

# **ANALISIS DAN PENCEGAHAN SQL INJECTION DENGAN HONEYPOT**

**SKRIPSI**



**Oleh:  
Indro Lie  
140210018**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK DAN KOMPUTER  
UNIVERSITAS PUTERA BATAM  
2018**

# **ANALISIS DAN PENCEGAHAN SQL INJECTION DENGAN HONEYPOT**

**SKRIPSI**

**Untuk memenuhi salah satu syarat  
guna memperoleh gelar Sarjana**



**Oleh  
Indro Lie  
140210018**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK DAN KOMPUTER  
UNIVERSITAS PUTERA BATAM  
2018**

## **PERNYATAAN**

Dengan ini peneliti menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, dan/atau magister), baik di Universitas Putera Batam maupun di perguruan tinggi lain.
2. Skripsi ini adalah murni gagasan, rumusan, dan penelitian peneliti sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing.
3. Dalam skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini peneliti buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka peneliti bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi.

Batam, 3 Februari 2018  
Yang membuat pernyataan,

Indro Lie  
140210018

# **ANALISIS DAN PENCEGAHAN SQL INJECTION DENGAN HONEYPOT**

**Oleh  
Indro Lie  
140210018**

## **SKRIPSI**

**Untuk memenuhi salah satu syarat  
guna memperoleh gelar Sarjana**

**Telah disetujui oleh Pembimbing pada tanggal  
seperti tertera di bawah ini**

**Batam, 3 Februari 2018**

**Andi Maslan, S.T., M.SI.**

**Pembimbing**

## ABSTRAK

Seiring dengan perkembangan zaman, pemanfaatan terhadap website ikut berkembang. Perkembangan tersebut membawa dampak positif dan juga dampak negatif. Salah satu dampak negatif adalah perkembangan tersebut meningkatkan potensi terjadinya peretasan pada website. Salah satu teknik peretasan website yang sering digunakan adalah SQL Injection. Teknik tersebut meretas suatu website dengan memasukkan suatu perintah SQL ke dalam variabel yang akan dibaca oleh database. Oleh karena itu, database akan membaca variabel tersebut sebagai suatu perintah yang harus dijalankan, bukan sebagai sebuah nilai dalam suatu variabel. Honeypot terbukti dapat mencegah peretasan dengan teknik SQL Injection. Oleh karena itu dalam penelitian ini, peneliti menggunakan Honeypot untuk melindungi suatu website dari peretasan dengan SQL Injection. Kemudian peneliti membahas mengenai cara kerja SQL Injection dalam peretasan website tersebut beserta cara pencegahannya dengan Honeypot. Mula-mula peneliti akan menggunakan suatu tool yang bernama sqlmap untuk melakukan SQL Injection terhadap web server. Setelah itu, Honeypot ditambahkan ke dalam jaringan dan konfigurasi pada *firewall* jaringan diubah agar semua *request http* dikirim menuju ke Honeypot. Setelah pemasangan Honeypot, dilakukan pengujian terhadap Honeypot dengan sqlmap untuk membuktikan bahwa web server telah berhasil dilindungi. Dari hasil pengujian, Honeypot berhasil mencegah peretasan pada web server dengan teknik SQL Injection. Honeypot melindungi web server dengan mengalihkan serangan SQL Injection ke Honeypot itu sendiri.

Kata Kunci: SQL Injection, website, peretasan, SQL, Honeypot.

## **ABSTRACT**

*Along with the world developing, the use of website also developed. The developments had brought both positive and negative impacts. One of the negative impacts is that the developments increase the potential of website hacking. One of the most used techniques for hacking website is SQL Injection. This technique hacked a website by adding SQL query into variable that will be read by the database. Therefore, the database will read the variable as a command to execute, not as a value in variable. Honeypot was proven able to prevent SQL Injection from hacking a website. Therefore in this study, the researcher used Honeypot to protect a website from hacking with SQL Injection. After that, the researcher analyze how SQL Injection works to hack a website and how to use Honeypot to prevent the hack. At first, the researcher will use a tool called sqlmap to hack the web server with SQL Injection. After that, Honeypot will get installed to the network and the configuration in the firewall will get changed, so that any http request will be send to Honeypot. After the Honeypot installed, the Honeypot will get tested with sqlmap to prove that the web server get protected. Based on the testing result, the Honeypot able to protect web server from hacking with SQL Injection technique. Honeypot protects the website by making itself as a target to attack instead.*

*Keywords: SQL Injection, website, hacking, SQL, Honeypot.*

## KATA PENGANTAR

Puji dan syukur peneliti panjatkan kepada Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam. Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Ibu Nur Elfi Husda, S.Kom., M.SI. selaku Rektor Universitas Putera Batam.
2. Bapak Andi Maslan, S.T., M.SI. selaku Pembimbing Skripsi Peneliti dan Ketua Program Studi Teknik Informatika Universitas Putera Batam.
3. Bapak Alvendo Wahyu Aranski, S.Kom.,M.Kom. selaku dosen pembimbing akademik peneliti.
4. Bapak Arif Rahman Hakim, S.Kom., M.Kom. selaku dosen pengajar peneliti.
5. Ibu Yusli Yenni, S.Kom., M.Kom. selaku dosen pengajar peneliti.
6. Dosen dan Staff Universitas Putera Batam.
7. Teman-teman yang telah memberikan semangat dan dukungan dalam penyusunan skripsi ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Batam, Februari 2018

Penulis



## DAFTAR ISI

### HALAMAN SAMPUL DEPAN

|                         |     |
|-------------------------|-----|
| HALAMAN JUDUL.....      | ii  |
| HALAMAN PERNYATAAN..... | iii |
| HALAMAN PENGESAHAN..... | iv  |
| ABSTRAK.....            | v   |
| <i>ABSTRACT</i> .....   | vi  |
| KATA PENGANTAR .....    | vii |
| DAFTAR ISI.....         | ix  |
| DAFTAR TABEL.....       | xi  |
| DAFTAR GAMBAR .....     | xii |
| DAFTAR LAMPIRAN.....    | xiv |

### BAB I PENDAHULUAN

|                                     |   |
|-------------------------------------|---|
| 1.1. Latar Belakang Penelitian..... | 1 |
| 1.2. Identifikasi Masalah .....     | 4 |
| 1.3. Pembatasan Masalah .....       | 4 |
| 1.4. Perumusan Masalah.....         | 5 |
| 1.5. Tujuan Penelitian.....         | 5 |
| 1.6. Manfaat Penelitian.....        | 5 |

### BAB II KAJIAN PUSTAKA

|                                       |    |
|---------------------------------------|----|
| 2.1. Teori Dasar .....                | 7  |
| 2.1.1. Jaringan Komputer.....         | 7  |
| 2.1.2. Standar Jaringan Komputer..... | 8  |
| 2.1.3. Jenis Jaringan Komputer.....   | 8  |
| 2.1.4. Model OSI Layer .....          | 11 |
| 2.2. Teori Khusus .....               | 15 |
| 2.2.1. Web Server.....                | 15 |
| 2.2.2. SQL Injection.....             | 15 |
| 2.2.3. Honeypot.....                  | 20 |
| 2.3. Tools.....                       | 22 |
| 2.4. Penelitian Terdahulu.....        | 24 |
| 2.5. Kerangka Pemikiran .....         | 27 |

### BAB III METODE PENELITIAN

|                                                                      |    |
|----------------------------------------------------------------------|----|
| 3.1. Desain Penelitian .....                                         | 29 |
| 3.2. Analisis Jaringan Lama .....                                    | 30 |
| 3.3. Rancangan Jaringan Yang Dibangun/ Rancangan Jaringan Baru ..... | 35 |
| 3.4. Lokasi dan Jadwal Penelitian .....                              | 39 |
| 3.4.1. Lokasi Penelitian.....                                        | 39 |
| 3.4.2. Jadwal Penelitian .....                                       | 40 |

#### BAB IV HASIL PENELITIAN DAN PEMBAHASAN

|        |                                                                               |    |
|--------|-------------------------------------------------------------------------------|----|
| 4.1.   | Hasil Penelitian.....                                                         | 41 |
| 4.1.1. | Hasil Analisis Jaringan Yang Lama.....                                        | 41 |
| 4.1.2. | Implementasi Rancangan Jaringan Baru / Instalasi Honeypot .....               | 50 |
| 4.1.3. | Pengujian Jaringan Baru/ Pengujian Honeypot .....                             | 59 |
| 4.2.   | Pembahasan.....                                                               | 65 |
| 4.2.1. | Cara Kerja Teknik SQL Injection Dalam Meretas Suatu Website .....             | 65 |
| 4.2.2. | Cara Mencegah Peretasan Teknik SQL Injection Dengan Menggunakan Honeypot..... | 68 |

#### BAB V SIMPULAN DAN SARAN

|      |               |    |
|------|---------------|----|
| 5.1. | Simpulan..... | 74 |
| 5.2. | Saran .....   | 74 |

#### DAFTAR PUSTAKA

#### DAFTAR RIWAYAT HIDUP

#### LAMPIRAN

## DAFTAR TABEL

|                                                      |    |
|------------------------------------------------------|----|
| <b>Tabel 3.1</b> Perangkat Keras Jaringan .....      | 31 |
| <b>Tabel 3.2</b> Spesifikasi Web Server .....        | 32 |
| <b>Tabel 3.3</b> Perangkat Lunak Web Server.....     | 32 |
| <b>Tabel 3.4</b> Spesifikasi Komputer Honeypot ..... | 36 |
| <b>Tabel 3.5</b> Software Honeypot.....              | 37 |
| <b>Tabel 3.6</b> Jadwal Penelitian.....              | 40 |

## DAFTAR GAMBAR

|                    |                                                         |        |
|--------------------|---------------------------------------------------------|--------|
| <b>Gambar 2.1</b>  | False result hasil dari Blind SQL Injection .....       | 19     |
| <b>Gambar 2.2</b>  | True result hasil dari Blind SQL Injection .....        | 19     |
| <b>Gambar 2.3</b>  | HIHAT .....                                             | 23     |
| <b>Gambar 2.4</b>  | Sqlmap .....                                            | 24     |
| <b>Gambar 2.5</b>  | Kerangka Pemikiran .....                                | 27     |
| <b>Gambar</b>      | <b>3.1</b> .....                                        | Desain |
| Penelitian.....    | 29                                                      |        |
| <b>Gambar 3.2</b>  | Diagram Jaringan Lama.....                              | 30     |
| <b>Gambar 3.3</b>  | Web Server .....                                        | 31     |
| <b>Gambar 3.4</b>  | Memulai sqlmap .....                                    | 33     |
| <b>Gambar 3.5</b>  | Sqlmap melakukan SQL Injection.....                     | 35     |
| <b>Gambar 3.6</b>  | Diagram Jaringan Baru .....                             | 35     |
| <b>Gambar 3.7</b>  | Honeypot.....                                           | 37     |
| <b>Gambar 3.8</b>  | File check_post.php .....                               | 38     |
| <b>Gambar 3.9</b>  | Perintah untuk meneruskan request .....                 | 39     |
| <b>Gambar</b>      | <b>4.1</b> Admin login .....                            | 41     |
| page.....          | 41                                                      |        |
| <b>Gambar 4.2</b>  | Halaman setelah login.....                              | 42     |
| <b>Gambar 4.3</b>  | Inspect Element (1).....                                | 43     |
| <b>Gambar 4.4</b>  | Inspect Element (2).....                                | 43     |
| <b>Gambar 4.5</b>  | Menjalankan sqlmap .....                                | 44     |
| <b>Gambar 4.6</b>  | Hasil dari sqlmap .....                                 | 45     |
| <b>Gambar 4.7</b>  | Hasil dari sqlmap .....                                 | 46     |
| <b>Gambar 4.8</b>  | Hasil sqlmap terhadap login.php .....                   | 47     |
| <b>Gambar 4.9</b>  | Log file sqlmap .....                                   | 48     |
| <b>Gambar 4.10</b> | Tes login pada web server .....                         | 49     |
| <b>Gambar 4.11</b> | Contact Search Page dari Web Server .....               | 49     |
| <b>Gambar 4.12</b> | Membuat database MySQL melalui phpMyAdmin .....         | 51     |
| <b>Gambar 4.13</b> | Impor tabel database .....                              | 52     |
| <b>Gambar 4.14</b> | Membuat user baru pada database .....                   | 52     |
| <b>Gambar 4.15</b> | Konfigurasi hak user pada database .....                | 53     |
| <b>Gambar 4.16</b> | File insertionFile.txt.....                             | 54     |
| <b>Gambar 4.17</b> | Perintah untuk memasang HIHAT .....                     | 55     |
| <b>Gambar 4.18</b> | File contast.php.....                                   | 55     |
| <b>Gambar 4.19</b> | File check_post.php .....                               | 56     |
| <b>Gambar 4.20</b> | File check_get.php.....                                 | 57     |
| <b>Gambar 4.21</b> | File check_cookie.php .....                             | 57     |
| <b>Gambar 4.22</b> | Penentuan penerusan request .....                       | 58     |
| <b>Gambar 4.23</b> | HIHAT .....                                             | 59     |
| <b>Gambar 4.24</b> | Halaman yang ditampilkan kepada user setelah login..... | 60     |
| <b>Gambar 4.25</b> | Proses dari sqlmap .....                                | 61     |

|                    |                                                             |    |
|--------------------|-------------------------------------------------------------|----|
| <b>Gambar 4.26</b> | Perintah menentukan penerusan request pada Honeypot .....   | 62 |
| <b>Gambar 4.27</b> | Hasil dari sqlmap .....                                     | 62 |
| <b>Gambar 4.28</b> | Tes login pada Honeypot .....                               | 63 |
| <b>Gambar 4.29</b> | Halaman yang ditampilkan kepada attacker setelah login..... | 64 |
| <b>Gambar 4.30</b> | HIHAT mencatat request.....                                 | 65 |
| <b>Gambar 4.31</b> | Perintah PHP memeriksa username dan password.....           | 66 |
| <b>Gambar 4.32</b> | Memasukkan komentar pada PHP .....                          | 67 |
| <b>Gambar 4.33</b> | Perintah PHP pada Honeypot (1).....                         | 69 |
| <b>Gambar 4.34</b> | Perintah PHP pada Honeypot (2).....                         | 69 |
| <b>Gambar 4.35</b> | Perintah PHP pada Honeypot (3).....                         | 69 |
| <b>Gambar 4.36</b> | Perintah PHP pada Honeypot (4).....                         | 70 |
| <b>Gambar 4.37</b> | Mencari nilai string pada variabel .....                    | 70 |
| <b>Gambar 4.38</b> | Hasil penilaian terhadap request .....                      | 71 |
| <b>Gambar 4.39</b> | File check_post.php .....                                   | 72 |
| <b>Gambar 4.40</b> | Perintah PHP meneruskan request.....                        | 73 |

## **DAFTAR LAMPIRAN**

**Lampiran 1** Surat Izin Penelitian

**Lampiran 2** Surat Balasan Izin Penelitian