

LAPORAN TUGAS AKHIR

ANALISIS KEAMANAN MENGGUNAKAN WEB
APLIKASI BWAPP TERHADAP SERANGAN
XSS DAN SQL INJECTION



REZA RAFSANJANI P

1410652019

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER

2016

HALAMAN PENGESAHAN

ANALISIS KEAMANAN MENGGUNAKAN WEB APLIKASI BWAPP TERHADAP SERANGAN XSS DAN SQL INJECTION

Oleh :

**Reza Rafsanjani Prayogo
1410652019**

Telah mempertanggung jawabkan Laporan Tugas Akhirnya pada sidang
Tugas Akhir pada tanggal 9 September 2016 Sebagai salah satu syarat kelulusan
dan mendapatkan gelar Sarjana Komputer (S.Kom)
di

Universitas Muhammadiyah Jember

Disetujui oleh,

Dosen Penguji :

Dosen Pembimbing :

**Yeni Dwi Rahayu, S.ST, M.Kom
NPK. 11 03 590**

**Victor Wahanggara, S. Kom
NPK. 12 09 739**

**Triawan Adi Cahyanto, M. Kom
NPK. 12 03 719**

**Mengesahkan,
Dekan Fakultas Teknik**

**Mengetahui,
Ketua Program Studi Teknik
Informatika**

**Ir. Suhartinah, M.T
NPK. 95 05 246**

**Yeni Dwi Rahayu, S.ST, M.Kom
NPK. 11 03 590**

KATA PENGANTAR

Segala puji dan syukur kami panjatkan kehadiran Tuhan Yang Maha Esa, karena telah melimpahkan rahmat dan hidayah-Nya sehingga laporan Tugas Akhir yang telah penulis susun selama satu semester ini dapat diselesaikan dengan baik.

Laporan Tugas Akhir ini merupakan salah satu syarat yang harus dipenuhi untuk menyelesaikan pendidikan S-1 pada Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember.

Pada kesempatan ini penulis ingin menyampaikan rasa terima kasih kepada semua pihak yang telah membantu penulis dalam menyusun laporan Tugas Akhir ini, antara lain:

1. **Teristimewa buat kedua orang tua tercinta**, ayahanda Supriyadi dan ibunda Sujarwati Ningsih, atas perhatian dan dukungan serta doanya selama ini.
2. Bapak **Victor Wahanggara, S. Kom** , selaku dosen pembimbing yang telah membimbing penulis dalam pembuatan aplikasi dan laporan Tugas Akhir ini.
3. Seluruh dosen Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember.
4. Bapak/Ibu staf pengajaran jurusan S-1 Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember.

5. Teman teman yang turut memberi arahan, motivasi kepada penulis dalam menyelesaikan laporan ini

Penulis sadar laporan Tugas Akhir ini masih jauh dari sempurna dengan segala kekurangannya. Untuk itu penulis harapkan adanya kritik dan saran dari semua pihak demi kesempurnaan dari laporan Tugas Akhirini. Akhir kata, semoga laporan ini dapat bermanfaat bagi rekan-rekan mahasiswa dan pembaca sekalian.

Jember, 21 Nopember 2016

Penulis

DAFTAR ISI

| | |
|-------------------------------------|----------|
| Cover | i |
| Lembar pengesahan | ii |
| Lembar Pernyataan | iii |
| Abstrak | iv |
| Abstract | v |
| Halaman persembahan | vi |
| Kata pengantar | viii |
| Halaman Motto | x |
| Daftar isi | xi |
| Daftar Gambar | xiv |
| Daftar tabel | xvi |
| BAB 1 PENDAHULUAN | 1 |
| 1.1.Latar Belakang | 1 |
| 1.2. Rumusan Masalah | 2 |
| 1.3. Batasan Masalah | 2 |
| 1.4. Tujuan | 2 |
| 1.5. Manfaat | 3 |
| BAB 2 TINJAUAN PUSTAKA | 4 |
| 2.1. Keamanan Web | 4 |
| 2.2. Aspek Dasar Keamanan Web | 4 |

| | |
|--|-----------|
| 2.3. Serangan-Serangan Keamanan Web | 5 |
| 2.4. Macam-macam Penyerang | 6 |
| 2.5. Keamanan Komputer | 8 |
| 2.6. Ancaman Keamanan | 10 |
| 2.7. Tipe-tipe Ancaman Komputer | 10 |
| 2.8. HTML | 11 |
| 2.9. PHP | 11 |
| 2.10. Tipe Data | 11 |
| 2.11. Jenis Tipe Data | 12 |
| 2.12. My SQL | 14 |
| 2.13. Tipe Ancaman pada Aplikasi web | 14 |
| 2.14. SQL Injection | 17 |
| 2.15. Penyebab SQL Injection | 17 |
| 2.16. Pencegahan SQL Injection | 19 |
| 2.17. XSS (Cross Site Scripting) | 19 |
| 2.18. Pencegahan serangan XSS (Cross Site Scripting) | 20 |
| 2.19. BWAPP | 20 |
| BAB 3 METODOLOGI PENELITIAN | 22 |
| 3.1. Metode atau Teknik Pengerjaan | 22 |
| 3.2. Skenario Penelitian | 23 |
| 3.2.1. SQL Injection | 23 |

| | |
|--|----|
| 3.2.2. XSS (Cross Site Scripting) | 24 |
| 3.3. Kerangka Penelitian | 26 |
| 3.3.1. SQL Injection | 26 |
| 3.3.2. XSS (Cross Site Scripting) | 27 |
| BAB 4 HASIL DAN PEMBAHASAN | 28 |
| 4.1. Mekanisme SQL Injection | 28 |
| 4.2. Memberi pencegahan SQL Injection | 34 |
| 4.3. Pengujian setelah diberi pencegahan | 35 |
| 4.4. Analisis SQL Injection | 37 |
| 4.5. Mekanisme XSS (Cross Site Scripting) | 38 |
| 4.6. Memberi pencegahan XSS (Cross Site Scripting) | 40 |
| 4.7. Pengujian setelah diberi pencegahan | 41 |
| 4.8. Analisis XSS (Cross Site Scripting) | 42 |
| 4.9. Analisis keseluruhan | 43 |
| BAB 5 KESIMPULAN DAN SARAN | 45 |
| 5.1. Kesimpulan | 45 |
| 5.2. Saran | 45 |
| Daftar Pustaka | 46 |
| LAMPIRAN | 47 |
| Biodata Penulis | 48 |

DAFTAR GAMBAR

| | |
|--|----|
| Gambar 2.1. Tampilan web bwapp | 21 |
| Gambar 2.2. Beberapa tipe serangan pada bwapp | 21 |
| Gambar 3.1. Diagram alir SQL Injection | 26 |
| Gambar 3.2. Diagram alir XSS (Cross Site Scripting) | 27 |
| Gambar 4.1. Manipulasi dengan single quote | 29 |
| Gambar 4.2. Hasil error setelah menambahkan single quote | 29 |
| Gambar 4.3. Mencari celah SQL Injection | 29 |
| Gambar 4.4. Fungsi union select..... | 30 |
| Gambar 4.5. Kolom yang bisa diinjeksi..... | 30 |
| Gambar 4.6. Menampilkan informasi database melalui URL..... | 31 |
| Gambar 4.7. Informasi kolom pada database | 31 |
| Gambar 4.8. Kolom tabel user dalam database | 32 |
| Gambar 4.9. Menampilkan informasi pada tabel user | 32 |
| Gambar 4.10. Beberapa user pada database | 32 |
| Gambar 4.11. Manipulasi URL menampilkan password | 33 |
| Gambar 4.12. Hasil informasi password pada user | 33 |
| Gambar 4.13. Enkripsi password | 33 |
| Gambar 4.14. Script PHP | 34 |
| Gambar 4.15. Modifikasi sebelum diberi pencegahan | 34 |
| Gambar 4.16. Hasil balikan dari database | 35 |

| | |
|--|----|
| Gambar 4.17. Method anti single quote | 35 |
| Gambar 4.18. Kode anti SQL Injection | 35 |
| Gambar 4.19. Penetrasi setelah diberi pencegahan | 35 |
| Gambar 4.20. Gagal mencoba penetrasi SQL Injection | 36 |
| Gambar 4.21. Source code method Get | 37 |
| Gambar 4.22. Form input untuk penetrasi XSS | 38 |
| Gambar 4.23. Hasil balikan form input | 39 |
| Gambar 4.24. Script penetrasi XSS | 39 |
| Gambar 4.25. Informasi setelah penetrasi XSS | 39 |
| Gambar 4.26. Source code sebelum diberi pencegahan..... | 41 |
| Gambar 4.27. Source code pencegahan XSS | 41 |
| Gambar 4.28. Penetrasi ulang serangan XSS..... | 41 |
| Gambar 4.29. Gagal penetrasi serangan XSS | 42 |

DAFTAR TABEL

| | |
|--|----|
| Tabel 4.1. celah keamanan | 31 |
| Tabel 4.2. Hasil uji coba serangan SQL Injection | 34 |
| Tabel 4.3. Hasil uji coba setelah diberi pencegahan | 36 |
| Tabel 4.4. Hasil ujicoba serangan XSS (Cross Site Scripting) | 40 |
| Tabel 4.5. Hasil ujicoba setelah diberi pencegahan | 42 |
| Tabel 4.6. Celah keamanan yang bisa diinjeksi | 43 |
| Tabel 4.7. Celah keamanan yang tidak bisa diinjeksi | 43 |
| Tabel 4.8. Celah keamanan penetrasi XSS (Cross Site Scripting) | 43 |
| Tabel 4.9. Celah keamanan setelah diberi pencegahan | 44 |

DAFTAR PUSTAKA

- Andrea, Adelphia. 2016. "Cepat Belajar Hacking". Elex Media Komputindo
- AQua, Onix. 2013. "Cara Hacking Website Dengan Teknik Manual SQL Injection", <http://indocyberarmy.blogspot.com/2013/02/cara-hacking-website-dengan-teknik-sql.html>.
- DuPaul, Neil. 2016. "SQL Injection Cheat Sheet & Tutorial : Vulnerabilities & How to Prevert SQL Injection Attack", <http://www.veracode.com/security/sql-injection>.
- Clarke, J., 2009, SQL Injection Attacks and Defense. Burlington: Syngress Publishing and Elseiver.
- Chandraleka, Happy. "Siapa Bilang nge-Hack Itu Susah". Elex Media Komputindo
- Digdo, Pringgo, Girindro. 2012. "Analisis Serangan dan Keamanan pada Aplikasi Web". Elex Media Komputindo
- Kristanto, Andri. 2010. "Kupas Tuntas PHP & My SQL". Cable Book
- Kurniawan, Dedik. 2013. "Buku Pintar Teknik Hacking". Elex Media Komputindo
- Muammar, Ahmad. 2013. "Web Hacking (basic)". OSCP
- McCluer, Stuart. 2009. "Web Hacking-Serangan dan Pertahanannya". Andi Publisher
- Sitorus, Eryanto. 2006. "Hacker dan Keamanan". Andi Publisher
- Zam, Efy. 2015 "Teknik Hacking dengan SQL Injection". Elex Media Komputindo
- Zam, Efy. 2015 "Hacking aplikasi web : Uncensored". Jasakom