

Mendeteksi Keamanan Website SMP Negeri 1 Blahbatuh Menggunakan Metode Open Web Application Security Project (OWASP) Versi 2.11: XSS & Rate Limiting

¹I Made Agus Jana Januraga, ²Gede Bagus Parmadi Wijaya, ³Laurensius Patrick, ⁴I Made Edy Listartha
Fakultas Teknik dan Kejuruan, Teknik Informatika, Universitas Pendidikan Ganesha
Jl Udayana No. 11, Singaraja, Kec. Buleleng, Kabupaten Buleleng, Bali.
¹parmadi1411@gmail.com

Abstract

Detecting website security vulnerabilities is very important and can estimate the risks that exist in the sustainability of an organization. The transition to the scope of the website is used by some criminals with the aim of stealing user's confidential information for their own benefit. In this study, the mechanism of the risk assessment method was carried out on the website of SMP Negeri 1 Blahbatuh. Where the website is the official website of the school to fulfill teaching and learning activities managed by the school. To determine the level of risk on the website, the Open Web Application Security Project (OWASP) XSS and Rate Limiting methods are used to detect security vulnerabilities on the website. XSS or better known as Cross Site Scripting is an attack that performs code injection using an application's website page. The perpetrators of this XSS or Cross Site Scripting act by executing a malicious script on the victim's browser by entering malicious code on the web page. Rate limiting or commonly known as rate limiting is a form of strategy used by someone to test security vulnerabilities on the web or limit network traffic. This is used to limit how often someone can repeat the same action within a certain period of time. For example, trying to enter the school's website by logging in to its website using a random account to an indefinite limit to test how secure the website is.

Keyword: XSS, Rate Limiting, OWASP, Website Testing

Abstrak

Mendeteksi kerentanan keamanan website adalah hal yang sangat penting dan dapat memperkirakan risiko yang ada pada keberlangsungan suatu organisasi. Terjadinya transisi ke dalam lingkup website dimanfaatkan oleh beberapa pelaku kejahatan dengan bertujuan mencuri informasi rahasia pengguna demi menguntungkan diri sendiri. Pada Penelitian ini dilakukan mekanisme metode asesmen risiko pada website SMP Negeri 1 Blahbatuh. Dimana website tersebut merupakan website resmi dari sekolah untuk memenuhi kegiatan belajar mengajar yang dikelola oleh pihak sekolah. Untuk mengetahui tingkat risiko pada website, maka digunakannya metode Open Web Application Security Project (OWASP) XSS dan Rate Limiting untuk mendeteksi kerentanan keamanan pada website. XSS atau lebih dikenal dengan Cross Site Scripting merupakan suatu serangan yang melakukan injeksi code dengan menggunakan halaman website suatu aplikasi. Pelaku kejahatan dari XSS atau Cross Site Scripting ini melakukan aksinya dengan cara mengeksekusi suatu skrip berbahaya pada browser korban dengan cara memasukkan kode berbahaya pada halaman webnya. Rate limiting atau yang biasa dikenal dengan pembatasan tarif merupakan suatu bentuk strategi yang digunakan seseorang untuk melakukan uji coba terhadap kerentanan keamanan pada web tersebut atau pembatasan lalu lintas jaringan. ini gunanya untuk membatasi seberapa sering seseorang tersebut dapat mengulangi tindakan yang sama dalam jangka waktu tertentu. contohnya mencoba masuk ke website sekolah dengan login di halaman websitenya menggunakan akun yang acak sampai limit yang tak telah ditentukan untuk menguji seberapa aman website tersebut. ont

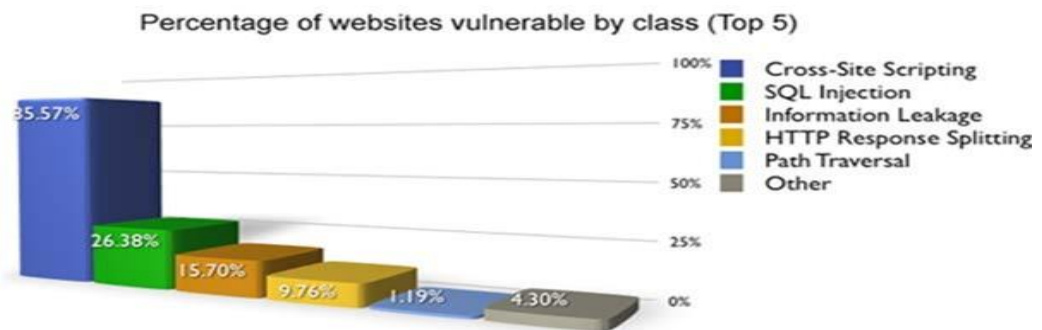
Keyword: XSS, Rate Limiting, OWASP, Website Testing

I. PENDAHULUAN

Pengujian sistem keamanan aplikasi berbasis *website* adalah hal yang penting di era perkembangan aplikasi berbasis *web* yang melaju dengan pesat. Semakin berkembangnya aplikasi berbasis *web* juga diiringi dengan tingginya serangan keamanan dari berbagai teknik ancaman. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Perkembangan di dunia internet sudah

mencapai suatu tahap yang begitu pesat, sehingga tidak mengherankan apabila setiap orang dapat mengakses *website* yang diinginkan. Keamanan pada *website* sangat erat kaitannya dengan jaringan, untuk mengakses sebuah *web* pasti memerlukan koneksi jaringan. Pada saat ini sangat pesat perkembangan teknologi *web*, jaringan, dan bermacam-macam ancaman keamanan yang perlu dihadapi, seperti adanya ancaman terhadap kerahasiaan yang sering dihadapi adalah peretas, virus-virus dari internet maupun berasal dari media transfer data fisik seperti *flashdisk*, *hardisk* eksternal, melalui jaringan LAN, *download* file tanpa keamanan, *Trojan horse*, aktivitas user yang mengabaikan atau yang tidak terorisasi dan banyak hal lagi beberapa ancaman keamanan yang terkadang tidak kita sadari. Keamanan pada sistem informasi berbasis *website* sangatlah penting untuk menjaga kesesuaian dan integritas data. Sistem keamanan sebuah *website* harus perlu diperhatikan dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak berhak. Berbagai macam alasan peretas atau *hacker* mencari celah pada *website server* bertujuan untuk mendapatkan informasi dari sebuah organisasi ataupun perusahaan untuk memenuhi kepentingan-kepentingan yang menyebabkan kerugian pada pihak lain. Hasil dari analisa kerentanan dapat membantu pengelola dan pengembang sistem untuk mencegah dan mengatasi dampak risiko yang ditemukan pada sistem. Belum adanya *Security Assessment* pada sistem informasi *website* SMP Negeri 1 Blahbatuh. Oleh karena itu perlu adanya *Security Assessment* (Penilaian keamanan) pada sistem tersebut Metode untuk menguji keamanan *website* adalah metode OWASP. *The Open Web Application Security Project* (OWASP) merupakan yayasan nirlaba yang didedikasikan guna untuk meningkatkan keamanan *website*. OWASP beroperasi di komunitas terbuka bahwa di mana siapa pun dapat berpartisipasi dan berkontribusi pada proyek yang dilakukan.

Mengetahui celah keamanan secara manual akan kurang efektif meningkatkan keamanan pada *website*. Sehingga kita perlu melakukan penilaian terhadap risiko *website* dengan mempertimbangkan perbedaan faktor-faktor yang terkait dengan *web* akan memberikan penjelasan yang lebih memfokuskan untuk mengamankan *website* lebih baik lagi. Dengan mengikuti langkah ini, kita dapat memperkirakan tingkat kerentanan *website* dan dapat membuat suatu keputusan mengenai risiko tersebut. Sehingga, faktor risiko akan memprioritaskan masalah pada *web* dengan cara yang lebih baik daripada menganalisis secara acak. Bagian yang terdeteksi kerentanan dapat secara cepat ditindak lanjuti. *Framework* yang digunakan adalah OWASP versi 2.11.



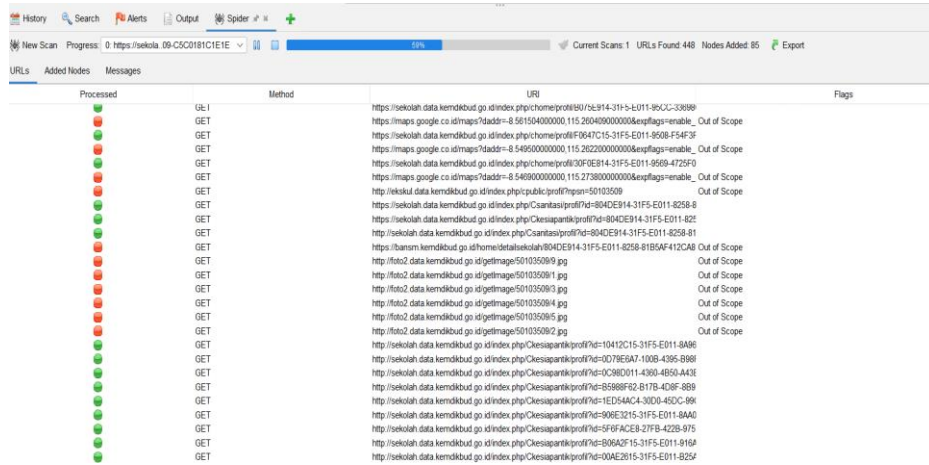
Gambar 1. Prosentase Kerentanan Website

Pada penelitian kali ini, untuk mendeteksi kerentanan keamanan pada *website* sekolah terdapat beberapa metode yang akan kami gunakan diantaranya ISSAF, OSSTMM, NIST, OWASP. Tapi diantara keempat metode itu yang tepat digunakan untuk *penetration testing* adalah OWASP.

II. HASIL DAN PEMBAHASAN

A. OWASP

Mendeteksi kerentanan pada *website* dengan penelitian menggunakan aplikasi OWASP untuk mengetahui celah keamanan yang ada pada *website* sekolah. Dimana pengembangan *website* yang sudah dibangun menggunakan bahasa pemrograman *PHP Native* dan *framework CI (code igniter)* sebagai *website* sekolah. Gambar 2 adalah tampilan dari proses scanning menggunakan aplikasi OWASP.



Gambar 2. Tools OWASP Scanner

Setelah melakukan proses scanning pada gambar 2, berikut akan menggambarkan hasil celah keamanan yang keluar pada sistem informasi.

Alert type	Risk	Count
Directory Browsing	Medium	41 (5.0%)
X-Frame-Options Header Not Set	Medium	41 (5.0%)
Absence of Anti-CSRF Tokens	Low	57 (7.0%)
Cookie No HttpOnly Flag	Low	5 (0.6%)
Cookie without SameSite Attribute	Low	5 (0.6%)
Incomplete or No Cache-control Header Set	Low	122 (15.0%)
Server Leaks Information via "X-Powered-By," HTTP Response Header Field(s)	Low	144 (17.6%)
Timestamp Disclosure - Unix	Low	152 (18.6%)
X-Content-Type-Options Header Missing	Low	146 (17.9%)
Ketidakcocokan Charset	informasi	18 (2,2%)
Keterbukaan Informasi - Komentar Mencurigakan	informasi	85 (10,4%)
Total		816

Gambar 3 Alert Type

Pada gambar 3, diketahui beberapa peringatan yang terjadi, setiap tipe peringatan terdapat risiko dari *low* hingga *medium* dan memiliki persentase setiap risikonya. Setelah mengetahui peringatan, risiko, dan persentase yang terjadi pada website sekolah tersebut, selanjutnya akan diperlihatkan juga ancaman yang bisa terjadi pada *website* ini.

		Risk			
		High	Medium	Low (>=	Informational
		(= High)	(>= Medium)	(>= Low)	ional)
Site	https://smpn1blahbatuh.sch.id	0 (0)	82 (82)	631 (713)	103 (816)

Gambar 4. Tabel Risk

Gambar 4 merupakan hasil analisis risk dari sistem informasi berbasis *web* pada SMP Negeri 1 Blahbatuh. Pada tabel risk, terdapat URL <https://smpn1blahbatuh.sch.id> yang memiliki total risiko *high* yaitu 0, risiko *medium* adalah 82, risiko *low* adalah 631, risiko *informational* adalah 103.

		Confidence				
		User	High	Medium	Low	Total
		Confirmed				
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	0 (0.0%)	82 (10.0%)	0 (0.0%)	82 (10.0%)
	Low	0 (0.0%)	0 (0.0%)	479 (58.7%)	152 (18.6%)	631 (77.3%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	103 (12.6%)	103 (12.6%)
	Total	0 (0.0%)	0 (0.0%)	561 (68.8%)	255 (31.2%)	816 (100%)

Gambar 5. Risk & Confidence

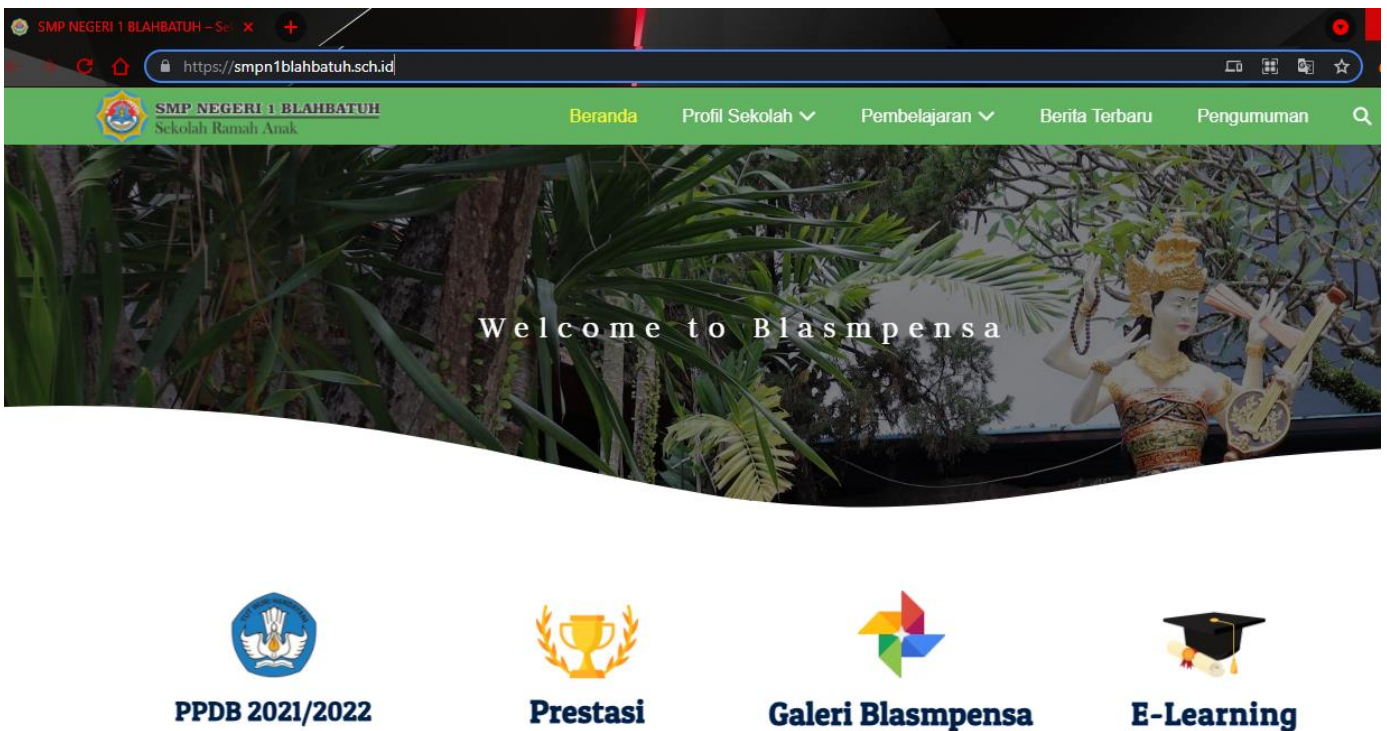
Gambar 5 merupakan hasil analisis *Risk & Confidence* dari sistem informasi berbasis *web* pada SMP Negeri 1 Blahbatuh. Pada tabel risk & confidence, memiliki total risk & confidence dengan *high* yaitu 0 (0,0%), *medium* adalah 82 (10,0%), *low* adalah 631 (77,3%), *informational* yaitu 103 (12,6%), sehingga *risk & confidence* memiliki total keseluruhan sebagai berikut; *User confirmed* adalah 0 (0,0%), *high* adalah 0 (0,0%), *medium* adalah 561 (68,8%), *low* adalah 255 (31,2%), dan total keseluruhan adalah 816 (100%).

B. XSS (Cross Site Scripting)

Berikut ini merupakan proses dari pengujian kerentanan XSS (*Cross Site Scripting*) pada *website* SMP Negeri 1 Blahbatuh. Pada proses pengujian kerentanan XSS (*Cross Site Scripting*) ini kami mencoba untuk memasukkan sebuah *script payload* pada tempat *URL website* dari SMP Negeri 1 Blahbatuh. Disini kami ingin melihat apakah ada perubahan yang terjadi pada halaman *website* apabila kami menginputkan *script payload*-nya.

Kami mencoba memasukkan *script payload* berikut ini ke dalam *website* : "><script>alert(%27XSS%27)</script>". *Script* ini bisa dimasukkan di bagian depan, tengah maupun belakang. Apabila setelah kami memasukkan *script payload* tersebut pada *websitenya* terdapat perubahan atau pemberitahuan

maka dapat dipastikan *website* tersebut mempunyai kerentanan XSS (*Cross Site Scripting*). Berikut ini proses XSS (*Cross Site Scripting*) yang kami lakukan pada *website* <https://smpn1blahbatuh.sch.id/>.



Gambar 6. Tampilan Halaman Awal Website

Ini merupakan proses awal yang dilakukan yaitu masuk ke dalam laman *website* <https://smpn1blahbatuh.sch.id/> sebelum nantinya kita akan memasukkan *script payload* pada *search bar website* dari SMP Negeri 1 Blahbatuh.



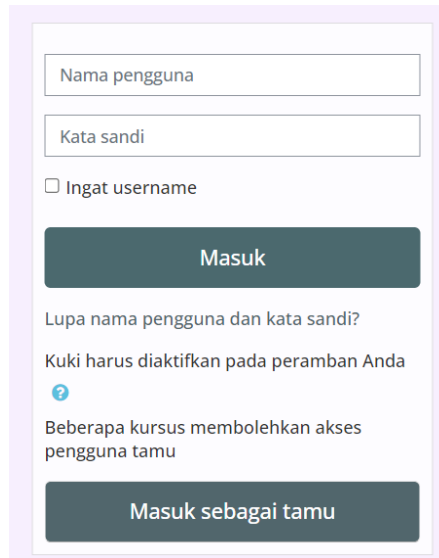
Gambar 7. Tampilan Setelah Memasukkan Script Payload

Ini merupakan tampilan ketika dimasukkan *script payload* ke dalam laman *website* resmi SMP Negeri 1 Blahbatuh dengan URL <https://smpn1blahbatuh.sch.id/>. Terlihat pada gambar 7, setelah kami melakukan uji kerentanan dengan cara memasukkan *source payload* pada *search bar website-nya* berubah tampilannya seperti gambar 7.

C. Rate Limiting

Berikut ini adalah proses dari *rate limiting* yang merupakan jumlah akses suatu *endpoint* di dalam suatu *website* dalam waktu tertentu. Beberapa situs *web* menerapkan *rate limiting* guna menjaga kestabilan sistem agar dapat

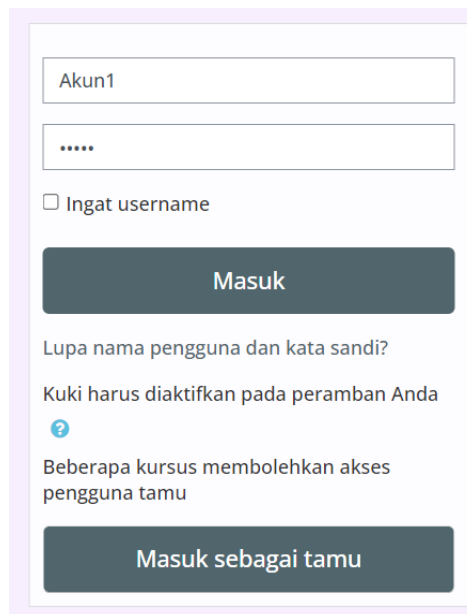
terus berjalan dan melayani permintaan data. Seperti pada analisis kali ini, web yang digunakan sebagai bahan analisis yaitu *website* resmi dari sekolah SMP Negeri 1 Blahbatuh.



The image shows a login form with the following elements: a text input field labeled 'Nama pengguna', a text input field labeled 'Kata sandi', a checkbox labeled 'Ingat username', a dark green button labeled 'Masuk', a link 'Lupa nama pengguna dan kata sandi?', a note 'Kuki harus diaktifkan pada peramban Anda' with a question mark icon, a note 'Beberapa kursus membolehkan akses pengguna tamu', and a dark green button labeled 'Masuk sebagai tamu'.

Gambar 8. Halaman E-Learning

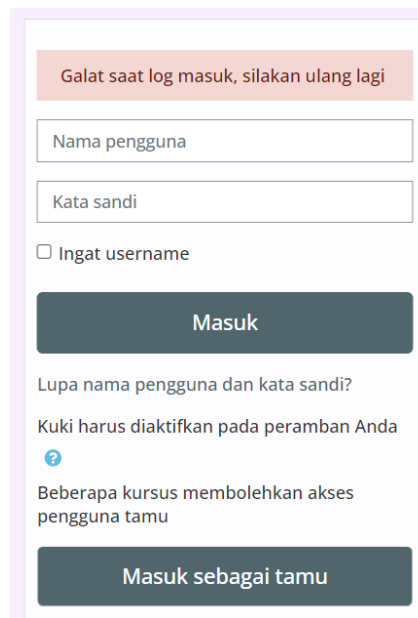
Pada Gambar 8 *website* ini, tepatnya pada halaman *e-learning* sekolah terdapat kolom nama pengguna dan kata sandi yang harus diisi untuk memasuki halaman berikutnya.



The image shows the same login form as in Gambar 8, but with the 'Nama pengguna' field filled with 'Akun1' and the 'Kata sandi' field filled with '.....'. The 'Masuk' button is highlighted with a dark green background.

Gambar 9. Mengisi kolom

Proses gambar 9, pada kolom nama pengguna dan kata sandi kita mengisi kolom tersebut secara acak mulai dari nama pengguna “akun1” sampai dengan “akun10” dan *password* yang kita isi adalah “12345” sebanyak 10 akun, jika nama pengguna dan *password* yang kita masukan benar maka akan berlanjut ke halaman berikutnya, dan jika kita memasukkan *username* dan *password* yang salah, maka kita akan melihat tampilan notifikasi seperti pada Gambar 10.

The image shows a login form with a light purple border. At the top, there is a red error message box that says "Galat saat log masuk, silakan ulang lagi". Below this are two input fields: "Nama pengguna" and "Kata sandi". There is a checkbox labeled "Ingat username" which is currently unchecked. A dark blue button labeled "Masuk" is positioned below the input fields. Underneath the button, there is a link "Lupa nama pengguna dan kata sandi?". Below that, a note states "Kuki harus diaktifkan pada peramban Anda" with a blue question mark icon. At the bottom, there is a note "Beberapa kursus membolehkan akses pengguna tamu" and a dark blue button labeled "Masuk sebagai tamu".

Gambar 10. Muncul Notifikasi

Terlihat pada gambar 9, setelah memasukkan nama pengguna dan *password* yang salah sebanyak 10x *website* tersebut tetap memunculkan notifikasi “Galat saat log masuk, silakan ulang lagi” dapat dinyatakan bahwa *website* ini tidak memiliki *rate limiting* pada halaman *login* sehingga *website* ini memiliki risiko dieksploitasi atau tindakan yang bertujuan untuk mengambil keuntungan atau memanfaatkan sesuatu secara sewenang-wenang.

III. KESIMPULAN

Berdasarkan hasil analisis dan penelaahan yang telah dilakukan pada *website* SMP Negeri 1 Blahbatuh menggunakan *security assessment* dengan menggunakan 3 metode kerentanan *website* yaitu menggunakan *rate limiting*, *XSS (Cross Site Scripting)* dan *OWASP* terhadap *website* sekolah maka dapat ditarik kesimpulan:

1. Perlu adanya penilaian risiko kerentanan keamanan pada sebuah *website* agar bisa memiliki potensi risiko keamanan sebelum *website* di *upload* ke *server* produksi dan di *publish* ke publik.
2. Terdapat 816 resiko dengan 561 medium resiko dan 255 *low* resiko itu berarti kerentanan keamanan *website* sekolah ini cukup memprihatinkan.
3. Keamanan *website* SMP Negeri 1 Blahbatuh rentan terhadap suatu serangan yang berdampak buruk pada sistem *website* yang mereka kelola, hal ini terlihat pada kerentanan *rate limiting*, *XSS (Cross site scripting)*, dan *OWASP* yang memungkinkan bagi seorang *attacker* mengambil alih sistem yang dikelola.
4. Penguji menggunakan *script code payload* agar bisa mengetahui apakah terdapat kerentanan pada *website* sistem SMP Negeri 1 Blahbatuh.
5. Dengan adanya *OWASP* ini dapat memudahkan penguji dalam melakukan uji kerentanan pada suatu *website*.
6. Suatu *website* perlu dilakukan uji kerentanan agar dapat mengetahui apakah adanya kerentanan yang dapat berakibat fatal pada *website* saat dijalankan.

REFERENSI

- [1] Hutagalung, R. H., Nugroho, L. E., Hidayat, R., 2017, Menentukan Dampak Resiko Keamanan Berbasis Pendekatan Owasp, Prosiding SNATI F Ke-4 Tahun 2017, Kudus, Indonesia.
- [2] Fernando, Y. I., Abdillah, R., 2016, Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM), Jurnal CoreIT, Vol. 2, No.1, Hal 33 – 40.
- [3] Kesuma, M. C., Shiddiqi, A. M., Pratomo, B. A., 2013, Pencari Celah Keamanan pada Aplikasi Web, Tugas Akhir, Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember.
- [4] Rao, R. M., Durgesh, P., 2010, Security risk assessment of Geospatial Weather Information System (GWIS): An OWASP based approach, (IJCSIS) International Journal of Computer Science and Information

Security, Vol. 8, No. 5, Hal 24 – 32

- [5] Shanley, A., Johnstone, M. N., 2015, Selection of penetration testing methodologies: A comparison and evaluation, Australian Information Security Management Conference. Western Australia. 30 November – 2 Desember 2015.
- [6] Bahrún ghózáli, Kusrini, Sudarmawan, 2017, Mendeteksi kerentanan keamanan aplikasi website menggunakan metode Owasp (open web application security project) untuk penilaian risk rating, citec journal, vol 4, no 4
- [7] OWASP. (2010). The ten Most Critical Web. Open Web Application Security Project (OWASP). https://owasp.org/www-pdf-archive/OWASP_Top_10_-_2010_FINAL_Indonesia_v1.0.1.pdf