15. SQL Injection dengan SQLMAP

Disusun oleh :

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

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

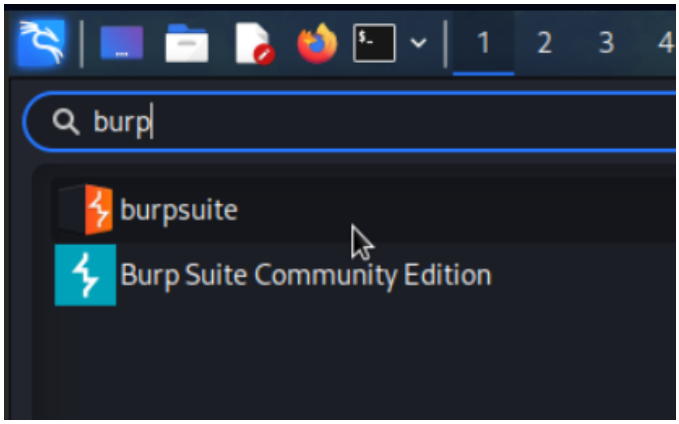
🔍 Information Gathering

Pada tampilan awal DVWA klik bagian SQL Injection

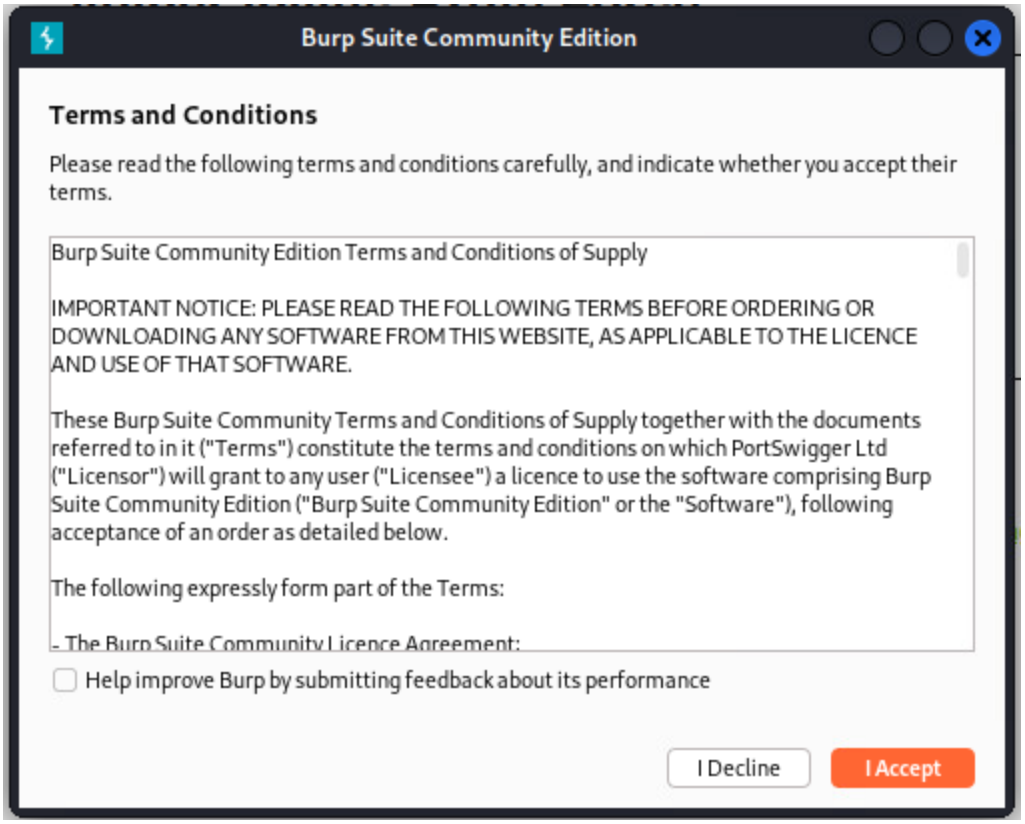
Berbeda dengan SQL Injection pada level low, di level medium ini untuk mengambil data user digunakan dropdown untuk memilih ID user, sehingga penyerang tidak bisa menginputkan payload sql injection langsung ke text field.

Lalu bagaimana cara memodifikasi ID yang diinput agar bisa melakukan serangan dari ID tersebut? Disini bisa menggunakan burp suite.

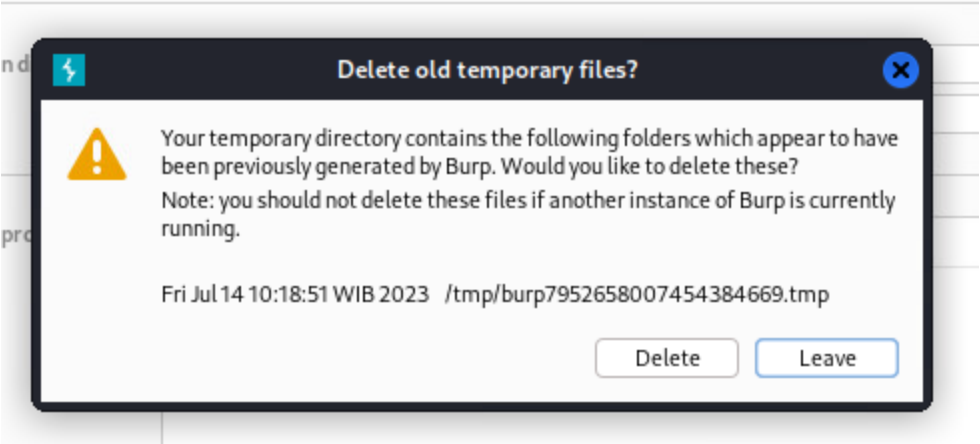
Buka Burp Suite



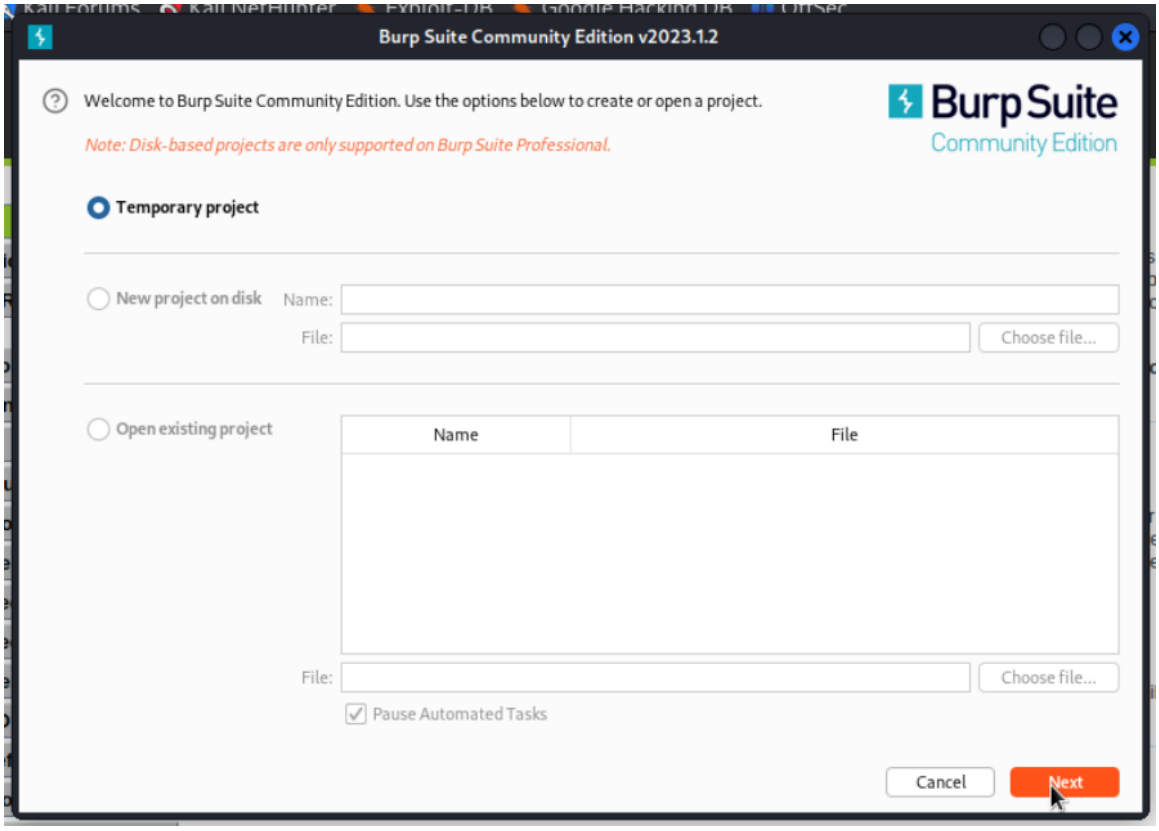
Klik I Accept



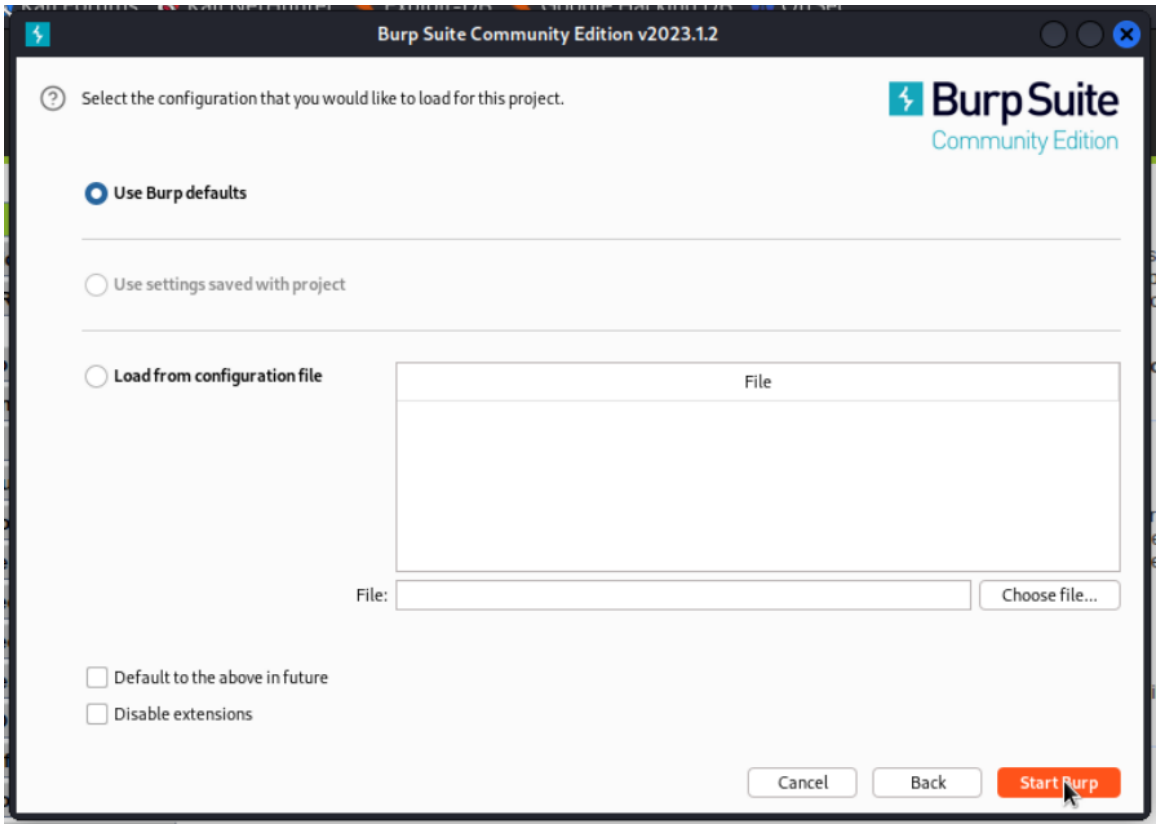
Klik Leave



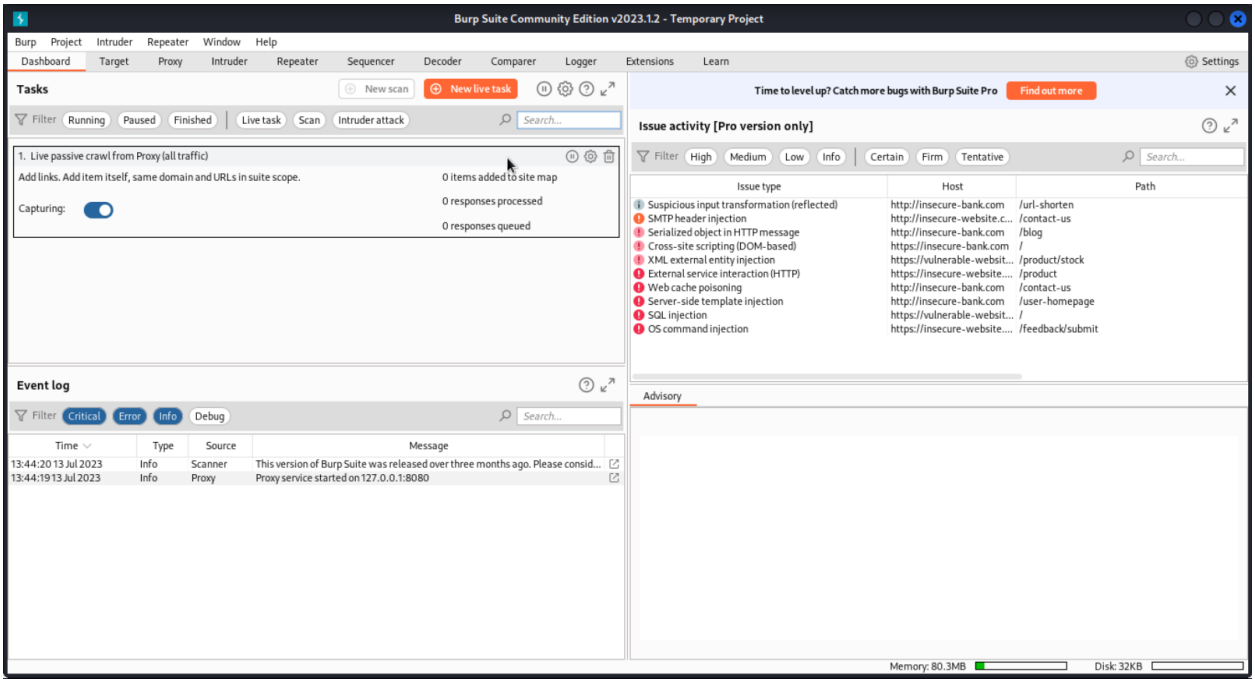
Klik next



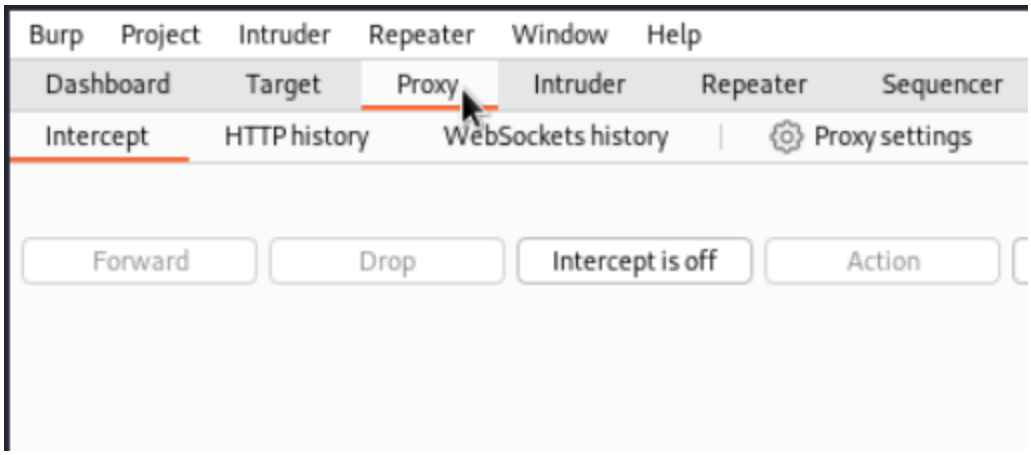
Klik Start Burp



Tampilan Burp Suite

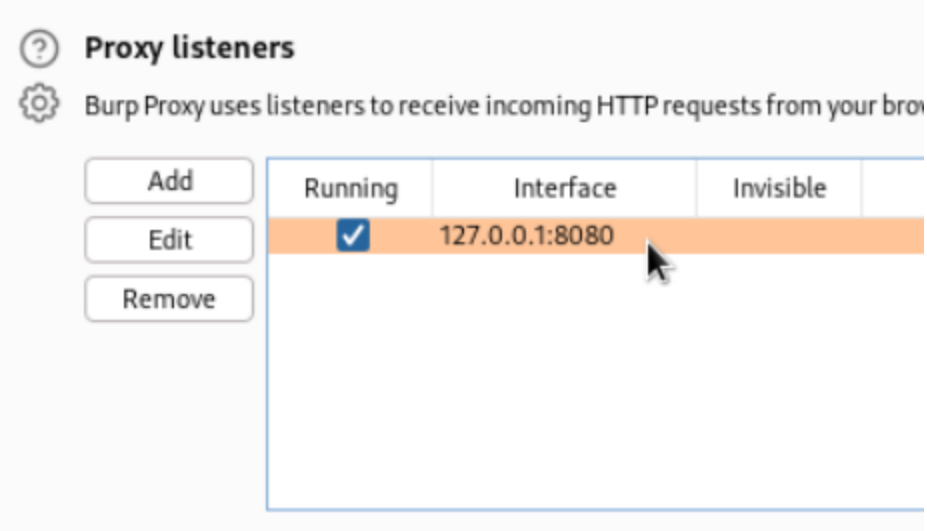


Klik tab Proxy

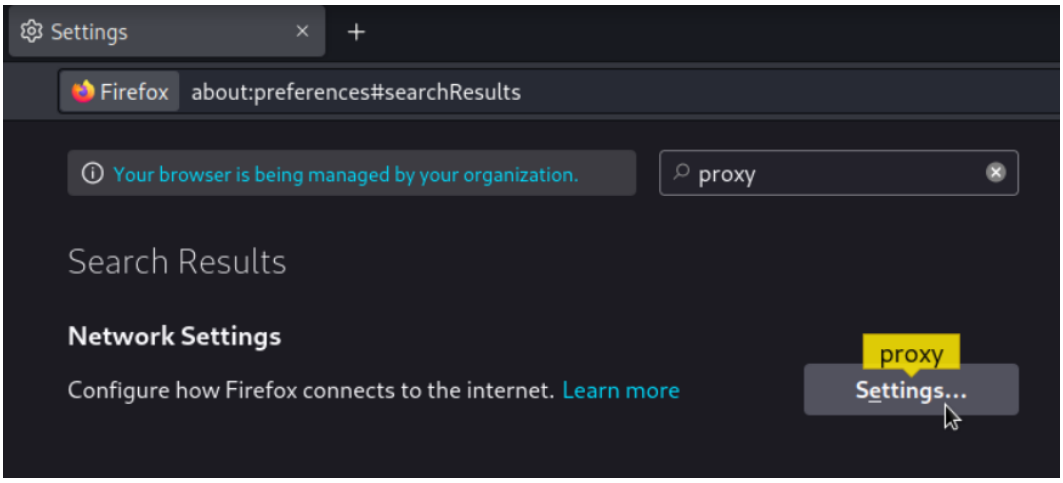


Klik Proxy settings dan pastikan pada Proxy listeners terdapat alamat IP dan port yang running

IP dan port ini yang nanti akan dijadikan proxy oleh browser

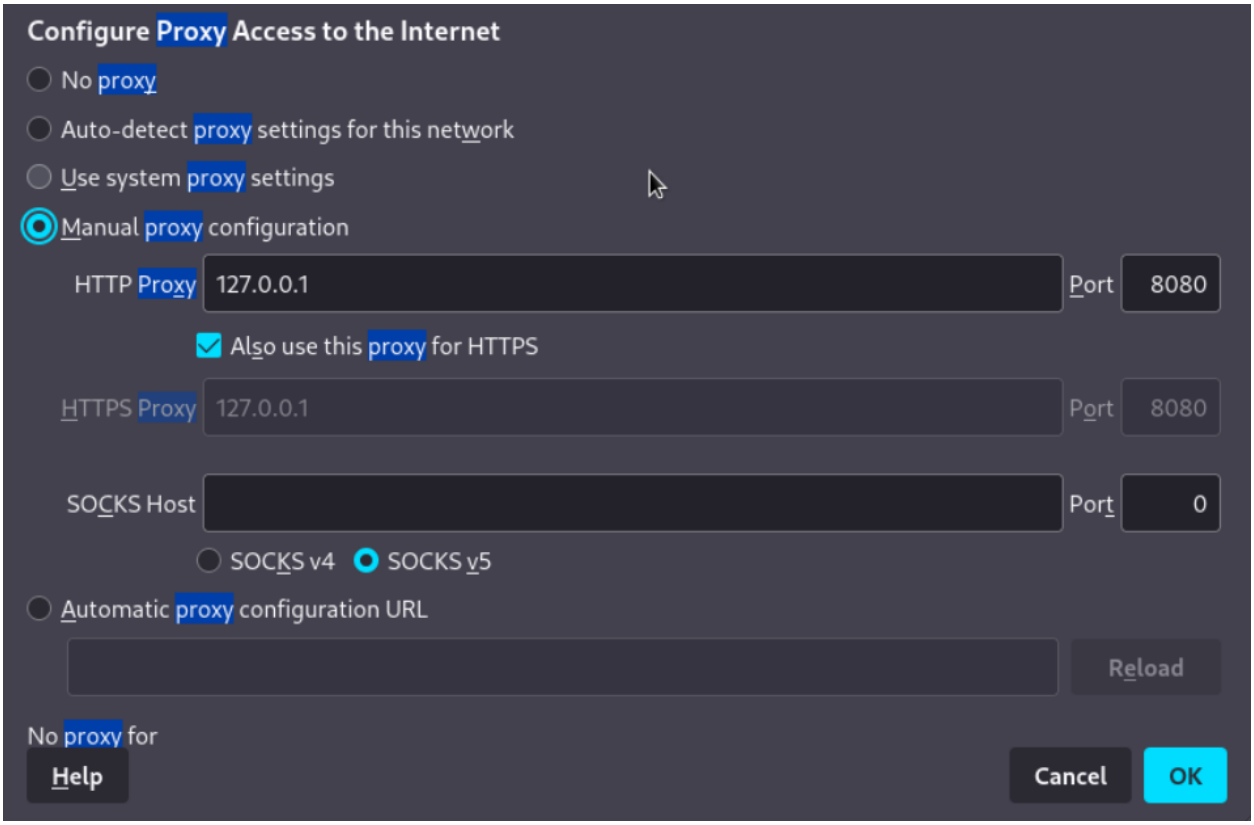


Kembali ke browser, pada Firefox masuk ke settings dan pada kolom pencarian ketikkan proxy

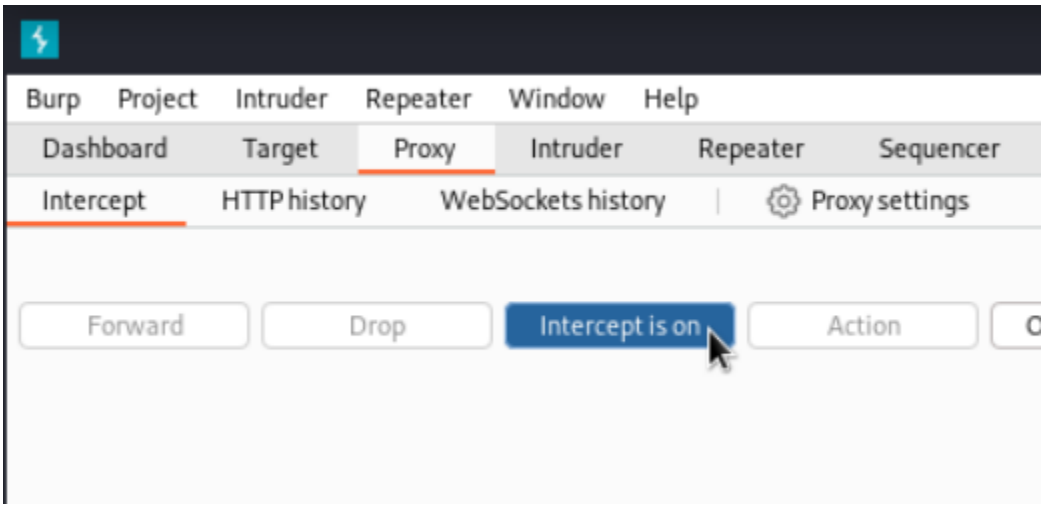


Didalamnya ganti “Use system proxy settings” menjadi “Manual proxy configuration”

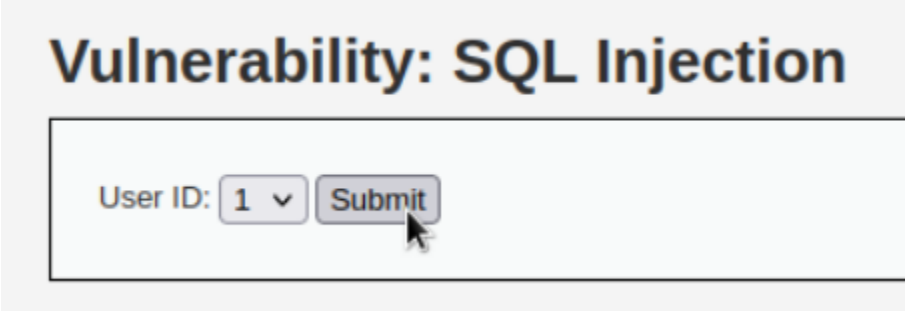
Pada HTTP Proxy masukkan IP dan Port yang sebelumnya didapat dari Burp Suite lalu klik OK



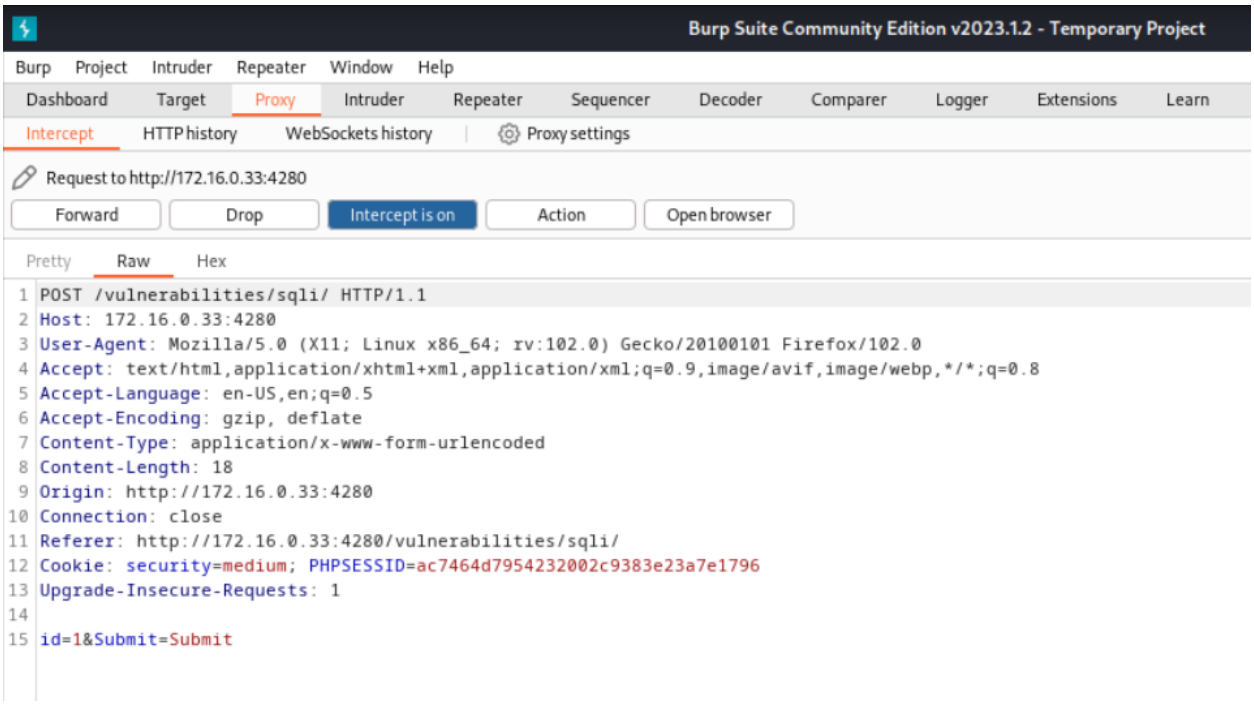
Buka Burp Suite, aktifkan intercept dengan klik tombol “Intercept is off”



Kembali masuk ke browser, ke halaman SQL Injection lalu klik submit dengan ID 1



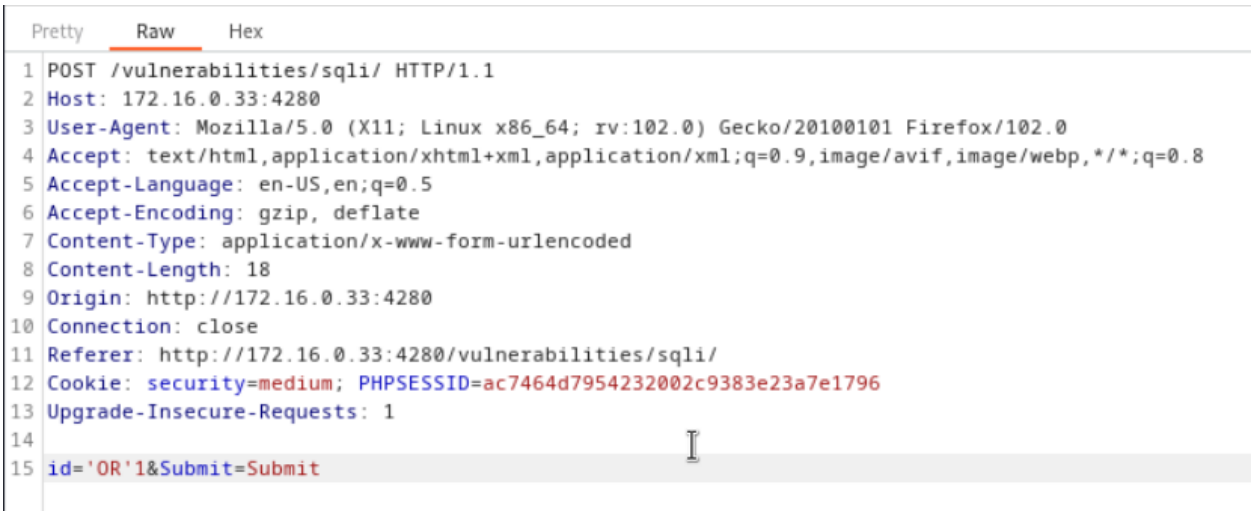
Akan muncul window burp suite seperti berikut



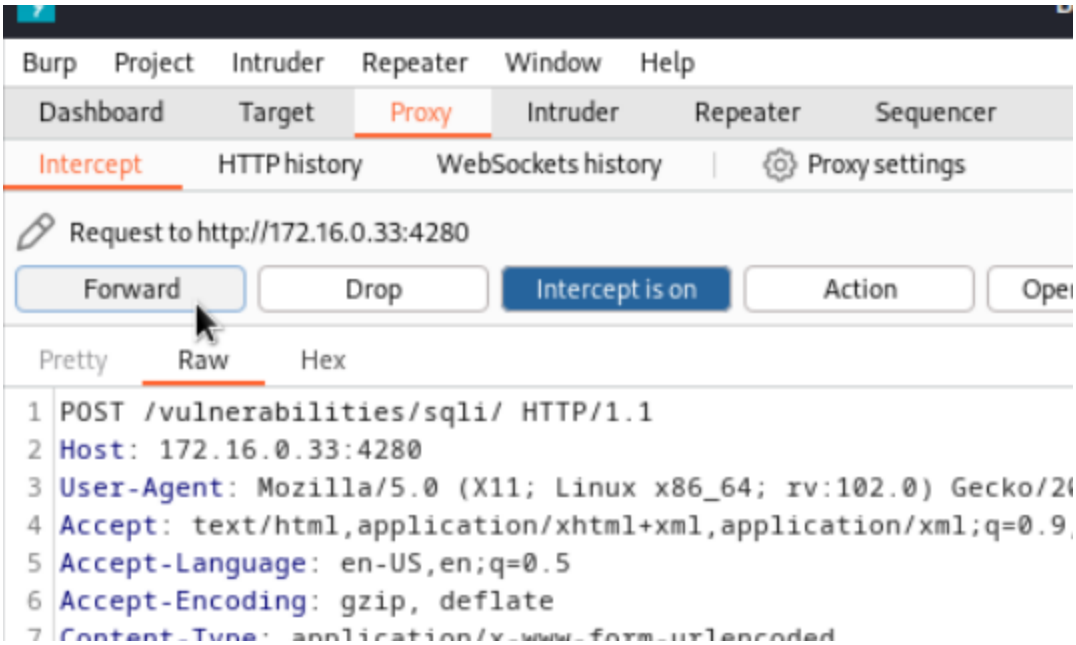
Hasil intercept di baris terakhir didapatkan nilai dari ID yang tadi diinputkan, namun dari sini nilai ID bisa diganti dengan payload yang diinginkan

Coba ganti value id yang tadinya 1 menjadi payload berikut

```
'OR'1
```



Klik forward



Maka hasilnya kurang lebih akan seperti berikut

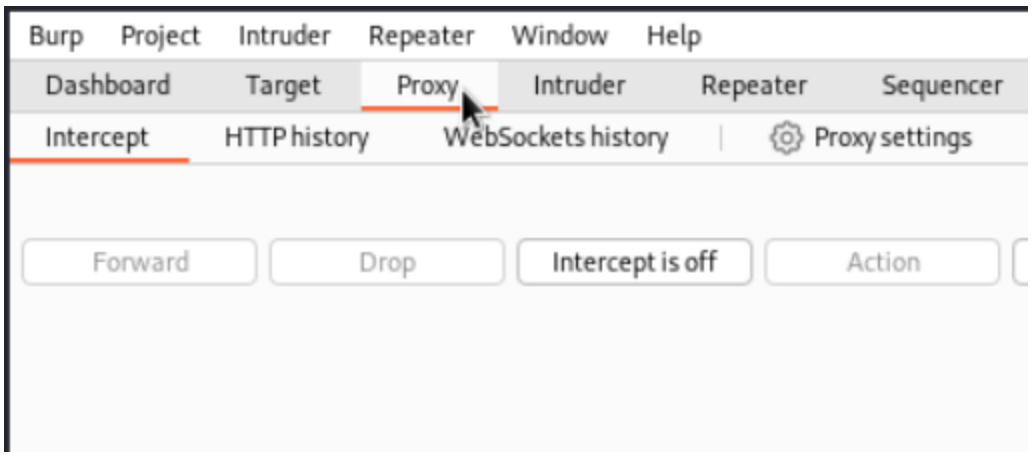
```
Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check th
e manual that corresponds to your MariaDB server version for the right syntax to use near
 '\'OR\'1' at line 1 in /var/www/html/vulnerabilities/sqli/source/medium.php:12 Stack trac
e: #0 /var/www/html/vulnerabilities/sqli/source/medium.php(12): mysqli_query(Object(mysql
i), 'SELECT first_na...') #1 /var/www/html/vulnerabilities/sqli/index.php(34): require_onc
e('/var/www/html/v...') #2 {main} thrown in /var/www/html/vulnerabilities/sqli/source/medi
um.php on line 12
```

Ternyata payload SQL Injection biasa tidak dapat memberikan hasil, untuk kasus ini diketahui ada 2 cara yaitu menggunakan UNION based injection dan SQLMap

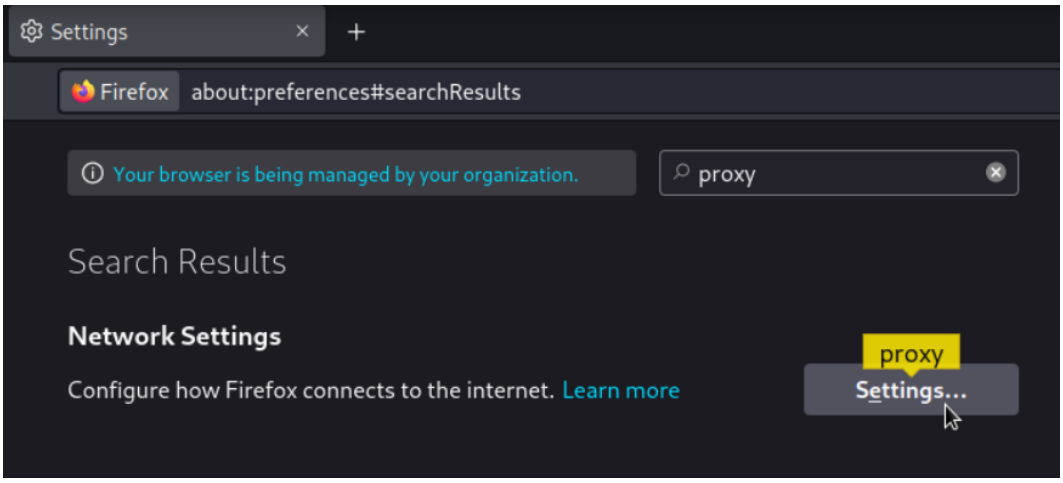
☠️ UNION based injection

Pada tampilan awal DVWA klik bagian SQL Injection

Pada burp suite masuk ke tab Proxy

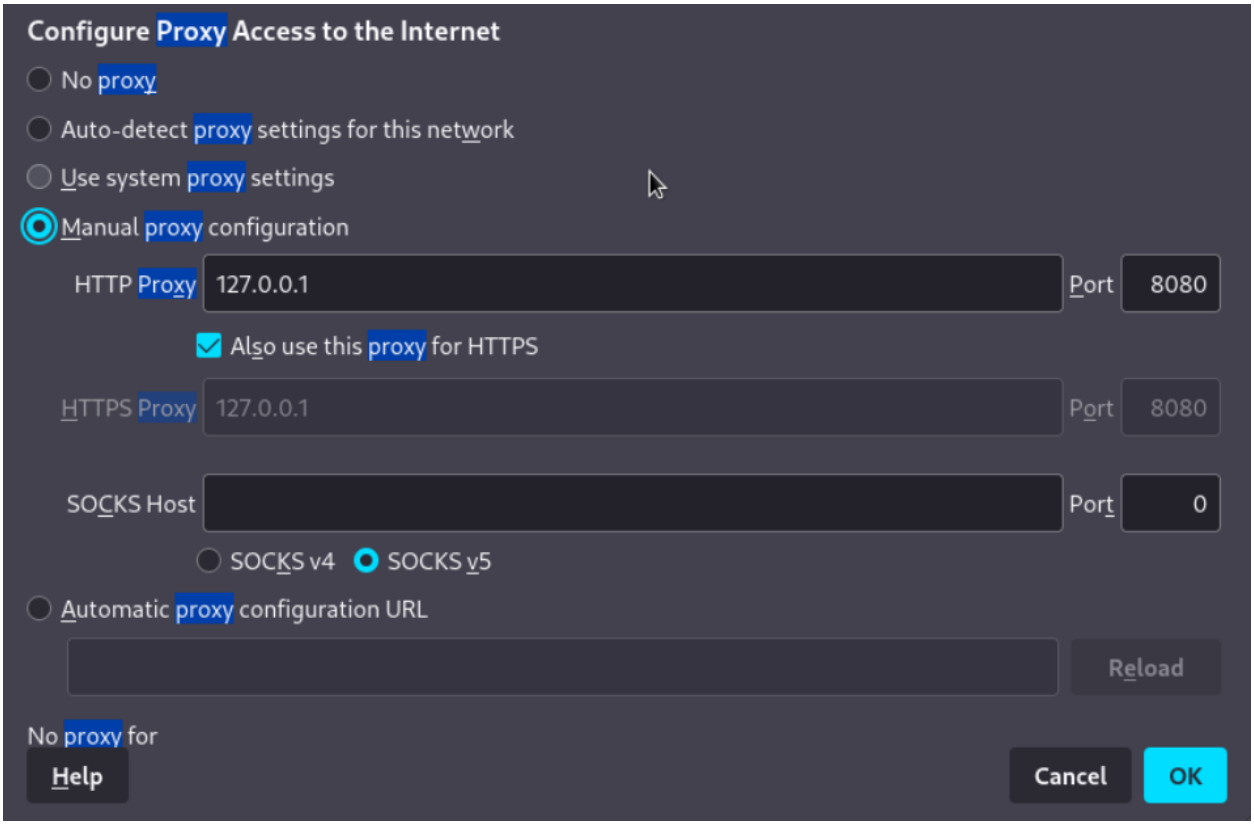


Kembali ke browser, pada Firefox masuk ke settings dan pada kolom pencarian ketikkan proxy

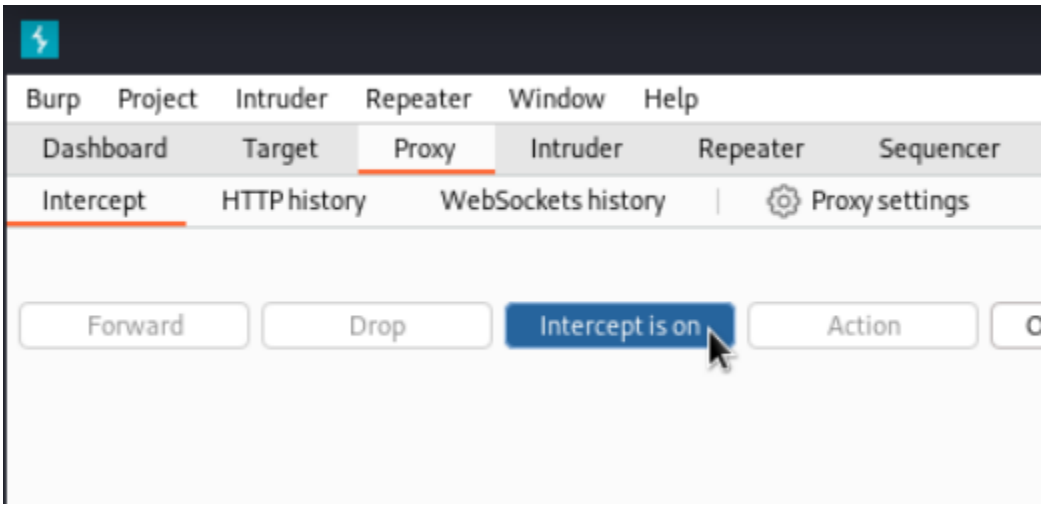


Didalamnya ganti “Use system proxy settings” menjadi “Manual proxy configuration”

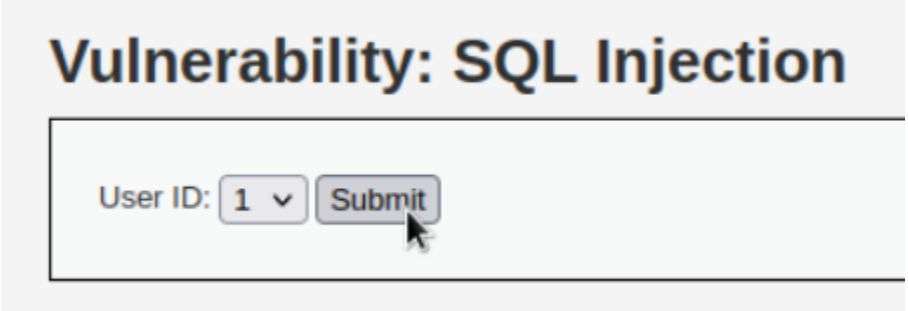
Pada HTTP Proxy masukkan IP dan Port yang sebelumnya didapat dari Burp Suite lalu klik OK



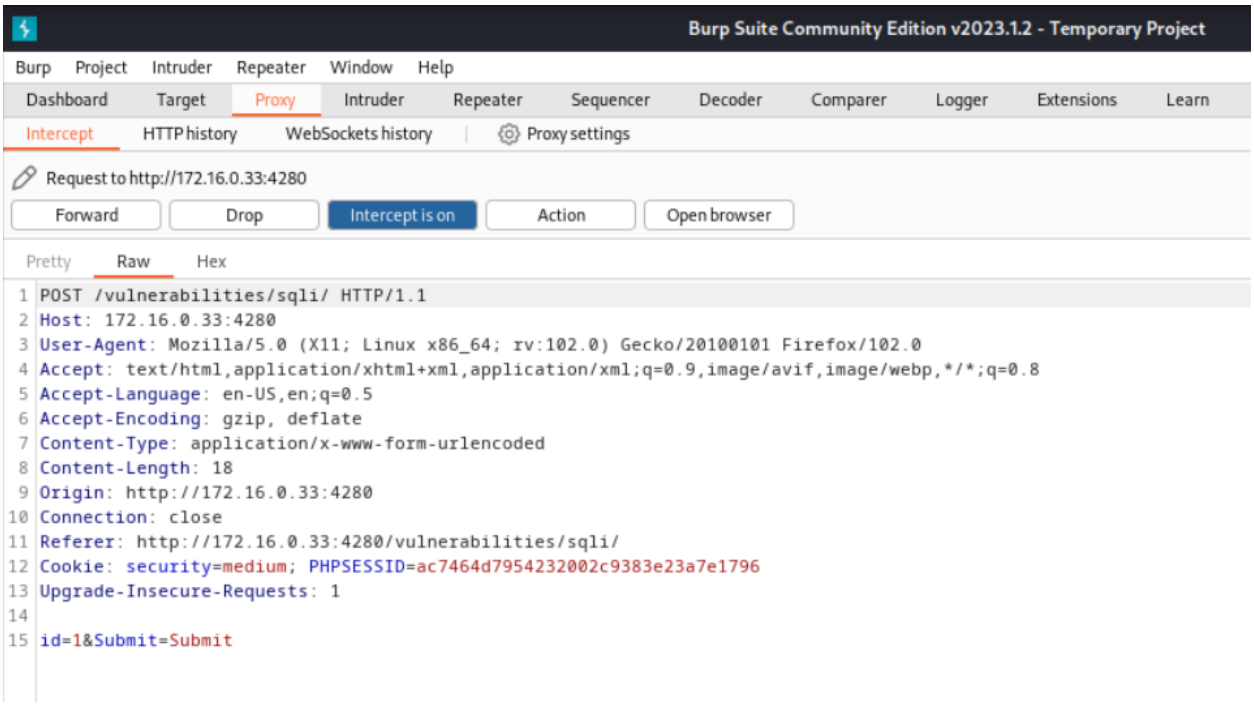
Buka Burp Suite, aktifkan intercept dengan klik tombol “Intercept is off”



Kembali masuk ke browser, ke halaman SQL Injection lalu klik submit dengan ID 1



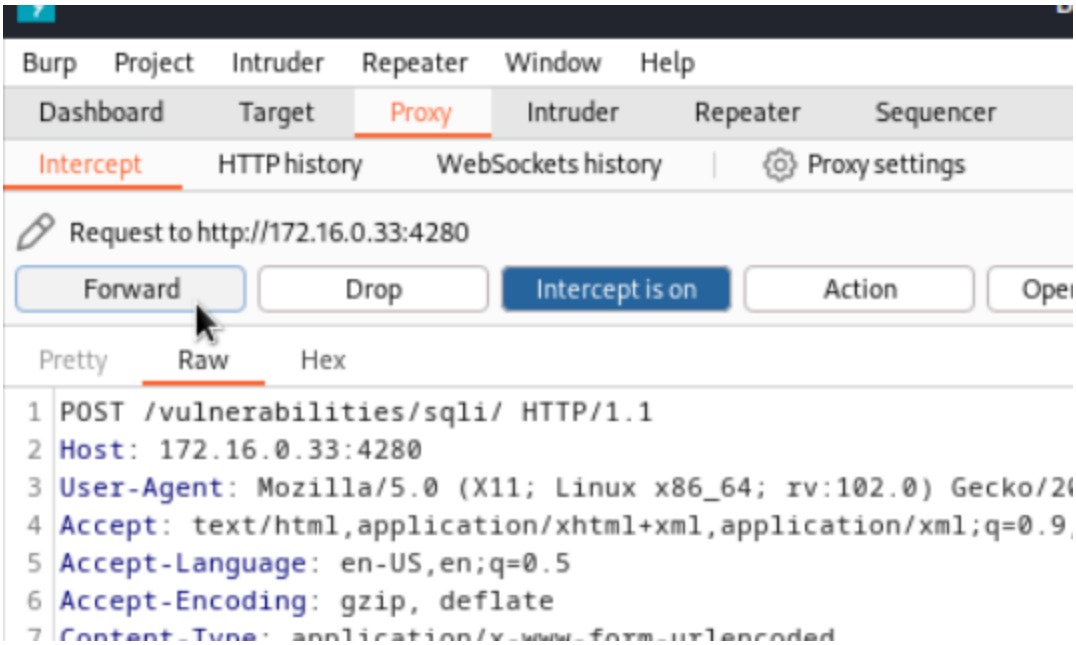
Akan muncul window burp suite seperti berikut



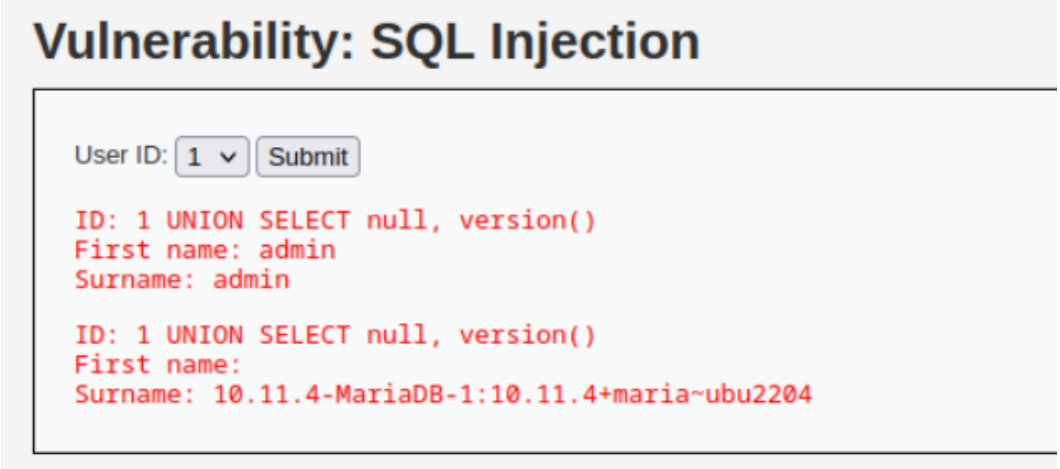
Pada bagian bawah, tambahkan payload pada value ID sehingga menjadi seperti berikut

```
id=1 UNION SELECT null, version()
```

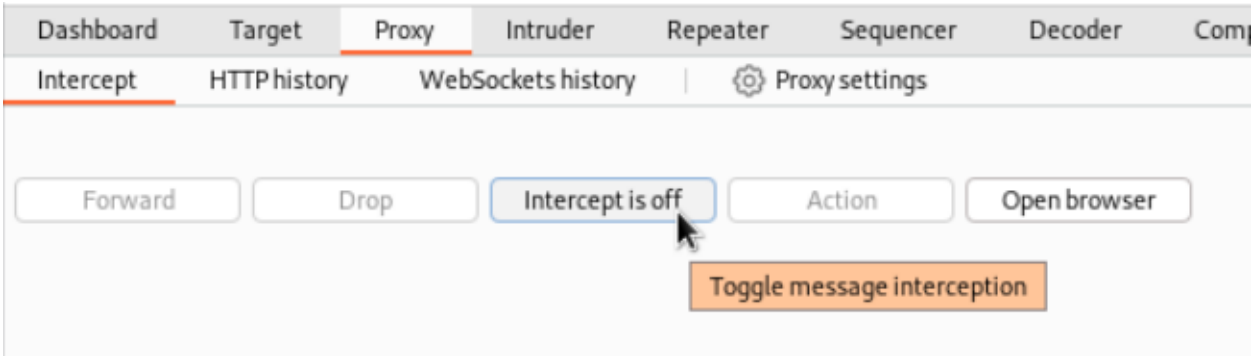
Klik forward



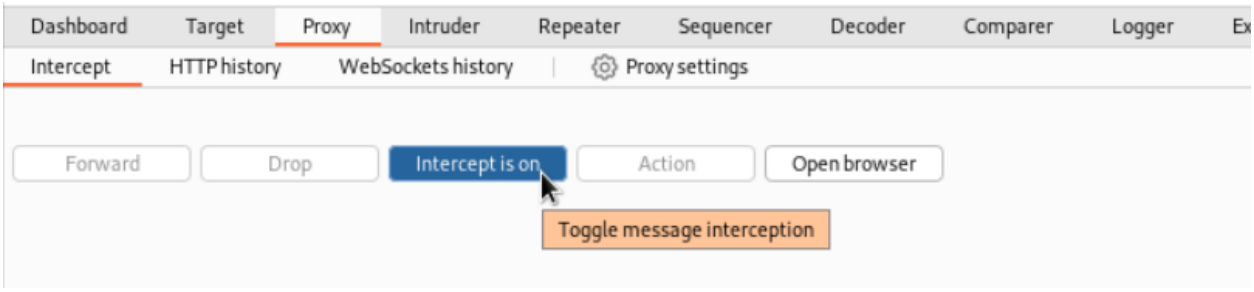
Maka pada halaman DVWA akan muncul versi SQL yang digunakan

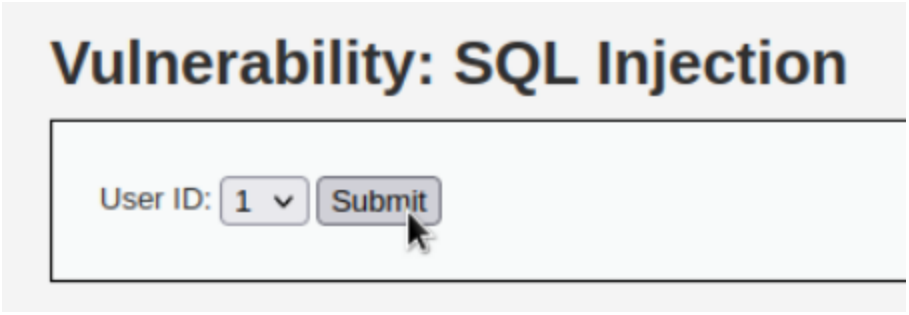


Selanjutnya coba untuk memunculkan semua tabel yang ada pada database. Matikan intercept pada Burp Suite, lalu buka kembali halaman SQL Injection pada DVWA.

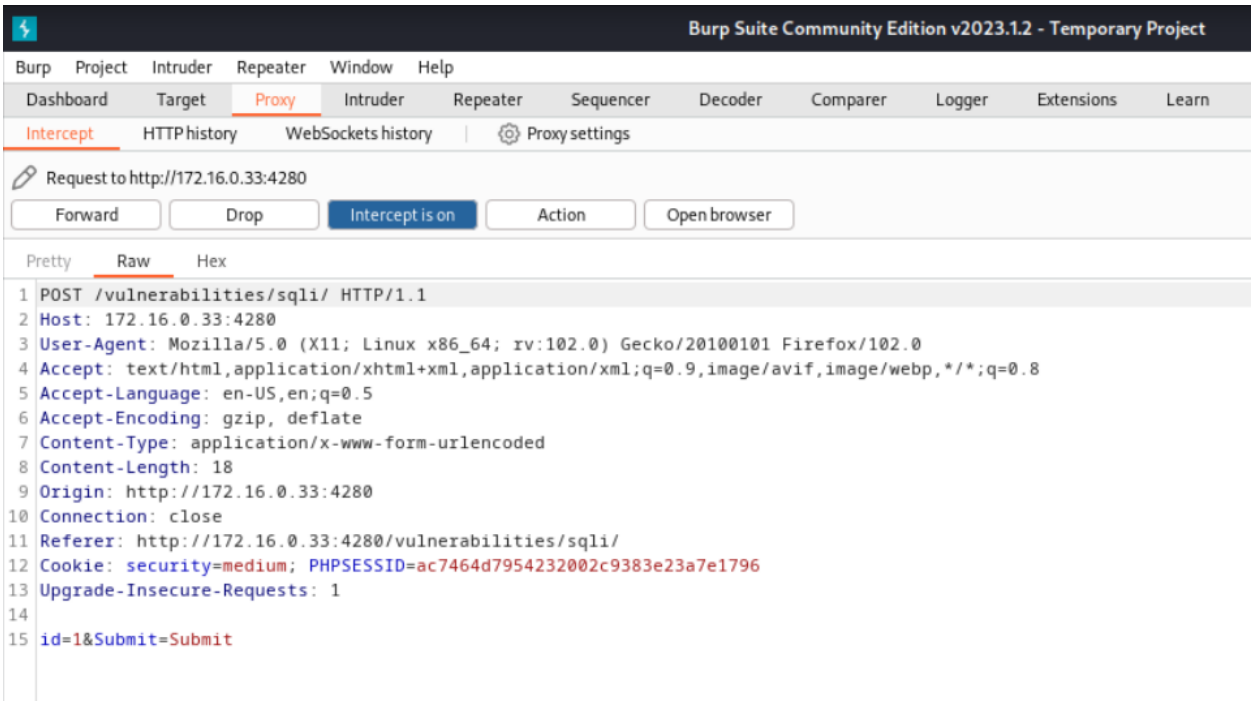


Kembali ke Burp Suite dan nyalakan kembali mode intercept, kemudian masuk ke browser, ke halaman SQL Injection lalu klik submit dengan ID 1



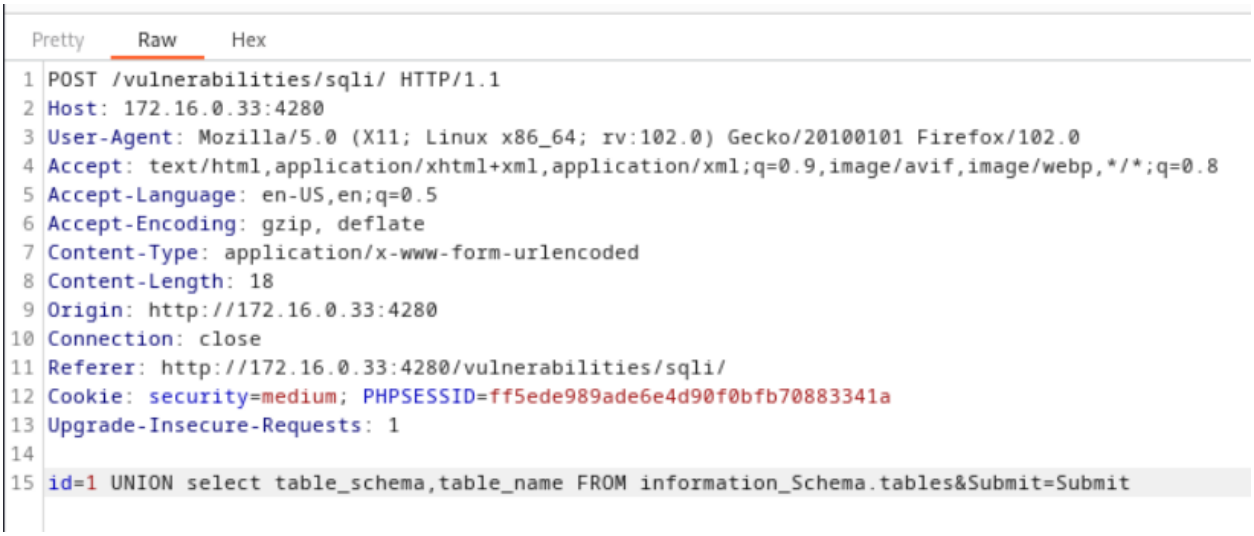


Akan muncul window burp suite seperti berikut

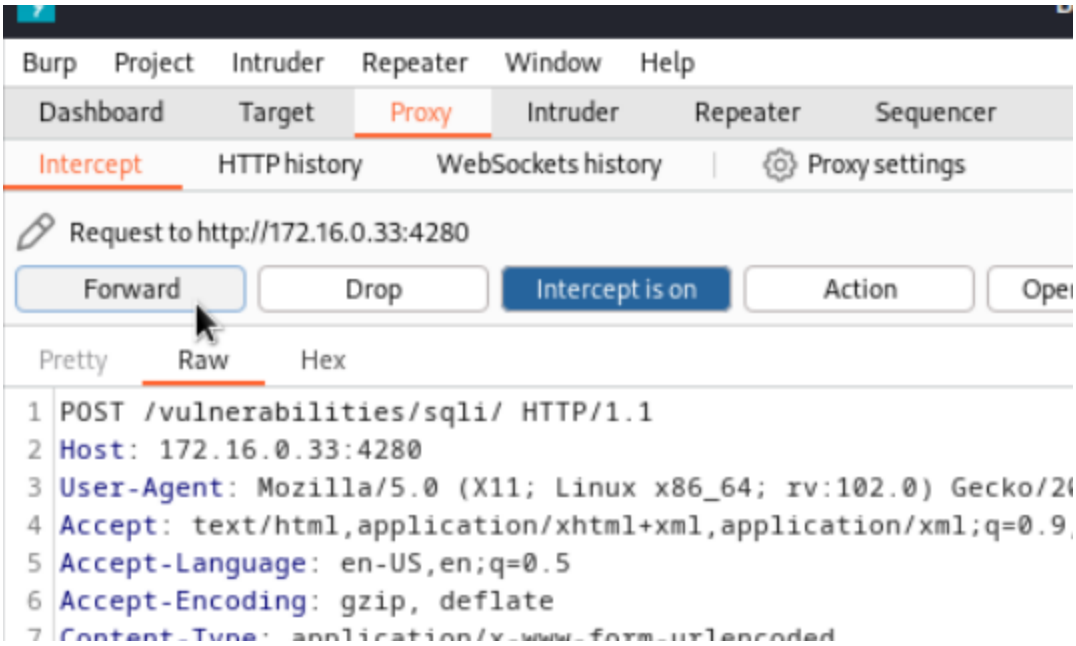


Pada bagian bawah, tambahkan payload pada value ID sehingga menjadi seperti berikut

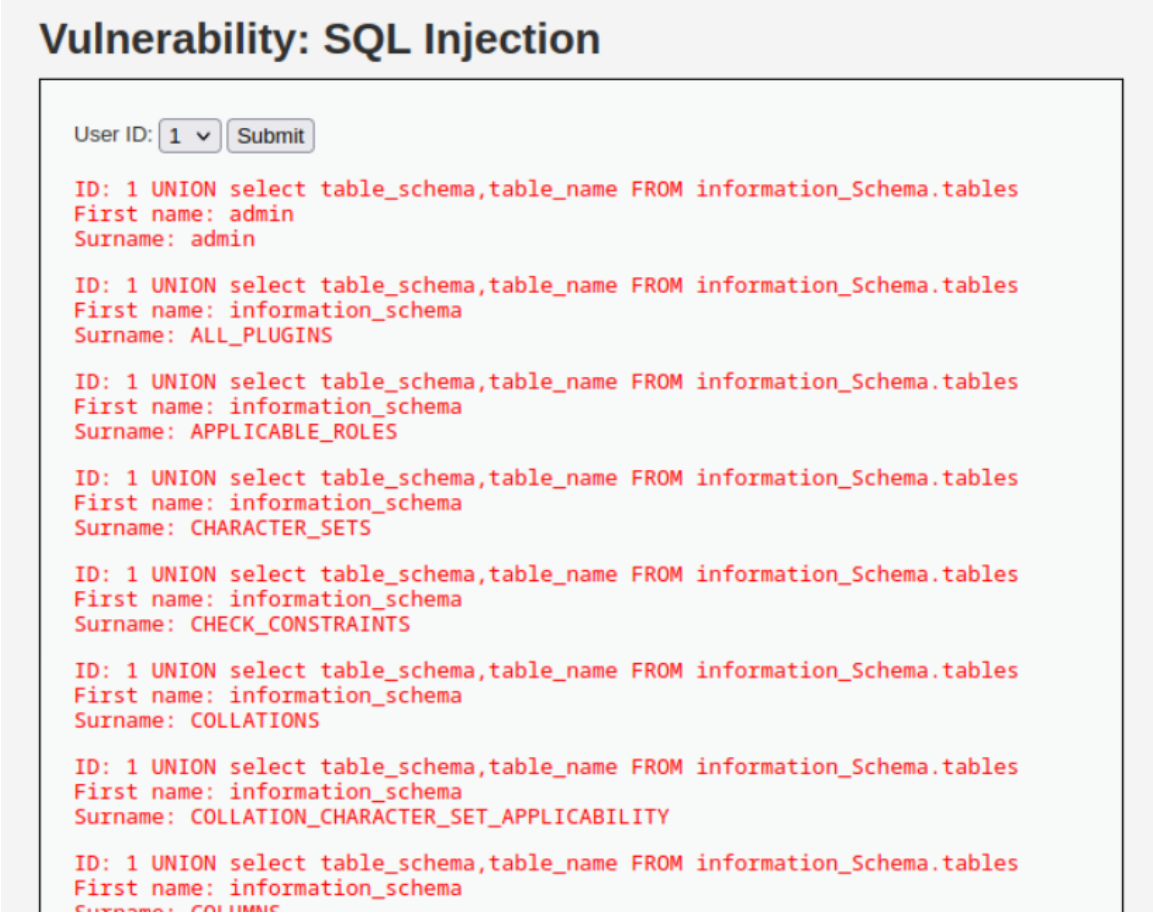
```
UNION select table_schema,table_name FROM information_Schema.tables
```



Klik forward



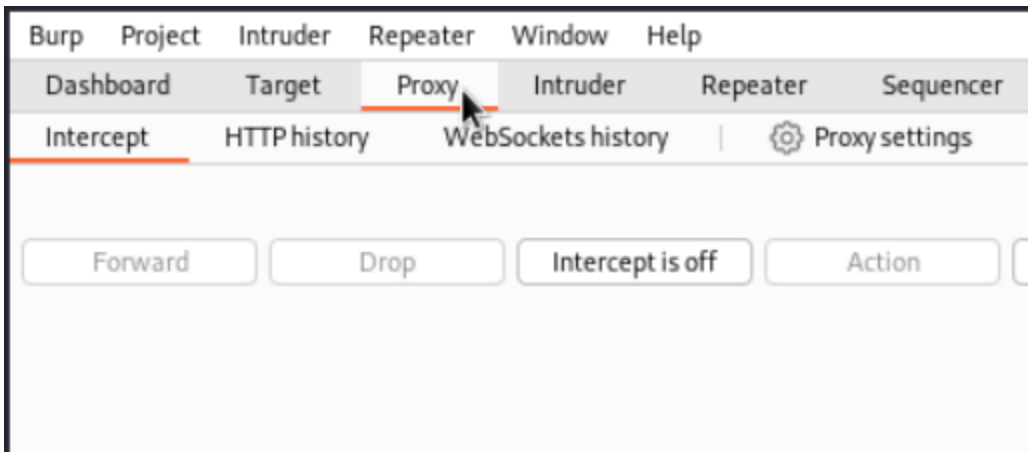
Maka akan muncul seluruh tabel yang ada pada database



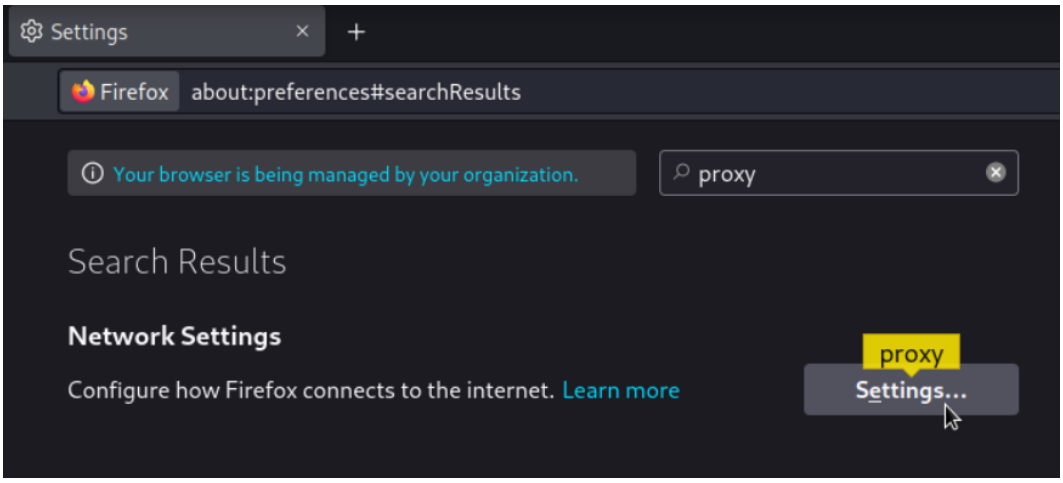
☠️ SQLMap

Pada tampilan awal DVWA klik bagian SQL Injection

Pada burp suite masuk ke tab Proxy

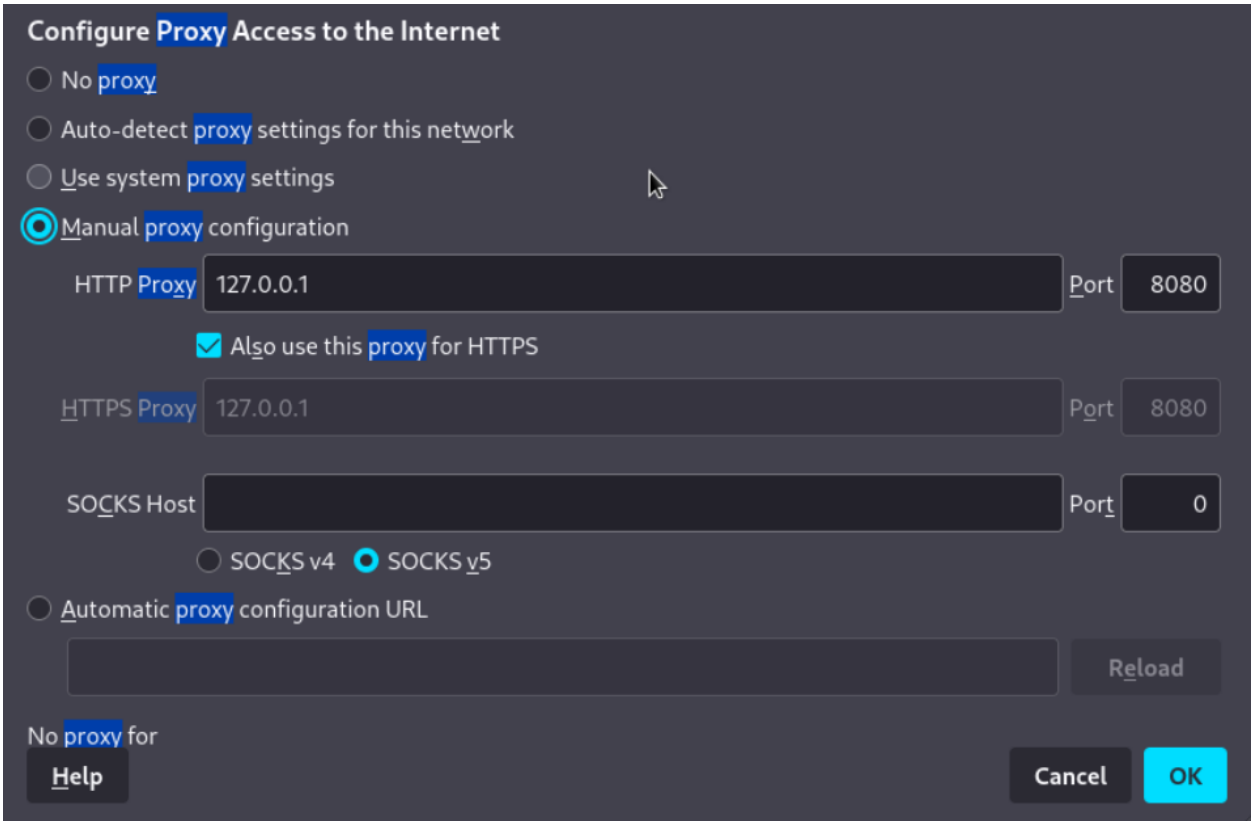


Kembali ke browser, pada Firefox masuk ke settings dan pada kolom pencarian ketikkan proxy

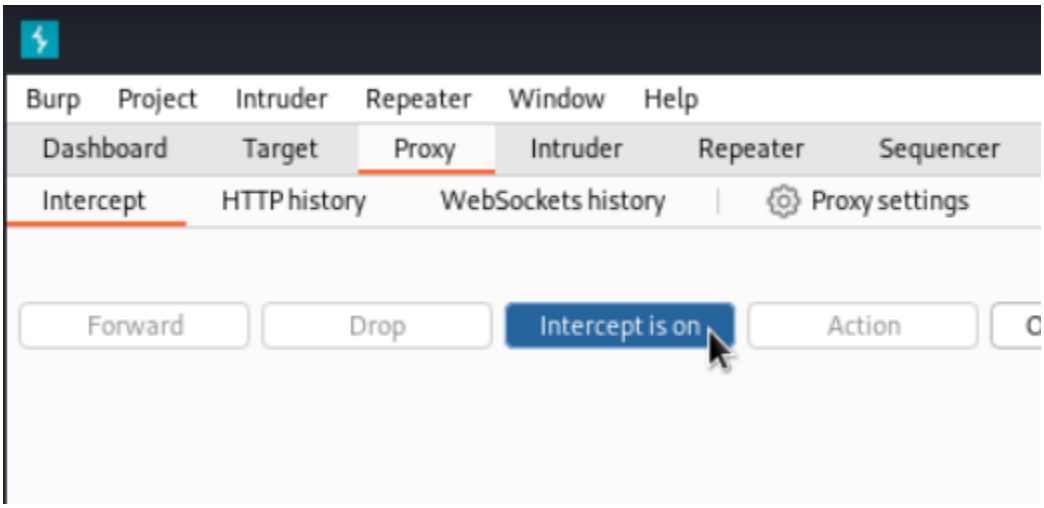


Didalamnya ganti “Use system proxy settings” menjadi “Manual proxy configuration”

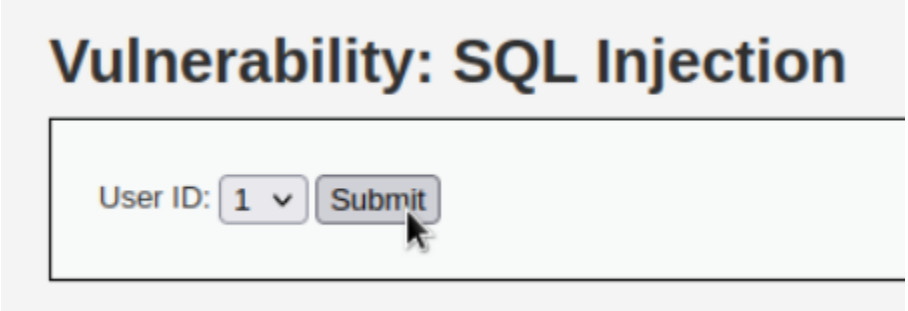
Pada HTTP Proxy masukkan IP dan Port yang sebelumnya didapat dari Burp Suite lalu klik OK



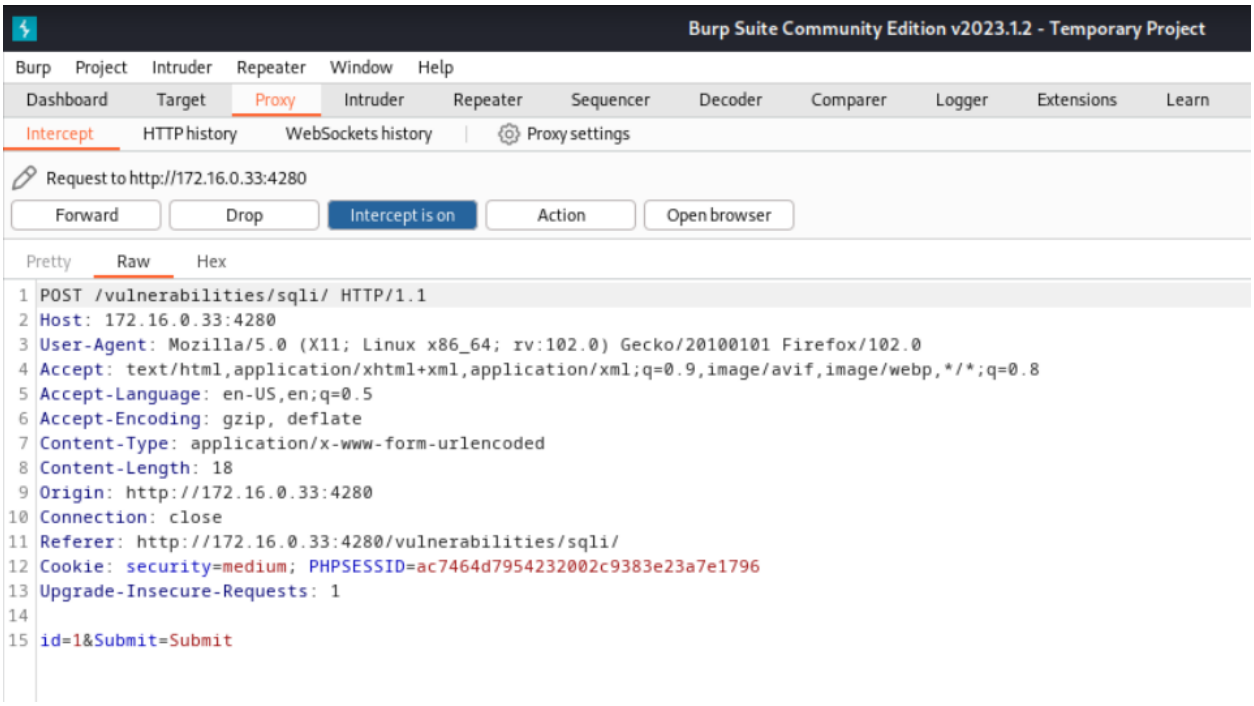
Buka Burp Suite, aktifkan intercept dengan klik tombol “Intercept is off”



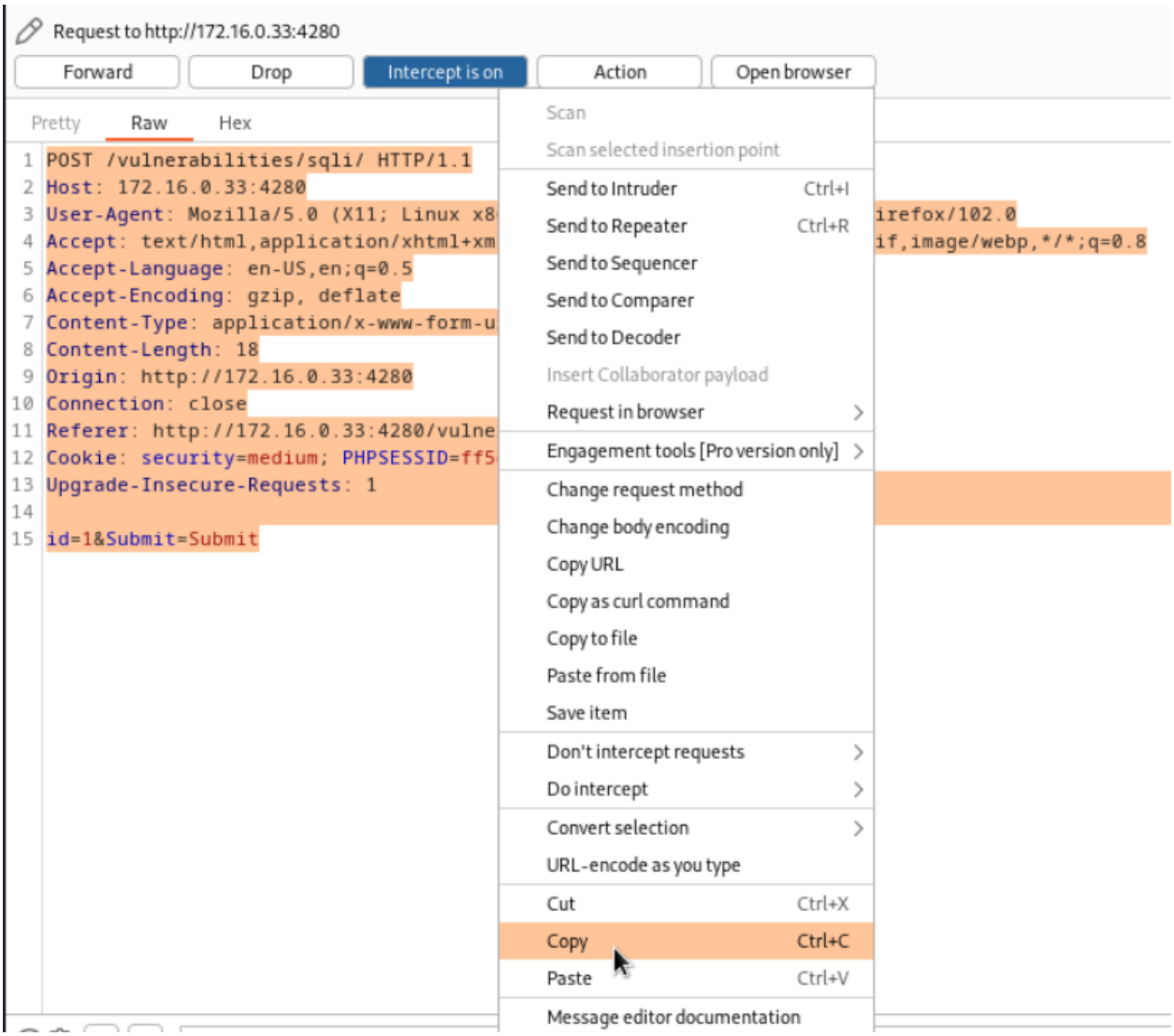
Kembali masuk ke browser, ke halaman SQL Injection lalu klik submit dengan ID 1



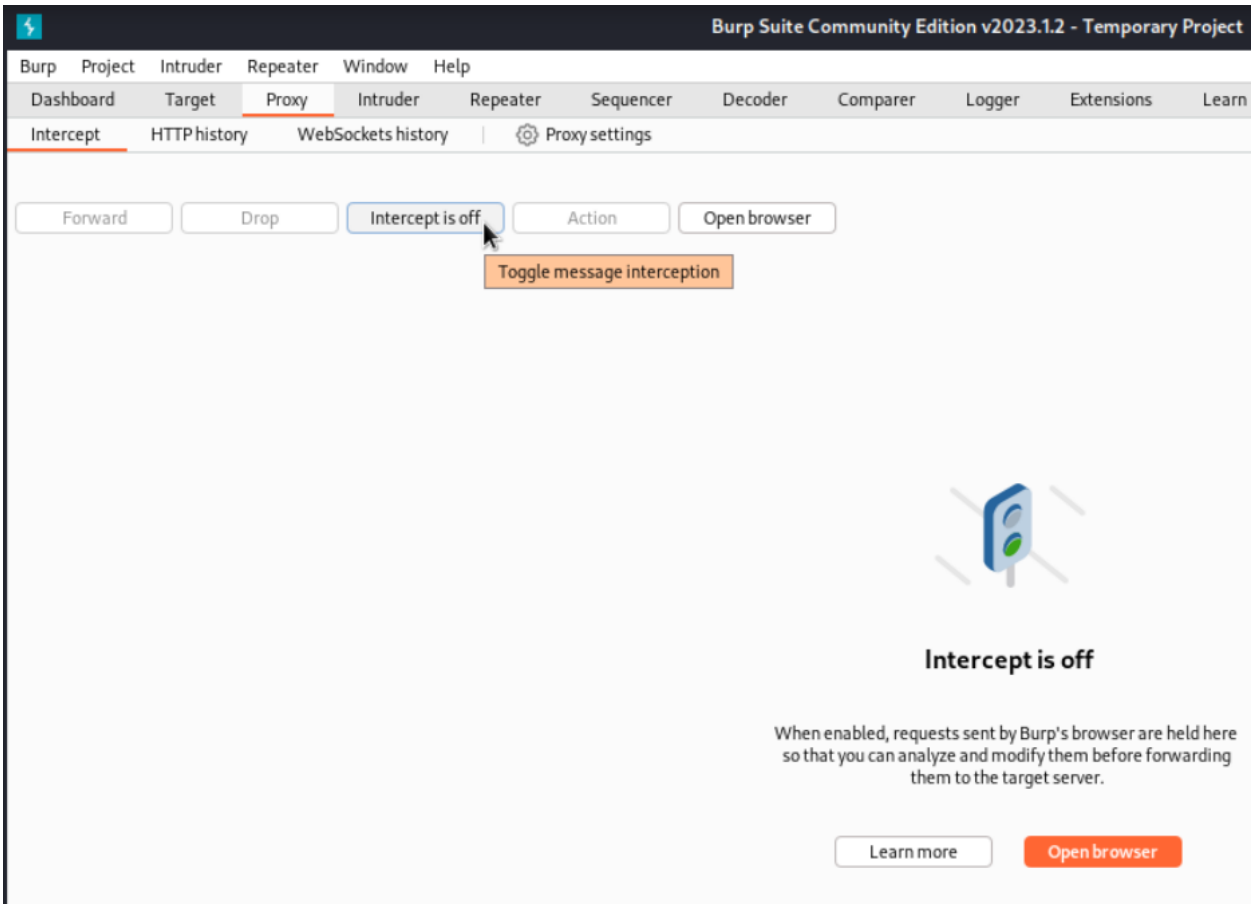
Akan muncul window burp suite seperti berikut



Copy text yang ada pada Raw



Matikan intercept pada Burp Suite

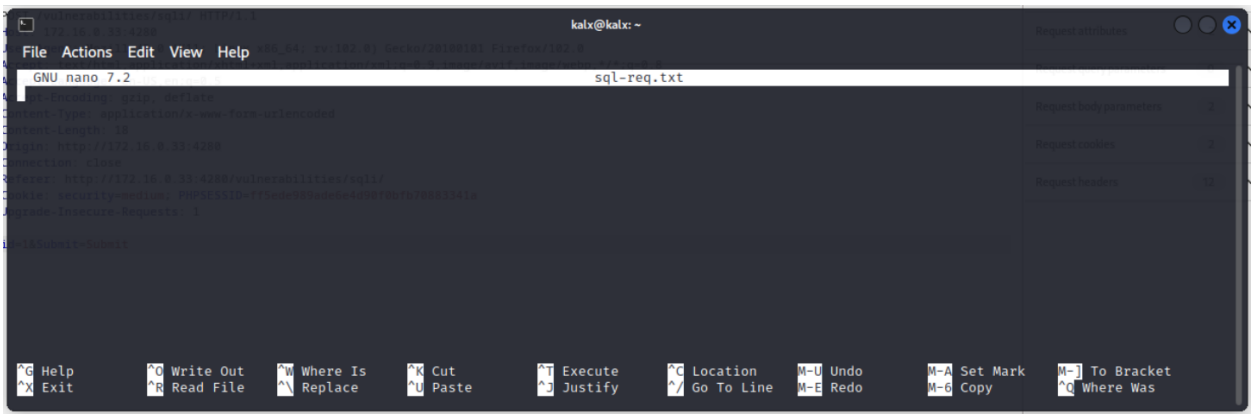


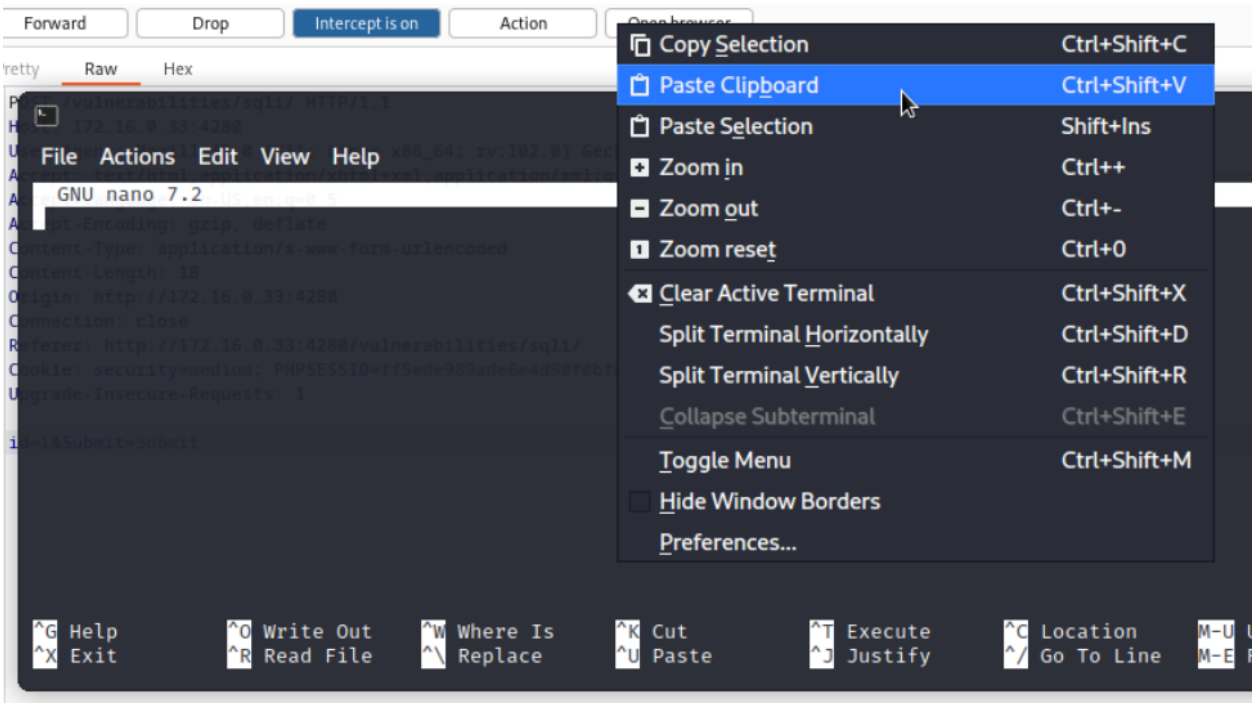
Buka terminal, masuk ke direktori user

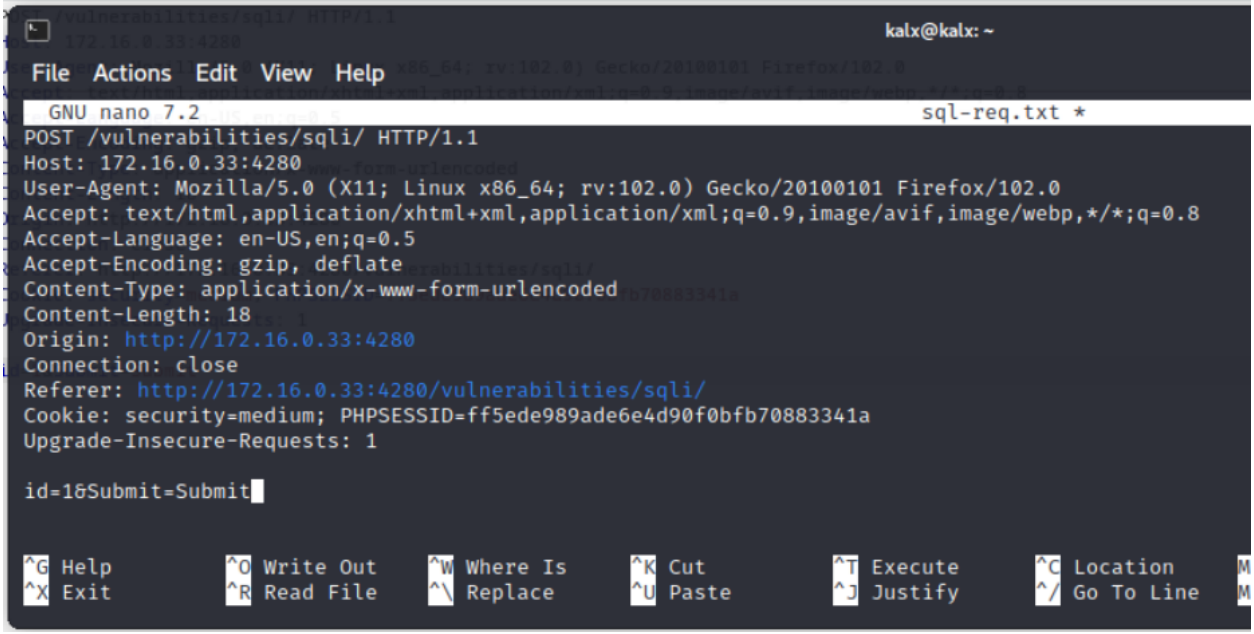
```
cd
```

Buat file baru dengan nama `sql-req.txt`, lalu paste kan text tadi

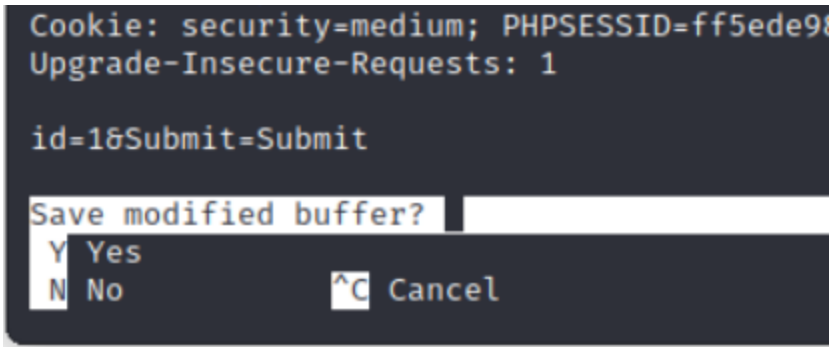
```
nano sql-req.txt
```


kalx@kalx: ~
File Actions Edit View Help
GNU nano 7.2
sql-req.txt
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify
^C Location
^/ Go To Line
M-U Undo
M-E Redo
M-A Set Mark
M-6 Copy
M-] To Bracket
^Q Where Was

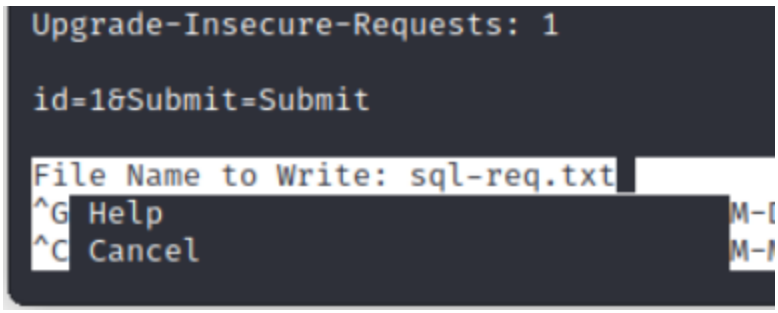

Forward
Drop
Intercept is on
Action
Raw
Hex
File Actions Edit View Help
GNU nano 7.2
Copy Selection Ctrl+Shift+C
Paste Clipboard Ctrl+Shift+V
Paste Selection Shift+Ins
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom reset Ctrl+0
Clear Active Terminal Ctrl+Shift+X
Split Terminal Horizontally Ctrl+Shift+D
Split Terminal Vertically Ctrl+Shift+R
Collapse Subterminal Ctrl+Shift+E
Toggle Menu Ctrl+Shift+M
Hide Window Borders
Preferences...
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify
^C Location
^/ Go To Line



Save dengan ctrl+x, Lalu tekan Y



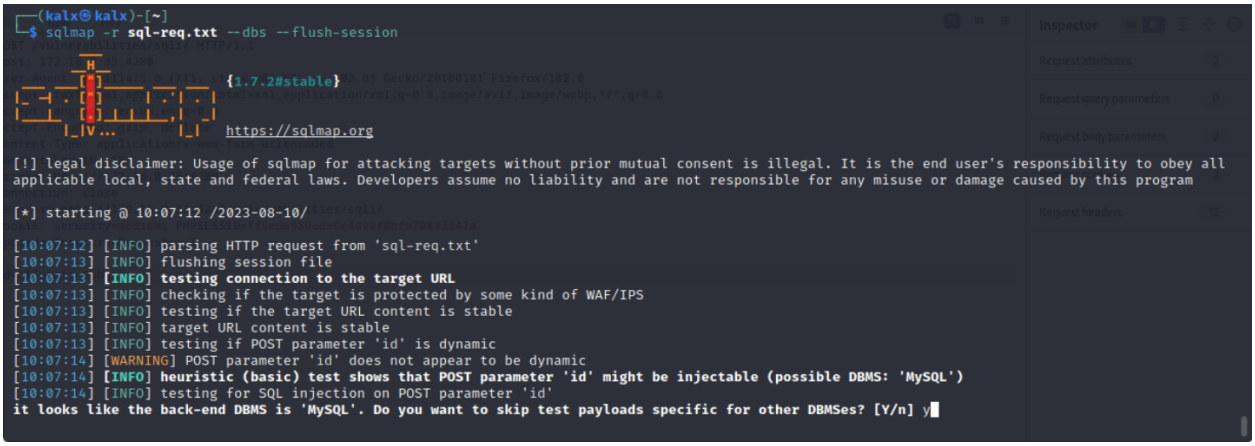
Lalu tekan enter



Masih di direktori yang sama, gunakan file `sql-req.txt` tadi untuk mengeksekusi SQLMap

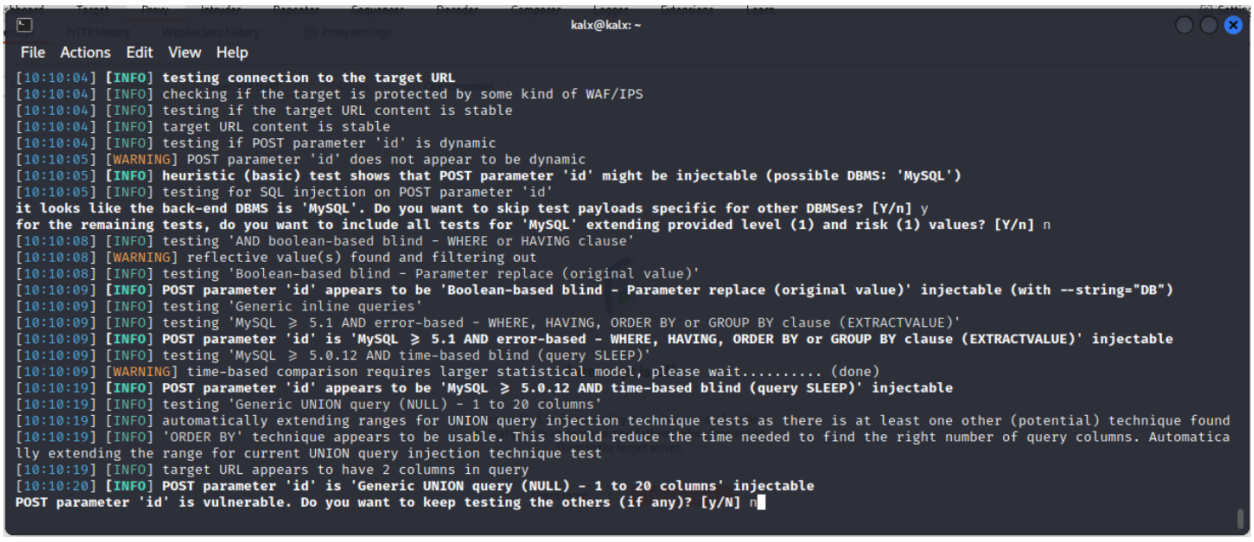
```
sqlmap -r sql-req.txt --dbs
```

Tekan y lalu enter

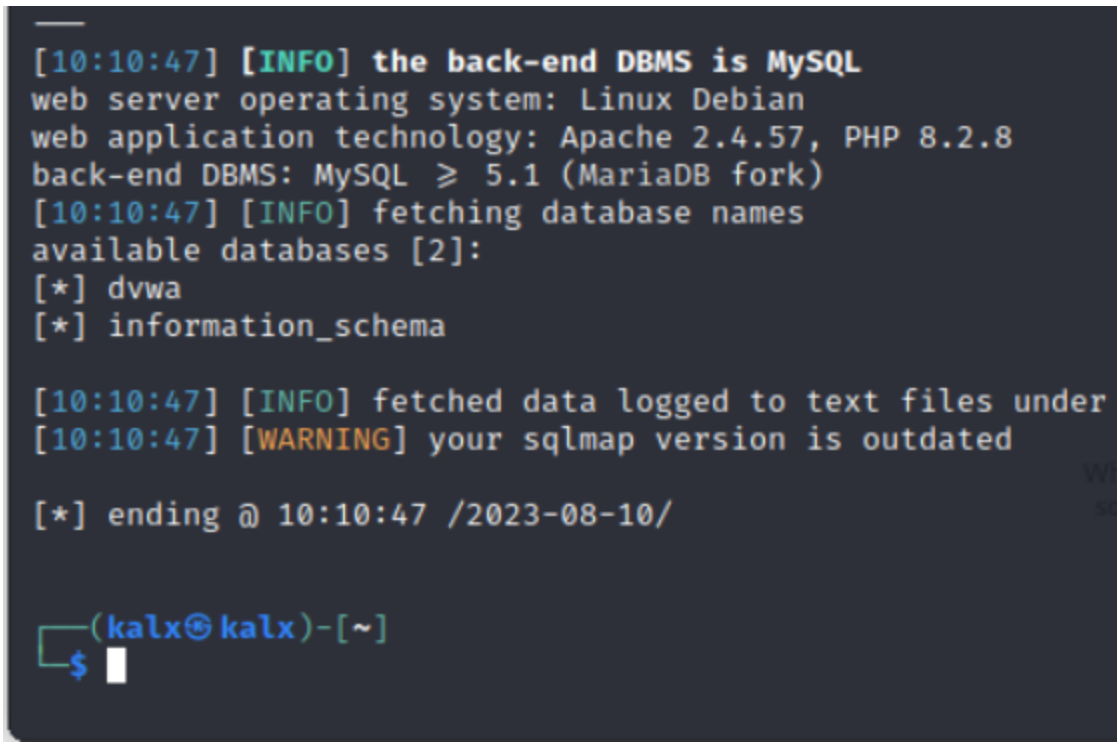


Tekan n lalu enter

Tekan n lalu enter

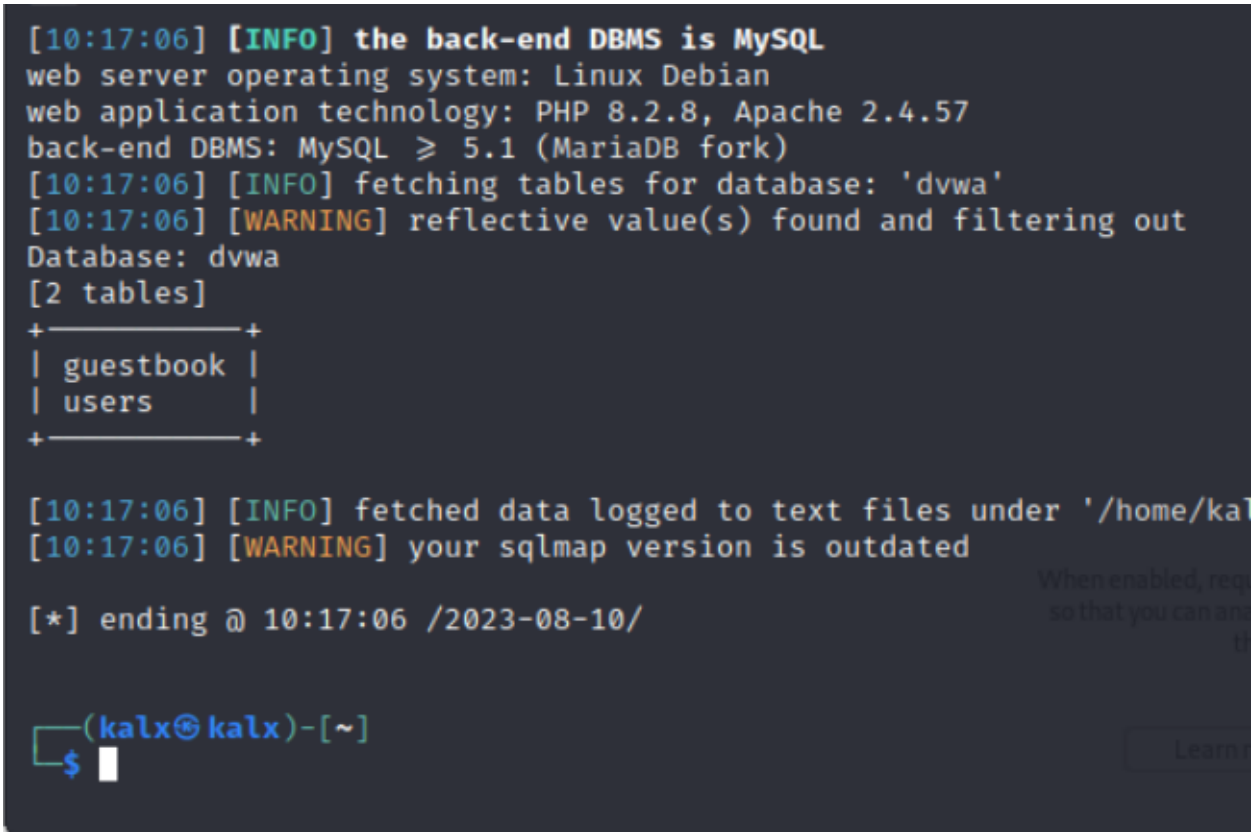


akan muncul 2 database yaitu dvwa dan information_schema , sejauh ini database yang kemungkinan berisi data user ada di database dvwa sedangkan db information_schema hanya berisi data default sistem mysql



Selanjutnya coba untuk melihat tabel yang ada pada database dvwa dengan memodifikasi perintah sebelumnya. Gunakan perintah berikut

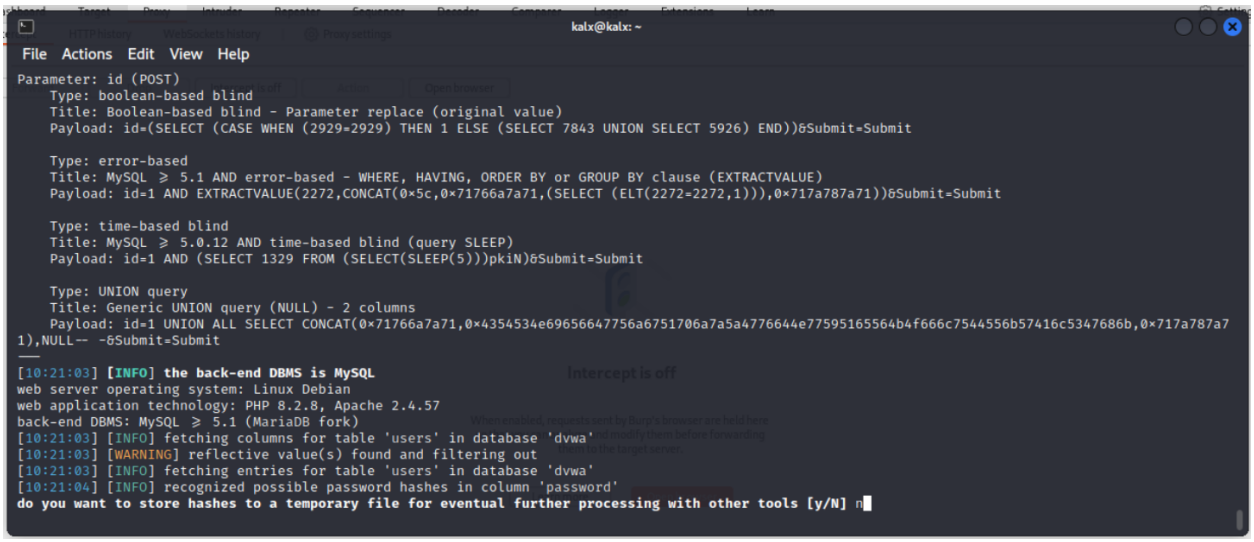
```
sqlmap -r sql-req.txt -D dvwa --tables
```



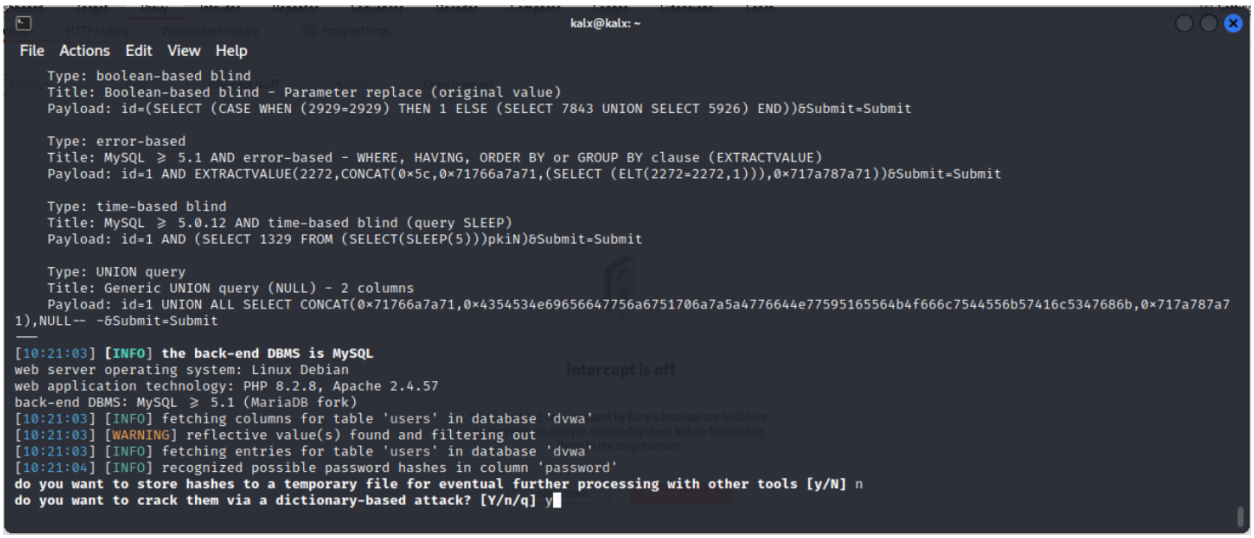
Muncul 2 tabel, yaitu guestbook dan users, coba untuk melihat isi dari tabel users menggunakan perintah berikut

```
sqlmap -r sql-req.txt -D dvwa -T users --dump
```

Ketik n lalu enter



Ketik y lalu enter



Langsung tekan enter

Tekan n lalu enter

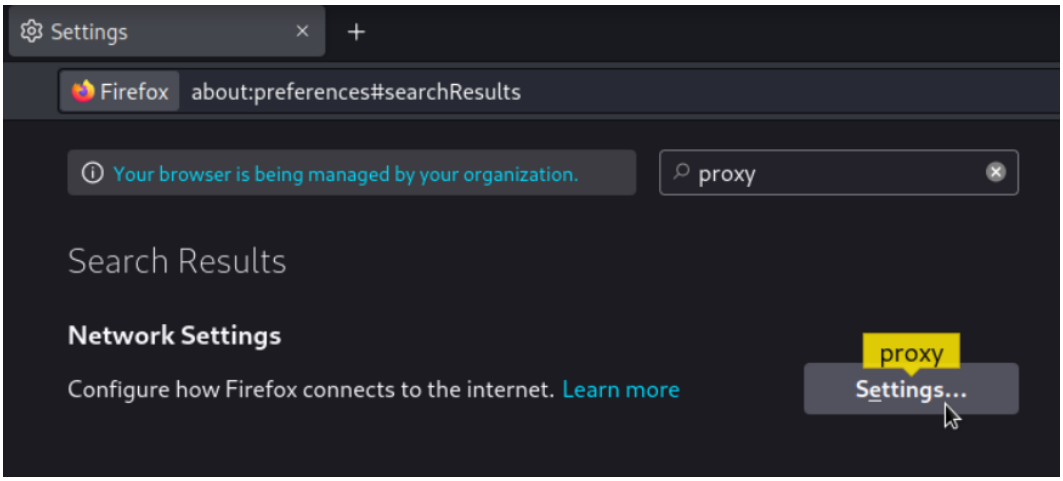
Tunggu proses crack selesai

Akan muncul isi dari tabel users

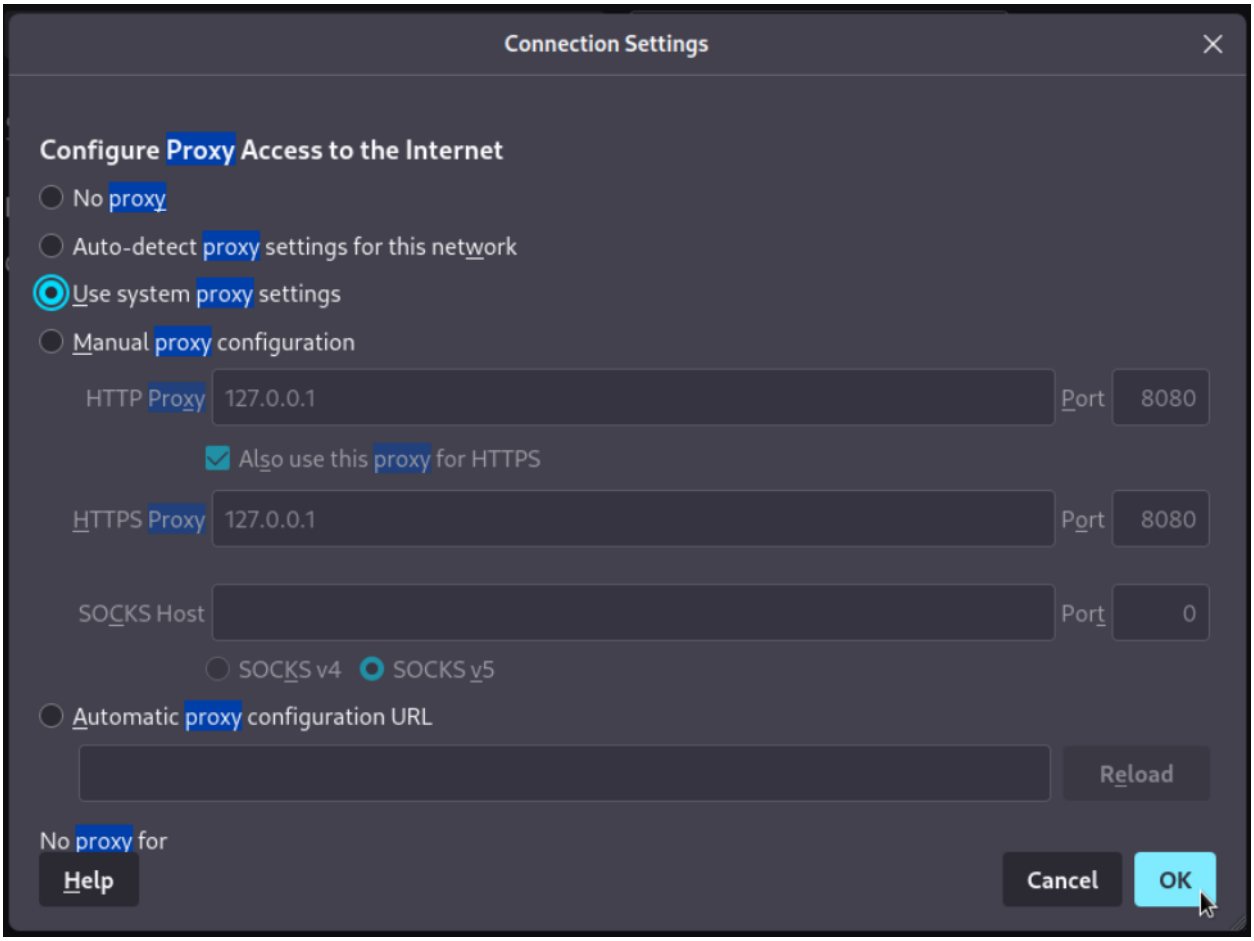
🧹 Clean up

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