In Search

e-ISSN: 2580-3239
p-ISSN: 2085-7993
Volume 24 No. 1 Juli 2025

Analisis Keamanan Situs ".go.id" Terhadap Serangan Web Defacement "Judi Online"

Pinaya Agustin, Ahmad Wahyu
Informatika, Fakultas Teknologi dan Informatika, Universitas Informatika dan Bisnis Indonesia
Email: agustinpinaya09@gmail.com; a.wahyu7789@gmail.com.

Abstrak

Era digitalisasi membawa teknologi menjadi bagian penting dalam pelayanan pemerintah kepada masyarakat. Namun, situs pemerintah dengan domain ".go.id" rentan terhadap serangan *web defacement*, khususnya yang menyisipkan konten perjudian *online*. Penelitian ini bertujuan menganalisis kerentanan keamanan pada situs pemerintah, metode serangan yang digunakan, dan solusi yang dapat diterapkan. Dengan pendekatan deskriptif berbasis kajian literatur, penelitian ini mengidentifikasi serangan seperti *SQL injection*, *Cross-Site Scripting (XSS)*, dan *file upload vulnerability* sebagai metode utama eksploitasi. Hasil penelitian menunjukkan lemahnya pengelolaan keamanan sistem menjadi penyebab utama serangan. Rekomendasi yang diberikan meliputi pengujian penetrasi, penilaian kerentanan, dan implementasi panduan *OWASP* untuk meningkatkan keamanan situs. Pendekatan ini diharapkan mampu mengurangi risiko serangan *web defacement* di masa mendatang.

Kata Kunci: *Web defacement*, keamanan situs, domain ".go.id", serangan cyber, *SQL infection*.

Abstract

The digital era has integrated technology into government services for the public. However, government situss with the ".go.id" domain are vulnerable to web defacement attacks, particularly those embedding online gambling content. This study aims to analyze security vulnerabilities in government situss, the attack methods used, and potential solutions. Using a descriptive approach based on literature review, the research identifies SQL injection, Cross-Site Scripting (XSS), and file upload vulnerabilities as primary exploitation methods. The findings reveal that poor security management is the main cause of attacks. Recommendations include penetration testing, vulnerability assessments, and implementing OWASP guidelines to enhance site security. This approach is expected to mitigate the risk of web defacement attacks in the future.

Keywords: *web defacement, site security, ".go.id" domain, cyber attacks, SQL injection.*

1 PENDAHULUAN

Era digitalisasi merupakan salah satu terobosan pemerintah dalam memajukan suatu daerah dengan menggunakan teknologi komunikasi dan informasi melalui konsep yang telah diatur secara maksimal untuk kepentingan masyarakat dalam pengelolaan sumber daya (Setiawan & Lomi, 2024). Situs merupakan salah satu upaya pemerintah untuk menunjang warga karena sifatnya tidak dibatasi ruang dan waktu, sehingga memiliki fleksibilitas jam kerja.

e-ISSN: 2580-3239
p-ISSN: 2085-7993
Volume 24 No. 1 Juli 2025

Penggunaan teknologi ini kemudian menjadi sebuah tempat dimana masyarakat dapat berkomunikasi dan belajar mengenai komunitasnya juga sebagai sarana pemerintah dalam melayani masyarakat (Hendarto & Handayani, 2024). Tetapi penggunaan situs ini menjadi celah terjadinya *cybercrime*, terutama pada situs yang menggunakan domain ".go.id", serangan tersebut menduduki peringkat pertama pada tahun 2018 yaitu sebanyak 30,75% dibandingkan dengan situs domain .id lainnya (Fazlurrahman & Hariyadi, 2019). Salah satu serangan siber yang marak terjadi adalah *web defacement* perjudian *online* yang menyusup melalui situs pemerintahan akibat dari lemahnya keamanan pada beberapa situs pemerintahan. Insiden ini terdeteksi cukup masif hingga menyebabkan puluhan bahkan ratusan situs terdampak. Halaman judi *online* pada situs pemerintahan ini merupakan dampak nyata dari *web defacement* judi *online*, salah satu alasan situs milik pemerintah menjadi incaran pelaku cybercrime adalah untuk menghindari situs tersebut diblokir oleh pihak berwenang (CSIRT-BARSEL, 2024).

Permasalahan utama dalam hal ini adalah, mengapa situs pemerintah dengan domain ".go.id" menjadi target yang rentan terhadap serangan *web defacement* yang berisi konten perjudian *online*. Isu ini menunjukkan kelemahan pada sistem keamanan yang digunakan oleh beberapa situs pemerintah, sehingga diperlukan pemahaman lebih lanjut mengenai mekanisme serangan dan bagaimana pengamanan yang kurang memadai menjadi penyebabnya. Selain itu, penting untuk menganalisis metode yang sering digunakan oleh pelaku untuk mengeksploitasi celah keamanan yang ada, agar langkah mitigasi dapat dirumuskan secara komprehensif.

Analisis ini bertujuan untuk memberikan pemahaman konseptual mengenai penyebab kerentanan situs pemerintahan terhadap serangan *web defacement*, khususnya yang berkaitan dengan konten perjudian *online*. Pendekatan ini juga mencakup identifikasi metode serangan yang sering digunakan dan bagaimana pola-pola tersebut dapat diatasi dengan strategi keamanan yang lebih baik. Dengan mengeksplorasi konsep-konsep ini, analisis diharapkan dapat menawarkan solusi strategis yang relevan untuk memperkuat sistem keamanan pada situs pemerintahan dengan domain ".go.id", sehingga ancaman serupa dapat diminimalisasi di masa depan.

2 KAJIAN PUSTAKA

Situs merupakan sekumpulan halaman berisi informasi berbentuk digital, informasi tersebut dapat berupa teks, gambar, audio, video, animasi atau gabungan dari semuanya (Sidik, 2019), fungsi situs dalam pemerintahan adalah sebagai sarana komunikasi dan informasi antara pemerintah dengan masyarakat. Tetapi tidak jarang fungsi tersebut tidak tersampaikan dengan baik akibat dari celah yang dimiliki oleh suatu situs, maka terjadilah cybercrime.

Cybercrime dapat diartikan sebagai kejahatan virtual dengan memanfaatkan perangkat yang terhubung ke internet, dan mengeksploitasi perangkat lain (Arifah, 2011), adanya kelemahan pada sistem operasi, perangkat lunak, atau situs dapat dimanfaatkan untuk melakukan kejahatan seperti pencurian data, *SQL injection*, skimming, malware, *web defacement* dan lain-lain. Dalam kasus *web defacement* judi *online* pada situs pemerintahan, biasanya para pelaku menemukan celah melalui *SQL injection* (CSIRT-BARSEL, 2024).

Web defacement merupakan salah satu cybercrime yang menyerang situs dengan mengubah tampilan (Nurjanah & Insanudin, 2016). Terdapat bermacam-macam cara yang digunakan oleh pelaku, seperti *SQL injection*, mencuri password, dan cara lainnya, tujuan utama pelaku mengubah tampilan situs diantaranya adalah, untuk mencoreng nama baik, menyampaikan pesan politik juga digunakan untuk mengambil keuntungan pribadi. Biasanya halaman awal situs langsung berubah ketika serangan deface terjadi, lain kasus dengan situs pemerintahan, para pelaku memanfaatkan halaman yang jarang dilihat oleh pengguna situs, mengubah tampilan menjadi sebuah halaman judi *online*, kemudian dipasarkan tanpa khawatir terkena blokir.

Permainan judi *online* merupakan salah satu jenis kejahatan dalam teknologi informasi yang bertentangan dengan nilai, norma, agama, kesusilaan, serta dapat membahayakan kehidupan bermasyarakat, bangsa, dan negara. Karena jika seseorang sudah kecanduan judi dan tidak memiliki

e-ISSN: 2580-3239
p-ISSN: 2085-7993
Volume 24 No. 1 Juli 2025

harta benda lagi untuk ditaruhkan, maka ia akan melakukan segala cara supaya mereka mendapatkan harta untuk ditaruhkan, baik itu dengan meminjam ke relasinya ataupun melakukan tindak kejahatan demi tercapainya tujuan orang tersebut (Nurdiana, Aisyah, & Ilham, 2022). Pada awalnya, judi dilakukan secara konvensional, para pemain akan bertemu secara langsung di suatu tempat yang menyediakan permainan judi, kini permainan judi mengikuti perkembangan teknologi, mempermudah akses pemain, juga menghilangkan rasa cemas karena judi konvensional rawan diketahui oleh orang sekitar.

3 METODE PENELITIAN

Analisis ini menggunakan metode deskriptif dengan pendekatan kajian pustaka, di mana data diperoleh dari sumber-sumber sekunder seperti artikel jurnal, laporan resmi, dan berita yang relevan dengan topik. Pendekatan ini bertujuan untuk memahami kerentanan situs pemerintah dengan domain ".go.id" terhadap serangan *web defacement* yang mengandung konten perjudian *online*.

Tahapan penelitian ini meliputi pengumpulan data yang dilakukan melalui studi literatur dari sumber terpercaya, seperti laporan Badan Siber dan Sandi Negara (BSSN) serta penelitian sebelumnya terkait *web defacement* dan keamanan situs. Data yang diperoleh kemudian dianalisis secara deskriptif untuk mengidentifikasi penyebab utama kerentanan, metode serangan yang sering digunakan, serta solusi yang dapat diterapkan. Hasil analisis tersebut disusun secara sistematis guna memberikan gambaran konsep dan rekomendasi yang relevan. Penelitian ini memiliki batasan, yaitu hanya berfokus pada kajian literatur tanpa pengumpulan data lapangan, dengan analisis yang difokuskan pada situs pemerintah dengan domain ".go.id" serta kasus *web defacement* yang terkait dengan perjudian *online*.

4 HASIL DAN PEMBAHASAN

4.1 Pengumpulan Data

Untuk mengidentifikasi situs pemerintah dengan domain ".go.id" yang telah disusupi konten perjudian *online*, dapat dilakukan pencarian menggunakan mesin pencari seperti Google, untuk menemukan kata atau frasa yang cocok (Broida, 2009), Dengan memasukkan kata kunci terkait perjudian *online*, seperti "gacor", "casino", "slot", atau "poker", ditambah dengan operator "site: .go.id" (misalnya, "gacor site: .go.id"), akan muncul hasil pencarian yang menunjukkan situs-situs pemerintah yang kemungkinan telah mengalami defacement dengan konten perjudian *online* seperti yang dapat dilihat pada Gambar 1. Apabila salah satu situs diakses, maka muncul tampilan halaman judi *online* yang dapat dilihat pada Gambar 2. Hal ini menunjukkan bahwa serangan *web defacement* dengan muatan perjudian *online* masih marak terjadi dan menargetkan domain ".go.id". Salah satu alasan utama penyerang menyasar situs pemerintah adalah untuk menghindari pemblokiran oleh pihak berwenang, mengingat situs dengan domain ".go.id" dianggap resmi dan terpercaya (CSIRT-BARSEL, 2024). Pengumpulan data ini didukung oleh penelitian yang dilakukan oleh (Suharjo & Setyaningsih, 2024), yang mengidentifikasi dan menganalisis peretasan pada domain situs dari data Google Cache.

e-ISSN: 2580-3239
p-ISSN: 2085-7993
Volume 24 No. 1 Juli 2025

Gambar 1. Hasil pencarian "gacor in site ".go.id" menggunakan google.com

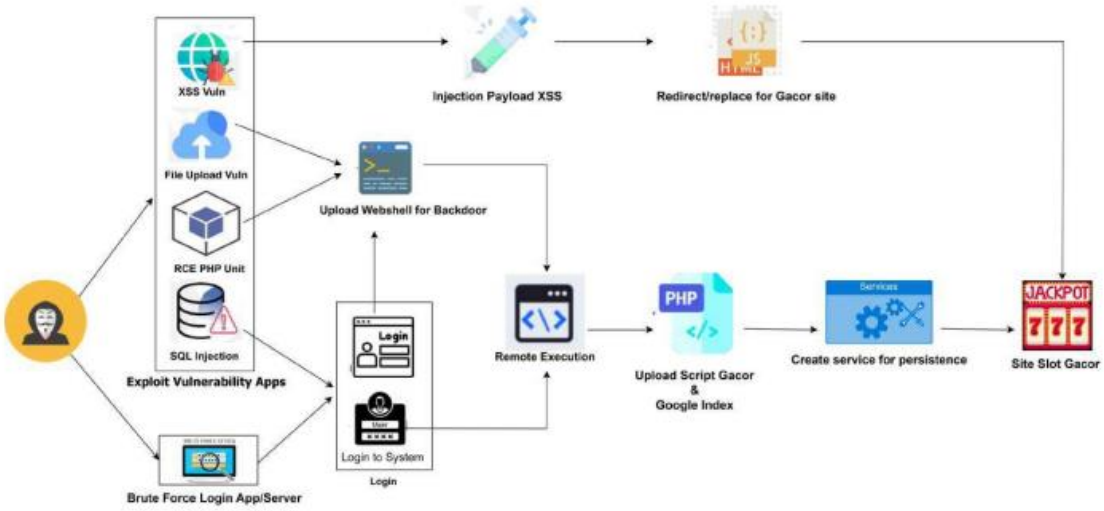
Gambar 2. Halaman dmpbandung pada domain dmpbandung".go.id"

e-ISSN: 2580-3239
p-ISSN: 2085-7993
Volume 24 No. 1 Juli 2025

4.2 Analisis Data

Serangan web defacement pada situs pemerintah umumnya memanfaatkan berbagai kerentanan keamanan menggunakan alur serangan seperti yang dapat dilihat pada Gambar 3, juga memanfaatkan kerentanan pada sebuah situs antara lain:

- ***Cross-Site Scripting (XSS)*:** Penyerang menyisipkan skrip berbahaya ke dalam halaman web yang kemudian dijalankan oleh pengguna, memungkinkan penyerang mengubah tampilan situs atau mencuri informasi sensitif. Menurut (Fazlurrahman & Hariyadi, 2019), serangan XSS dapat digunakan untuk mengubah tampilan situs web pemerintah.
- ***File Upload Vulnerability*:** Penyerang mengunggah file berbahaya, seperti webshell, melalui fitur unggah yang tidak aman, memberikan akses tidak sah ke server web. BSSN mencatat bahwa serangan *web defacement* sering memanfaatkan kelemahan ini (CSIRT-BARSEL, 2024).
- ***PHP Unit Vulnerability*:** Kerentanan pada PHP Unit dapat dieksploitasi untuk mengeksekusi kode berbahaya dari jarak jauh, memungkinkan penyerang menginstal backdoor atau webshell (CSIRT-BARSEL, 2024). BSSN menekankan pentingnya memperbarui komponen PHP untuk mencegah eksploitasi semacam ini.
- ***SQL injection*:** Penyerang menyisipkan pernyataan SQL berbahaya melalui input pengguna, memungkinkan akses tidak sah ke basis data dan potensi pengambilalihan situs. (Fazlurrahman & Hariyadi, 2019), menyebutkan bahwa serangan *SQL injection* dapat digunakan untuk mengubah konten situs web pemerintah.
- ***Brute Froce Login*:** *Brute force* adalah teknik serangan atau tindakan penyerang secara paksa pada sistem keamanan situs dengan menggunakan percobaan menebak akun dan sandi pengguna atau admin (CSIRT-BARSEL, 2024).



Gambar 3. Alur serangan situs

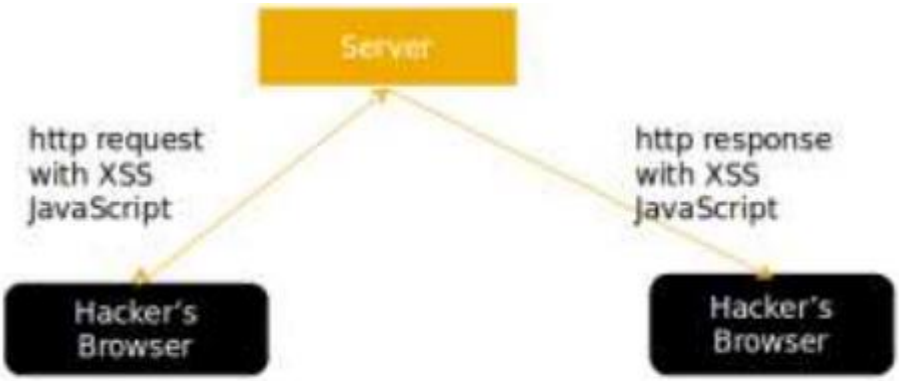
Penyerang akan mencoba memanfaatkan kerentanan sebuah situs untuk mendapatkan hak akses, kemudian menyisipkan *webshell* atau *payload XSS* yang berfungsi sebagai pengubah tampilan menjadi situs judi *online*. Dalam kasus ini banyak dari penyerang menggunakan metode *Cross-Site Scripting (XSS)* untuk mengubah tampilan atau fungsi sebuah situs pemerintahan menjadi situs judi *online*.

Cara kerja Serangan *XSS* berbeda dari kebanyakan serangan lapisan aplikasi lainnya, yang mana *XSS* berfokus pada menyerang pengguna aplikasi, bukan aplikasi maupun server itu sendiri (Suroto & Asman, 2021), Misalnya sebuah potongan kode

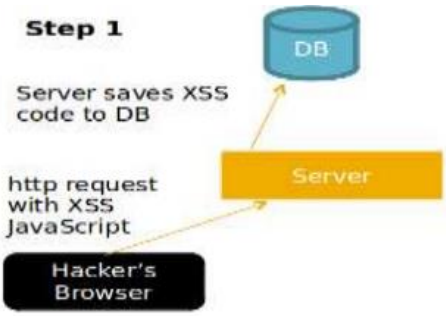
e-ISSN: 2580-3239
p-ISSN: 2085-7993
Volume 24 No. 1 Juli 2025

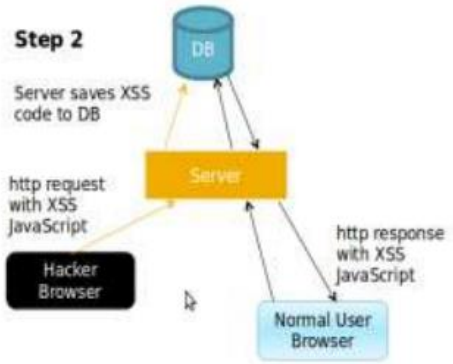
"<script>alert ('this site has been hacked') ;</script>"

Kebanyakan website memiliki banyak titik injeksi, seperti *search fields*, *feedback forms* atau *cookies,* secara umum, serangan *XSS* dijabarkan pada Gambar 4 dan Gambar 5. Tujuan yang paling umum dari serangan *XSS* adalah untuk mengumpulkan data *cookie*, *cookie* digunakan untuk menyimpan informasi berupa sesi, preferensi pengguna atau informasi *login* yang dapat dimanfaatkan oleh penyerang untuk masuk kedalam sistem, terdapat 3 tipe pada serangan *XSS*, *Presistent, Reflected,* dan *DOM Based*.



Gambar 4. Serangan *XSS* Secara Umum





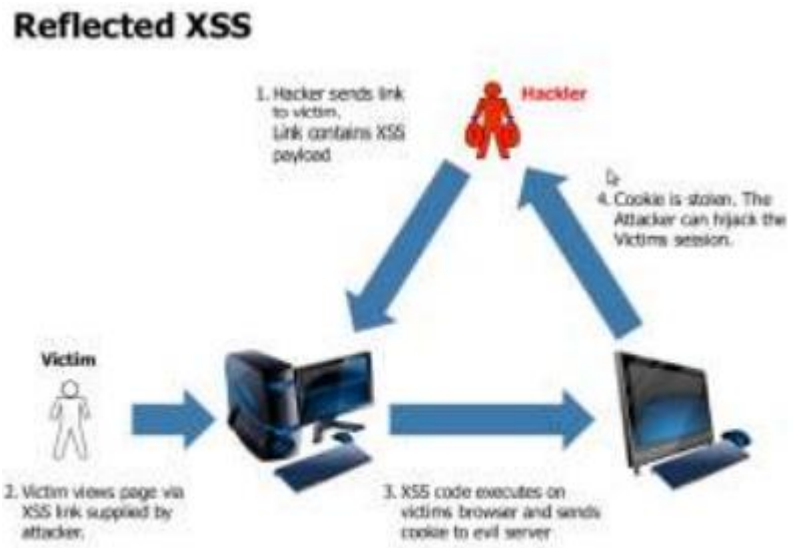
Gambar 5. Alur Serangan *XSS Presistent*

e-ISSN: 2580-3239
p-ISSN: 2085-7993
Volume 24 No. 1 Juli 2025

Serangan *presistent* pada *XSS* berarti kode *XSS* akan disimpan ke dalam penyimpanan persisten seperti *database*, akibatnya, dapat terlihat juga oleh pengguna lain, sebagai contoh pada Gambar 6 dimasukan *script* kemudian *script* tersebut disimpan oleh aplikasi, dan dapat terlihat oleh semua pengguna.

Gambar 6. Injeksi *XSS* dengan tipe presistent

Sementara serangan *XSS* dengan jenis *reflected* berarti kode *XSS* hanya ditampilkan untuk halaman berikutnya untuk pengguna yang sama, dan tidak akan disimpan ke dalam penyimpanan presisten, alur serangan pada jenis *reflected* dapat dilihat pada Gambar 7.



Gambar 7. Sistem Kerja Serangan *Reflected XSS*

Penyerang memberikan sebuah tautan *XSS* kepada korban, kemudian korban melakukan akses tautan tersebut sehingga sistem mengirimkan informasi seperti *cookies* kepada penyerang, hal ini menyebabkan penyerang dapat masuk kedalam sistem secara leluasa.

e-ISSN: 2580-3239
p-ISSN: 2085-7993
Volume 24 No. 1 Juli 2025

Kemudian serangan *XSS* berbasis *DOM,* merupakan serangan akibat dari memodifikasi "lingkungan" DOM di browser korban yang digunakan oleh script sisi klien asli, sehingga kode sisi klien berjalan dalam sebuah cara "tak terduga". Artinya, halaman itu sendiri (respon HTTP tersebut) tidak berubah, tapi kode sisi klien yang terkandung dalam halaman mengeksekusi berbeda karena modifikasi berbahaya yang telah terjadi di lingkungan DOM. Hal ini berbeda dengan serangan lain *XSS*, dimana *payload* serangan ditempatkan di halaman respon (karena cacat sisi server). Sebagai contoh.

var pos = document.URL.indexOf ("name =") + 5; document.write

(document.URL.substring (pos, document.URL.length)); ...

http://www.vulnerable.site/welcome.html?na me=Joe

Berdasarkan penelitian yang dilakukan oleh (Suharjo & Setyaningsih, 2024), ditemukan bahwa dalam kurun waktu 81 hari, terdapat 7.604 konten pada 445 domain ".go.id" yang diretas, dan dalam 43 hari, terdapat 3.576 konten pada 252 domain ac.id yang diretas. Jenis peretasan yang dominan pada domain ".go.id" adalah *Reflected XSS* in search (45%) dan konten terhack (45%).

Hal ini menunjukkan bahwa serangan *web defacement* yang mengubah tampilan situs pemerintah menjadi halaman perjudian *online* telah meningkat secara signifikan pada tahun 2024. Penting bagi para pemilik situs terutama pemerintah melakukan pemeliharaan situs untuk mengidentifikasi kerentanan pada sebuah situs.

4.3 Penyusunan Hasil

Berdasarkan hasil analisis, serangan *web defacement* pada situs pemerintah dengan domain ".go.id" menunjukkan peningkatan signifikan dalam serangan yang membawa konten perjudian *online*. Kerentanan yang paling sering dimanfaatkan adalah XSS, File Upload Vulnerability, PHP Unit Vulnerability, dan *SQL injection*. Penyerang menggunakan berbagai teknik untuk mengeksploitasi celah ini, yang mengarah pada perubahan tampilan situs atau pengambilalihan kontrol situs.

Untuk mengurangi risiko dan melindungi situs pemerintah dari serangan semacam itu, rekomendasi metode yang tepat adalah:

- **Penetration Testing (Pengujian Penetrasi):** Metode ini melibatkan simulasi serangan terhadap sistem untuk mengidentifikasi dan mengeksploitasi kerentanan yang ada. Tujuannya adalah untuk memahami sejauh mana sistem dapat bertahan dari serangan nyata. Penelitian oleh (Omeiza & Tweneboah, 2018) menekankan pentingnya pengujian penetrasi dalam mengidentifikasi kelemahan keamanan pada portal institusi pendidikan.
- **Vulnerability Assessment (Penilaian Kerentanan):** Proses ini melibatkan identifikasi, kuantifikasi, dan prioritisasi kerentanan dalam sebuah sistem. Berbeda dengan penetration testing yang berfokus pada eksploitasi, vulnerability assessment lebih menekankan pada identifikasi potensi kerentanan. (Bairwa, Mewara, & Gajrani, 2014) membahas pendekatan proaktif dalam menilai keamanan aplikasi web melalui penggunaan pemindai kerentanan.
- **Vulnerability Scanners (Pemindai Kerentanan):** Alat otomatis seperti Acunetix, Nessus, dan OpenVAS digunakan untuk memindai aplikasi web terhadap berbagai kerentanan yang diketahui. (Erturk & Rajan, 2017) melakukan studi kasus mengenai efektivitas pemindai kerentanan web dalam mendeteksi kelemahan keamanan.
- **Metodologi *OWASP* (Open Web Application Security Project):** *OWASP* menyediakan panduan dan alat untuk mengidentifikasi serta mengatasi kerentanan pada aplikasi web. Proyek ini mencakup daftar kerentanan paling kritis yang dikenal sebagai *OWASP* Top Ten, yang dapat digunakan sebagai acuan dalam evaluasi keamanan. (Fauzi, Hermawan, Adhy, & Maesaroh,

e-ISSN: 2580-3239
p-ISSN: 2085-7993
Volume 24 No. 1 Juli 2025

2024) menerapkan metode *OWASP* dan PTES dalam menganalisis kerentanan keamanan web pada situs pemerintahan desa.

Dengan menerapkan metode-metode tersebut, pemerintah dapat mengidentifikasi dan menangani kerentanan pada situs mereka, sehingga meningkatkan keamanan dan mengurangi risiko terhadap ancaman *web defacement*.

5 SIMPULAN

Dapat disimpulkan bahwa serangan *web defacement* dengan konten perjudian *online* telah menjadi ancaman yang signifikan pada situs pemerintah dengan domain ".go.id". Kerentanan utama yang dimanfaatkan adalah Cross-Site Scripting (XSS), File Upload Vulnerability, PHP Unit Vulnerability, dan *SQL injection*. Untuk melindungi situs dari serangan ini, disarankan agar pemerintah mengimplementasikan pengujian penetrasi, pemindaian kerentanan secara rutin, serta melakukan pembaruan sistem dan komponen perangkat lunak secara berkala. Selain itu, meningkatkan kesadaran keamanan pengelola situs dan menerapkan metode keamanan seperti *OWASP* untuk mengurangi risiko. Penelitian lebih lanjut dapat difokuskan pada pengembangan sistem deteksi dini berbasis kecerdasan buatan untuk mempercepat respons terhadap potensi serangan.

DAFTAR PUSTAKA

Arifah, D. A. (2011). KASUS CYBERCRIME DI INDONESIA. *Jurnal Bisnis dan Ekonomi (JBE)*, 185-195.

Bairwa, S., Mewara, B., & Gajrani, J. (2014). Vulnerability Scanners-A Proactive Approach To Assess Web Application Security. *arXiv*.

Broida, R. (2009). *Use Google to Search Within One Site.* Retrieved from PCWorld: https://www.pcworld.com/article/533353/use_google_to_search_within_one_site.html

CSIRT-BARSEL. (2024, Februari). *PANDUAN PENANGANAN INSIDEN.* Retrieved from Computer Security Incident Response Team Barito Selatan: https://csirt.baritoselatankab.go.id/storage/uploads-guidances/PANDUAN-PENANGANAN-INSIDEN-WEB-DEFACEMENT-JUDI-*ONLINE*-ttd.pdf

Erturk, E., & Rajan, A. (2017). Web Vulnerability Scanners: A Case Study. *arXiv*.

Fauzi, R. M., Hermawan, R., Adhy, D. R., & Maesaroh, S. (2024). Analisis Kerentanan Keamanan Web Menggunakan Metode *OWASP* dan PTES di Web Pemerintahan Desa XYZ. *Power Elektronik : Jurnal Orang Elektro*, 225-231.

Fazlurrahman, & Hariyadi, D. (2019). Analisis Serangan Web Defacement pada Situs Web Pemerintah Menggunakan ELK Stack. *JISKA*, 1 - 8.

Hendarto, D. H., & Handayani, R. S. (2024). Pencegahan Kejahatan Siber Terkait Distribusi Perjudian *Online* di Indonesia dalam Rangka Mewujudkan Keamanan dan Ketertiban Masyarakat. *Syntax Admiration*.

Nurdiana, M., Aisyah, N., & Ilham, S. N. (2022). FENOMENA JUDI *ONLINE* DI DAERAH JAKARTA SELATAN. *Jurnal Pendidikan, Politik, Budaya, Bahasa, Manajemen, Komunikasi, Pemerintahan, Humaniora, dan Ilmu Sosial (Perspektif)*, 105-110.

Nurjanah, T. S., & Insanudin, E. (2016). *Hack Database Website Menggunakan Python dan Sqlmap Pada Windows.* Retrieved from Hack Database Website Menggunakan Python dan Sqlmap Pada Windows: https://www.researchgate.net/profile/Tanti-Siti-Nurjanah/publication/303372599_Hack_Database_Website_Menggunakan_Python_dan_Sqlmap_Pada_Windows/links/573fd5c908ae9f741b3223c4/Hack-Database-Website-Menggunakan-Python-dan-Sqlmap-Pada-Windows.pdf

e-ISSN: 2580-3239
p-ISSN: 2085-7993
Volume 24 No. 1 Juli 2025

Omeiza, D., & Tweneboah, J. O. (2018). Web Security Investigation through Penetration Tests: A Case study of an Educational Institution Portal. *arXiv*.

Setiawan, R., & Lomi, P. Y. (2024). Penggunaan Website kemendagri.go.id Sebagai Bentuk Peningkatan Kualitas Layanan Publik. *Jurnal Ilmiah Administrasi Pemerintahan Daerah*, 43-57.

Sidik, A. (2019). *Teori, Strategi, dan Evaluasi Merancang Website dalam Perspektif Desain.* Banjamasin: Universitas Islam Kalimantan.

Suharjo, I., & Setyaningsih, P. W. (2024). Identifikasi Dan Analisis Terjadinya Peretasan Pada Domain Website dari Data Google Cache. *Unipdu*, 61-70.

Suroto, S., & Asman, A. (2021). ANCAMAN TERHADAP KEAMANAN INFORMASI OLEH SERANGAN CROSS-SITE SCRIPTING (XSS) DAN METODE PENCEGAHANNYA. *Zona Komputer*, 11-19.