Jurnal Indonesia Sosial Teknologi: p–ISSN: 2723 - 6609
e-ISSN : 2745-5254
Vol. 2, No. 4 April 2021

ANALISIS KEAMANAN WEBSITE DENGAN *INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF)* DAN *OPEN WEB APPLICATION SECURITY PROJECT (OWASP)* DI RUMAH SAKIT XYZ

Agus Rochman, Rizal Rohian Salam, dan Sandi Agus Maulana
Sekolah Tinggi Manajemen Ilmu Komputer, STMIK LIKMI
Email: agus.rochman@gmail.com, rizalroihan@gmail.com,
sandimaulana2@yahoo.com

Abstract

Computer security systems are increasingly needed along with the increasing number of users connected to the internet network, this can lead tocrime cyber by irresponsible people. This research was conducted at a Hospital Information System. One of them is a web server for HRD information. This system contains employee data and employee attendance data. Webserver security is usually an issue for administrators. Often these problems are ignored and problems can be traced when a disaster occurs. Without a good security system, no matter how good the information system technology is, it will endanger an agency or organization itself. Based on this background, it is necessary to evaluate the existence of security gaps (vulnerabilities) and weaknesses of the HRD information system website. The research method uses the Information System Security Assessment Framework and the Open Web Application Security Project by using tools niktoto look for vulnerabilities, zap flows and operating systems using linux. The test results can be concluded as a solution to solve the problem of the weaknesses of the HRD Information System webserver. Testing should be done more than once in depth, perform maintenance processes on hardware, software, and networks, perform port filters and periodically increase server security, either by using an original antivirus or scanning regularly.

Keyword: *security; data; vulnerability; penetration testing; ISSAF; OWASP*.

Abstrak

Sistem keamanan komputer semakin dibutuhkan seiring dengan meningkatnya pengguna yang terhubung ke jaringan internet, hal ini dapat memicu terjadinya tindak kejahatan *cyber* oleh orang yang tidak bertanggung jawab. Penelitian ini dilakukan pada Sistem Informasi sebuah Rumah Sakit. Salah satunya web server untuk informasi HRD. Sistem ini berisikan data karyawan dan data absensi karyawan. Keamanan webserver biasanya merupakan masalah bagi administrator. Sering kali permasalahan tersebut terabaikan dan permasalahan dapat ditelusuri ketika terjadi bencana. Tanpa sistem keamanan yang baik, sehebat apapun teknologi sistem informasi akan membahayakan suatu instansi atau organisasi itu sendiri. Berdasarkan latar belakang tersebut, maka dibutuhkan evaluasi mengenai adanya celah keamanan (vulnerability) dan kelemahan dari website sistem informasi HRD. Metode penelitian menggunakan Information *System Security*

Assesment Framework dan *Open Web Application Security Project* dengan menggunakan *tools* nikto untuk mencari celah keamanan (vulnerability), owas zap dan sistem operasi menggunakan linux. Hasil Pengujian disimpulkan dapat menjadi solusi untuk mengatasi permasalahan terhadap kelemahan webserver Sistem Informasi HRD. Pengujian sebaiknya dilakukan lebih dari 1 kali secara mendalam, melakukan proses maintenance terhadap *hardware, software*, maupun jaringan, melakukan *filter port* dan melakukan peningkatkan keamanan server secara berkala, baik dengan cara menggunakan antivirus original maupun scanning secara berkala.

Kata kunci: keamanan; data; vulnerability; penetration testing; ISSAF; OWASP.

Pendahuluan

Semakin bertambahnya pengguna internet namun tidak diimbangi dengan adanya sumber daya manusia atau administrator jaringan yang mumpuni di bidangnya maka ancaman – ancaman tindak kejahatan *Cyber* akan muncul. Maka dari itu dibutuhkan sumber daya manusia atau administrator yang handal di bidangnya sehingga dapat menjaga keamanan data serta informasi yang ada di dalam sistem dengan baik (Hermawan, 2015). Keamanan komputer menjadi penting karena ini berkaitan dengan data pribadi (*Privacy*), integritas (*Integrity*), hak akses atau verifikasi (*Autentication*), kerahasiaan (*Cofidentiality*) dan ketersediaan (*Availability*). Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) merilis survei penetrasi dan perilaku pengguna internet tahun 2018. Disebutkan jumlah pengguna internet mencapai 171, 17 juta jiwa.

Selain itu Indonesia merupakan salah satu negara yang web server nya sering dibobol oleh hacker baik berkala nasional maupun internasional (Yunanri et al., 2017). Sejak Oktober tahun 2018 Rumah Sakit XYZ Purwakarta telah menerapkan absensi kehadiran karyawan dengan mesin absensi (fingerscan) yang telah terintegrasi dengan aplikasi berbasis web. Aplikasi absensi karyawan online tersebut diberi nama Sistem HRD. Sejak oktober tahun 2018 sampai tahun 2019, Sistem HRD telah beberapa kali mengalami pengembangan baik dari sisi fitur maupun data yang disimpan.

Data yang tersimpan pada database Sistem HRD berisi data karyawan dan data kehadiran karyawan. Data kehadiran tersebut selanjutnya digunakan untuk pemberian reward and punishment setiap bulannya. Mengingat pentingnya data yang tersimpan maka perlu diterapkan pengujian keamanan dari aplikasi Sistem HRD. Pengujian keamanan tersebut dilakukan untuk mengetahui tingkat kerentanan agar terhindar dari serangan dari pihak yang tidak bertanggung jawab.

Salah satu metode untuk menguji aplikasi berbasis web adalah metode ISSAF (*Information System Security Assessment Framework) dan OWASP (Open Web Application Security Project*) yang dikeluarkan oleh owasp.org sebuah organisasi non-profit yang berdedikasi pada keamanan aplikasi berbasis web (Afif, 2017). Metode ini

bebas digunakan oleh siapa saja yang ingin mengetahui kerentanan dari sebuah aplikasi web (Dirgahayu et al., 2016).

Kamus Bahasa Indonesia Kontemporer karangan (Salim & Salim, 1991) menjabarkan pengertian analisis sebagai berikut. Analisis adalah penyelidikan terhadap suatu peristiwa (perbuatan, karangan dan sebagainya) untuk mendapatkan fakta yang tepat (asal usul, sebab, penyebab sebenarnya, dan sebagainya). Keamanan web adalah serangkaian prosedur, praktek, dan teknologi untuk melindungi web server, pengguna web, dan organisasi sekitarnya (Yunanri et al., 2017). Keamanan melindungi terhadap perilaku tak terduga. Keamanan web telah sering dianggap oleh praktisi web sebagai kunci kerberhasilan atau kegagalan vendor online yang terkait dengannya. Sering web developer kesulitan untuk menerapkan kebijakan mengenai keamanan di dalam aplikasi web yang mereka bangun.

Sistem keamanan komputer digunakan untuk menjamin agar sumber daya tidak digunakan atau dimodifikasi orang yang tidak di otorisasi. Pengamanan termasuk masalah teknis, manajerial, legalitas dan politis (Janner, 2006). Menurut (Joko Saputro, 2018) penetration Testing merupakan metode evaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan kegitan security audit. Simulasi serangan yang dibuat seperti kasus yang bisa dibuat oleh *black hat hacker, crecker*, dan sebagainya. Tujuannya adalah menentukan dan mengetahui macam – macam serangan yang mungkin terjadi karena kelemahan sistem. Menurut (Caselli et al., 2013) *Information System Security Assessment Framework* (ISSAF) yang dikeluarkan oleh OSSIG (*Open System Security Information Group*) merupakan kerangka terstruktur yang mengkategorikan penilaian keamanan sistem informasi dalam berbagai domain dan rincian kriteria evaluasi atau pengujian khusus untuk masing-masing domain.

Metode Penelitian

A. Analisis Permasalahan

Pengujian celah keamanan (penetration testing) pada website sistem HRD ini sangat diperlukan. Hal ini dikarenakan website sistem HRD tersebut memegang peranan penting di Rumah Sakit XYZ. Penetration testing ini dilakukan dengan tujuan untuk mengetahui apakah terdapat celah-celah keamanan pada website sistem HRD.

B. Analisis Kebutuhan

Berikut analisis kebutuhan perangkat untuk melakukan *penetration testing,* dapat dilihat pada tabel 3.1 di bawah ini:

Tabel 3.1

Analisis Kebutuhan Perangkat

No.	Perangkat	Spesifikasi
1.	Laptop	Intel Celeron 1.60 Gbz. RAM 4 GB

2.	Sistem Operasi	Linux
3.	Vulnerability Tools	Nikto
4.	Penetration Tools	OWASZAP
5.	Modem	Indihome

C. Analisis Sistem

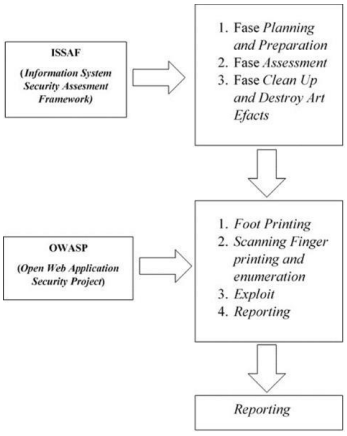
Tools yang digunakan adalah program yang sudah sesuai dengan langkah vulnerability assessment dan penetration testing (Nájera-Gutiérrez, 2016). Tools yang digunakan dapat dilihat pada Table 3.2:

Tabel 3.2

Tahapan yang digunakan dalam penelitian

No.	**Step (Metode)**	**Tools**
Information System Security Asessment Framework (ISSAF)		
1.	Planning and Preparation	WhoIS
2.	Assessment	Nikto
3.	Clean – up and Destroy ArteFacts	Nikto
Open Web Application Security Project (OWASP)		
1.	Footprinting	Nikto
2.	Enumeration and Scanning Fingerprinting	Nikto
3.	Exploit	OWASP ZAP
4.	Reporting	Manual

D. Alur Pengujian



Gambar 3.2 Alur Pengujian

Fase awal dalam tahap pengujian diawali dengan *fase planning and preparation* kemudian diakhiri dengan tahapan pembuatan report dimana detaill dari tahapan pengujian ini akan di bahas secara detai pada bagian hasil dan pembahasan.

Hasil dan Pembahasan

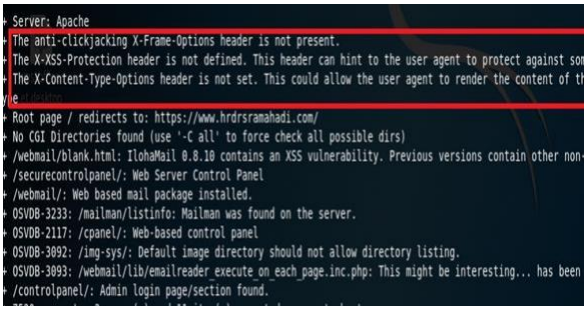
A. Pencarian Celah Keamanan dengan Framework Information System SecurityAssessment Framework (ISSAF)

1) *Fase Planning and Preparation*

Fase planning and preparation merupakan tahapan awal dalam melakukan persiapan dan pengumpulan informasi dari target yang akan dilakukan *penetration testing.*

2) *Fase Assessment*

Pada *fase assessment* penulis mulai melakukan *penetration testing* dan mencari celah keamanan website dengan menggunakan *tools Nikto*. *Nikto* merupakan salah satu *tools* dari Sistem Operasi Kali Linux yang digunakan untuk melakukan pencarian celah keamanan dengan bermodalkan nama domain website (Muniz & Lakhani, 2015). Hasil *Scanning* menggunakan Nikto dapat dilihat di gambar 4.1 di bawah ini :



Gambar 4.1 Hasil Scanning Nikto

3) *Fase Clean Up and Destroy Artefacts*

Dalam *fase* ini, penulis menghapus semua jejak *scanning vulnerability* yang dilakukan menggunakan *tools* Nikto.

B. Pengujian Celah Keamanan dengan Open Web Application Security Project (OWASP)

1) *Footprinting*

Pada *fase* ini penulis mencoba mendapatkan informasi lebih banyak lagi dibandingkan dari *fase planning and preparation*. *Fase planning and preparation* kita mendapatkan informasi dari target berupa ip address public, dan port yang digunakan. Tahap footprinting ini akan lebih detail lagi dalam melakukan pengujian, penulis menggunakan website https://whois.net. Hasil Scanning dengan *Whois* dapat dilihat di gambar 4.2 di bawah ini:

Gambar 4.2 Hasil Scanning dengan WhoIs

2) *Scaning Fingerprinting and Enumeration*

Pada *fase* ini penulis mengidentifikasi *host, port* dan *services* dalam suatu jaringan. *Tools* yang digunakan pada *fase* ini adalah Nikto. Hasil dari *fase* ini dapat dilihat pada Gambar 4.3 di bawah ini:

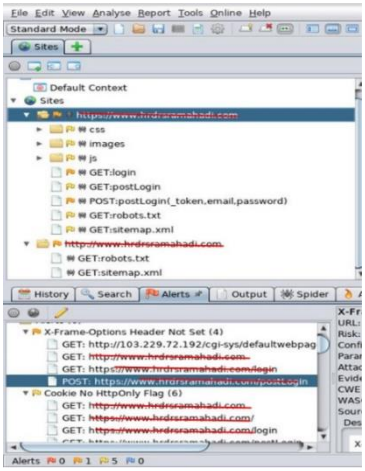
Gambar 4.3 Hasil Scanning dengan Nikto

3) *Exploit*

Fase Exploit merupakan fase pengujian celah keamanan yang ditemukan, informasi yang diperoleh pada fase sebelumnya bisa digunkan sebagai bahan untuk melakukan pengujian celah keamanan. Pada fase exploit ini ada 3 pengujian yang perlu dilakukan berdasarkan *framework Open Web Application Security Project* (OWASP). Yaitu:

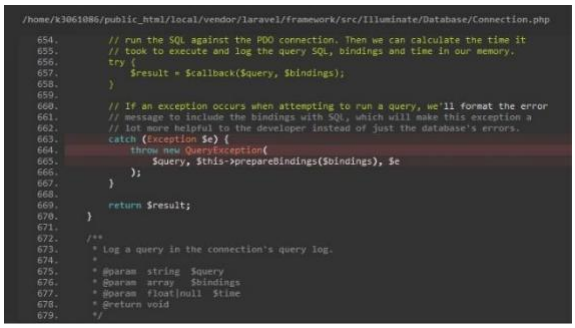
a) *Authentication Testing*

Pada *authentication testing* ini bertujuan untuk melakukan pengujian pada proses authentication / pengecekan login user yang terdaftar pada website target. Pada umumnya nama file yang berisi perintah authentication / pemeriksaan user ini bernama "ceklogin" atau "*postLogin*". Hasil *scanning* celah keaman dengan menggunakan OWASP ZAP dapat dilihat pada gambar 4.4:



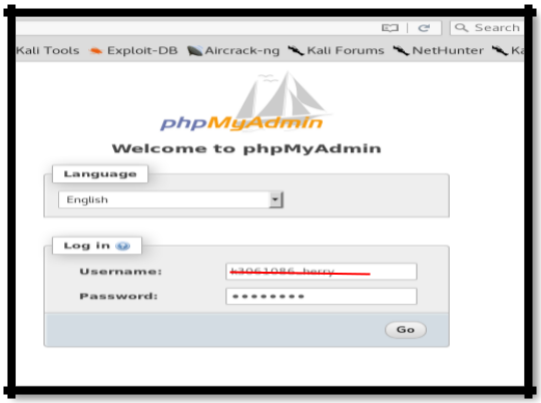
Gambar 4.4 Hasil Scanning dengan OWASP ZAP

Hasil pengujian dengan OWASP ZAP pada file authentikasi target yaitu file postLogin.php dapat dilihat pada gambar 4.5 di bawah ini :



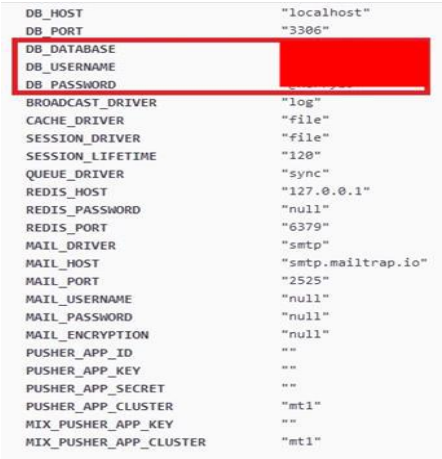
Gambar 4.5 Hasil Pengujian pada file postLogin.php

Hasil pengujian pada gambar 4.5 menunjukkan bahwa website target masih mengaktifkan notifikasi error apabila ada kesalahan penulisan kode (Muhsin & Fajaryanto, 2016). Hal dapat menjadi celah yang dapat diexploitasi sehingga menjadi jalan masuk untuk mengakses ke database. Disini penulis melakukan pengujian lebih dari satu kali untuk mendapatkan kelemahan pada website target. Berikut hasil pengujian file postLogin.php yang ke tiga kali nya. Dapat dilihat pada gambar 4.6 di bawah ini :



Gambar 4.6 Hasil Pengujian ke 2 pada file postLogin.php

Dari hasil pengujian di atas, didapatkan *username* dan *password database* yang selanjutnya coba dimasukkan ke halaman *public html website* target. Halaman *public html* target dapat dilihat pada gambar 4.7 di bawah ini :



Gambar 4.7 Halaman *Public HTML target*

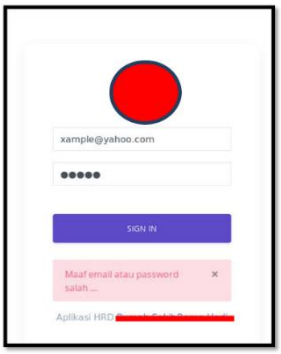
Setelah masuk ke database target, terdapat beberapa table yang dapat diexploitasi. Sampai dengan fase ini, membuktikan bahwa website target memiliki kelamahan pada proses authentikasi.

b) *Authorization Testing*

Authorization testing merupakan pengujian yang memungkinkan akses ke sumber daya bagi mereka yang diizinkan untuk menggunakannya. Setelah ditemukan kelamahan pada proses autentikasi dan berhasil masuk ke database target. Penulis melakukan *authorization testing* yang bertujuan untuk mendapatkan akses ke website target melalui halaman login. Pada fase ini, penulis berusaha untuk membuat username dan password baru, tanpa mengganti username dan password yang telah ada. Disini penulis menambahkan user account baru dengan username xample@yahoo.com dan password 12345. Seprti pada gambar 4.8 di bawah ini :

Gambar 4.8 Menambahkan *user account* baru melalui *database*

Selanjutnya mencoba memasukkan username dan password yang telah dibuat dengan mengakses halaman login target. www.hrdrs***.com/login . Seperti pada gambar 4.9 dibawah ini :



Gambar 4.9 *Login* dengan *user* baru.

Muncul pemberitahuan bahwa *username* atau *password* salah. Hal ini dikarenakan *website* target menggunakan *security* yang mengharuskan setiap penambahan user account baru harus melalui halaman website target tidak bisa melalui database. Dapat dilihat pada pengaturan *user account* yang terdapat pada *database website* target. Dimana kolom *password* berisi pesan yang telah dienkripsi, sedangkan *user account* xample@yahoo.com pada kolom *password* tidak dienskripsi. Dikarenakan *user account*

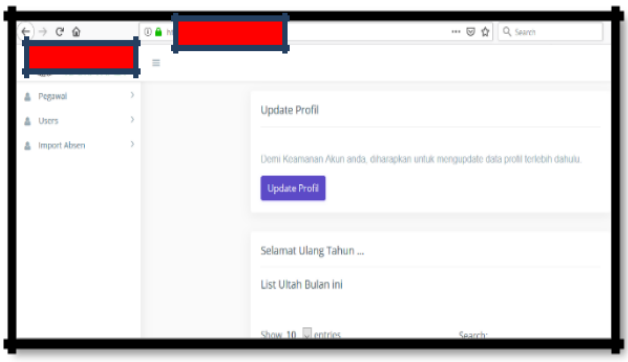
xample@yahoo.com ditambahkan melalui *database*. Seperti pada gambar 4.10 di bawah ini :

Gambar 4.10 Perbedaan user account lama dan baru

Jadi pada *fase authorization testing* ini, *website* target memiliki keamanan yang bagus. Walaupun telah berhasil masuk ke database target. Namun tidak bisa menambahkan hak akses pada *user account* baru melalui database. Pemberian hak akses hanya bisa dilakukan melalui halaman website target.

c) *Session Management Testing*

Pada fase ini, penulis melakukan pengujian pada *website* target. Apakah memiliki *session* untuk mencegah kemungkinan bisa mengakses halaman sebelumnya dengan menekan "backspace" atau tidak. Pada fase ini penulis menggunakan web browser mozilla firefox. Penulis meminta *username* dan *password* yang telah terdaftar di *website* target kepada *administrator* jaringan. Seperti pada gambar 4.11 di bawah ini :



Gambar 4.11 Halaman *home website* target

Website target memiliki session sehingga apabila telah melakukan logout tidak dapat kembali mengakses halaman home tanpa login ulang.

4) *Reporting*

Dari hasil pengujian celah keamanan dapat dilihat pada tabel 4.1 di bawah ini:

Tabel 4.1 Hasil Pengujian Celah Kemanan

No.	Celah Keamananan	Keterangan
1.	Cross Site Scripting (XSS)	Ditemukan celah dimana attacker bisa mengambil password dari cookie website yang belum terdenskripsi. Notifikasi error penulisan script masih diaktifkan, sehingga terlihat nama dan letak *database* target
2.	Injection Flaws	Tidak ditemukan
3.	Malicious File Execution	Tidak ditemukan
4.	Insecure Direct Object Reference	Tidak ditemukan
5.	Cross Site Request Forgery (CSRF)	Tidak ditemukan
6.	Information Leakage and Improper Error Handling	Tidak ditemukan
7.	Broken Authentication and Session Management	Tidak ditemukan
8.	Insecure Cryptographic Storage	Tidak ditemukan
9.	Insecure Communications	Tidak ditemukan
10.	Failure to Restrict URL Access	Tidak ditemukan

Kesimpulan

Dari hasil pencarian celah keamanan (*vulnerability testing*) dan pengujian celah keamanan (*penetration testing*) ditemukan beberapa kelamahan yang teradapat pada website target. Kelamahan tersebut dapat *diexploitasi* hingga database target dapat diakses oleh pihak yang tidak berwenang atau tidak memiliki hak akses. Beberapa kelemahan yang ditemukan diantaranya:

1. *Website* target masih mengaktifkan notifikasi error apabila ada kesalahan pada penulisan kode program. Hal ini memungkinkan adanya celah untuk mengakses database target.
2. *Website* target mengaktifkan halaman *public html*. Hal ini memungkinkan adanya akses langsung ke halaman database phpMyAdmin tanpa login ke cpanel.
3. *Website* target memberi nama file yang berfungsi sebagai autentikasi dengan nama file yang mudah ditebak dan umum. File yang dimaksud adalah file postLogin.php. Hal ini memudahkan peretas menemukan file yang berfungsi untuk autentikasi.

Namun website target telah menggunakan *security* berupa enkripsi pada penulisan *password user account*. Hal ini dapat mengamankan *website* dari pembuatan *user account* yang tidak dikenal melalui database.

Bibliography

Afif, M. (2017). *Implementasi Keamanan OWASP Terhadap Aplikasi Berbasis GTFW*. STMIK AKAKOM Yogyakarta.

Aryasa, K., Paulus, Y. T., 2017, *Implementasi Secure Hash Algorithm-1 Untuk Pengamanan Data Dalam Library Pada Pemrograman Java*, Citec Journal, Vol. 1, No. 1, Hal 57 – 66.

B. Ghozali, Kusrini, and Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) untuk Penilaian Risk Rating", Citec J., vol. 4, no. 4, pp. 264–275, 2017

Caselli, M., Kargl, F., & Limmer, T. (2013). *D5. 1 Security Testing Methodology*. CRISALIS.

Fernando, Y. I., Abdillah, R., 2016, *Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM)*, Jurnal CoreIT, Vol. 2, No.1, Hal 33 – 40.

Dirgahayu, R. T., Prayudi, Y., & Fajaryanto, A. (2016). P*enerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server*. *Network Engineering Research Operation*, *1*(3).

Hermawan, R. (2015). *Kesiapan Aparatur Pemerintah dalam Menghadapi Cyber Crime di Indonesia*. *Faktor Exacta*, *6*(1), 43–50.

Hutagalung, R. H., Nugroho, L. E., Hidayat, R., 2017, *Menentukan Dampak Resiko Keamanan Berbasis Pendekatan OWASP*, Prosiding SNATI F Ke-4 Tahun 2017, Kudus, Indonesia.

I. P. Agus and E. Pratama, "Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study : X Company)", Int. J. Comput. Netw. Inf. Secur., no. July, pp. 8–12, 2019.

Jajang Ruhiyat, Angga Setiyadi, "Sistem Monitoring Website Dengan Metode ISSAF Di Dinas Komunikasi dan Informatika Kabupaten Tangerang", Unikom, 2018

Janner, S. (2006). *Pengenalan Teknologi Komputer dan Informasi*. *Yogyakarta: Andi*.

Muhsin, M., & Fajaryanto, A. (2016). *Penerapan Pengujian Keamanan Web Server*

Menggunakan Metode OWASP versi 4 (Studi Kasus Web Server Ujian Online). *Multitek Indonesia*, *9*(1), 31–42.

Muniz, J., & Lakhani, A. (2015). *Web penetration testing with kali linux*. Packt Publishing Ltd. First Edition, Birmingham.

Nájera-Gutiérrez, G. (2016). *Kali Linux Web Penetration Testing Cookbook*. Packt Publishing Ltd.

OWASP Risk Rating Methodology, https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, diakses tanggal 23 Oktober 2018

Salim, P., & Salim, Y. (1991). *Kamus bahasa Indonesia kontemporer*. Edisi Pertama.

Web Application Security Consortium, http://www.webappsec.org/, yang diakses tanggal 23 Oktober 2018

Yunanri, Y., Riadi, I., & Yudhana, A. (2017). *Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST)*. *Annual Research Seminar (ARS)*, *2*(1), 300–304.

Y. W, I. Riadi, and A. Yudhana, "Analisis Deteksi Vulnerability Pada Webserver Open Journal System Menggunakan OWASP Scanner", JURTI, vol. 2, no. 1, pp. 1–8, 2018.