e-ISBN 978-623-93343-4-5
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 15 September 2021

Pengujian Celah Keamanan *Website* Menggunakan Teknik *Penetration Testing* dan Metode OWASP TOP 10 pada *Website* SIM xxx

Yum Thurfah Afifa Rosaliah[1], Jayanta[2], Bayu Hananto[3]
Informatika / Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. Rs. Fatmawati, Pondok Labu, Jakarta Selatan, DKI Jakarta, 12450, Indonesia
yumafifa4@gmail.com[1], anta.jayanta@gmail.com[2], bayuhananto8086@gmail.com[3]

Abstrak. *Website* merupakan sekumpulan halaman pada suatu *domain* di internet yang dibuat dengan tujuan tertentu dan dapat diakses secara luas melalui halaman depan menggunakan URL *website*. SIM (*Security Information Management*) merupakan sistem yang digunakan sebagai pemantauan suatu sistem lainnya, bertujuan untuk melihat kegiatan yang bersifat keamanan. Sehubung dengan meninggkatnya peggunaan *digital hardware* saat ini, semakin meningkat peluang kejahatan siber seperti halnya kebocoran data. *Penetration testing* adalah salah satu cara untuk mensimulasikan metode yang mungkin akan digunakan oleh penyerang untuk menerobos mekanisme keamanan dan mendapatkan akses secara ilegal ke dalam suatu sistem. OWASP *TOP* 10 adalah daftar yang dirilis oleh komunitas OWASP yang berisikan 10 daftar teratas celah keamanan yang dapat mengancam keamanan suatu website. Penelitian ini bertujuan untuk mengetahui apakah SIM xxx memiliki celah keamanan. Setelah melakukan uji penetrasi menggunakan metode OWASP TOP 10 terhadap *website* SIM xxx terdapat 4 celah keamanan. Metode OWASP TOP 10 efektif dijadikan sebagai standard keamanan untuk melakukan uji penetrasi.

Kata Kunci: Website, SIM, Penetration Testing, OWASP TOP 10.

1. Pendahuluan

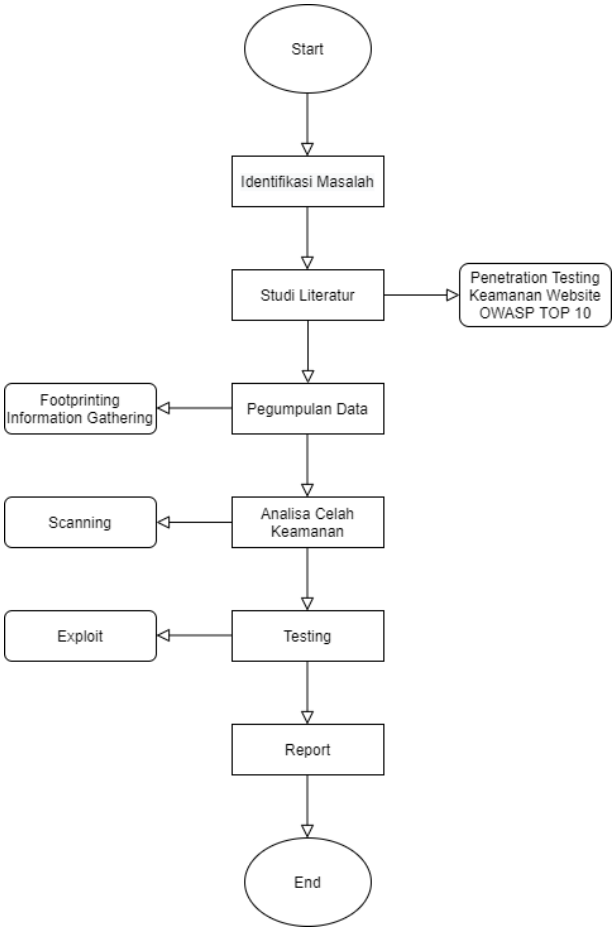
Seiring dengan perkembangan teknologi, Internet sudah menjadi kebutuhan bagi setiap pengguna *digital hardware* saat ini. Hampir semua aktivitas yang dilakukan sehari-hari membutuhkan internet sebagai penunjang keperluannya. Seperti halnya komunikasi, mencari informasi, transaksi digital, dan bahkan hiburan pun saat ini marak dengan penggunaan internet. Semakin maraknya penggunaan internet dikalangan masyarakat luas, semakin bertambahnya peluang kejahatan siber. Seperti halnya kebocoran data yang berisikan informasi dari suatu website oleh oknum tak bertanggung jawab yang dapat merugikan banyak pihak. Kebocoran data atau perusakan dapat mengancam setiap saat seiring dengan meningkatnya sumber daya manusia. Berdasarkan Pasal 26 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur bahwa penggunaan data pribadi harus dilakukan dengan sepersetujuan orang yang bersangkutan, dan bahwa setiap orang yang dilanggar haknya dapat mengajukan gugatan. Perlu dilakukannya pengujian celah atau biasa disebut uji penetrasi keamanan terhadap *website* guna meminimalisir penjahat siber dapat menembus sistem keamanan yang sudah ada. Dengan adanya pengujian celah keamanan tersebut dapat menjadi sebuah solusi yang digunakan sebagai tolak ukur untuk memperbaiki sistem keamanan *website* selanjutnya.

Studi Kasus yang akan menjadi objek penelitian ini yaitu *Website* Sistem Informasi Manajemen (SIM) xxx. SIM merupakan sistem yang digunakan sebagai pemantauan suatu sistem lainnya, yang dimana pemantauan tersebut difungsikan untuk melihat sebuah kegiatan yang bersifat keamanan. Sebuah *server* tidak dapat memantau dirinya sendiri sehingga diperlukan suatu sistem yang dapat memonitoring kegiatan yang ada pada *server*. *Server management and monitoring* diperlukan agar *admin* dapat memantau dengan mudah apa saja yang terjadi pada *server*. Untuk itu SIM dapat dipertimbangkan sebagai suatu sistem informasi yang cukup penting untuk dilakukannya pengamanan yang kuat dikarenakan merupakan sebuah sistem informasi yang berisikan banyak data krusial pengguna yang merupakan dosen maupun data mahasiswa, guna meminimalisir hal-hal yang tidak diinginkan seperti pencurian data, penyalaah gunaan data, dan bahkan pengambil alihan sistem oleh pihak *attacker*.

Untuk mencari tahu kekurangan apa saja yang dimiliki website SIM xxx tersebut, pada penelitian ini akan dilakukan uji penetrasi berdasarkan standar keamanan yang ada pada OWASP TOP 10.

Hasil dari penelitian ini adalah untuk menemukan celah keamanan yang terdapat pada *website* Sistem Informasi Manajemen (SIM) xxx yang akan digunakan sebagai landasan atau rujukan untuk perbaikan sistem keamanan guna meminimalisir celah untuk masuk ke *website* SIM xxx.

2. Metodelogi Penelitian



Gambar. 1. Flowchart Alur Penelitian.

2.1 Identifikasi Masalah

Maraknya permasalahan kebocoran data suatu *website* yang berisikan informasi para *user* membuat peneliti tertarik menjadikan *pentration testing* sebagai tema penelitian ini. Jika diuraikan, masalah yang terjadi, diantaranya:

1. Kurang *secure* pengamanan yang ada pada suatu *domain website*.
2. Tingkat pencurian data pada suatu aplikasi *website* yang tinggi.
3. Tingkat kesadaran pihak instansi tentang rentannya pembobolan data pada aplikasi *website* suatu instansi apabila tidak sering dilakukannya *penetration testing*.

2.2 Studi Literatur

Studi Literatur dilakukan dalam upaya mencari dan mengumpulkan data beserta informasi yang berkaitan dengan penelitian, diantaranya mengenai *website*, SIM, *penetration testing*, *vulnerability*, serta pengimplementasian mengenai metode OWASP *TOP* 10. Studi literatur ini dilakukan dari berbagai sumber, diantaranya *e-book*, jurnal penelitian, *website*, buku, dll. Sumber pustaka pada penelitian ini dicantumkan dalam daftar pustaka.

2.2.1 Website

Website atau biasa disebut Situs web adalah kumpulan halaman khusus yang saling berhubungan dan saling berhubungan untuk domain di Internet yang dapat diakses secara luas dari halaman beranda Anda dari browser menggunakan URL pada halaman web. Fitur paling dasar dari sebuah situs web adalah memiliki informasi / konten statis, yaitu hampir tidak berubah.. (Waryanto, 2018).

2.2.2 SIM

SIM (*Security Information Management*) merupakan sistem yang digunakan sebagai pemantauan suatu sistem lainnya, yang dimana pemantauan tersebut difungsikan untuk melihat sebuah kegiatan yang bersifat keamanan. SIM mencakup manajemen ancaman, pemantauan real-time insiden keamanan dan memicu reaksi yang tepat jika terjadi insiden. Dengan demikian, data yang dikumpulkan disatukan untuk mengurangi jumlah data dan memfasilitasi penggunaan untuk bereaksi dengan tepat terhadap peristiwa keamanan (Vielberth and Pernul, 2018).

2.2.3 Vulnerabillity

Vulnerability dapat didefinisikan sebagai kerentanan jaringan komputer atau lubang keamanan, dan kerentanan keamanan dipahami sebagai kelemahan program/infrastruktur yang memungkinkan sistem untuk dieksploitasi. Kerentanan ini disebabkan oleh kesalahan desain, pembuatan, atau implementasi sistem. Kerentanan ini digunakan sebagai sarana bagi peretas untuk mendapatkan akses tidak sah ke sistem. Peretas sering mengeksploitasi kerentanan yang ditemukan. (Kholiq, 2017).

2.2.4 Penetration Testing

Penetration testing adalah salah satu cara untuk mensimulasikan metode yang mungkin akan digunakan oleh penyerang untuk menghindari atau menerobos mekanisme keamanan dan mendapatkan akses secara ilegal ke dalam suatu sistem. (Hernawan dan Kho, 2019).

2.2.5 OWASP TOP 10

OWASP TOP 10 atau yang biasa disebut OWASP 10 adalah sebuah daftar teratas kerentanan keamanan yang dapat mengancam keamanan suatu *website* yang dirilis oleh komunitas OWASP. daftar ini terus berkembang dan berubah-ubah mengikuti perkembangan teknologi *website*/aplikasi web yang terus berkembang. (OWASP TOP 10, 2017).

2.3 Pengumpulan Data

Pengumpulan data dilakukan dengan dua tahap, yaitu *information gathering* dan *footprinting*. *Information Gathering* dan *Footprinting* dilakukan guna mencari beberapa data yang berisikan informasi seperti alamat IP, Spesifikasi Server yang digunakan, dan banyak informasi penting lainnya yang akan digunakan sebagai landasan

untuk melakukan eksploitasi menggunakan berbagai tools sepert *Netcraft*, *Whois*, HTT*Print*, *Whatweb*, dan *Nmap*. *Footprinting* merupakan bagian dari *information gathering* yang bertujuan untuk mencari spesifikasi *server*. Dan *tools* yang digunakan pada proses *Footprinting* adalah HTTP*print*.

2.4 Analisa Celah Keamanan

Analisis kerentanan akan dilakukan dengan *vulnerability scanning*. *Vulnerabilty scanning* dilakukan dengan menganalisis data-data, ciri-ciri, dan struktur jaringan yang sudah diketahui sebelumnya. Tujuan dari *vulnerability scanning* adalah untuk mengidentifikasi kerentanan yang terpapar pada jaringan komputer menggunakan sebuah tools yang dirancang khusus untuk mencari celah keamanan, Tools yang digunakan pada penelitian ini yaitu OWASP ZAP.

2.5 Testing

Pada bab ini berisi mengenai pengujian (*penetration testing*) berdasarkan 10 *Standard* keamanan OWASP *TOP* 10 2017 pada *website* Sistem Informasi Manajemen (SIM) xxx menggunakan beberapa jenis *tools* yang berbeda yang bertujuan untuk menguji apakah *website* Sistem Informasi Manajemen (SIM) memiliki celah keamanan. Dan berikut daftar celah keamanan yang diterapkan OWASP.

	OWASP Top 10 - 2017
→	A1:2017-Injection
→	A2:2017-Broken Authentication
↘	A3:2017-Sensitive Data Exposure
U	A4:2017-XML External Entities (XXE) [NEW]
↘	A5:2017-Broken Access Control [Merged]
↗	A6:2017-Security Misconfiguration
U	A7:2017-Cross-Site Scripting (XSS)
☒	A8:2017-Insecure Deserialization [NEW, Community]
→	A9:2017-Using Components with Known Vulnerabilities
☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Gambar. 2. Standard Keamanan OWASP TOP 10.

2.6 Report

Pada bab ini berisi penjelasan secara detail hasil *report* uji penetrasi yang sudah dilakukan yang dapat digunakan untuk pedoman perbaikan *website* selanjutnya.

3. Hasil dan Pembahasan

3.1 Information Gathering

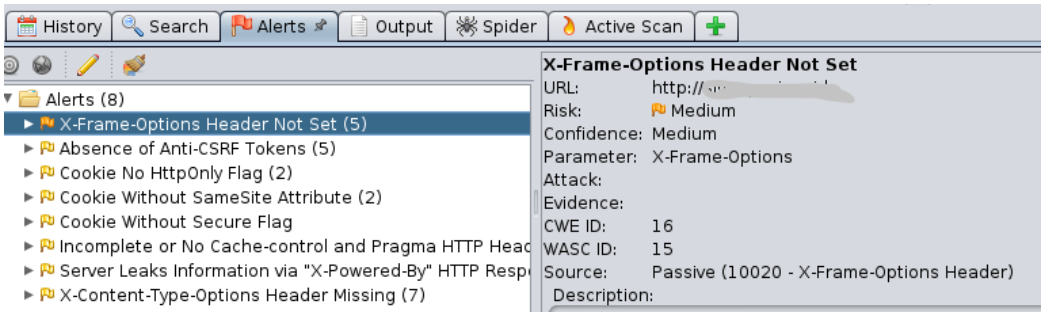
Berikut hasil yang didapat dari proses tersebut.

Tabel 10. Hasil Information *Gathering.*

No	Proses	Hasil Akhir
1	*Netcraft*	IP *Address*, yaitu 103.xxx.xx.x
2	*Whois*	Alamat *Hosting*, *Server*, *Email*, dan Informasi lainnya terkait *Website* SIM xxx, yaitu Jl xxx, Jakarta xxx, xxx.net.id.
3	HTT*Print*	*Apache*/2.2.15(*Cent*OS)
4	N*map*	*Open Port* : *Port* 22/SSH, *Port* 80/HTTP, *Port* 5443/*Postgre*SQL, *Port* 443/SSL
5	*Whatweb*	HTTP *Header*

3.2 Scanning

Berikut hasil *Scanning vulnerabillity* menggunakan *tools* OWASP ZAP versi 2.9.0



Gambar. 3. Hasil Scanning.

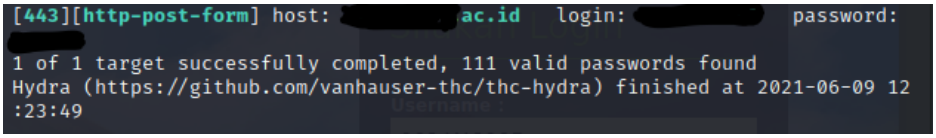
Vulner/celah keamanan yang diambil adalah yang medium risk dari hasil scanning vulnerabillity diatas adalah tidak adanya header X-Frame-Options dalam respons HTTP untuk melindungi dari serangan Clickjacking sehingga serangan Clickjacking dapat saja dilakukan dari luar terhadap website SIM xxx.

3.3 Testing

Berikut hasil temuan pada proses *Testing* yang telah dilakukan pada *Website* SIM xxx berdasarkan 10 standard keamanan yang ada pada OWASP TOP 10 2017.

3.3.1 Broken Authentication

Broken Authentication pada halaman website menggunakan *tools hydra* pada kali linux. Dan berikut hasil yang didapatkan.

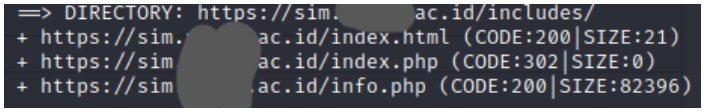


Gambar. 4. Hasil Hydra.

Dilihat dari hasil percobaan *bruteforce* diatas dapat disimpulkan percobaan *bruteforce* berhasil dilakukan dan terdapat celah untuk masuk pada *website* SIM xxx. Dan hasil yang diperoleh, terdapat banyak *username* dan *password* yang ditemukan dari hasil percobaan *bruteforce* menggunakan *hydra* dengan bantuan bebarapa informasi *post* http dari hasil *scanning burproxy* yang dilakukuan. Salah satu yang dapat digunakan untuk mencoba masuk ke sistem SIM xxx.

3.3.2 Sensitive Data Exposure

Pencarian *file* tertentu pada *website* SIM xxx dilakukan menggunakan *tools dirb* pada kali linux. Dan berikut hasil temuan *file* yang bisa diakses pada *website* SIM xxx.



Gambar. 5. Hasil Dirb.

Status *Code* 200 diatas menandakan berhasil/ditemukannya direktori pada URL yang dapat diakses pada alamat *website*. Dan berikut hasil yang diperoleh dari percobaan URL yang didapat berdasarkan informasi yang ada pada gambar diatas

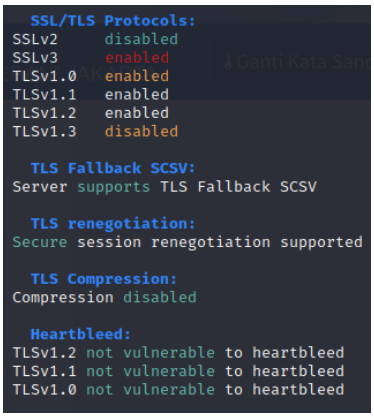
Gambar. 6. Hasil Pencarian URL.

Gambar diatas merupakan *file* data yang yang dapat diakses oleh *public* tanpa perlu masuk ke sistem *website* SIM xxx. Dapat dilihat dari gambar diatas bahwa Info.php berisi beberapa informasi yang sangat *detail* terhadap konfigurasi yang ada pada sistem *website* SIM xxx. Dari *Database* hingga informasi yang ada pada *server* seperti *open port configuration* dan data penting lainnya yang menguntungkan pihak *attacker*. Info.php perlu di*set* ulang agar *public* maupun attacker tidak dapat mengakses *file* yang termasuk dalam *sensitive* data tersebut.

3.3.3 Security Misconfiguration

[10] Configuration port ssl

SSLScan dilakukan pada *Kali Linux Operating System*. Berikut hasil yang didapat dari scan port SSL



Gambar. 7. Hasil SSLScan.

Dari gambar dilihat dapat dilihat bahwa SSLv3 statusnya *enabled*. SSL, dan penerusnya TLS, adalah protokol *kriptografi* yang dirancang untuk menyediakan keamanan komunikasi melalui Internet. Di ranah web, mereka menyediakan HTTPS, tetapi mereka juga digunakan untuk protokol aplikasi lain. SSLv1 tidak pernah dirilis secara publik, dan SSLv2 dengan cepat ditemukan tidak aman. SSLv3 telah dibuat, dan, bersama dengan TLSv1/1.1/1.2 yang lebih baru, saat ini masih digunakan untuk mengamankan lapisan *transport* Internet.

Seperti yang terjadi pada SSLv2, baru-baru ini *Google Engineering* menunjukkan bahwa SSLv3 rusak (dengan teknik eksploitasi yang dikenal sebagai *POODLE*) dan tidak boleh digunakan lagi. Ada tambalan, tetapi itu tidak mengurangi masalah sepenuhnya karena hanya akan berfungsi jika kedua sisi koneksi telah ditambal. SSLv3 hampir berusia 18 tahun, tetapi dukungan untuknya tetap tersebar luas. *Klien* dan *server* harus menonaktifkan SSLv3 sesegera mungkin.

3.3.4 Clickjacking Testing hasil dari vullnerabillity scanning

Gambar. 8. Hasil Clickjacking.

Seperti hasil yang didapat dari *vullnerabillity scan* menggunakan OWASP ZAP sebelumya, terdapat celah untuk melakukan *clickjacking*. *Clickjacking* termasuk kerentanan yang cukup serius dan dikategorikan *medium warnin*g. Apabila *clickjacking* dilakukan oleh *hacker* bisa berdampak cukup serius, hacker dapat memanfaatkan *clickjacking* untuk mengambil *username* dan *password* dari *click button* yang sudah terkena *attack clickjacking*.

3.4 Report

Table 11. *Report.*

Metode	status	Hasil temuan
SQL Injection	Tidak Ditemukan	All tested parameters do not appear to be injectable
Broken Authentication	Ditemukan	1 of 1 target successfully completed, 41 valid password found hydra
Sensitive Data Exposure	Ditemukan	DIRECTORY: https://Alamat_Website.AC.ID/includes/ + https://Alamat_Website.AC.ID/info.php (code:200|SIZE:82396)
XML External Entities (XXE)	Tidak ditemukan	No response
Broken access control:	Tidak ditemukan	1. No response 2. Code 302
Security Misconfiguration 1. SSL setting info 2. Scan openssl heartbleed	1. Ditemukan 2. Tidak ditemukan	1. SSLV3 enabled 2. No heartbeat response Looks like it isn't leaked information
Cross-site-scripting (XSS)	Tidak ditemukan	Length 3867 Length 496
Insecure Deserialization	Tidak ditemukan	Not vulnerable
Using components with vulnerabilities	Tidak ditemukan	103.xxx.xx.x:5432 - LOGIN FAILED
Insuficient logging and monitoring	Tidak ditemukan	could not connect: the host (103.xxx.xx.x:22) was unreachable
Clickjacking from vulnerabillity scanning	Ditemukan	You've been clickjacked

Ancaman-ancaman pada *website* yang terjadi pada tahun 2017 sudah didata oleh OWASP (*Open Web Application Security Project*) dan sudah tercatat pada OWASP Top 10 Security – 2017. Pada OWASP Top 10 Security, terdapat beberapa ancaman dan tingkat resiko dari dampak serangan yang telah diklasifikasikan oleh OWASP. Tingkat ancaman yang diberi nilai sudah dihitung dengan kalkulator khusus dari NIST (*National Institute of Standards and Technology*) yang disebut CVSS (*Common Vunlnerability Scoring System*) dengan rentang *score* 0.0 sampai 10.0. Ancaman tersebut telah digambarkan pada Tabel 4.2.

Table 12. Daftar Ancaman Keamanan berdasarkan metode OWASP TOP 10.

Sumber: https://www.owasp.org/images/0/0a/OWASP_Top_10_2017_GM_%28en%29.pdf

No	Ancaman	CVSS Score	Persentase yang Sering Terjadi	Status
1	Injection	8.0	35%	Tidak Ditemukan
2	Broken Authentication	7.0	74%	Ditemukan
3	Sensitive Data Exposure	7.0	28%	Ditemukan
4	XML External Entities (XXE)	7.0	2%	Tidak Ditemukan
5	Broken Access Control	6.0	53%	Tidak ditemukan
6	Security Misconfiguration	6.0	79%	Ditemukan
7	Cross-site Scripting (XSS)	6.0	77%	Tidak Ditemukan
8	Insecure Deserialization	5.0	2%	Tidak Ditemukan
9	Using Component with Known Vulnerabilities	4.7	28%	Tidak Ditemukan
10	Insufficient Logging & Monitoring	4.0	2%	Tidak Ditemukan

4. Kesimpulan

1. Setelah melakukan uji penetrasi menggunakan metode OWASP TOP 10 terhadap *website* SIM xxx terbukti memiliki 4 celah keamanan yang perlu untuk dilakukan perbaikan guna keamanan *website* SIM xxx kedepannya.

2. Pengujian celah keamanan website SIM(Sistem Informasi Manajemen) dengan Metode OWASP adalah dengan melakukan testing terhadap 10 *standard* keamanan yang ada pada OWASP TOP 10 yaitu *Injection* menggunakan SQL*Map*, *Broken Authentication* menggunakan *hydra*, *Sensitive Data Exposure* menggunakan *Dirb*, *Broken Access Control* menggunakan *Burpsuite*, XXE (XML *External Entities*) menggunakan *Burpsuite*, *Security Misconfiguration* menggunakan SSL*Scan* dan *Heartbleed Bug*, XXS (*Cross Site Scripting*) menggunakan *script manual* dan *burpsuite*, *Insecure Deserialization* menggunakan *Burpsuite*, *Using Components with known vulnerabillities* menggunakan *metasploit framework*, *insufficient logging and monitoring* menggunakan *Metasploit Framework.*

3. Adapun celah keamanan yang ditemukan adalah *Broken Authentication*, *Sensitive Data Exposure*, dan *Security Misconfiguration.* Adapun celah lain yang ditemukan namun tidak termasuk dalam TOP 10 keamanan OWASP yaitu *Clickjacking.*

4. Dari hasil yang didapatkan pada bab IV diatas, dapat disimpulkan bahwa metode OWASP TOP 10 efektif dijadikan sebagai standard keamanan untuk melakukan uji penetrasi terhadap suatu *website.* Hal itu disebabkannnya dengan *standard* keamanan yang dimiliki OWASP lengkap dan detail dilihat dari konfigurasi halaman *website* maupun konfigurasi *server*. Banyak hasil temuan yang mengacu pada 10 *standard* keamanan OWASP tersebut. Maka dari itu metode OWASP TOP 10 menjadi rekomendasi untuk para *pentester* dalam melakukan uji penetrasi menggunakan Metode OWASP Top 10 2017.

Referensi

[1] Jai Narayan Goel.,B.M.Mehtre, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology". 3rd International Conference on Recent Trends in Computing 2015 (ICRTC2015), University of Hyderabad. India: Elsevier, PP710 – 715, 2015.

[2] Waryanto. (2018, januari 22). Pengertian Website Lengkap dengan Jenis dan Manfaatnya. Retrieved from NIAGAHOSTER Blog: https://www.niagahoster.co.id/blog/pengertianwebsite/#Apa_Itu_Website.

[3] Vielberth, M. and Pernul, G. (2018) 'A Security Information and Event Management Pattern', *Federal Ministry of Education and Research*, 1, pp. 1–12.

[4] Kholiq, I. A. (2017, April 9). CELAH KEAMANAN JARINGAN (Vulnerability). Retrieved from CORETAN SEORANGAMATIR: http://imamfolkharmony.blogspot.com/2017/04/celah-keamananjaringan.html.

[5] Kho, Y., & Hernawan, F. Y. (2019). Bug Hunting 101 - Web Application Security Testing. AlFursanID.

[6] OWASP, "The ten Most Critical Web Application Security Risk", The Open Web Application Security Project, 2010. http://www.owasp.org).

[7] OWASP (2017) 'The Ten Most Critical Web Application Security Risks Important Notice Request for Comments GM Golden Master', *Top 10 Security - 2017*. Available at: https://www.owasp.org/images/0/0a/OWASP_Top_10_2017_GM_%28en%29.pdf.