VISUALISASI CYBERMAP SERANGAN CROSS SITE SCRIPTING (XSS) SECARA REALTIME DEMI MENJAGA KEDAULATAN DATA INDONESIA

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

ADITIYA GUNANTA

09011181520001

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2020

LEMBAR PENGESAHAN

VISUALISASI CYBERMAP SERANGAN CROSS SITE SCRIPTING (XSS) SECARA REALTIME DEMI MENJAGA KEDAULATAN DATA INDONESIA

PROPOSAL TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
Oleh :

Aditiya Gunanta

09011181520001

Indralaya, Desember 2020
Mengetahui,

Pembimbing Tugas Akhir I	Pembimbing Tugas Akhir II
Deris Stiawan, M.T., Ph.D.	**Ahmad Heryanto,S.Kom., M.T**
NIP 197806172006041002	**NIP.197806172006041002**

Ketua Jurusan Sistem Komputer

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

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan tugas akhir dengan judul "Pengembangan Robot Hexapod Untuk Menginpeksi Objek Kebocoran Gas". Pada penyusunan laporan tugas akhir ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT dan terima kasih kepada yang terhormat :

1. Orang tuaku, Bapak Yuniar Bayazit dan Ibu Evriyanti yang telah memberikan do'a dan dukungannya serta memberikan motivasi untuk tetap selalu berusaha dan Tawakal
2. Adikku, Minanti Tiyan Saputri yang sudah membantu memberikan support dan semangat selama proses pembuatan tugas akhir ini.
3. Bapak Jaidan Jauhari, S.Pd., M.T., Selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. Selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph.D.Selaku Pembimbing 1 Tugas Akhir Di Jurusan Sistem Komputer
6. Bapak Ahmad Heryanto,S.Kom., M.T Selaku Pembimbing 2 Tugas Akhir Di Jurusan Sistem Komputer.
7. Bapak Ahmad Fali Oklilas, S.T., M.T. Selaku Pembimbing Akademik Di Jurusan Sistem Komputer
8. Seluruh Dosen Jurusan Sistem Komputer Fasilkom Universitas Swijaya
9. Seluruh teman-teman angkatan 2015 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
10. Kepada orang spesial Qonita Amyra Nisrina yang sudah mensupport dalam segala hal baik materi,fisik dan logis serta turut andil yang cukup besar dalam pembuatan tugas akhir ini.
11. Seluruh Teman-teman Pemondokan Kelapa Gading yang telah memberikan support dan semangat

12. Kepada Geng UCUN Iko,Sari,Tomcun yang sudah mensupport dan menemani proses pembuatan tugas akhir ini

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari kesempurnaan, oleh karena itu kritik dan saran yang membangun sangat penulis harapkan sebagai bahan acuan dan perbaikan untuk penulis dalam menyempurnakan laporan ini.

Semoga laporan tugas akhir ini bisa bermanfaat bagi pembaca ataupun bagi penulis sendiri. Demikian yang bisa penulis sampaikan.

Wassalamu'alaikum Wr.Wb

Palembang, Desember 2020

Aditiya Gunanta

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Aditiya Gunanta
NIM	: 09011181520001
Jurusan	: Sistem Komputer
Judul	: VISUALISASI CYBERMAP SERANGAN CROSS SITE SCRIPTING (XSS) SECARA REALTIME DEMI MENJAGA KEDAULATAN DATA INDONESIA

Hasil Pengecekan Software iThenticate/Turnitin: 9 %

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 sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Indralaya, Desember 2020

Material 6000

Aditiya Gunanta

NIM. 09011181520001

VISUALISASI CYBERMAP SERANGAN CROSS SITE SCRIPTING (XSS) SECARA REALTIME DEMI MENJAGA KEDAULATAN DATA INDONESIA

Aditiya Gunanta, Deris Stiawan, Ph. D. , Ahmad Heryanto, S.kom, .M. T

Abstrac

Kejahatan *Cyber Crime* merupakan Tindakan yang dapat mengancam keaman siapa saja, dan dapat mengakibatkan kerugian yang cukup besar jika terjadi pada sebuah kelompok ataupun industri berskala besar, salah satu jenis kejahatan tersebut iyalah *Cross Site Scripting (XSS).* Pada penelitian ini akan dilakukan deteksi dari serangan tersebut dan juga melakukan visualisasi serangan yang telah di deteksi, proses visualisasi sendiri berdasarkan GEO-IP dengan tujuan mengetahui darimana asal daripada serangan yang telah di tangkap dan dideteksi.

Keyword : Cyber Crime, Cross Site Scripting, XSS, GEO-IP, Log Management

LEMBAR PENGESAHAN

VISUALISASI CYBERMAP SERANGAN CROSS SITE SCRIPTING (XSS) SECARA REALTIME DEMI MENJAGA KEDAULATAN DATA INDONESIA

PROPOSAL TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
Oleh :

Aditiya Gunanta

09011181520001

Indralaya, Desember 2020

Mengetahui,

Pembimbing Tugas Akhir I	Pembimbing Tugas Akhir II
Deris Stiawan, M.T., Ph.D.	Ahmad Heryanto,S.Kom., M.T
NIP 197806172006041002	NIP.197806172006041002

Ketua Jurusan Sistem Komputer

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

DAFTAR ISI

Daftar Gambar

DAFTAR TABEL

BAB I

Pendahuluan

1.1 Latar belakang

Cyber-Security adalah bagian penting dalam semua jenis *Cyber-Physical System* (CPS). Dalam mengecaluasi resiko CPS, penetapan model hirarki kuantitatif berdasarkan seberapa tinggi tingkat serangan yang mengancam, tingkat keberhasilan dari seragan serta konsekuensi serangan yang teradi, dapat diperkirakan resiko yang disebabkan oleh serangan yang sedang berlangsung di tingkat host maupun tingkat system. [1] Seiring berjalan nya waktu, pertukaran informasi tentang ancaman dan kelemahan baru telah menjadi dasar *Cyber-Defense* yang efektif dalam beberapa tahun terakhir. [2]

Perkembangan *Cyber-Security* Disebabkan oleh semakin tinggi nya tingkat ancaman serta semakin beragam jenis serangan yang dapat di lakukan pada tingkat host dan juga tingkat system, adapun salah satu jenis serangan yang akan penulis angkat pada penelitian kali ini ialah perobaan serangan *Cross Site Scripting* (XSS) pada server *Science and Technology Index* (SINTA) ristekdikti, Berdasarkan website resmi dari ristekdikti, SINTA merupakan sebuah portal yang di gunakan untuk melakukan pengukuran kinerja ilmu pengetahuan dan teknologi yang meliputi beberapa aspek antara lain kinerja peneliti, penulis, kinerja jurnal, dan kinerja institusi Iptek. Pada kasus kali ini, penulis melakukan ekstraksi file log server pada server SINTA untuk mendeteksi adanya percobaan serangan XSS pada server tersebut, XSS merupakan salah satu ancaman pada keamanan computer yang memungkinkan penyerang mendapatkan akses atas informasi sensitif ketika JavaScript,ActiveX,FLASH atau HTML dari tautan XSS di eksekusi oleh korban. [3] Setelah melakukan ekstraksi dan deteksi dari data log tersebut penulis akan melakukan Analisa trafik data hasil dari serangan yang terjadi, Analisa trafik merupakan prosedur rutin, tetapi tidak hanya satu serangan yang teridentifikasi, tetapi juga langkah-langkah untuk membentuk ulang gambaran kejadian yang terjadi. [4]

Setelah mendapat kan hasil dari data log di atas, maka langkah berikut nya ada lah memvisual kan data tersebut. Visualisasi yang di lakukan berdasarkan

Geo-IP. Pada penelitian sebelum nya pendekatan analitik visual dimaksud kan untuk mendeteksi kejanggalan ini namun hanya sedikit referensi *integrated geographical* yang tersedia. Data Geo-IP sebagian besar digunakan untuk table pencarian namun data ini kurang di minati dan kurang di apresiasi. [5]

1.2 Tujuan Penelitian

Adapun tujuan penelitian ini yaitu :

1. Mengektraksi data log server dari SINTA
2. Mendeteksi ada nya serangan XSS pada data log server SINTA
3. Membuat visualisasi dari serangan XSS pada data log server SINTA

1.3 Manfaat penelitian

Adapun mafaat penelitian ini yaitu :

1. Dapat mendeteksi adanya serangan XSS pada server SINTA
2. Dapat menampilkan secara visual serangan XSS yang dilakukan

1.4 Rumusan Masalah

Adapun permasalahan yang dibahas yaitu :

1. Bagaimana mengektraksi data log menjadi format CSV
2. Bagaimana mendeteksi serangan dari hasil eksstraksi data
3. Bagaimana memvisualkan serangan yang terjadi

1.5 Batasan Masalah

Adapun Batasan masalah yang dibahas yaitu :

1. Serangan yang akan di deteksi yaitu *Cross-Site Scripting* (XSS)
2. Pada tugas akhir ini dataset yang digunakan adalah dataset SINTA
3. Visualisasi akan di lakukan secara realtime

1.6 Sistematika Penulisan

Adapun sistematika penulisan pada tugas akhir ini iyalah sebagai berikut :

1. **BAB I Pendahuluan**

Pada BAB I akan berisikan latar belakang masalah, tujuan dan manfaat serta metodelogi penelitian dan sitematika penulisan.

2. **BAB II Tinjauan Pustaka**

Pada BAB II ini akan berisikan dasar teori dari *Cross-Site Scripting* (XSS),data log management, dan visualisasi data.

3. **BAB III Analisis dan Pengumpulan Data**

Pada BAB III akan membahas analisis data berupa ekstraksi data dari log server SINTA dan pengumpulan data hasil deteksi serangan XSS pada dataset SINTA

4. **BAB IV Hasil dan Analisis sementara**

Pada BAB IV akan berisi hasil dari pengumpulan data serangan XSS dan Analisa dari hasil deteksi serangan tersebut.

5. **BAB V Kesimpulan Sementara dan Saran**

Pada BAB V berisi kan kesimpulan dari bab-bab sebelum nya yang telah dibahas pada halaman sebelum nya dan juga akan berisikan saran yang kiranya akan berguna di penelitian berikut nya

DAFTAR PUSTAKA

[1] W. Wu, R. Kang, and Z. Li, “Risk assessment method for cyber security of cyber physical systems,” *Proc. 2015 1st Int. Conf. Reliab. Syst. Eng. ICRSE 2015*, pp. 0–4, 2015, doi: 10.1109/ICRSE.2015.7366430.

[2] F. Skopik and S. Filip, “Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators,” *2019 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2019*, pp. 1–8, 2019, doi: 10.1109/CyberSecPODS.2019.8885134.

[3] M. Dayal, N. Singh, and R. S. Raw, “A comprehensive inspection of cross site scripting attack,” *Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2016*, pp. 497–502, 2017, doi: 10.1109/CCAA.2016.7813770.

[4] I. Kotenko, M. Kolomeets, A. Chechulin, and Y. Chevalier, “A visual analytics approach for the cyber forensics based on different views of the network traffic,” *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol. 9, no. 2, pp. 57–73, 2018.

[5] A. Ulmer, M. Schufrin, D. Sessler, and J. Kohlhammer, “Visual-Interactive Identification of Anomalous IP-Block Behavior Using Geo-IP Data,” *2018 IEEE Symp. Vis. Cyber Secur. VizSec 2018*, 2019, doi: 10.1109/VIZSEC.2018.8709182.

[6] K. Pranathi, S. Kranthi, A. Srisaila, and P. Madhavilatha, “Attacks on Web Application Caused by Cross Site Scripting,” *Proc. 2nd Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2018*, no. Iceca, pp. 1754–1759, 2018, doi: 10.1109/ICECA.2018.8474765.

[7] P. Panggabean, “Analisis Network Security Snort Metode Intrusion Detection System Untuk Optimasi Keamanan Jaringan Komputer,” *Jursima*, vol. 6, no. 1, p. 1, 2018, doi: 10.47024/js.v6i1.107.

[8] A. S. Ashoor and S. Gore, “Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS),” *Commun. Comput. Inf. Sci.*, vol. 196 CCIS, pp. 497–501, 2011, doi: 10.1007/978-3-642-22540-6_48.

[9] S. Niccolini, R. G. Garroppo, S. Giordano, G. Risi, and S. Ventura, “SIP intrusion detection and prevention: Recommendations and prototype implementation,” *1st IEEE Work. VoIP Manag. Secur. VoIP MaSe 2006*, pp. 45–50, 2006, doi: 10.1109/voipms.2006.1638122.

[10] J. Gómez, C. Gil, N. Padilla, R. Baños, and C. Jiménez, “Design of a Snort-Based Hybrid Intrusion,” *Proc. 10th Int. Work. Artif. Neural Networks*, pp. 515–522, 2009.