Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server

Dr. Raden Teduh Dirgahayu, S.T., M.Sc.[1)], Yudi Prayudi, S.Si., M.Kom.[2)], Adi Fajaryanto[3)]
[1), 2),3)]Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Jl. Kaliurang Km. 14,5 Yogyakarta
Email : teduh.dirgahayu@fti.uii.ac.id[1)], yusufyudi@gmail.com[2)], adifajaryanto@gmail.com[3)]

Abstrak

Untuk mengamankan web server dariserangan hacker maka sebaiknya para pemilik web server melakukan self test terhadap server mereka sendiri. Melalui self test ini, para pemilik web server akan mengetahui letak kerentanan dari sistem yang ada. Salah satu metode self test ini adalah penetration test. Metode ini sama dengan aktivitas hacking namun dilakukan secara legal. Penelitian ini, metode implementasi penetration test yang akan digunakan adalah ISSAF (Information Systems Security Assessment Framework) dan OWASP versi 4. IKIP PGRI Madiun sebagai salah satu instansi pendidikan sudah mempunyai web server sendiri sejak tahun 2010. Berdasarkan wawancara dengan pengelola web server IKIP PGRI Madiun, sejak pertama kali web server online sampai saa tini web server berhasil dibobol oleh hacker beberapa kali dalam setahun dan belum pernah dilakukan penetration test pada web servernya. Hasil pengujian dan analisa dengan metode ISSAF menunjukkan bahwa sistem web server IKIP PGRI Madiun masih dapat ditembus dan mengambil alih hak akses administrator, sedangkan dengan metode OWASP versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik.

Kata kunci: *webserver, pentest, owasp, issaf, framework.*

Abstract

To secure web server from hacker attacks then it should be the owner of the web server performs a self test on their own servers. Through self this Test, the owner of the web server will know where the vulnerabilities of the existing system. One method is the self test penetration test. This method is the same as hacking activity yet done legally. In this reaserch, implementation penetration test method to be used is ISSAF (Information Systems Security Assessment Framework) and OWASP PGRI Madiun version 4. Teachers 'Training College as one of the educational institutions already have their own web server since 2010. Based on interviews with managers of the web server PGRI Madison Teachers' Training College, since the first online web server to a web server tini SAA successfully compromised by hackers several times a year and have never performed penetration test on a web server. Results of the testing and analysis method showed that the system ISSAF web server PGRI Madison Teachers' Training College can still penetrate and take over the administrator permissions, while the method of OWASP version 4 shows that the management of authentication, authorization and session management has not been implemented properly.

Keyword : *webserver, pentest, owasp, issaf, framework.*

1. Pendahuluan

Pertumbuhan teknologi yang semakin pesat memberikan dampak positif pada berbagai bidang, termasuk internet. Website menjadi alternatif bagi korporasi sebagai media promosi maupun media interaksi dengan pelanggan, Website dapat dengan mudah diakses oleh orang banyak dari manapun dan kapanpun. Pada tahun 2015, Indonesia diperkirakan akan ada lonjakan penggunaan internet sebesar 22 juta pengguna. Tren meningkatnya pengguna internet sudah terlihat sejak tahun 2009 dan diperkirakan akan terus meningkat [1].

Kemudahan akses ini membuat banyak orang maupun instansi membangun sistem webserver tanpa memperhatikan apakah webserver yang dibangun sudah aman atau belum terhadap gangguan. Gangguan tersebut diantaranya berupa serangan MaliciousCode atau Malware. MaliciousCode atau

Malware merupakan jenis serangan yang paling banyak menyerang Website. Webserver yang paling rentan adalah Website milik perusahaan di bidang perbankan yaitu sebesar 81%. Kerentanan tersebut hanya 50% yang berhasil diperbaiki dengan rata-rata waktu memperbaiki selama 107 hari (Gambar 1).

Gambar 1 *White Hat Security Website Security Statistic Report*

Isu kerentanan ini didukung oleh laporan yang dirilis oleh Akamai sebagai pengawas lalu lintas internet pada tahun 2013 menyebutkan bahwa .com menjadi domain yang paling banyak diserang oleh hacker [2]. Untuk mengamankan webserver dari serangan *hacker* maka sebaiknya para pemilik webserver melakukan *selftest* terhadap server mereka sendiri. Melalui selftest ini, para pemilik webserver akan mengetahui letak kerentanan dari sistem yang ada. Salah satu metode *selftest* ini adalah penetrationtest. Metode ini sama dengan aktivitas hacking namun dilakukan secara legal. *Penetrationtest (pentest*) merupakan metode yang efektif untuk menguji kerentanan sistem. Dengan demikian penetrationtest adalah proses mencoba untuk mendapatkan akses ke dalam sebuah sistem tanpa ada pengetahuan tentang username, password dan akses lainnya. Jika fokusnya adalah pada sumber daya komputer, maka contoh dari penetrasi yang sukses akan mendapatkan atau menghancurkan dokumen-dokumen rahasia, basis data dan informasi lain yang dilindungi. Pengujian terhadap aplikasi web dengan metode *penetration testing* merupakan metode yang komprehensif mengidentifikasi kerentanan sistem [3]. Dalam pengujian penetrasi ada beberapa metode yang sering dipakai seperti Information Systems *Security Assessment Framework* (ISSAF), OWASP versi 4 dan OSSTMM. Penelitian ini, metode implementasi *penetration test* yang akan digunakan adalah ISSAF (*Information Systems Security Assessment Framework*) dan OWASP versi 4. Keduanya dipilih karena bersifat *opensource*, bebas digunakan oleh siapa saja. ISSAF yang dikeluarkan oleh OSSIG (*Open System SecurityInformation Group*) merupakan kerangka terstruktur yang mengkategorikan penilaian keamanan sistem informasi dalam berbagai domain dan rincian kriteria evaluasi atau pengujian khusus untuk masing-masing domain.

Sedangkan OWASP singkatan dari *Open Web Application Security Project* yang dikeluarkan oleh OWASP *Foundation* sebagai organisasi non-profit amal di Amerika Serikat berdiri pada tahun 2004. OWASP adalah organisasi internasional dan OWASP Foundation mendukung upaya OWASP di seluruh dunia. IKIP PGRI Madiun sebagai salah satu instansi pendidikan sudah mempunyai webserver sendiri sejak tahun 2010. Webserver IKIP PGRI Madiun terdiri dari dua domain yaitu ikippgrimadiun.ac.id dan ejournal.ikippgrimadiun.ac.id. Berdasarkan wawancara dengan pengelola webserver IKIP PGRI Madiun, sejak pertama webserver online sampai saat ini webserver berhasil dibobol oleh *hacker* beberapa kali dalam setahun dan belum pernah dilakukan *penetrationtest* pada webservernya. Mengingat isu tentang keamanan webserver cukup penting serta kondisi webserver pada IKIP PGRI Madiun yang mengalami serangan beberapa kali dalam setahun oleh hacker maka dalam penelitian ini dilakukan pengujian terhadap webserver IKIP PGRI menggunakan *penetration testing*, agar dapat direkomendasikan upaya untuk meminimalisir tingkat kerentanan sistem yang ada.

1.1. Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah pada penelitian ini adalah:

1. Bagaimana mengidentifikasi kerentanan sistem?
2. Bagaimana hasil pengujian dan analisis kerentanan webserver menggunakan metode ISSAF dan OWASP versi 4?.

1.2. Batasan Masalah

Batasan masalah dalam objek penelitian ini adalah:

1. Studi yang dilakukan terbatas pada pengujian keamanan webserver dengan domain ikippgrimadiun.ac.id menggunakan framework ISSAF dan domain ejournal.ikippgrimadiun.ac.id menggunakan *framework* OWASP versi 4 fokus pada *Authentication Testing, Authorization Testing, Session Management Testing*.
2. Metode *penetration tes*t diterapkan pada pemodelan webserver situs resmi IKIP PGRI Madiun.
3. Identifikasi kerentanan sistem webserver menggunakan aplikasi *Acunetix*.

1.3. Tujuan dan Manfaat Penelitian

1. Mengidentifikasi kerentanan sistem pada webserver IKIP PGRI Madiun.
2. Mengetahui hasil pengujian dan analisis pengujian keamanan webserver menggunakan ISSAF dan OWASP versi 4
3. Penelitian ini diharapkan dapat menjadi bahan masukan bagi pihak stakeholder pada IKIP PGRI Madiun untuk mengetahui tingkat kerentanan dari webserver yang ada.

1.4. Penelitian Terkait

Pada penelitian [4] menyoroti bagaimana seorang konsultan keamanan yang berpengalaman diperlukan untuk melakukan penetrasi yang baik dan perannya untuk memberikan keamanan sistem dengan mengharapkan serangan keamanan. Lembaga-lembaga kantor perusahaan di mana terpasang sistem jaringan perlu menyebarkan petugas keamanan yang mengetahui serangan keamanan yang modern dan mencoba untuk mengembangkan mekanisme untuk mengatasi serangan keamanan. Sebagai alat pengukuran, penetration testing merupakan paling kuat ketika diintegrasi ke dalam proses pengembangan sehingga temuan dapat membantu memperbaiki desain, dan implementasi.

Pada penelitian [5] yang melakukan serangkaian penetrationtest pada *Open Stack Essex Cloud Management Software*. Beberapa jenis *penetrationtest* dilakukan seperti *network protocol and command line fuzzing, session hijacking and credentialtheft*. Dengan menggunakan teknik ini, kerentanan pada sistem dieksploitasi dan ditemukan oleh penyerang dan dimungkinkan untuk mendapatkan akses ke informasi rahasia yang terdapat pada server *Open Stack*, atau untuk mendapatkan hak administratif penuh pada server. Untuk mengatasi kerentanan ini, direkomendasikan penggunaan protokol yang aman, seperti HTTPS (*Hypertext Transfer ProtocolSecure*), untuk komunikasi antara pengguna *cloud dan Open Stack Horizon Dashboard*, untuk mengenkripsi semua file yang disimpan pengguna atau informasi login pengguna.

Issac (2012) dari SANS Institute menerangkan bahwa untuk penetrasi tester yang profesional, pengujian teknologi web menjadi salah satu keterampilan dasar yang harus dimiliki. Metode pengujian HTTP untuk aplikasi web atau server hanya satu bagian dari pengujian tersebut, hasilnya dapat dianggap minor selama tes, namun teknik sederhana ini dapat membuka pintu ke tingkat berikutnya. Meskipun tampak sangat sederhana, hal itu tidak mudah untuk menerapkan teknik ini, sehingga adalah penguji penetrasi perlu untuk berlatih agar menjadi lebih mahir dalam penggunaannya.

2. Dasar teori

ISSAF *(Information System SecurityAssessmentFramework*) dirancang untuk mengevaluasi sistem. Framework ini terdiri tiga fase pendekatan dan sembilan langkah penilaian. Pendekatan ini meliputi tiga tahap berikut:

- Fase I: *Planning and Preparation.* Fase ini berisi langkah-langkah untuk bertukar informasi, merencanakan dan mempersiapkan tes. Sebelum melakukan pengujian Perjanjian Assessment

resmi akan ditandatangani dari kedua pihak. Ini akan memberikan perlindungan hukum pada kedua belah pihak. Perjanjian ini akan juga menentukan tim yang terlibat, tanggal, waktu dan ketentuan lainnya.

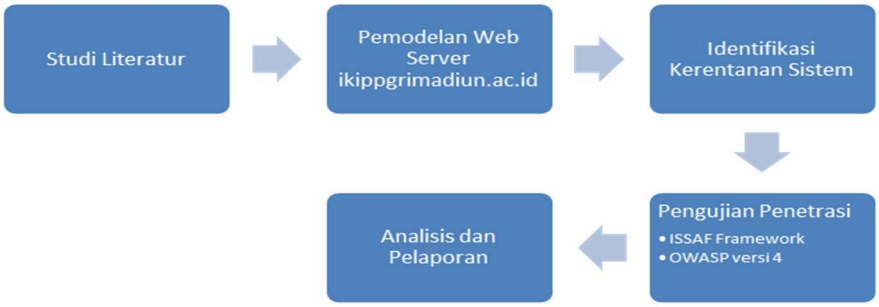
- Fase II: *Assessment.* Fase ini merupakan fase pelaksanaan uji penetrasi. Pada fase assessment dilakukan pendekatan bertingkat, seperti yang ditunjukkan pada Gambar 2. Setiap tingkatan akan memberikan akses lebih luas ke aset informasi yang diinginkan.
- *Clean-upandDestroyArtefacts.* Semua informasi yang dibuat atau disimpan pada sistem yang diuji harus dihapus. Jika tidak mungkin menghapus dari remotesystem, semua file ini (dengan lokasi mereka) harus disebutkan dalam laporan teknis sehingga staf teknis klien dapat menghapus setelah laporan diterima.

OWAPS 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.

Framework yang digunakan pada OWASP versi 4 adalah sebagai berikut :

- *Authentication Testing*. Otentikasi merupakan tindakan membangun dan mengkonfirmasi sesuatu bahwa klaim yang dibuat adalah benar. Otentikasi sebuah objek dapat berarti mengkonfirmasikan sumbernya, sedangkan otentikasi seseorang sering terdiri dari verifikasi identitasnya. Otentikasi tergantung pada satu atau lebih faktor otentikasi.Dalam keamanan komputer, otentikasi adalah proses mencoba untuk memverifikasi identitas digital pengirim komunikasi. Sebuah contoh umum dari proses tersebut adalah log proses. Pengujian skema otentikasi berarti memahami bagaimana proses otentikasi bekerja dan menggunakan informasi tersebut untuk menghindari mekanisme otentikasi.
- *Authorization Testing*. Otorisasi merupakan konsep yang memungkinkan akses ke sumber daya bagi mereka yang diizinkan untuk menggunakannya. Pengujian untuk otorisasi berarti memahami bagaimana proses otorisasi bekerja, dan menggunakan informasi tersebut untuk menghindari mekanisme otorisasi.Otorisasi adalah proses yang datang setelah otentikasi berhasil, sehingga tester akan memverifikasi titik ini setelah ia memegang identitas yang sah. Selama ini jenis penilaian, harus diverifikasi apakah mungkin untuk memotong skema otorisasi, menemukan kerentanan jalur traversal, atau menemukan cara meningkatkan hak-hak istimewa yang ditugaskan untuk tester.
- *Session Management Testing* didefinisikan sebagai himpunan semua kontrol yang mengatur interaksi fullstate antara pengguna dan aplikasi berbasis web [6]. Hal ini secara luas mencakup apa pun dari bagaimana otentikasi pengguna dilakukan, bagaimana mereka logout. Lingkungan aplikasi web yang populer, seperti ASP dan PHP, memberikan pengembang dengan *built-in* rutinitas penanganan sesi. Beberapa jenis identifikasi token biasanya dikeluarkan, yang disebut sebagai "ID Sesi" atau Cookie.

4. Metodologi Penelitian



Gambar 2. *Tahapan Penelitian*

a. Studi Literatur

Pada tahap awal dilakukan studi literatur yang bertujuan untuk menjelaskan kajian pustaka dari teori-teori penunjang yang mendukung konstruksi penelitian. Kegiatan ini dilakukan dengan membaca buku, jurnal, artikel laporan penelitian, dan situs-situs di internet. Keluaran dari studi literatur ini adalah terkoleksinya referensi yang relevan dengan rumusan masalah. Tujuannya adalah untuk memperkuat permasalahan serta sebagai dasar teori dalam melakukan studi dan juga menjadi dasar untuk melakukan penelitian.

b. Pemodelan webserver

Pemodelan webserver ini menggunakan aplikasi virtual machineVirtualBox dengan spesifikasi webserver antara lain menggunakan Single prosesor, Monitor VGA dengan resolusi min. 800 x 600, Memory 512 MB RAM, Harddisk kapasitas 40 Gigabyte atau lebih, CD-ROMdrive, Mouse, Keyboard, Sistem Operasi Linux CentOS, Webserver Apache2, DatabaseMySQL 5.4, Telnet, IP 192.168.100.10/24.

Kemudian spesifikasi virtual machine yang digunakan untuk menguji adalah Single prosesor, Monitor VGA dengan resolusi min. 800 x 600, Memory 512 MB RAM, Harddisk kapasitas 40 Gigabyte atau lebih, CD-ROMdrive, Mouse, Keyboard.

c. Identifikasi kerentanan Sistem

Identifikasi kerentanan pada model webserver IKIP PGRI Madiun menggunakan aplikasi Acunetix. Implementasi *Penetration Test.* Metode pengujian menggunakan 2 metode yaitu ISSAF dan OWASP versi 4 serta memakai konsep black-boxtest.

d. Analisis dan Pelaporan

Tahap ini akan dilakukan aktifitas pembuatan laporan hasil implementasi Penetration Test dengan menggunakan ISSAF dan OWASP versi 4.

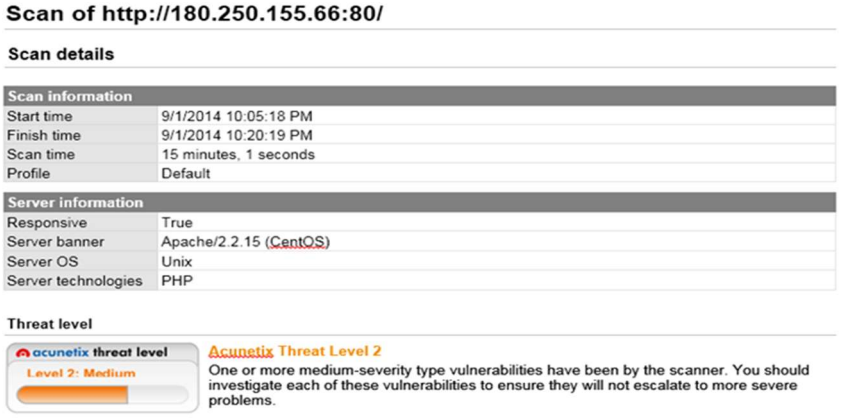
5. Pengujian dan Pembahasan

a. Studi Literatur

Pada tahap ini dilakukan pengumpulan bahan literature yang sesuai dengan masalah yang dihadapi. Literatur sebagian besar didapat bersumber dari Internet dan ada beberapa berasal dari buku.

b. Pemodelan Web Server IKIP PGRI MADIUN

Pengujian penetrasi dilakukan tidak secara real time pada saat server sedang berjalan, namun webserver yang ada di IKIP PGRI Madiun dibuat tiruannya melalui mesin virtual yaitu Virtual Box versi 4.3.10. Identifikasi kerentanan sistem dilakukan dengan bantuan tool Acunetix. Berdasarkan hasil scan, menghasilkan kerentanan level medium seperti pada gambar 3.



Scan of http://180.250.155.66:80/

Scan details

Scan information	
Start time	9/1/2014 10:05:18 PM
Finish time	9/1/2014 10:20:19 PM
Scan time	15 minutes, 1 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.2.15 (CentOS)
Server OS	Unix
Server technologies	PHP

Threat level

acunetix threat level
Level 2: Medium

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Gambar 3 *Hasil scan Acunetix*

c. Pengujian menggunakan ISSAF

Berikut ini hasil pengujian menggunakan framework ISSAF seperti terlihat pada tabel 4.4 dengan dua kegiatan uji mengalami gagal.

Tabel 1 *Ringkasan Hasil Uji ISSAF*

Tahapan	*Source*	*Tools*	Status
Information Gathering	Domain Info	Whois, SSL Scan	OK
	SSL (secure Socket Layer)	SSL Scan	X
Network Mapping	Network Info	Zen Map	OK
Vulnerability Identification	Web Scanner Vulnerability	Acunetix	OK
Penetration	DoS Attack	Low Orbit Ion Canon	OK
	SQL Injection	Havij	X
	Metasploits	Armitage	OK
Gaining Access & Privilege Escalation	Backdoor	Php Rootkits	OK
Enumerating Further	Backdoor	Php Rootkits	OK
Compromise Remote User/Site	Backdoor	Php Rootkits	OK
Maintaining Access	Backdoor	Php Rootkits	OK
Covering Tracks	Backdoor	Php Rootkits	OK

d. Hasil Analisa ISSAF Framework

Pada fase *Information Gathering*, hasil dari *who is* terlihat bahwa ada informasi nama. Nama yang tercantum digunakan untuk mencari informasi melalui *social engineering* dan nomor telp dapat digunakan oleh orang-orang yang tidak bertanggung jawab. Seorang penyerang dengan melihat nama yang tercantum dalam *who is* diasumsikan bahwa dia memiliki kekuasaan yang lebih dan menjadi target yang menarik. Solusi untuk hal ini adalah mencantumkan posisi jabatan pada informasi *who is* bukan nama asli. Ini juga memudahkan pihak managemen apabila ada perpindahan jabatan.

Selain informasi pada *who is*, pada fase *Information Gathering* diketahui bahwa ikippgrimadiun.ac.id dan ejournal.ikippgrimadiun.ac.id tidak memiliki SSL (*Secure Socket Layer*) sehingga pada saat pengiriman data oleh *client* kepada server tidak melalui enkripsi. Tanpa adanya enkripsi maka data yang dikirim akan mudah dibaca (diendus) oleh pihak yang tidak bertanggung jawab. Solusi untuk celah kerentanan ini adalah dengan menggunakan SSL untuk proses pengiriman data.

Selama proses pengujian, target mememiliki celah pada alamat 180.250.155.66/images dan 180.250.155.66/images/ukm yang diunduh secara langsung tanpa memerlukan otentifikasi. Hal ini memerlukan perhatian khusus agar pihak admin segera melakukan pembatasan pada *htaccess* agar information *disclosure* tidak terulang. Pada fase *Gaining Access and Privilege*, penguji berhasil mendapatkan *password* administrator dengan mudah, karena password yang terdeteksi berupa karakter sehingga potensi untuk ditebak cukup besar. Setelah fase ini berhasil masuk maka proses mendapatkan *user root* menggunakan aplikasi netcat dan *back door root* kits menjadi dapat berlangsung dengan lancar.

e. Hasil Pengujian OWASP versi 4

Tabel 2 *Hasil Pengujian OWASP versi 4*

Tahapan	Tool	Keterangan
Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)	WebScarab	Tidak lolos
Testing for default credentials (OTG-AUTHN-002)	Brutus	Lolos
Testing for Weak lock out mechanism (OTG-AUTHN-003)	Browser Mozilla Firefox	Tidak lolos
Testing for bypassing authentication schema (OTG-AUTHN-004)	WebScarab	Tidak lolos
Test remember password functionality (OTG-AUTHN-005)	WebScarab	Tidak lolos
Testing for Browser cache weakness (OTG-AUTHN-006)	Browser Mozilla Firefox	Tidak lolos
Testing for Weak password policy (OTG-AUTHN-007)	Brutus	Lolos
Testing for Weak security question/answer (OTG-AUTHN-008)	-	Tidak lolos
Testing for weak password change or reset functionalities (OTG-AUTHN-009)	-	Lolos
Testing for Weaker authentication in alternative channel (OTG-AUTHN-010)	-	Lolos
Testing Directory traversal/file include (OTG-AUTHZ-001)	WFuzz	Lolos
Testing for bypassing authorization schema (OTG-AUTHZ-002)	Dirb	Tidak lolos
Testing for Privilege Escalation (OTG-AUTHZ-003)	WebScarab	Lolos
Testing for Insecure Direct Object References (OTG-AUTHZ-004)	Browser Mozilla Firefox	Tidak lolos
Testing for Bypassing Session Management Schema (OTG-SESS-001)	Dirb	Tidak lolos
Testing for Cookies attributes (OTG-SESS-002)	Zed Attack Proxy	Lolos
Testing for Session Fixation (OTG-SESS-003)	Zed Attack Proxy	Lolos
Testing for Exposed Session Variables (OTG-SESS-004)	Zed Attack Proxy	Lolos
Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)	OWASP CSRF Tester	Tidak lolos
Testing for logout functionality (OTG-SESS-006)	Browser Mozilla Firefox	Lolos
Test Session Timeout (OTG-SESS-007)	Browser Mozilla Firefox	Tidak lolos
Testing for Session puzzling (OTG-SESS-008)	Zed Attack Proxy	Tidak lolos

f. Hasil Analisa Framework OWASP versi 4

Berdasarkan hasil pengujian menggunakan OWASP versi 4 pada tabel 4.4 terlihat bahwa pada tahapan OTG-AUTHN-001, OTG-AUTHN-004, OTG-AUTHN-005, OTG-AUTHN-006, dan OTG-AUTHN-008 aplikasi tidak lolos pengujian, sehingga proses otentifikasi pemakai berpotensi untuk diendus oleh pihak yang tidak bertanggung jawab dalam proses pengiriman data penting. Pada pengujian otorisasi, tahapan OTG-AUTHZ-002 dan OTG-AUTHZ-004 tidak lulus pengujian dan ini merupakan false alarm sehingga untuk pengujian otorisasi aplikasi ini lolos uji.

Tahapan OTG-SESS-007 dan OTG-SESS-008 dilakukan pengujian mengenai session yang ada. Pada OTG-SESS-007 session timeout tidak ada sehingga memungkinkan apabila pemakai

meninggalkan komputer maka ada kemungkinan session yang ditinggalkan dimanfaatkan oleh pemakai lain yang tidak berhak. Pada OTG-SESS-008, aplikasi ini menggunakan variabel session yang sama selama lebih dari satu tujuan sehingga penyerang dapat mengakses halaman secara acak.

Rekomendasi Framework ISSAF dan OWASP versi 4

Dari penelitian yang telah dilakukan, maka rekomendasi untuk stake holder IKIP PGRI Madiun adalah sebagai berikut :

a. Pemasangan SSL (*Secure Socket Layer*) pada proses pengiriman data oleh client ini terkait hasil pengujian pada tabel 1, sehingga data yang dikirim terenkripsi.
b. Dilakukan pembatasan pada link 180.250.155.66/images/ukm dan 180.250.155.66/images dengan melakukan perubahan pada file .htaccess yang terletak pada direktori /www atau pada sub direktori, agar tidak dapat dibuka secara langsung.
c. Penerapan IDS (*Intrusion Detection System*) agar serangan dari pihak yang tidak bertanggung jawab dapat dideteksi, dan IPS (*Intrusion Prevention System*) berfungsi untuk mendeteksi serangan kemudian membelokkan serangan.
d. Menerapkan Rekomendasi OWASP Top 10 untuk mencegah penanaman *back door root kits* pada web server.[7]
e. Mengimplementasi session timeout.untuk menghindari pembajakan akun oleh penyerang (solusi hasil penetrasi OWASP Tahapan *Test Session Timeout* (OTG-SESS-007)).

5. Kesimpulan

Hasil pengujian dan analisa dengan metode ISSAF menunjukkan bahwa sistem web server IKIP PGRI Madiun masih dapat ditembus dan mengambil alih hak akses administrator, sedangkan dengan metode OWASP versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik.

6. DaftarPustaka

[1] Assosiasi Penyelenggara Jasa Internet Indoneisa. (2012). Retrieved May 17, 2014, from http://www.apjii.or.id/v2/read/page/halaman-data/9/statistik.html

[2]J Thomson, F. (2013, Desember). Akamai. Retrieved Mei 19, 2014, from http://www.akamai.com/dl/akamai/akamai-soti-q413.pdf?WT.mc_id=soti_Q413

[3] Bacudio, A. G. (2011). AnOverview of Penetration Testing. Journal of Network Security & Its Applications.

[4] Naik, N. (2009). Penetration Testing A RoadmaptoNetwork.

[5] Ralph La Barge, T. M. (2012). CloudPenetration Testing.

[6] MatteoMeucciandFriends. (2014). OWASP Testing Guide 4.0. The OWASP Foundation.

[7] Dave Wichers. (2013, Juni 12). OWAPS Top Ten. RetrievedDecember 1, 2014, from OWAPS Documentation Project: https://www.owasp.org/images/1/17/OWASP_Top-10_2013--AppSec_EU_2013_-_Dave_Wichers.pdf