ANALISIS KERENTANAN *WEBSITE* SMP NEGERI 3 SEMARAPURA MENGGUNAKAN METODE PENGUJIAN *RATE LIMITING* DAN OWASP

Desi Dwi Cahyani[1,] *, Luh Putu Windy Puspita Dewi[2], Kadek Dika Rama Suryadi[3], I Made Edy Listartha[4]

[1,2,3,4] Prodi Sistem Informasi Jurusan Teknik Informatika Fakultas Teknik dan Kejuruan Universitas Pendidikan Ganesha, Jln. Udayana No. 11 Singaraja 81116 INDONESIA

Abstrak

Sistem informasi saat ini memiliki peranan yang sangat penting baik dalam membantu tercapainya pembelajaran yang dilaksanakan secara daring ataupun memberikan informasi sekolah kepada siswa-siswi dan masyarakat. Hal ini menjadi dasar bagi SMPN 3 Semarapura untuk membangun sebuah sistem informasi berbasis *website*. *Website* yang menampilkan informasi seperti ini tidak boleh memiliki kerentanan, karena informasi yang dimiliki dapat di rubah atau menjadi jembatan perantara ke sistem lain untuk tujuan yang tidak baik. Pengujian yang dilakukan pada *website* ini adalah *rate limitting* dan XSS. Pengujian ini memanfaatkan aplikasi OWASP ZAP dalam melakukan analisis. Hasil analisis ini menyimpulkan bahwa *website* tidak memiliki kedua kerentanan yang diujikan.

Kata Kunci:
Rate limiting, xss, owasp zap, penetration testing

Abstract

Information systems currently have a very important role both in helping to achieve online learning or providing school information to students and the community. This became the basis for SMPN 3 Semarapura to build a website-based information system. Websites that display information like this should not have vulnerabilities, because the information held can be changed or become an intermediary bridge to other systems for bad purposes. The tests carried out on this website are rate limiting and XSS. This test utilizes the OWASP ZAP application in conducting the analysis. The results of this analysis conclude that the website does not have both vulnerabilities tested.

Keywords:
Rate limiting, xss, owasp zap, penetration testing

1. PENDAHULUAN

Saat ini penggunaan internet dan sistem informasi semakin bertambah dengan pesat namun hal tersebut tidak diimbangi dengan adanya sumber daya manusia atau administrator jaringan yang ahli dengan bidangnya, sehingga risiko ancaman - ancaman tindak kejahatan *cyber* akan muncul(Listartha, Arna, Saskara, Gede, & Santyadiputra, 2021). Oleh dari itu dibutuhkan sumber daya manusia atau administrator yang Handal di bidangnya untuk menjaga keamanan data serta informasi yang ada di dalam sistem. Keamanan sistem informasi sangat penting karena hal ini berkaitan dengan data pribadi, hak akses, integritas, kerahasiaan dan ketersediaan.

Sistem informasi saat ini memiliki peranan yang sangat penting baik dalam membantu tercapainya pembelajaran yang dilaksanakan secara daring ataupun memberikan informasi sekolah kepada siswa-siswi dan masyarakat, khususnya Sekolah Menengah Pertama Negeri (SMPN) 3 Semarapura. *Website* SMP Negeri 3 Semarapura memberikan informasi kepada masyarakat umum dan siswa - siswi mengenai SMP Negeri 3 Semarapura yakni mengenai informasi umum sekolah, visi, misi, tujuan, struktur organisasi, agenda kegiatan-kegiatan di sekolah, jumlah guru dan staf tata usaha serta jumlah siswa aktif di SMP Negeri 3 Semarapura.

Informasi yang dimiliki ini harus dapat dijaga integritas dan ketersediaannya, sehingga perlu dilakukan pengujian secara berkala untuk mengetahui lebih cepat akan yang dimiliki. Ada dua kerentanan yang dianalisis yaitu *rate limiting* dan XSS. Kerentanan *rate limiting* akan memberikan resiko adanya *request* yang berlebihan pada suatu fungsi yang harusnya dibatasi. Kemudian kerentanan XSS yang memungkinankan melakukan injeksi kode berbahaya pada sistem, terlebih lagi kerentanan ijeksi ini merupakan rangking pertama pada OWASP Top 10.

Dengan demikian penulis melakukan analisis terhadap *Website* SMP Negeri 3 Semarapura dengan tujuan untuk menguji apa saja kerentanan yang terdapat pada *Website* SMP Negeri 3 Semarapura dan tingkat risiko dalam menentukan dampak yang dihasilkan dari analisa kerentanan agar terhindar dari adanya risiko ancaman tindak kejahatan *cyber*. Penilaian tingkat risiko kerentanan keamanan *Website* ini diuji dengan menggunakan aplikasi OWASP ZAP(The OWASP *Foundation*, 2018). Hasil dari analisa kerentanan ini dapat membantu pengembang serta pengelola sistem untuk mencegah dan mengatasi dampak risiko yang ditemukan pada sistem.

2. METODE

Penelitian ini menggunakan metode pengujian *Rate limiting*, *Payload* XSS, OWSAP (Open Web *Application Security Project*) sebagai kerangka acuan untuk menganalisis kerentanan yang dimiliki oleh *Website* SMP Negeri 3 Semarapura.

A. *Rate limiting*

Rate limit yaitu jumlah akses suatu *endpoint* dalam sebuah aplikasi dalam waktu tertentu atau dapat diartikan sebagai strategi untuk membatasi lalu lintas jaringan. Hal ini membatasi seberapa sering seseorang dapat mengulangi tindakan dalam jangka waktu tertentu misalnya, mencoba masuk ke akun (Altaf, Rashid, Dar, & Rafiq, 2015). Beberapa penyedia layanan data menerapkan *rate limiting* guna menjaga kestabilan sistem agar dapat terus berjalan dan melayani permintaan data.

B. XSS

XSS merupakan kependekan dari istilah *Cross Site Scripting*. XSS merupakan salah satu jenis serangan injeksi *code*. XSS terjadi ketika penyerang menggunakan aplikasi web untuk mengirim atau menyuntikkan kode berbahaya, yang umumnya dalam bentuk skrip browser sisi klien ke halaman web yang dilihat oleh pengguna lain. XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau *client script code* lainnya ke suatu situs. Serangan ini akan seolah-olah datang dari situs tersebut. (Farah, Shojol, Hassan, & Alam, 2016) .

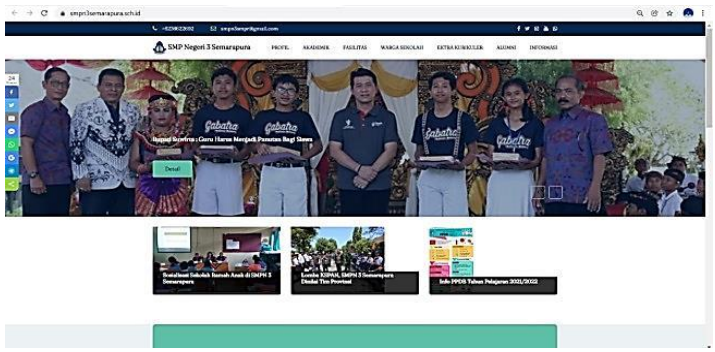
C. *Scanning* OWASP

OWASP singkatan dari *Open Web Application Security Project* merupakan sebuah komunitas terbuka yang di mana dikontribusikan untuk memungkinkan sebuah organisasi atau perusahaan mengembangkan serta memelihara aplikasi yang dapat dipercaya atau bisa diartikan sebagai sebuah organisasi yang berfokus pada keamanan dari sebuah web aplikasi (Bach-Nutman, n.d.).

3. HASIL DAN PEMBAHASAN

A. *Rate limiting*

Hal pertama yang dilakukan sebelum melakukan pengujian dengan *rate limiting* adalah membuka *Website* SMP Negeri 3 Semarapura terlebih dahulu yaitu smpn3semarapura.sch.id. Gambar 1 merupakan halaman utama dari *Website* SMP Negeri 3 Semarapura.

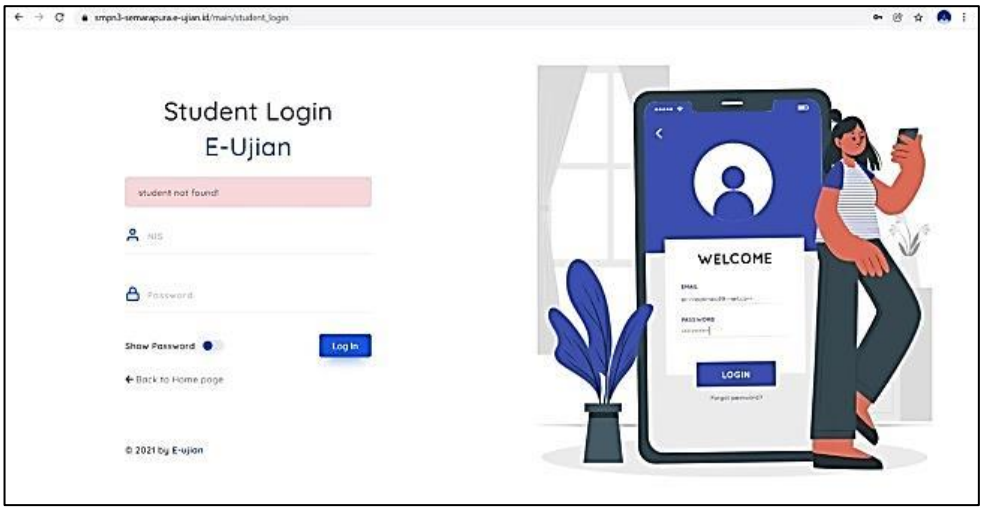


Gambar 1. Halaman Utama

Selanjutnya melakukan *rate limiting* pada salah satu menu *Website*, peneliti menggunakan menu *login Website*. Pada *Website* terdapat pilihan *login* yaitu *admin*, guru dan mahasiswa seperti pada gambar 2.

Gambar 2. Menu Login

Melakukan *login* pada *Website* dengan *username* dan *password* sesuai dengan acak dan menekan tombol *login*. Jika terdapat *popup "Student not found*" seperti pada gambar 3, maka dilakukan *login* kembali dengan *Username* dan *Password* yang lain. Proses l*ogin* ini dilakukan beberapa kali dan pengujian *login* ini dilakukan sebanyak 15 kali. Hal ini dilakukan untuk mengetahui apakah *Website menerapkan rate limiting* pada menu *login*.

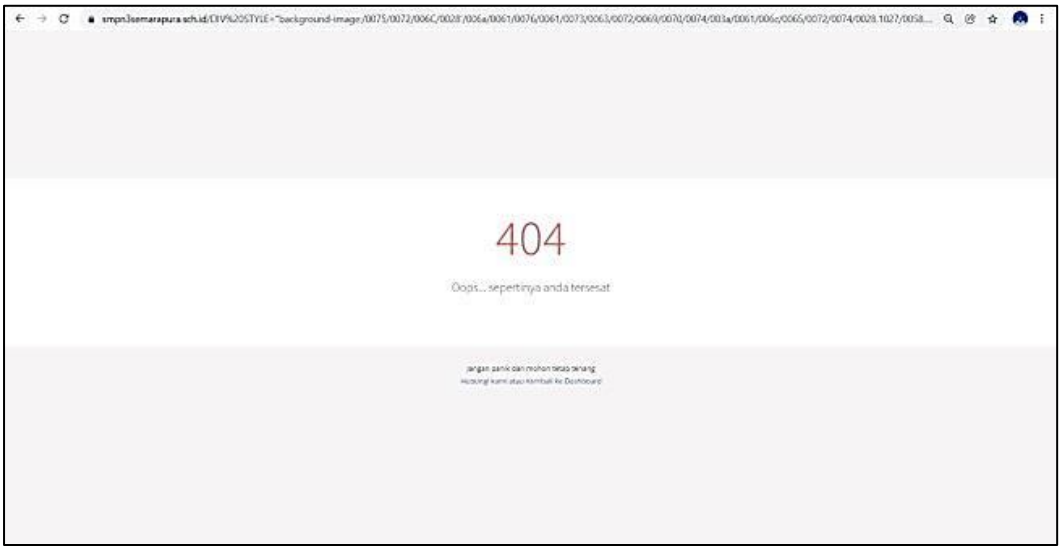


Gambar 3. Notifikasi student not found

Setelah beberapa kali mencoba dengan *Username* dan *Password* berbeda tetapi hanya muncul *popup* "*student not fond"* saja, maka *Website* dapat dikatakan tidak menerapkan *rate limiting* untuk memblokir sementara atau permanen dari sekian kali kesalahan yang dilakukan.

B. XSS

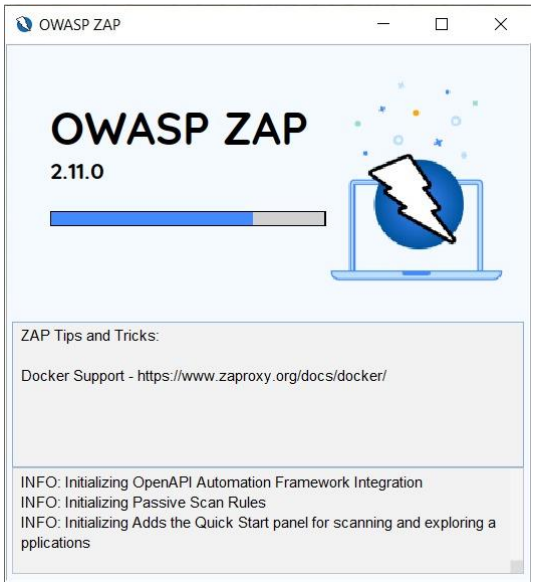
Pengujian ini dilakukan pada parameter-parameter URL yang memiliki nilai yang dimunculkan kembali pada halaman utama dari *Website*. Setelah memasukkan beberapa *Payload XSS Website* memunculkan halaman *Website error*. Hal ini membuktikan bahwa *payload* yang dimasukkan ini tidak tereksekusi.



Gambar 4. *Website* tidak mengeksekusi *payload* XSS

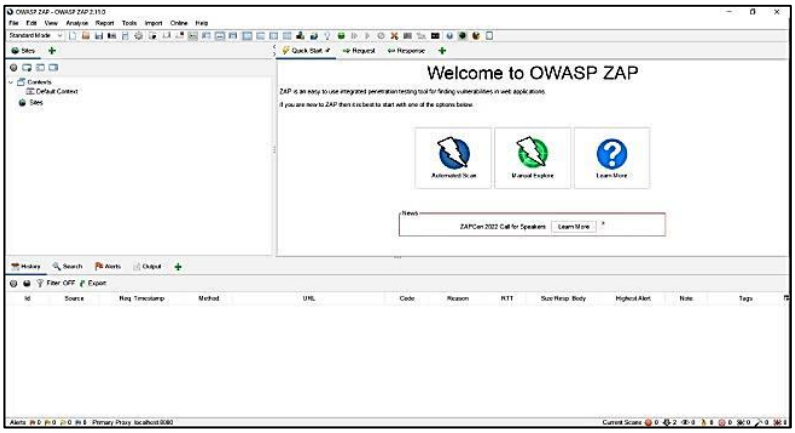
C. *Scanning* OWASP

Pengujian OWASP dilakukan dengan *menggunakan* aplikasi *OWASP ZAP*, Gambar 5 merupakan tampilan ketika membuka aplikasi *OWASP*.



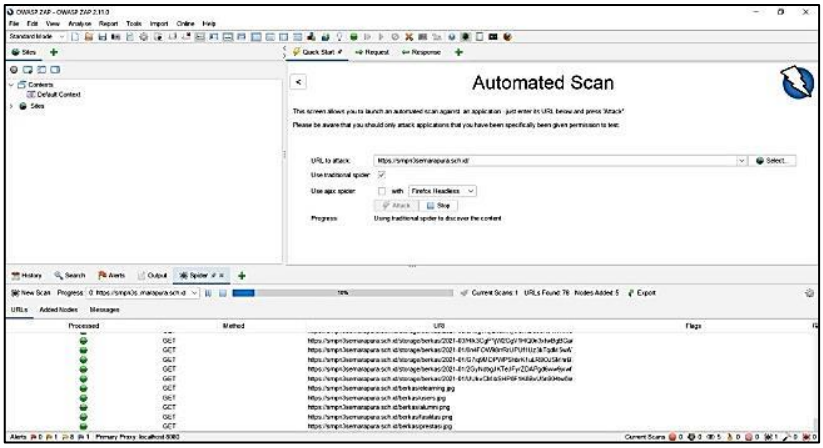
Gambar 5. Aplikasi OWASP ZAP

Setelah proses membuka aplikasi *OWASP* selesai, dapat melihat beberapa fitur *scan* seperti pada gambar 6. Proses selanjutnya menggunakan fitur *Automated Scan*.



Gambar 6. Halaman utama OWASP ZAP

Selanjutnya masukkan *link website* SMP Negeri 3 Semarapura pada kolom "URL *to attack" dan menekan* tombol *Attack.* Proses *scanning Website* berjalan dengan melihat struktur dari *Website* tersebut dan melakukan simulasi serangan secara langsung seperti pada gambar 7.



Gambar 7. Proses *scanning*

Setelah proses *scanning* selesai, analisis dilakukan pada *report* hasil scan untuk melihat kerentanan yang terdapat pada *website*. Hasil analisis terhadap *website* smpn3semarapura.sch.id menunjukkan bahwa *website* tersebut dalam level kerentanan *Low* dan *Medium*. Hal ini ditunjukkan dengan ditemukan web *alerts* pada kategori *Medium*, *Low* dan *Informational* seperti pada gambar 8.

Gambar 8. Hasil *scan Website* menggunakan OWASP ZAP

Gambar 9 menunjukkan jumlah peringatan untuk setiap tingkat risiko dan keyakinan yang disertakan dalam laporan. Persentase dalam tanda kurung menunjukkan hitungan sebagai persentase dari jumlah total lansiran yang disertakan dalam laporan, dibulatkan ke satu tempat desimal.

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	0 (0.0%)	22 (6.4%)	0 (0.0%)	22 (6.4%)
	Low	0 (0.0%)	0 (0.0%)	264 (76.5%)	28 (8.1%)	292 (84.6%)
	Informational	0 (0.0%)	0 (0.0%)	19 (5.5%)	12 (3.5%)	31 (9.0%)
	Total	0 (0.0%)	0 (0.0%)	305 (88.4%)	40 (11.6%)	345 (100%)

Gambar 9. Laporan tingkat risiko dari OWASP ZAP

Gambar 10 menunjukkan, untuk setiap situs yang satu atau lebih peringatannya dinaikkan, jumlah peringatan yang dinaikkan pada setiap tingkat risiko. Lansiran dengan tingkat kepercayaan "*False Positive*" telah dikeluarkan dari penghitungan ini. Angka dalam tanda kurung adalah jumlah peringatan yang dinaikkan untuk situs pada atau di atas tingkat risiko tersebut.

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://smpn3semarapura.sch.id	0 (0)	22 (22)	292 (314)	31 (345)

Gambar 10. Jumlah peringatan berdasarkan situs dan risiko dari OWASP ZAP

Gambar 11 menunjukkan jumlah peringatan dari setiap jenis peringatan, bersama dengan tingkat risiko jenis peringatan. Persentase dalam tanda kurung mewakili setiap hitungan sebagai persentase, dibulatkan ke satu tempat desimal, dari jumlah total lansiran yang disertakan dalam laporan ini.

Alert type	Risk	Count
Vulnerable JS Library	Medium	3 (0.9%)
X-Frame-Options Header Not Set	Medium	19 (5.5%)
Absence of Anti-CSRF Tokens	Low	27 (7.8%)
Cookie No HttpOnly Flag	Low	20 (5.8%)
Cookie Without Secure Flag	Low	40 (11.6%)
Cross-Domain JavaScript Source File Inclusion	Low	68 (19.7%)
Incomplete or No Cache-control Header Set	Low	20 (5.8%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	21 (6.1%)
Timestamp Disclosure - Unix	Low	28 (8.1%)
X-Content-Type-Options Header Missing	Low	68 (19.7%)
Information Disclosure - Suspicious Comments	Informational	31 (9.0%)
Total		345

Gambar 11. Jumlah peringatan berdasarkan jenis kerentanan dari OWASP ZAP

4. SIMPULAN DAN SARAN

Berdasarkan Analisis yang telah dilakukan, *Website* Sekolah SMP Negeri 3 Semarapura belum menerapkan *Rate limiting* pada bagian *Login* dan *Search* pada fitur Perpustakaan. Tanpa adanya fungsi

pembatasan ini, simulasi memasukkan *username* dan *password* sebanyak-banyaknya dapat dilakukan hingga mungkin menemukan kombinasi yang tepat, umumnya serangan ini dikenal dengan *brute force attack*. Serangan ini saat ini banyak diatasi dengan menerapkan *captcha* setelah beberapa kali kombinasi salah, maupun melakukan blokir sementara.

Sedangkan hasil dari XXS menunjukkan bahwa *playload* yang dimasukkan tidak tereksekusi oleh *Website* yang menunjukkan bahwa *Website* aman dari serangan XSS. Kemudian berdasarkan Analisis Kerentanan *Website* yang dilakukan dengan menggunakan OWASP maka, hasil yang diperoleh dari proses *Report* ZAP menunjukkan bahwa *Website* SMP Negeri 3 Semarapura memiliki persentase risiko atau level kerentanan *Low* dan *Medium*. Hal ini ditunjukkan dengan ditemukan web *alerts* pada kategori *Medium*, *Low* dan *Informational*.

Daftar Pustaka

Altaf, I., Rashid, F. ul, Dar, J. A., & Rafiq, M. (2015). Vulnerability assessment and patching management. *2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI)*, 16–21. IEEE. https://doi.org/10.1109/ICSCTI.2015.7489631

Arikunto. (1998). *Prosedur Penelitian*. Jakarta: Rinneka Cipta.

Bach-Nutman, M. (n.d.). *Understanding The Top 10 OWASP Vulnerabilities*.

Clancey, W. J. (1979). *Transfer of Rule-Based Expertise Through a Tutorial Dialogue*. Stanford University.

Engelmore, R., & Morgan, A. (1986). *Blackboard Systems* (Addison, Ed.). Wesley.

Farah, T., Shojol, M., Hassan, M., & Alam, D. (2016). Assessment of vulnerabilities of web applications of Bangladesh: A case study of XSS & CSRF. *2016 Sixth International Conference on Digital Information and Communication Technology and Its Applications (DICTAP)*, 74–78. IEEE. https://doi.org/10.1109/DICTAP.2016.7544004

Hasling, D. W., Clancey, W. J., & Rennels, G. R. (1983). Strategic Explanations in Consultation. *The International Journal of Man-Machine Studies*, 3–19.

Listartha, E., Arna, G., Saskara, J., Gede, D., & Santyadiputra, S. (2021). PENGUJIAN KERENTANAN DAN PENETRASI KEAMANAN PADA APLIKASI WEB MANAJEMEN SKRIPSI PRODI XYZ. *ScientiCO : Computer Science and Informatics Journal*, *4*(2), 1–14.

Rice, J. (1986). *Polygon: A System for Parallel Problem Solving*. Standford.

The OWASP Foundation. (2018). OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks. *2017 7th International Conference on Power Systems, ICPS 2017*.