OPTIMALISASI RANCANG BANGUN KEAMANAN SISTEM INFORMASI DALAM KEAMANAN WEBSITE SISTEM AKADEMIK TERHUBUNG DENGAN E-LEARNING PADA SMK HARAPAN BANGSA DARI SERANGAN SQL INJECTION DAN CROSS SITE SCRIPTING

LAPORAN SKRIPSI

DESSY PUTRI ALVINI **4817050081**

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2021

OPTIMALISASI RANCANG BANGUN KEAMANAN SISTEM INFORMASI DALAM KEAMANAN WEBSITE SISTEM AKADEMIK TERHUBUNG DENGAN E-LEARNING PADA SMK HARAPAN BANGSA DARI SERANGAN SQL INJECTION DAN CROSS SITE SCRIPTING

LAPORAN SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

DESSY PUTRI ALVINI

4817050081

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2021

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama	**: Dessy Putri Alvini**
NIM	**: 4817050081**
Tanggal	**: 14 Juni 2021**
Tanda Tangan	**:** 

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama	: Dessy Putri Alvini
NIM	: 4817050081
Program Studi	: Teknik Multimedia dan Jaringan
Judul Skripsi	: Optimalisasi Rancang Bangun Keamanan Sistem Informasi Dalam Keamanan Website Sistem Akademik Terhubung Dengan E-Learning Pada SMK Harapan Bangsa Dari Serangan SQL Injection Dan Cross Site Scripting

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 16, Bulan Juni, Tahun 2021 dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I	: Fachroni Arbi Murad,S.Kom., M.Kom.	( )
Penguji I	: Indri Neforawati, S.T., M.T.	( )
Penguji II	: Maria Agustin, S.Kom., M.Kom.	( )
Penguji III	: Noorlela Marcheta, S.Kom., M.Kom.	( )

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Mauldy Laya, S.Kom., M.Kom.

NIP. 197802112009121003

KATA PENGANTAR

Puji dan Syukur kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan skripsi ini dengan judul "Optimalisasi Rancang Bangun Keamanan Sistem Informasi Dalam Keamanan Website Sistem Akademik Terhubung Dengan E-Learning Pada SMK Harapan Bangsa Dari Serangan SQL Injection Dan Cross Site Sripting". Penulisan laporan skripsi ini dilakukan untuk memenuhi syarat mencapai gelar Sarjana Terapan Politeknik. Penulis menyadari tanpa bantuan dan bimbingan dari berbagai pihak semasa perkuliahan hingga penyusunan laporan skripsi ini, sangat sulit bagi penulis dapat menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Mauldy Laya, S. Kom., M. Kom. selaku ketua jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta;
2. Bapak Defiana Arnaldy, S Tp., M. Si selaku ketua program studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta;
3. Bapak Fachroni Arbi Murad, S. Kom., M. Kom selaku dosen pembimbing yang telah membimbing serta menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan laporan skripsi ini;
4. Seluruh Dosen pengajar Jurusan Teknik Informatika dan Komputer pada Politeknik Negeri Jakarta;
5. Bapak Ali Imran selaku penghubung antara penulis dengan SMK Harapan Bangsa dan mengarahkan penulis dalam penelitian;
6. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan berupa moral dan material;
7. Sahabat dekat penulis yaitu Salwa Alifiah Putri Kamal, Ayu Sari Maulida, Mohammad Yasin, Rusdi Rajab Maulana, Rachmat Ramadhan, Abby Rafdi Cakrasena, dan Muhammad Rafif Fathian yang memberikan dukungan untuk menyelesaikan skripsi ini;

3. Sahabat sekaligus teman sekelompok saat Magang dan Skripsi yaitu Nur Suci Aviva dan Shafira Azzahra yang memberikan semangat dan membantu penulis dalam menyelesaikan laporan ini;
4. Serta teman teman TIK 2017 yang juga membantu penulis dalam menyelesaikan laporan skripsi ini;

Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 15 Mei 2021

Penulis

OPTIMALISASI RANCANG BANGUN KEAMANAN SISTEM INFORMASI DALAM KEAMANAN WEBSITE SISTEM AKADEMIK TERHUBUNG DENGAN E-LEARNING PADA SMK HARAPAN BANGSA DARI SERANGAN SQL INJECTION DAN CROSS SITE SCRIPTING

Abstrak

SMK Harapan Bangsa merupakan salah satu Sekolah Menengah Kejuruan Swasta yang berlokasi di Kota Depok yang dikelola oleh suatu yayasan. SMK Harapan Bangsa berkeinginan untuk mempunyai website sistem informasi akademik terhubung dengan e-learning dengan tujuan untuk membantu guru dan staff sekolah dalam melakukan manajemen absensi, agenda kegiatan, pengumuman, jadwal pelajaran dan juga laporan mengenai nilai siswa untuk membuat kegiatan menjadi lebih efektif dan efisien. Tetapi SMK Harapan Bangsa membutuhkan website dengan memiliki tingkat keamanan yang baik untuk mengamankan dari adanya celah yang memungkinkan serangan berupa SQL Injection dan Cross Site Scripting (XSS). Untuk itu dalam penelitian ini difokuskan pada optimalisasi rancang bangun keamanan sistem informasi dalam keamanan website sistem akademik terhubung dengan e-learning pada SMK Harapan Bangsa agar terciptanya website yang mudah digunakan, efisien dan dapat memperkecil adanya celah serangan SQL Injection dan Cross Site Scripting pada sistem informasi akademik tersebut sehingga aman untuk digunakan. Dikarenakan serangan SQL Injection dan Cross Site Scripting tergolong kedalam ancaman beresiko tinggi terhadap keamanan website. Dalam penelitian keamanan website sistem informasi akademik yang terhubung dengan e-learning pada SMK Harapan Bangsa menggunakan framework Laravel dan Bootstrap, dan melakukan Scanning Vulnerability menggunakan Acunetix, metode Penetration Testing celah keamanan yang diuji khususnya SQL Injection (menggunakan tools SQLMAP) dan Cross Site Scripting (XSS) dengan memasukan javascript, pencegahannya serta cara untuk menutup celahnya.

Kata Kunci: *Keamanan Informasi; Keamanan Website; Laravel; Penetration Testing; Scanning Vulnerability; SQL Injection; SQL MAP; XSS.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Internet merupakan media informasi yang sangat dibutuhkan masyarakat luas tidak terkecuali pada sebuah instansi pendidikan yang sangat membutuhkan jaringan internet untuk memenuhi kebutuhan seperti penilaian siswa, absensi siswa, absensi guru, jadwal pembelajaran, pengumuman dan lain-lain. Dengan mengandalkan internet, instansi pendidikan seperti pada SMK Harapan Bangsa menggunakan dan membutuhkan sistem informasi akademik terhubung dengan *e-learning* berbasis website yang dapat meningkatkan efisiensi dan efektifitas dalam penggunaannya. Sehingga diperlukannya sistem yang terjaga keamanan nya karena keamanan bertujuan untuk menciptakan rasa aman bagi manusia salah satunya keamanan di dunia teknologi. Kejahatan di dunia teknologi dan informasi terutama pada aplikasi website sangat sering terjadi contohnya kejahatan berupa serangan *SQL Injection* yaitu merupakan ancaman dengan memasukan code SQL berbahaya untuk mengambil database website serta melakukan *bypass verifikasi* akun pada website, dan juga kejahatan berupa *Cross Site Scripting* yaitu merupakan ancaman menginputkan code javascript berbahaya pada kolom dinamis website sehingga script yang dimasukan oleh penyerang akan terus berjalan setiap halaman yang terinjeksi dipanggil. Adanya kesalahan penulisan kode program dalam pembuatan website dimanfaatkan oleh penyerang dengan melakukan penyerangan *SQL Injection* dan *Cross Site Scripting*. Menurut BSSN (Badan Siber dan Sandi Negara) Sebanyak 32% dari aplikasi web paling tidak memiliki satu kerentanan SQL dan juga webappsec merilis bahwa sebanyak 35,57% kerentanan berupa *Cross Site Scripting*. Dari permasalahan tersebut, maka penulis melakukan optimalisasi rancang bangun keamanan sistem informasi dalam keamanan website sistem akademik terhubung dengan *E-Learning* pada SMK Harapan Bangsa untuk melakukan pencegahan dari serangan *SQL Injection* dan *Cross Site Scripting* (XSS) dan menutup celah keamanan.

Tahap-tahap yang dilakukan untuk optimalisasi rancang bangun keamanan pada aplikasi berbasis web meliputi *scope, reconnaissance, vulnerability detection, information analysis & planning,* dan *penetration testing*. Pada proses vulnerability detection dalam menemukan celah keamanan pada website dengan bantuan aplikasi yaitu Acunetix. Dan juga dilakukannya penyerangan berupa *SQL Injection* dan *Cross Site Scripting* untuk membuktikan website sistem informasi akademik pada SMK Harapan Bangsa aman, serta cara untuk menutup celahnya. Sehingga sistem informasi akademik terhubung dengan *e-learning* pada SMK Harapan Bangsa dapat digunakan untuk melakukan berbagai kegiatan meliputi pembelajaran, absensi, penilaian siswa dan lain lain dengan aman dan nyaman.

1.2 Perumusan Masalah

Berdasarkan hal-hal yang telah diuraikan dalam latar belakang, maka rumusan masalah dalam skripsi ini yaitu bagaimana optimalisasi rancang bangun keamanan sistem informasi dalam keamanan website sistem akademik terhubung dengan *e-learning* pada SMK Harapan Bangsa dari serangan *SQL Injection* dan *Cross Site Scripting* dengan melakukan *Penetration Testing* mengujikan *SQL Injection* dan *Cross Site Scripting* serta bagaimana cara untuk menutup celahnya.

1.3 Batasan Masalah

Berdasarkan latar belakang tersebut, dapat diuraikan batasan masalah untuk dibahas dalam penelitian ini yaitu:

1. Optimalisasi Rancang Bangun Keamanan Sistem Informasi Dalam Keamanan Website Sistem akademik terhubung dengan *E-Learning* pada SMK Harapan Bangsa dari serangan *SQL Injection* dan *Cross Site Scripting*.
2. Mengumpulkan informasi website sistem informasi akademik terhubung dengan *e-learning* pada SMK Harapan Bangsa dengan menggunakan tools Wappalyzer.
3. *Scanning Detection* untuk mencari celah keamanan website sistem informasi akademik yang terhubung dengan *e-learning* pada SMK Harapan Bangsa.

5. Melakukan analisis hasil dari *scanning detection* menampilkan celah keamanan pada website.
6. Melakukan *penetration testing* dengan yang diuji yaitu *SQL Injection* dengan menggunakan SQLMap untuk mendapatkan database pada website dan *Cross Site Scripting* (XSS) dengan *type Stored* XSS untuk memunculkan *message box* serangan XSS.
7. Menutup celah keamanan hasil dari *penetration testing SQL Injection* dan *Cross Site Scripting*.

1.4 Tujuan dan Manfaat

Berdasarkan perumusan masalah diatas maka didapatkan tujuan dan manfaat dari penelitian ini, yaitu:

1.4.1 Tujuan

Tujuan dari optimalisasi rancang bangun keamanan sistem informasi dalam keamanan website sistem akademik terhubung dengan *e-learning* pada SMK Harapan Bangsa yaitu untuk mencari celah kemanan pada website sistem akademik. Sehingga, dapat mencegah serta mengamankan dari serangan peretasan atau pencurian informasi seperti serangan *SQL Injection dan Cross Site Scripting* (XSS) dan langkah-langkah menutup celah keamanannya.

1.4.2 Manfaat

Manfaat pada optimalisasi rancang bangun keamanan sistem informasi dalam keamanan website sistem akademik terhubung dengan *e-learning* pada SMK Harapan Bangsa agar dapat mengetahui celah keamanan pada website sehingga dapat terhindar dari serangan berupa *SQL Injection* dan *Cross Site Scripting*. Serta user dapat menggunakan sistem informasi akademik yang terhubung dengan *e-learning* berbasis website dengan aman dan nyaman.

1.5 Metode Penyelesaian Masalah

Pada penelitian ini penulis menggunakan metode penelitian dengan pendekatan metode VAPT (*Vulnerability Assessment & Penetration Testing*) yaitu metode langkah-langkah untuk mendeteksi, mengidentifikasi dan mempelajari kelemahan yang dimiliki dari suatu sistem atau infrastruktur yang berbasis teknologi informasi dan pengujian keamanan suatu sistem informasi untuk mengetahui kelemahan sistem, dengan melakukan serangan ke sistem dengan memanfaatkan *vulnerability (hacking*), tanpa melakukan tindakan yang menyebabkan kerusakan sistem.

Tahapan-tahapan pada metode VAPT (*Vulnerability Assessment & Penetration Testing*) yaitu:

1. ***Scope***

   Pada tahapan ini peneliti menentukan ruang lingkup penelitian, seperti yang dijabarkan sebelumnya pada batasan masalah. Penelitian ini berfokus pada menemukan dan mengeksploitasi kerentanan website sistem akademik terhubung dengan *E-Learning* pada SMK Harapan Bangsa.

2. ***Reconnaissance***

   Tahapan selanjutnya mengumpulkan informasi awal tentang sistem pada website. Informasi itu dapat berupa sistem operasi yang dipakai web server, alamat IP, database yang digunakan dan port yang terbuka pada target yang diuji.

3. ***Vulnerability Detection***

   Pencarian celah keamanan pada target. Hasil dari temuan celah keamanan ini terbatas pada tools acunetix yang nantinya digunakan sebagai dasar perencanaan pada tahap berikutnya.

4. ***Information Analysis & Planning***

   Pada tahap ini penulis melakukan analisis pada hasil pencarian celah dan melakukan perencanaan pengujian yang didasarkan pada celah yang didapatkan. Hasil analisis kemudian dilanjutkan dengan perencanaan simulasi penyerangan.

Penetration testing

Pada tahap ini peneliti melakukan serangan terhadap target berdasarkan analisis dan perencanaan yang dirancang pada fase sebelumnya.

Privilege Escalation

Dengan memanfaatkan celah keamanan yang berhasil dilakukan pada proses penetration testing. Pemanfaatan celah yang dimaksud adalah manajemen data dan pemanfaatan hak akses.

Reporting

Tahap terakhir yaitu tahap penulisan laporan hasil penelitian.

BAB V

PENUTUP

5.1 Kesimpulan

Setelah melakukan tahapan analisis, perancangan, implementasi dan evaluasi dilakukan pada website sistem akademik terhubung dengan E-Learning pada SMK Harapan Bangsa agar terhindar dari serangan *SQL Injection* dan *Cross Site Scripting* (XSS). Maka dapat diambil kesimpulan sebagai berikut:

a. Terdapat celah keamanan *SQL Injection* dan *Cross Site Scripting* (XSS) dengan high risk pada website sistem akademik terhubung dengan E-Learning pada SMK Harapan Bangsa.
b. *Penetration testing SQL Injection* dan *Cross Site Scripting* (XSS) dapat dilakukan pada website sistem akademik terhubung dengan E-Learning pada SMK Harapan Bangsa dan sukses.
c. Setelah celah *SQL Injection* dan *Cross Site Scripting* (XSS) diberi pengaman, hasil *penetration testing* tidak dapat dilakukan karena sudah diberikan script tambahan pada codingan website nya untuk menutup celah.

5.2 Saran

Saat ini penelitian mengenai *penetration testing* yang dilakukan pada website sistem akademik terhubung dengan E-Learning pada SMK Harapan Bangsa, yaitu menggunakan *tools* SQLmap untuk melakukan *SQL Injection* dan juga *Cross Site Scripting* (XSS) yang dilakukan secara sederhana dengan hanya memunculkan *message box* untuk mengganggu user. Oleh karena itu, penulis menyarankan untuk pengembangan penelitian ini dengan melakukan *penetration testing SQL* Injection dengan metode *Blind* SQL yaitu tanpa menggunakan *tools* dan juga melakukan *penetration testing Cross Site Scripting* (XSS) dengan mengambil cookies pengguna.

DAFTAR PUSTAKA

Albert Sagala, E. M. (2014). DETEKSI, IDENTIFIKASI DAN PENANGANAN WEB MENGGUNAKAN SQL. *Seminar Nasional Ilmu Komputer2014 (SNIKOM)* .

Bagus Wicaksono, R. Y. (2020). PENGUJIAN CELAH KEAMANAN APLIKASI BERBASIS WEB. *Jurnal JARKOM Vol. 8 No. 1* .

Charania and V. Vyas. (2016). SQL Injection Attack :Detection and Prevention. *int Res. J. Eng. Techno*.

Ciamppa, M. (2012). *Security + Guide to Network Security Fundamentals*. Boston: Course Technology.

Clarke, J. (2009). *SQL Injection Attacks and Defense*. Burlington: Syngress.

Engebretson, P. (2011). *The Basics of hacking and penetration Testing*. Waltham: Elsevier.

Harsono. (2002). *Implementasi Kebijakan dan Politik*.

Kiezun, A. G. (2009). Automatic creation of SQL injection. *International Conference on Software*, 119-209.

Kiezun, G. d. (2009). *SQL injection*.

kingthorin, n. (n.d.). *SQL Injection*.

Liu, M. Z. (2019). A Survey of Exploitation and Detection Methods of XSS. *IEEE access*.

Meucci, A. M. (2014). *The Testing Guide v4*.

Muhammad Mushlih, R. F. (2019). PENETRATION TESTING TOOL UNTUK MENGUJI KERENTANAN SQL. *Prosiding SNRT (Seminar Nasional Riset Terapan)*.

Muhammad Mushlih, R. F. (2019). PENETRATION TESTING TOOL UNTUK MENGUJI KERENTANAN SQL. *Prosiding SNRT (Seminar Nasional Riset Terapan)*. Banjarmasin.

Ojha, M. K. (2014). Attack Penetration System for SQL Injection. *Int. J. Adv. Comput. Res.*, *vol. 4*, *no. 2*, 724–732.

Putra, S. S. (2017). Penanggulangan Serangan XSS, CSRF, SQL Injection. *Jurnal Pendidikan dan Teknologi Informasi Vol. 4, No. 2*, 289-300 .

R. M. Pandurang, D. C. (2016). A mappingbased podel for preventing Cross site. *Conf. Next Gener.*, 414–418.

Rahajeng Ellysa, M. H. (2013). Pendeteksi Serangan SQL Injection Menggunakan Algoritma SQL Injection Free Secure pada Aplikasi Web. *JURNAL TEKNIK POMITS Vol. 2, No. 1*.

Rahmawati. (2017). Sistem Informasi Akademik Berbasis Web. *Indonesian Journal on Networking and*.

Reza Rafsanjani Prayogo, V. W. (n.d.). Analisis keamanan menggunakan web aplikasi bwapp terhadap serangan.

Sahtyawan, R. (2019). PENERAPAN ZERO ENTRY HACKING DIDALAM SECURITY. *JURNAL OF INFORMATION SYSTEM MANAGEMENT*, 18-21.

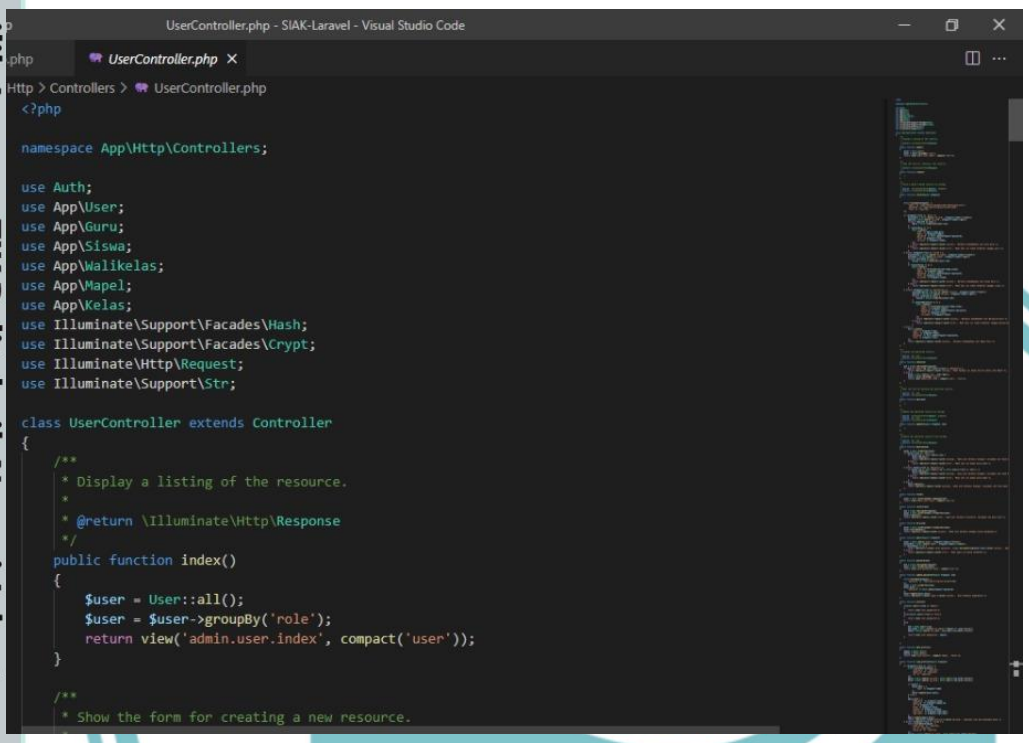
Sarno, I. (2009). *Sistem Manajemen Keamanan Informasi*. Surabaya: Itspress.

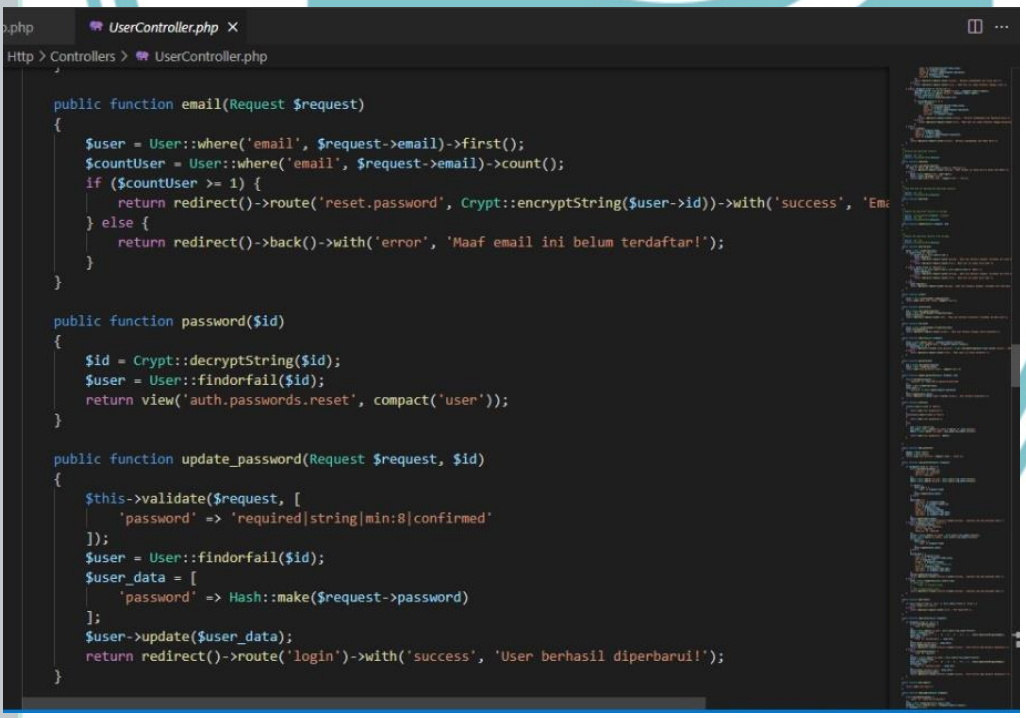
Sudiharyanto Lika, R. D. (2018). ANALISA SERANGAN SQL INJEKSI MENGGUNAKAN SQLMAP. *Jurnal Sistem dan Teknologi Informasi*, Volume 4, No.2, 2018, pg. 88 - 94 .

Wahab, S. A. (2001). *Analisis Kebijakan Dari Formulasi ke Implementasi Kebijaksanaan Negara* .

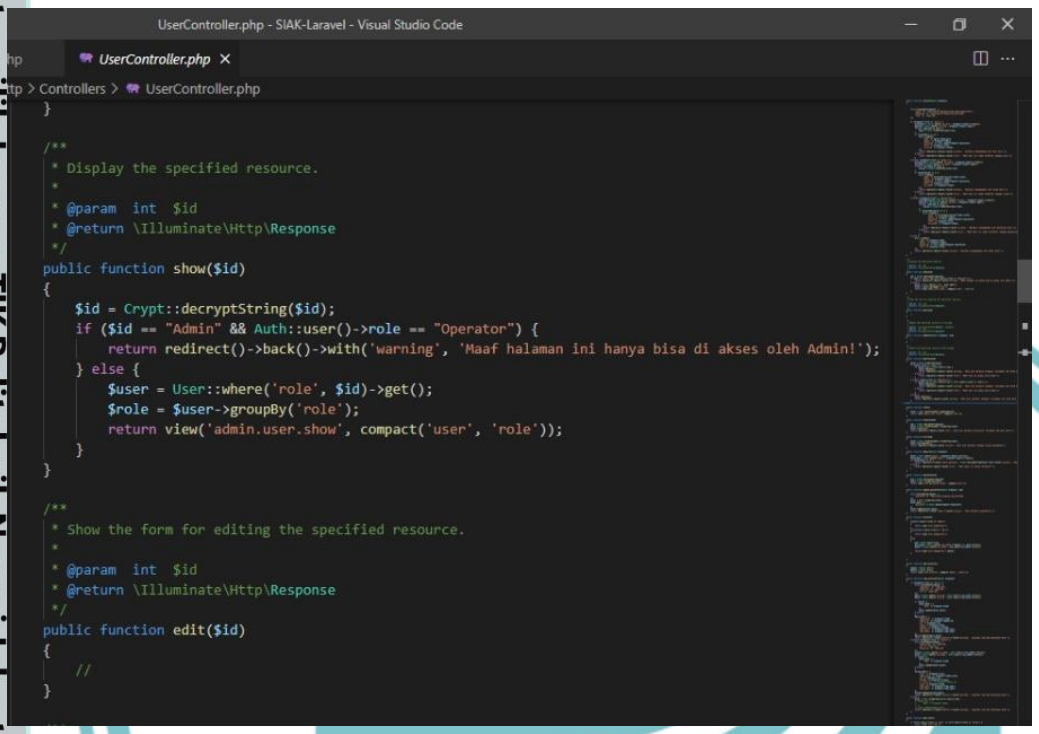
Yunanri W, I. R. (2018). Analisis Deteksi Vulnerability Pada Webserver Open Jurnal Sistem Menggunakan OWASP Scanner. *JURTI*.

1. **Pada UserController setelah dipasang pencegahan *SQL Injection***

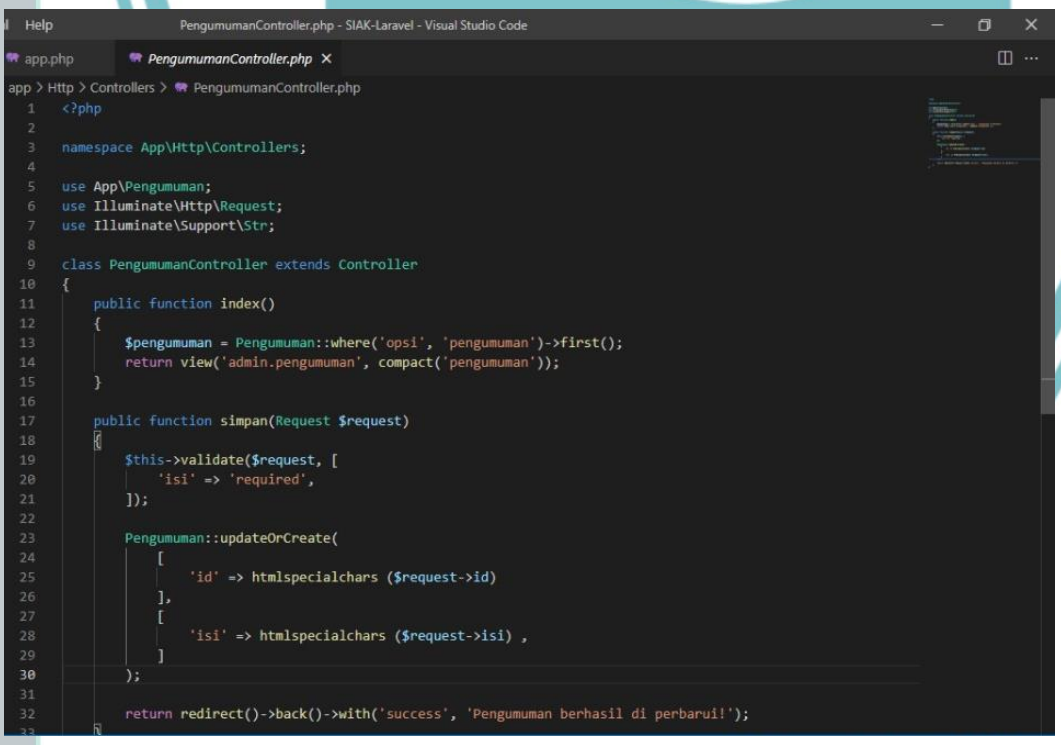




(Lanjutan)

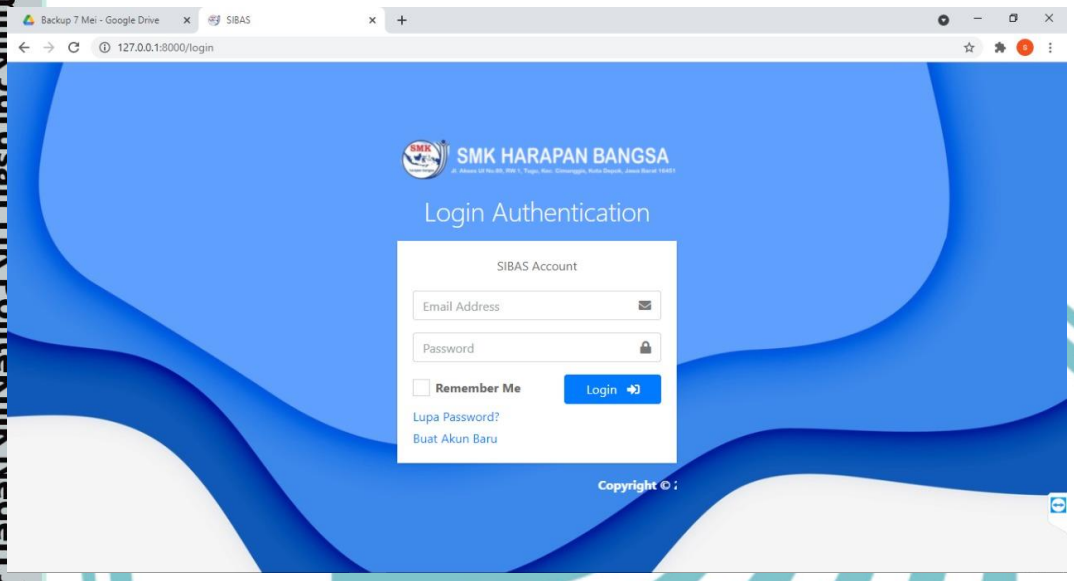


2. Pada Pengumuman setelah diberi pencegahan *Cross Site Scripting* (XSS)

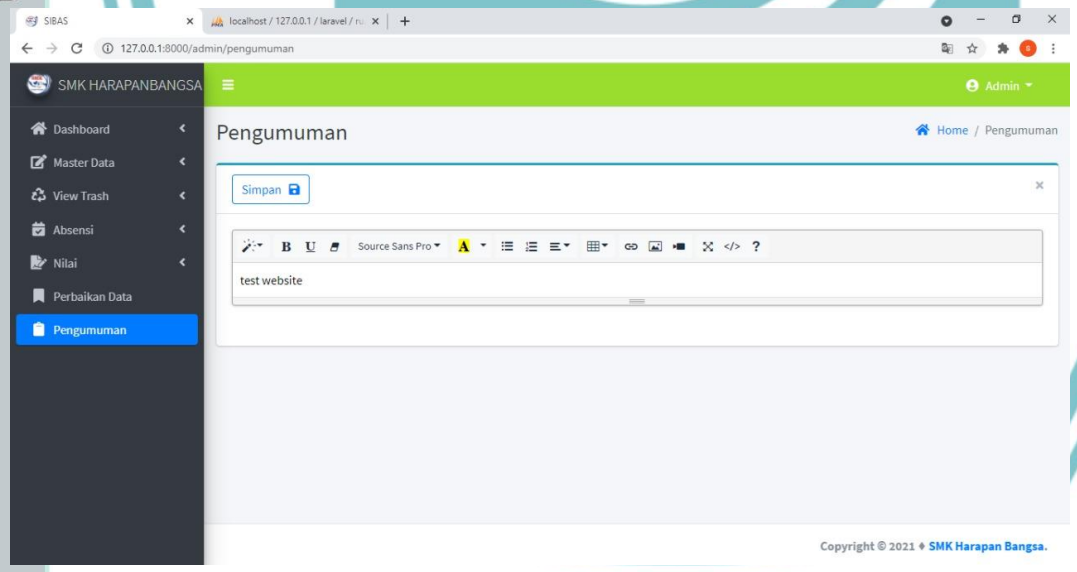


Lampiran – Tampilan Front-end

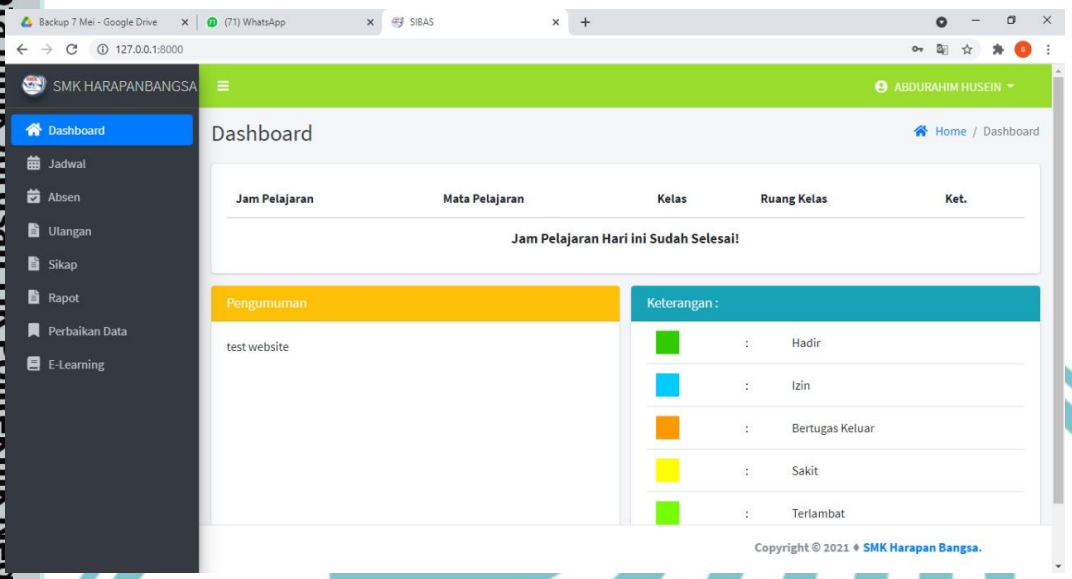
1. **Tampilan Form Login**



2. **Tampilan Form Admin Input Pengumuman**



3. **Tampilan Dashboard Siswa**



4. **Tampilan Dashboard Guru**