VARIABLE RESEARCH JOURNAL
Volume 01, Number 01, April 2024
E-ISSN: 3032-4084
Open Access

ANALISA KEAMANAN WEBSITE TERHADAP SERANGAN HTML INJECTION MENGGUNAKAN METODE PENETRASION TESTING

WEBSITE SECURITY ANALYSIS AGAINST HTML INJECTION USING THE METHOD PENETRASION TESTING

M. Akil [1]*, Erick Irawadi Alwi[2], Syahrul Mubarak Abdullah[3]
[1,2,3] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia Makassar, Indonesia
Email: malikaqil23985@gmail.com

ARTICLE INFO

Article history:
Received January 20, 2024
Revised February 18, 2024
Accepted April 10, 2024
Available online April 15, 2024

Kata Kunci:
Keamanan Website, HTML Injection, Metode Penetrasion Testing

Keywords:
Website Security, HTML Injection, Penetrasion Testing Methods

ABSTRAK

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisa kerentanan HTML Injection pada website Jakarta Globe menggunakan metode Penetrasion Testing. Dalam penelitian ini terdapat beberapa tahap dalam pengumpulan data. Hasil dari analisa kerantanan yang sudah dilakukan menggunakan metode penetrasion testing terhadap domain https://jakartaglobe.id/ terdapat celah kerentanan diantaranya yaitu kode HTML Injeksi hanya mengizinkan injeksi tag HTML tertentu, ketika website tidak menangani data yang disediakan pengguna dengan benar, penyerang dapat memberikan kode HTML yang valid.

ABSTRACT

This research aims to identify and analyze HTML Injection vulnerabilities on the Jakarta Globe website using the Penetrasion Testing method. In this study there are several stages in data collection. The results of the vulnerability analysis that has been carried out using the penetrasion testing method on the https://jakartaglobe.id/ domain, there are vulnerabilities including the HTML Injection code only allows the injection of certain HTML tags, when the website does not handle the user-supplied data correctly, the attacker can provide valid HTML code.

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat saat ini, membuat teknologi berperan sangat penting dalam kehidupan sehari-hari, dengan adanya jaringan komputer kita dapat dengan mudah mengakses suatu informasi dan data. Di era saat ini hampir seluruh manusia mengandalkan jaringan komputer untuk menyimpan data dan informasi[13]. Khususnya website juga mengalami perkembangan. Website atau situs dapat diartikan sebagai kumpulan halaman-halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara, maupun interaktif memiliki keuntungan yang menghubungkan (link) dari dokumen dengan dokumen lainnya (hypertext) yang dapat diakses melalui browser[1].

Di era internet dan World Wide Web, keamanan sistem telah menjadi isu penting dalam informasi berbasis web global. Hal ini dapat dilihat dari komitmen yang kuat dari para profesional keamanan sistem, komunitas riset, dan vendor perangkat lunak[2]. Menurut laporan digital OWASP Top 10 adalah dokumen yang tersedia di situs web mereka. Laporan ini mencakup 10 resiko keamanan aplikasi web teratas yang diberi peringkat secara sistematis, dengan mempertimbangkan aspek-aspek tertentu seperti ukuran dampak, tingkat kerentanan, dan frekuensi kelemahan yang ditemukan. Seperti pada Gambar 1 serangan injeksi adalah kerentanan keamanan besar lainnya yang mungkin berlanjut pada tahun 2022. Kelemahan ini dapat menyebabkan kerusakan dan hasil yang tidak diinginkan [3].

Kini website telah menjadi sumber informasi untuk berbagai bidang dan kalangan. Sebagai sumber informasi terbuka sebuah website dengan mudah dapat diakses banyak orang. Untuk itu,

perkembangan dan pemilik situs gagal melindungi keamanan website dan sebagaian besar diabaikan oleh pengembang website dan komunitas keamanan[4]. Keamanan sebuah website merupakan hal yang penting, karena untuk melindungi informasi-informasi yang ada. Karena meski dapat di akses banyak orang, dalam sebuah website juga terdapat informasi penting yang harus di jaga seperti data pengguna, informasi pribadi dan sebagainya. Jika kemanan suatu website tidak diperhatikan vulnerability maka kerentanan tersebut dapat digunakan oleh pihak tidak bertanggung jawab untuk mengambil keuntungan [5].

Semakin bertambahnya peluang kejahatan siber. Seperti halnya kebocoran data yang berisikan informasi dari suatu website oleh oknum tak bertanggung jawab yang dapat merugikan banyak pihak. Kebocoran data atau perusakan dapat mengancam setiap saat seiring dengan meningkatnya sumber daya manusia. Perlu dilakukannya pengujian celah atau biasa disebut uji penetrasi keamanan terhadap website guna meminimalisir penjahat siber dapat menembus sistem keamanan yang sudah ada. Dengan adanya pengujian celah keamanan tersebut dapat menjadi sebuah solusi yang di gunakan sebagai tolak ukur untuk memperbaiki sistem keamanan website selanjutnya[6].

Website Jakarta Globe merupakan surat kabar harian Indonesia berbahasa Inggris. Harian ini diterbitkan mulai tanggal 12 November 2008, periode ini marak dengan tidak berhasilnya media cetak, akibat munculnya media internet. Website yang berdomain https://jakartaglobe.id yang memanfaatkan jaringan internet yaitu web, sebagai media dalam menyampaikan informasi surat kabar dalam bentuk website kepada masyarakat guna memudahkan dalam penyampaian informasi. Selain tampilan yang mudah digunakan, website harus memiliki keamanan yang tinggi agar terhindar dari kebocoran, manipulasi, pencurian data dan berpindahnya hak pengelolaan yang diakibatkan oleh pihak yang tidak bertanggung jawab. Website jakarta globe berfungsi untuk menyampaikan informasi kabar berita, maka dari itu keamanan yang diterapkan perlu diperhatikan. Dikhawatirkan meskipun bekerja secara optimal namun terdapat lubang-lubang kerentanan yang dapat dieksploitasi terhadap sistem yang digunakan, seperti serangan HTML Injection yang menyebabkan defacement virtual hingga pencurian data cookie. Dengan alasan yang telah dijelaskan maka penulis memutuskan dalam mengatasi masalah ini salah satu langkah yang dapat ditempuh adalah dengan melakukan analisis terhadap sistem keamanan pada Jakarta Globe dan telah di lakukan scanning yang hasil nya terdapat celah kerentanan HTML Injection.

Berdasarkan latar belakang yang telah diuraikan diatas, maka tujuan yang diharapkan tercapai dalam melakukan penelitian ini adalah mengidentifikasi dan menganalisa kerentanan *HTML Injection* pada *website* Jakarta Globe menggunakan metode *Penetrasion Testing.*

METODE

Penelitian ini menggunakan metode *penetrasion testing (*pentest). Dalam penelitian ini terdapat beberapa tahap dalam pengumpulan data. Tahapan yang dilakukan berupa pengumpulan dokumen seperti jurnal, buku, paper ilmiah, tugas akhir atau dari media digital seperti internet. Selain dari itu informasi juga didapatkan melalui hasil analisa website yang ber-subdomain https://jakartaglobe.id, dengan tahapan-tahapan yang ditetapkan bertujuan untuk mendapatkan informasi yang diperlukan dalam penyelesaian masalah. Adapun tahapan yang diterapkan dalam penelitian ini adalah sebagai berikut:

a. Scanning
   Tahap awal dalam melakukan idetinfikasi target yaitu dengan cara mengumpulkan segala bentuk informasi mengenai website berdomain https://jakartaglobe.id yang akan diuji oleh pentest dengan menggunakan tools Nikto dan Who.is untuk mendeteksi parameter dan menganalisa informasi yang ditemukan untuk mengidentifikasi kerentanan HTML Injection.
b. Vulnerability Analisi
   Setelah melakukan pengumpulan informasi pada tahap Scanning, selanjutnya melakukan analisis terhadap informasi yang telah dikumpulkan untuk mengidentifikasi kerentanan HTML Injection yang ada pada target dan menentukan metode serangan HTML Injection yang paling efektif.
c. Exploit
   Pada tahapan ini penulis setelah mendapatkan celah kerentanan HTML Injection, akan melakukan berbagai percobaan dan pengujian terhadap web berdomain https://jakartaglobe.id dengan menggunakan berbagai cara dan teknik mengeksploitasi kerentanan seperti Hackbar sebagai injeksi manual, berdasarkan informasi yang didapat dalam tahapan scanning, dan vulnerability analisis sebelumnya.
d. Reporting
   Setelah ditemukan ancaman atau serangan, maka selanjutnya adalah melakukan report dan merekomendasikan penanganan keamanan website tersebut sebagai hasil akhir analisis.

HASIL DAN PEMBAHASAN

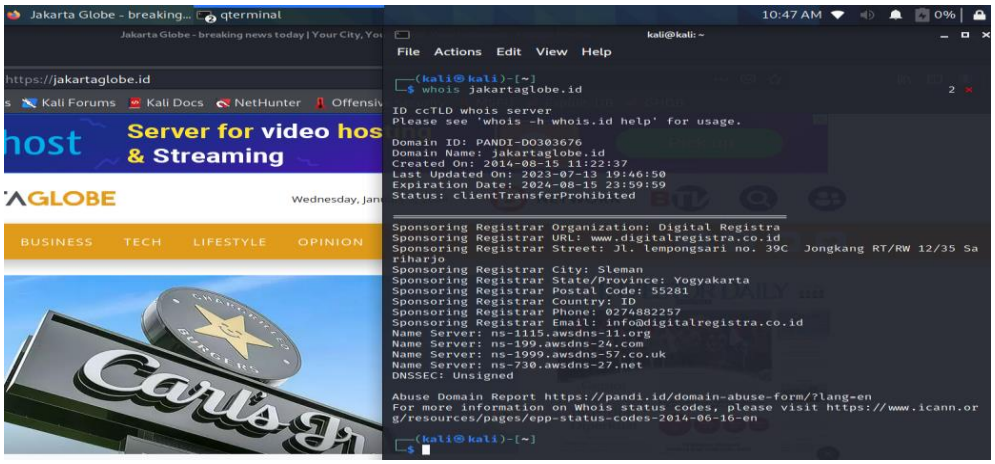
Hasil Penelitian

1. Identifikasi Masalah

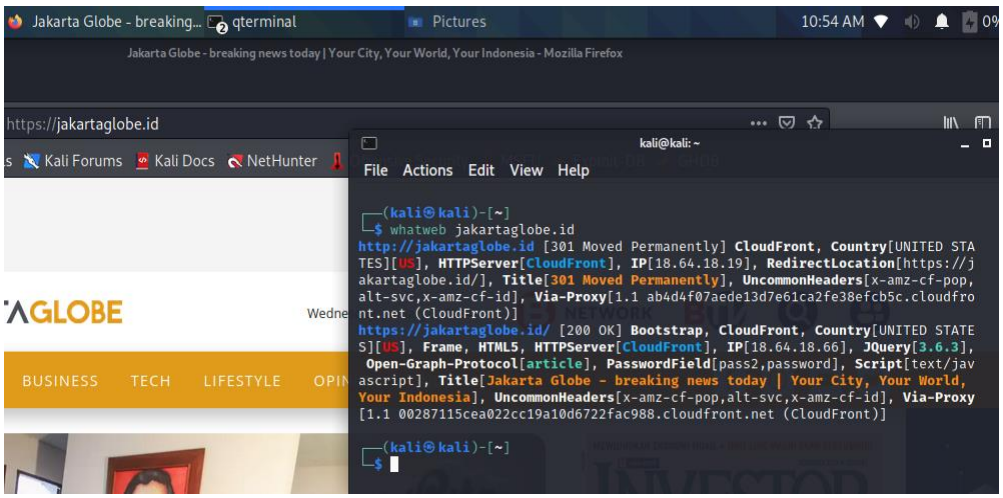
   Pada tahap ini, peneliti melakukan identifikasi terhadap masalah yang akan diteliti. Dalam penelitian ini, masalah yang diidentifikasi adalah kerentanan website terhadap serangan HTML Injection. Serangan HTML Injection merupakan salah satu jenis serangan web yang memanfaatkan celah keamanan pada aplikasi web untuk menyisipkan kode HTML berbahaya ke dalam halaman web. Kode berbahaya tersebut dapat digunakan untuk mencuri informasi pengguna, menyebarkan malware, atau mengarahkan pengguna ke situs web berbahaya.

2. Scanning

   Tahapan selanjutnya di lakukan proses Scanning antara lain untuk mengumpulkan segala bentuk informasi mengenai website, dari proses scanning yang telah dilakukan menggunakan tools who'is dan whatweb, memberikan informasi yang berisi tentang website yang berdomain https://jakartaglobe.id/ dan alamat Jl. Jend. Gatot Subroto kav. 35-36 Jakarta 12650, Indonesia. Kemudian infomasi teknologi yang digunakan oleh target, website JakartaGlobe dibuat dengan java scrip, framwork boostrap, html 5, nama server LiteSpeed, dan website ip 18.64.18.19. dapat dilihat pada gambar 7 dan 8.



Gambar 6. Proses Scanning Tools Who'is

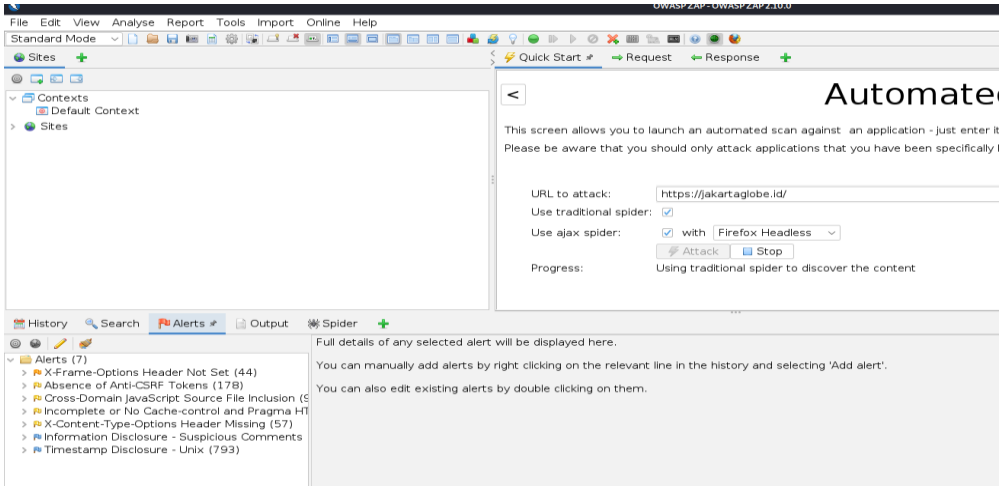


Gambar 7. Hasil Scanning dari Tools whatweb

3. Vulnerability Analisi

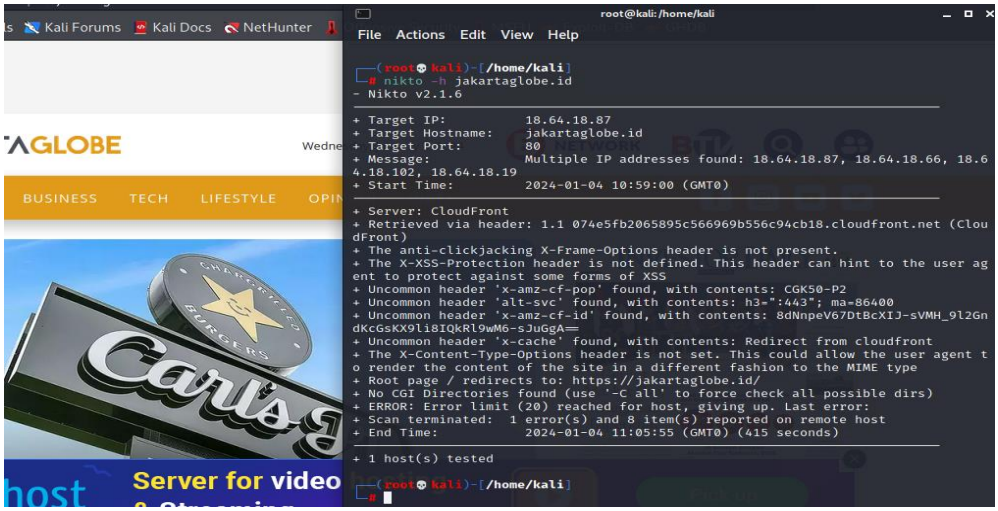
   Tahapan selanjutnya di lakukan proses scanning untuk menganalisa informasi kemungkinan celah keamanan yang ada pada website target, dari proses scanning yang telah dilakukan

menggunakan tools otomatisasi OWASPZap[19], memberikan informasi yang berisi alert kerentanan pada website terdiri dari X-Frame-Options Header, Absence of Anti-CSRF Tokens, Cross-Domain JavaScript Source File Inclusion, Incomplete or No Cache-Control and Pragma HTTP Header Set dan X-Content-Type-Options-Header Missing, terdapat celah keamanan berupa HTML Injection pada web target yang berdomain https://jakartaglobe.id/ yang level kerentanannya “Medium” di antara seperti pada Gambar 8.

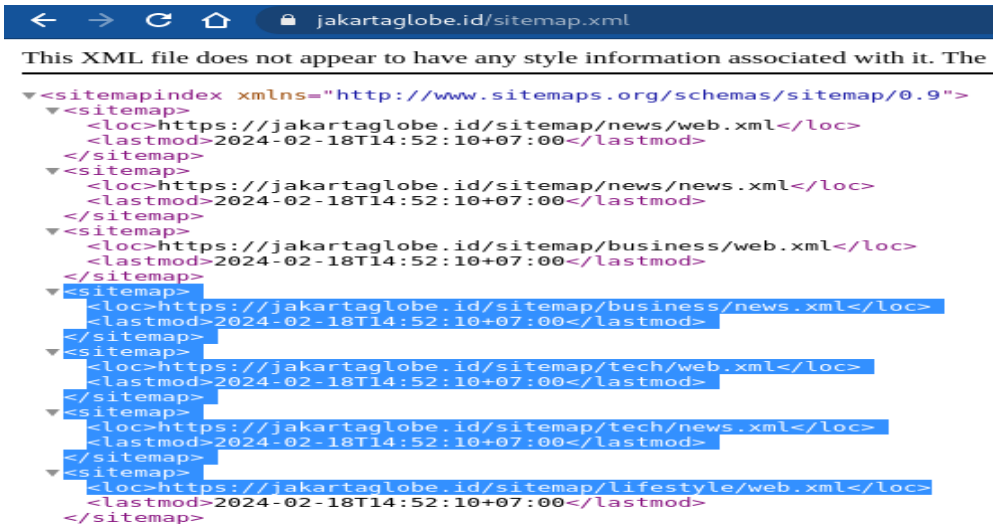


Gambar 8. Hasil Scanning dari Tools OwaspZap

Tahapan selanjutnya di lakukan scanning menggunakan tools Nikto untuk menganalisa celah keamanan yang memungkinkan menemukan berbagai jenis kerentanan, termasuk dapat menghasilkan laporan HTML dan XML.



Gambar 9. Proses Scanning menggunakan Tools NIKTO

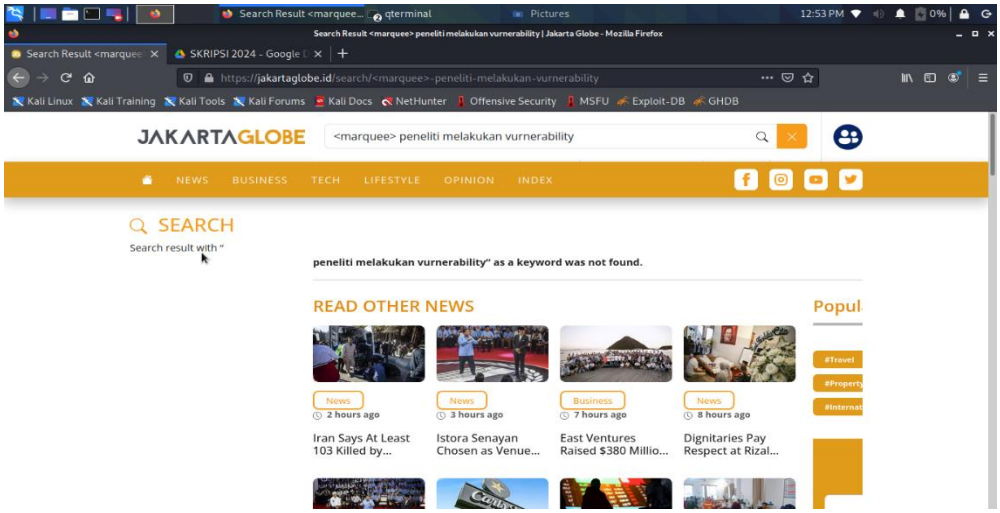


Gambar 10. Proses Scanning sitemap xml

Berdasarkan pada gambar 9 informasi yang diberikan dari tools NIKTO, bahwa adanya kesalahan pada headernya yang tidak di proteksi pada sisi clien sehingga penulis dapat menyisipkan kode berbahaya yang dapat merugikan website.

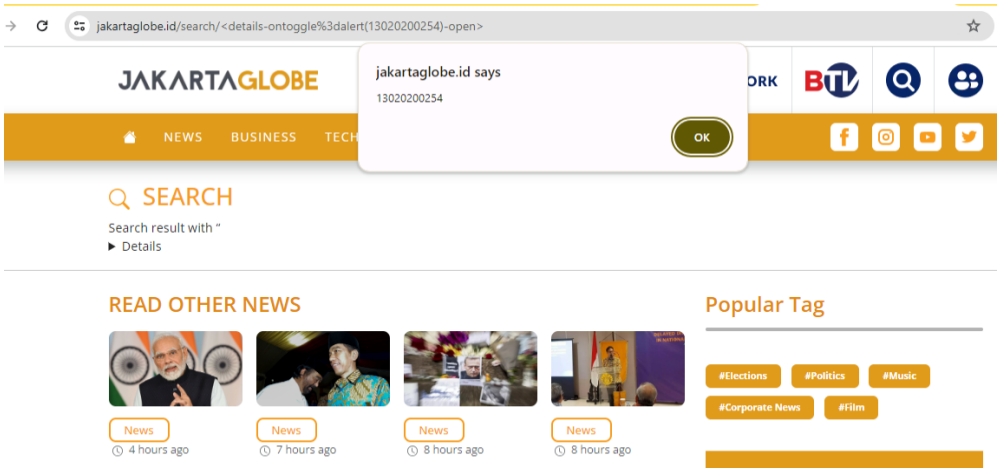
4. Eksploitasi

Tahapan exploitasi bertujuan untuk membuktikan bahwa celah kerentanan yang ditemukan pada tahapan vulnerability analisis, dapat digunakan untuk memanfaatkan celah keamanan yang diketahui berdasarkan informasi dari hasil scanning dengan tools OWASPZap dan NIKTO [20], ditemukan celah kerentanan X-Frame-Options Header, kerentanan ini biasanya berisi kerentanan HTML Injection, penyebab dari celah keamanan adalah kurangnya pemfilteran terhadap metakarakter yang memungkinkan untuk menyisipkan script berbahaya untuk di eksekusi pada website target menggunakan script kode HTML Injection. Kerentanan ini saya temukan pada barch search https://jakartaglobe.id. Dengan memanfaatkan input berita yang tidak ada di jakartaglobe. Sistem akan memberikan rekomendasi berita. Input user akan terefleksi pada pesan rekomendasi. Pada dasarnya sistem telah menfilter input yang bermuatan xss seperti javascript, onalert, onload, confirm dan sebagianya, namun tidak memfilter kode HTML lainnya. disajikan pada gambar 12 dan 13,14.

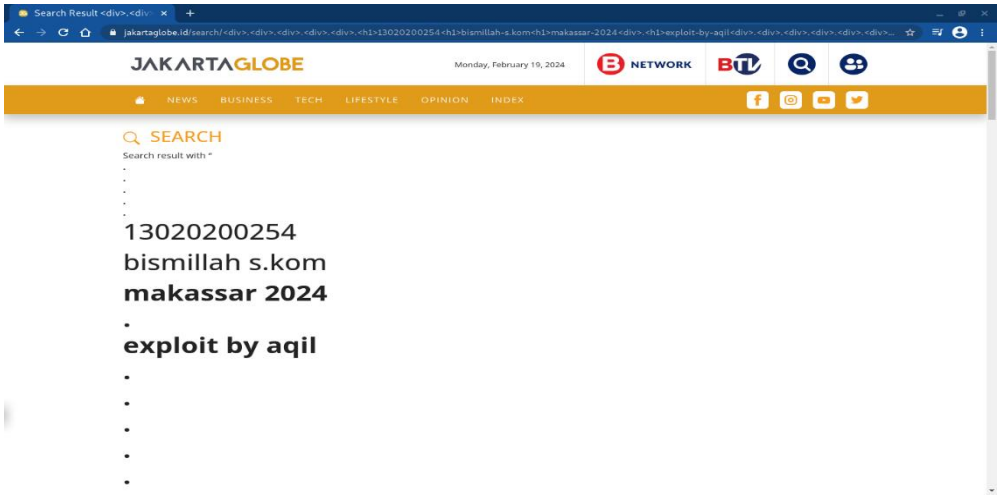


Gambar 11. Proses Injeksi serangan HTML Injection

Tahapan selanjutnya yaitu uji kemungkinan kerentanan serangan HTML Injection dilakukan secara manual yang memungkinkan menyisipkan kode script berbahaya untuk dieksekusi pada website target menggunakan kode injeksi HTML, di sajikan pada gambar 12,13.



Gambar 12. Proses Injeksi serangan HTML Injection

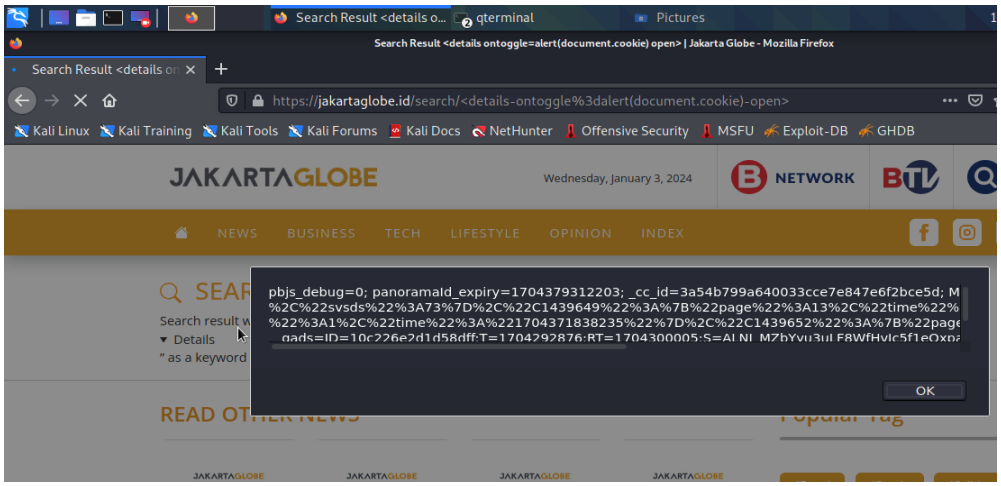


Gambar 13. Proses Injeksi Serangan HTML Injection

Dari gambar 12 dan 13 terlihat kode injeksi HTML yang di suntikkan berhasil, penulis menampilkan Nim dan nama di tampilan website yang ada pada gambar.

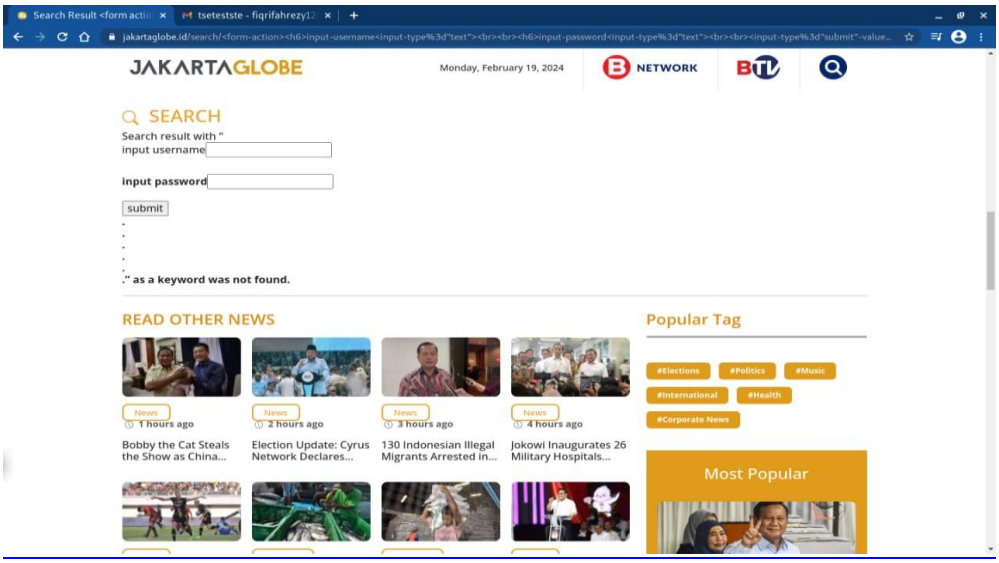
Proses selanjutnya yaitu uji kemungkinan kerentanan serangan pencurian data cookie berupa file kecil yang dibuat oleh situs web yang anda kunjungi dan di simpan di komputer anda. yaitu dengan menyuntikkan kode berbahaya ke situs web yang sah. Ketika pengguna mengunjungi situs web yang terinfeksi HTML Injection. seperti pada Gambar 14.

Gambar 14. Proses Injeksi serangan HTML Injection



Gambar 15. Proses Injeksi pencurian cookie

Pada tahap ini contoh proses injeksi HTML pada halaman web yang sederhana dengan dua form input ketika diklik, halaman akan meminta kita untuk memasukkan namakita, dan kemudian akan terinput. Jika tidak ada sanitasi masukan yang diterapkan, hal ini berpotensi menjadi sasaran yang mudah untuk serangan Injeksi HTML.



Gambar 16. Proses Injeksi serangan HTML Injection

Pembahasan

Hasil dari analisa kerantanan yang sudah dilakukan menggunakan metode penetrasion testing terhadap domain https://jakartaglobe.id/ terdapat celah kerentanan diantaranya yaitu kode HTML Injeksi hanya mengizinkan injeksi tag HTML tertentu, ketika website tidak menangani data yang disediakan pengguna dengan benar, penyerang dapat memberikan kode HTML yang valid. Serangan ini dapat di sisipkan dan dieksekusi pada kolom pencarian (bar search), biasanya melalui nilai parameter, dampak dari pengujian tersebut adalah defacing halaman web. Hal ini melibatkan menyisipkan kode HTML baru untuk mengubah tampilan halaman web, bahkan mengubah seluruh halaman. Jenis serangan ini dapat menyebabkan kerusakan reputasi yang parah bagi perusahaan yang menjalankan aplikasi web tersebut. Berdasarkan framework OWASP yang mencantumkan kerentanan dengan tingkat keparahan medium dapat dilihat pada tabel 4.

Kerentanan Website JakartaGlobe			
Jenis	URL	Risk	Condifence
X-Frame-Options Header Not Set	https://jakartaglobe.id/	Medium	Medium
Absence Of Anti-CSRF Tokens	https://jakartaglobe.id/	Low	Medium
Cross-Domain JavaScript Source File Inclusion	https://jakartaglobe.id/	Low	Medium
Incomplete or No Cache-Control and Pragma HTTP Header Set	https://jakartaglobe.id/	Low	Medium
X-Content-Type-Options-Header Missing	https://jakartaglobe.id/	Low	Medium

Tabel 4. Kerentanan Website JakartaGlobe

Proses pengujian keamanan website didapatkan beberapa celah yang mendeteksi 5 sub file vulnerability dengan status low dan medium. Dari hasil tersebut diberikan rekomendasi pengelola website melakukan konfigurasi ulang file vulnerability untuk meningkatkan keamanan website. selain itu pengelola secara terus menerus melakukan peningkatan keamanan website ke jenjang yang lebih tinggi, agar tidak ada serangan yang akan datang nantinya. Berikut adalah penjelasan singkat tentang kerentanan, resiko, dan rekomendasi yang di temukan berdasarkan framework OWASP Top 10 vulnerability pada Tabel 5.

Tabel 5. jenis kerentanan

No	Jenis Kerentanan	Resiko	Rekomendasi
1	Injection	Kerentanan ini terjadi ketika aplikasi tidak memvalidasi atau memfilter input pengguna dengan benar dan memungkinkan injeksi kode HTML jahat. Serangan injeksi HTML yaitu dapat merusak deface-mengubah konten halaman yang terlihat. Misalnya mungkin menggunakan injeksi HTML yang disimpan untuk memasukkan iklan visual, juga dapat memasukkan kode HTML berbahaya yang bertujuan merusak reputasi halaman website, misalnya karena alasan politik atau pribadi.	Untuk mengatasi kerentanan injeksi HTML, lakukan validasi dan sanitasi input pengguna,gunakan encoding UTF-8 dan atur Content-Type header dengan benar, perbarui perangkat lunak, lakukan pengujian keamanan rutin dan terapkan mekanisme pertahanan XSS seperti CSP, X-XSS-Protetion Header, dan filter XSS.

KESIMPULAN

Penelitian tentang Analisa keamanan Website terhadap serangan HTML Injection telah selesai dilakukan. Proses analisa website JakartaGlobe dengan beberapa kegiatan, yakni scanning, vulnerability analisis dan exploitasi. Telah berhasil dilakukan analisa dan pengujian keamanan pada domain web JakartaGlobe menggunakan beberapa tools di antaranya NIKTO, OWASPZap terhadap serangan luar oleh orang yang tidak bertanggung jawab yang dapat merugikan JakartaGlobe.

DAFTAR PUSTAKA

[1] Rusdiana,B. C. S., 2019. Analisa Keamanan Website Terhadap Serangan Cross-Site Request Forgery (CSRF). Cross-Site Request Forgery (CSRF), Volume 1, pp. 21-29.

[2] K. A. Sedek, N. Osman, M. N. Osman, and H. K. Jusoff, “Developing a Secure Web Application Using OWASP Guidelines,” Comput. Inf. Sci., 2009, doi: 10.5539/cis.v2n4p137.

[3] Testbytes, “What is OWASP? Top 10 OWASP Vulnerabilities,”2020. https://www.testbytes.net/what-is-owasp-top-vulnerabilities/ (accessed Sep. 18, 2021).

[4] Chen, C., Mitchell, C.J. and Tang, S. (2013). Ubiquitos one-time password service using the Generic Authentication Architecture. Mobile Networks and Application, 18(5). pp.738-747.

[5] Kamilah, I., Ritzkal & Hendrawan, A. H., 2019. Analisa Keamanan Vulnerability pada server absensi kehadiran laboratorium di program studi teknik informatika. Seminar nasional sains dan teknologi.

[6] Rosaliah, Y. T. A., Jayanta, J., & Hananto, B. (2021). Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx. In Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya (Vol. 2, No. 2, pp. 752-761).

[7] Erlangga, M. F. E. (2021). Analisa Celah Keamanan Dalam Pengembangan Website E-Commerce (Studi Kasus: Mataharimu. Com). Computing Insight: Journal of Computer Science, 3(2), 20-27

[8] Bhatia, B., & Sharma, C. “An Effective Implementation of HTML Injection”.

[9] J. T. Elektro and P. N. Medan, “Perancangan Website pada PT Ratu Enim Palembang,” pp. 15-27

[10] Sucuri, “Website Security: How to Secure & Protect Your Website,” sucuri.net, 2019.

[11] Shella, “Apa Itu Web Security? Tips Untuk Melindungi Website dari Serangan Hacker,” IDS Digital College, 2020.

[12] Andria, “Analisa Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux,” Gener.j., vol. 4, no. 2, pp.69-79, 2020.

[13] Ilham, Karina Fitriwulandari Ilham, Erick Irawadi Alwi, and Farniwati Fattah. "Penerapan dan Analisis Network Security Snort Menggunakan Intrusion Detection System pada Serangan UDP Flood." INFORMAL: Informatics Journal 8.1 (2023): 94-100.

[14] N. Nunung. “Distribusi gamma.Distribusi Gamma”. 2012

[15] Fathur, Muhammad. “Tanggung jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen, 2(1), 43-60”. 2020.

[16] Juardi, D. (2017). Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus. Syntax Jurnal Informatika, 6(1).

[17] Dirgahayu, T., Prayudi, Y., & Fajaryanto, A. “Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server”. Jurnal Ilmiah NERO, 1(3), 190-197. 2015.

[18] Mulyanto, Yudi, et al. "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)." Journal of Information System Research (JOSH) 4.1 (2022): 202-209.

[19] Pratama, E., & Wiradarma, A. “Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study : X Company)”.2019.