CESS (Journal of Computer Engineering System and Science) **p-ISSN :2502-7131**
Vol. 5 No. 2 Juli 2020 **e-ISSN :2502-714x**

ANALISIS KEAMANAN SISTEM INFORMASI BERBASIS WEBSITE DENGAN METODE *OPEN WEB APPLICATION SECURITY PROJECT* (OWASP) VERSI 4: *SYSTEMATIC REVIEW*

Anggi Elanda[1], Robby Lintang Buana[2]

[1,2] *STMIK ROSMA*
Jl. Kertabumi No. 62 Karawang 41311
[1]anggi@rosma.ac.id, [2]robby.buana@mhs.rosma.ac.id

Abstrak—**OWASP (Open Web Application Security Project) versi 4 yang dikeluarkan oleh organisasi none profit yang bernama owasp.org yang berdedikasi pada keamanan aplikasi berbasis web. Systematic review ini ditujukan untuk mengulas apakah metode Open Web Application Security Project (OWASP) banyak digunakan untuk mendeteksi keamanan di dalam sebuah Sistem Informasi berbasis website. Dalam systematic review ini, kami mengulas 3 literatur dari beberapa sumber penerbit dan melakukan komparasi terkait hasil OWASP versi 4 dan tingkat keamanan dari sebuah web server dari sumber penerbit.**

Kata Kunci— **OWASP, Kerentanan *Website*, Pendeteksian Keamanan *Website***

Abstract— **OWASP (Open Web Application Security Project) version 4 issued by a non-profit organization called owasp.org which is dedicated to the security of web-based applications. This systematic review is intended to review whether the Open Web Application Security Project (OWASP) method is widely used to detect security in a website-based Information System. In this systematic review, we review 3 literature from several publisher sources and make a comparison regarding OWASP version 4 results and the security level of a web server from the publisher's source.**

Keywords— ***OWASP, Website Vulnerability, Website Security Detection***

I. PENDAHULUAN

Aplikasi web server sering kali mendapatkan serangan dari berbagai pihak yang tidak bertanggung jawab yang sering kali disebut *hacker* atau peretas. Berbagai macam alasan *hacker* mencari celah pada web server bertujuan untuk mendapatkan informasi pada sebuah organisasi dan perusahaan untuk kepentingan – kepentingan yang membuat kerugian pada pihak lain. Salah satu metode untuk menguji keamanan aplikasi berbasis web adalah metode OWASP. OWASP merupakan organisasi non-profit amal di Amerika Serikat yang didirikan pada tanggal 21 April 2004 yang berdedikasi untuk membuat *framework* pengujian keamanan yang bebas digunakan oleh siapa saja.

Mengetahui celah keamanan sendiri tidak akan membantu manajemen untuk meningkatkan keamanan pada aplikasi. Melakukan penilaian pada resiko aplikasi dengan mempertimbangkan perbedaan faktor-faktor yang terkait dengan aplikasi akan memberikan penjelasan yang lebih dan menodong untuk mengamankan aplikasi lebih baik lagi. Dengan mengikuti pendekatan ini, organisasi dapat memperkirakan tingkat kerentanan aplikasi dan dapat membuat keputusan mengenai resiko tersebut. Juga faktor resiko akan memprioritaskan masalah pada aplikasi dengan cara yang lebih baik daripada pendekatan yang dilakukan secara acak. Bagian yang memiliki lebih banyak resiko dapat secara cepat di tindak lanjuti dan selanjutnya ke prioritas berikutnya.

Framework yang digunakan pada OWASP versi 4 adalah sebagai berikut : (1) *Authentication Testing*, Otentikasi merupakan tindakan membangun dan mengkonfirmasi sesuatu bahwa klaim yang dibuat adalah benar. (2) *Authorization Testing*, Otorisasi merupakan konsep yang memungkinkan akses ke sumber daya bagi mereka yang diizinkan untuk menggunakannya. (3) *Session Management Testing*, didefinisikan sebagai himpunan semua kontrol yang mengatur interaksi *fullstate* antara pengguna dan aplikasi berbasis web. Dalam *systematic review* ini, membahas hasil dari pengujian OWASP versi 4 dan tingkat keamanan dari sebuah web server dari beberapa jurnal penerbit.

II. METODE

Metode yang digunakan dalam melakukan *systematic review* ini berbasis pada *protocol* PRISMA (*Preferred Reporting Item for Systematic Review and Meta-Analysis*) [1]. PRISMA menyediakan sebanyak 27 *check list* dalam penulisan *systematic review*.

Literatur yang kami ulas ialah literatur yang membahas tentang Analisis Keamanan Sistem Informasi berbasis website dan menggunakan aplikasi OWASP sebagai metode pengenalannya. Kriteria kelayakan kami terapkan pada literatur yang kami ulas, yaitu literatur yang diterbitkan pada penerbit

dalam bidang Computer Science yang sudah memiliki reputasi baik dan terindeks Scopus. Dalam hal ini, kami memilih literatur yang diterbitkan oleh Perpustakaan Nasional Indonesia. Kami hanya memilih literatur yang diterbitkan pada 2014 atau lebih demi menjamin hasil analisis sistem keamanan yang akan kami ulas. Ada Batasan tipe literatur yang akan kami ulas. Kami hanya menerima jurnal akademik.

Dalam mencari literatur kami menggunakan kata kunci sebagai berikut di Penerbit Perpustakaan Nasional indonesia :

- "OWASP" & Analisis Keamanan WebServer
- "Open Web Application Security Project"
- Uji Kerentanan WebServer
- "OWASP Top 10"
- Keamanan WebServer

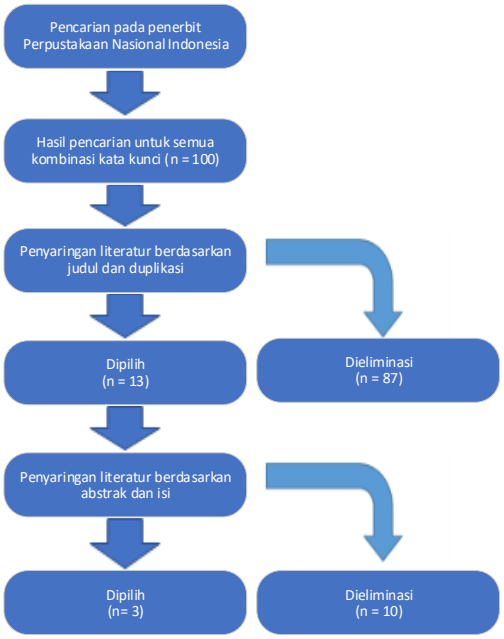
Referensi yang terkumpul dari proses pencarian akan mengalami beberapa penyaringan. Pada penyaringan pertama, kami mengeliminasi semua literatur yang bukan jurnal akademik dan hanya menerima literatur yang bersifat terbuka untuk publik. Pada penyaringan kedua, kami menilai relevansi literatur berdasarkan judul dan mengeliminasi literatur yang tidak bersesuaian. Setelah itu, kami mengeliminasi beberapa literatur yang duplikat. Selanjutnya, kami memastikan kembali relevansi literatur dengan membaca abstrak dan melakukan skimming isi literatur. Proses penyaringan literatur dilakukan secara independent oleh kami.

Setelah referensi literatur didapatkan, kami melakukan pratinjau terhadap bahan tulisan yang akan dijadikan rujukan dalam kajian systematic review ini. Kemudian hasil dari pratinjau tersebut kami muat ke dalam sebuah rangkuman (summary) yang memuat tentang: 1) Tahap yang ditawarkan, dan 2) hasil yang diperoleh dari masing-masing literatur. Proses pemilihan data untuk dimasukkan ke dalam tabel dilakukan dengan mengacu pada persamaan Tahap yang ada pada literatur penerbit. Dalam systematic review ini, kami memfokuskan komparasi pada Tahap yang ditawarkan dan hasil yang diperoleh. Proses validasi bahan bacaaan dilakukan dengan menggunakan metode peer review yang dilakukan oleh kami terhadap bahan bacaan yang dibaca oleh kami lainnya.

III. HASIL DAN PEMBAHASAN

Pencarian yang dilakukan di Perpustakaan Nasional Indonesia menghasilkan total sitasi sebanyak 100. Namun, dari 100 sitasi itu, dilakukan proses penyaringan berdasarkan judul, Kami hanya memilih referensi dengan judul yang sesuai dengan topik systematic review ini. Setelah melakukan penyaringan berdasarkan kesesuaian judul dan mengeliminasi beberapa literatur yang duplikat, kami mendapatkan sebanyak 13 literatur yang relevan.

Setelah itu, Kami melakukan penyaringan kembali literatur yang didapatkan untuk mendapatkan literatur yang benar-benar sesuai dengan kriteria topik systematic review ini. Penyaringan terakhir ini kami lakukan dengan membaca abstrak dan skimming literatur. Pada tahap akhir ini kami mendapat 3 literatur yang memenuhi syarat. Hasil tersebut yang kami jadikan referensi untuk melakukan literatur review.



Gbr. 1 Alur proses pencarian literatur

Karakteristik literatur yang kami terima ialah literatur yang memiliki kesesuaian dengan topik yaitu membahas tentang Analisis Keamanan Sistem Informasi WebServer dengan menggunakan metode OWASP. kami hanya menerima tipe literatur akademik jurnal dan dapat diunduh dengan jenis PDF yang diterbitkan hanya pada tahun 2014 atau lebih.

Dalam membandingkan ketiga literatur kami membuat enam tabel yaitu :

a. Tabel 1 Identifikasi Sistem Informasi yang diuji dan Hasil Pengujian OWASP versi 4 (Authentication Testing) yang terdiri dari 8 Kolom, yaitu : Sistem Informasi/WebServer yang diteliti kerentanannya ; Penggunaan Tools Acunetix Web Vulnerability Scanner;Acunetix Threat Level;Tahap OTG-AUTHN-001; Tahap OTG-AUTHN-002; Tahap OTG-AUTHN-003; Tahap OTG-AUTHN-004; Tahap OTG-AUTHN-005
b. Tabel 2 Hasil Pengujian OWASP versi 4 (Authentication Testing dan Authorization Testing) yang terdiri dari 9 Kolom yaitu : Tahap OTG-AUTHN-006; Tahap OTG-AUTHN-007; Tahap OTG-AUTHN-008; Tahap OTG-AUTHN-009; Tahap OTG-AUTHN-010; Tahap OTG-AUTHZ-001; Tahap OTG-AUTHZ-002; Tahap OTG-AUTHZ-003; Tahap OTG-AUTHZ-004.

c. Tabel 3 Hasil Pengujian OWASP versi 4 (Session Testing) yang terdiri dari 8 kolom yaitu : Tahap OTG-SESS-001; Tahap OTG-SESS-002; Tahap OTG-SESS-003; Tahap OTG-SESS-004; Tahap OTG-SESS-005; Tahap OTG-SESS-006; Tahap OTG-SESS-007; Tahap OTG-SESS-008.
d. Tabel 4 Tools Pengujian OWASP versi 4 (Authentication Testing) yang terdiri dari 8 Kolom, yaitu : Tools OTG-AUTHN-001; Tools OTG-AUTHN-002; Tools OTG-AUTHN-003; Tools OTG-AUTHN-004; Tools OTG-AUTHN-005; Tools OTG-AUTHN-006; Tools OTG-AUTHN-007; Tools OTG-AUTHN-008.
e. Tabel 5 Tools Pengujian OWASP versi 4 (Authentication Testing, Authorization Testing dan Session Testing) yang terdiri dari 8 Kolom, yaitu : Tools OTG-AUTHN-009; Tools OTG-AUTHN-010; Tools OTG-AUTHZ-001; Tools OTG-AUTHZ-002; Tools OTG-AUTHZ-003; Tools OTG-AUTHZ-004; Tools OTG-SESS-001; Tools OTG-SESS-002.
f. Tabel 6 Tools Pengujian OWASP versi 4 (Session Testing) yang terdiri dari 6 Kolom yaitu, : Tools OTG-SESS-003; Tools OTG-SESS-004; Tools OTG-SESS-005; Tools OTG-SESS-006; Tools OTG-SESS-007; Tools OTG-SESS-008.

TABEL I
IDENTIFIKASI SISTEM INFORMASI YANG DIUJI DAN HASIL PENGUJIAN OWASP VERSI 4 (AUTHENTICATION TESTING)

Literatur	Sistem Informasi/Webserver	Memakai Acunetix	Acunetix Threat Level	OTG-AUTHN-001	OTG-AUTHN-002	OTG-AUTHN-003	OTG-AUTHN-004	OTG-AUTHN-005
[2]	Aplikasi Ujian Online	Ya	Level 3 : High	Tidak Lolos	Lolos	Tidak Lolos	Tidak Lolos	Tidak Lolos
[6]	Website www.xyz.com	Tidak	-	Lolos	Lolos	Lolos	Lolos	Lolos
[7]	WebServer	Ya	Level 2 : Medium	Tidak Lolos	Lolos	Tidak Lolos	Tidak Lolos	Tidak Lolos

Berdasarkan Tabel I : Sistem Informasi Literatur [2] yang diuji oleh OWASP versi 4 adalah Aplikasi Ujian Online. Pengujian Sistem Informasi Literatur 2 menggunakan aplikasi Acunetix dengan Threat Level dengan hasil Level 3 : High. Literatur [6] menggunakan Website www.xyz.com dan tidak menggunakan aplikasi Acunetix. Dalam Literatur [7] menguji WebServer dan menggunakan aplikasi Acunetix dengan Threat Level dengan hasil Level 2 : Medium.

Dalam hasil pengujian OWASP versi 4 tahapan pertama yaitu Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001), Aktifitas yang dilakukan pada tahap ini yaitu : Memastikan bahwa data pengguna kredensial terenkripsi dari web browser ke server dan memastikan halaman login diakses melalui HTTPS. Dalam tahap ini Literatur [2] dan Literatur [7] dinyatakan tidak lolos sedangkan Literatur [6] dinyatakan Lolos.

Pada tahap berikutnya yaitu Testing for default credentials (OTG-AUTHN-002), Aktifitas yang dilakukan pada tahap ini yaitu : Memeriksa konfigurasi dan password default dari halaman login dengan prediksi. Dalam tahap ini Literatur [2], Literatur [6] dan Literatur [7] dinyatakan Lolos.

Tahap berikutnya yaitu Testing for Weak lock out mechanism (OTG-AUTHN-003), Aktifitas yang dilakukan pada tahap ini yaitu : Menguji dengan beberapa kali salah login untuk memeriksa apakah terjadi lock out atau pemblokiran. Dalam tahap ini Literatur [2] dan Literatur [7] dinyatakan Tidak Lolos sedangkan Literatur [6] dinyatakan Lolos.

Tahap berikutnya yaitu Testing for bypassing authentication schema (OTG-AUTHN-004), Aktifitas yang dilakukan pada tahap ini yaitu : Menguji skema otentikasi dengan memanfaatkan log dihalaman dengan memodifikasi parameter URL. Dalam tahap ini Literatur [2] dan Literatur [7] dinyatakan Tidak Lolos sedangkan Literatur [6] dinyatakan Lolos. Tahap berikutnya yaitu Test remember password functionality (OTG-AUTHN-005), Aktifitas yang dilakukan pada tahap ini yaitu : Pengujian dengan melihat log password yang disimpan dan autocomplete yang masih diaktifkan. Dalam tahap ini Literatur [2] dan Literatur [7] dinyatakan tidak lolos sedangkan Literatur [5] dinyatakan Lolos.

TABEL II
HASIL PENGUJIAN OWASP VERSI 4 (AUTHENTICATION TESTING DAN AUTHORIZATION TESTING)

Literatur	OTG-AUTHN-006	OTG-AUTHN-007	OTG-AUTHN-008	OTG-AUTHN-009	OTG-AUTHN-010	OTG-AUTHZ-001	OTG-AUTHZ-002	OTG-AUTHZ-003	OTG-AUTHZ-004
[2]	Tidak Lolos	Lolos	Lolos	Lolos	Lolos	Lolos	Tidak Lolos	Lolos	Tidak Lolos
[6]	Tidak Lolos	Lolos	-	-	-	Lolos	Lolos	Lolos	-
[7]	Tidak Lolos	Lolos	Tidak Lolos	Lolos	Lolos	Lolos	Tidak Lolos	Lolos	Tidak Lolos

Berdasarkan Tabel II Dalam hasil pengujian OWASP versi 4 pada tahap ke-6 yaitu : Testing for Browser cache weakness (OTG-AUTHN-006), Aktifitas yang dilakukan pada tahap ini yaitu : Penguji cache browser dari tombol “back” untuk melihat sumber daya yang ditampilkan sebelumnya. Dalam tahap ini Literatur [2], Literatur [6] dan Literatur [7] dinyatakan Tidak Lolos.

Tahap berikutnya yaitu : Testing for Weak password policy (OTG-AUTHN-007), Aktifitas yang dilakukan pada tahap ini yaitu : Melakukan brute force menggunakan kamus password. Dalam tahap ini Literatur [2], Literatur [6] dan Literatur [7] dinyatakan Lolos.

Tahap berikutnya yaitu : Testing for Weak security question/answer (OTG-AUTHN-008). Dalam tahap ini Literatur [2] dinyatakan Lolos sedangkan Literatur [7]

dinyatakan Tidak Lolos dan Literatur [6] tidak melakukan pengujian di tahap ini.

Tahap berikutnya yaitu : Testing for weak password change or reset functionalities (OTG-AUTHN-009). Dalam tahap ini Literatur [2] dan Literatur [7] dinyatakan Lolos sedangkan Literatur [6] tidak melakukan pengujian di tahap ini.

Tahap berikutnya yaitu : Testing for Weaker authentication in alternative channel (OTG-AUTHN-010). Dalam tahap ini Literatur [2], Literatur [7] dinyatakan Lolos sedangkan Literatur [6] tidak melakukan pengujian di tahap ini.

Tahap berikutnya yaitu : Testing Directory traversal/file include (OTG-AUTHZ-001), Aktifitas yang dilakukan pada tahap ini yaitu : Percobaaan akses web document root atau root directory, dengan menyisipkan string seperti menebak lokasi file seperti \\server_or_ip\path\to\file.abc untuk sistem operasi Windows. Dalam tahap ini Literatur [2], Literatur [6] dan Literatur [7] dinyatakan Lolos.

Tahap berikutnya yaitu : Testing for bypassing authorization schema (OTG-AUTHZ-002), Aktifitas yang dilakukan pada tahap ini yaitu : Percobaan dilakukan pada halaman administrator, Apakah dapat diakses secara langsung tanpa adanya proses autentifikasi pada alamat admin. Dalam tahap ini Literatur [2] dan Literatur [7] dinyatakan Tidak Lolos sedangkan Literatur [6] dinyatakan Lolos.

Tahap berikutnya yaitu : Testing for Privilege Escalation (OTG-AUTHZ-003), Aktifitas yang dilakukan pada tahap ini yaitu : Menguji kesalahan pemrograman yang memungkinkan pengguna mendapatkan hak istimewa dengan memeriksa hidden field HTML. Dalam tahap ini Literatur [2], Literatur [6] dan Literatur [7] dinyatakan Lolos.

Tahap berikutnya yaitu : Testing for Insecure Direct Object References (OTG-AUTHZ-004) Dalam tahap ini Literatur [2] dan Literatur [7] dinyatakan Tidak Lolos sedangkan Literatur [6] tidak melakukan pengujian di tahap ini.

TABEL IIIII
HASIL PENGUJIAN OWASP VERSI 4 (SESSION TESTING)

Literatur	OTG-SESS-001	OTG-SESS-002	OTG-SESS-003	OTG-SESS-004	OTG-SESS-005	OTG-SESS-006	OTG-SESS-007	OTG-SESS-008
[2]	Tidak Lolos	Lolos	Lolos	Lolos	Tidak Lolos	Lolos	Tidak Lolos	Tidak Lolos
[6]	Lolos	Lolos	Lolos	Lolos	Lolos	Lolos	Lolos	-
[7]	Tidak Lolos	Lolos	Lolos	Lolos	Tidak Lolos	Lolos	Lolos	Tidak Lolos

Berdasarkan Tabel III Dalam pengujian OWASP versi 4 pada tahap-15 yaitu : Testing for Bypassing Session Management Schema (OTG-SESS-001), Aktifitas yang dilakukan pada tahap ini yaitu : Pengujian dilakukan pada session cookies yang dikirim oleh server dengan cara melakukan percobaan akses halaman dengan cookie, kemudian coba lagi tanpa cookie apakah rentan terhadap hijacking. Dalam tahap ini Literatur [2] dan Literatur [7] dinyatakan Tidak Lolos sedangkan Literatur [6] dinyatakan Lolos.

Tahap berikutnya yaitu : Testing for Cookies attributes (OTG-SESS-002), Aktifitas yang dilakukan pada tahap ini yaitu : Pengujian terhadap atribut cookies yang digunakan apakah sudah menggunakan secure attribute, http only attribute, domain attribute, path attribute, expires attribute. Dalam tahap ini Literatur [2], Literatur [6] dan Literatur [7] dinyatakan Lolos.

Tahap berikutnya yaitu : Testing for Session Fixation (OTG-SESS-003), Aktifitas yang dilakukan pada tahap ini yaitu : Melakukan pengujian terhadap session ID apakah terjadi pembaharuan session ID setelah otentikasi berhasil. Dalam tahap ini Literatur [2], Literatur [6] dan Literatur [7] dinyatakan Lolos.

Tahap berikutnya yaitu : Testing for Exposed Session Variables (OTG-SESS-004), Aktifitas yang dilakukan pada tahap ini yaitu : Pengujian terhadap cookies, session id, hidden field, apakah apakah setiap kali proses otentikasi berhasil, user menerima token sesi yang berbeda melalui channel yang dienkripsi setiap kali melakukan permintaan HTTP. Dalam tahap ini Literatur [2], Literatur [6] dan Literatur [7] dinyatakan Lolos.

Tahap berikutnya yaitu : Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005), Aktifitas yang dilakukan pada tahap ini yaitu : Memeriksa apakah aplikasi rentan dengan serangan Cross Site Request Forgery (CSRF) dimana serangan ini dapat memanipulasi alamat URL yang valid. Dalam tahap ini Literatur [2] dan Literatur [7] dinyatakan Tidak Lolos sedangkan Literatur [6] dinyatakan Lolos.

Tahap berikutnya yaitu : Testing for logout functionality (OTG-SESS-006), Aktifitas yang dilakukan pada tahap ini yaitu : Pengujian terhadap serangan cross site scripting apakah terdapat validasi halaman. Dalam tahap ini Literatur [2], Literatur [6] dan Literatur [7] dinyatakan Lolos.

Tahap berikutnya yaitu : Test Session Timeout (OTG-SESS-007), Aktifitas yang dilakukan pada tahap ini yaitu : Pengujian terhadap batas waktu diam pada aplikasi untuk jumlah waktu tertentu, apakah terdapat log out otomatis, dan memastikan tidak dapat menggunakan tombol back pada sesi yang sama. Dalam tahap ini Literatur [2] dinyatakan Tidak Lolos sedangkan Literatur [6] dan Literatur [7] dinyatakan Lolos.

Tahap berikutnya yaitu Testing for Session puzzling (OTG-SESS-008). Dalam tahap ini Literatur [2] dan Literatur [7] dinyatakan Tidak Lolos sedangkan Literatur [6] tidak melakukan pengujian di tahap ini.

TABEL IV
TOOLS PENGUJIAN OWASP VERSI 4 (AUTHENTICATION TESTING)

Literatur	Tools OTG-AUTHN-001	Tools OTG-AUTHN-002	Tools OTG-AUTHN-003	Tools OTG-AUTHN-004	Tools OTG-AUTHN-005	Tools OTG-AUTHN-006	Tools OTG-AUTHN-007	Tools OTG-AUTHN-008
[2]	Webscarab	Brutus	Browser Mozilla Firefox	Webscarab	Webscarab	Browser Mozilla Firefox	Brutus	-
[6]	Browser Mozilla Firefox	Netsparker	OWASP ZAP Attack Proxy dan Browser Mozilla Firefox	Browser Mozilla Firefox dan Netsparker	Mozilla Firefox dan OWASP ZAP Attack Proxy	Mozilla Firefox dan OWASP ZAP Attack Proxy	Mozilla Firefox dan Netsparker	-
[7]	Webscarab	Brutus	Browser Mozilla Firefox	Webscarab	Webscarab	Browser Mozilla Firefox	Brutus	-

Berdasarkan Tabel IV, Dalam tahap OTG-AUTHN-001 Literatur [2] dan Literatur [7] menggunakan Tools WebScarab sedangkan Literatur [6] menggunakan Tools Browser Mozilla Firefox.

Berikutnya dalam tahap OTG-AUTHN-002 Literatur [2] dan Literatur [7] menggunakan Tools Brutus sedangkan Literatur [6] menggunakan Tools Netsparker.

Berikutnya dalam tahap OTG-AUTHN-003 Literatur [2] dan Literatur [7] menggunakan Tools Browser Mozilla Firefox, sedangkan Literatur [6] menggunakan Tools OWASP ZAP Attack Proxy dan Browser Mozilla Firefox.

Berikutnya dalam tahap OTG-AUTHN-004 Literatur [2] dan Literatur [7] menggunakan Tools WebScarab sedangkan Literatur [6] menggunakan Tools Browser Mozilla Firefox dan Netsparker.

Berikutnya dalam tahap OTG-AUTHN-005 Literatur [2] dan Literatur [7] menggunakan Tools WebScarab sedangkan Literatur [6] menggunakan Tools Browser Mozilla Firefox dan OWASP ZAP Attack Proxy.

Berikutnya dalam tahap OTG-AUTHN-006 Literatur [2] dan Literatur [7] menggunakan Tools Browser Mozilla Firefox sedangkan Literatur [6] menggunakan Tools Mozilla Firefox dan OWASP ZAP Attack Proxy.

Berikutnya dalam tahap OTG-AUTHN-007 Literatur [2] dan Literatur [7] menggunakan Tools Brutus sedangkan Literatur [6] menggunakan Tools Mozilla Firefox dan Netsparker.

Berikutnya dalam tahap OTG-AUTHN-008 Literatur [2] dan Literatur [7] tidak menggunakan Tools dalam tahap ini, sedangkan Literatur [6] tidak melakukan pengujian di tahap ini.

TABEL V
TOOLS PENGUJIAN OWASP VERSI 4 (AUTHENTICATION TESTING, AUTHORIZATION TESTING DAN SESSIONTESTING)

Literatur	Tools OTG-AUTHN-009	Tools OTG-AUTHN-010	Tools OTG-AUTHZ-001	Tools OTG-AUTHZ-002	Tools OTG-AUTHZ-003	Tools OTG-AUTHZ-004	Tools OTG-SESS-001	Tools OTG-SESS-002
[2]	-	-	WFuzz	Dirb	WebScarab	Browser Mozilla Firefox	Dirb	Zed Attack Proxy
[6]	-	-	OWASP Zap Attack Proxy dan Netsparker	Netsparker dan Mozilla Firefox	OWASP Zap Attack Proxy, Netsparker dan Mozilla Firefox	-	OWASP Zap Attack Proxy dan Google Chrome (Plugin)	OWASP Zap Attack Proxy dan Google Chrome (Plugin)
[7]	-	-	WFuzz	Dirb	WebScarab	Browser Mozilla Firefox	Dirb	Zed Attack Proxy

Berdasarkan Tabel V dalam tahap OTG-AUTHN-009 Literatur [2] dan Literatur [7] tidak menggunakan Tools dalam tahap ini, sedangkan Literatur [6] tidak melakukan pengujian di tahap ini.

Berikutnya dalam tahap OTG-AUTHN-010 Literatur [2] dan Literatur [7] tidak menggunakan Tools dalam tahap ini, sedangkan Literatur [6] tidak melakukan pengujian di tahap ini.

Berikutnya dalam tahap OTG-AUTHZ-001 Literatur [2] dan Literatur [7] menggunakan Tools WFuzz sedangkan literatur [6] menggunakan Tools OWASP Zap Attack Proxy dan Netsparker.

Berikutnya dalam tahap OTG-AUTHZ-002 Literatur [2] dan Literatur [7] menggunakan Tools Dirb sedangkan Literatur [6] menggunakan Tools Netsparker dan Browser Mozilla Firefox.

Berikutnya dalam tahap OTG-AUTHZ-003 Literatur [2] dan Literatur [7] menggunakan Tools WebScarab sedangkan Literatur [6] menggunakan Tools OWASP ZAP Attack Proxy, Netsparker dan Browser Mozilla Firefox.

Berikutnya dalam tahap OTG-AUTHZ-004 Literatur [2] dan Literatur [7] menggunakan Tools Browser Mozilla Firefox sedangkan Literatur [6] tidak melakukan pengujian di tahap ini.

Berikutnya dalam tahap OTG-SESS-001 Literatur [2] dan Literatur [7] menggunakan Tools Dirb sedangkan Literatur [6] menggunakan Tools OWASP ZAP Attack dan Google Chrome (Plugin).

Berikutnya dalam tahap OTG-SESS-002 Literatur [2] dan Literatur [7] menggunakan Tools Zed Attack Proxy sedangkan Literatur [6] menggunakan Tools OWASP ZAP Attack Proxy dan Google Chrome (Plugin).

TABEL VI
TOOLS PENGUJIAN OWASP VERSI 4 (SESSION TESTING)

Literatur	Tools OTG-SESS-003	Tools OTG-SESS-004	Tools OTG-SESS-005	Tools OTG-SESS-006	Tools OTG-SESS-007	Tools OTG-SESS-008
[2]	Zed Attack Proxy	Zed Attack Proxy	OWASP CSRF Tester	Browser Mozilla Firefox	Browser Mozilla Firefox	Zed Attack Proxy
[6]	OWASP Zap Attack Proxy dan Google Chrome (Plugin)	OWASP Zap Attack Proxy dan Google Chrome (Plugin)	Netsparker dan Mozilla Firefox	Browser Mozilla Firefox	Browser Mozilla Firefox	-
[7]	Zed Attack Proxy	Zed Attack Proxy	OWASP CSRF Tester	Browser Mozilla Firefox	Browser Mozilla Firefox	Zed Attack Proxy

Berdasarkan Tabel VI dalam tahap OTG-SESS-003 Literatur [2] dan Literatur [7] menggunakan Tools Zed Attack Proxy sedangkan Literatur [6] menggunakan Tools OWASP ZAP Attack Proxy dan Google Chrome (Plugin).

Berikutnya dalam tahap OTG-SESS-004 Literatur [2] dan Literatur [7] menggunakan Tools Zed Attack Proxy sedangkan Literatur [6] menggunakan Tools OWASP ZAP Attack Proxy dan Google Chrome (Plugin).

Berikutnya dalam tahap OTG-SESS-005 Literatur [2] dan Literatur [7] menggunakan Tools OWASP CSRF Tester sedangkan Literatur [6] menggunakan Tools Netsparker dan Mozilla Firefox.

Berikutnya dalam tahap OTG-SESS-006 Literatur [2], Literatur [6] dan Literatur [7] menggunakan Tools Browser Mozilla Firefox.

Berikutnya dalam tahap OTG-SESS-007 Literatur [2], Literatur [6] dan Literatur [7] menggunakan Tools Browser Mozilla Firefox. Berikutnya dalam tahap OTG-SESS-008 Literatur [2] dan Literatur [7] menggunakan Tools Zed Attack Proxy sedangkan Literatur [6] tidak melakukan pengujian di tahap ini.

IV. KESIMPULAN

Pada Literatur [2] yang menguji sebuah Aplikasi Ujian Online Berdasarkan Hasil Pengujian OWASP versi 4 dari tabel I sampai tabel III terlihat bahwa pada proses otentifikasi terdapat kerentanan yaitu pada pengujian OTG-AUTHN-001, OTG-AUTHN-003, OTG-AUTHN-004, OTG-AUTHN-005, OTG-AUTHN-006 sehingga proses ini perlu mendapat perbaikan. Pada proses pengujian otorisasi terdapat kerentanan pada OTG-AUTHZ-002, OTG-AUTHZ-004, namun setelah dilakukan pengecekan diatas hasilnya adalah false alarm sehingga proses otorisasi sudah berjalan dengan baik, sedangkan pada manajemen sesi terdapat kerentanan pada OTG-SESS-001, OTG-SESS-005, OTG-SESS-007, OTG-SESS-008.

Pada Literatur [6] yang menguji sebuah Website www.xyz.com Berdasarkan Hasil Pengujian OWASP versi 4 dari tabel I sampai tabel III terlihat pada proses otentifikasi terdapat kerentanan yaitu OTG-AUTHN-006 sehingga proses ini perlu mendapat perbaikan dan seharusnya dalam proses otentifikasi harus menjalani keseluruhan tahapan. Tahapan- tahapan yang dilewati di proses otentifikasi yaitu : OTG-AUTHN-008, OTG-AUTHN-009, OTG-AUTHN-010. walaupun secara keseluruhan pada proses otentifikasi sudah lolos semua kecuali OTG-AUTHN-006 dan melewati beberapa tahapan. Pada proses pengujian otorisasi tidak terdapat kerentanan artinya sistem sudah dikatakan aman dalam hal otorisasi walaupun ada tahapan yang dilewati yaitu OTG-AUTHZ-004. Dalam proses pengujian manajemen sesi tidak terdapat kerentanan artinya sistem yang diuji sudah aman walaupun ada tahapan yang dilewati yaitu : OTG-SESS-008.

Pada Literatur [7] yang menguji sebuah WebServer Berdasarkan hasil pengujian menggunakan OWASP versi 4 pada tabel I sampai tabel III terlihat pada proses otentifikasi terdapat kerentanan yaitu terdapat kerentanan yaitu OTG-AUTHN-001, OTG-AUTHN-003, OTG-AUTHN-004, OTG-AUTHN-005, OTG-AUTHN-006, OTG-AUTHN-008 sehingga proses ini perlu mendapat perbaikan. Pada proses pengujian otorisasi terdapat kerentanan pada OTG-AUTHZ-002, OTG-AUTHZ-004, namun setelah dilakukan pengecekan diatas hasilnya adalah false alarm sehingga proses otorisasi sudah berjalan dengan baik, sedangkan pada manajemen sesi terdapat kerentanan pada OTG-SESS-001, OTG-SESS-005, OTG-SESS-008.

Dari penjabaran diatas, dapat disimpulkan bahwa Sistem Informasi berbasis website atau Webserver yang ter-aman dari ketiga literatur tersebut adalah Literatur [6] yang menguji sebuah website www.xyz.com dikarenakan website tersebut hampir keseluruhan tahap dalam pengujian OWASP versi 4 dinyatakan Lolos walaupun ada tahapan dalam pengujian OWASP yang dilewati.

REFERENSI

[1] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and P. Grp, "*Preferred Reporting Items for Systematic Reviews and Meta-Analyses: 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_Top-10_2013AppSec_EU_2013_-_Dave_Wichers.pdf

[6] Moh Yunus, "*Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan*

Framework Owasp Versi 4", Jurnal Ilmiah Informatika Komputer Volume 24 No. 1,pp. 38-50, April 2019

[7] Dr. Raden Teduh Dirgahayu, S.T., M.Sc., Yudi Prayudi, S.Si., M.Kom., Adi Fajaryanto, "*Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server*", Jurnal Ilmiah NERO Vol. 1 No. 3, pp. 190-197, 2015