PENETRATION TESTING TOOL UNTUK MENGUJI KERENTANAN *SQL INJECTION* SECARA OTOMATIS BERBASIS *WEB*

Muhammad Mushlih [1], Rahimi Fitri [2], Isna Wardiah [3]
Politeknik Negeri Banjarmasin [1,2,3]
mushlih@pentester.id [1], rahimi_fitri@poliban.ac.id [2], isnawardiah@poliban.ac.id [3]

ABSTRACT

Security is one very important aspect of an information system. Therefore many companies invest funds to strengthen their network systems. One of the most effective methods is Penetration Testing (Pentesting). By doing Pentesting, existing security holes can be identified and corrected as soon as possible. But not everyone is able to do Pentesting, because there are many stages that must be done. Based on the description of the problem above, the author raises the title "Penetration Testing Tool to Test SQL Injection Vulnerability Automatically Web-Based". To test the vulnerability on a website here the author chose to use the SQL Injection method. This method was chosen because the vulnerability is always included in the Top 10 OWASP vulnerabilities, which means this method is one of the most frequently found attack methods on the web. This Penetration Testing Tool can help administrators or service owners to periodically Pentesting web applications at a later date. So that web managers can immediately do the prevention and security of the web that they manage to reduce the risk of unwanted attacks from both outside and inside that can result in losses.
Keywords: *Penetration Testing, SQL Injection, Vulnerabilities, Web.*

ABSTRAK

Keamanan merupakan salah satu aspek yang sangat penting dari sebuah sistem informasi. Oleh karena itu banyak perusahaan menginvestasikan dana untuk memperkuat sistem jaringannya. Salah satu metode yang paling efektif adalah melakukan *Penetration Testing (Pentesting)*. Dengan melakukan *Pentesting*, celah-celah keamanan yang ada dapat diketahui dan diperbaiki secepatnya. Namun tidak semua orang mampu melakukan *Pentesting*, karena ada banyak tahapan yang harus dilakukan. Berdasarkan uraian masalah diatas, penulis mengangkat judul "*Penetration Testing Tool* untuk Menguji Kerentanan *SQL Injection* Secara Otomatis Berbasis *Web"*. Untuk menguji kerentanan pada suatu web di sini penulis memilih untuk menggunakan metode *SQL Injection*. Metode ini dipilih karena kerentanan tersebut selalu masuk *Top* 10 *OWASP vulnerabilities* yang artinya metode ini merupakan salah satu metode serangan yang paling sering ditemukan terhadap *web*. *Penetration Testing Tool* ini dapat membantu administrator atau pemilik layanan dalam melakukan *Pentesting* pada aplikasi *web* secara berkala di kemudian hari. Sehingga pengelola *web* dapat segera melakukan pencegahan dan pengamanan terhadap *web* yang mereka kelola guna mengurangi resiko serangan yang tidak diinginkan baik dari luar maupun dalam yang dapat mengakibatkan kerugian.
Kata Kunci: Penetration Testing, SQL Injection, Vulnerabilities, Web.

PENDAHULUAN

Keamanan merupakan salah satu aspek yang sangat penting dari sebuah sistem informasi (Dharmawan, Eka Adhitya, dkk, 2013). Keamanan komputer adalah sebuah tindakan pencegahan yang dilakukan untuk melindungi sebuah sistem dari serangan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Tanpa keamanan yang baik, maka data-data pengguna belum dapat dikatakan aman. Hal tersebut pastinya akan mempengaruhi kepercayaan pengguna dalam menggunakan sistem tersebut.

Penetration Testing (Pentesting) merupakan suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan organisasi / perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut. Orang yang melakukan kegiatan ini disebut *Penetration Tester (Pentester)*.

Perusahaan besar yang menyimpan data-data sensitif (seperti Bank) tentu tidak ingin jaringannya dibobol oleh orang tidak bertanggung jawab, yang kemudian bisa mengambil alih

kontrol jaringan dan menimbulkan kerugian yang sangat besar. Oleh karena itu banyak perusahaan menginvestasikan dana untuk memperkuat sistem jaringannya. Salah satu metode paling efektif adalah melakukan *Pentesting*. Dengan melakukan *Pentesting*, celah-celah keamanan yang ada dapat diketahui dan dengan demikian dapat diperbaiki secepatnya.

Di era perkembangan digitalisasi yang sangat pesat ini, *SQL Injection* masih menjadi ancaman keamanan yang serius di Internet. Karena penggunaan internet untuk berbagai layanan online meningkat, begitu juga ancaman keamanan yang ada di *web* tentu akan meningkat. *SQL Injection* merupakan suatu teknik peretasan yang memungkinkan penyerang mendapatkan akses yang tidak sah ke dalam *database* kemudian menyerang atau mengubah data-data yang berada di dalam *database* (Kiezun, Guo, dkk., 2009).

Berdasarkan data dari Akamai Q2 pada tahun 2016 (Fernandez, Arteaga, dkk., 2016), *SQL Injection* merupakan ancaman yang sering terjadi pada aplikasi *web server* setelah *Local File Inclusion (LFI)* dengan persentase sebesar 44.11%, diikuti dengan *Cross-Site Scripting (XSS)* dengan persentase sebesar 5.91% dan *Remote File Inclusion* (RFI) 2.27%. Teknik *SQL Injection* ini digunakan dengan cara memasukkan perintah-perintah *SQL* melalui alamat *URL (Uniform Resource Locator)* atau melalui kolom masukan yang nantinya akan dieksekusi oleh server ketika meminta data ke dalam *database*. Tidak semua orang mampu melakukan *Pentesting* terhadap kerentanan *SQL Injection*, karena dalam melakukannya ada banyak tahapan yang harus dilakukan dan dalam tiap tahapan tersebut seseorang harus mengerti sintaks *SQL (Structured Query Language)*.

Berdasarkan permasalahan tersebut, maka penulis berinisiatif membuat sebuah *Penetration Testing Tool* untuk Menguji Kerentanan *SQL Injection* Secara Otomatis Berbasis *Web*. Harapan kedepannya dengan adanya *Penetration Testing Tool* ini diharapkan dapat membantu administrator atau pemilik layanan dalam melakukan *Pentesting* pada aplikasi *web* secara berkala di kemudian hari. Sehingga pengelola *web* dapat segera melakukan pencegahan dan pengamanan terhadap *web* yang mereka kelola guna mengurangi resiko serangan yang tidak diinginkan baik dari luar maupun dalam yang dapat mengakibatkan kerugian.

METODE PENELITIAN

Dalam pembuatan *Penetration Testing Tool* untuk Menguji Kerentanan *SQL Injection* Secara Otomatis Berbasis *Web* ini, terdapat tahapan pengumpulan data. Teknik yang digunakan pada tahapan pengumpulan data adalah studi literatur atau biasa disebut dengan studi pustaka. Studi literatur atau studi pustaka merupakan sebuah proses pengumpulan data dan informasi berupa teori-teori yang berhubungan dengan masalah yang diteliti. Studi literatur dilakukan dengan mencari jurnal ilmiah, paper ilmiah, dan tugas akhir di internet. Adapun data-data yang dibutuhkan untuk membangun aplikasi ini, diantaranya teori pengujian celah keamanan pada aplikasi atau sistem berbasis *website*, teori pembuatan aplikasi pengujian celah keamanan menggunakan bahasa pemrograman *python*.

Pembuatan *Penetration Testing Tool* untuk Menguji Kerentanan *SQL Injection* Secara Otomatis Berbasis *Web* ini membutuhkan beberapa aplikasi dan modul yang dapat mendukung perancangan aplikasi. Untuk mengetahui aplikasi dan modul yang akan digunakan, maka diperlukan analisis terhadap kebutuhan aplikasi. Metode analisis yang digunakan dalam merancang dan membangun aplikasi ini, diantaranya analisis kebutuhan perangkat lunak, analisis kebutuhan masukan (*input*), analisis kebutuhan proses, dan analisis kebutuhan keluaran (*output*).

Analisis Kebutuhan Perangkat Lunak

Pada proses perancangan dan pembuatan aplikasi terdapat beberapa komponen perangkat lunak yang digunakan. Dalam perangkat lunak sistem, peneliti menggunakan sistem operasi *BackBox Linux*. Dalam pembuatan aplikasi, digunakan bahasa pemrograman *python* versi 3.6. Untuk *text editor*, digunakan *Visual Studio Code*.

Analisis Kebutuhan Masukan

Pada proses analisis kebutuhan masukan, pengguna akan diminta untuk memasukkan alamat aplikasi *website* target berupa *URL* atau *IP address* beserta parameter dan datanya. Setelah memasukkan alamat *website* target, selanjutnya aplikasi akan melakukan pengujian terhadap target tersebut.

Analisis Kebutuhan Proses

Proses yang dibutuhkan oleh aplikasi pengujian celah keamanan ini berupa analisis terhadap *website* yang akan diuji apakah rentan terhadap serangan *SQL Injection* atau tidak. Pertama-tama aplikasi akan melakukan pengumpulan data berupa ukuran halaman ketika dalam kondisi normal dan error. Tujuan dari pengumpulan data tersebut adalah sebagai pembanding ukuran halaman untuk mendapatkan metode yang tepat untuk melakukan *SQL Injection* terhadap website target. Dari metode yang tepat itulah yang nantinya akan digunakan dalam proses pengujian serangan *SQL Injection* baik itu untuk mengetahui kerentanan maupun untuk eksploitasi lebih dalam.

Analisis Kebutuhan Keluaran

Keluaran akhir yang dihasilkan oleh *Penetration Testing Tool* ini adalah informasi apakah aplikasi target rentan terhadap serangan *SQL Injection* atau tidak. Apabila target rentan terhadap jenis serangan *SQL Injection*, maka aplikasi akan memberikan keluaran informasi berupa *Database*, *Table* dan *Column* dari target.

HASIL DAN PEMBAHASAN

Pada tahapan ini, akan dilakukan pengujian terhadap aplikasi yang telah dibuat sebelumnya untuk mengetahui apakah hasil yang dikeluarkan oleh aplikasi telah sesuai dengan yang diharapkan atau belum. Pengujian ini dilakukan dengan 2 tahap, yaitu pengujian dengan *website* target indonesia dan pengujian dengan *website* target luar negeri.

Pengujian Dengan Website Target Indonesia

Pada tahap ini akan dilakukan pengujian aplikasi dengan alamat *website* target indonesia. Di sini yang akan menjadi target pengujian adalah *website* milik Politeknik Manufaktur Negeri Bangka Belitung. Alamat target beserta parameternya dapat dilihat pada Tabel 1.

Tabel 1. *Website* Target Indonesia

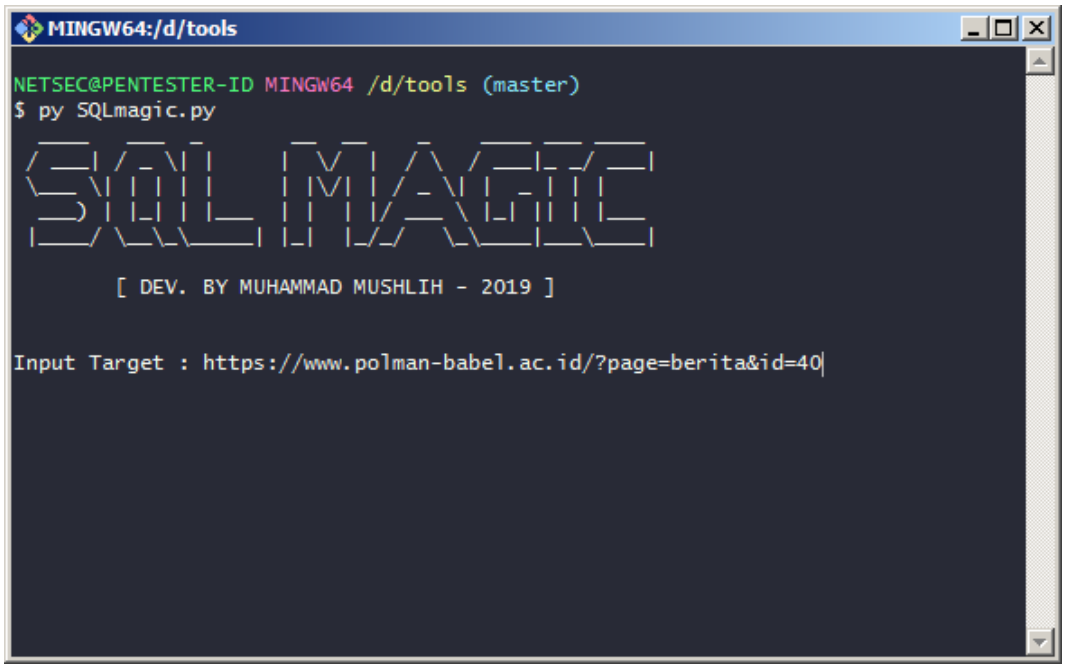
Alamat	Parameter
https://www.polman-babel.ac.id/	?page=berita&id=40

Setelah memasukkan alamat target beserta parameternya pada *Penetration Testing Tool* seperti pada Gambar 1, maka selanjutnya tekan enter untuk memulai proses pengujian, jika sudah selesai maka hasilnya akan seperti Gambar 2. Dari hasil keluaran pada pengujian ini dapat dilihat bahwa website target rentan terhadap serangan *SQL Injection* ditandai dengan adanya *Output Location*, hanya dalam hitungan 16.36 detik *Penetration Testing Tool* ini mampu mengambil semua struktur database pada website target. Untuk melihat struktur databasenya ketik perintah berikut pada terminal :

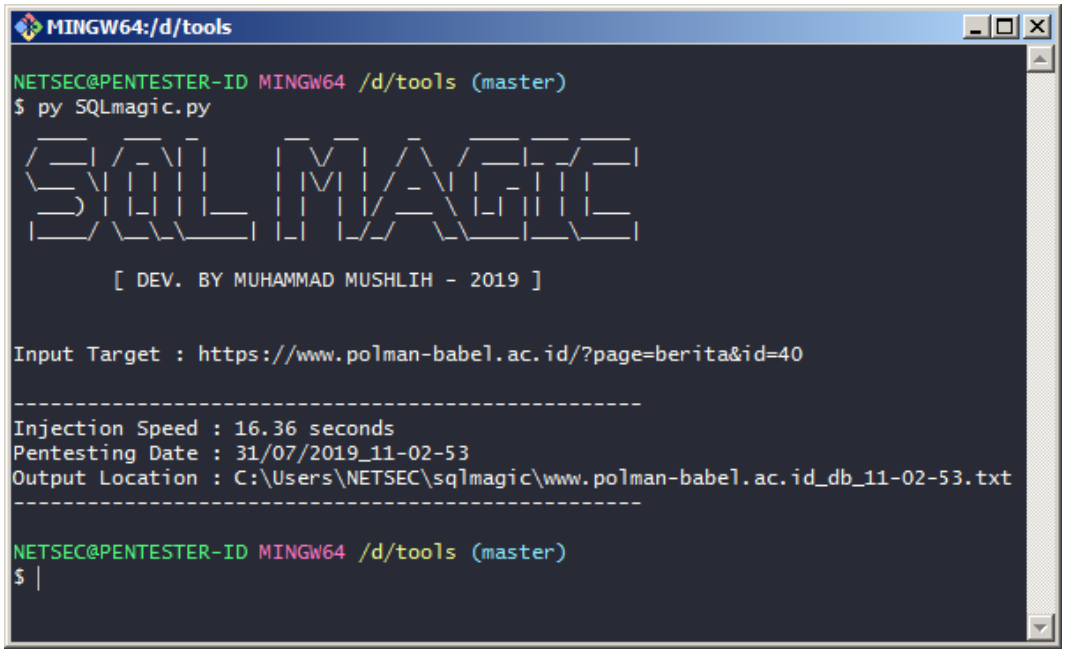
```
less ~/sqlmagic/www.polman-babel.ac.id_db_10-42-35.txt
```

Kemudian tekan enter dan hasilnya akan seperti pada Gambar 3.

ISSN 2341-5662 (Cetak)
ISSN 2341-5670 (Online)

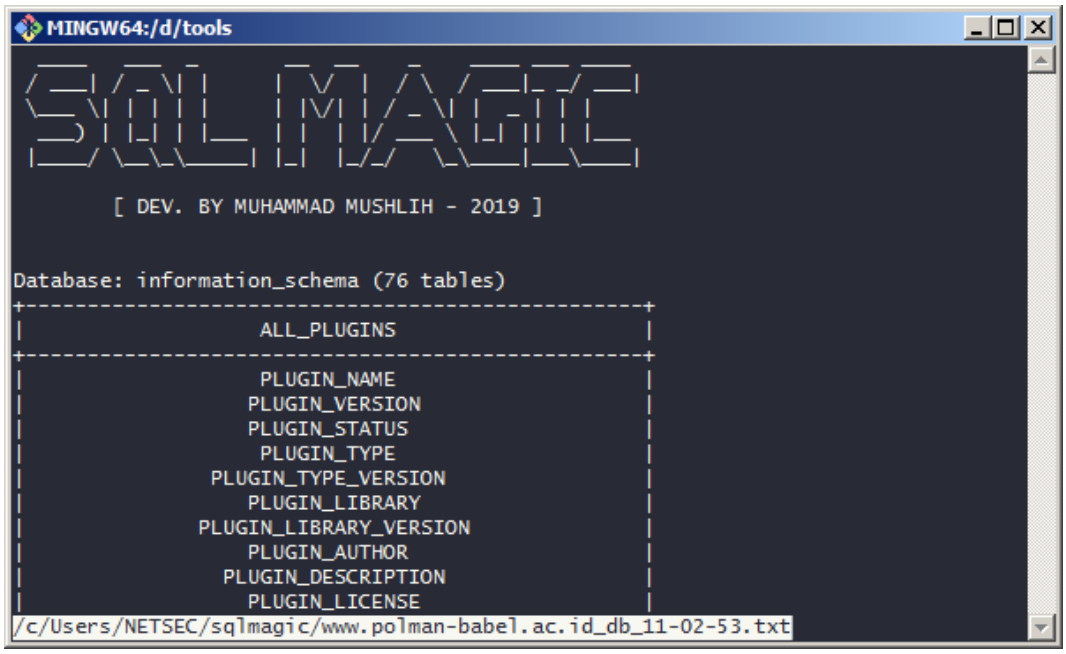


Gambar 1. Proses *Input* Alamat Target Website Indonesia



Gambar 2. Hasil *Output* Target Website Indonesia

ISSN 2341-5662 (Cetak)
ISSN 2341-5670 (Online)



Gambar 3. Struktur Database Target Website Indonesia

Pengujian Dengan Website Target Luar Negeri

Pada tahap ini akan dilakukan pengujian aplikasi dengan alamat *website* target luar negeri. Di sini yang akan menjadi target pengujian adalah *website* milik salah satu stasiun televisi yang ada di London yaitu United Brain Networks Ltd. Alamat target beserta parameternya dapat dilihat pada Tabel 2.

Tabel 2. Website Target Luar Negeri

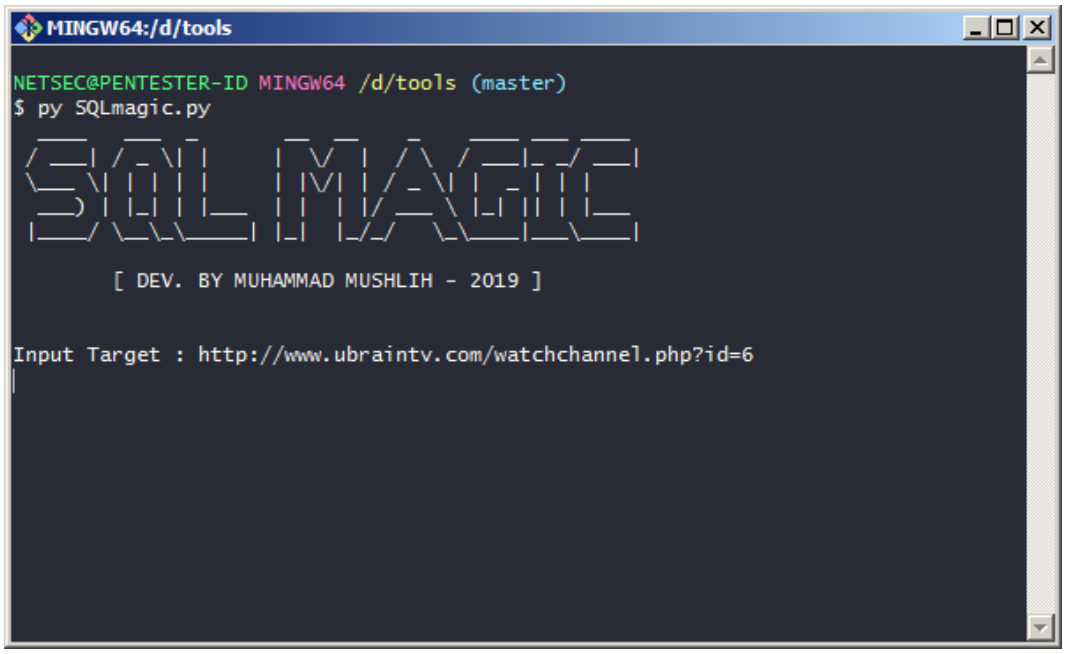
Alamat	Parameter
http://www.ubraintv.com/	watchchannel.php?id=6

Setelah memasukkan alamat target beserta parameternya pada *Penetration Testing Tool* seperti pada Gambar 4, maka selanjutnya tekan enter untuk memulai proses pengujian, jika sudah selesai maka hasilnya akan seperti Gambar 5. Dari hasil keluaran pada pengujian ini dapat dilihat bahwa website target rentan terhadap serangan *SQL Injection* ditandai dengan adanya *Output Location*, hanya dalam hitungan 18.47 detik *Penetration Testing Tool* ini mampu mengambil semua struktur database pada website target. Untuk melihat struktur databasenya ketik perintah berikut pada terminal:

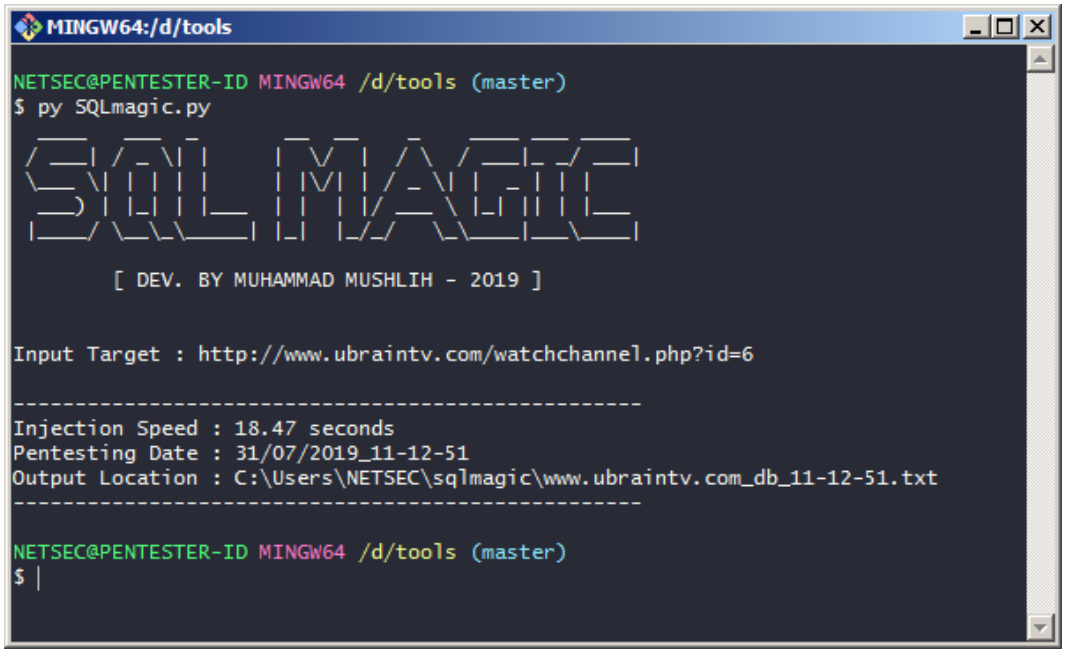
```
less ~/sqlmagic/www.ubraintv.com_db_11-12-51.txt
```

Kemudian tekan enter dan hasilnya akan seperti pada Gambar 6.

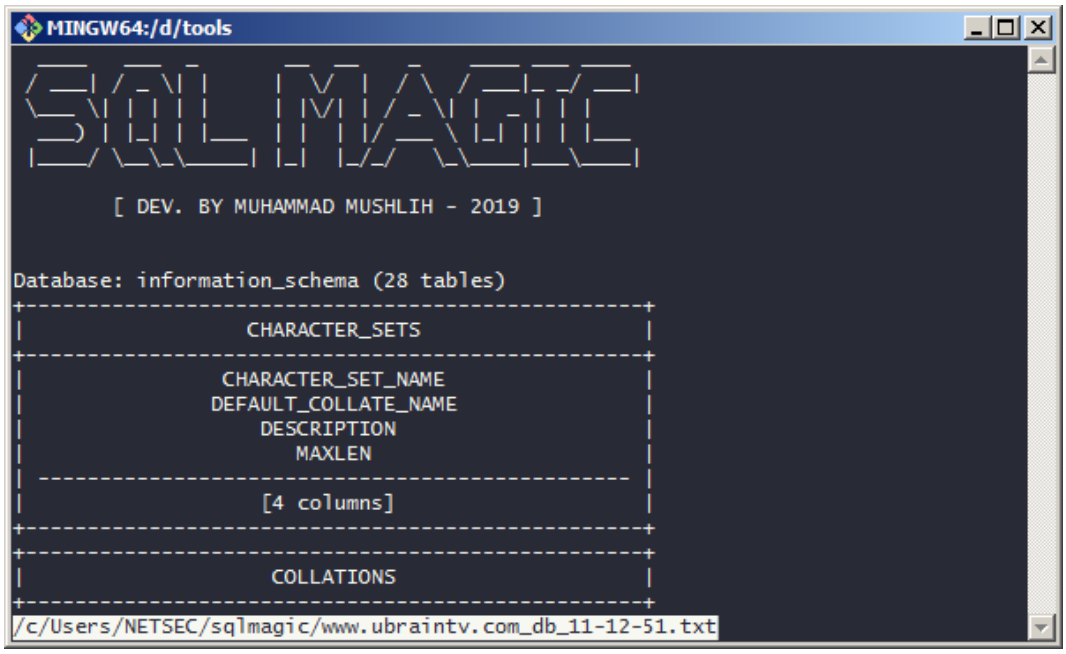
ISSN 2341-5662 (Cetak)
ISSN 2341-5670 (Online)



Gambar 4. Proses Input Alamat Target Website Luar Negeri



Gambar 5. Hasil Output Target Website Luar Negeri



Gambar 6. Struktur Database Target Website Luar Negeri

KESIMPULAN

Setelah melakukan penelitian dan implementasi, hasil yang didapatkan adalah *Penetration Testing Tool* yang telah dibangun mampu melakukan uji kerentanan *SQL Injection* secara otomatis. Sehingga pengguna dapat segera melakukan pencegahan dan pengamanan terhadap *web* yang mereka kelola guna mengurangi resiko serangan yang tidak diinginkan baik dari luar maupun dalam yang dapat mengakibatkan kerugian.

DAFTAR PUSTAKA

Dharmawan, Eka Adhitya , Erni Yudaningtyas, M. S. (2013). Perlindungan Web pada Login Sistem Menggunakan Algoritma Rijndael. *Universitas Brawijaya*, *7*(1), 77–84.

Fernandez, D., Arteaga, J., & Caltum, E. (2016). Akamai's State of Internet / Security Q2 2016 Report.

Kiezun, A., Guo, P. J., Jayaraman, K., & Ernst, M. D. (2009). Automatic creation of SQL injection and cross-site scripting attacks. *Proceedings - International Conference on Software Engineering*, 199–209. https://doi.org/10.1109/ICSE.2009.5070521

OWASP Top 10 - 2013. *OWASP Top 10*, 22. https://doi.org/1 Owasp. (2017). OWASP Top 10 - 2017.