

5. Brute Force Attack dengan OWASP ZAP

Disusun oleh :

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

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

Install OWASP ZAP

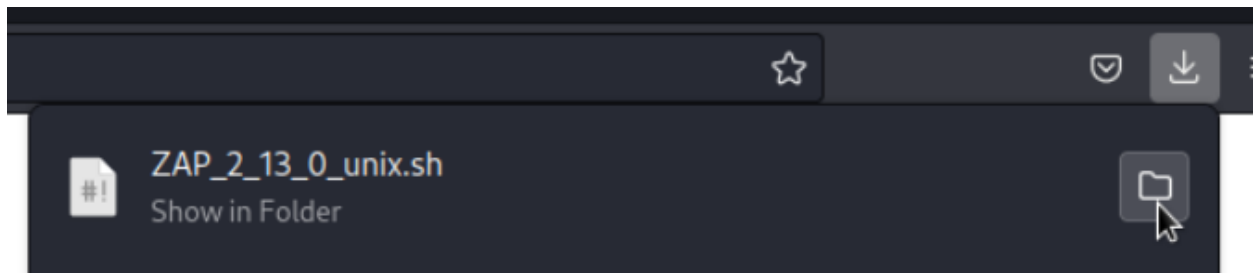
Buka browser pada Kali Linux dan download OWASP ZAP melalui link berikut

<https://www.zaproxy.org/download/>

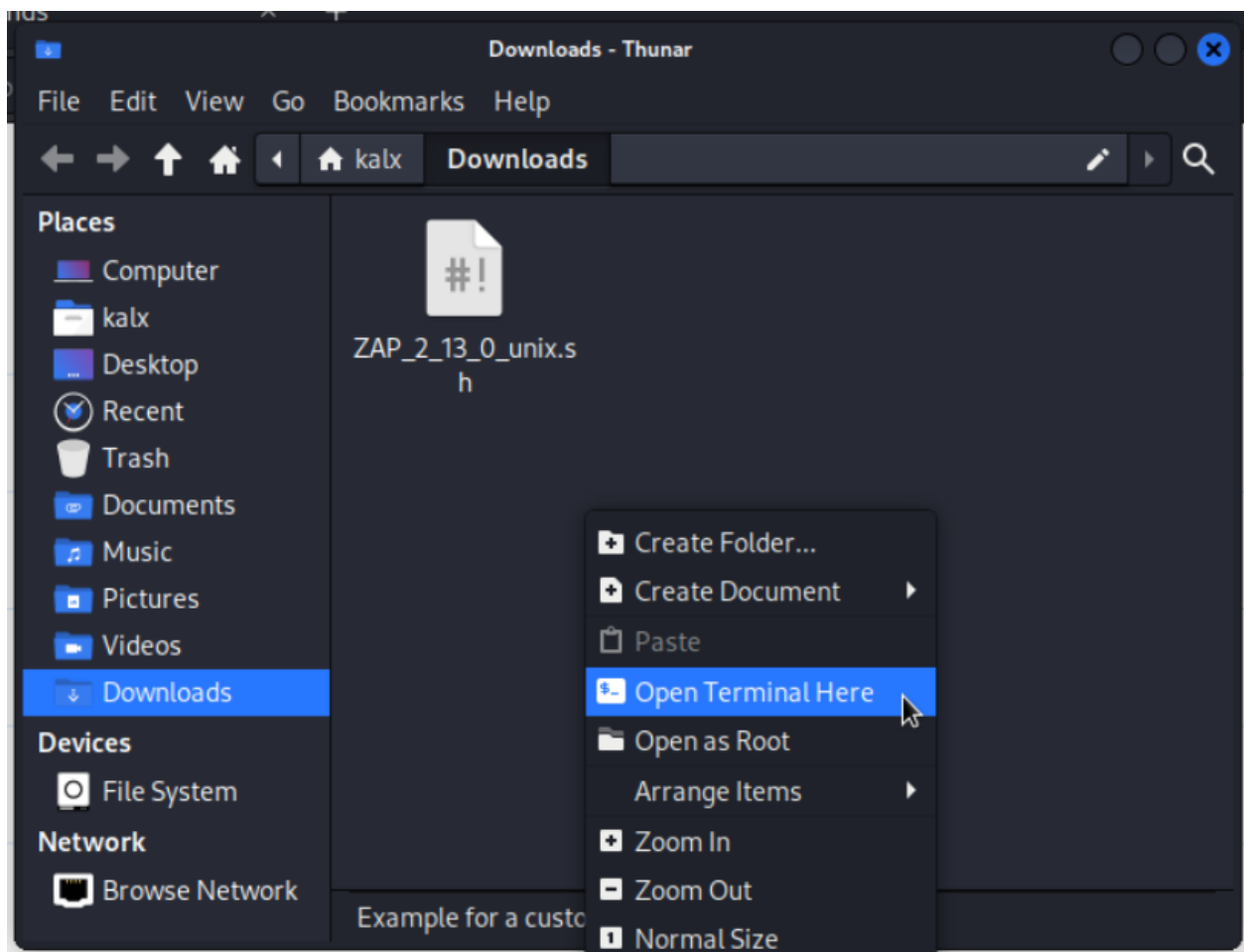
Pilih Linux Installer

ZAP 2.13.0		
Windows (64) Installer	195 MB	Download
Windows (32) Installer	195 MB	Download
Linux Installer	199 MB	Download
Linux Package	196 MB	Download
macOS (amd64) Installer	224 MB	Download
macOS (aarch64) Installer	223 MB	Download
Cross Platform Package	225 MB	Download
Core Cross Platform Package	88 MB	Download

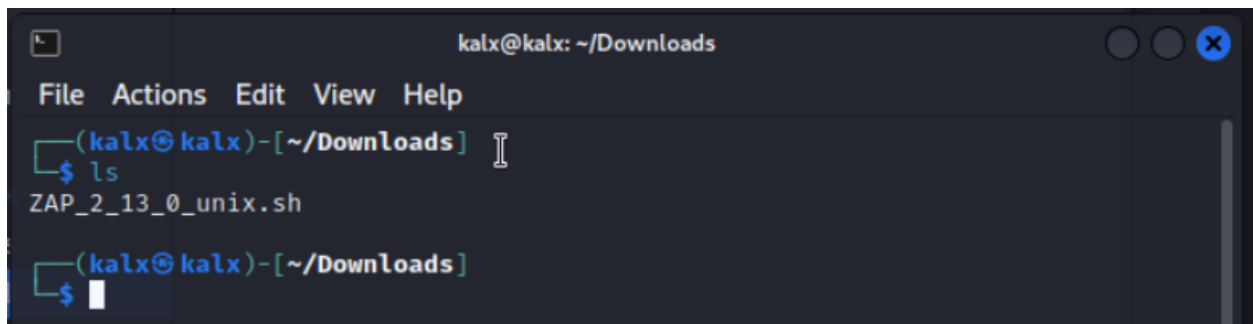
Buka folder file yang sudah terdownload



Klik kanan pada direktori dan pilih “Open Terminal Here” dan terminal baru akan terbuka



Ketik `ls` untuk memastikan file OWASP ZAP ada dalam direktori

A terminal window titled 'kalx@kalx: ~/Downloads' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kalx@kalx)-[~/Downloads]'. The user enters '\$ ls' and the output is 'ZAP_2_13_0_unix.sh'. The prompt returns to '(kalx@kalx)-[~/Downloads]' with a cursor on the next line.

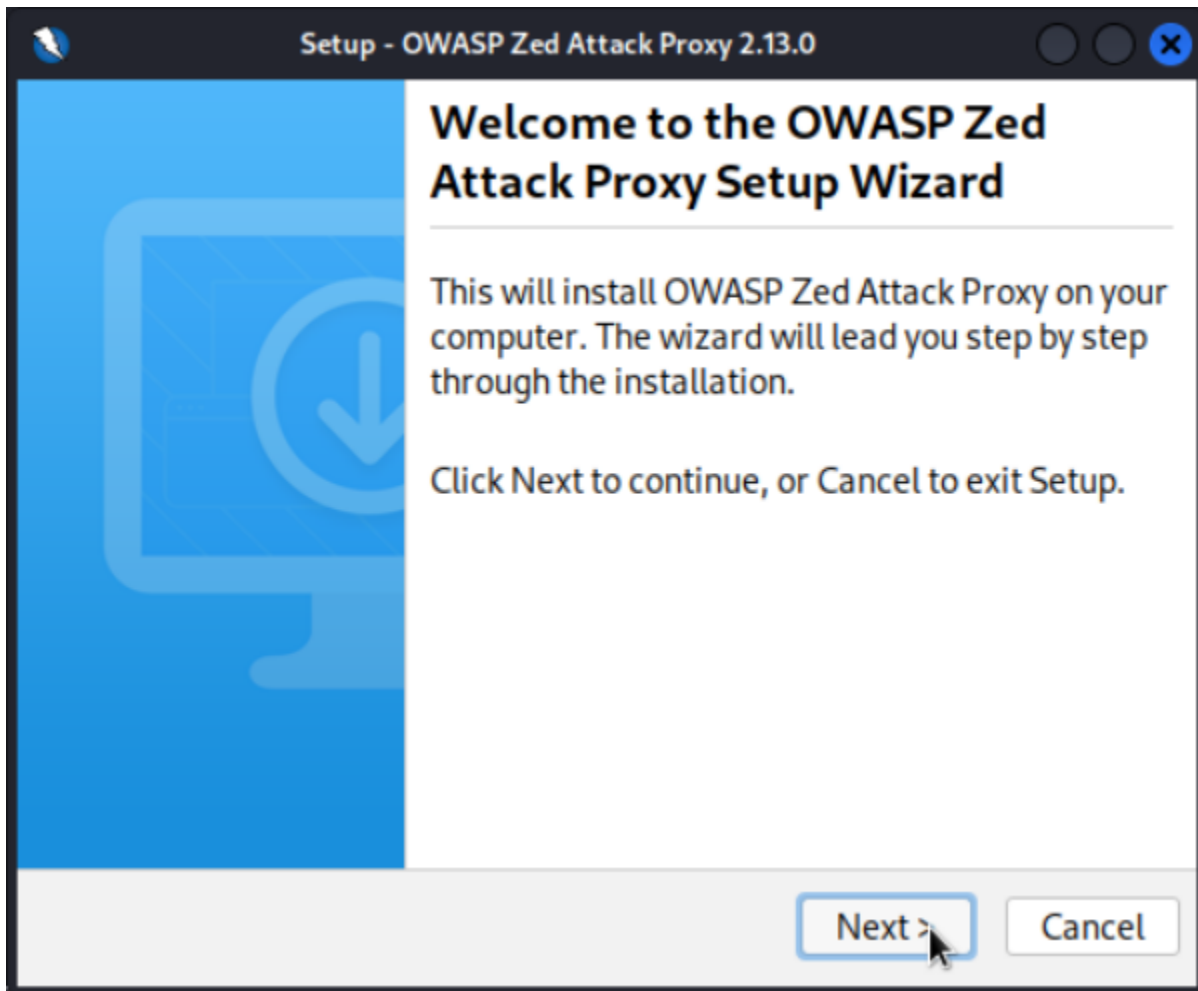
```
kalx@kalx: ~/Downloads
File Actions Edit View Help
(kalx@kalx)-[~/Downloads]
$ ls
ZAP_2_13_0_unix.sh
(kalx@kalx)-[~/Downloads]
$
```

Untuk menjalankan instalasi, ketik perintah berikut

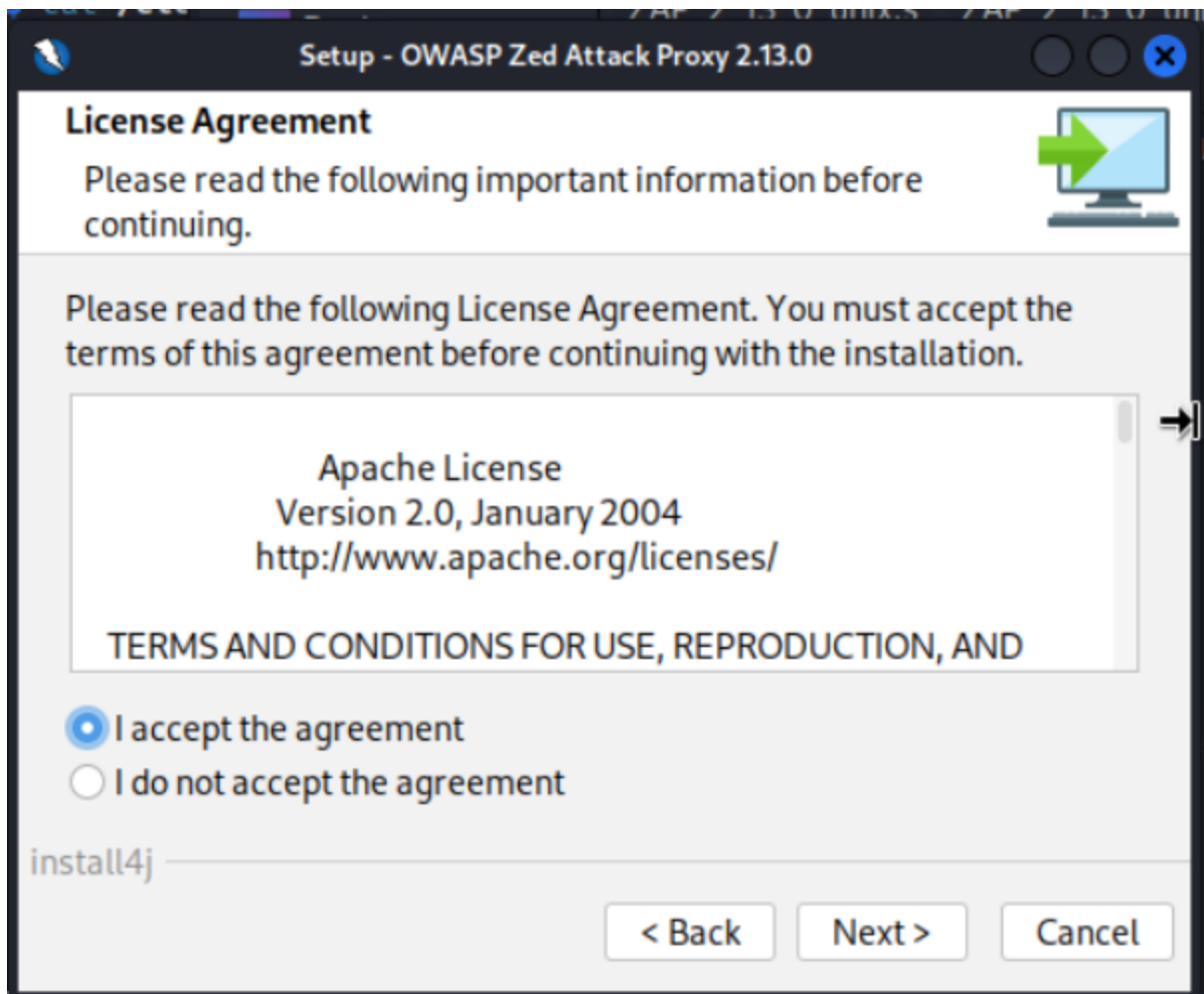
```
sudo sh ZAP_2_13_0_unix.sh
```

Masukkan password user jika diminta

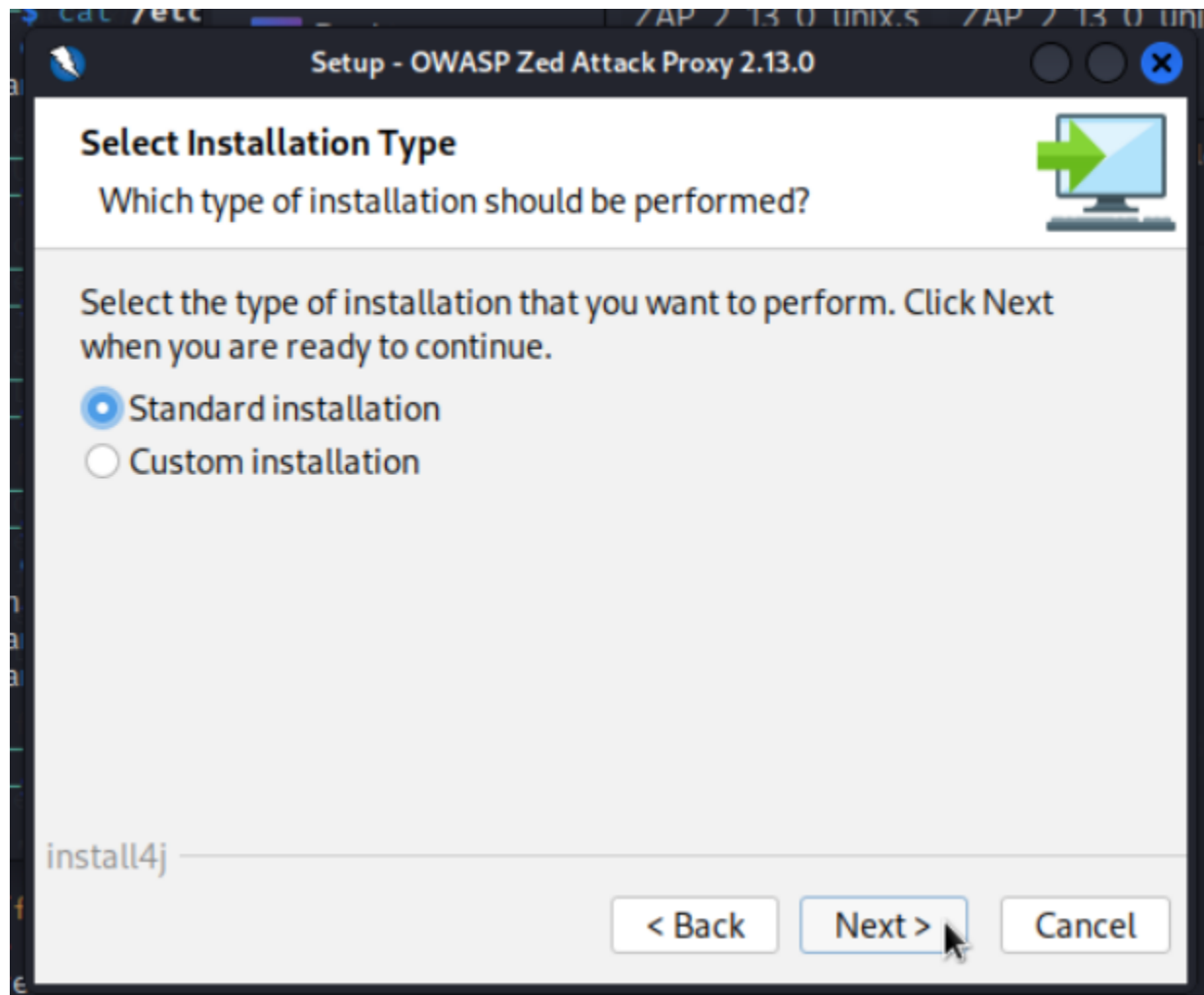
Selanjutnya pop up installer akan terbuka, Klik Next



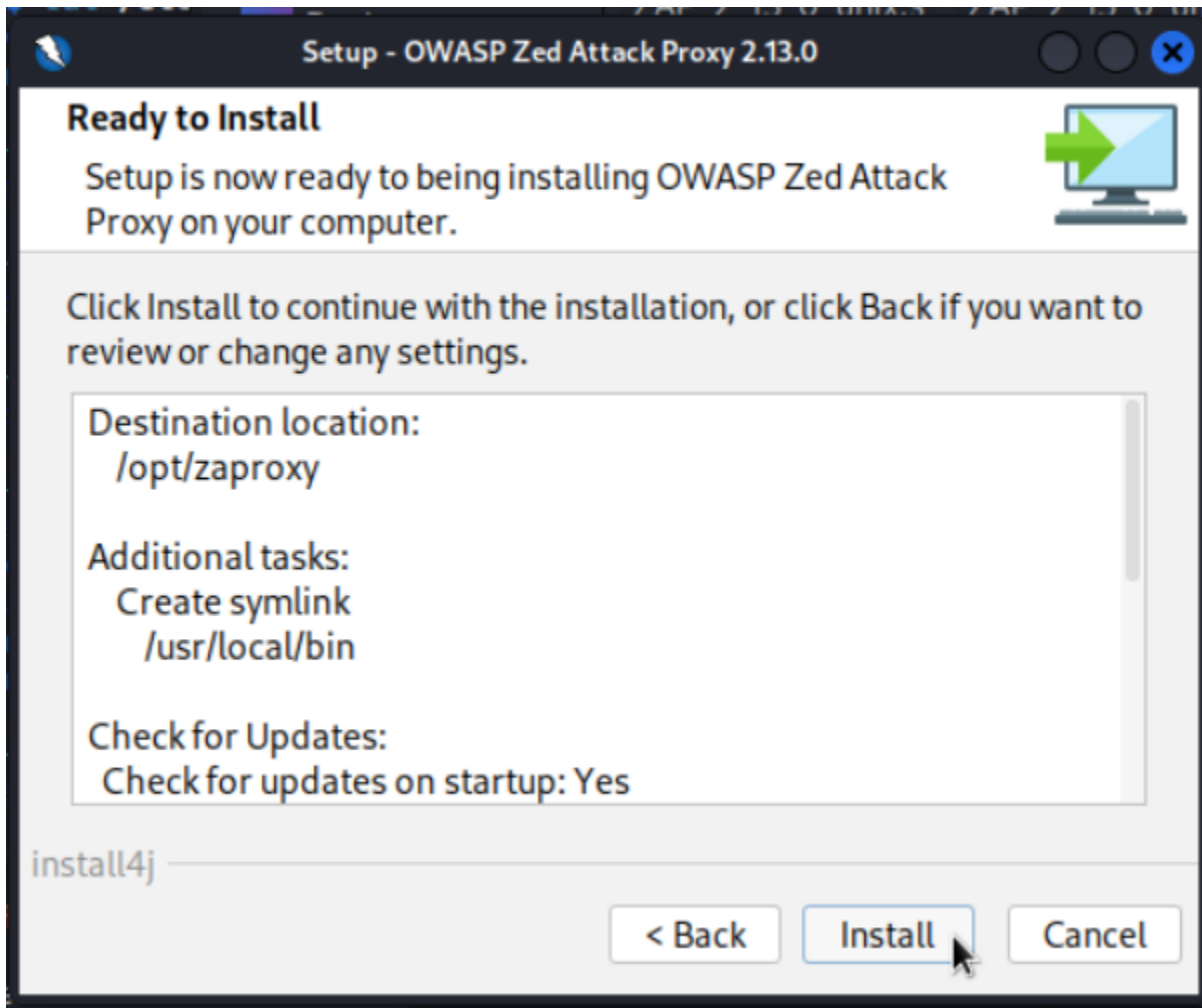
Pilih accept lalu Next



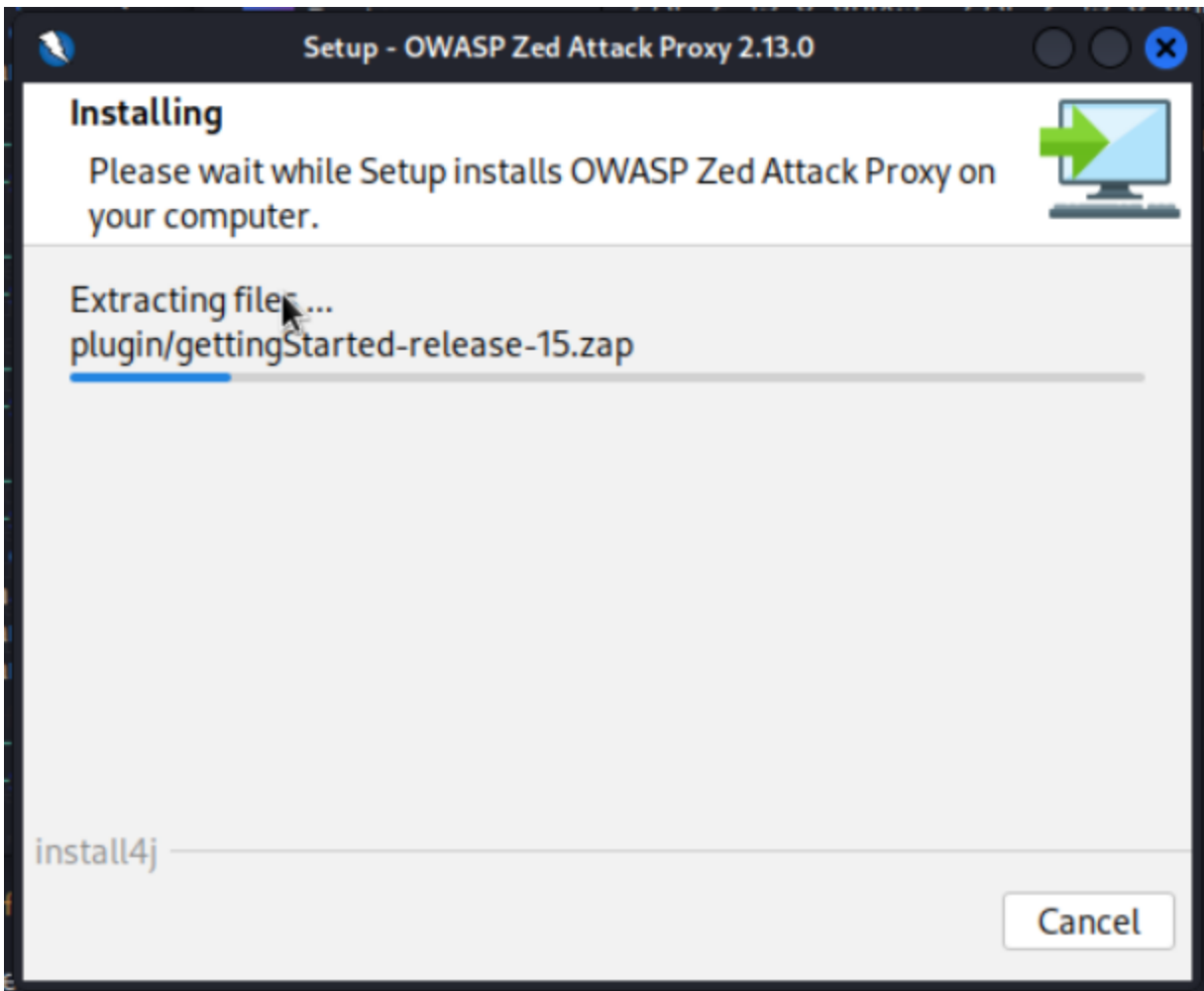
Pilih Standard installation lalu klik Next



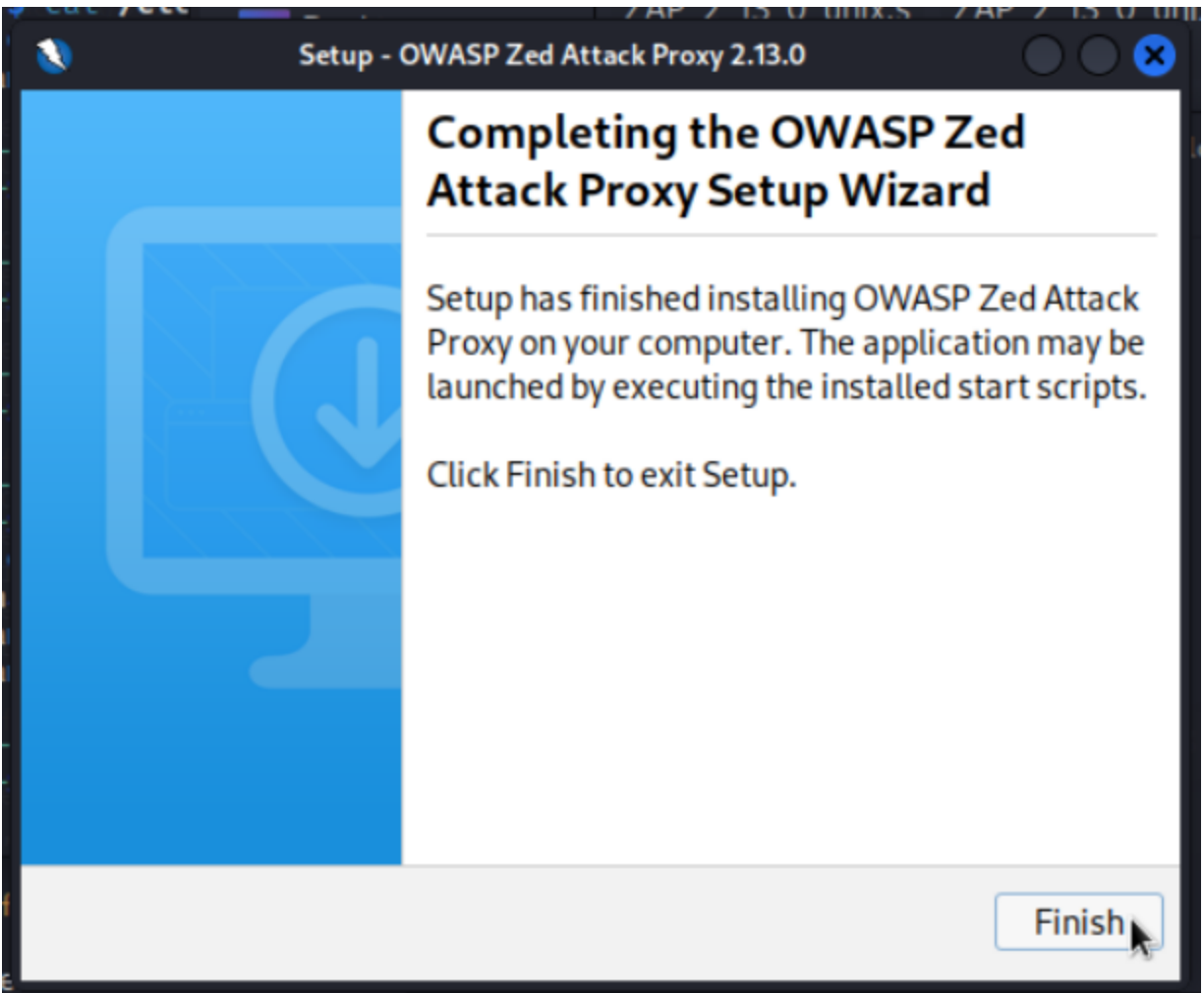
Klik Install



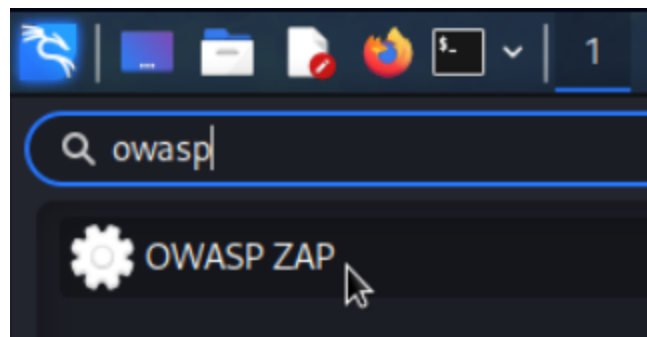
Tunggu proses install selesai



Setelah instalasi selesai, klik Finish

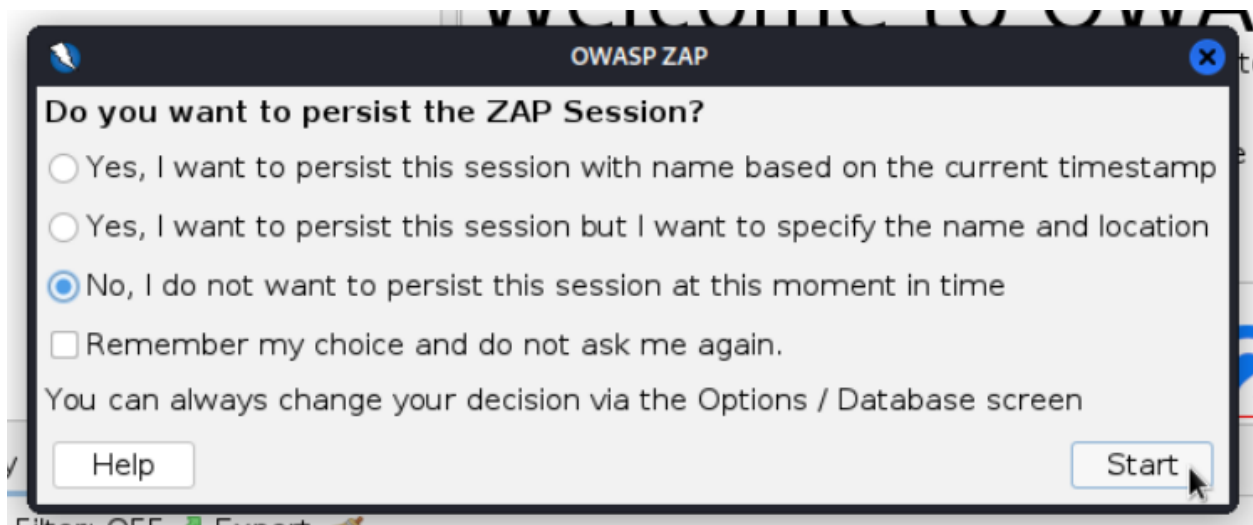


Pastikan OWASP ZAP telah terinstall

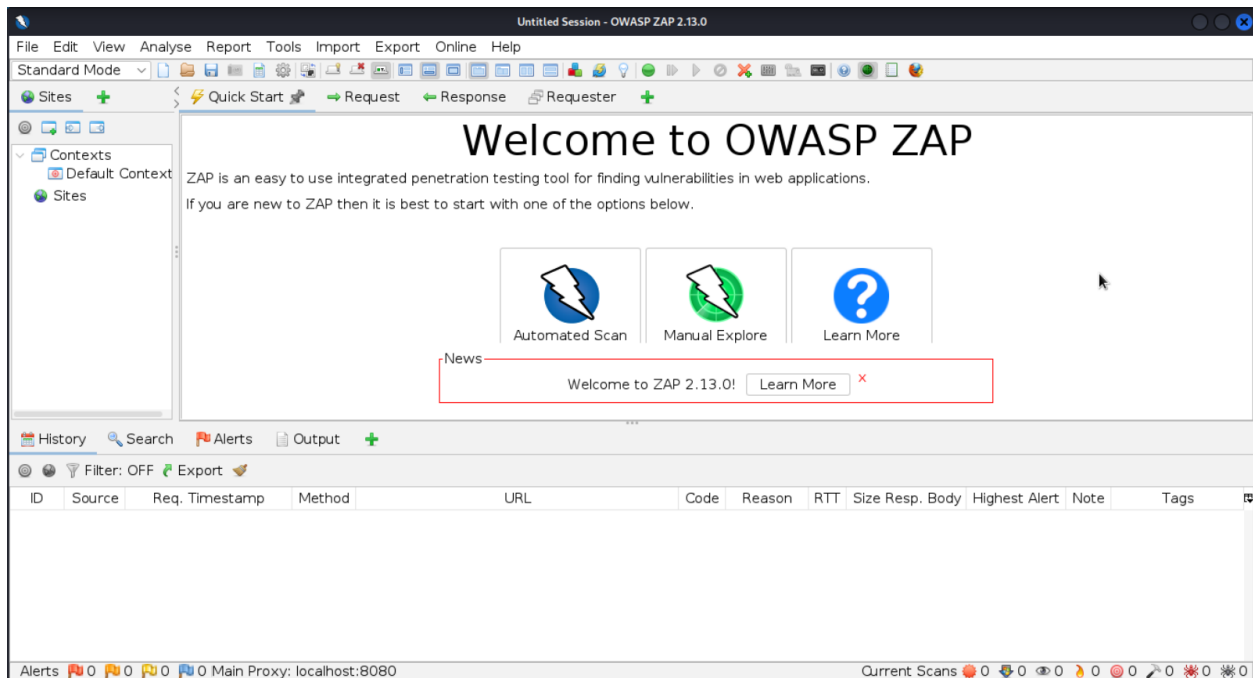




Pilih No, lalu Start

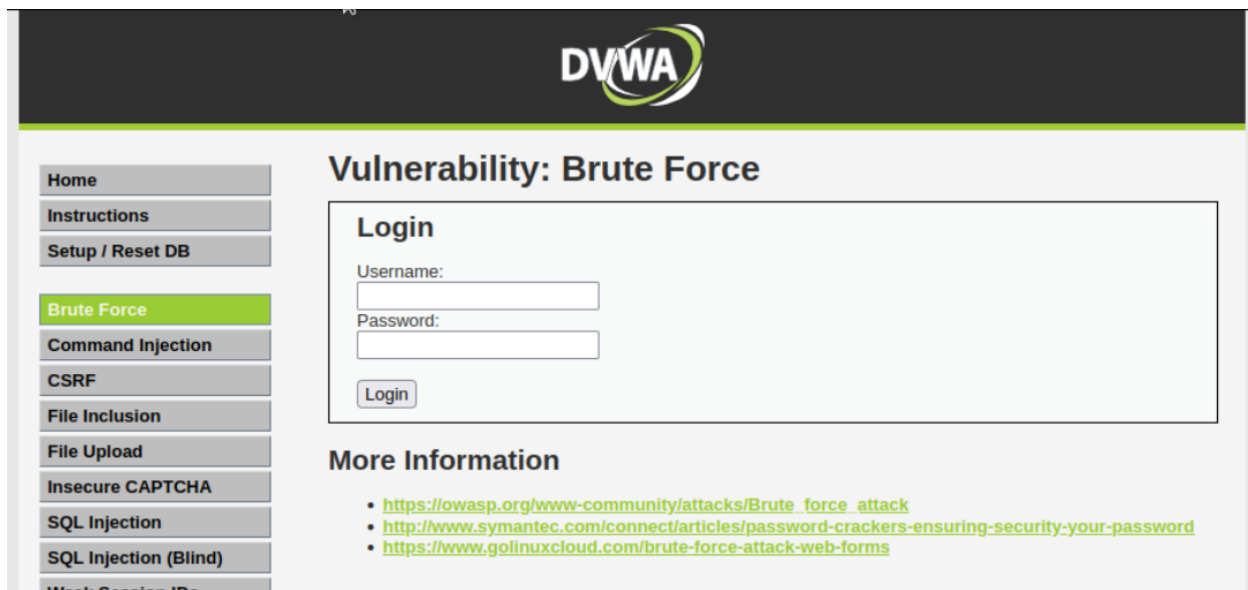


OWASP ZAP berhasil diinstall

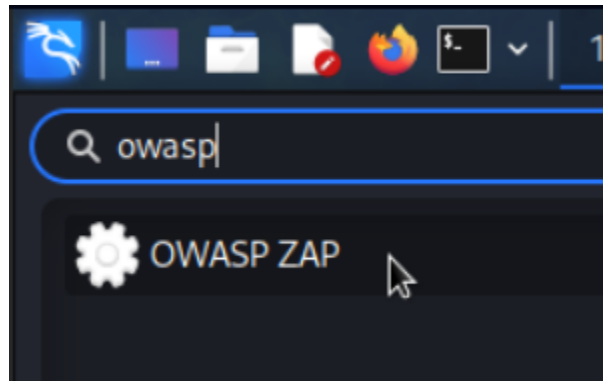


Brute Force dengan OWASP ZAP

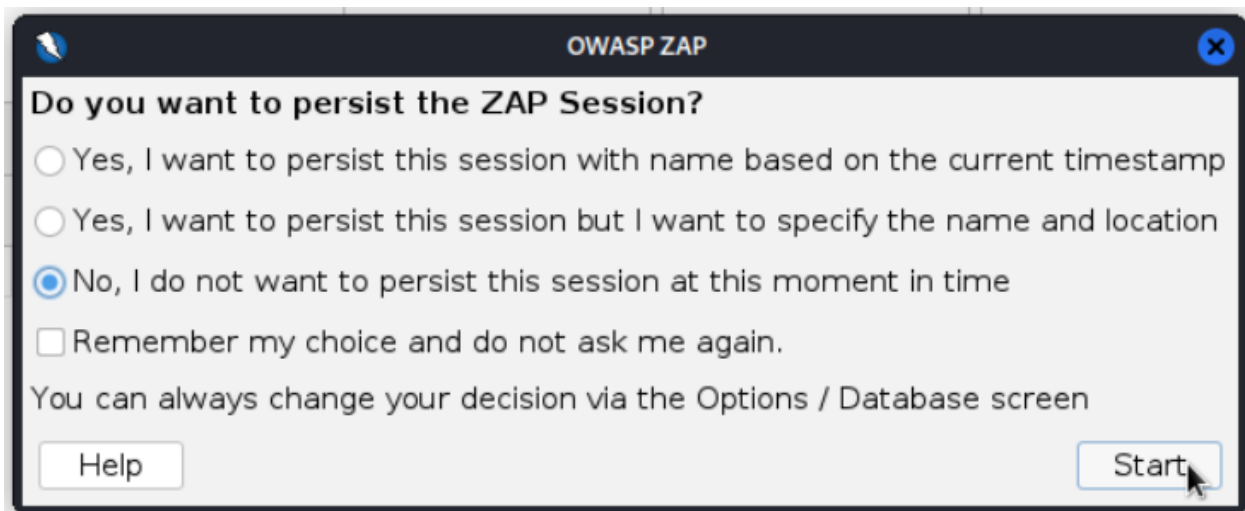
Pada tampilan awal DVWA klik bagian Brute Force



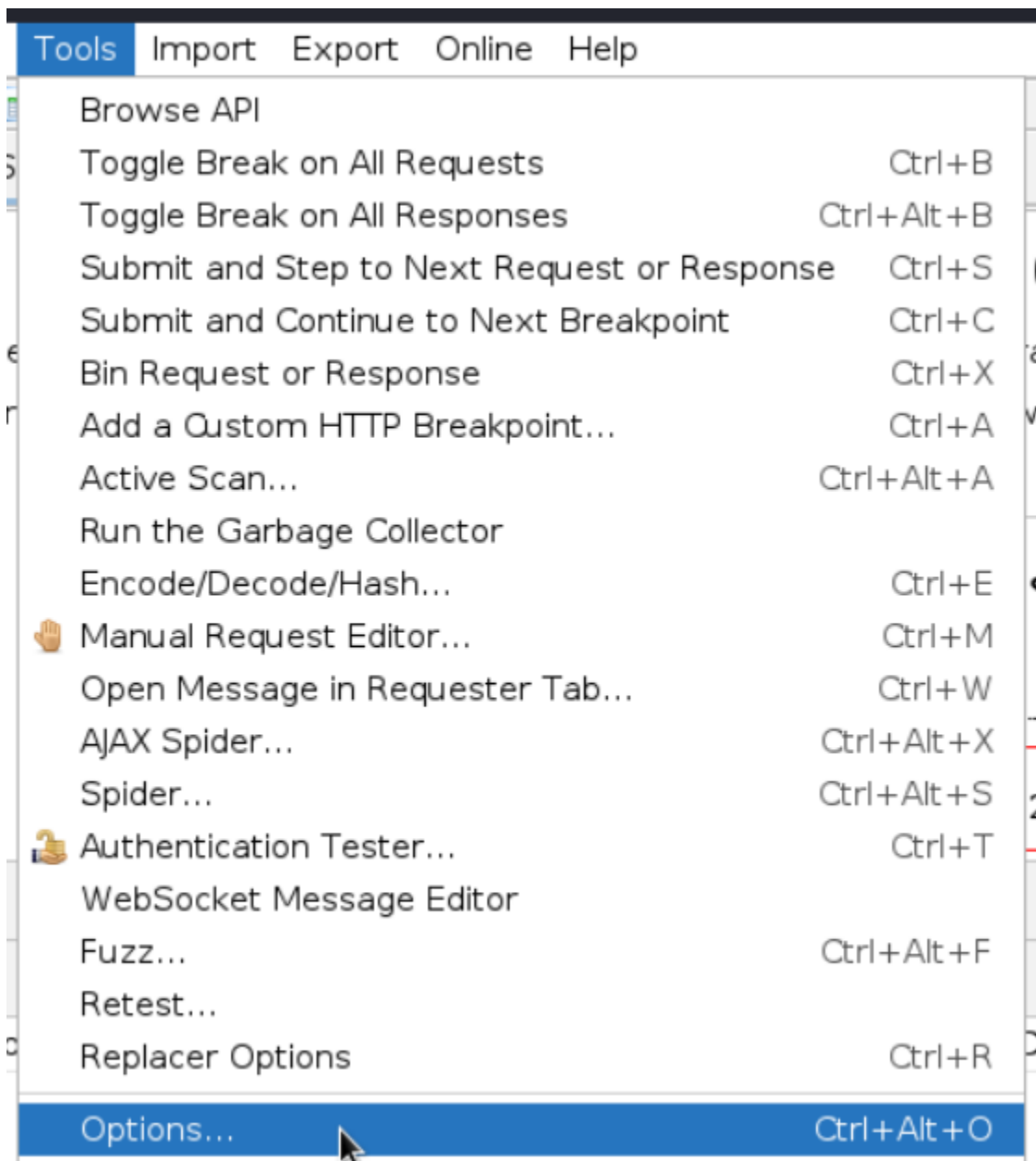
Buka OWASP ZAP yang telah terinstall



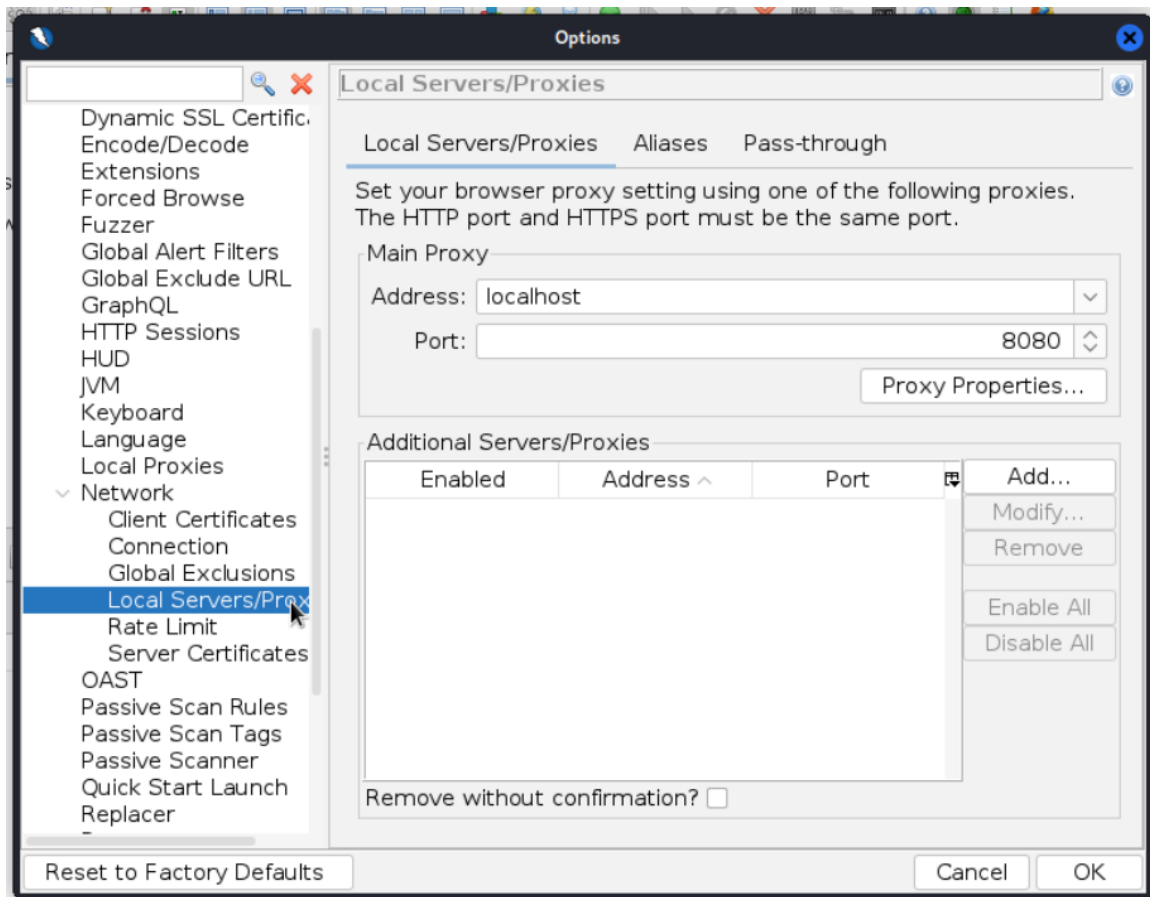
Pilih No, lalu Start



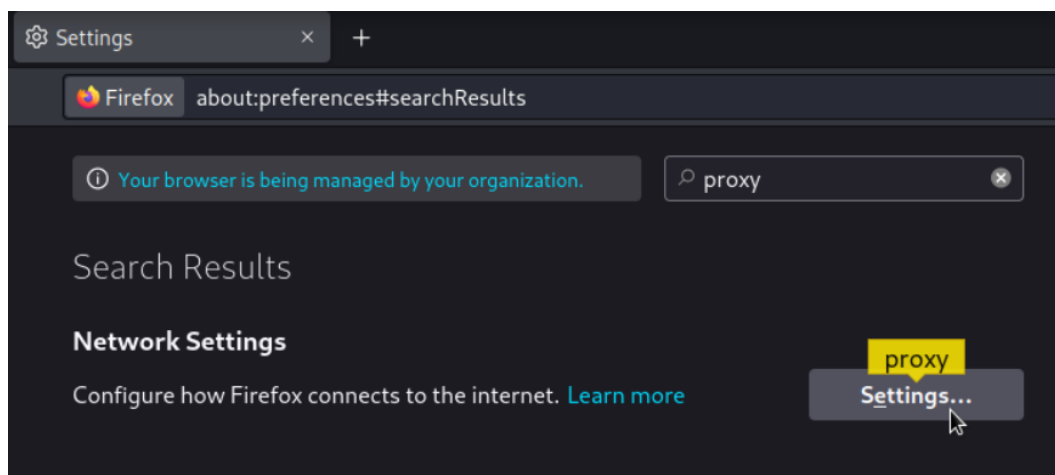
Klik tab Tools lalu pilih Options



Cari Network lalu pilih Local Servers/Proxies, pastikan Address dan Port sudah terisi Address dan Port ini yang nanti akan dijadikan proxy oleh browser

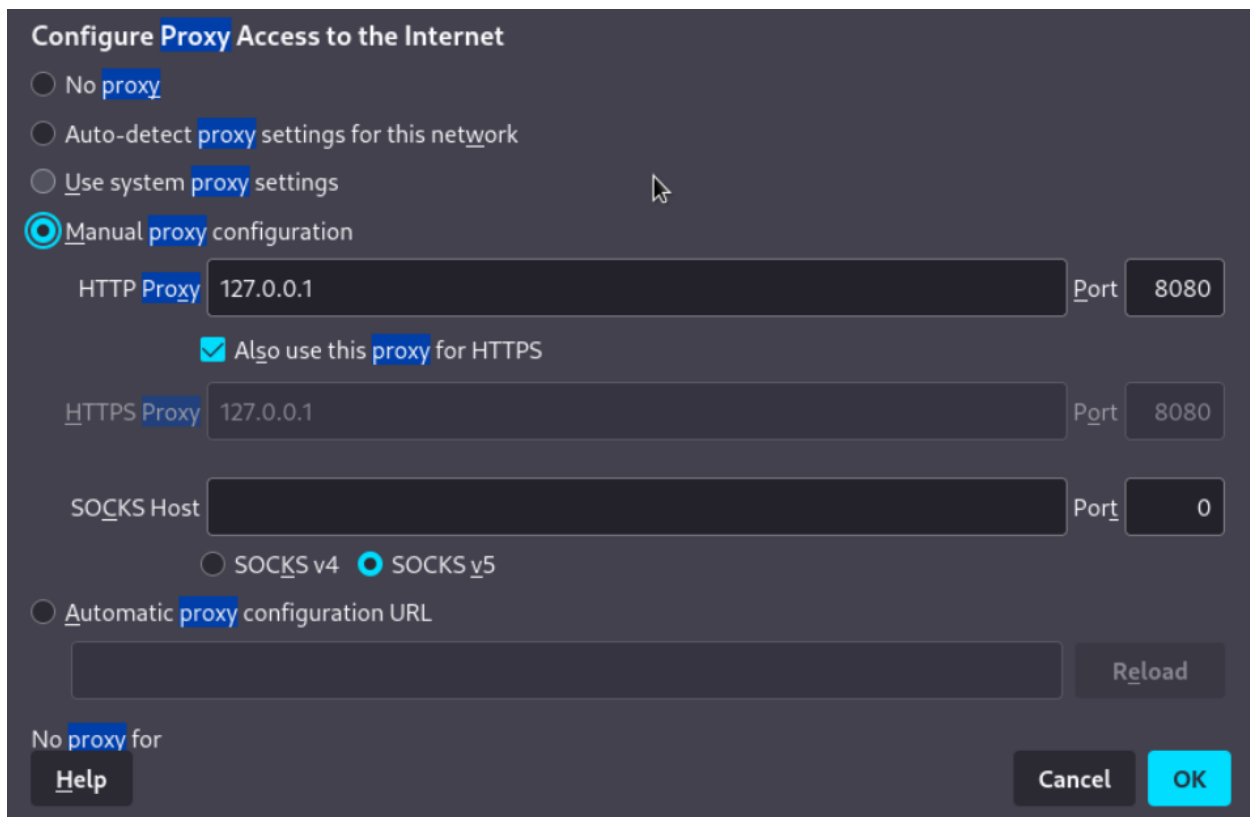


Kembali ke browser, pada Firefox masuk ke settings dan pada kolom pencarian ketikkan proxy



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

Pada HTTP Proxy masukkan IP dan Port yang sebelumnya didapat dari OWASP ZAP lalu klik OK



Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy: 127.0.0.1 Port: 8080

☒ Also use this proxy for HTTPS

HTTPS Proxy: 127.0.0.1 Port: 8080

SOCKS Host: Port: 0

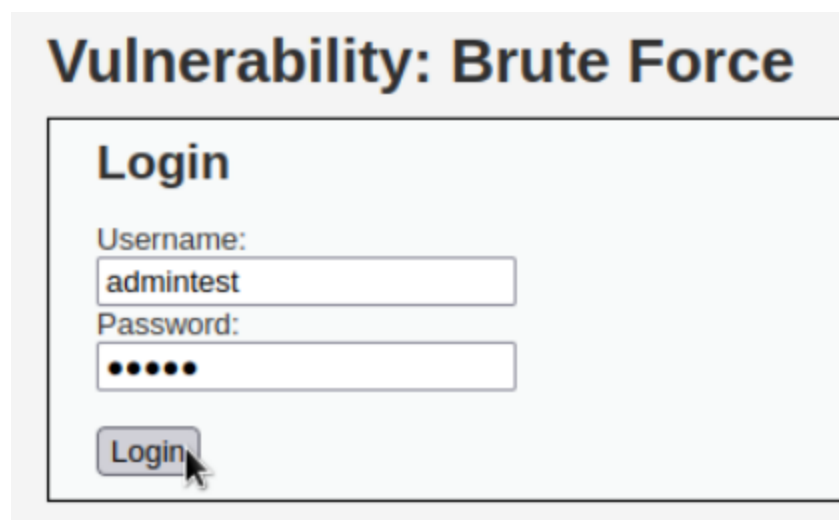
☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

No proxy for

[Help](#) [Cancel](#) [OK](#)

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



Vulnerability: Brute Force

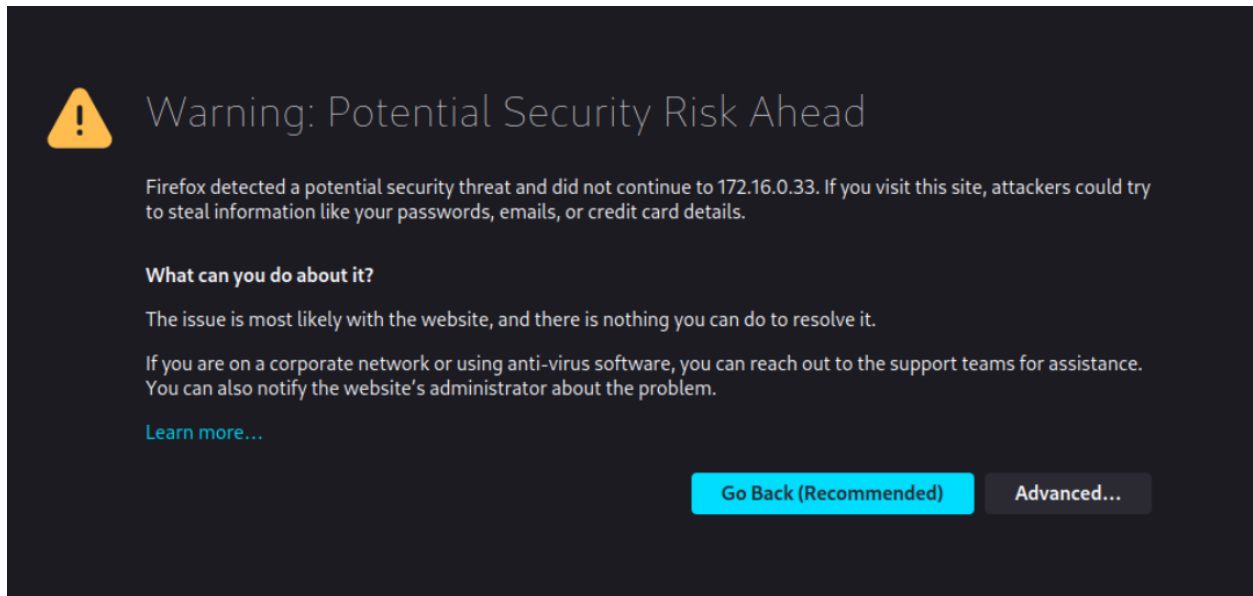
Login

Username: admintest

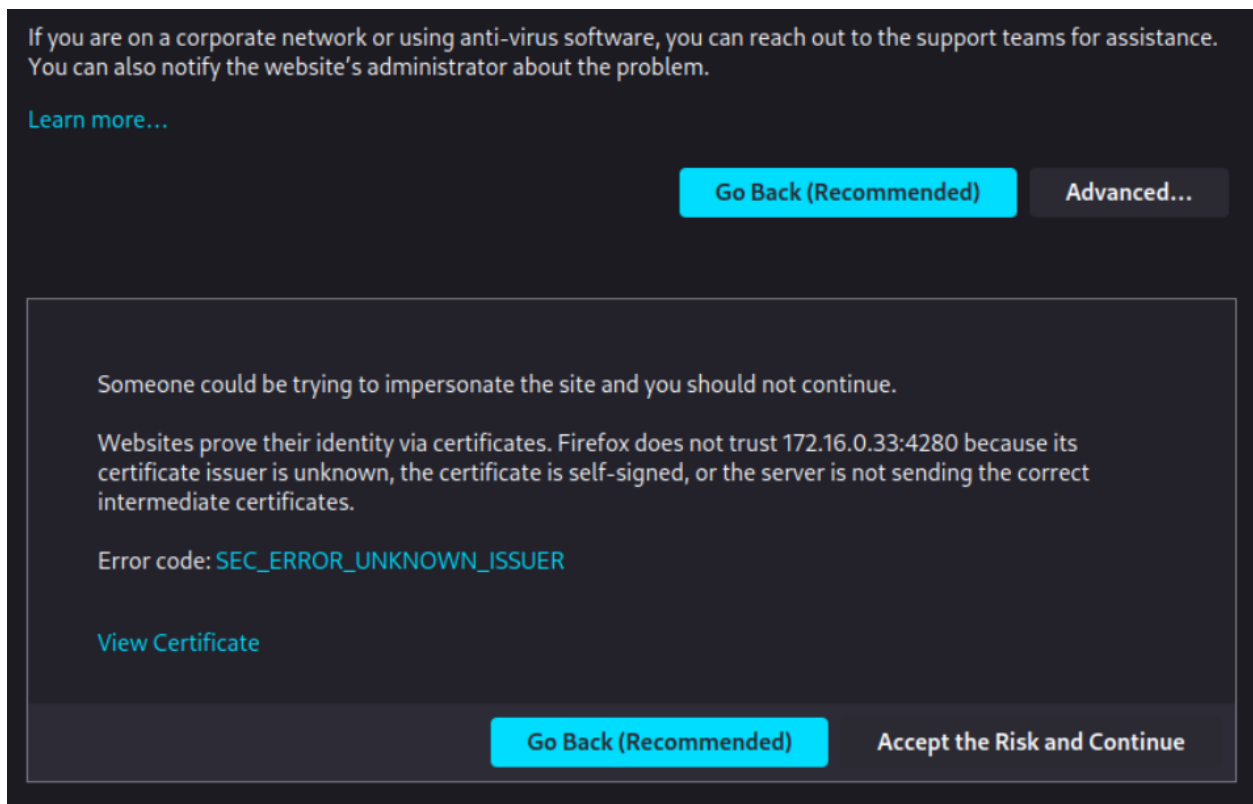
Password: •••••

[Login](#)

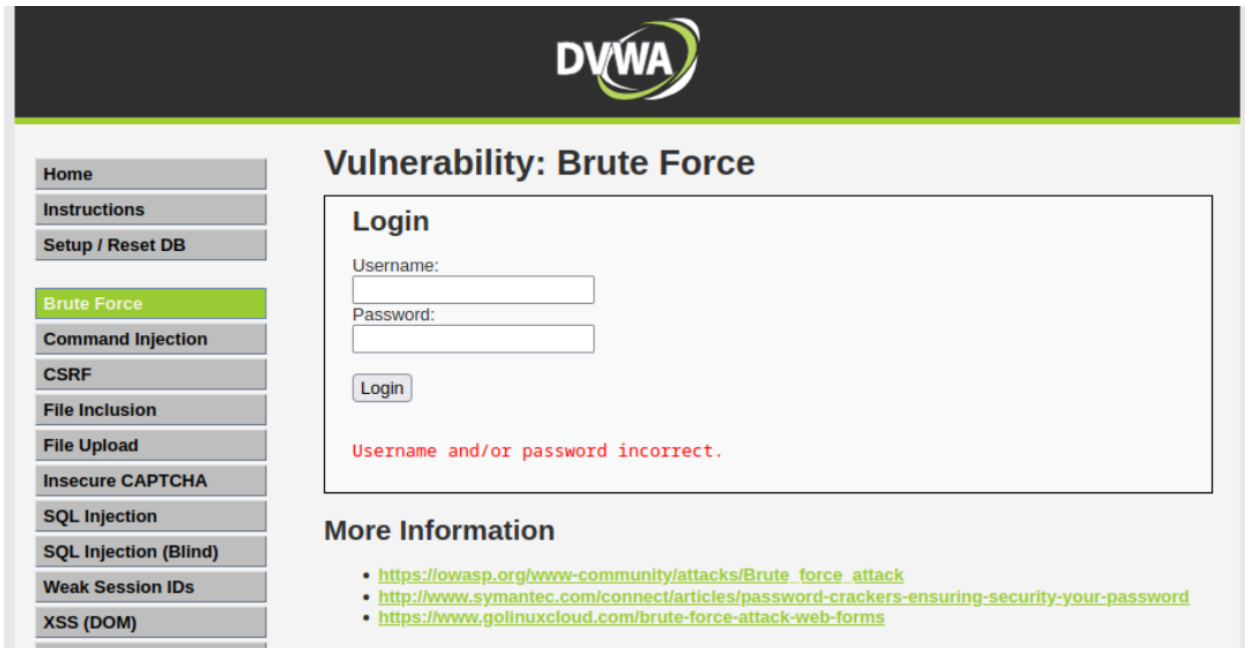
Tekan Login, jika muncul warning, klik Advanced



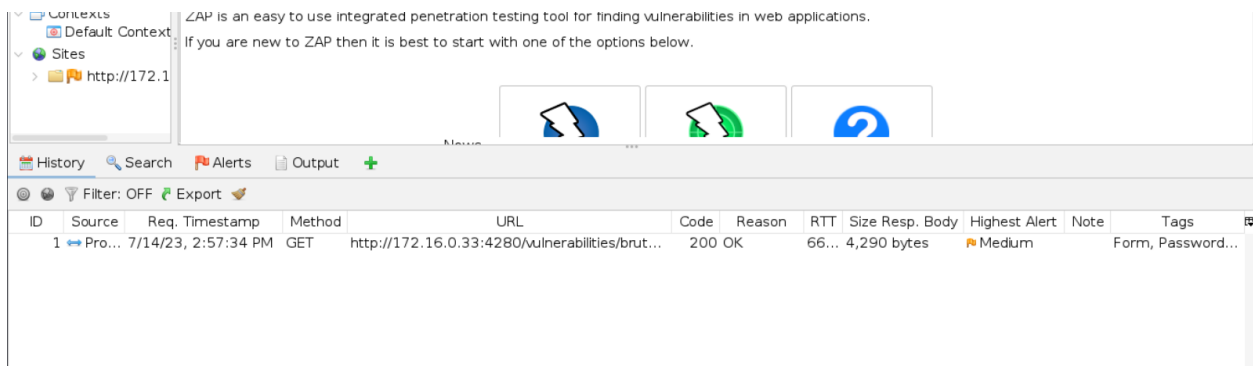
Klik Accept the Risk and Continue



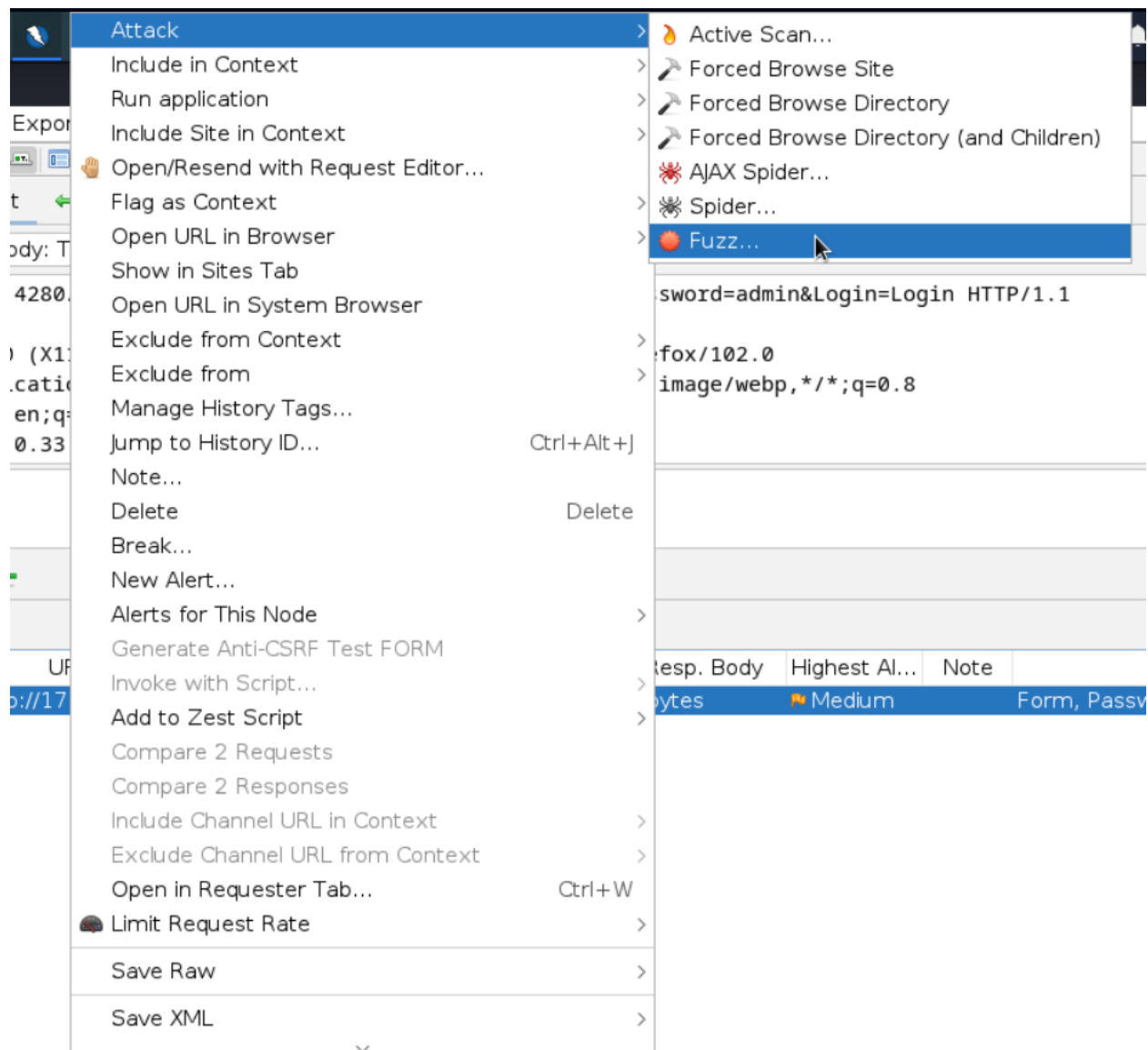
Maka akan dikembalikan ke halaman DVWA



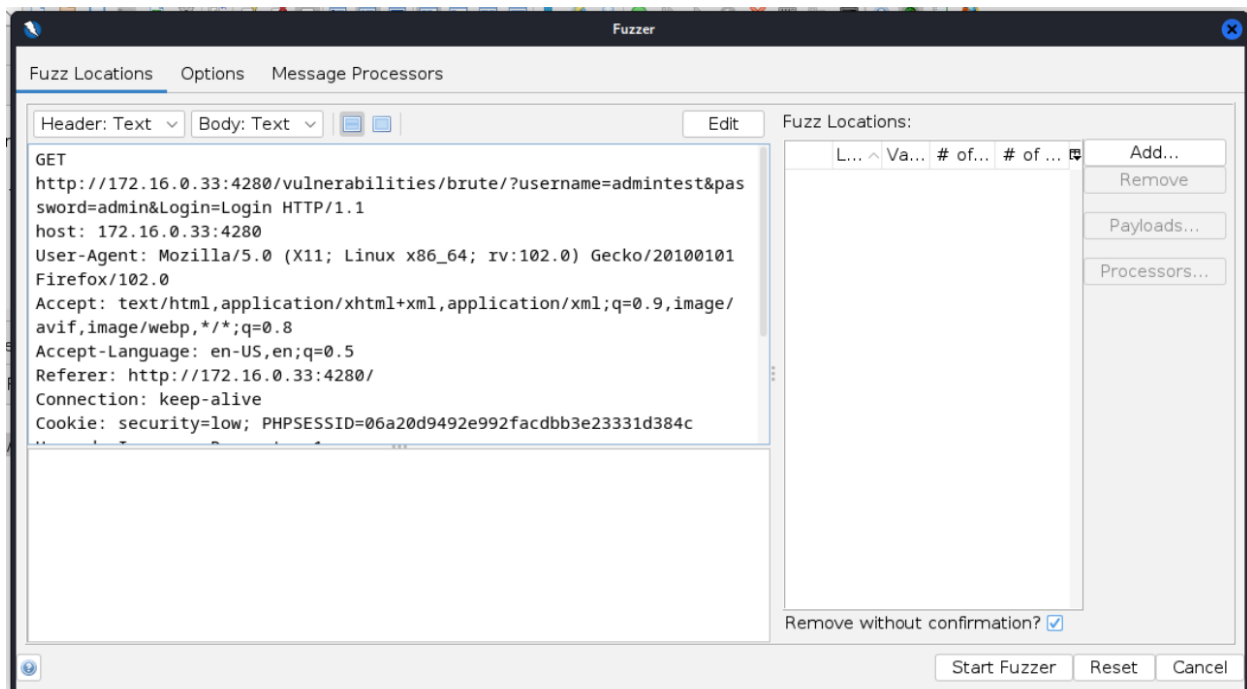
Kembali ke OWASP ZAP, pada bagian History akan muncul hasil capture dari browser



Klik kanan pada hasil capture lalu pilih Attack → Fuzz

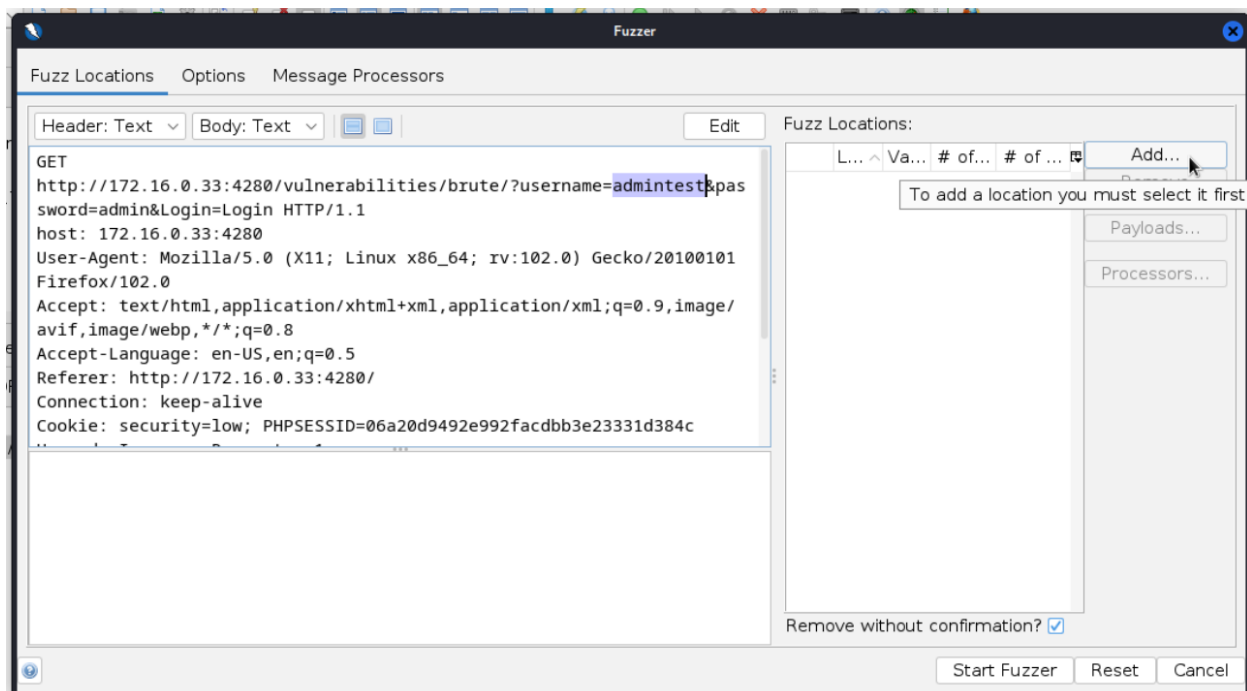


Akan muncul window baru, disini tahap identifikasi payload dilakukan

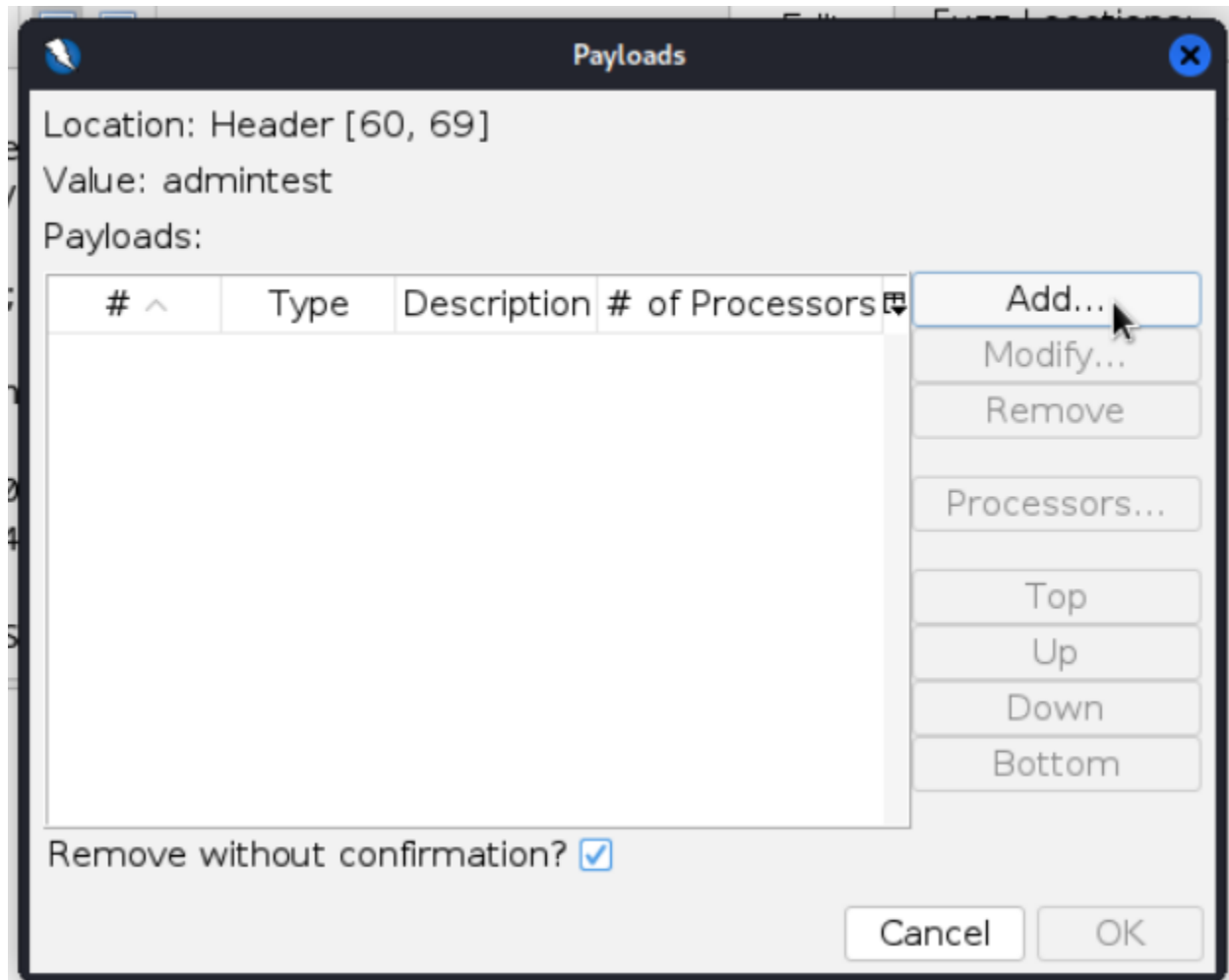


Untuk membuat payload, seleksi string dari variabel yang akan dijadikan payload, lalu klik add

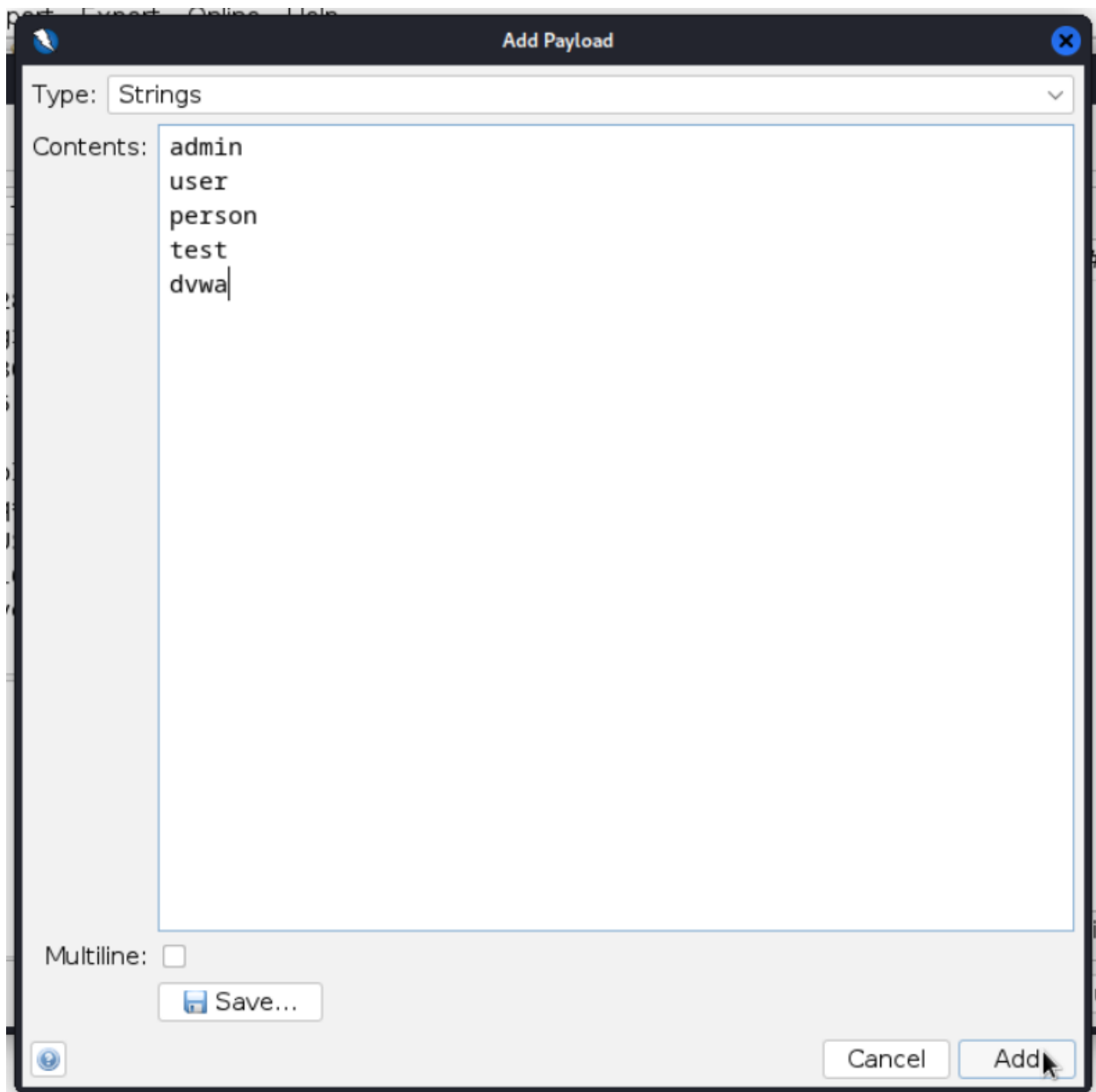
Contoh disini akan melakukan brute force pada username dan password, maka seleksi nilai string dari username terlebih dahulu lalu klik Add



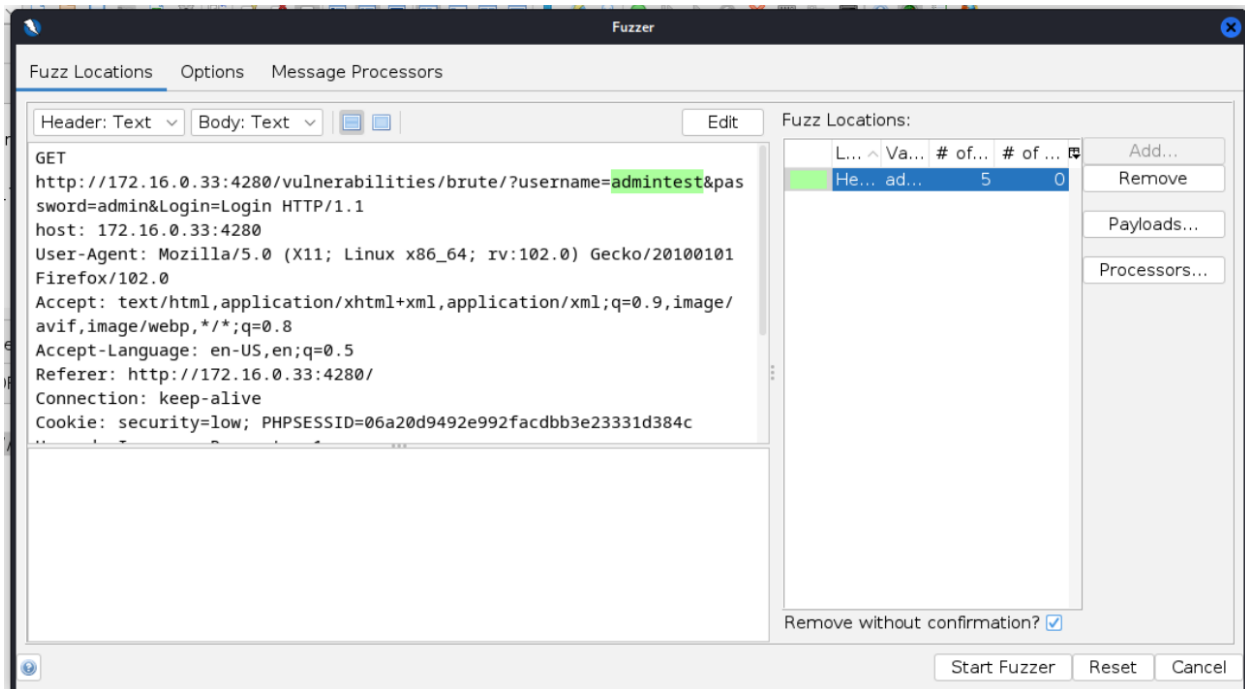
Klik Add



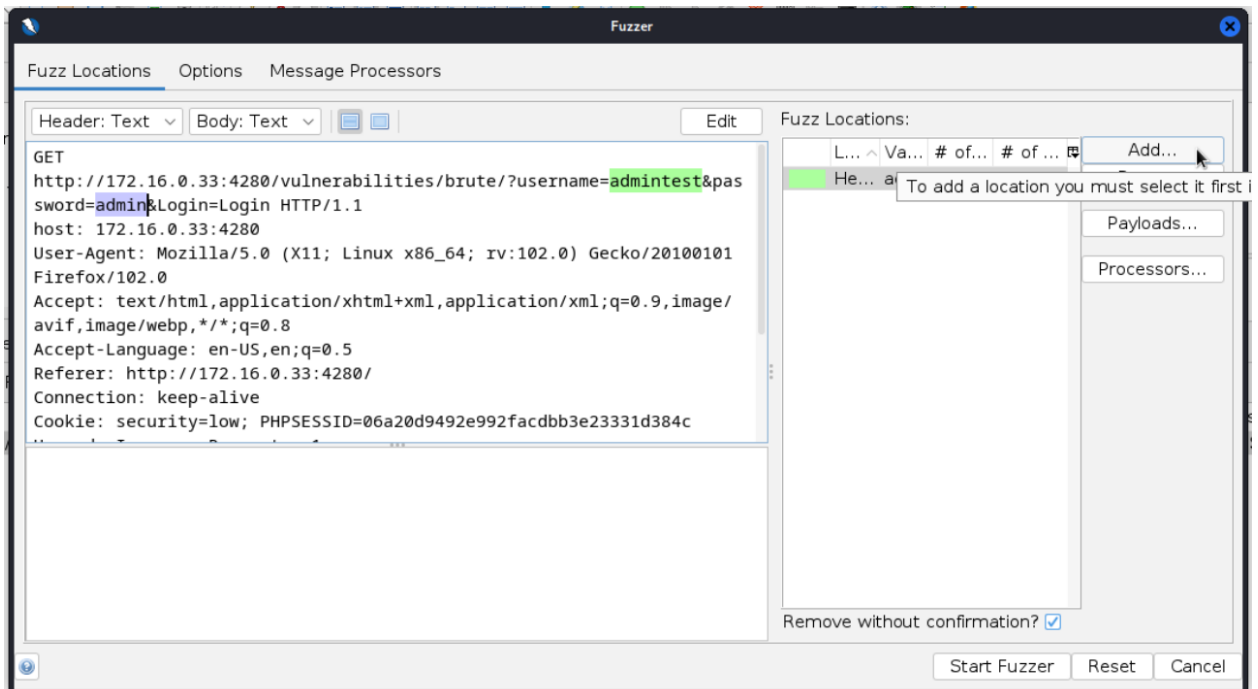
Akan muncul window baru, pada bagian Contents isikan word list atau daftar kata yang akan digunakan untuk brute force username, setelah selesai, klik Add



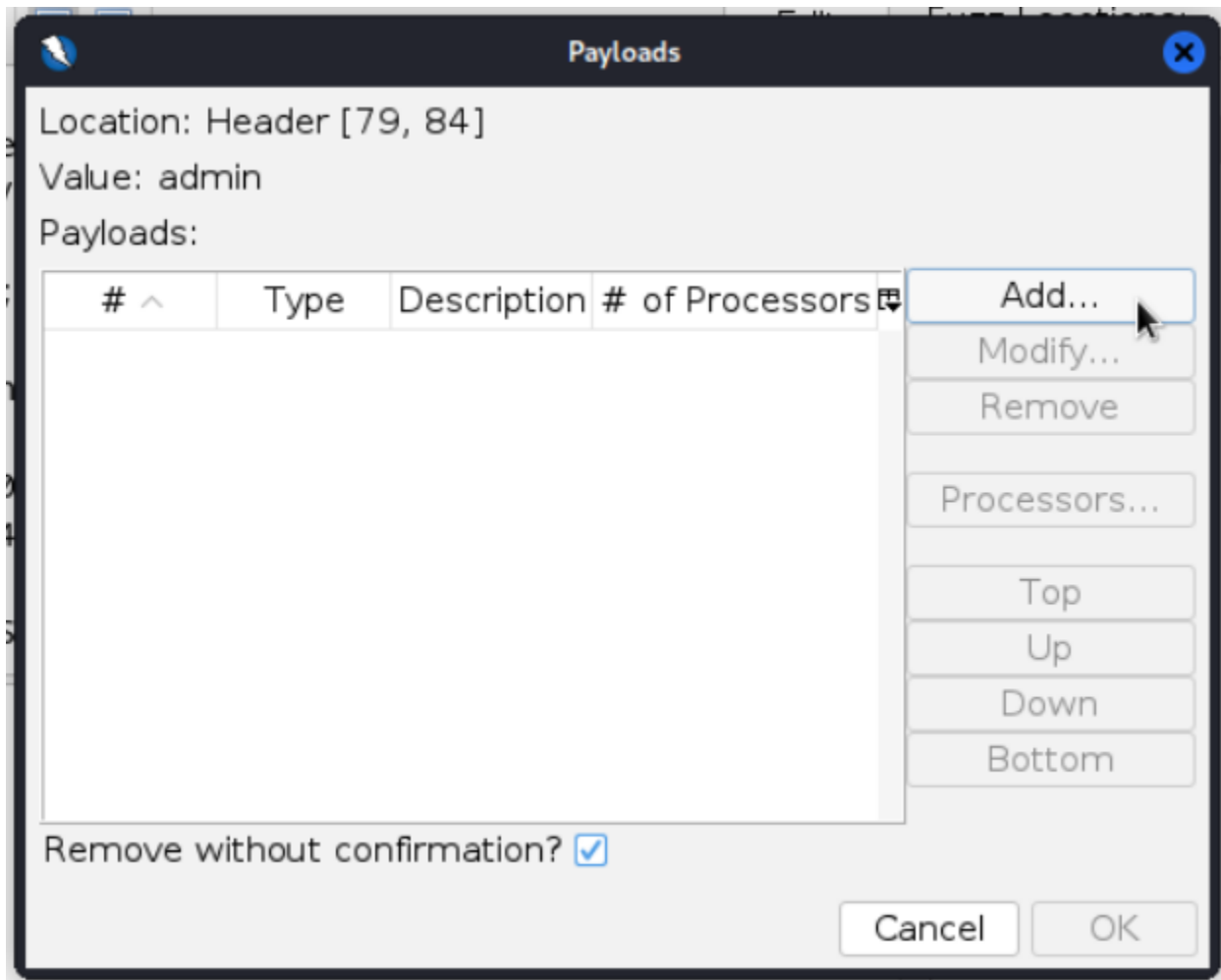
Setelah itu payload username akan terseleksi dengan warna tertentu



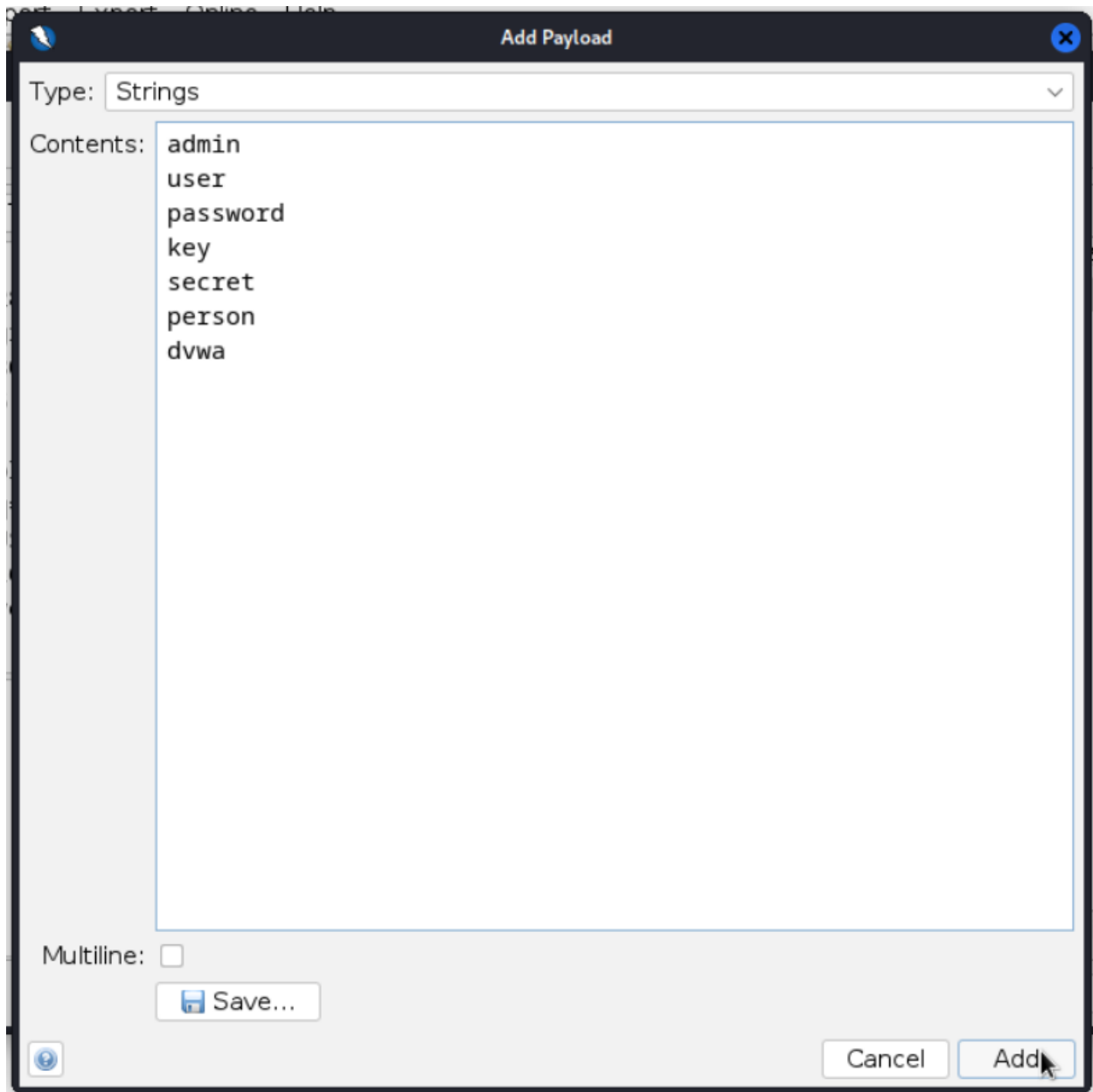
Selanjutnya buat payload untuk password, sama seperti pembuatan payload username, seleksi string dari password, lalu klik Add



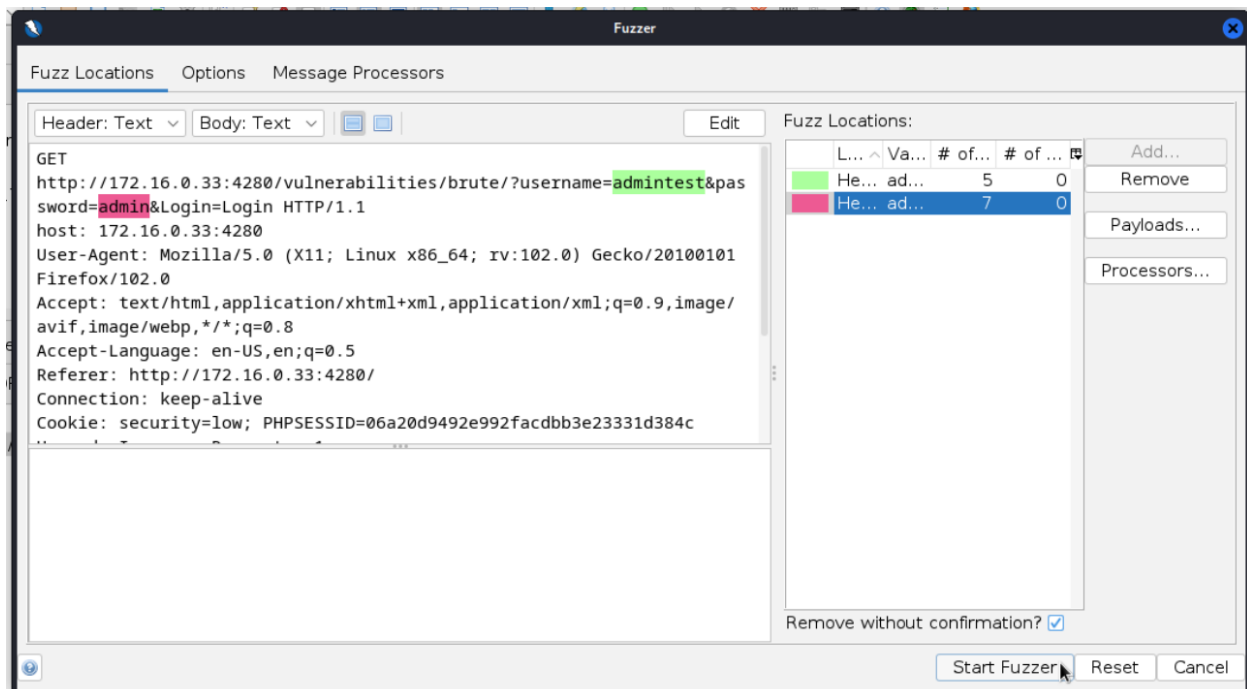
Add



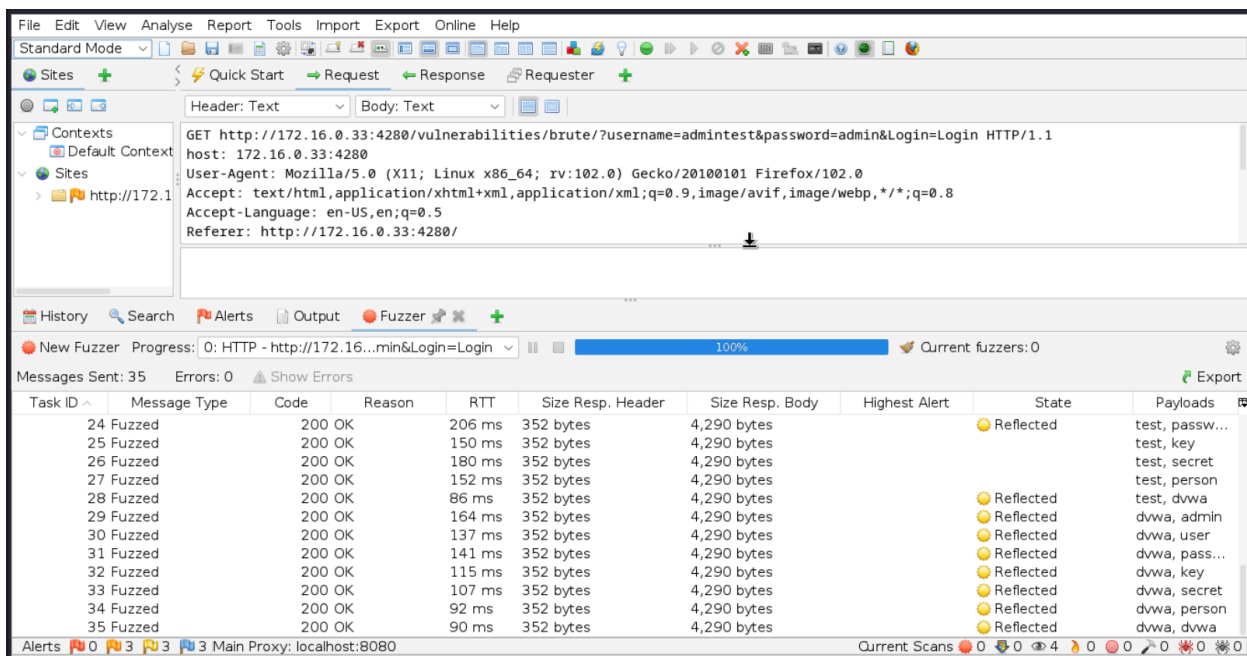
Isikan word list lalu klik Add



Pada tahap ini kedua payload telah dibuat, selanjutnya klik Start Fuzzer



Akan hasil dari Fuzzer



Setelah proses brute force selesai untuk mengetahui username dan password yang benar dapat dilihat dari nilai "Size Resp. Body", nilai yang berbeda dari yang lain merupakan kombinasi username dan password yang benar. Untuk mempermudah

dalam pencarian, nilai “Size Resp. Body” dapat diurutkan dari yang terkecil ke terbesar atau sebaliknya.

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
3 Fuzzed		200 OK		327 ms	353 bytes	4,328 bytes		Reflected	admin, password
0 Original		200 OK		66 ms	353 bytes	4,290 bytes	Medium		
1 Fuzzed		200 OK		103 ms	353 bytes	4,290 bytes		Reflected	admin, admin
2 Fuzzed		200 OK		167 ms	353 bytes	4,290 bytes		Reflected	admin, user
4 Fuzzed		200 OK		104 ms	353 bytes	4,290 bytes		Reflected	admin, key
5 Fuzzed		200 OK		287 ms	353 bytes	4,290 bytes		Reflected	admin, secret
6 Fuzzed		200 OK		98 ms	353 bytes	4,290 bytes		Reflected	admin, person
7 Fuzzed		200 OK		153 ms	353 bytes	4,290 bytes		Reflected	admin, dvwa
8 Fuzzed		200 OK		130 ms	353 bytes	4,290 bytes		Reflected	user, admin
9 Fuzzed		200 OK		208 ms	352 bytes	4,290 bytes		Reflected	user, user
10 Fuzzed		200 OK		211 ms	352 bytes	4,290 bytes		Reflected	user, password
11 Fuzzed		200 OK		213 ms	352 bytes	4,290 bytes		Reflected	user, key

Expo

Payloads

admin, password

admin, admin

Kombinasi yang benar adalah username: admin dan password: password

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

Vulnerability: Brute Force

Login

Username:

Password:

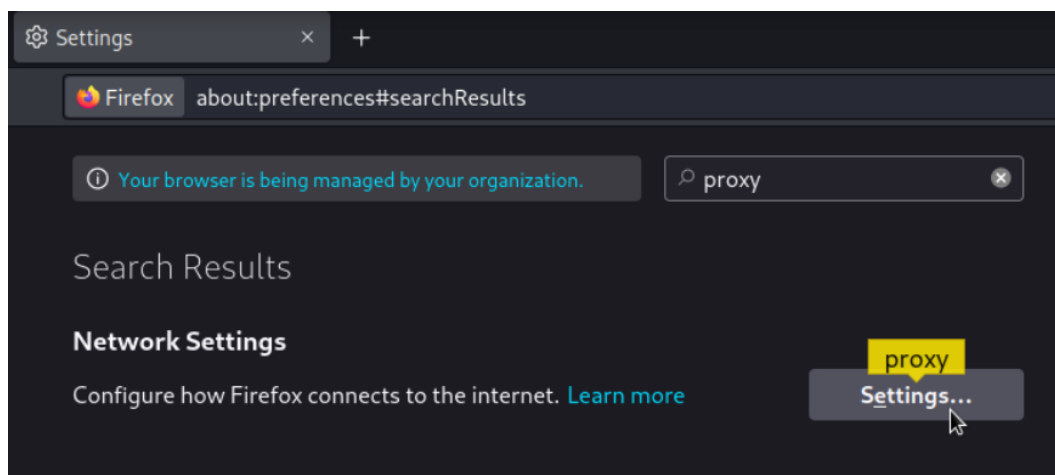
Welcome to the password protected area admin



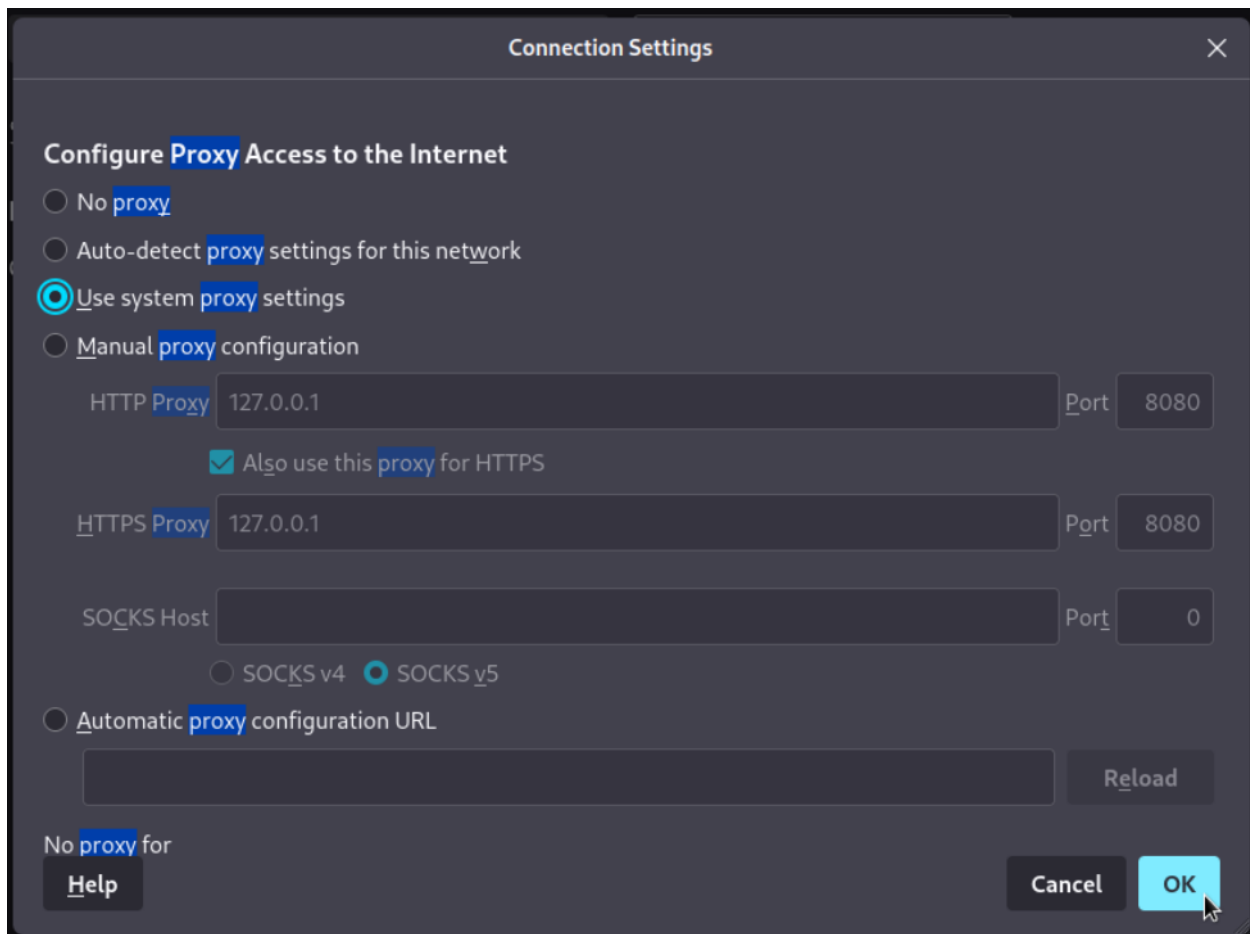
Clean up

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