

Pengembangan Aplikasi Scanning Defacement Judi Online untuk Website Profile pada Server

Missi Hikmatyar¹, Aso Sudiarjo², Ruuhwan³, Mizar Ismu Arief⁴, Nizar Fadilah⁵

^{1,2,3,4,5}Teknik Informatika, Fakultas Teknik Universitas Perjuangan Tasikmalaya, Jl.PETA No. 177 Kota Tasikmalaya, 46115, Indonesia
e-mail: missi@unper.ac.id¹, asosudiarjo@unper.ac.id², ruuhwan@unper.ac.id³, 2103010101@unper.ac.id⁴, 2103010093@unper.ac.id⁵

INFORMASI ARTIKEL

Sejarah Artikel:

Diterima Redaksi : 31 Oktober 2024

Revisi Akhir : 05 November 2024

Diterbitkan Online : 30 November 2024

Kata Kunci:

Defacement, Server, Web Profile, Slot, Perguruan Tinggi

Korespondensi :

Telepon / Hp : +62 822-2526-3325

E-mail : missi@unper.ac.id

A B S T R A K

Web Profile Perguruan Tinggi menghadapi masalah, di mana hasil pencarian dengan kata kunci tertentu menampilkan konten terkait judi online yang berasal dari website yang telah disusupi. Kondisi ini menunjukkan adanya celah keamanan yang dimanfaatkan oleh pihak tidak bertanggung jawab untuk menyusupi dan memodifikasi konten website. Keamanan situs web menjadi aspek krusial dalam menjaga integritas informasi dan reputasi penyedia layanan digital. Salah satu ancaman umum adalah defacement, yaitu modifikasi ilegal terhadap konten atau tampilan situs web oleh pihak tak berwenang. Defacement adalah bentuk serangan siber yang melibatkan perubahan tampilan atau konten situs web, yang dapat merusak reputasi dan kepercayaan pengguna terhadap situs tersebut. Penelitian ini bertujuan untuk mengembangkan aplikasi pemindai defacement otomatis yang berfungsi pada situs web profil yang di-hosting pada server. Aplikasi ini dirancang untuk memindai perubahan yang mencurigakan pada halaman web dan memberikan notifikasi kepada administrator apabila terdeteksi adanya modifikasi yang tidak sah. Aplikasi ini memanfaatkan algoritma pencocokan pola dan hashing untuk mendeteksi perubahan tak terduga pada konten situs web. Metode yang digunakan mencakup pemantauan berkala terhadap halaman web dan perbandingan integritas data untuk mendeteksi perubahan yang tidak sah secara cepat dan efisien. Hasil pengujian menunjukkan bahwa aplikasi ini mampu mendeteksi defacement dengan akurasi tinggi dan memberikan notifikasi real-time kepada administrator, sehingga dapat dilakukan tindakan segera untuk mengatasi kerusakan. Aplikasi ini diharapkan dapat menjadi solusi efektif dalam memperkuat keamanan situs web profil serta mengurangi dampak negatif dari serangan defacement terhadap server.

1. PENDAHULUAN

Kemajuan teknologi informasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk di dunia pendidikan. Institusi pendidikan, seperti Universitas Perjuangan Tasikmalaya, sangat bergantung pada website mereka sebagai media utama untuk menyampaikan informasi kepada mahasiswa, staf, dan masyarakat umum. Website ini digunakan untuk berbagai tujuan, mulai dari informasi akademik, administrasi, hingga promosi kegiatan kampus. Oleh karena itu, keamanan website menjadi aspek yang sangat krusial. Namun, seiring dengan perkembangan teknologi, ancaman terhadap keamanan website juga semakin meningkat. Salah satu ancaman yang sering dihadapi adalah web defacement. Dalam kasus defacement slot, hacker memodifikasi tampilan atau menyisipkan halaman baru di website yang telah diretas, dengan tujuan mengalihkan pengguna ke situs judi online atau membuat backlink yang akan terindeks oleh mesin pencari seperti Google [1]. Hal ini tidak hanya merusak reputasi institusi tetapi juga melanggar hukum dan etika, mengingat judi online dilarang di banyak negara termasuk Indonesia [2].

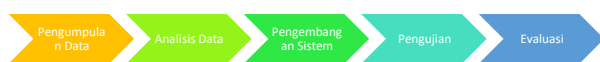
Universitas Perjuangan Tasikmalaya menghadapi masalah serupa, di mana hasil pencarian dengan kata kunci tertentu menampilkan konten terkait judi online

yang berasal dari website Universitas Perjuangan Tasikmalaya yang telah disusupi. Kondisi ini menunjukkan adanya celah keamanan yang dimanfaatkan oleh pihak tidak bertanggung jawab untuk menyusupi dan memodifikasi konten website [3]. Menyikapi masalah ini, dibutuhkan sebuah sistem keamanan web yang efektif mendeteksi untuk mencegah terjadinya defacement slot. Sistem ini harus mampu melakukan scanning terhadap file dan folder di server untuk mengidentifikasi infeksi terhadap perubahan yang mencurigakan. Selain itu, sistem harus memiliki mekanisme pencegahan yang dapat meminimalkan risiko serangan serupa di masa mendatang. Penelitian yang akan dilakukan adalah membangun sebuah sistem keamanan web yang dirancang khusus mendeteksi untuk mencegah defacement slot pada website Universitas Perjuangan Tasikmalaya. Jurnal Informatics and Digital Expert (INDEX) merupakan jurnal yang diterbitkan oleh Jurusan Informatika Fakultas Teknik Universitas Perjuangan, Tasikmalaya. INDEX memuat naskah hasil-hasil penelitian di bidang Informatika dan Teknologi Informasi. Penelitian yang akan dilakukan adalah membangun aplikasi anti slot untuk mendeteksi ransomware pada website menggunakan metode pengembangan Scrum [4]

Pengembangan *defacement detection* dilakukan [5] dengan melakukan pendeteksian pola serangan dari 40.000 serangan termasuk pada pola teks. Ada kebutuhan akan pendekatan yang bermanfaat untuk mengamankan situs web di internet. Web akan menjadi lebih mudah dipahami ketika kita mempelajari bagaimana membangun mekanisme keamanan [6]. Pertumbuhan layanan berbasis web akan memaksa kita untuk lebih berhati-hati dan membangun infrastruktur web yang sangat aman, bergantung pada server web yang aman. Salah satu serangan paling kritis yang melibatkan internet adalah perusakan situs web [7]. meninjau teknik pendeteksian perusakan situs web dan alat pendeteksi perusakan serta menentukan implementasi masing-masing studi [8], teknik pembelajaran berbasis mesin, dan alat lain yang digunakan dalam bidang ini. Teknik deteksi perusakan dapat dikategorikan ke dalam tiga kategori: deteksi berbasis anomali, deteksi berbasis tanda tangan, dan teknik pembelajaran mesin. Kami meninjau deteksi perusakan berdasarkan algoritma pembelajaran mesin dan mendiskusikan teknik yang disebutkan secara rinci dalam setiap studi penelitian. menyoroti bahwa model deteksi perusakan berdasarkan kombinasi teknik machine learning dan tanda serangan [9] adalah yang terbaik karena tingkat akurasi sangat baik. *Web Defacement* adalah serangan dengan tujuan utama merubah tampilan sebuah *website* baik halaman utama maupun halaman lain terkait dengannya diistilahkan sebagai *Web Defacement*. Hal ini biasa dilakukan oleh para *attacker* atau penyerang karena berbagai hal dan memungkinkan untuk diserang sehingga website yang terkait dengannya menjadi sasaran. *Web defacement* belakangan ini marak terjadi pada situs milik pemerintah dan pendidikan, terutama *web defacement judi online*. Dampak nyata dari *web defacement judi online* yaitu situs menampilkan halaman judi *online*. Hal ini tidak hanya merusak reputasi institusi tetapi juga melanggar hukum dan etika, mengingat judi *online* dilarang di banyak negara termasuk Indonesia.

2. METODE

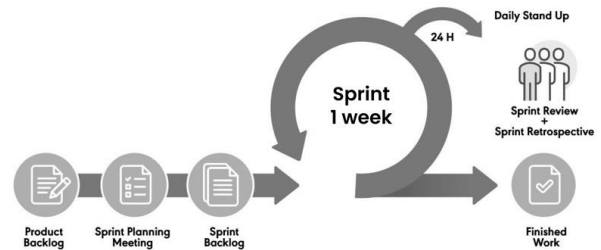
pada proses pengembangan aplikasi terdapat beberapa Langkah yang akan dilakukan, berikut gambar 2 merupakan metodologi penelitian.



Gambar 1. Metodologi Penelitian

Lokasi Penelitian dilakukan di Universitas Perjuangan Tasikmalaya, atau pada situs web *unper.ac.id*. Tahap awal adalah melakukan pengumpulan data malicious dan kata kunci terkait dengan judi. Pengumpulan data dilakukan dengan studi literatur dengan mengumpulkan kata kunci yang dibutuhkan. Setelah itu melakukan analisis data dengan melakukan klasifikasi antara kata dengan kelasnya, penentuan kelas diberikan berdasarkan pada dampak

serangan [10]. Setelah data yang dibutuhkan didapatkan, kemudian melakukan pengembangan sistem dengan metode *scrum*. Tahap ini adalah melakukan pembuatan aplikasi untuk mendeteksi kata kata yang sudah dikumpulkan ditahap sebelumnya.



Gambar 2. Alur Pengembangan Metode Scrum

Setelah aplikasi selesai kemudian melakukan pengujian dengan menerapkannya di server kemudian dilakukan evaluasi.

Pengembangan aplikasi *antislot* pada deteksi *defacement* menggunakan metode *Scrum* (4), berikut gambar 3 merupakan Gambaran metode scrum.

Pada tahap awal pengembangan dengan metode *scrum* dilakukan pembuatan *product backlog*. *Product backlog* adalah daftar segala perintah atau kegiatan yang mungkin diperlukan dalam produk dan merupakan sumber tunggal persyaratan untuk setiap perubahan harus dibuat dalam pengembangan produk (4). *Product backlog* berisi daftar semua fitur, fungsi, kebutuhan, penyempurnaan, dan perbaikan yang merupakan perubahan yang akan dilakukan untuk produk dalam rilis mendatang.

Pada penelitian ini fitur *product backlog* dibuat dan disusun oleh *product owner*.

1. *Sprint Planning*

Sprint Planning dibuat untuk merencanakan kolaborasi pekerjaan yang dapat dilakukan oleh tim *scrum*. Pada *sprint planning* membahas tentang hal yang akan dilakukan untuk meningkatkan hasil yang diperoleh dari *sprint* tersebut [4]. Pada *sprint planning* keluaran yang dihasilkan adalah berupa *sprint backlog*. *Sprint backlog* ini berisi target modul-modul aplikasi yang harus diselesaikan pada setiap *sprint*. Isi *sprint backlog* merupakan bagian dari *product backlog*.

2. *Daily Scrum*

Tahap ini merupakan praktik untuk memantau kinerja dan mensinkronisasi pekerjaan. Setiap hari perlu diadakan standup meeting untuk melaporkan hal yang telah setiap anggota tim kerjakan.

3. *Sprint Review*

Sprint review diadakan di akhir *sprint* untuk meninjau keperluan untuk merubah atau menambahkan *product backlog*. Pada pertemuan ini tim *scrum* dan *stakeholder* yang terlibat berkolaborasi untuk membahas hal-hal yang telah selesai dilakukan pada saat *sprint* [4].

4. *Sprint Restrospective*

Tahapan ini dilakukan oleh seluruh tim *scrum* untuk meninjau kegiatan *sprint* yang telah selesai dilaksanakan agar dapat meningkatkan kinerjanya pada *sprint* selanjutnya [4].

3. HASIL

Analisis sistem dapat di definisikan sebagai suatu penguraian dari suatu sistem informasi yang utuh ke dalam bagian-bagian komponennya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan-permasalahan, kesempatan-kesempatan, hambatan-hambatan yang terjadi dan kebutuhan-kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikan terhadap sistem yang sedang berjalan tersebut. Gambar 3 merupakan model aplikasi *defacement slot* yang akan dikembangkan.

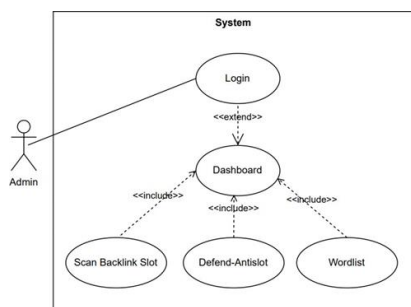


Gambar 3. Model Bisnis Aplikasi

3.1. Perancangan Sistem

1. Use Case Diagram

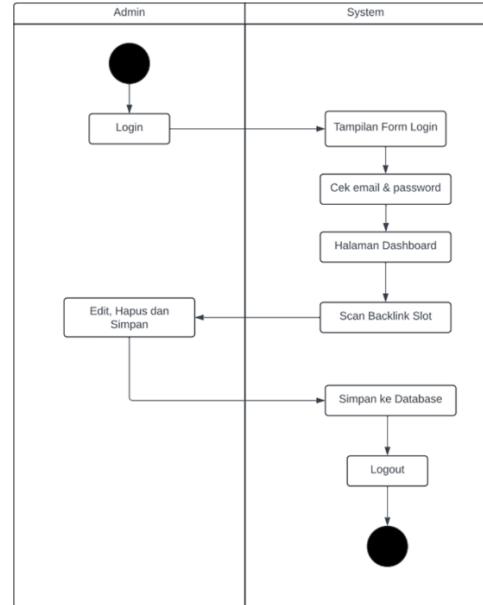
Use Case Diagram ini menjelaskan mengenai pengelolaan dan akses *website* secara keseluruhan. Adapun *Use Case Diagram* dari Rancang Bangun Aplikasi *Scanning* untuk Pencegahan *Defacement Slot* Berbasis *Website* ditunjukkan pada gambar 4.



Gambar 4. Use Case Diagram

2. Activity Diagram

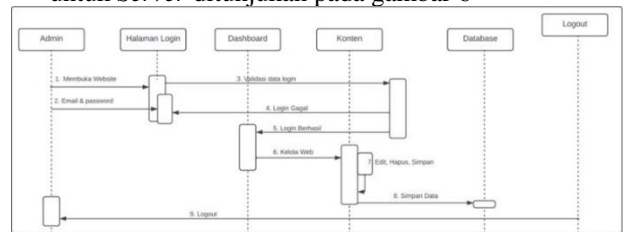
Adapun *Activity Diagram* Rancang Bangun Aplikasi *Scanning* untuk Pencegahan *Defacement Slot* Berbasis *Website* untuk *Server* ditunjukkan pada gambar 5.



Gambar 5. Activity Diagram

3. Sequence Diagram

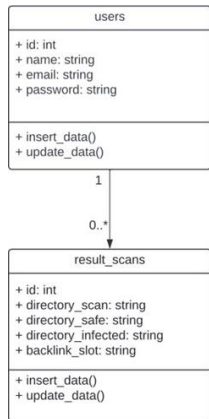
Sequence Diagram adalah suatu diagram yang menggambarkan interaksi antar objek dan mengindikasikan komunikasi diantara objek-objek tersebut. Berikut digambarkan *sequence diagram* dari Rancang Bangun Aplikasi *Scanning* untuk Pencegahan *Defacement Slot* Berbasis *Website* untuk *Server* ditunjukkan pada gambar 6



Gambar 6. Sequence Diagram

4. Class Diagram

Class Diagram adalah yang digunakan untuk menampilkan beberapa kelas yang ada dalam sistem perangkat lunak yang akan dikembangkan. *Class Diagram* menunjukkan hubungan antar kelas dalam sistem yang sedang dibangun dan bagaimana mereka saling berkolaborasi untuk mencapai satu tujuan. Gambar 7 merupakan *class diagram*.



Gambar 7. Class Diagram

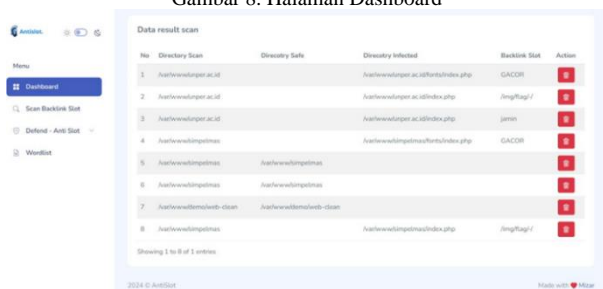
3.2. Implementasi Sistem

Tahap implementasi sistem merupakan proses perubahan sistem yang telah dirancang pada sebelumnya menjadi sistem yang dapat dijalankan. Aplikasi Scanning untuk Pencegahan Defacement Slot berbasis Website ini memerlukan perangkat lunak (software) dan perangkat keras (hardware) dalam pembuatannya agar sistem dapat berjalan sesuai dengan yang diharapkan.

Untuk dapat menjalankan Aplikasi Scanning untuk Pencegahan Defacement Slot berbasis Website ini dapat langsung dijalankan di semua browser yang tersedia di Komputer ataupun Laptop. Sesuai dengan perancangan sistem yang telah dikemukakan sebelumnya pada pembuatan Aplikasi Scanning untuk Pencegahan Defacement Slot berbasis Website ini terdapat satu tingkat yaitu Administrator. Gambar 8 dan 9 merupakan tampilan dashboard



Gambar 8. Halaman Dashboard



Gambar 9. Halaman Hasil Scan

3.3. Pengujian

Pengujian dilakukan dengan melakukan pengumpulan data berupa kata kunci yang sering keluar pada web profile. Data yang dikumpulkan, diperoleh dari beberapa web profile yang terkena defacement. Kata kunci yang digunakan adalah kata kunci yang mengandung unsur promosi judi online seperti slot, depo, maxwin dan lain-lain. Tabel 1 merupakan wordlist kata kunci yang sering muncul

Tabel 1. Wordlist

No	Word	No	Word
1	depo 5k	21	raja168
2	deposit	22	raja288 link
3	dijamin cuan	23	resmi
4	GACOR	24	rp 10.000,00
5	gacor link	25	scater
6	GAMPANG MENANG	26	sgacor/
7	gas4d	27	tergacor
8	hoki	28	terpercaya
9	img/sgacor/	29	zona66
10	jackpot	30	slot online gacor
11	jamin	31	img/sgacor/
12	JOS168	32	bocoran-slot-terbaru
13	makin-gacor/	33	Slot bet 200
14	max win	34	b200/
15	maxwin	35	Slot Mahjong
16	menang mudah	36	sgacor
17	nomorslot	37	smahjong
18	pasaran	38	Link Slot Demo Platform Pragmatic Play
19	paste.ee	39	5Unsur Slot
20	poker99	dst

Kata kunci yang dikumpulkan kemudian dilakukan proses klasifikasi pada kata-kata yang sering keluar. Semakin sering keluar maka status kata tersebut termasuk kategori High. Klasifikasi terdiri dari tiga kategori yaitu High, Middle dan Low tergantung pada sering dan tidaknya kata kunci tersebut keluar. Gambar 10 merupakan hasil scanning pada website yang terinfeksi defacement.



Gambar 10. Hasil Pengujian Scanning

4. KESIMPULAN

Pengembangan sistem keamanan web yang mampu mendeteksi keberadaan Defacement Slot pada Website Perguruan Tinggi menghasilkan Aplikasi Scanning untuk Pencegahan Defacement Slot yang telah dirancang dan dibangun menggunakan Framework Laravel & MySQL berhasil mendeteksi keberadaan defacement slot pada website Perguruan Tinggi. Merancang dan Mengimplementasikan langkah-langkah pencegahan untuk mengurangi risiko terjadinya

serangan *defacement slot* di masa mendatang, Implementasi langkah-langkah ini memastikan bahwa *website* Perguruan Tinggi tetap aman dan terlindungi dari ancaman *defacement* secara berkelanjutan.

DAFTAR PUSTAKA

- [1] Hariyadi D. Analisis Serangan Web Defacement pada Situs Web Pemerintah Menggunakan ELK Stack | Hariyadi | JISKA (Jurnal Informatika Sunan Kalijaga). JISKA Res Cent [Internet]. 2019;4(1):1–8. Available from: <http://202.0.92.5/saintek/JISKA/article/view/1439>
- [2] Aji BB. Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website. *Cyber Secur dan Forensik Digit*. 2023;6(1):25–9.
- [3] Nguyen TH, Dau Hoang X, Nguyen DD. Detecting Website Defacement Attacks using Web-page Text and Image Features. *Int J Adv Comput Sci Appl*. 2021;12(7):215–22.
- [4] Hron M, Obwegeser N. Why and how is Scrum being adapted in practice: A systematic review. *J Syst Softw*. 2022;183(September 2020).
- [5] Banerjee S, Swearingen T, Shillair R, Bauer JM, Holt T, Ross A. Using Machine Learning to Examine Cyberattack Motivations on Web Defacement Data. *Soc Sci Comput Rev*. 2022;40(4):914–32.
- [6] Albalawi M, Aloufi R, Alamrani N, Albalawi N, Aljaedi A, Alharbi AR. Website Defacement Detection and Monitoring Methods: A Review. *Electron*. 2022;11(21).
- [7] Ghaleb FA, Alsaedi M, Saeed F, Ahmad J, Alasli M. Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning. *Sensors*. 2022;22(9):1–19.
- [8] Desmon J, Hidayatulloh S, Jumaryadi Y. Systematic Literature Review: Serangan Deface Website Sebagai Bentuk Kejahatan Siber. *Just IT J Sist Informasi, Teknol Inf dan Komput* [Internet]. 2024;14(2):80–149. Available from: <https://jurnal.umj.ac.id/index.php/just-it/index>
- [9] Xuan C Do, Nguyen HD, Nikolaevich TV. Malicious URL detection based on machine learning. *Int J Adv Comput Sci Appl*. 2020;11(1):148–53.