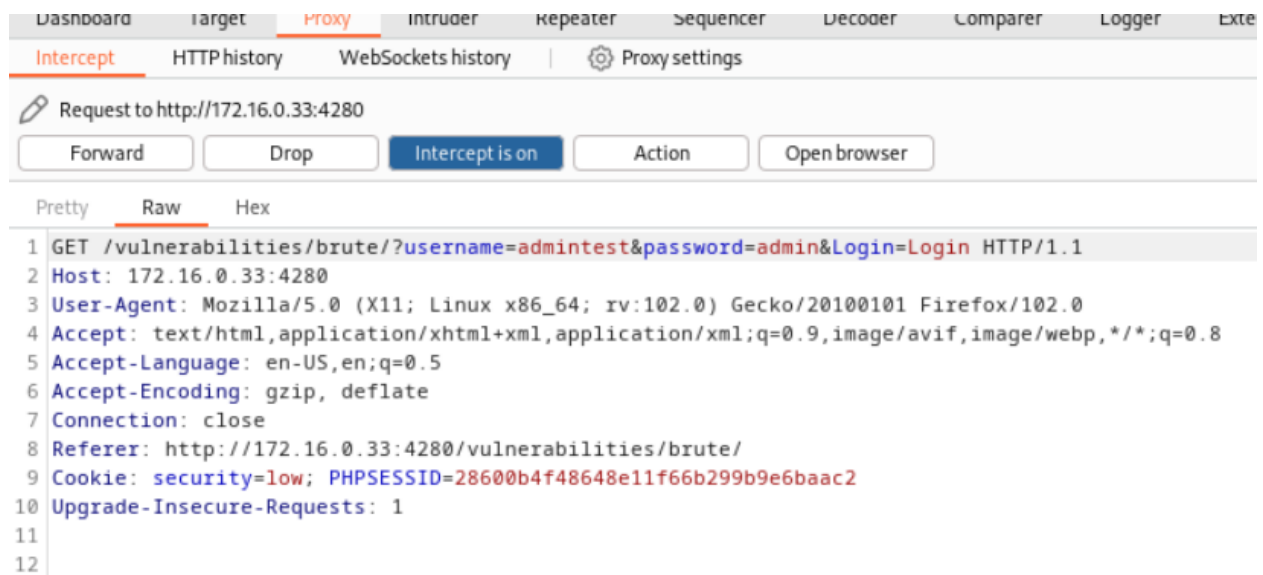
Buka Burp Suite, aktifkan intercept dengan klik tombol “Intercept is off”



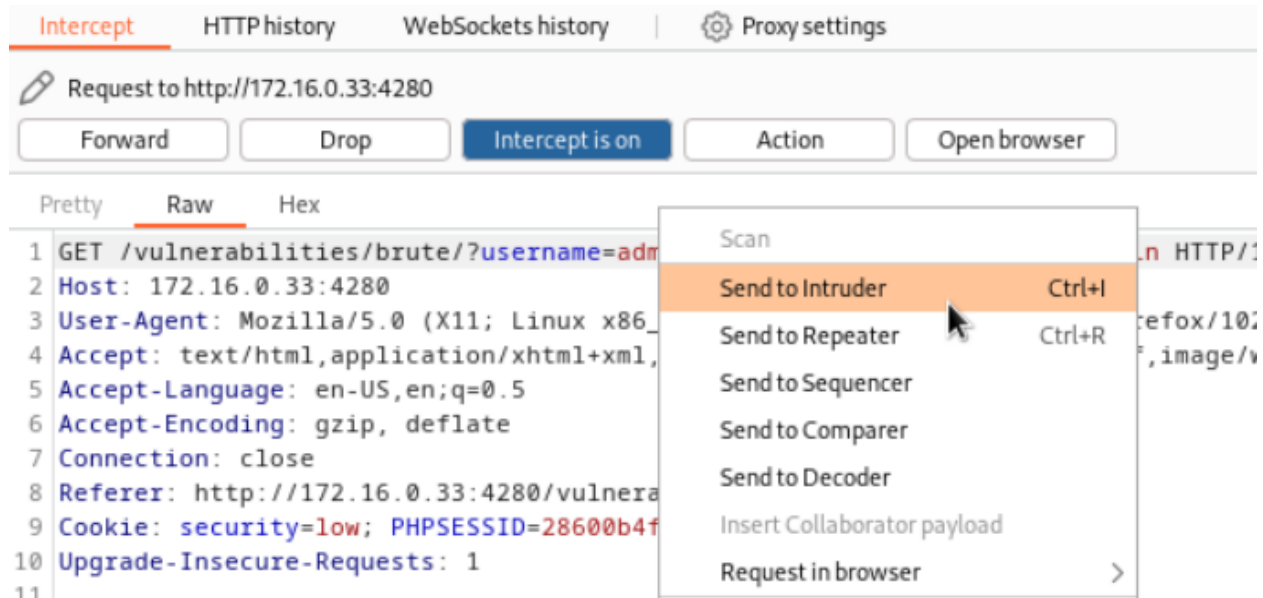
Kembali ke tab Brute Force DVWA, pada field username dan password isikan data apa saja lalu klik Login, ini hanya akan digunakan agar burp suite dapat melakukan intercept



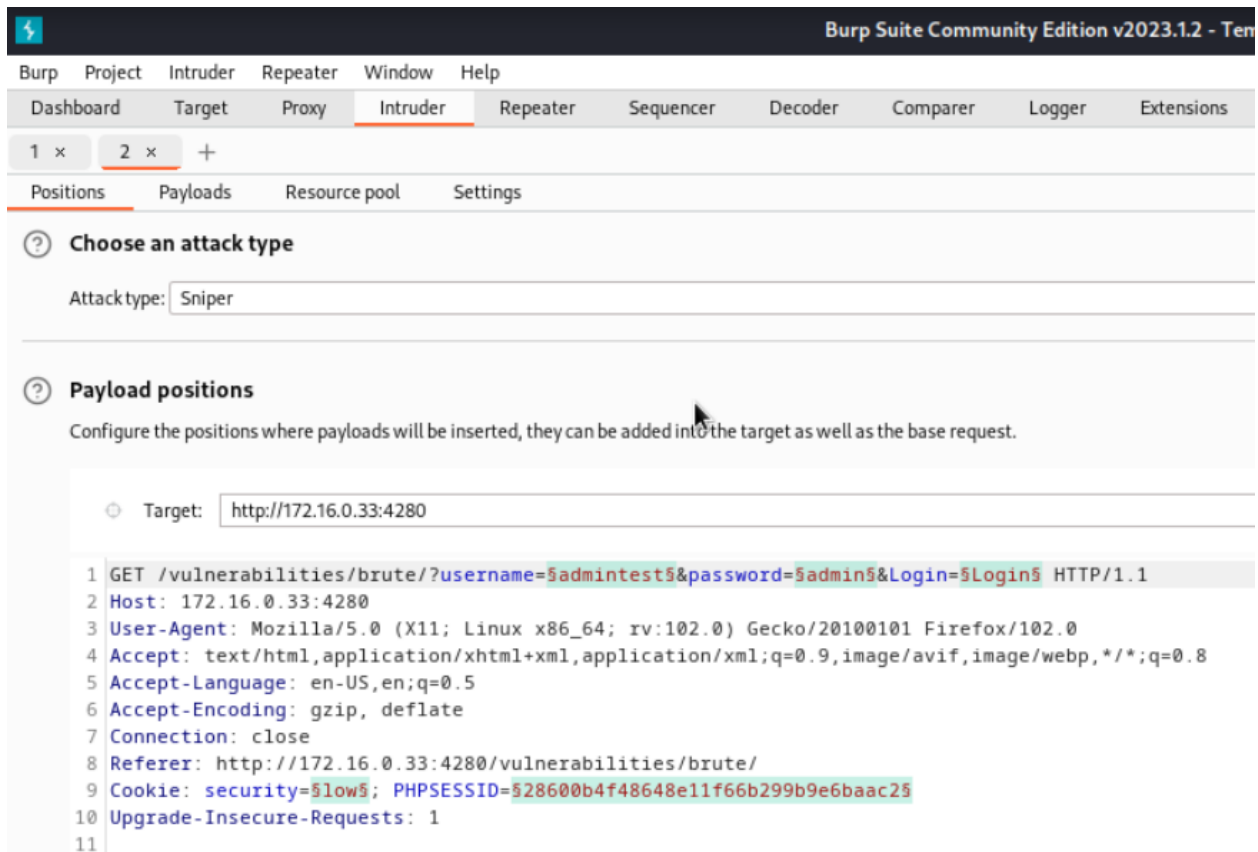
Saat tombol Login ditekan akan muncul pop up dari Burp Suite yang menampilkan hasil intercept. Di dalamnya pada baris 1 akan tampak data yang telah diinputkan pada field username dan password



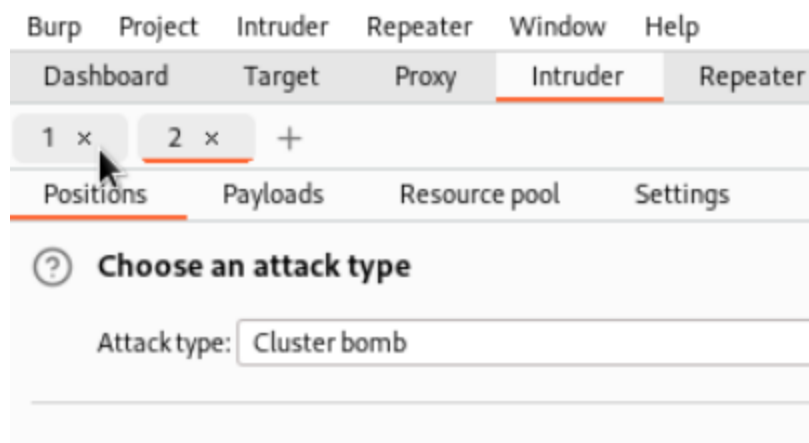
Klik kanan pada hasil intercept lalu pilih “Send to Intruder”



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

```

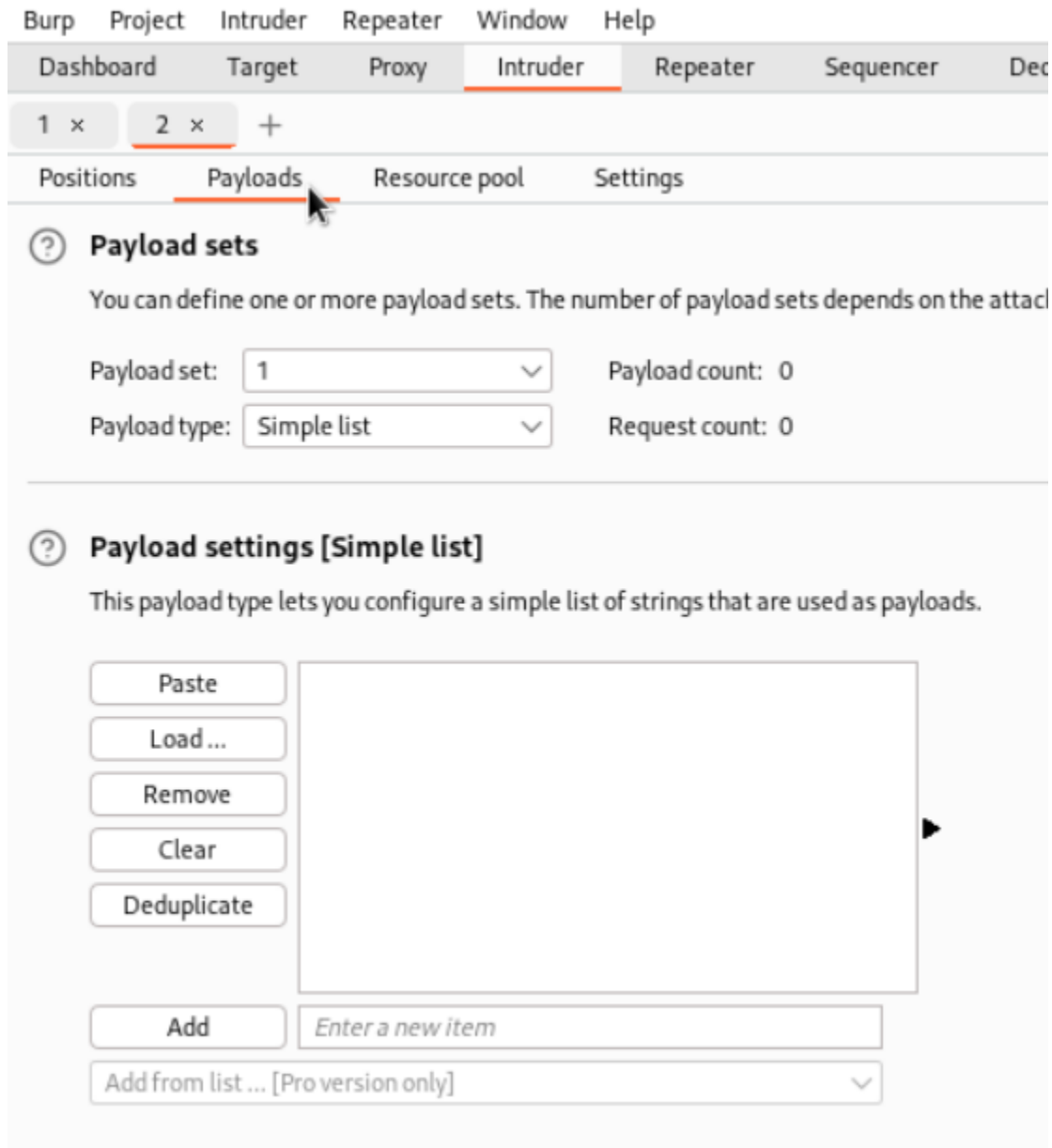
```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.0.33:4280/vulnerabilities/brute/
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 diisi dengan mengimport file word list atau daftar kata yang akan digunakan, atau bisa dibuat secara satu persatu dengan mengetikkan kata lalu klik Add.

? **Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

admin

user

dvwa

person

Add

Add from list ... [Pro version only] ▼

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.

Payload sets

You can define one or more payload sets. The number of payload sets depends on the a

Payload set: Payload count: 5

Payload type: Request count: 20

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

admin
password
secret
user
key

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

Positions **Payloads** Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: Payload count: 5

Payload type: Request count: 20

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

2. Intruder attack of http://172.16.0.33:4280 - Temporary attack - Not saved to project file

Attack Save Columns

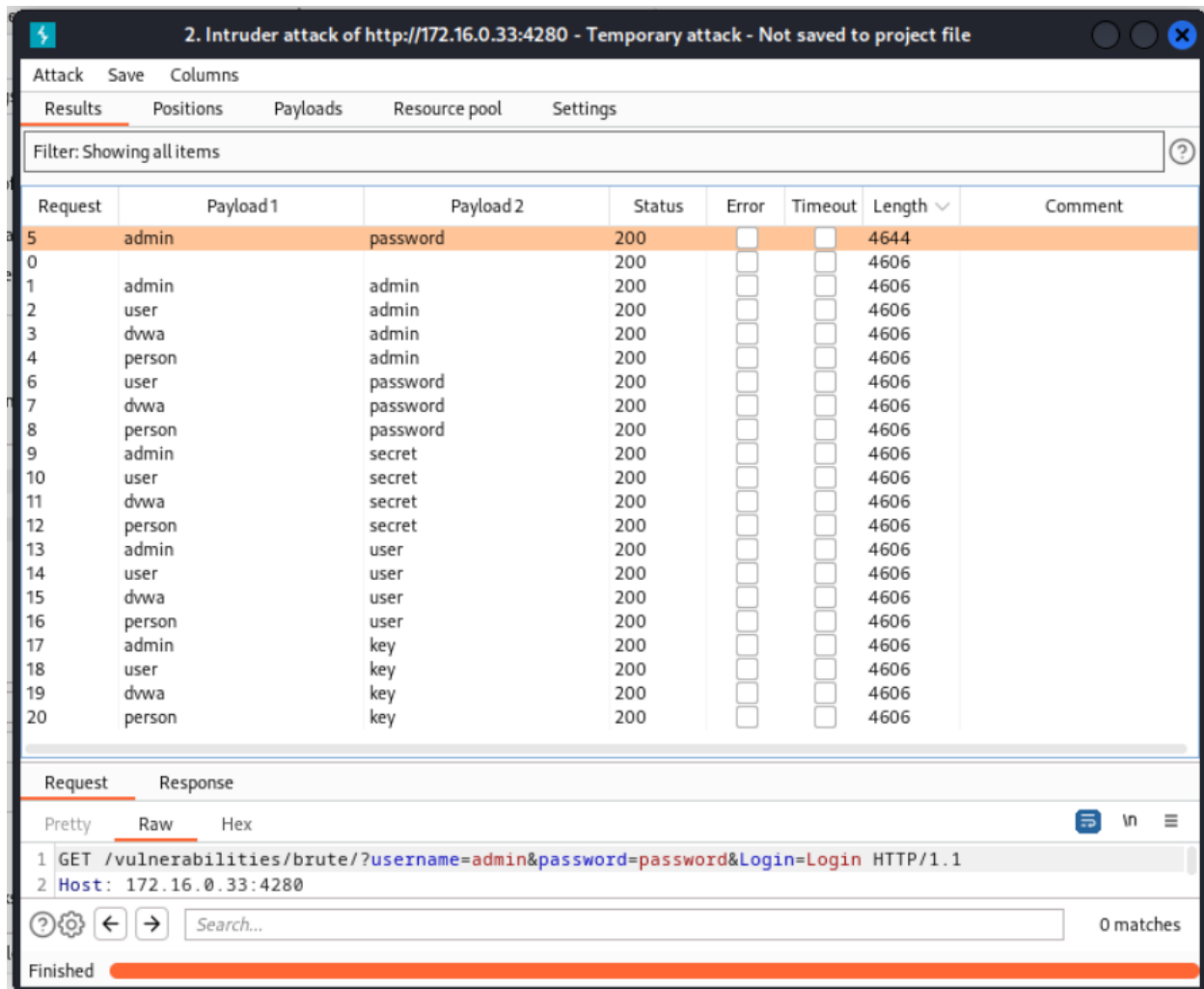
Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
1	admin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
2	user	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
3	dwva	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
4	person	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
5	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4644	
6	user	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
7	dwva	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
8	person	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
9	admin	secret	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
10	user	secret	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
11	dwva	secret	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
12	person	secret	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
13	admin	user	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
14	user	user	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
15	dwva	user	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
16	person	user	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
17	admin	key	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
18	user	key	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
19	dwva	key	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	
20	person	key	200	<input type="checkbox"/>	<input type="checkbox"/>	4606	

Finished

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

Vulnerability: Brute Force

Login

Username:

Password:

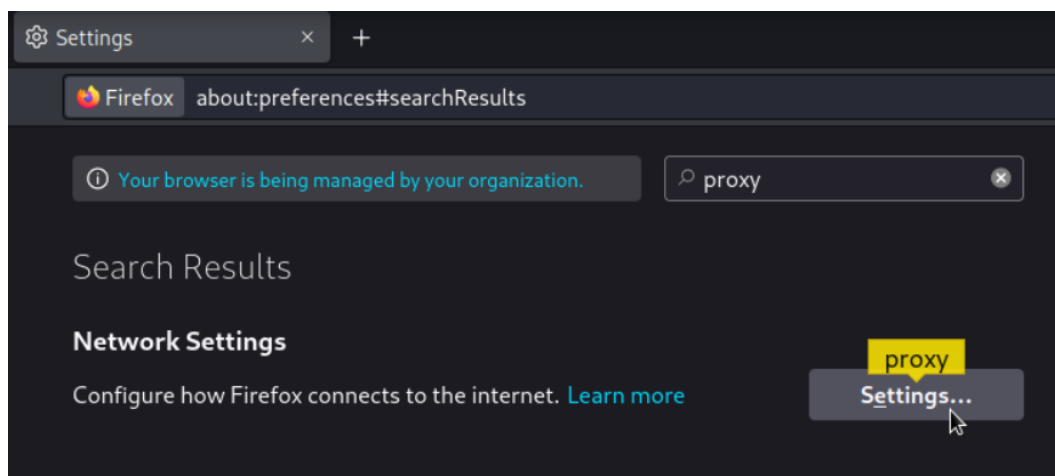
Welcome to the password protected area admin



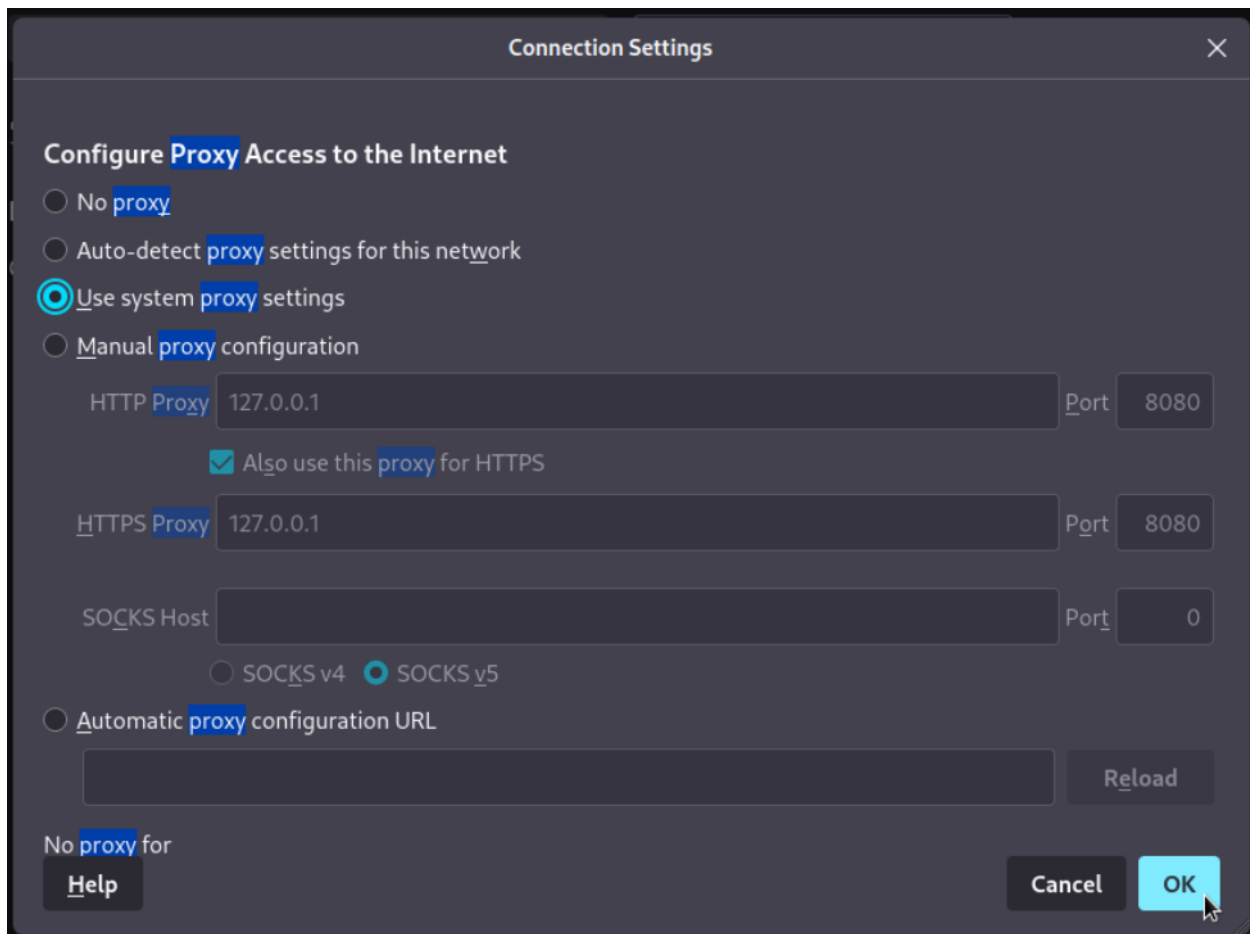
Clean up

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