

PEMBERIAN DUKUNGAN TEKNIS DAN REKOMENDASI PADA PENANGANAN PERETASAN WEBSITE STIKES JAYAPURA

Evanita Veronica Manullang^{1*}, Marla Sheilamita Shalin Pieter¹

¹Teknik Informatika, Universitas Sains dan Teknologi Jayapura

Padang Bulan, Abepura, Jayapura, Papua

e-mail: ^{1*}eva.manullang@gmail.com, ²marlasheila.pieter@gmail.com

Abstrak

Website kampus merupakan asset penting karena dapat menjadi media untuk menyampaikan informasi kepada publik. Penggunaan website juga bukan hanya sekedar menjadi media informasi namun sudah banyak dikembangkan agar dapat memberikan layanan bagi pengguna public, contohnya bagi kampus yaitu penerimaan mahasiswa baru, registrasi ulang mahasiswa dan berbagai aplikasi yang diharapkan akan meningkatkan pelayanan yang diberikan oleh kampus tersebut. Namun peningkatan penggunaan teknologi ini diiringi juga dengan peningkatan kejahatan siber. Salah satu kampus di Jayapura yaitu STIKES Jayapura mengalami peretasan website yang dilakukan oleh peretas yang menamakan diri mereka Kalimalang BlackHat Team. Metode yang akan digunakan untuk mengatasi permasalahan tersebut yaitu dengan melakukan proses pemeriksaan atau pencekan pada semua asset yang berkenaan dengan website seperti server, kode program dan pengguna website, melakukan analisa celah keamanan website dari hasil proses pemeriksaan yang dilakukan, serta memberikan rekomendasi perbaikan yang harus dilakukan. Oleh karena masalah tersebut, pengabdian yang dilakukan saat ini yaitu melakukan analisis celah keamanan website untuk menemukan pintu masuk serangan dan juga memberikan rekomendasi perbaikan yang harus dilakukan sehingga tidak terjadi serangan yang sama dikemudian hari. Hasil yang diperoleh yaitu ditemukan celah keamanan pada kode program yang digunakan untuk membangun website sehingga terjadi serangan xss (cross site scripting) dan perlu dilakukan perbaikan pada website yang ada saat ini. Rekomendasi yang diberikan dapat digunakan oleh pihak Mitra agar lebih teliti dalam memilih partner untuk membuat aplikasi, serta mendapatkan pemahaman baru berkaitan dengan keamanan website dan penanganannya sehingga tidak akan terulang dikemudian hari, serta rekomendasi yang diberikan dapat dijadikan dasar untuk melakukan perbaikan website.

Kata kunci: keamanan website, kalimalang blackhat, xss

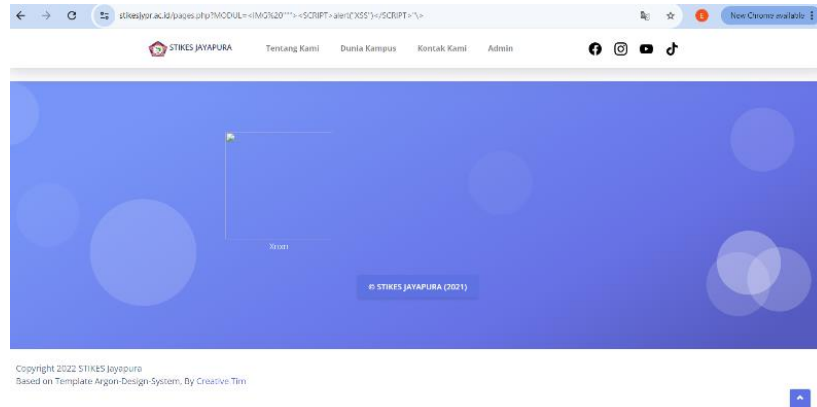
I. Pendahuluan

Industri 4.0 atau Revolusi Industri Keempat merupakan istilah umum yang digunakan untuk tingkatan perkembangan industri teknologi di Dunia. Pada tingkatan keempat ini, dunia fokus kepada teknologi yang bersifat digital, oleh karena itu teknologi informasi sangat menjadi tumpuan untuk industri guna mempermudah dan mempercepat berbagai proses termasuk informasi. Perubahan yang sangat cepat terkadang meluputkan developer dalam melakukan pengujian terhadap aplikasi yang dibangun [1].

STIKES Jayapura merupakan kampus yang membidangi bidang-bidang Kesehatan. Untuk meningkatkan pelayanan kepada mahasiswa dan masyarakat, STIKES Jayapura memanfaatkan teknologi website sebagai media penyampaian informasi. Website yang ada saat ini telah mengalami dua kali serangan yang sama dimana peretas yang mengatasnamakan diri mereka kalimalang blackhat team melakukan perubahan pada gambar dan informasi yang muncul pada halaman utama website dan beberapa halaman lainnya dengan gambar yang disiapkan oleh peretas. STIKES Jayapura juga tidak hanya menggunakan website sebagai media informasi,

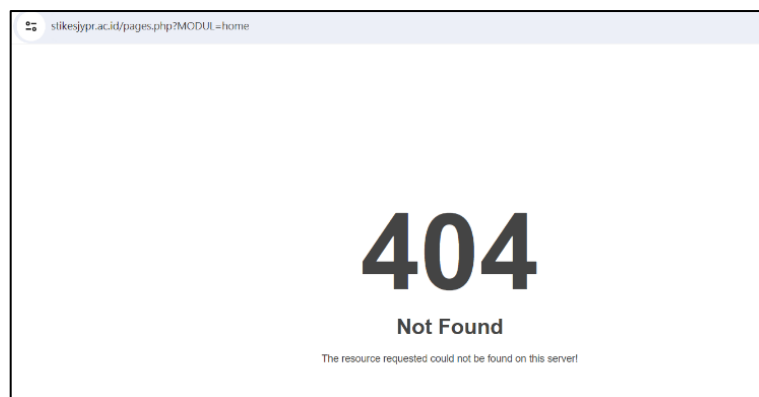
namun terdapat beberapa aplikasi website lain yang tidak dapat disebutkan dalam tulisan ini karena bersifat rahasia.

Website dan aplikasi yang digunakan ditujukan untuk memberikan pelayanan yang cepat namun sejak terjadi serangan, website tidak dapat digunakan lagi. Awalnya serangan dilakukan dengan menginjeksi kode program kemudian berlanjut hingga website tidak dapat diakses.



Gambar 1. Tampilan website saat terjadi serangan

Saat server mendeteksi adanya serangan pada website, khususnya melalui injeksi kode atau dikenal dengan istilah Cross-Site Scripting atau XSS maka server akan melakukan pemblokiran [2] agar tidak terjadi proses injeksi yang lebih serius sehingga membahayakan server. Akibat pemblokiran yang terjadi maka website tidak dapat diakses seperti terlihat pada Gambar 2.



Gambar 2. Tampilan website terakhir

Peretasan website tentunya sangat mengganggu dan menimbulkan kerugian bagi Kampus STIKES Jayapura, dimana Masyarakat tidak dapat mengakses kebutuhan informasi seperti penerimaan mahasiswa baru, dan informasi lainnya.

2. METODE PENGABDIAN

Metode pengabdian yang dilakukan yaitu:

1. Melakukan pengecekan pada semua aset yang terhubung dengan website seperti server, kode program dan pengguna website.
2. Melakukan analisa celah keamanan website dari hasil pengecekan yang telah dilakukan.
3. Memberikan rekomendasi perbaikan yang harus dilakukan.

Kegiatan pengabdian ini dilakukan secara online dan tertutup karena berhubungan dengan kerahasiaan data dan informasi, termasuk informasi yang dapat dibagikan dalam tulisan ini. Standar uji yang dilakukan berdasarkan standar yang diperoleh dari website *Open Worldwide Application Security Project (OWASP)* pada alamat <https://owasp.org/www-community/attacks/xss/> dan menggunakan berbagai informasi dari penelitian-penelitian yang telah dilakukan sebelumnya.

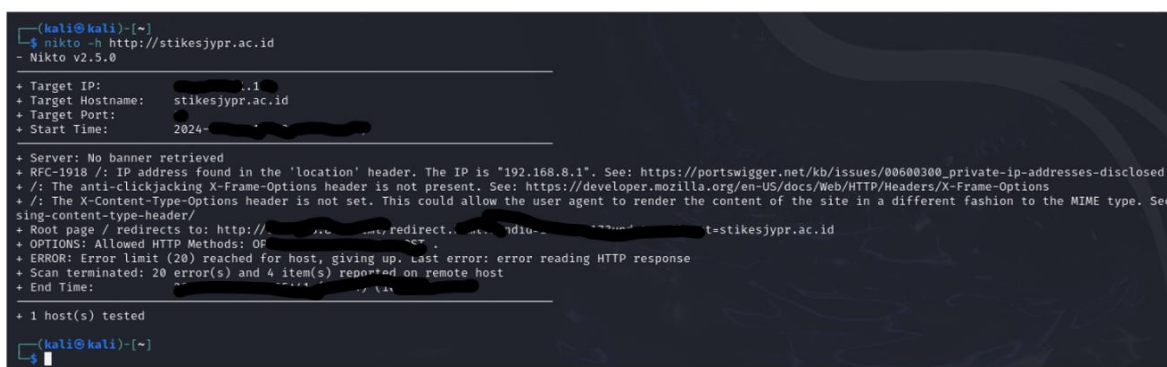
Tabel 1. Jadwal Kegiatan

| No | Kegiatan | Waktu |
|----|--|------------------|
| 1 | Menerima surat permintaan bantuan teknis analisis celah keamanan | 8 Mei 2024 |
| 2 | Melakukan pengecekan website | 9 Mei 2024 |
| 3 | Melakukan pengecekan server | 10 – 11 Mei 2024 |
| 4 | Mencari penelitian dengan kasus yang sama | 13 – 15 Mei 2024 |
| 5 | Melakukan diskusi guna menemukan permasalahan lain yang memungkinkan adanya pemicu peretasan | 16 – 18 Mei 2024 |
| 6 | Melakukan pengecekan ulang, analisis, diskusi dan perumusan permasalahan utama pada website | 20 – 22 Mei 2024 |
| 7 | Penyusunan Laporan Rekomendasi | 23 Mei 2024 |
| 8 | Penyerahan Rekomendasi | 24 Mei 2024 |

3. HASIL DAN PEMBAHASAN

Berdasarkan metode pengabdian yang telah disebutkan sebelumnya, tahapan pertama yang dilakukan yaitu dengan melakukan pendampingan pengecekan berbagai aset yang ada. Setelah melakukan pengecekan pada server dengan melihat log server (data log bersifat rahasia), hasilnya tidak ditemukan anomali sehingga dapat dinyatakan aman. Sedangkan saat melakukan pengecekan pada kode dan pengguna ditemukan beberapa celah keamanan pada bagian header sehingga terjadi serangan.

Pengecekan atau proses pemeriksaan dilakukan dengan menggunakan berbagai *tools* sehingga dapat dilakukan validasi hasil pemeriksaan keamanan dengan akurat. Untuk *tools* pertama yang digunakan adalah nikto dan menggunakan sistem operasi kali linux. *Tools* nikto pada kali linux merupakan *tools* yang khusus digunakan untuk melakukan pemeriksaan kerentanan pada website [3]. Hasil pemeriksaan atau pengecekan ditunjukkan pada Gambar 3.



```
(kali@kali)-[~]
└─$ nikto -h http://stikesjypr.ac.id
- Nikto v2.5.0

+ Target IP: 192.168.8.1
+ Target Hostname: stikesjypr.ac.id
+ Target Port: 80
+ Start Time: 2024-05-08 10:10:10

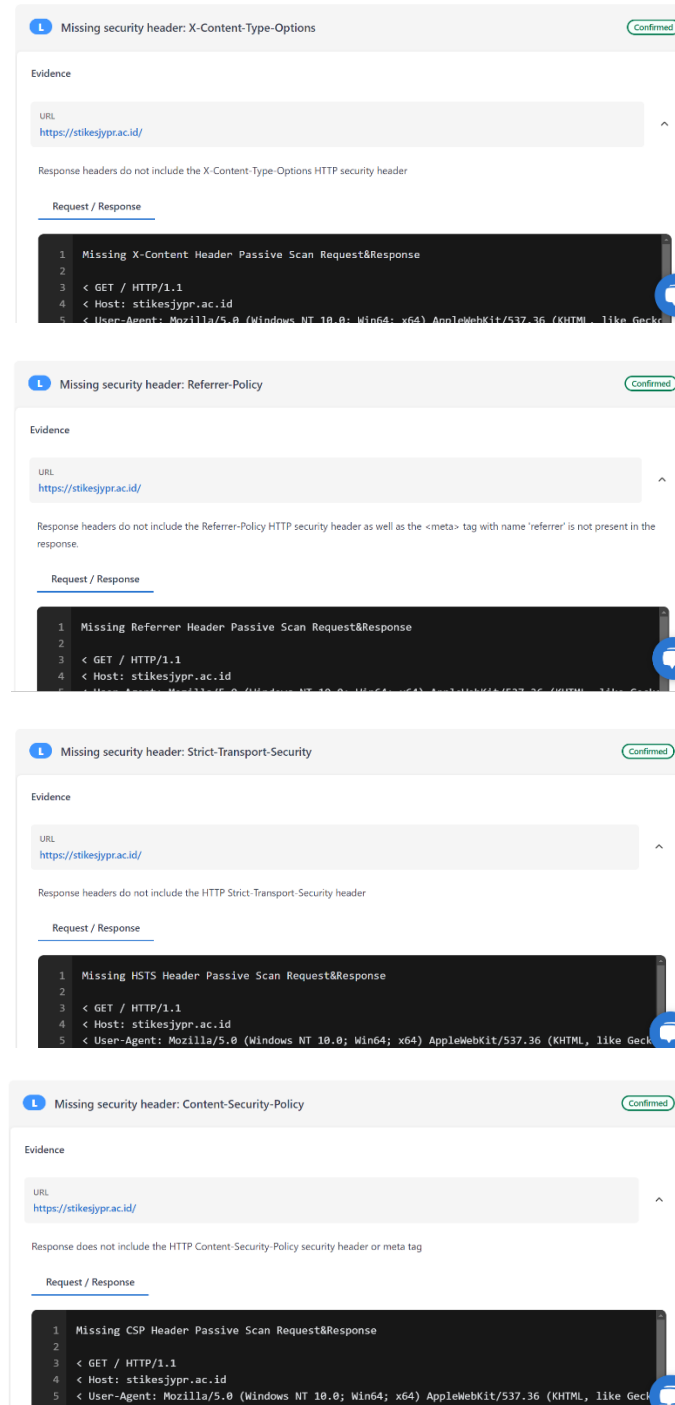
+ Server: No banner retrieved
+ RFC-1918 /: IP address found in the 'location' header. The IP is "192.168.8.1". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See https://owasp.org/www-community/attacks/xss/
+ Root page / redirects to: http://stikesjypr.ac.id
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, PATCH, OPTIONS
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time: 2024-05-08 10:10:10

+ 1 host(s) tested

(kali@kali)-[~]
```

Gambar 3. Hasil pengujian *tools* nikto kali linux

Proses pengecekan tahap kedua dilakukan dengan menggunakan *tools penetrasi testing* yang terdapat pada website <https://owasp.org/> dan hasil yang diperoleh ditunjukkan seperti pada Gambar 4.



Gambar 4. Hasil Pengecekan *tools penetrasi testing*

Kedua tools yang digunakan untuk melakukan pengecekan menunjukkan hasil :
Tools Nikto : The anti-clickjacking X-Frame-Options header is not present.
Tools Nikto : The X-Content-Type-Options header is not set.
Tools Pentest : Missing security header : X-Content-Type-Options

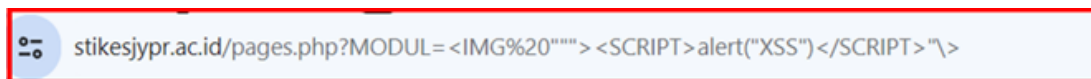
Corresponding Author: eva.manullang@gmail.com *

Received on: Mei 2024 , Accepted on : Juni 2024

Tools Pentest : Missing security header : Refferer-Policy
Tools Pentest : Missing security header : Strict-Transport-Security
Tools Pentest : Missing security header : Content-Security-Policy

Berdasarkan hasil yang dimunculkan oleh kedua *tools* yang digunakan dapat disimpulkan bahwa terdapat kelemahan pada pengaturan “header” website yang mengakibatkan website dapat diinjeksi dengan script berbahaya seperti xss script. Hal ini dapat dilihat pada hasil pengecekan pada Gambar 4 dan Gambar 5 dimana semuanya menerangkan bahwa belum adanya pengamanan yang baik pada header website. Serangan xss dianggap sepele oleh sebagian pihak, namun serangan ini tetap berbahaya untuk sebuah website[4].

Celah yang ditemukan mudah diserang dengan *HTML Malicious Tag*[5] seperti yang ditunjukkan pada Gambar 5.



Gambar 5. Header yang disusupi *HTML Malicious Tag*

Adapun rekomendasi yang telah diberikan agar digunakan sebagai dasar untuk melakukan perbaikan antara lain :

1. Memastikan software baik cms, plugin dan berbagai kode sumber yang digunakan untuk membuat website selalu diperbaharui dan melakukan perbaikan pada bagian header website.
2. Mengimplementasikan protokol https pada situs yang digunakan. [6]
3. Mengurangi ketergantungan kode sumber eksternal yang sudah usang.
4. Membuat jadwal rutin untuk *maintenance* website.

4. Simpulan

Kegiatan pengabdian ini sangat bermanfaat bagi mitra dikarenakan maraknya kejahatan siber saat ini yang telah mengakibatkan lumpuhnya website mitra dan sudah terjadi dua kali dengan jenis serangan yang sama. Hasil pengabdian masyarakat yang telah dilakukan oleh tim berupa penjelasan teknis terkait kondisi website, server dan hal-hal apa saja yang membuat website dapat diserang. Hasil dokumen rekomendasi untuk setiap celah keamanan yang ditemukan juga telah diserahkan kepada pihak mitra yang dapat dijadikan dasar untuk melakukan perbaikan. Tindak lanjut dari rekomendasi yang diberikan sangat perlu dilakukan dan diharapkan dapat menjadi pondasi untuk peningkatan keamanan berbagai aset digital yang dimiliki oleh mitra.

5. Saran

Saran yang dapat diberikan untuk pengembangan pengabdian di kemudian hari yaitu pihak mitra dapat menjalin Kerjasama dengan Kampus USTJ secara khusus Fakultas Ilmu Komputer sehingga dapat dilakukan kegiatan pengabdian secara rutin dan memberikan dampak positif bagi mitra di kemudian hari.

6. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada pihak mitra yakni Ketua STIKES Jayapura Ibu Efytaningrum Dwi Wahyu Astutik, M.Tr.Keb yang telah memberikan kepercayaan kepada USTJ dalam memberikan dukungan teknis pada permasalahan yang dihadapi, Rektor Universitas Sains dan Teknologi Jayapura Ibu Dr. Yuyun N. Ali Kastella, M.Pd, dan Bapak Dr. Ir. Jusuf Haurissa, M.T selaku Kepala Pengelola Jurnal Pengabdian Masyarakat USTJ yang telah memberikan dukungan terhadap keberhasilan pengabdian dan terbitnya publikasi hasil pengabdian ini.

7. Daftar Pustaka

- [1] A. Zirwan, "Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner," *Jurnal Informasi dan Teknologi*, pp. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.
- [2] S. E. Prasetyo, H. Haeruddin, and K. Ariesryo, "Website Security System from Denial of Service attacks, SQL Injection, Cross Site Scripting using Web Application Firewall," *Antivirus : Jurnal Ilmiah Teknik Informatika*, vol. 18, no. 1, pp. 27–36, May 2024, doi: 10.35457/antivirus.v18i1.3339.
- [3] "Vulnerability Assessment pada Website Rekrutasi Asisten (IRIS) Fakultas Rekayasa Industri menggunakan Nikto dan Nessus."
- [4] A. Wira Utama and A. Senja Fitriani, "Techniques For Testing Website Security Using The Escaping Metacharacter Method Teknik Menguji Keamanan Website Dengan Menggunakan Metode Escaping Metacharacter," 2022.
- [5] Brij B. Gupta and Pooja Chaudhary, *Cross-Site Scripting Attacks: Classification, Attack, and Countermeasures*. Boca Raton: CRC Press, 2020.
- [6] G. T. A. Ramadhani, M. R. R. Steyer, M. H. Maulidan, and A. Setiawan, "Analisis Kerentanan WordPress dengan WPScan dan Teknik Mitigasi," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 15, Jun. 2024, doi: 10.47134/pjese.v1i4.2613.