e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 8 No. 1, Juni, 2024, **Hal. 75-83**
DOI: 10.29408/edumatic.v8i1.25267

Monitoring dan Pencegahan Serangan Judi *Online* (Slot Gacor) pada Website

Endi Sjaiful Alim [1], Nuroji [1], M. Asep Rizkiawan [2,*], Tirta Anhari [1], Bahar Sobari [1]

[1] Program Studi Teknik Informatika, Universitas Muhammadiyah Prof. DR. HAMKA, Indonesia
[2] Program Studi Teknik Elektro, Universitas Muhammadiyah Prof. DR. HAMKA, Indonesia
[*] Correspondence: asep@uhamka.ac.id

Received: 1 Februari 2024 | Revised: 3 Februari 2024 | Accepted: 26 Februari 2024 | Published: 20 Juni 2024

Abstrak
Website merupakah sebuah sarana yang cukup kompleks dalam menyajikan informasi. Keamanan sebuah website menjadi sangat penting guna menunjang reputasi dari website tersebut. Maraknya judi *online* sekarang sudah merambah ke website, yang paling berbahaya adalah Ketika website sudah disusupi dengan *page* judi *online*. Tujuan dari penelitian adalah melakukan pencegahan dan pemantauan website terhadap serangan *hacker* judi *online*. Penelitian ini menggunakan pendekatan metode deskriptif yaitu dengan melakukan pemantauan dan pengamatan pada website, kami berusaha untuk memberikan penjelasan mendalam mengenai pemantauan dan pencegahan terhadap serangan judi *online* (Slot Gacor) dengan memanfaatkan layanan *Cloudflare*. *Cloudflare* diimplementasikan sebagai sistem keamanan pada website. Pada penelitian ini website yang menjadi studi kasus adalah website bpti.uhamka.ac.id dengan lokasi penelitian berada di ruang data center UHAMKA. Teknik pengumpulan data dan analisa data dilakukan pengamatan secara langsung melalui website *cloudflare*. Data yang dianalisis berupa grafik dan *path url* uang telah di blok. Hasil penelitian Dalam kurun waktu 8 hari terdapat 126 *path url* yang dapat di *block* oleh *cloudflare* dan semuanya berisikan judi *online* dengan kebanyakan merupakan slot gacor. *Cloudflare* telah berhasil memblokir peretas dengan memfilter *URL* jalur dari situs web asal.

Kata kunci: keamanan website; web application firewall; cloudflare; judi online

Abstract
A website is a complex tool for presenting information. The security of a website is very important to support the reputation of the website. The rise of online gambling has now penetrated the website, the most dangerous is when the website has been infiltrated with an online gambling page. The purpose of the research is to prevent and monitor the website against online gambling hacker attacks. This research uses a descriptive method approach, namely by monitoring and observing the website, we try to provide an in-depth explanation of monitoring and preventing online gambling attacks (Slot Gacor) by utilizing Cloudflare services. Cloudflare is implemented as a security system on the website. In this research, the website that became a case study was the bpti.uhamka.ac.id website with the research location in the UHAMKA data center room. Data collection techniques and data analysis are carried out by direct observation through the cloudflare website. The data analyzed in the form of graphs and money url paths have been blocked. Research results Within 8 days there were 126 url paths that could be blocked by cloudflare and all of them contained online gambling with most of them being gacor slots. Cloudflare has successfully blocked hackers by filtering path URLs from the originating website.
.

Keywords: *website security; web application firewall; cloudflare; online gambling*

PENDAHULUAN

Diera teknologi digital saat ini kemudahan informasi menjadi salah satu bagian yang sangat penting. Kemudahan untuk mengakses suatu infomasi menjadi salah satu cara yang saat ini dibutuhkan oleh orang banyak (Makmur, 2019; Nguyen & Nguyen, 2020). Website tidak bisa dipisahkan dari sumber informasi yang mudah diakses oleh orang banyak, Sebuah situs web adalah suatu halaman yang berisi informasi yang dapat diakses ketika komputer kita terhubung ke internet (Fatkhurozzi, 2021; Pratama et al., 2023). Situs web memungkinkan semua orang di seluruh dunia untuk mendapatkan dan mengelola informasi dari berbagai sumber yang tersedia di internet. Saat ini, situs web dapat menyajikan berbagai jenis media, termasuk teks, gambar, suara, dan video (Harnita, 2010). dengan demikian Peningkatan kecepatan internet dan pertumbuhan jumlah pengguna internet juga ikut berperan dalam meningkatnya akses ke situs-situs web (Assiroj, 2022; Laksmiati, 2022). Keamanan pada website menjadi sangat penting dan ramai isu pembicaraan nya di dunia maya (Damayanti & Hikmah, 2022; Nuroji, 2023), website yang baik tentu website yang terhindar dari para *hacker* yang merugikan website seperti menyisipkan iklan pada website (Alim & Jin, 2019). Berbicara keamanan website tentu sangat kompleks, tidak ada satupun keamanan yang tidak memiliki celah kelemahan dan kerentanan (Helmiawan et al., 2020; Shahid et al., 2022; Srivatanakul & Annansingh, 2022), namun tentu terdapat bagaimana cara menanggulangi dan mengurangi serta mengantisipasi dari serangan para *hacker* yang tidak bertanggung jawab. karena tentu ini akan sangat berdampak buruk bagi reputasi website yang telah disusupi *hacker*, terlebih lagi pemasangan iklan judi online pada *page* website yang tentu sudah jelas ini dilarang oleh pemerintah (Karli et al., 2023).

Website masih sangat berpengaruh peran nya pada saat ini untuk lebih memudahkan informasi berita dan yang lain nya. Hal ini juga diterapkan oleh Badan Pengembangan Teknologi Informasi (BPTI) Universitas Muhammadiyah Prof. DR. HAMKA dalam memanfaatkan website sebagai sarana media penyampaian informasi dan hal lain nya, selaku badan di lingkungan Universitas Muhammadiyah Prof. DR. HAMKA yang menjadi pusat dari teknologi informasi (Alim, 2017; Rizkiawan et al., 2023), melalui laman website bpti.uhamka.ac.id penyampaian informasi berkaitan dengan kampus, berita-berita, kegiatan yang telah dilaksanakan serta video tentang teknologi informasi yang berkembang. Sebagai badan teknologi informasi tentu BPTI menjadi sorotan dan menjadi percontohan dari fakultas, Lembaga, badan maupun biro dilingkungan Universitas Muhammadiyah Prof. DR. HAMKA berkaitan dengan bagaimana tampilan, pnengelolaan dan isi dari website. Dengan demikian tentu Badan Pengembangan Teknologi Informasi (BPTI) Universitas Muhammadiyah Prof. DR. HAMKA harus selalu menjaga bagaimana websitenya dapat terjaga baik dari segi tampilan, isi konten dan frekuensi dalam mengisi websitenya. Namun demikian, ternyata kendala dan permasalahan pada website, yaitu serangan dari para *hacker* yang masuk dan menyisipkan iklan kedalam *page* website, tidak sedikit juga website dari berbagai kalangan yang luput dari serangan *hacker* yang memanfaatkan celah kelemahan keamanan dari website. Termasuk juga website yang dikelola oleh Badan Pengembangan Teknologi Informasi (BPTI) Universitas Muhammadiyah Prof. DR. HAMKA tak luput dari serangan *hacker* yang menyisipkan iklan pada *page* website. Saat ini yang paling banyak disisipkan oleh *hacker* adalah tentang judi online, termasuk kategori kejahatan atau sering dikenal *cyber crime*. Menjalankan tindakan keamanan pada suatu situs web menjadi sangat penting karena situs web sering menjadi target peretas untuk pelaksanaan eksploitasi, yang dapat berdampak merugikan pada integritas dan kinerja situs web itu sendiri (Ita et al., 2019).

Web application firewall adalah sebuah teknik perlindungan untuk website yang dapat mencegah serangan dari pihak yang tidak diinginkan seperti attacker atau hacker (Ardiansyah et al., 2023). Dalam penelitian ini *Web Aplication firewall* (WAF) pada *cloudflare* digunakan untuk menangkal atau memberikan keamanan pada web dari serangan *hacker* yang

menyisipkan judi *online* pada *page* website bpti.uhamka.ac.id. penelitian ini sangat penting dilakukan untuk menjadi salah satu solusi dari permasalahan tentang judi *online* yang saat ini marak dilakukan oleh *hacker* dengan menyisipkan *path url* pada *page* website yang dituju. keamanan website merupakan salah satu aspek yang sangat penting untuk dipertimbangkan. Serangan *cyber* seperti SQL *injection*, *cross-site scripting*, dan DDoS dapat merusak reputasi dan keandalan sebuah website.

Penelitian tentang keamanan website, Pada penelitian (Hermanto & Haeruddin, 2022) peningkatan sistem keamanan website menggunakan metode OWASP sebuah *framework open source* bertujuan untuk menyediakan informasi tentang kerentanan keamanan dan memberikan saran perbaikan yang dapat diterapkan pada layanan berbasis web. Pendekatan ini telah menjadi pedoman untuk menganalisis dan melakukan pengecekan keamanan pada suatu situs web. Melalui analisis ini, dapat mengidentifikasi risiko ancaman yang mungkin timbul pada layanan website tertentu dan mempermudah tindakan pencegahan berdasarkan rekomendasi yang diberikan. Dalam penelitian yang dilakukan (Purba et al., 2022) dalam menganalisis sistem keamanan web menggunakan metode *application scanning*. Penelitian yang dilakukan (Andria, 2020), alat yang digunakan adalah WEBPWN3R, sebuah pemindai Keamanan Aplikasi Web yang bersifat *open source*, alat ini dapat melakukan analisis dan mendeteksi keberadaan *bug* pada suatu situs web. Pengujian dilaksanakan menggunakan komputer dengan sistem operasi Kali Linux. Tujuan dari penelitian nya adalah untuk menganalisis potensi kerentanan keamanan pada suatu situs web, memberikan bantuan kepada administrator atau pengelola situs untuk mendeteksi dan mengetahui kemungkinan kerentanan keamanan yang ada, sehingga mereka dapat segera melakukan perbaikan yang tepat berdasarkan temuan celah keamanan di situs web tersebut. Penelitian yang dilakukan (Tania et al., 2018) dalam melakukan evaluasi keamanan, digunakan metode *Vulnerability Assessment* untuk mengidentifikasi aset-aset pada website, kemudian menganalisis kerentanan yang terdeteksi, mempertimbangkan risiko yang diwakili dalam bentuk angka, dan menyajikan solusi perbaikan.

Pada penelitian ini yang membedakan dengan penelitian lain nya adalah metode yang digunakan dalam melakukan pengamanan pada website dengan memanfaatkan layanan *cloudflare*, artikel ilmiah yang membahas pencegahan dari serangan *hacker* tentang judi online pada website masih belum ada. Tujuan dari penelitian melakukan pencegahan dan pemantauan website terhadap serangan hacker dalam hal ini judi online. Studi kasus yang dilakukan adalah pada website bpti.uhamka.ac.id.

METODE

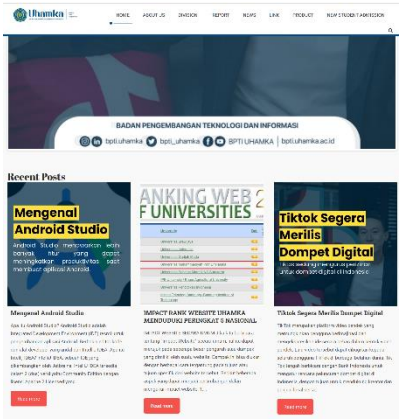
Penelitian ini menggunakan metode deskriptif. Penelitian Deskriptif adalah kami berupaya menggambarkan dengan rinci sesuatu yang sedang kami amati sejelas mungkin selama proses penelitian. Hal ini melibatkan pengamatan langsung oleh kami terhadap situasi di lapangan dan upaya untuk membuat gambaran yang mendalam. Dalam pendekatan deskriptif, kami berusaha untuk memberikan penjelasan mendalam mengenai pemantauan dan pencegahan terhadap serangan judi *online* (Slot Gacor) dengan memanfaatkan layanan *Cloudflare*. Tahap selanjutnya kami dalam melakukan pengaturan *cloudflare* mempelajari secara terus menerus dan melakukan pengulangan terhadap cara kerja *cloudflare* untuk keamanan website. *cloudflare* dipasang sebagai sistem keamanan pada website. Penelitian ini menggunakan *cloudflare*. *Cloudflare* merupakan salah satu jaringan terbesar yang beroperasi di Internet. Orang-orang menggunakan layanan *Cloudflare* untuk tujuan meningkatkan keamanan dan kinerja situs web dan layanann kecepatan koneksi internet pada saat mengunjungi website. Penerapan *cloudflare* di implementasikan pada website bpti.uhamka.ac.id. dalam penelitian ini aspek yang di teliti adalah tentang *path url* yang masuk dan terblok serta jumlah banyaknya *path url* yang terblokir. Tahap awal pada penelitian ini

adalah identifikasi masalah pada tahap ini menjelaskan bahwa masalah yang terjadi adalah serangan *hacker* pada website bpti.uhamka.ac.id yang terdapat iklan judi *online* pada *page* website. Pada tahap selanjutnya yaitu mempersiapkan web aplikasi *cloudflare* untuk kemudian di implementasikan atau dipasang pada website bpti.uhamka.ac.id. Tahapan selanjutnya adalah tahapan Instalasi atau pemasangan *cloudflare* pada website bpti.uhamka.ac.id Tahap selanjutnya yaitu implementasi *cloudflare* dengan membuat kata kunci pada *Web Aplication firewall* (WAF), pada menu *security* di web aplikasi *cloudflare* atau diebut juga membuat aturan agar *cloudflare* dapat memblokir *hacker* yang menyisipkan iklan judi *online* pada website. Tahapan selanjutnya yaitu menganalisa website yang telah di pasang *cloudflare* apakah masih bisa masuk serangan dari *hacker* ke website. Teknik pengumpulan data dan analisa data dilakukan secara langsung melalui pengamatan website *cloudflare*. Data yang dianalisis berupa grafik dan *path url* uang telah di blok

HASIL DAN PEMBAHASAN

Hasil

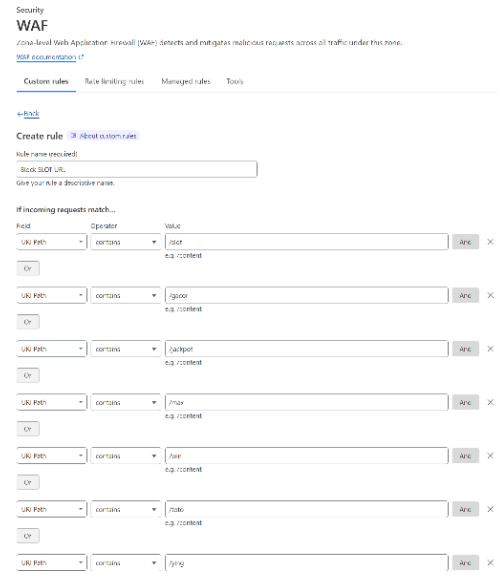
Website bpti.uhamka.ac.id yang sudah diimplementasikan dengan *cloudflare*. Penerapan dan pemasangan *cloudflare* pada website bpti.uhamka.ac.id guna mencegah dan mengantisipasi serangan *hacker*. Terdapat banyak konten didalam website, baik berupa narasi, gambar maupun video, dapat dilihat pada gambar 1. Website bpti.uhamka.ac.id merupakan website yang menjadi sorotan dan percontohan oleh website di lingkungan UHAMKA baik fakultas, badan, lembaga maupun biro.



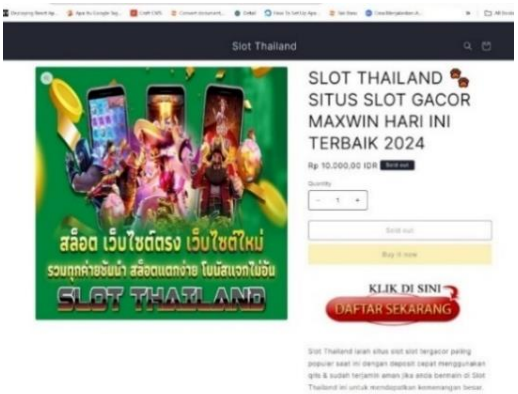
Gambar 1. Tampilan website bpti.uhamka.ac.id

Pada *cloudflare* terdapat menu *security* WAF (*Web Application Firewall*), dimana ini merupakan menu pada *cloudflare* yang digunakan untuk memblokir situs ataupun *contains* yang mengandung arti ataupun kata yang disisipkan pada page website. Terdapat *custom rules* pada menu WAF yang digunakan untuk memasukan (*rules*) atau *keyword* untuk mem*filter* contains dari *hacker* yang akan memasukan atau menyisiplan *page* didalam website, dapat dilihat pada gambar 2 yang menunjukan WAF *custom rules.*

Selanjutnya terdapat kasus pada *page* website pada gambar 3 yang disisipi oleh *hacker* dengan page berisikan situs judi online pada *path url* /sthailand/. Hal ini bisa masuk kedalam *page* website karena pada *cloudflare security* WAF pada *custome rules* tidak dibuat kan aturan *contains* /sthailand/ untuk di blok oleh *cloudflare.* Dengan masuknya *path url* dari judi online tersebut, kemudian dapat mendapatkan *rules* ataupun *contains* yang berhubungan dengan *path url* /sthailand/.

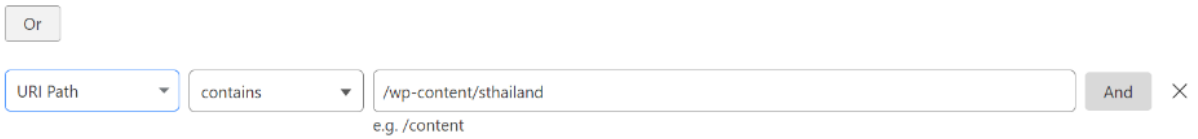


Gambar 2. Tampilan *custome rules* waf

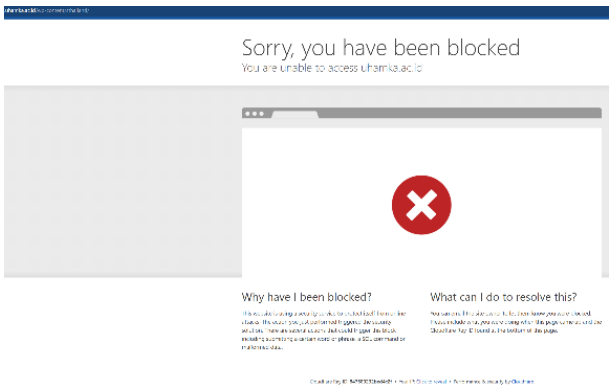


Gambar 3. Tampilan website yang sedang terkena *hack*

Sementara itu, pada gambar 4 Langkah preventif yang dilakukan adalah dengan masuk pada *cloudflare* ke menu *security* WAF yang didalan *security* WAF tedapat *custome rules* yang kemudian akan bertugas sebagai *filter* dari website. Kata kunci atau *contains* yang sudah dimasukan *cloudflare security* WAF pada *custome rules.* Selanjutnya pada gambar 5 adalah hasil dari *contains* yang telah di masukan pada *waf security* berhasil berfungsi dengan baik. *Cloudflare* dapat segera memblokir *page website* dengan *url path* /sthailand/ pada website bpti.uhamka.ac.id yang terkena *hacker* judi *online*, setelah di masukan *path url* /sthailand/ pada *waf security*.

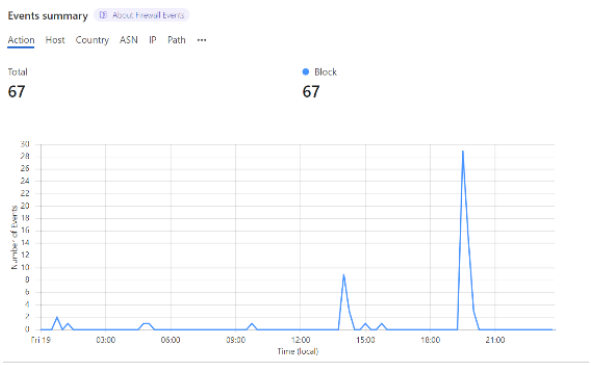


Gambar 4. *cloudflare security* WAF pada *custome rules*

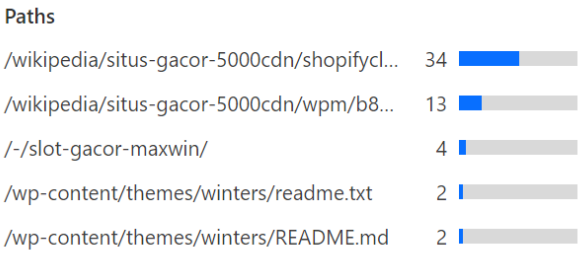


Gambar 5. *Page* yang sudah terblok

Pada gambar 6 dan 7 merupakan Hasil pemantauan dan Analisa pada website bpti.uhamka.ac.id dalam kurun waktu 8 hari dengan pengambilan data 1x24 jam berturut-turt pada tanggal 16-23 Januari 2024 pukul 00:00 sampai 23.59. Analisa dilakukan pada *cloudflare*. Setelah *cloudflare* diimplementasikan dan di *setting* pada WAF *cloudflare*. WAF *security* pada *cloudflare* akan bertindak sebagai keamanan di website, dengan cara akan melakukan pemblokiran pada *page* apabila ada *hacker* yang mencoba menyisipkan *path url* yang tidak dikenal. Dalam hal ini pemblokiran yang dilakukan adalah tentang judi *online*. WAF *Cloudflare* melakukan pemblokiran berdasarkan kata kunci atau *path url* yang telah dimasukan pada WAF *security cloudflare*.



Gambar 6. Jumlah *path url* yang sudah di blokir

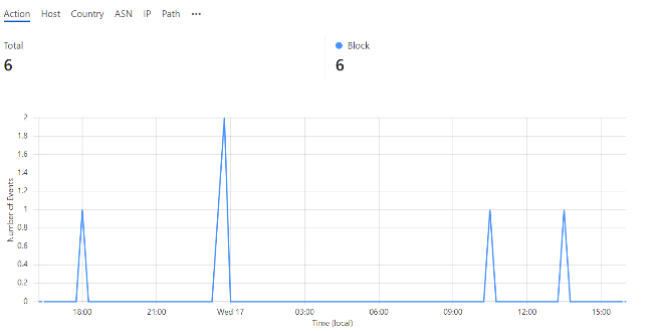


Gambar 7. *Path url* yang terblokir

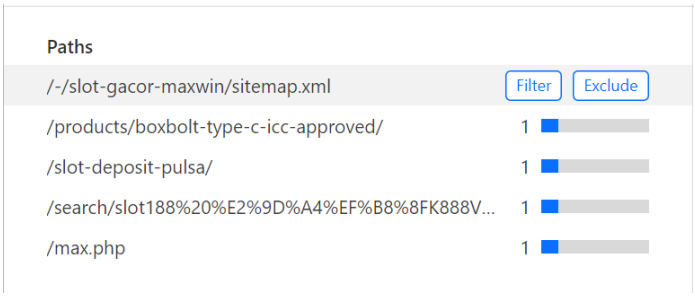
Pembahasan

Monitoring dan Pencegahan Serangan Judi *Online* pada Website merupakan suatu cara untuk melakukan pemantauan terhadap keamanan website melalui *dashboard cloudflare* dan sekaligus dalam melakukan pencegahan terhadap *hacker* yang mencoba melakukan *inject* atau melakukan *hacking* terhadap website. Implementasi dan Konfigurasi WAF *Cloudflare* dapat

dilakukan dengan langkah-langkah yang relatif mudah. Kami mengaktifkan *Web Aplication firewall* (WAF) *Cloudflare* melalui *dashboard Cloudflare* dan mengatur aturan keamanan yang sesuai dengan kebutuhan website. Berdasarkan hasil temuan pemantauan yang dilakukan selama 8 hari dengan pengambilan data 1x24 jam mendapatkan jumlah *path url* yang dapat di blok oleh *cloudflare* sejumlah 126 dengan masing-masing berbeda *path url* yang dapat dilihat pada *cloudflare*. Dengan menggunakan *Web Aplication firewall* (WAF) *Cloudflare*, dalam kurun waktu pemantauan kami mengamati dengan melalui *dashboard cloudflare*. Dengan demikian penerapan *Web Aplication firewall* (WAF) *Cloudflare* cukup efektif untuk menangkal dan memblokir dari serangan *cyber*. Perbandingan pada penelitian sebelumnya terletak pada hasil dan metode nya, hasil dari penelitian ini menunjukan *path url* dan jumlah *path url* yang terblokir hasil ini murni dari serangan yang dilakukan oleh pihak luar atau disebut *hacker* pengujian dilakukan secara alamiah tidak mengguanakan *inject* yang direncanakan atau yang dibuat serta penelitian penggunaan *Web Aplication firewall* (WAF) *cloudflrare* terbilang penelitian baru. Pada gambar 8 dan 9 merupakan sebagian data dari hasil temuan, berupa grafik dan *path url* pada *dashboard cloudflare* yang berhasil di blok.



Gambar 8. Grafik jumlah *path url* yang sudah di blokir.



Gambar 9. *Path url* yang terblokir

Selain dengan melakukan pengamatan secara langsung pada *dashboard cloudflare* dalam penelitian ini kami melakukan riset terhadap penelitian sebelumnya yang sudah ada dan yang berkaitan dengan penelitian ini. Pada penelitian yang dilakukan oleh Rahmadyanto & Chandra, 2023 mengenai analisis keamanan *Content Delivery Network* (CDN) *Cloudflare* (Studi kasus: Web Hakazon). Dimana penelitian mereka telah melakukan pengujian keamanan adalah menggunakan serangan rekayasa yang dibuat sendiri yaitu dengan membuat *Cross Site Scripting* dan *SQL Injection.*

Pada penelitian ini pengujian dilakukan secara alamiah dan organik yaitu berasal dari *hacker* yang telah menyisipkan *path url* judi *online* pada *page* website bpti.uhamka.ac.id. tentu ini menjadi suatu kehandalan dalam mencegah serangan dari *hacker* yang meyisipkan *path url* pada page website dengan tanpa izin pemilik website. Pada hasil penelitian ini menunjukan bahwa *Web Application Firewall* (WAF) *Cloudflare* dapat melakukan blok terhadap path url

yang masuk tanpa izin dengan maksud melakukan serangan hacking dengan menyisipkan *path url* pada website.

SIMPULAN

Penggunaan *Web Application Firewall* (WAF) *Cloudflare* dapat menjadi langkah yang efektif dalam meningkatkan keamanan website. Dengan fitur keamanan yang canggih dan kemudahan implementasi. WAF *Cloudflare* dapat membantu melindungi website dari serangan *cyber* dan menciptakan lingkungan *online* yang lebih aman. Namun, pengguna perlu memahami tantangan dan melakukan konfigurasi yang tepat untuk memaksimalkan keamanan website. Dengan demikian, penggunaan WAF *Cloudflare* dapat menjadi strategi yang efektif dalam upaya meningkatkan keamanan website dan melindungi data sensitif dari serangan *cyber*. Dapat dilihat dari gambar yang menjelaskan tentang penanganan dan pemblokiran terhadap *hacker* yang menyerang website. *cloudfllare* berhasil memblokir *hacker* yang akan menyisipkan *page* pada website. *Cloudflare* menggunakan teknologi yang baik untuk memantau lalu lintas web dan mengidentifikasi potensi ancaman, sehingga dapat menghalangi serangan sebelum mencapai website. Hal ini berdampak baik bagi website bpti.uhamka.ac.id dengan menggunakan WAF *cloudflare* website menjadi terhindar dari serangan *hacker* yang akan melakukan penyisipan pada *page website*.

REFERENSI

Alim, E. S. (2017). Information Technology (IT) Architecture Based on Cloud Computing for Muhammadiyah Higher Education Institutions (HEIs). *US-China Education Review A*, *7*(4) 209-217. https://doi.org/10.17265/2161-623x/2017.04.004

Alim, E. S., & Jin, H. (2019). Data security and privacy assurance for cloud computing in education based on a third-party auditor. *Basic and Clinical Pharmacology and Toxicology*, , 2(1), 142-144

Andria. (2020). Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux. *Generation Journal*, *4*(2) 69-76. https://doi.org/10.29407/gj.v4i2.14532

Ardiansyah, Y., Sunandar, M. A., & Muhyidin, Y. (2023). Implementasi Kemanan Website Dengan Metode Firewall Aplikasi Web (WAF) Studi kasus: Web Desa Wantilan. *Jurnal Mahasiswa Teknik Informatika*, *7*(3), 2018–2025.

Assiroj, P. (2022). Implementasi Metode Search Engine Optimization (Seo) Pada Situs Web Imigrasi Wonosobo. *Infotech Journal*, *8*(1) 41-52. https://doi.org/10.31949/infotech.v8i1.2239

Damayanti, T. H., & Hikmah, I. R. (2022). Network Forensic Serangan DoS pada Jaringan Cloud berdasarkan Generic Framework for Network Forensics (GFNF). *Edumatic: Jurnal Pendidikan Informatika*, *6*(2), 334–343. https://doi.org/10.29408/edumatic.v6i2.6466

Fatkhurozzi, M. (2021). Analisa Keamanan Website Menggunakan Metode Footprinting Dan Vulnerability Scanning Pada Website Kampus. *Prosiding Seminar Nasional Informatika Bela Negara*, *2* 125-131. https://doi.org/10.33005/santika.v2i0.74

Harnita. (2010). *Membangun Website Tanpa Modal: Mengunakan CMS Wordpress Beserta domain dan Hosting Gratis*. Wahana Komputer.

Helmiawan, M. A., Firmansyah, E., Fadil, I., Sofivan, Y., Mahardika, F., & Guntara, A. (2020, October). Analysis of Web Security Using Open Web Application Security Project 10. *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*. 1-5 https://doi.org/10.1109/CITSM50537.2020.9268856

Hermanto, H., & Haeruddin, H. (2022). Peningkatan Sistem Keamanan Website Menggunakan Metode OWASP. *Jurnal Ilmu Komputer Dan Bisnis*, *13*(1) 94-104. https://doi.org/10.47927/jikb.v13i1.277

Ita, S. F. N., Cut, B., & Sanusi. (2019). Uji Keamanan Website Terhadap Serangan Path Traversal Pada Website Pendataan Warga. *KANDIDAT*, *1*(1), 15–20.

Karli, K., Harvelian, A., Safitri, A. M., Wahyudi, A., & Pranacitra, R. (2023). Penyuluhan Pengabdian Hukum dalam Mengatasi Dampak Negatif Judi Online terhadap Kesejahteraan Buruh. *PUNDIMAS: Publikasi Kegiatan Abdimas*, *2*(2) 86-92. https://doi.org/10.37010/pnd.v2i2.1266

Laksmiati, D. (2022). Pengujian Optimasi Performa Website Menggunakan Cloudflare Dengan Metode Stress Test. *Akrab Juara : Jurnal Ilmu-Ilmu Sosial*, *7*(3) 261-272. https://doi.org/10.58487/akrabjuara.v7i3.1903

Makmur, T. (2019). Teknologi Informasi. *Info Bibliotheca: Jurnal Perpustakaan Dan Ilmu Informasi*, *1*(1). https://doi.org/10.24036/ib.v1i1.12

Purba, P. M., Amandha, A. C., Purnama, R. H., & Ikhwan, A. (2022). Analisis Keamanan Website Prodi Sistem Informasi Uinsu Menggunakan Metode Application Scanning. *Jurnal Informatika Teknologi dan Sains (Jinteks)*, *4*(4), 325-329. https://doi.org/10.51401/jinteks.v4i4.2065

Nguyen, T. D., & Nguyen, H. H. (2020). An Improving Way For Website Security Assessment. *REV Journal on Electronics and Communications*, *10*(1–2). https://doi.org/10.21553/rev-jec.239

Nuroji, N. (2023). Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan komputer sebagai pencegahan serangan Port-Scanning. *Journal of Data Science and Information System (DIMIS)*, *1*(2), 41–49. https://doi.org/10.58602/dimis.v1i2.44

Pratama, Z. P., Mappeasse, Muh. Y., & Purnamawati, P. (2023). Pengembangan Sistem Informasi Arsip Persuratan Berbasis Web pada Sekretariat Dewan Perwakilan Rakyat Daerah Kabupaten Dogiyai Provinsi Papua. *INTEC Journal: Information Technology Education Journal*, *2*(3), 57–62. https://doi.org/10.59562/intec.v2i3.576

Rahmadyanto, E. P., & Chandra, D. W. (2023). Analisis keamanan Content Delivery Network (CDN) Cloudflare (Studi kasus: Web Hakazon). *Jutisi: Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, *12*(3), 1818–1929.

Rizkiawan, M. A., Ramza, H., & Alim, E. S. (2023). Sistem Informasi Pencatatan Aset Dan Peminjaman Barang Menggunakan Metode Pengembangan Agile Pada Bpti Uhamka. *Journal of Scientech Research and Development*, *5*(2) 461-473. https://doi.org/10.56670/jsrd.v5i2.217

Shahid, J., Hameed, M. K., Javed, I. T., Qureshi, K. N., Ali, M., & Crespi, N. (2022). A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions. *Applied Sciences (Switzerland)*, *12*(8) 1-23. https://doi.org/10.3390/app12084077

Srivatanakul, T., & Annansingh, F. (2022). Incorporating active learning activities to the design and development of an undergraduate software and web security course. *Journal of Computers in Education*, *9*(1) 1-26. https://doi.org/10.1007/s40692-021-00194-9

Tania, A. M., Setiyadi, D., & Khasanah, F. N. (2018). Keamanan website menggunakan vulnerability assessment. *Informatics for Educators and Professionals*, *2*(2) 171-180.