ANALISIS SERANGAN REFLECTED XSS ATTACKS PADA APLIKASI WEB DENGAN METODE BAYESIAN NETWORK

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

Ryston Galatians Sihombing

09011381722098

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

Lembar Pengesahan

ANALISIS SERANGAN REFLECTED XSS ATTACKS PADA APLIKASI WEB DENGAN METODE BAYESIAN NETWORK

TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

Oleh :

Ryston Galatians Sihombing

09011381722098

Indralaya, Mei 2022

Mengetahui,

Pembimbing Tugas Akhir I	Pembimbing Tugas Akhir II
Ahmad Heryanto, S.Kom., M.T.	**Tri Wanda Septian, M.Sc**
NIP. 198701222015041002	**NIP. 1901062809890001**

Ketua Jurusan Sistem Komputer

Dr.Ir.Sukemi,M.T.

NIP. 197806112010121004

Halaman Persetujuan

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 10 Maret 2022

Tim Penguji :

1. Ketua Sidang : Ahmad Zarkasi, M.T
2. Sekretaris Sidang : Rendyansyah, M.T
3. Penguji Sidang : Huda Ubaya, M.T
4. Pembimbing I : Ahmad Heryanto, S.Kom., M.T
5. Pembimbing II : Tri Wanda Septian, M.Sc

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T

NIP. 196612032006041001

iii

Halaman Pernyataan

Yang bertanda tangan dibawah ini :

Nama	: Ryston Galatians Sihombing
Nim	: 09011381722098
Prorgram Studi	: Sistem Komputer
Judul Penelitian	: Analisis Serangan Reflected XSS Attacks pada Aplikasi Web dengan Metode *Bayesian Network.*

Hasil Pengecekkan *Software iTehnticate/ Turnitin* : 5%

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

Demikian surat pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, Mei 2022

Ryston Galatians Sihombing

NIM. 09011381722098

Halaman Persembahan

“Jangan ingat lelahnya belajar, tapi ingatlah buah manisnya yang bisa dipetik kelak Ketika sukses”

“Jadilah diri kita sendiri karena itu lebih baik daripada berpura-pura menjadi orang lain”

“Kesuksesan itu bukan ditunggu, tetapi diwujudkan lewat usaha dan kerja keras”

Kata Pengantar

Segala Puji dan Syukur penulis panjatkan kepada Tuhan yang maha Esa, berkat rahmat karunia serta ijin-Nya sehingga penulis dapat menyelesaikan penulisan tugas akhir dengan judul **"Analisa Serangan Reflected XSS pada Aplikasi Web dengan metode Bayesian Network".** Penulisan tugas akhir ini dibuat dalam rangka memenuhi persyaratan untuk menyelesaikan pendidikan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya untuk memperoleh gelar strata 1.

Pada Kesempatan ini, penulis menyampaikan ucapan terima kasih kepada semua pihak untuk setiap bimbingan, semangat, dukungan, dan doa yang diberikan kepada penulis sehingga terselesaikannya tugas akhir ini. Ucapan terima kasih penulis sampaikan kepada:

1. Tuhan Yang Maha Esa, yang telah memberikan segalanya kepada penulis berupa Kesehatan, orang tua, pembimbing, teman, rezeki, dll sehingga dapat menyesaikan laporan tugas akhir ini.
2. Orang tuaku terkasih, Papa Rowon Sihombing dan Mama Ganda Marlinang Siahaan, adek-adek ku Thania dan Gyto tersayang, dan semua keluarga besarku, yang selalu ada dan tidak pernah lelah dalam mendidik serta memberikan dukungan baik secara moril maupun materil kepada penulis demi lancarnya penulisan tugas akhir ini.
3. Bapak Ahmad Heryanto, M.T dan Bapak Tri Wanda Septian, M.Sc selaku dosen pembimbing tugas akhir, yang telah memberikan bimbingan, masukan, semangat, dan kemudahan kepada penulis dalam menyelesaikan tugas akhir ini.
4. Bapak Bambang Tutuko M.T selaku pembimbing akademik, yang telah membimbing penulis dari semester satu hingga terselesainya tugas akhir ini dengan baik.
5. Bapak Dr.Ir. H. Sukemi M.T selaku ketua jurusan sistem komputer fakultas ilmu komputer Universitas Sriwijaya.

6. Seluruh dosen jurusan sistem komputer fakultas ilmu computer universitas sriwijaya.
7. Staff dijurusan sistem komputer, yang telah banyak membantu penyelesaian proses administrasi.
8. Staff difakultas ilmu komputer, bagian akademik, kemahasiswaan, tata usaha, perlengkapan, dan keuangan, yang telah membantu penyelesaian proses administrasi.
9. Seluruh petinggi atau pimpinan yang ada dilingkungan fakultas ilmu komputer universitas sriwijaya, yang telah membantu proses administrasi selama dikampus
10. Almamater.

Indralaya, Mei 2022

Ryston Galatians Sihombing
NIM. 09011381722098

Analisis Serangan *Reflected XSS* Attacks Pada *Aplikasi Web* Dengan Metode *Bayesian Network*

Ryston Galatians Sihombing (09011381722098)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email : galatian09@gmail.com

Abstrak

Semakin pesatnya perkembangan teknologi informasi dalam *aplikasi web*, maka gangguan atau tindakan – tindakan para penyerang (hacker) semakin meningkat juga. Hal ini dapat kita lihat di media-media cetak, ataupun elektronik, dimana media tersebut memberitakan aksi-aksi para hacker untuk menyerang situs-situs web yang ada. Serangan *reflected XSS* merupkan jenis serangan yang berusaha mencoba memasukan atau menyuntikkan beberapa kode script, dimana kode script disini dapat disimpan di database yang ada dalam situs web, dalam hal ini script yang telah dimasukkan dikembalikan ke server aplikasi pengguna. Misalnya pesan kesalahan yang ditunjukkan akan dapat dimunculkan pada browser client yang lain. Pola serangan dari reflected XSS pada dataset *dataset for Deep learning | Kaggle,* akan dapat dikenali dengan beberapa parameter seperti sentence, label, ngram1, ngram2 dan ngram3. Hasil dari pengolahan dataset dievaluasi untuk dianalisa dengan metode bayesian network untuk dapat diketahui seberapa besar akurasi dari Analisa serangan reflected XSS. Dari hasil analisa disini didapatkan nilai akurasi sebesar 99.71% nilai presisi sebesar 99.85%, nilai recall sebesar 99,72% dan nilai f1 – score sebesar 99.78%.

Kata Kunci : Analisa Serangan Reflected XSS pada aplikasi web dengan Metode *Bayesian Network*

Analysis Of Reflected XSS Attacks On Web Applications With Method On Bayesian Network

Ryston Galatians Sihombing (09011381722098)
Departement of Computer Engineering, Faculty of Computer Science,
University of Sriwijaya
Email : galatian09@gmail.com

Abstract

The more rapid the development of information technology in web applications, the interference, or the actions of attackers (hackers) are increasing as well. We can see this in print or electronic media, where these media report the actions of hackers to attack existing websites. XSS reflected attack is a type of attack that tries to insert or inject some script code, where the script code here can be stored in an existing database on the website, in this case the script that has been entered is returned to the user's application server. For example, the error message shown will be displayed in other client browsers. Attack pattern of reflected XSS on dataset dataset for Deep learning | Kaggle, will be recognized by several parameters such as sentence, label, ngram1, ngram2 and ngram3. The results of the dataset processing are evaluated for analysis using the Bayesian network method to determine how much accuracy the XSS reflected attack analysis is. From the results of the analysis here, the accuracy value is 99.71%, the precision value is 99.85%, the recall value 99,72 and the f1 – score value is 99.78%.

Keywords : *Analysis of Reflected XSS Attacks On Web Applications With Method On Bayesian Network*

Daftar isi

Daftar Gambar

Daftar Tabel

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dari tahun 2017 – 2021 Open Web Application Security Project (OWASP) Top Ten, menempatkan serangan XSS pada urutan 7 dari 10 serangan yang paling berbahaya terhadap pengguna akun, dan hal ini membuat pengguna merasa sangat terganggu dan bahkan mengalami kerugian material maupun non - material.

XSS (Cross Site Scripting) adalah salah satu jenis serangan keamanan dalam suatu website dengan memanfaatkan celah keamanan pada form input website. XSS terdiri dari 3 kategori yaitu Stored XSS, Reflected XSS dan DOM Based XSS, ketiga jenis xss ini sangat sering mengganggu pada aplikasi yang ada di web[1]. Dalam tugas akhir ini penulis membahas reflected xss sesuai judul yaitu menganalisa serangan reflected xss dalam aplikasi web dengan metode *Bayesian Network*.

Dibawah ini penulis merangkum beberapa penelitian sebelumnya dimana fokus dari peneliti sebelumnya merupakan teknik untuk meniadakan peluang terkena kode SQL dan XSS yaitu:

Pada penelitian ini [2] mereka membuat penelitian dengan memakai metode aplikasi dengan nama program ardilla. Pada program yang dibuat team mereka, bisa di aplikasikan untuk mengujian dalam aplikasi *web - site* dengan mencoba jenis celah keamanan *SQL d*an *XSS*. Dari percobaan yang mereka lakukan, didapat hasil sampai mencapai celah lebih 60 serangan keamanan pada lima *website*. Dan dari kelima website tersebut menghasilkan perbedaan nilai kerentanan. Dari ringkasan tersebut diatas team ini hanya membahas serangan *SQL d*an *XSS* tidak membahas secara khusus reflected.

Selanjutnya, pada penelitian [3] melakukan penelitian dengan menggunakan teknik deteksi dan peniadaan kode sumber secara otomatis dari serangan XSS pada aplikasi web. Teknik ini akan mampu meniadakan kode kerentanan dan juga mendeteksi termasuk meniadakan peluang terkena kode input yang sudah ada sebelumnya dari serangan secara langsung. Dimana dengan cara menscaning

seluruh data di dalam kode pemrograman yang ada akan mendeteksi langsung kode yang memiliki peluang terkena XSS yang akan digantikan oleh fungsi encoding dan escaping oleh OWASP ESAPI. Dari ringkasan tersebut diatas team ini hanya membahas serangan *SQL d*an *XSS* tidak membahas secara khusus reflected.

Pada penelitian lainnya [4], team ini menggunakan teknik deteksi dan penghilangan kode sumber secara otomatis dari serangan XSS pada aplikasi web yang dari awal diterbitkan. Dalam penelitian ini mereka sepakat untuk mengusulkan dengan plug dan eclipse dimana sanggup mengetahui dan meniadakan peluang terkena sumber kode XSS pada program Javascript. Hal ini sangat relevan pada saat kode program yang baru diterbitkan yang selanjutnya ditulis. Dari ringkasan tersebut diatas team ini hanya membahas serangan *SQL d*an *XSS* tidak membahas secara khusus reflected.

Dari hasil ringkasan yang dicapai ketiga penelitian diatas relatif sama,yaitu sama-sama melakukan encoding dan escaping seluruh masukan pemakai dari peluang tersisipnya kode javascript “virus” dari XSS.

Dalam Tugas Akhir ini, fokus penulis adalah menganalisa serangan *reflected XSS* terhadap aplikasi web dengan metode *Bayesian Network (BN)*. BN memiliki kelebihan karena mampu menampilkan probabilitas keterkaitan di antara peristiwa-peristiwa yang saling berhubungan maupun yang tidak saling berhubungan dan bahkan dalam membangun tipe model yang di inginkan dapat dengan cepat dibentuk tanpa membutuhkan waktu lama, juga dapat ditambahkan langsung variable-variable yang dibutuhkan dalam keadaan struktur atapun jaringan dalam proses pembentukan, sehingga metode BN memungkinkan dapat digunakan pada area yang lebih luas. Dan untuk pengolahan data awal disini penulis menggunakan machine learning *Turicreate,* karena Turicreate adalah solusi sumber terbuka yang menyederhanakan pengembangan model pembelajaran mesin. *Turicreate* menyediakan toolkit untuk klasifikasi gambar, deteksi objek, klasifikasi teks dan beberapa lainnya.

1.2 Tujuan

Adapun tujuan dari penelitian dalam tugas akhir ini yaitu:

1. Dapat mengimplementasikan Analisis Serangan *Reflected or Non-Persistent Cross Site Scripting* Attacks pada Aplikasi Web.
2. Menerapkan metode *Bayesian Network (BN)* untuk menganalisa serangan *Reflected or Non-Persistent Cross Site Scripting* Attacks.

1.3 Manfaat

Manfaat yang diharapkan bisa dicapai setelah membaca penelitian tugas akhir ini sebagai berikut :

1. Dapat mempelajari serangan *Reflected or Non – Persistent Cross Site Scripting* Attacks pada aplikasi web.
2. Dapat mencegah terjadinya serangan *Reflected or Non-Persistent Cross Site Scripting* Attacks lebih dini.
3. Dapat menerapakan penggunaan *Bayesian Network (BN)* dalam menganalisa serangan *Reflected or Non-Persistent Cross Site Scripting* Attacks.

1.4 Rumusan dan Batasan Masalah

Dari latar belakang sebelumnya sudah dijelaskan, dan adapun batasan permasalahan dalam skripsi disini bisa disimpulkan yaitu:

1. Pengujian ini tertuju pada serangan *Reflected or Non – Persistent Cross Site Scripting* Attacks pada Aplikasi Web.
2. Analisa yang digunakan dalam penelitian skripsi disini menerapkan *Bayesian Network (BN)* dengan menggunakan program algoritma turicreate untuk mengklasifikasian dataset sebelum di proses di *Bayesian Network*
3. Tidak membahas cara mencegah serangan *Reflected or Non – Persistent Cross Site Scripting* Attacks pada Aplikasi Web.
4. Data penelitian yang dipakai merupakan dataset X*SS data – set for Deep learning | Kaggle*

1.5 Metodologi Penelitian

Metodologi yang diaplikasikan dalam penelitian ini memiliki sejumlah tahapan, yaitu :

1. Tahap Pertama (Studi Pustaka)

   Tahap yang dilaksanakan sesudah masalah yang telah dibahas sesuai dengan kerelevanan penelitian terdahulu berdasarkan buku, paper, artikel, dan jurnak yang memiliki hubungan dengan penelitian yang bernama "Analisa Serangan Reflected Xss Attacks Pada Aplikasi Web Dengan Metode Bayesian Network" ini.

2. Tahap Kedua (Pengolahan Data)

   Tahapan ini merupakan tahapan bagaimana cara mengolah sebuah data mentah menjadi data siap olah, mengkategorikan data dengan menggunakan algoritma *Turicreate*. Lalu menentukan perangkat yang dibutuhkan pada penelitian, baik berupa perangkas keras atau perangkat lunak (hardware ataupun software).

3. Tahap Ketiga (Analisa Serangan Reflected XSS)

   Tahapan ini merupakan tahapan proses analisa serangan reflected XSS dengan menggunakan algortima *Bayesian Network*. Setelah itu diteruskan pada proses validasi dengan menggunakan beberapa parameter percobaan sesuai pada parameter – parameter serangan yang telah ditetapkan oleh batasan masalah.

4. Tahap keempat (Hasil dan Analisa)

   Tahapan ini adalah tahap setelah mendapatkan data hasil dari tahap ketiga, selanjutya yaitu melakukan analisis terhadap hasil yang berhasil diperoleh sebelumnya sampai diperoleh hasil yang objective.

5. Tahap kelima (Kesimpulan dan Saran)

   Tahapan akhir berisi tentang kesimpulan dan saran dari bab-bab sebelumnya mengenai analisis serangan reflected XSS terhadap aplikasi web dengan metode *Bayesian Network*. Bab ini juga berisikan saran yang mungkin dapat digunakan untuk penelitian selanjutnya.

1.6 Sistematika Penulisan

Untuk melancarkan proses penyelesaian tugas akhir dan membahas setiap daftar isi dalam setiap bab, maka dibuatlah sistematika penulisan yaitu:

BAB I. PENDAHULUAN

Bagian ini menjelaskan secara sistematis tentang dasar penelitian seperti latar belakang, rumusan, tujuan, manfaat, batasan masalah, metodologi penelitian, dan sistematika penulisan

BAB II. TINJAUAN PUSTAKA

Bagian ini berisi penjelasan teori yang dipakai sebagai dasar untuk menyelesaikan yang dibahas pada tugas akhir ini. Adapun topik dalam bagian penelitian ini diantaranya pembahasan teori-teori dasar seperti Cross-Site Scripting (XSS), Reflected XSS, Store XSS, DOM Based XSS, Vulnerability, Arsitektur Website dan algoritma *Bayesian Network* (BN), machine learning *Turicreate* yang memiliki hubungan dengan penelitian ini.

BAB III. METODOLOGI PENELITIAN

Bagian ini menjelaskan secara runtut tentang proses penelitian. Dan juga meliputi tahap merancang sistem dan penerapan metode dalam penelitian ini.

BAB IV. PENGUJIAN DAN ANALISIS

Bagian ini berisi penjelasan hasil pengujian yang dilakukan serta analisa data yang didapatkan dari hasil pengujian yang dilakukan.

BAB V. KESIMPULAN DAN SARAN

Bagian ini menjelaskan kesimpulan hasil analisa yang telah dilakukan, serta menjawab semua tujuan yang ingin dicapai seperti yang dijelaskan pada BAB ini.

Daftar Pustaka

[1] S. Fogie, J. Grossman, H. Robert, A. Rager, and P. Petkov, “Cross Site Scripting Exploits and Defense,” 2007, doi: https://doi.org/10.1016/B978-1-59749-154-9.X5000-8.

[2] A. Kiezun, P. J. Guo, K. Jayaraman, and M. D. Ernst, “Automatic creation of SQL injection and cross-site scripting attacks,” *Proc. - Int. Conf. Softw. Eng.*, no. May, pp. 199–209, 2009, doi: 10.1109/ICSE.2009.5070521.

[3] L. K. Shar and H. B. K. Tan, “Defending against cross-site scripting attacks,” *Computer (Long. Beach. Calif).*, vol. 45, no. 3, pp. 55–62, 2012, doi: 10.1109/MC.2011.261.

[4] P. Bathia, B. Beerelli, Laverdière, and Marc-André, “Assisting Programmers Resolving Vulnerabilities in Java Web Applications,” *Assist. Program. Resolv. Vulnerabilities Java Web Appl.*, vol. Communicat, pp. 133:268-279, 2011, doi: 10.1007/978-3-642-17881-8_26.

[5] M. Mushlih, R. Fitri, and I. Wardiah, “Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web,” *Semin. Nas. Ris. ...*, vol. 5662, no. November, pp. 41–47, 2019, [Online]. Available: http://e-prosiding.poliban.ac.id/index.php/snrt/article/view/409.

[6] R. Barnett, “Ryan Barnett - Background,” *XSS Str. Fight*, 2011.

[7] Y. Zhou and P. Wang, “An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence,” *Comput. Secur.*, vol. 82, pp. 261–269, 2019, doi: 10.1016/j.cose.2018.12.016.

[8] A. Avancini and M. Ceccato, “Security testing of web applications: A search-based approach for cross-site scripting vulnerabilities,” *Proc. - 11th IEEE Int. Work. Conf. Source Code Anal. Manip. SCAM 2011*, no. May 2014, pp. 85–94, 2011, doi: 10.1109/SCAM.2011.7.

[9] E. Athanasopoulos, A. Krithinakis, and E. P. Markatos, “Hunting Cross-Site Scripting Attacks in the Network,” *W2SP 2010 Web 2.0 Secur. Priv. Work.*, 2010, [Online]. Available: http://w2spconf.com/2010/papers/p12.pdf.

[10] Tinaliah, “Aplikasi Sistem Pakar Untuk Diagnosa Penyakit Hewan Ternak Sapi Dengan Bayesian Network,” vol. 5, 2015.

[11] A. Ouali, A. R. Cherif, and M.-O. Krebs, “Data mining based Bayesian networks for best classification,” *Data Min. based Bayesian networks best Classif.*, 2006, doi: https://doi.org/10.1016/j.csda.2005.09.012.

[12] W. Suharso and A. Djunaidy, “Analisis Customer Churn Menggunakan Bayesian Belief Network (Studi Kasus: Perusahaan Layanan Internet),” *Anal. Cust. Churn Menggunakan Bayesian Belief Netw. (Studi Kasus Perusah. Layanan Internet)*, vol. 4, no. 5, pp. 323–335, 2013, doi: 10.24089/j.sisfo.2013.09.003.

[13] G. F. Cooper and E. Herskovits, “A Bayesian Method for the Induction of Probabilistic Networks from Data,” *Mach. Learn.*, vol. 9, no. 4, pp. 309–347, 1992, doi: 10.1023/A:1022649401552.

[14] J. Cheng and R. Greiner, “Comparing Bayesian Network Classifiers,” pp. 101–108, 2013, [Online]. Available: http://arxiv.org/abs/1301.6684.