Analisis Kerentanan *XSS* dan *Rate Limiting* Pada *Website* SMAN 8 Denpasar Menggunakan *Framework OWASP ZAP*

G.A.Septiawan[1], K.W.S.Irawan[2], I.Mayasari[3] dan I.M.E.Listartha[4]
[1,2,3,4]*Sistem Informasi, Fakultas Teknik dan Kejuruan, Universitas Pendidikan Ganesha*
Jl. Udayana No. 11, Singaraja - Bali
E-mail : angga.septiawan@undiksha.ac.id[1], wulan.sari@undiksha.ac.id[2], indah.mayasari@undiksha.ac.id[3], listartha@undiksha.ac.id[4]

Abstract—In the digital era now almost everyone accesses the internet, the website is one of the sites pn the internet that can store and disseminate all information. Along with the development of technology, the security of a website began to be threatened because of the rise of attacks carried out by digital criminals. Websites that have a weak security system will be vulnerable to threat attacks that can occur at any time. Cases of vulnerabilities that are often encountered are Cross Site Scripting (XSS) and Rate Limiting. To anticipate this the OWASP ZAP apllication can be used to test XSS vulnerabilities that exist on a website, one of which is on the SMA Negeri 8 Denpasar school website. XSS vulnerability testing is done by scanning, the generating a report. Through this report, an analysis is carried out to prove whether or not there is an XSS vulnerability on the website in question. Meanwhile, the Rate Limiting vulnerability was tested manually on the website login feature of SMA Negeri 8 Denpasar, by entering the username and password randomly and repeatedly.

Abstrak—Pada era digital sekarang hampir semua orang mengakses *internet*, *Website* merupakan salah satu situs yang ada di *internet* yang dapat menyimpan dan menyebarkan segala informasi. Seiring dengan perkembangan teknologi, keamanan suatu *website* mulai terancam karena maraknya serangan-serangan yang dilakukan oleh penjahat digital. *Website* yang memiliki sistem keamanan yang lemah akan rentan oleh serangan ancaman yang dapat terjadi sewaktu-waktu. Kasus kerentanan yang sering ditemui yakni *Cross Site Scripting (XSS*) dan *Rate Limiting*. Untuk mengantisipasi hal tersebut, aplikasi *OWASP ZAP* dapat dimanfaatkan untuk menguji kerentanan *XSS* yang ada pada sebuah website, salah satunya pada website sekolah SMA Negeri 8 Denpasar. Pengujian kerentanan *XSS* dilakukan dengan cara melakukan pemindaian, kemudian *generate report*. Melalui *report* tersebut, dilakukan analisis untuk membuktikan ada atau tidaknya kerentanan *XSS* pada *website* yang bersangkutan. Sedangkan, kerentanan *Rate Limiting* diuji secara manual pada fitur *login website* SMA Negeri 8 Denpasar, dengan cara memasukkan *username* dan *password* secara acak dan berulang-ulang.

Kata Kunci—OWASP ZAP, Rate Limiting, XSS, Kerentanan

I. PENDAHULUAN

Pada era digital sekarang hampir semua orang mengakses *internet*, dari anak kecil sampai orang dewasa juga sudah mengetahui. *Website* merupakan salah satu situs yang ada di *internet* yang dapat menyimpan dan menyebarkan segala informasi[1]. Pengguna yang berhak dapat memperoleh informasi serta data yang terdapat didalamnya. Umumnya, informasi dan data tersimpan dalam suatu database server[2]. Banyaknya data dan informasi yang tersebar di *internet* juga diiringi dengan tingginya serangan keamanan. *Website* yang memiliki sistem keamanan yang lemah akan rentan oleh serangan-serangan ancaman yang dapat terjadi sewaktu-waktu. Sering terjadi permasalahan keamanan sistem yang kadang terabaikan dan bahkan malah terletak diurutan kedua atau urutan terakhir dalam daftar yang dianggap penting[3]. Salah satu masalah keamanan pada aplikasi berbasis web adalah *Cross site scripting (XSS*) dan *Rate Limiting*.

XSS pertama kali ditemukan pada awal tahun 1990 oleh *World Wide Web[4]*. *XSS* merupakan bentuk serangan injeksi yang dilakukan dengan menyisipkan kode berbahaya melalui fasilitas interaksi yang diberikan *website*[5]. Ketika aplikasi gagal dalam melakukan validasi terhadap masukan pengguna, maka hal tersebut dapat terjadi. Akibat dari serangan *XSS* peretas dapat mencuri *cookie*, membajak akun, manipulasi konten web, hingga mengambil informasi yang sifatnya pribadi dan berbagai macam aktifitas berbahaya lainnya.

Selain *XSS*, terdapat kerentanan lainnya, yaitu Rate Limiting. Rate Limiting sendiri merupakan sebuah batasan yang diatur bagi pengguna ketika melakukan suatu tindakan dalam *website*[6]. Misalnya, suatu *website* membatasi percobaan login pengguna, sehingga ketika login dilakukan berulang dengan *username* dan *password* yang salah, maka akun terjadi pemblokiran. Jika suatu *website* tidak

menerapkan *Rate Limiting* (No *Rate Limiting*), maka hal tersebut akan menimbulkan kemungkinan kerentanan yang lebih besar pada suatu *website* untuk disalahgunakan.

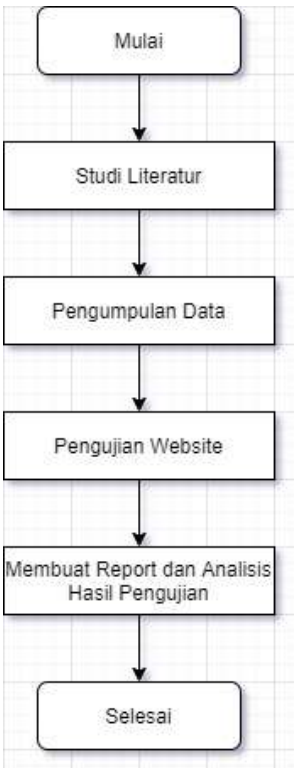
Open Web Application Security Project atau *OWASP* berfokus pada peningkatan keamanan perangkat lunak[7]. Pedoman *OWASP* diterapkan di seluruh perangkat lunak untuk pengembangan (*SDLC*) dalam aplikasi pengembangan yang meliputi perencanaan sistem, analisis sistem, perancangan sistem, implementasi, dan pengujian[8].

OWASP ZAP ini dapat dimanfaatkan untuk menguji kerentanan sebuah *website* dengan cara melakukan pemindaian (*scanner*), terutama dalam menguji *Cross Site Scripting (XSS)*. Melalui *OWASP ZAP*, nantinya akan diketahui kerentanan-kerentanan apa saja yang terdapat pada *website* yang bersangkutan, dimana kerentanan tersebut akan terangkum dalam sebuah *report*[9]. Sementara itu, untuk menguji kerentanan *Rate Limiting* pada sebuah *website* akan dilakukan cara manual, yakni memasukkan *username* dan *password* secara berulang.

Penelitian ini bertujuan untuk menganalis dan mengetahui kerentanan yang terdapat pada *website* SMAN 8 Denpasar dengan melakukan pengujian *XSS* dan *Rate Limiting* menggunakan *framework OWASP ZAP*. Hasil dari kerentanan yang diperoleh dapat digunakan sebagai tindak lanjut untuk mengamankan *website* yang berguna untuk meningkatkan keamanan *website* dengan cara menutup celah kerentanan yang ada.

II. METODE PENELITIAN

Metode penelitian ini menggunakan teknik seperti yang disusun pada gambar 1.



Gambar. 1 Alur dari metode penelitian

A. *Studi Literatur*

Pada tahap ini melakukan pencarian untuk mendapatkan informasi dari literasi-literasi terdahulu sebagai dasar atau landasan teori terhadap permasalahan yang sesuai atau sejenis dengan penelitian ini.

B. *Pengumpulan Data*

Pada tahap ini dilanjutkan dengan mengumpulkan data target sasaran, dimana sasaran dari penelitian ini yaitu website sekolah SMA Negeri 8 Denpasar.

C. *Pengujian Website*

Selanjutnya, masuk ke tahap pengujian *Website* untuk membuktikan adanya kerentanan *XSS (Cross Site Scripting)* dengan menggunakan aplikasi *OWASP ZAP* dan pengujian kerentanan *Rate Limiting*. Dalam pengujian *XSS*, diperlukan url dari *website* yang dituju untuk melakukan pemindaian *(scan* otomatis).

D. *Report dan Hasil Pengujian*

Setelah pemindaian mencapai 100%, selanjutnya dilakukan generate report untuk memperoleh hasil pengujian sebagai bahan dalam proses analisis. Sementara itu, untuk *Rate Limiting*, dilakukan dengan pengujian secara manual pada fitur login yang terdapat dalam *website* SMA Negeri 8 Denpasar, dengan cara memasukkan *password* dan *username* secara acak dan berulang-ulang, kemudian dilanjutkan dengan melakukan analisis. Setelah proses analisis, tahap akhir dari penelitian ini adalah penyusunan laporan.

III. HASIL DAN PEMBAHASAN

A. *Tahapan Pengujian*

Pengujian yang dilakukan menggunakan *OWASP ZAP* pada *website* SMA Negeri 8 Denpasar memiliki fokus yang dituju yaitu *Input Validation Testing* pada kerentanan *XSS* (*Cross Site Scripting)*, sedangkan pengujian secara manual memiliki fokus *Input Validation Testing* pada kerentanan *Rate Limiting* dengan detail sebagai berikut.

Tabel 1.
Tahapan Pengujian *XSS* dan *Rate Limiting*

Fokus	Tahapan	Aktivitas	Alat
	Testing for Reflected Cross Site Scripting	Pengujian yang dilakukan dengan memeriksa kerentanan terhadap *Cross Site Scripting*	*OWASP ZAP*
Input Validation Testing	*Testing for Stored Cross Site Scripting*	Pengujian yang dilakukan dengan memeriksa kerentanan terhadap *Cross Site Scripting.*	*OWASP ZAP*

	Testing for Rate Limiting	Pengujian yang dilakukan dengan memeriksa kerentanan terhadap Rate Limiting pada fitur login	*Google Chrome*	

B. Hasil Pengujian

Berdasarkan hasil *generate report* dari *aplikasi OWASP ZAP* mengenai pengujian *XSS (Cross Site Scripting*) dan pengujian *Rate Limiting* secara manual, didapatkan hasil pengujian kerentanan sebagai berikut.

Tabel 2.
Hasil Pengujian *XSS* dan *Rate Limiting*

Fokus	Tahapan	Aktivitas	Alat	Hasil
	Testing for Reflected Cross Site Scripting	Pengujian yang dilakukan dengan memeriksa kerentanan terhadap C*ross Site Scripting.*	*OWASP ZAP*	Ditemukan satu kerentanan pada *Reflected XSS.*
Input Validation Testing	*Testing for Stored Cross Site Scripting*	Pengujian yang dilakukan dengan memeriksa kerentanan terhadap *Cross Site Scripting.*	*OWASP ZAP*	Tidak ditemukan kerentanan pada *Stored XSS.*
	Testing for Rate Limiting	Pengujian yang dilakukan dengan memeriksa kerentanan terhadap *Rate Limiting* pada fitur login.	*Google Chrome*	Ditemukan kerentanan pada *Rate Limiting*

IV. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa pengujian dilakukan menggunakan aplikasi *OWASP ZAP* dan dilakukan secara manual untuk mengetahui kerentanan yang terdapat pada *website* sekolah SMA Negeri 8 Denpasar. Fokus dari pengujian ini adalah *Input Validation Testing* pada kerentanan XSS (*Cross Site Scripting*) dan *Rate Limiting.* Hasil yang diperoleh berdasarkan pengujian tersebut yakni ditemukan adanya kerentanan XSS dan *Rate Limiting*. Dimana dalam *website* SMA Negeri 8 Denpasar tidak terdapat batasan untuk pengguna *login* ke dalam *website* sehingga pengguna dapat *login* berkali - kali untuk mencoba dan tidak ada pemblokiran oleh sistem. Mengenai pengembangan lebih lanjut, penulis menyarankan untuk pengembang *website* SMA Negeri 8 Denpasar yaitu perlu dilakukan tindakan keamanan dan perbaikan terhadap *website* SMA Negeri 8 Denpasar untuk mencegah terjadinya hal - hal berbahaya yang memicu kejahatan.

DAFTAR PUSTAKA

[1] Cholily, Y. M., Putri, W. T., & Kusgiarohmah, P. A. 2019. "Pembelajaran di era revolusi industri 4.0," *In Seminar & Conference Proceedings of UMT.*

[2] Hasugian, P. S. 2018. "Perancangan *Website* Sebagai Media Promosi Dan Informasi, "*Journal Of Informatic Pelita Nusantara*, 3(1).

[3] Siradjuddin, H. K. 2019. "Aplikasi E-Learning Al-Islam Kemuhammadiyahan pada STMIK Muhammadiyah Jakarta," *JIKO (Jurnal Informatika dan Komputer)*, 2(1), 14-18.

[4] Hydara, A. B. M. Sultan, H. Zulzalil, and N. Admodisastro, (2014), "Current state of research on cross-site scripting (XSS) – A systematic literature review," Inf. Softw. Technol.

[5] Neha Gupta. 2015. "*XSS Defense: An Approach for Detecting and Preventing Cross Site Scripting Attacks '. COMPUSOFT, An international journal of advanced computer technology,* (Volume-IV, Issue-III) March-2015.

[6] Wajong, A. M. 2012. "Kerentanan yang Dapat Terjadi di Jaringan Komputer pada Umumnya, "*ComTech: Computer, Mathematics and Engineering Applications*, 3(1), 474-481.

[7] *OWASP, —OWASP Risk Rating Methodology - OWASP.‖ [Online].Available*:https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology. [Accessed: 19-Jun-2017].

[8] M. Yunus, "ANALISIS KERENTANAN APLIKASI BERBASIS WEB MENGGUNAKAN KOMBINASI SECURITY *TOOLS PROJECT* BERDASARKAN *FRAMEWORK OWASP* VERSI 4," *Jurnal Ilmiah Informatika Komputer*, vol. 24, no. 1, pp. 37–48, 2019, doi: 10.35760/ik.2019.v24i1.1988.

[9] Robinson, Memen Akbar dan M.F. Ridha. 2018. "*SQL Injection and Cross Site Scripting Prevention using OWASP ModSecurity Web Application Firewall". International Journal on Informatics Visualization Vol.2.* No. 4 2018; 286 – 292.