IMPLEMENTASI DAN ANALISIS *OPEN SOURCE* RAPTORWAF PADA APLIKASI WEB BERDASARKAN STANDAR PTES

IMPLEMENTATION AND ANALYSIS OF OPEN SOURCE RAPTORWAF ON WEB APPLICATION BASED ON PTES STANDARDS

Irmalistia Alfiani[1], Adityas Widjajarto[2], Avon Budiyono[3]

[1,2,3] Universitas Telkom, Bandung
[1]**irmalistia@student.telkomuniversity.ac.id**, [2]**adtwjrt@telkomuniversity.co.id**,
[3]**avonbudi@telkomuniversity.ac.id**

Abstrak

***Web application firewall* merupakan suatu metode sebagai pengamanan dari serangan pada aplikasi web. Implementasi *web application firewall* dapat memblokir beberapa serangan, dari sisi permasalahan keamanan dapat di lakukan analisis seberapa efisien *web application firewall* dalam melindungi aplikasi web. Pada penelitian ini implementasi dan analisis *web application firewall* dilakukan berdasarkan *vulnerability* dan *threat* dalam pengujian serangan pada aplikasi web yang telah terpasang *web application firewall* sebagai *control*. Eksperimen dilakukan berdasarkan standar PTES (*Penetration Testing Execution Standard*) sebagai dasar untuk eksploitasi terhadap kerentanan. *Web application firewall* mampu memblokir tiga serangan dengan efektivitas 60% secara kuantitatif. Sedangkan secara kualitatif, menggunakan hasil *vulnerability scanning* dengan Acunetix berdasarkan tingkat *severity* kerentanan yang dapat diamankan oleh *web application firewall*.**

Kata kunci : ***web application firewall, vulnerability, threat, control, PTES***

Abstract

Web application firewall is a method of protecting against threat attacks on web applications. The implementation of the web application firewall can block several attacks, in terms of security problems, it can be analyzed how efficient the web application firewall is in protecting web applications. In this study, the implementation and analysis of the web application firewall is carried out based on vulnerabilities and threats in testing attacks on web applications that have installed a web application firewall as a control. The experiment was conducted based on the PTES (Penetration Testing Execution Standard) standard as the basis for the exploitation of five vulnerabilities. Web application firewall is able to block three attacks, with efectivity 60% as quantitative result. While qualitative, using the results of vulnerability scanning with Acunetix based on the severity of the vulnerability that can be secured by web application firewall.

Keywords: ***web application firewall, vulnerability, threat, control, PTES***

1. Pendahuluan

Layanan IT berbasis web sangat popular seiring dengan perkembangan zaman dan pengguna aktif dunia internet dari seluruh dunia. Penggunaan aplikasi web memudahkan aktivitas dalam melakukan pertukaran informasi. Keamanan pada level aplikasi merupakan perlindungan aplikasi dari berbagai kemungkinan serangan. Dengan tidak adanya keamanan pada aplikasi maka akan ada banyak kemungkinan serangan dari para *attacker* yang memanfaatkan kerentanan. *Attacker* merupakan seseorang yang memiliki kemampuan cenderung untuk kepentingan tertentu. Kerentanan atau biasa disebut *vulnerability* dapat mengundang para *attacker* untuk melakukan serangan dengan tujuan *illegal*[1].

Mengamankan aplikasi web dapat dilakukan dengan memasang *firewall*, anti virus, dan lainnya. *Firewall* merupakan perangkat lunak dalam jaringan yang bisa melakukan pemantauan lalu lintas jaringan, dan membuat pembatas antara jaringan yang bisa terpercaya dan tidak terpercaya[2]. *Web application firewall* (WAF) adalah suatu metode pengamanan pada aplikasi web, untuk mencegah adanya ancaman dari *attacker*. Tujuan penggunaan *web application firewall* untuk meminimalkan serangan yang mungkin terjadi.

Penelitian ini, melakukan penelitian implementasi dan analisis *tool open source web application firewall* Menggunakan RaptorWAF pada DVWA dengan *Penetration Testing Execution Standard*. Analisis ini ditujukan untuk mengetahui efektivitas dari *tool* RaptorWAF dalam mendukung keamanan sebuah aplikasi web.

2. Dasar Teori

2.1 Aplikasi Web

Aplikasi berbasis web menggunakan protokol HTTP, pada sisi *server* akan berkomunikasi dengan *client*

melalui *web server*. Sebuah *client* HTTP seperti *web browser*, akan memulai permintaan atau *request* dengan membuat hubungan TCP/IP ke *port* tertentu, misalnya *port* 80 [3].

2.2 Aset IT

Aset IT merupakan pendukung operasional yang berkaitan dengan kegiatan yang ada, sehingga dalam pengelolaannya memiliki fungsi yang penting untuk menjaga kondisi aset IT tersebut[4].

2.3 *Vulnerability*

Vulnerability adalah kelemahan dalam sebuah desain sistem, impelementasi sebuah sistem atau operasi dan manajemen yang dapat untuk dimanfaatkan dalam melanggar kebijakan sebuah keamanan. *Vulnerability* dapat dipicu secara tidak sengaja atau dieksploitasi secara sengaja yang menyebabkan pelanggaran keamanan[5].

2.4 *Threat*

Threat yaitu kegiatan yang melakukan sebuah penelitian atau analisis untuk memutuskan kerentanan mana yang paling rentan terhadap ancaman dunia maya. Ancaman ini dianggap sebagai sesuatu yang berdampak negatif apabila memengaruhi *Confidentiality, Integrity, Availability* dalam suatu layanan[6].

2.5 *Control*

Control yaitu menempatkan langkah-langkah untuk mengelola ancaman / kerentanan yang teridentifikasi dimana dari tindakan, perangkat, prosedur, atau teknik tersebut dapat menghilangkan atau mengurangi kerentanan, ancaman dapat diblokir oleh kontrol kerentanan. *Control* merupakan pengaman yang melindungi sistem dari ancaman[7].

2.6 *Web Application Firewall*

Menurut *Web Application Security Consortium* (WASC) *Web application firewall* (WAF) diartikan sebagai sebuah perangkat perantara, yang berada antara *web client* dan *web server*, menganalisis pesan pada OSI Layer-7 ketika terjadi pelanggaran dalam kebijakan keamanan yang telah ditentukan. *Firewall* merupakan sebuah perangkat perantara, yang berada antara *web client* dan *web server*, menganalisis pesan pada OSI Layer-7 ketika terjadi pelanggaran dalam kebijakan keamanan yang telah ditentukan.

2.7 PTES

Teknis *Penetration Testing Execution Standard* (PTES) menentukan prosedur yang akan diikuti selama melakukan pengujian. Tujuan dari *Penetration Testing* adalah untuk mengidentifikasi titik-titik lemah dalam sistem keamanan organisasi khususnya system komputer [8]. Hasil laporan Tahapan PTES itu sendiri terdiri dari *Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation, Reporting.*

2.8 *Walkthrough*

Walkthrough merupakan cara untuk melakukan identifikasi dan menilai sejak awal apakah desain yang diusulkan memenuhi persyaratan dan memenuhi tujuan [9].

2.9 *Activity Diagram*

Activity Diagram merupakan serangkaian rancangan aliran aktivitas dalam sebuah sistem yang memiliki komponen dengan bentuk tertentu serta dihubungkan menggunakan tanda panah sebagai urutan aktivitas yang terjadi dari awal hingga akhir. *Activity Diagram* menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis[10].

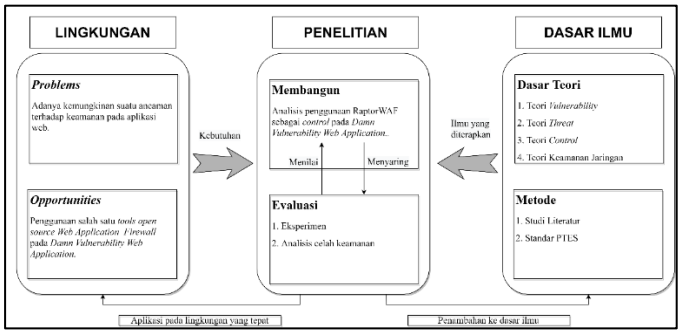
2.10 *Data Flow Diagram*

Data flow diagram digunakan oleh analis sistem untuk merancang sistem pemrosesan informasi tetapi juga sebagai cara untuk model seluruh organisasi[10].

3. Metodologi Penelitian

3.1 Model Konseptual Penelitian

Model konseptual ini bertujuan untuk memudahkan dalam melakukan proses identifikasi permasalahan yang ditemukan dalam penelitian. Model konseptual yang akan digunakan dalam penelitian ini adalah sebagai berikut:

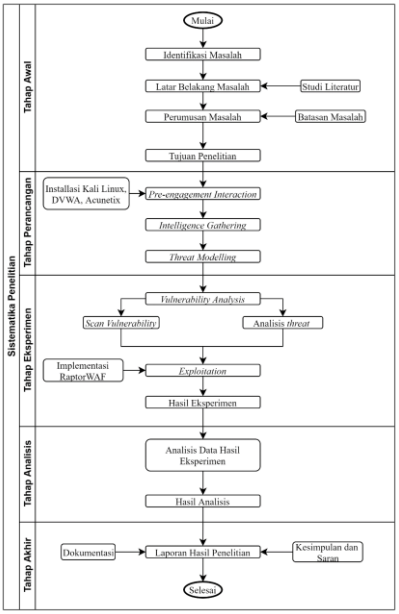


Gambar 1 Model Konseptual Penelitian

Dapat diketahui pada Gambar 1 bahwa terdapat tiga ruang lingkup yaitu lingkungan, penelitian dan dasar ilmu. Pada aspek lingkungan dipengaruhi oleh *problems* dan *opportunities* dimana hal tersebut mempengaruhi proses pada aplikasi web DVWA. Penelitian dilakukan untuk menganalisis efektivitas *Web Application Firewall* berdasarkan *vulnerability* dan *threat* yang dilakukan eksploitasi. Dasar ilmu yaitu berdasarkan teori *Vulnerability, Threat, Control,* Keamanan Aplikasi Web serta metode PTES *(Penetration Testing Execution Standards).*

3.2 Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah digunakan untuk menggambarkan alur penelitian yang akan dikerjakan sebagai gambaran untuk memecahkan masalah berikut:



Gambar 2 Sistematika Penyelesaian Masalah

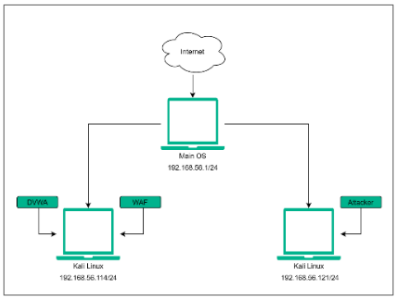
4. Perancangan dan Skenario Pengujian

4.1 *Pre-Engagement Interaction*

Pada tahap ini bertujuan menyediakan dan menjelaskan mengenai *tool* yang digunakan untuk membantu langkah suatu uji penetrasi. Pemilihan dan penggunaan *tool* yang tepat untuk suatu uji penetrasi akan bergantung pada hasil pengujian.

4.2 *Intelligence Gathering*

Pada tahap ini melakukan pencarian informasi atau mengumpulkan data terhadap target dengan memodelkan topologi eksperimen, IP *address* yang digunakan.



Gambar 3 Topologi Eksperimen

Pada Tabel 3 di bawah merupakan IP *address* yang digunakan pada penelitian kali ini:

Tabel 1 Daftar IP *Address*

Nama	*Host*	*Default Gateway*	IP *Address*
Main OS	Windows 10	192.168.56.1/24	192.168.56.1/24
VM1	Kali Linux Target		192.168.56.114/24
VM2	Kali Linux *Attacker*		192.168.56.121/24

4.3 *Threat Modelling*

Pada tahap ini membuat gambaran model ancaman berupa skenario pengujian berdasarkan *activity diagram* dan data *flow diagram*. *Threat modelling* dilakukan untuk dapat memahami serangan pada kerentanan yang didapatkan pada *vulnerability scanning*.

4.4 *Vulnerability Analysis*

Vulnerability Analysis merupakan tahap untuk mencari kerentanan dengan menggunakan *vulnerability scanning tool* yaitu Acunetix. Pada tahap ini bertujuan untuk mendapatkan kerentanan yang dapat dimanfaatkan oleh *attacker*.

4.5 *Exploitation*

Pada tahap eksploitasi dilakukan pengujian terhadap kerentanan yang didapatkan. Tujuan pada tahap ini adalah untuk mengetahui efektivitas RaptorWAF sebagai *web application firewall* dalam melindungi aset IT.

5. Analisis

5.1 Analisis *Vulnerability Scanning* Berdasarkan Data dari Acunetix

SQL *Injection* merupakan teknik yang menyalahgunakan kerentanan yang ada untuk mengakses *database*. Serangan dari kerentanan ini dapat menyebabkan *sharing* data ke tangan pihak yang tidak berwenang. Pada OWASP Top 10 termasuk kedalam *Injection* (A1) karena *attacker* bisa mendapatkan data dari *database* dengan menjalankan perintah yang tidak diinginkan. *Cross Site Scripting* merupakan serangan pada sisi *client* yang dapat menampilkan *script* berbahaya yang ditampilkan oleh *attacker*. Pada OWASP Top 10 termasuk kedalam *Cross Site Scripting* (A7) karena *attacker* dapat menggunakan XSS untuk mengirimkan skrip yang berbahaya ke pengguna tanpa curiga.

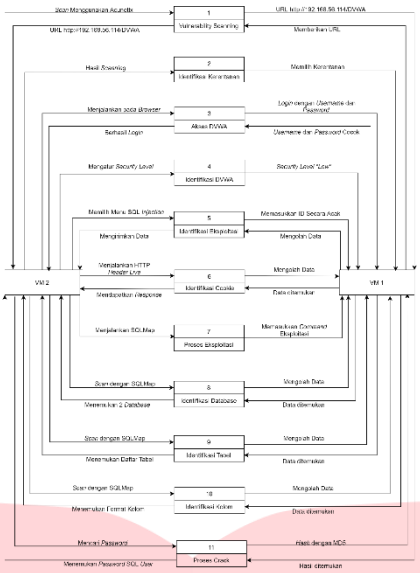
.

5.2 Perancangan *Data Flow Diagram*

Perancangan *walkthrough* ini dilakukan dengan langkah-langkah yang paling efisien dalam melakukan eksploitasi dan nantinya akan dilihat hasil eksploitasi apakah berhasil ditolak oleh WAF atau tidak.

a. Pengujian SQL *Injection* tanpa WAF

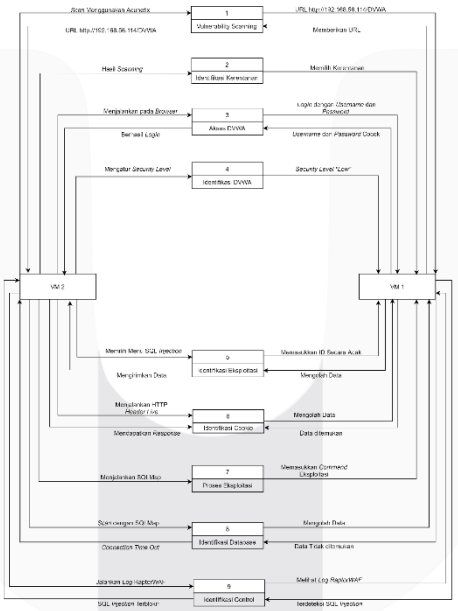
Pengujian pada *vulnerability scanning* didapatkan kerentanan SQL *Injection* sehingga dapat dilakukan eksploitasi menggunakan *tool* SQLMap. *Attacker* melakukan mengumpulkan informasi HTTP *Header* menggunakan HTTP Header Live kemudian dilakukan *command* eksploitasi. Dari hasil serangan yang dilakukan dengan memasukkan *command* didapatkan daftar *database*, tabel, kolom serta *username* dan *password*.



Gambar 4 Pengujian SQL Injection tanpa WAF

b. Pengujian SQL *Injection* terpasang WAF

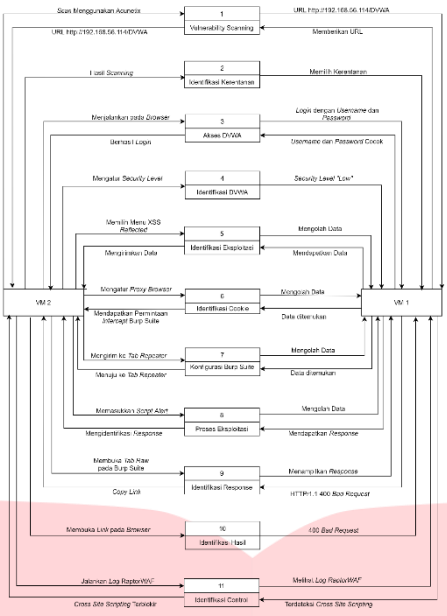
Pengujian pada *vulnerability scanning* didapatkan kerentanan SQL *Injection* sehingga dapat dilakukan eksploitasi menggunakan *tool* SQLMap. *Attacker* melakukan mengumpulkan informasi HTTP *Header* menggunakan HTTP Header Live kemudian dilakukan *command* eksploitasi. Dari hasil serangan yang dilakukan dengan memasukkan *command* pada *log* RaptorWAF terdeteksi SQL *Injection* sehingga serangan yang coba dilakukan berhasil ditolak.



Gambar 5 Pengujian SQL *Injection* Terpasang WAF

c. Pengujian *Cross-Site Scripting* Tanpa WAF

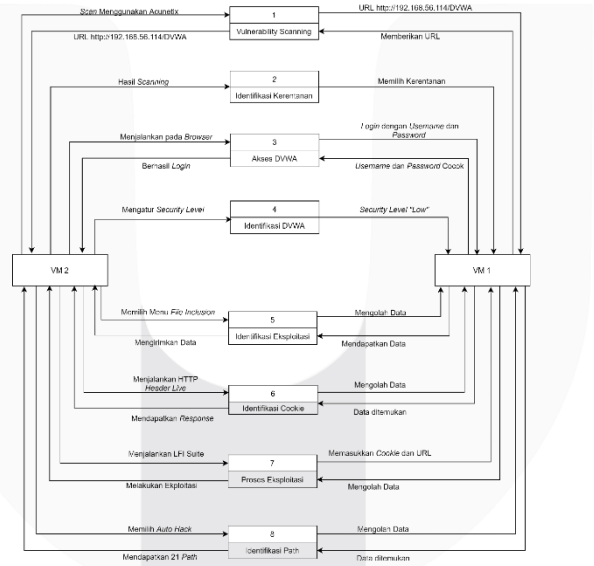
Pengujian pada *vulnerability scannin*g didapatkan kerentanan *Cross-Site Scripting* sehingga dapat dilakukan eksploitasi menggunakan *tool* Burp Suite. *Attacker* melakukan mengumpulkan informasi HTTP *Header* menggunakan Burp Suite kemudian dilakukan *command* eksploitasi. Dari hasil serangan yang dilakukan dengan memasukkan *script* yang berbahaya melalui Burp Suite, dapat memunculkan *pop up* pada halaman pengguna.



Gambar 6 Pengujian *XSS* Tanpa WAF

d. Pengujian *Cross-Site Scripting* Tanpa WAF

Pengujian pada *vulnerability scanning* didapatkan kerentanan *Cross-Site Scripting* sehingga dapat dilakukan eksploitasi menggunakan *tool* Burp Suite. *Attacker* melakukan mengumpulkan informasi HTTP *Header* menggunakan Burp Suite kemudian dilakukan *command* eksploitasi. Dari hasil serangan yang dilakukan dengan memasukkan *script* yang berbahaya melalui Burp Suite, pada *log* RaptorWAF terdeteksi *Cross-Site Scripting* sehingga serangan yang coba dilakukan berhasil ditolak.



Gambar 7 Pengujian *XSS* Terpasang WAF

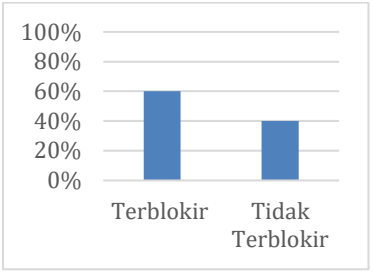
5.3 Analisis *Control* Secara Kuantitatif Berdasarkan *Vulnerabilty* dan *Threat*

Control merupakan langkah untuk mengelola ancaman atau kerentanan yang teridentifikasi dari tindakan tersebut yang dapat menghilangkan atau mengurangi kerentanan. Tabel 2 mendefinisikan hubungan antara *vulnerability*, *threat*, *control* setelah dilakukan eksploitasi, dimuali dari mendapatkan *vulnerability* menggunakan Acunetix, kemudian melakukan analisis *threat* dari *vulnerability* yang ada, serta implementasi RaptorWAF sebagai *control* dalam melindungi DVWA terhadap eksploitasi.

Tabel 2 Hasil RaptorWAF

Vulnerability	*Threat*	*Control*
SQL Injection	SQL *Injection*	Terblokir
Cross site scripting	*Cross Site Scripting*	Terblokir

Possible sensitive files	*Local File Inclusion*	Terblokir
Login page password-guessing attack	*Brute Force*	Tidak Terblokir.
Clickjacking: X-Frame-Options header missing	*Clickjacking*	Tidak terblokir



Gambar 8 Grafik Persentase

$$\frac{\text{Serangan } Threat \text{ Terblokir}}{\text{Total Serangan } Threat} \text{ x } 100\%$$

$$\frac{3}{5} \text{ x } 100\% = 60\%$$

Perhitungan secara kuantitatif berdasarkan serangan yang dilakukan pada DVWA dengan implementasi RaptorWAF sebagai *web application firewall*, didapatkan hasil 60% dari lima serangan yang dilakukan berhasil menolak tiga serangan. RaptorWAF sebagai *control defensive* untuk memperkuat perlindungan aset IT berdasarkan *vulnerability, threat, dan control*. Persentase yang didapatkan merupakan hitungan *relative* berdasarkan banyaknya percobaan yang dilakukan. Dalam hal ini, RaptorWAF tidak dapat melindungi aset IT secara sempurna, namun di angka 60% terbilang cukup tinggi karena mampu melindungi lebih dari 50% serangan *threat*. Gambar grafik merepresentasikan total dari serangan apakah terblokir atau tidak terblokir oleh RaptorWAF. Sumbu X mendefinisikan kategori terblokir dan tidak terblokir. Sedangkan sumbu Y mendefinisikan jumlah serangan *threat* yang terblokir dan tidak terblokir.

Tabel 3 Daftar Kerentanan Berdasarkan Skor

Vulnerability	CWE	CVE	CVSS3
SQL Injection	CWE-89	CVE-2017-11508	10.0
Possible sensitive files	CWE-200	CVE-2007-5172	7.5
Login page password-guessing attack	CWE-307	CVE-1999-1152	5.3
Cross site scripting	CWE-79	CVE-2017-9764	5.3
Clickjacking: X-Frame-Options header missing	CWE-693	CVE-2019-13924	4.3

1. SQL *Injection*
   Kerentanan ini termasuk kedalam CWE-89 *(Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'))* dimana seorang *attacker* dapat dengan mudah mendeteksi dan mengeksploitasi kerentanan *injection*. Kerentanan ini muncul dalam aplikasi seperti data yang menyimpan input pengguna dalam *database*. Pada penilaian default skor CVSS3 di Acunetix mendapatkan skor 10.
2. *Possible sensitive files*
   Kerentanan ini termasuk kedalam CWE-200 *(Exposure of Sensitive Information to an Unauthorized Actor)* yang membuat informasi sensitif tersedia bagi *attacker*, di mana kerentanannya adalah masalah kualitas yang mungkin secara tidak langsung mempermudah atau mempersulit untuk dideteksi. Pada penilaian default skor CVSS3 di Acunetix mendapatkan skor 7.5.
3. *Login page password-guessing attack*
   Kerentanan ini termasuk kedalam CWE-307 *(Improper Restriction of Excessive Authentication Attempts)* dimana seorang *attacker* dapat melakukan sejumlah upaya otentikasi yang sewenang-wenang dengan menggunakan kata sandi yang berbeda, dan akhirnya mendapatkan akses ke akun yang ditargetkan. Pada penilaian default skor CVSS3 di Acunetix mendapatkan skor 5.3.
4. *Cross site scripting*
   Kerentanan ini termasuk kedalam CWE-79 *(Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))* terlepas dari apakah itu disimpan atau dipantulkan ke sisi *client*. XSS dapat menyebabkan berbagai masalah bagi *client*, diantaranya kerentanan skrip dapat dieksploitasi untuk memanipulasi atau mencuri *cookie*, membuat permintaan yang dapat disalahartikan sebagai permintaan pengguna yang *valid*, atau mengeksekusi kode berbahaya. Pada penilaian default skor CVSS3 di Acunetix mendapatkan skor 5.3.
5. *Clickjacking: X-Frame-Options header missing*
   Kerentanan ini termasuk kedalam CWE-693 *(Protection Mechanism Failure)* yang mencakup tiga situasi yang berbeda. Mekanisme perlindungan hilang, tidak memadai dan diabaikan sehingga bisa dilakukan kemungkinan serangan oleh *attacker*. Pada penilaian default skor CVSS3 di Acunetix mendapatkan skor 4.3.

5.4 Analisis *Control* Secara Kualitatif Berdasarkan *Vulnerability* dan *Threat*

Analisis secara kualitatif untuk mengukur tingkat keparahan berdasarkan *High, Medium, Low level.* Pada tabel terdapat hasil data kerentanan dengan kualitas *severity* seperti berikut:

Tabel 4 *Severity* Kerentanan

Vulnerability	*Severity*
SQL Injection	*High*
Cross site scripting	*High*
Possible sensitive files	*Low*
Login page password-guessing attack	*Low*
Clickjacking: X-Frame-Options header missing	*Low*

Berdasarkan kualitas *severity* dari kerentanan yang didapatkan dan dilakukan eksploitasi, didapatkan *severity* yang terdiri dari dua *High* dan tiga *Low*. *Severity high* merupakan kerentanan yang paling berbahaya dan paling sering dilakukan serangan. Dalam hal ini RaptorWAF mampu menolak dua serangan dengan *severity High*. Sedangkan *Severity Low* merupakan kerentanan dimana kurangnya enkripsi data pada aplikasi web. Dalam hal ini RaptorWAF mampu menolak satu dari tiga serangan dengan *severity low*.

6. Kesimpulan

Pengujian lima serangan yang dilakukan meghasilkan perhitungan kuantitatif terhadap efektivitas RaptorWAF sebagai *control* aset IT yaitu sebesar 60%. Pengujian serangan berdasarkan *vulnerability* dan *threat* terhadap aset IT baik sebelum dan sesudah diimplementasikan RaptorWAF didapatkan tiga serangan berhasil diblokir diantaranya SQL *Injection, Cross-Site Scripting* dan *Local File* sedangkan dua lainnya yang tidak berhasil diblokir adalah *Clickjacking* dan *Brute Force.*

REFERENSI

[1] Mira Orisa and M. Ardita, "Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web," *J. Mnemon.*, vol. 4, no. 1, pp. 16–19, 2021, doi: 10.36040/mnemonic.v4i1.3213.

[2] S. Rheno Widianto and I. Abdullah Azzam, "Analisis Upaya Peretasan Web Application Firewall dan Notifikasi Serangan Menggunakan Bot Telegram pada Layanan Web Server," *Elektra*, vol. 3, no. 2, pp. 19–28, 2018.

[3] A. A. Zabar and F. Novianto, "Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux," *Komputa J. Ilm. Komput. dan Inform.*, vol. 4, no. 2, pp. 69–74, 2015, doi: 10.34010/komputa.v4i2.2427.

[4] Z. Rahman, A. P. Widodo, and A. Sukmaaji, "Sistem Informasi Manajemen Aset Ti Pada Kementerian Issn 2338-137X," vol. 5, no. 5, pp. 1–6, 2016.

[5] G. Learning, "CompTIA Security+ Official Study Guide," p. 335, 2014.

[6] A. ud D. Shafiq, "Vulnerability Threat Control Paradigm and CIA Triads – Computer Security," 2019. https://dzone.com/articles/vulnerability-threat-control-paradigm-and-cia-tria.

[7] T. Adiprabowo, "Metoda Pengajaran Manajemen Resiko Teknologi Informasi Di Perguruan Tinggi," *Semin. Nas. Sist. Inf. Indones.*, pp. 209–214, 2013.

[8] F. Y. Fauzan, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang dari keamanan web adalah sebanyak 96 dengan disimpulkan Acunetix Threat Level 2 yaitu pada level Medium yang artinya tidak ," vol. 9, no. 2, 2021.

[9] M. A. Rabbani, A. Budiyono, and A. Widjajarto, "IMPLEMENTASI DAN ANALISIS SECURITY AUDITING MENGGUNAKAN OPEN SOURCE SOFTWARE DENGAN FRAMEWORK MITRE ATT & CK IMPLEMENTATION AND ANALYSIS OF SECURITY AUDITING USING OPEN SOURCE SOFTWARE WITH MITRE ATT & CK FRAMEWORK," 2020.

[10] Hendini, "Field Assessment and Inheritance of Cassava Resistance to Superelongation Disease 1," *Crop Sci.*, 2016, doi: 10.2135/cropsci1983.0011183x002300020002x.