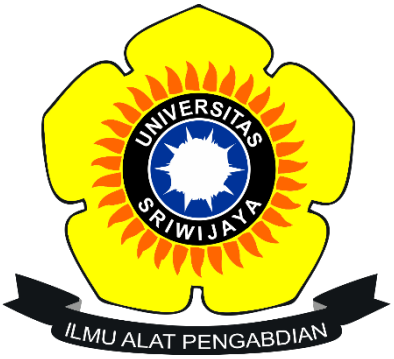
PENINGKATAN KEAMANAN WEB TERHADAP SERANGAN CROSS SITE SCRIPTING DENGAN METODE METACHARACTER

TUGAS AKHIR

Diajukan Untuk melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer



OLEH:

FRISKI EXAUDI

09011181722014

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

PENINGKATAN KEAMANAN WEB TERHADAP SERANGAN CROSS SITE SCRIPTING DENGAN METODE METACHARACTER

TUGAS AKHIR

Diajukan Untuk melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

FRISKI EXAUDI

09011181722014

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

HALAMAN PENGESAHAN

PENINGKATAN KEAMANAN WEB TERHADAP SERANGAN CROSS SITE SCRIPTING DENGAN METODE METACHARACTER

SKRIPSI

Program Studi Sistem Komputer

Jenjang S1

Oleh:

FRISKI EXAUDI

09011181722014

Indralaya, 17 Desember 2022

Mengetahui,

Pembimbing Tugas Akhir 1	Pembimbing Tugas Akhir 2
Ahmad Heryanto, S.Kom., M.T.	**Adi Hermansyah,S.Kom., M.T.**
NIP. 198701222015041002	**NIP.**

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP.196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu

Tanggal : 07 Desember 2022

Tim Penguji :

1. Ketua Sidang : Sarmayanta Sembiring, M.T.
2. Sekretaris Sidang : Abdurahman, S.Kom., M.Han.
3. Penguji Sidang : Aditya Putra Perdana P, M.T
4. Pembimbing I : Ahmad Heryanto, M.T.
5. Pembimbing II : Adi Hermansyah, M.T.

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Friski Exaudi

NIM : 09011181722014

Judul : Peningkatan Keamanan Web Terhadap Serangan Cross Site Scripting Dengan Metode Metacharacrter

Hasil Penyecekan *Software iThenticate/Turnitin* : 8%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Indralaya, Desember 2022

Friski Exaudi
NIM. 09011181722014

KATA PENGANTAR

Shalom Salam Sejahtera.

Puji dan syukur penulis panjatkan atas kehadirat Tuhan Yesus yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis sampai pada saat ini dapat menyelesaikan penyusunan tugas akhir ini dengan judul **"PENINGKATAN KEAMANAN WEB TERHADAP CROSS SITE SCRIPTING DENGAN METODE METACHARACTER"**

Pada penyusunan tugas akhir ini, tidak terlepas dari bantuan, bimbingan, ajaran serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan terima kasih kepada:

1. Tuhan yang Maha Esa yang telah memberikan berkah dan karunia-Nya kepada penulis dalam penyusunan tugas akhir ini.
2. Orangtua tercinta yang selalu memberikan motivasi, semangat dan do'a serta keluarga besar penulis yang tersayang.
3. Kakak ku tercinta yang selalu memberikan semangat dan do'a
4. Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya
5. Ibu Prof. Dr. Ir. Siti Nurmaini, M. T. selaku Dosen Pembimbing Akademik.
6. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Pembimbing Tugas Akhir 1.
7. Bapak Adi Hermansyah, S.Kom., M.T. selaku Pembimbing Tugas Akhir 2.
8. Mbak Renny selaku Admin Jurusan Sistem Komputer.
9. Kakak tingkat sistem komputer yang memberikan masukan selama perkuliahan.
10. Teman-teman seperjuangan yaitu Agung 17 yang merasakan suka dan duka bersama, terutama untuk savior dan yang tersisah yang telah memberikan semangat dalam menyelesaikan tugas akhir ini.
11. Pacar saya yang saya sayangi yaitu Veronika Oktavia Sinaga yang banyak membantu dan menyemangati saya dalam kesusahan, menemani menyusun berkas dan semua yang saya butuhkan.

12. Louis Sinaga,Suryani Siahaan dan Tessia Sinaga yang telah memminjamkan printernya.
13. Serta semua pihak yang tidak dapat penulis cantumkan satu persatu, yang membantu dan memberikan doa yang terbaik untuk kelancaran tugas akhir ini.
14. Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya.

Didalam penyusunan laporan tugas akhir ini penulis menyadari masih terdapat kekurangan dan kesalahan. Oleh karena itu, sebagai bahan perbaikan kedepannya penulis tentunya mengharapkan koreksi, saran, serta masukan terhadap isi dari tugas akhir ini.

Akhir kata, semoga dengan pembuatan penelitian tugas akhir ini akan menjadi tambahan ilmu dan pengembangan wawasan terhadap pengolahan citra digital dan dapat menjadi bahan refrensi bagi yang membacanya.

Shalom Salam Sejahtra.

Indralaya, Desember 2022

Friski Exaudi
NIM. 09011181722014

Peningkatan Keamanan Web Terhadap Serangan Cross Site Scripting Dengan Metode Metacharacrter

Friski Exaudi (09011181722014)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email : friskiexaudi@gmail.com

ABSTRAK

Sekarang semakin banyak munculnya website baru, maka tingkat traffic Cybercrime akan semakin meningkat juga. Cybercrime adalah tindak kejahatan yang dilakukan dengan memanfaatkan teknologi komputer sebagai alat kejahatan utama yang memanfaatkan perkembangan teknologi komputer khususnya internet. Salah satunya Cross Site Scripting (XSS) merupakan serangan pada halaman website atau website aplikasi. Cross Site Scripting (XSS) terjadi saat halaman web yang dibuat secara dinamis menampilkan input yang tidak divalidasi dengan benar. Hal ini memungkinkan penyerang untuk menanamkan malware Kode atau JavaScript ke halaman yang dihasilkan dan menjalankan skrip di mesin pengguna mana pun yang melihat situs itu. Hasil dari pengolahan serangan dievaluasi untuk dianalisa dengan metode metacharacter agar website tidak dapat di serang megunakan kode atau javascript dari serangan Cross Site Scripting (XSS). Dari hasil analisa disini didapatkan serangan Cross Site Scripting (XSS) tidak dapat masuk dan mencuri data website yang telah di coding metacharacter.

Kata Kunci : Peningkatan Keamanan Web Terhadap Serangan Cross Site Scripting Dengan Metode Metacharacrter

Improved Web Security Against Cross Site Scripting Attacks With the Metacharacter Method

Friski Exaudi (09011181722014)

Departement of Computer Engineering, Faculty of Computer Science,

University of Sriwijaya

Email : friskiexaudi@gmail.com

ABSTRACT

Now more and more new websites appear, the level of Cybercrime traffic will also increase as well. Cybercrime is a crime committed by utilizing computer technology as the main crime tool that utilizes developments in computer technology, especially the internet. One of them is Cross Site Scripting (XSS) which is an attack on a website page or website application. Cross Site Scripting (XSS) occurs when a dynamically generated web page displays input that is not properly validated. This thing enabled dan attacker to embed malware Code or JavaScript into the resulting page and run the script on any machine of the user viewing the site. The results of attack processing are evaluated for analysis using the metacharacter method so that websites cannot be attacked using code or JavaScript from Cross Site Scripting (XSS) attacks. From the results of the analysis here, it is found that Cross Site Scripting (XSS) attacks cannot enter and steal website data that has been coded metacharacter.

***Keywords* :** *Improved Web Security Against Cross Site Scripting Attacks With the Metacharacter Method*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

Daftar Lampiran

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada saat ini perkembangan teknologi sangatlah cepat dan tidak dapat dibendung lagi. Perkembangan teknologi yang semakin pesat sekarang ini menuntut kita untuk mengikuti arus perkembangan teknologi tersebut, begitu juga bagi instansi akan melakukan modernisasi seperti pemanfaatan teknologi komputer [1]. Dimana pada saat ini hampir disemua sektor memerlukan teknologi yang dimana teknologi tersebut digunakan untuk menggantikan pekerjaan manusia serta memfasilitasi dan juga mengikuti perkembangan jaman yang mulai menerapkan digitalisasi pada semua sektor dengan begitu banyak hal yang akan tergantikan dan juga terbaharui. Seperti contohnya zaman sekarang teknologi juga merambah ke sektor bisnis dan komerisal dengan ditandai banyak munculnya website jualan sebuah produk , barang , ataupun jasa. Dengan menggunakan website sebagai tempat berjualan otomatis pedagang tidak terlalu membutuhkan toko fisik , mereka hanya membuat toko online kemudian ditoko tersebutlah para pedagang menjual dan memasarkan produknya kekonsumen.

Dikarenakan jaman sekarang semakin banyak munculnya website baru maka tingkat traffic akan *Cybercrime* akan semakin meningkat juga. *Cybercrime* adalah tindak kejahatan yang dilakukan dengan memanfaatkan teknologi komputer sebagai alat kejahatan utama yang memanfaatakan perkembangan teknologi komputer khususnya internet [2]. Seperti contoh *Cybercrime* yang sering umum dipakai adalah teknik *Cross Site Scripting* (XSS) , *Cross Site Scripting* merupakan serangan pada halaman website atau website aplikasi. *Cross Site Scripting* pada umumnya digunakan untuk mengambil atau mencuri session cookies user , yang membuat penyerang menyamar atau berkamuflase sebagai korban atau target. Dengan begitu peretas bisa mendapat informasi data sensitif dari pada korban atau target tersebut. Terdapat tiga jenis serangan XSS yaitu: *reflected*, *stored* dan *DOM-*

based. *Reflected* XSS dieksekusi melalui browser dan terjadi jika website menyediakan tempat bagi pengguna untuk melakukan masukan. *Stored* XSS terjadi ketika kode berbahaya berhasil tersimpan ke dalam database dan dapat dieksekusi oleh pengguna lain (biasanya melalui sebuah link yang yang telah diinjeksi dengan kode berbahaya). *DOM-based* XSS terjadi ketika peretas dapat melakukan serangan XSS di sisi client side melalui DOM (Document Object Model), serangan ini dilakukan dengan memanfaatkan celah keamanan website pada bagian client side [3].

Berdasarkan penelitian yang pernah dilakukan oleh Stuttard [4] terhadap 100 lebih aplikasi web, ternyata masih banyak yang memiliki celah keamanan. Celah-celah keamanan yang ditemukan dan prosentasenya yaitu: Kesalahan Otentikasi (62%), Kesalahan Akses Kontrol (71%), *SQL injection* (32%), *Cross-site Scripting* – XSS (94%), Kebocoran Informasi (78%), dan Crosssite Request Forgery – CSRF (92%). Dengan demikian dianggap perlu melakukan pencegahan terhadap kejahatan Cross- site scripting. Celah keamanan dengan presentase terbesar adalah *Cross-site Scripting*– XSS (94%).

Pada penelitian lainnya[5], Algoritma deep learning dipakai seraya menemukan serangan *SQL injection* dan XSS. Kebaruan utama deteksi serangan injection menggunakan deep learning terdiri dari adopsi *Convolutional Deep Neural Network* dan dalam meningkatkan efektivitasnya melalui tahap pra-pemrosesan yang disesuaikan terkait SQL / XSS menjadi pasangan nilai. Eksperimen numerik yang dilakukan pada dataset dunia nyata untuk serangan SQL dan XSS menunjukkan bahwa, dengan pelatihan yang identik dan dengan bentuk jaringan neural yang sama, jenis pengkodean / nilai deteksi serangan injection menggunakan deep learning meningkatkan tingkat deteksi dari dasar sekitar 75% hingga akurasi 95% , Presisi 99%, dan nilai perolehan 92%.

Pada penelitian [6] , membahas bagaimana mengklasifikasikan serangan *Cross Site Scipting* (XSS) menggunakan 10 algoritma Machine Learning. Penelitian ini menggunakan dataset yang diperoleh dari sumber internet terpercaya yaitu XSSed, Alexa, dan Elgg berjumlah 1000 dimana terbagi

menjadi 400 data normal dan 600 data serangan. Dari proses klasifikasi yang dilakukan, algoritma Random Forest mendapatkan hasil terbaik yaitu nilai akurasi 97.2%, nilai presisi 97.7%, nilai sensitivitas 97.1%, dan nilai F1-score 97.4%.

Sehingga solusi yang ditawarkan adalah penggunaan *Metacharacter* untuk memfilter inputan yang merupakan sebuah payload untuk mentrigger error yang merefleksikan bug XSS. *Metacharacter* sendiri banyak digunakan dikarenakan kefektifanya dalam mengatasi bug dan juga penggunaanya yang cukup mudah dengan menggunakan beberapa statement yang telah tersedia. *Metacharacter* juga dapat dipadukan dengan filter dari HTML sehingga membuat filter menjadi berlapis - lapis. Sehingga sangat meminimalisir terjadinya bug XSS tersebut , untuk menjaga keamanan website perlu diaplikasikan disetiap page atau halaman yang mempunyai inputan seperti kolom search atau pencarian , form upload , form komentar dan lain - lain. Oleh karena itu penulis mengambil topik penelitian ini dengan judul "Peningkatan Keamanan Web Terhadap Serangan *Cross Site Scripting* Dengan Metode *Metacharacter*"

1.2 Tujuan

Bedasarkan latar belakang masalah yang telah penulis uraikan diatas maka penulis membuat tujuan sebagai berikut :

1) Untuk mengetahui bagaimana cara serangan *Cross Site Scripting* bekerja.
2) Untuk mengatasi serangan *Cross Site Scripting* dengan menggunakan metode *Metacharacter*.

1.3 Manfaat

Adapun manfaat dari penelitaian ini sebagai berikut :

1) Dapat menjadikan penelitian ini sebagai salah satu cara untuk menghindari resiko terhadap serangan *Cross Site Scripting* (XSS).
2) Dapat menerapkan metode *Metacharacter* dalam mengatasi serangan *Cross Site Scripting*.

1.4 Rumusan Masalah

Bedasarkan latar belakang masalah yang telah penulis uraikan diatas maka penulis merumuskan masalah sebagai berikut :

1) Apa bahaya yang ditimbulkan oleh serangan *Cross Site Scripting* ?
2) Bagaimana menggunakan metode *Metacharacter* untuk memfilter inputan dapat mencegah serangan *Cross Site Scripting*?

1.5 Batasan Masalah

Untuk menjaga fokus penilitian dalam Tugas Akhir ini, Batasan masalah penelitian sebagai berikut:

1) Website yang dibuat menggunakan bahasa pemograman web PHP dan HTML.
2) Website menggunakan hosting localhost xampp.
3) Membahas proses teknik ekploitasi *Cross Site Scripting* (XSS) pada website dan menggunakan 10 kode injeksi.
4) Membahas jenis teknik *Cross Site Scripting* (XSS) *Stored* dan self *Reflected* yang digunakan untuk mengeksploitasi website yang menggunakan bahasa pemrograman web PHP.
5) Website hanya dapat melakukan login saja dan hanya terdapat user dummy untuk simulasi stealing cookies dan session saja.
6) Website dummy hanya berisi fitur login , halaman artikel dan halaman home saja.
7) Pengamanan website menggunakan *Metacharacter*

1.6 Metodologi Penelitian

Pada Metodologi penelitian memiliki beberapa tahap sebagai berikut ini:

1. Tahap Pertama (Studi Pustaka / Literatur)
   Tahapan ini dilakukan setelah masalah yang telah di bahas sesuai dengan kerelevan penelitian sebelumnya yang mengacu banyaknya artikel, paper, jurnal dan buku yang berhubungan dengan penelitian ini yang berjudul

"*Peningkatan Keamanan Web Terhadap Serangan Cross Site Scripting Dengan Metode Metacharacter*".

2. Tahap Kedua (Penerapan Metode)

   Tahapan ini merupakan tahapan dimana menentukan perangkat-perangkat yang dibutuhkan pada penelitian ini, baik berupa perangkat keras maupun lunak.

3. Tahap Ketiga (Pengujian)

   Tahapan ini berupa pengujian yang sesuai dengan parameter-parameter serangan yang ditentukan oleh batasan masalah.

4. Tahap Keempat (Hasil dan Analisa)

   Tahapan ini berisi hasil pengujian pada penelitian tersebut kemudian dianalisa hasil tersebut guna mengetahui apa kelebihan dan kekurangan rancangan penelitian beserta faktor yang mempengaruhi.

5. Tahap Kelima (Kesimpulan dan Saran)

   Tahapan terakhir berisi tentang kesimpulan dan saran dari hasil studi pustaka, perancangan sistem dan analisa pada penelitian tersebut. Pada saran berisi poin-poin dari penulis untuk penelitian selanjutnya

1.7 Sistematik Peneilitian

a. Sistematika Penulisan

Sistematika penulisan laporan bertujuan untuk memudahkan dalam memahami laporan tugas akhir ini. Secara garis besar laporan tugas akhir ini dibuat dengan sistematika sebagai berikut :

BAB I PENDAHULUAN

Berisi pembahasan masalah umum yang meliputi latar belakang, rumusan masalah, batasan masalah, tujuan penilitan, manfaat penilitian, metodologi penilitian, dan sistematika penulisan laporan Tugas Akhir.

BAB II LANDASAN TEORI

Berisi pembahasan mengenai teori – teori yang mendukung pada proses penelitian yang dibuat.

BAB III METODOLOGI PENILITIAN

Berisi tentang analisis teknik *Cross Site Scripting* (XSS) dengan menggunakan metode Metacharakter yang digunakan dalam penelatian ini.

BAB IV HASIL DAN PEMBAHASAN

Berisi tentang hasil penilitian yang berupa tahapan dari hasil perancangan sistem sesuai dengan tujuan yang diharapkan.

BAB V KESIMPULAN DAN SARAN

Berisi tentang kesimpulan dari keseluruhan penilitian dan saran rekomendasi berdasarkan hasil penelitian.

Daftar Pustaka

[1] Q. Li, W. Li, J. Wang, and M. Cheng, "A SQL Injection Detection Method Based on Adaptive Deep Forest," *IEEE Access*, vol. 7, pp. 145385–145394, 2019, doi: 10.1109/ACCESS.2019.2944951.

[2] X. Zhang, Y. Zhou, S. Pei, J. Zhuge, and J. Chen, "Adversarial Examples Detection for XSS Attacks Based on Generative Adversarial Networks," *IEEE Access*, vol. 8, pp. 10989–10996, 2020, doi: 10.1109/ACCESS.2020.2965184.

[3] Vaigai College of Engineering, Institute of Electrical and Electronics Engineers. Madras Section, and Institute of Electrical and Electronics Engineers, *Proceedings of the 2017 International Conference on Intelligent Computing and Control Systems (ICICCS) : June 15-16, 2017*.

[4] I. Institute of Electrical and Electronics Engineers. Bombay Section. Symposium (2015 : Mumbai, Institute of Electrical and Electronics Engineers. Bombay Section, Shreemati Nathibai Damodar Thackersey Women's University. Usha Mittal Institute of Technology, and Institute of Electrical and Electronics Engineers, *IEEE Bombay Section Symposium : Theme: Frontiers of Technology: Fuelling Prosperity of Planet and People : September 10-11, 2015, Usha Mittal Institute of Technology, SNDT, Mumbai.*

[5] S. Abaimov and G. Bianchi, "CODDLE: Code-Injection Detection with Deep Learning," *IEEE Access*, vol. 7, pp. 128617–128627, 2019, doi: 10.1109/ACCESS.2019.2939870.

[6] M. Haris and U. Sharif, "Web Attacks Analysis and Mitigation Techniques Artificial intelligence and machine learning in healthcare View project Artificial Intelligence Against Cyber Attacks View project." [Online]. Available: www.ijert.org

[7] M. Akbar and M. Arif Fadhly Ridha, "SQL Injection and Cross Site Scripting Prevention Using OWASP Web Application Firewall."

[8] U. Sarmah, D. K. Bhattacharyya, and J. K. Kalita, "A survey of detection methods for XSS attacks," *Journal of Network and Computer Applications*, vol. 118. Academic Press, pp. 113–143, Sep. 15, 2018. doi: 10.1016/j.jnca.2018.06.004.

[9] P. Raman, ProQuest (Firm), and Carleton University. Theses and Dissertations. Computer Science., *Jaspin: Javascript based anomaly detection of cross-site scripting attacks*. 2008.

[10] A. F. Ella Hassanien Ahmad Taher Azar Tarek Gaber Roheet Bhatnagar Mohamed Tolba Editors, "Advances in Intelligent Systems and Computing 921 The International Conference on Advanced Machine Learning Technologies and Applications (AMLTA2019)." [Online]. Available: http://www.springer.com/series/11156

[11] M. Taufik Rizal, "PERANGKAT LUNAK TRACKING PENJUALAN PRODUK MAICIHBERBASIS MOBILEDAN WEB," 2012.

[12] S. Rochimah, D. Sunaryono, S. Kom, and M. Kom, "Komentar Semi Otomatis Untuk Memudahkan Pemahaman Pada Bahasa Pemrograman Java," 2017.

[13] O. E. S. Liando, J. Reimon Batmetan, and D. M. Demhi, “Cross-site Scripting Reflected as A Risk High-Level Attack on University Website,” 2022. [Online]. Available: http://192.100.0.65/gtadmisi/index.php?act=view&mod=home&sub=home Daftar&typ=ht