1. HASIL CEK_60960140

by 60960140 Te

Submission date: 15-Aug-2022 10:57AM (UTC+0700)
Submission ID: 1882612899
File name: Menggunakan_Open_Web_Application_Security_Project_Framework.pdf (734.17K)
Word count: 3951
Character count: 24385

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1468-1475
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.4099

Analisis Keamanan Sistem Informasi Akademik Menggunakan *Open Web Application Security Project Framework*

Muh. Amirul Mu'min [1,*], Abdul Fadlil[2], Imam Riadi[3]

[1] Program Studi Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2] Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[3]Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Email: [1,*]mumin2008048038@webmail.uad.ac.id, [2]fadlil@mti.ac.id, [3]imam.riadi@mti.ac.id
Email Penulis Korespondensi: mumin2008048038@webmail.uad.ac.id

Abstrak−Keamanan sistem informasi merupakan salah satu hal penting dalam perkembangan teknologi untuk melindungi data atau informasi yang komprehensif dan terstruktur. Sistem Informasi Akademik (SIA) memiliki layanan untuk menerima permintaan berupa halaman website protokol HTTP atau HTTPS dari klien yang disebut browser. Penyusup dapat meretas website tanpa sepengetahuan pemilik. Penelitian ini dilakukan untuk menemukan kerentanan SIA STIKES Guna Bangsa Yogyakarta. *Framework* yang digunakan adalah *Open Web Application Security Project* (OWASP) yang biaa digunakan untuk mengevaluasi sistem atau aplikasi. *Tools* yang digunakan adalah *WhoIs, SSL Scan, Nmap,* dan *OWASP Zap*. Hasil yang didapatkan yaitu menemukan 12 kerentanan dengan empat kerentanan pada level *medium* yakni *Absence of Anti-CSRF Tokens, Cross-Domain Misconfiguration, Missing Anti-clickjacking Header,* dan *Vulnerable JS Library*, enam pada level *low* yakni *Cookie Without Secure Flag*, *Cookie without SameSite Attribute, Cross-Domain JavaScript Source File Inclusion*, *Server Leaks Information via "X-Powered-By" HTTP Response Header Field), Timestamp Disclosure – Unix,* dan *X-Content-Type-Options Header Missing*, dan dua pada level *informational* yakni *Content-Type Header Missing* dan *Information Disclosure - Suspicious Comments*.

Kata Kunci: Keamanan; SIA; Website; OWASP; OWASP Zap

Abstract−Information system security is one of the important things in the development of technology to protect comprehensive and structured data or information. The Academic Information System (SIA) has a service to receive requests in the form of HTTP or HTTPS protocol website pages from clients called browsers. Intruders can hack websites without the owner's knowledge. This research was conducted to find the vulnerability of SIA STIKES Guna Bangsa Yogyakarta. The framework used is the Open Web Application Security Project (OWASP) which is usually used to evaluate systems or applications. The tools used are WhoIs, SSL Scan, Nmap, and OWASP Zap. The results obtained were finding 12 vulnerabilities with four vulnerabilities at the medium level, namely Absence of Anti-CSRF Tokens, Cross-Domain Misconfiguration, Missing Anti-clickjacking Header, and Vulnerable JS Library, six at the low level namely Cookie Without Secure Flag, Cookie without SameSite Attribute, Cross-Domain JavaScript Source File Inclusion, Server Leaks Information via "X-Powered-By" HTTP Response Header Field( ) Timestamp Disclosure – Unix, and X-Content-Type-Options Header Missing, and two at the informational level namely Content-Type Header Missing and Information Disclosure - Suspicious Comments.

Keywords: Security; SIA; Website; OWASP; OWASP Zap

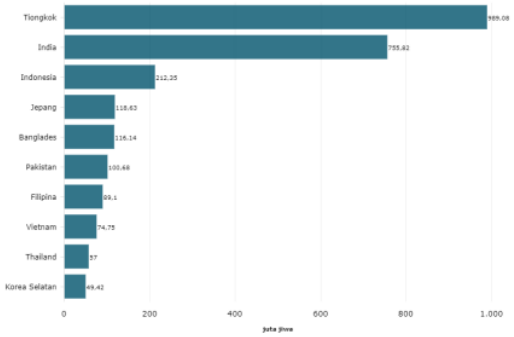
1. PENDAHULUAN

Seiring waktu dengan berkembangnya teknologi informasi dan komunikasi tidak dapat disangkal [1], hampir setiap aktivitas dalam kehidupan sehari-hari tidak terlepas dari teknologi yang ada dengan menggunakan media elektronik sehingga dapat menghubungkan yang satu dengan yang lainnya [2]. Penggunaan situs ini sangat sederhana, dan siapapun dapat mengaksesnya jika terhubung dalam jaringan i*nternet* dan dapat dibuka di komputer atau *smartphone* [3]. Berbagai aktivitas dapat dilakukan melalui teknologi informasi yang disebut sebagai *internet* [4] sebagai media termudah untuk memenuhi kebutuhan pencarian informasi yang diinginkan. Menurut *Internet world stats*, pengguna *Internet* Indonesia mencapai 212,35 juta pada Maret 2021. Berdasarkan indikator ini, Indonesia menempati urutan ketiga dalam hal jumlah pengguna. Internet paling Asia.

Pertama, ada China yang memiliki 98,08 juta pengguna *internet*. sementara di India berada di urutan kedua dengan 755,82 juta pengguna *internet*. Di tempat keempat adalah Jepang. 118,63 juta orang. Bangladesh berada di urutan kelima dengan 116,14 juta pengguna *internet*. Ke-6 Pakistan 168 juta pengguna internet. Pengguna *internet* terbesar ke-7 adalah Filipina dengan 89,1 juta. Setelah itu, Vietnam menempati urutan ke-8 dengan 74,75 juta pengguna *internet*. Thailand menempati urutan kesembilan dengan 57 juta pengguna *internet*. Korea menempati urutan ke-10 dengan 49,42 juta. Jumlah total pengguna *internet* di Asia adalah 2,77 miliar dari 4 orang. 33 miliar jiwa. Jumlah pengguna *Internet* di Asia adalah 53,4 miliar dari 5,17 miliar di dunia [5] seperti pada Gambar 1.

Submitted: **28/04/2022**; Accepted: **24/06/2022**; Published: **25/07/2022**

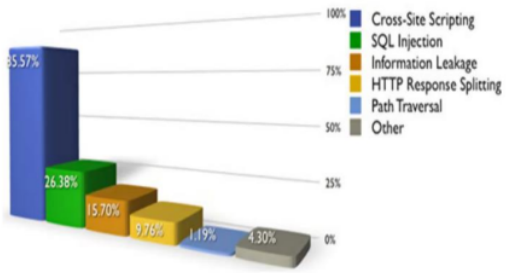
JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1468-1475
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.4099



Gambar 1. Pengguna internet di Asia Tenggara tahun 2021

Website merupakan salah satu aplikasi yang ada saat ini selain aplikasi *mobile* [6]. Pengembangan *website* terus berinovasi, dimulai dengan pemrograman terstruktur, pemrograman berbasis kerangka kerja berorientasi objek untuk *web* seluler aplikasi *web* yang dirancang untuk perangkat seluler dan desktop [7]. *Website* menyediakan sumber data dan informasi yang dapat diakses oleh siapa saja melalui *internet*. Internet dapat menggunakan perangkat lunak *browser* seperti *Internet Explorer, Mozilla Firefox, browser Opera,* dan *Google Chrome* [8].

Website yang aman ditunjukkan dengan sertifikat SSL *(Secure Socket Layer)* dan menggunakan *firewall* sebagai sistem untuk melindungi *website* dari serangan *malware* dengan meningkatkan proses pengembangan *website* dapat meminimalkan jumlah kerentanan pengembangan *webiste* [9]. Sedangkan *website* yang tidak aman dengan mudah biasa dikenal dengan HTTP *(Hypertext Transfer Protocol)* tanpa adanya *secure* di dalam *URL* tersebut. Website terkadang tidak bisa digunakan mengkompensasi serangan *hacking* atau *fishing*. Suatu hari nanti atau pada momen penting, situs *web* sering *down* dan sulit diakses oleh pelanggan. Operator juga memiliki masalah serius saat memulihkan situs tersebut, karena *website* tidak memiliki standar keamanan jaringan yang tinggi, sehingga sangat rentan serangan para *hacker* [10]. Ada beberapa faktor yang dapat menyebabkan kurangnya keamanan untuk situs *web*, seperti kesalahan penulisan kode dan kesalahan konfigurasi. Kesalahan penulisan kode pemrograman saat membuat aplikasi berbasis *website* sering digunakan oleh penyerang. Serangan yang biasa digunakan oleh penyerang antara lain *SQL Injection*, *Authentication,* dan *Cross-Site Scripting* (XSS). Jenis serangan yang umum digunakan adalah SQL injeksi (26,38%) dan XSS (35,57%) seperti yang ditunjukkan pada grafik statistik pada Gambar 2.



Gambar 2. Persentase kerentanan *website*

Keamanan sistem informasi saat ini menjadi salah satu masalah utama dalam perkembangan teknologi informasi dan komunikasi, sistem harus memastikan kerahasiaan, ketersediaan, dan integritas pada semua sumber daya informasi bukan hanya perangkat keras dan data [11]. Organisasi penting melakukan pendekatan yang komprehensif dan terstruktur untuk memastikan bahwa aset informasi organisasi dilindungi dari risiko yang mungkin dihadapi. Ketersediaan ini telah mendorong banyak orang dan organisasi untuk membangun sistem *web server*. Aspek keamanan sistem informasi meliputi kerahasiaan *(confidentiality)* yaitu informasi bisa dapat diakses hanya mereka yang berwenang untuk menerimanya dan kerahasiaan data, integritas *(integrity)* yaitu keakuratan informasi yang dilindungi oleh beberapa metode pemrosesan yang baik, dan ketersediaan *(availability)* harus tersedia untuk memperoleh informasi yang dicari [12]. Keamanan dianggap penting karena jika orang yang tidak bertanggung jawab mengakses informasi, keakuratan informasi dicurigai dan informasi menjadi tidak dapat stabil [13], sistem keamanan komputer ini juga digunakan untuk mencegah orang yang tidak berwenang menggunakan atau memodifikasi sumber daya [14]. Keamanan meliputi masalah teknis, administratif, hukum, dan politik.

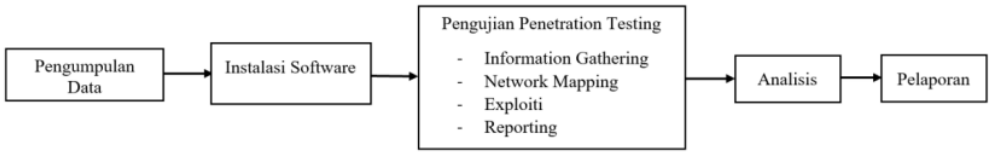
Submitted: **28/04/2022**; Accepted: **24/06/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1468-1475
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.4099

Salah satu *framework* yang digunakan adalah OWASP yaitu *framework* yang diterbitkan oleh komunitas OWASP yang berisi daftar 10 kerentanan teratas yang dapat membahayakan keamanan situs *web*. Daftar ini terus bertambah dan berubah seiring dengan berkembangnya teknologi situs *web* [15]. OWASP merupakan *framework* terstruktur, dengan beberapa langkah dalam mengelompokkan informasi untuk rencana uji keamanan, penilaian, dan laporan domain yang terverifikasi dan teranalisis. Ada empat *tools* yang digunakan dalam *framework* ini yaitu *WhoIs, SSL Scan, Nmap,* dan *OWASP Zap*. Penelitian [16] dilakukan dengan judul Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP Zap di Universitas Duta Bangsa Surakarta. Penelitian ini bertujuan untuk menemukan kelemahan pada sistem dan memperbaikinya. Refernsi [17] melakukan Analisis Keamanan Sistem Informasi Berbasis Website dengan Metode OWASP. Penelitian ini bertujuan untuk mendeteksi tingkat kerentanan pada Sistem informasi berbasis website. Referensi [18] Pengujian Celah Keamanan Website Menggunakan Teknik *Penetration Testing* dan Metode OWASP Pada *Website* SIM. Tujuannya untuk mengetahui apakah SIM *(Security Information Management)* memiliki celah kemanan atau tidak. Referensi [19] Analisis Keamanan *Website* Menggunakan Teknik *Footprinting* dan *Vulnerability Scanning*. Penelitian ini bertujuan untuk menganalisis keamanan pada *website* menggunakan *tools WhoIs, SSL Scan, Nmap, OWASP Zap* dengan metode OWASP. *Tools* yang dipakai dapat menemukan celah keamanan seperti *Injection, Broken authentication and session management,* Serangan XSS, *Insecure direct object references, Security misconfiguration, Sensitive data exposure, Missing function level access control, Cross-site request forgery (CSRF), Using Components with known vulnerabilities, Unvalidated redirects and forwards* [20]. Dari jenis serangan tersebut beberapa alasan seseorang untuk meretas adalah karena kesenangan, keuntungan dengan memeras korban dan menguji keamanan sistem, bisa juga karena ingin mendapatkan pengakuan. Kegiatan *hacking* memiliki banyak motivasi dan tujuan, baik positif maupun negatif. Peretas dapat mengeksploitasi kerentanan yang ada untuk mengeksploitasi di *internet* [21]. Salah satu bentuk serangan pada website menurut OWASP, kerentanan injeksi masih merupakan kerentanan paling umum dalam aplikasi *web* [22]. *SQL Injection* mewakili kerentanan yang memungkinkan penyerang memengaruhi kueri *SQL* yang dikirim ke database melalui aplikasi [23]. Salah satu cara untuk mencegah serangan pada *server web* adalah dengan menggunakan *firewall* (simulasi keamanan) baik dalam bentuk *software* maupun *hardware*. Secara garis besar, sistem ini menangani permintaan dari pengguna dan membedakan antara pengguna klien dan pengguna penyerang yang mengakses situs *web* di *server web* [24] dengan menggunakan istem pertahanan ini diharapkan dapat memberikan rekomendasi untuk peningkatan keamanan aplikasi web juga menjaga integritas data pada aplikasi tersebut [25]. Penelitian selanjutnya dapat melakukan dengan tahapan yang lebih spesifik menggunakan metode OWASP maupun metode yang berbeda dengan tahapan *penetration testing* untuk mendaptkan celah keamanan sesuai laporan identifikasi kerentanan menggunakan *tools OWASP Zap, Security Scan, maupun Acunetix Vulnerability Scanner*.

2. METODOLOGI PENELITIAN

Pada penelitian ini metode yang digunakan adalah OWASP sebagai metode yang berfokus untuk memperbaiki keamanan pada *software*. OWASP merupakan aplikasi *open soutce* yang siapapun bisa menggunakannya. Diperlukan alur penelitian untuk memenuhi tonggak yang diperlukan saat menulis penelitian ini [3]. Alur penelitian ini dapat dilihat pada Gambar 3.



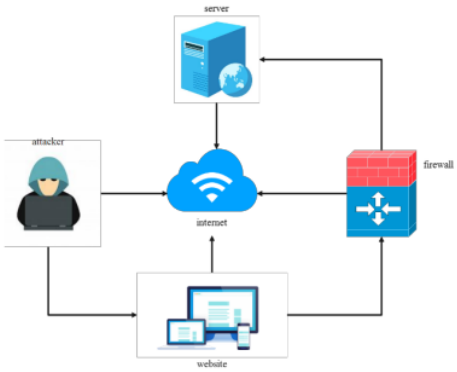
Gambar 3. Alur pada analisis OWASP *Framework*

1. Pengumpulan Data
   Pada langkah ini, mengumpulkan informasi tentang topik yang dipilih dan menyelesaikan survei.
2. Pengujian penetration testing
   Pada fase ini pengujian dijalankan pada *website*, ada empat fase dalam proses pengujian ini: *Information Gathering, Network Mapping, Exploiting,* dan *Reporting*.
3. Analisis
   Pada tahap ini, melakukan analisis pada *website* untuk menemukan kerentanan.
4. Pelaporan
   Pada tahap ini menguraikan secara detil hasil dari analisis yang telah diproses dan dimasukkan ke dalam laporan.

Pada Gambar 4. menunjukkan diagram skenario pada pengujian *website* menggunakan *tools* OWASP Zap.

Submitted: **28/04/2022**; Accepted: **24/06/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1468-1475
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.4099



Gambar 4. Skenario OWASP

Pada Gambar 4 menunjukkan skenario serangan pada penelitian ini. *Attacker* yang terhubung dalam sebuah jaringan *internet* mencoba mencari kerentanan pada *website* dengan menggunakan *tools* OWASP Zap. Kemudian *attacker* akan mendapatkan kerentanan pada *website* yang tidak terlindungi oleh *firewall* dalam *web server*. Proses pengujian menggunakan OWASP *framework* setelah tahap penyelesaian dan implementasi, alat yang digunakan dan fungsionalitas alat akan dijelaskan pada Tabel 1.

Tabel 1. Tools pada OWASP *Framework*

Tahapan	Tools	Keterangan
Information Gathering	WhoIs, SSL Scan	Mencari informasi website
Network Mapping	Nmap	Scan port
Exploit	OWASP Zap	Scan Kerentanan
Report	OWASP Zap	Vulnerability

3. HASIL DAN PEMBAHASAN

Pengujian penetrasi adalah upaya yang dapat dilakukan penyedia layanan untuk mengidentifikasi kerentanan, bertindak seperti peretas yang mengeksploitasinya, menguji keamanan sistem, dan menetapkan kontrol yang sesuai untuk mengurangi risiko [24]. Pada pengujian keamanan sistem informasi ini menggunakan *Framework* OWASP ada empat tahapan sebagai berikut:

3.1 Information Gathering

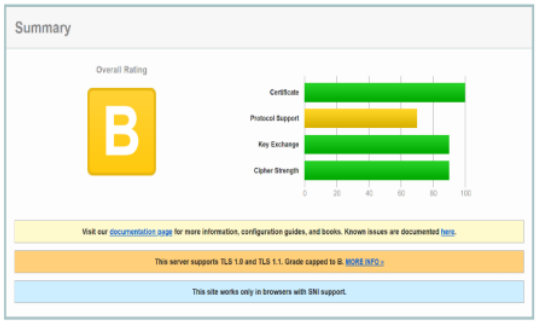
Pada tahap ini dilakukan pencarian informasi tentang *website*. Hal ini mencakup pencarian informasi yang lebih dalam mengenai *website*. Pada fase ini mendapatkan informasi yang diinginkan dalam *website* menggunakan *tools WhoIs Domain* dan *SSL Scan*. Hasil informasi *website* menggunakan *tools WhoIS* dapat dilihat pada Gambar 5.

Gambar 5. Tool WhoIS

Submitted: **28/04/2022**; Accepted: **24/06/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1468-1475
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.4099

Gambar 5. merupakan hasil dari *tools WhoIS* mendapatkan informasi mengenai *website* seperti tanggal pembuatan, tanggal pembaruan, tanggal kadarluasa, email registrasi, kontak registrasi, dan alamat *web hosting* yang dipakai. Gambar 6 merupakan hasil pencarian informasi menggunakan *tools SSL (Secure Socket Layer) Scan*

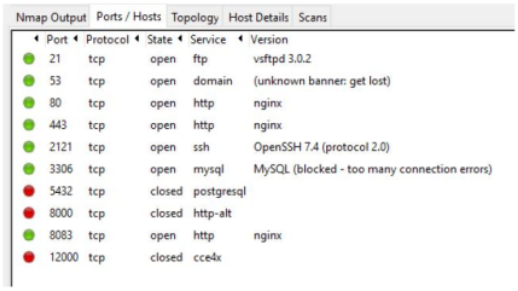


Gambar 6. Hasil *tools* SSL Scan

Gambar 6. menggunakan *tools* SSL *Scan* menemukan bahwa situs *web* tujuan sudah menggunakan protokol keamanan peringkat B SSL tetapi ada juga masalah yang perlu diperbaiki yaitu protokol dukungan dari server yang menggunakan versi yang lebih lama yaitu TLS 1.0 dan TLS 1.1

3.2 Network Mapping

Network Maping adalah tahap pemetaan dalam jaringan *web* yaitu untuk melakukan *scan ports/host* jaringan menggunakan *tools Nmap* dengan hasil dapat dilihat pada Gambar 7.



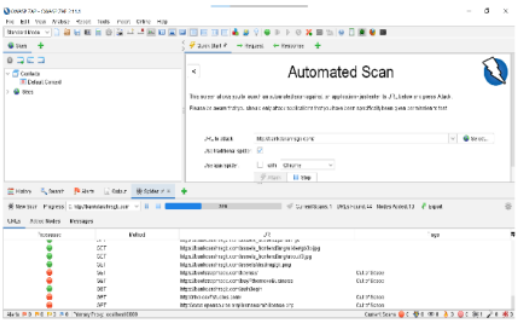
Port	Protocol	State	Service	Version
21	tcp	open	ftp	vsftpd 3.0.2
53	tcp	open	domain	(unknown banner: get lost)
80	tcp	open	http	nginx
443	tcp	open	http	nginx
2121	tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)
3306	tcp	open	mysql	MySQL (blocked - too many connection errors)
5432	tcp	closed	postgresql	
8000	tcp	closed	http-alt	
8083	tcp	open	http	nginx
12000	tcp	closed	cce4x	

Gambar 7. Hasil *tools* Nmap

Pengujian menggunakan *tools* Nmap didapakan tujuh *port* yang berstatus *open* yakni pada port 21, 53, 80, 443, 2121, 3306, dan 8083 dengan protocol TCP (*Transmission Control Protocol*) dan tiga port yang berstatus closed yakni 5432, 8000, dan 1200.

3.3 Exploit

Tahap ini merupakan pengujian celah keamanan yang ditemukan. Informasi yang diperoleh pada tahap sebelumnya dapat digunakan sebagai bahan untuk melakukan pengujian celah keamanan [25]. Pada Gambar 8 dapat dilihat hasil pemindaian *(scanning)* menggunakan *tools* OWASP Zap.

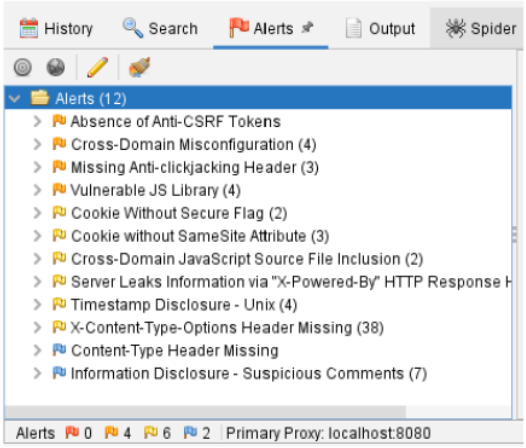


Gambar 8. Proses *scanning* menggunakan *tools* OWASP Zap

Submitted: 28/04/2022; Accepted: 24/06/2022; Published: 25/07/2022

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1468-1475
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.4099

Pada Gambar. 8 dilakukan *scanning* agar data dan informasi yang masuk bisa diketahui seberapa aman da ri aplikasi *web* serta semua risiko yang terkait dan juga untuk memukan kerentanan atau ancaman yang tertanam dalam aplikasi *web*. Gambar 9. merupakan hasil dari *scanning* menggunakan *tools* OWASP Zap



Gambar 9. Hasil *scanning* menggunakan *tools* OWASP Zap

Gambar 9. merupakan hasil *scanning* dari *tools* OWASP Zap dengan jumlah kerentan sebnayak 12, empat dengan level *medium*, enam dengan level *low* dan 2 dengan level *informational*. Dalam *scanning* ini tidak terdapat kerentanan dengan level *high* sehingga *website* masih tergolong aman, meskipun ada beberapa yang harus diperbaiki pada level *medium*. Hasil ringkasan dan laporan terperinci dari pencarian kerentanan dapat dilihat pada Tabel 2.

Tabel 2. Rekapitulasi kerentanan yang ditemukan

Risk Level	Number of Alerts
High	0
Medium	4
Low	6
Informational	2

Berdasarkan Tabel 2. yang digambarkan dalam bentuk presentase yaitu pada *risk level* kerentatan pada level *high* mendapatkan nilai 0% atau tidak ditemukan kerentananan apapun didalamnya, pada level *medium* mendapatkan nila 33,3% (4) kerentanan yaitu: *Absence of Anti-CSRF Tokens, Cross-Domain Misconfiguration, Missing Anti-clickjacking Header,* dan *Vulnerable JS Library*, pada pada level *low* mendapatkan nilai 50% (6) kerentanan yaitu: *Cookie Without Secure Flag, Cookie without SameSite Attribute, Cross-Domain JavaScript Source File Inclusion, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Timestamp Disclosure – Unix,* dan *X-Content-Type-Options Header Missing*, dan pada level *informational* mendapatkan nilai 16,7% (2) kerentanan yaitu: *Content-Type Header Missing* dan *Information Disclosure - Suspicious Comments*. Dari kerentanan yang didapatkan tersebut *website* masih bisa di kategori aman dengan tingkat kerentanan pada level *medium*.

3.4 Reporting

Pada tahap ini dilakukan pelaporan mengenai beberapa celah keamanan yang di dapatkan dari *website*. Hasil pengujian celah keamanan menggunakan OWASP Zap ditemukan beberapa kerenatan pada *website*. Top 10 OWASP dapat dilihat pada Tabel 3.

Tabel 3. Kerentanan Berdasrkan Top 10 OWASP 2021

Kerentanan	Solusi
A01:2021-Broken Accsess Control	Melakukan implementasi kerja sistem akses kontrol dan digunakan kembali pada seluruh aplikasi sehingga meminimalisir pengguna CORS *(Cross Origin Resource Sharing)*, agar user

Submitted: **28/04/2022**; Accepted: **24/06/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1468-1475
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.4099

Kerentanan	Solusi
	tidak dapat melakukan *create, read, update*, atau *delete record* secara bebas, model akses kontrol seharusnya membatasi hal tersebut dengan menggunakan *ownership* untuk tiap *record*, dan menonaktifkan direktori listing *web server*.
A05:2021-Security Misconfiguration	Pengelolah sistem dapat meninjau dan memperbarui konfigurasi yang sesuai untuk ke semua *security notes*, *updates* dan *patches* sebagai bagian dari proses *patch management*
A08:2021-Software and Data Integrity Failures	Gunakan tanda tangan digital atau mekanisme yang sama untuk memverifikasi bahwa perangkat lunak atau data berasal dari sumber yang diharapkan dan tidak dimanipulasi
A09:2021-Security Logging and Monitoring Failures	Sistem memberikan kontrol akses pada menu login untuk autentikasi terhadap pengguna

Pada Tabel 3. Hasil kerentanan pengujian sistem menggunakan *tools OWASP Zap* ditemukan empat kerentanan yang harus diperbaiki yaitu A01- *Broken Accsess Control*, A05-*Security Misconfiguration*, A08- *Software and Data Integrity Failures*, dan A09-*Security Logging and Monitoring Failures*.

4. KESIMPULAN

Berdasarkan hasil proses penelitian pada *website https://bankdarahrsgb.com/* menggunakan metode OWASP maka ditemukan hasil kerentanan dengan level medium. *OWASP Zap* mendapatkan 12 hasil kerentanan dengan empat pada kerentanan level *medium*, enam pada level *low* dan dua pada level *informational*. Hasil penelitian yang dicapai sesuai dengan tujuan penelitian yang diharapkan. Dari empat tahap dalam pengujian dengan menggunakan tiga *tools*. *Website* masih memiliki tingkat kerentanan yang tergolong cukup aman dari serangan *hacker*. Tetapi ada beberapa yang harus diperbaiki pada kerentanan A01-*Broken Access Control*, A05- *Security Misconfiguration*, A08- *Software and Data Integrity Failures*, dan A09- *Jquery* dengan versi 1.12.4 yang digunakan rentan diserang oleh *hacker*.

REFERENCES

[1] I. A. Huda, "Perkembangan Teknologi Informasi Dan Komunikasi (Tik) Terhadap Kualitas Pembelajaran Di Sekolah Dasar," *J. Pendidik. dan Konseling*, vol. 2, no. 1, pp. 121–125, 2020, doi: 10.31004/jpdk.v1i2.622.
[2] A. L. Weol, A. Wibowo, L. P. Dewi, and K. Kunci, "Analisa Manajemen Risiko Pada Perusahaan Real Estate X."
[3] S. Eko Prasetyo and N. Hassanah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf," *J. Ilm. Inform.*, vol. 9, no. 02, pp. 82–86, 2021, doi: 10.33884/jif.v9i02.3758.
[4] B. Tasya and K. Dewi, "Kajian Literatur : Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web," 2021.
[5] V. B. Kusnandar, "Pengguna Internet Indonesia Peringkat ke-3 Terbanyak di Asia," *Databooks.id*, p. 2021, 2021, [Online]. Available: https://databoks.katadata.co.id/datapublish/2021/10/14/pengguna-internet-indonesia-peringkat-ke-3-terbanyak-di-asia.
[6] G. Guntoro, L. Costaner, and M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, 2020, doi: 10.29100/jipi.v5i1.1565.
[7] T. A. Hanafi, C. Iswahyudi, P. S. Informatika, and F. T. Industri, "Jurnal SCRIPT Vol . 7 No . 2 Desember 2019 Aplikasi Pendeteksi Celah Keamanan Aplikasi Web Dengan Penetration Testing Menggunakan Metode Input Validation Jurnal SCRIPT Vol . 7 No . 2 Desember 2019 E- ISSN : 2338-6313," vol. 7, no. 2, pp. 132–141, 2019.
[8] H. O. L. Wijaya, "Implementasi Metode Pieces Pada Analisis Website Kantor Penanaman Modal Kota Lubuklinggau," *JUSIM (Jurnal Sist. Inf. Musirawas)*, vol. 3, no. 1, pp. 46–55, 2018, doi: 10.32767/jusim.v3i1.289.
[9] M. R. Hasan, S. Suhermanto, and S. Suharmanto, "Keamanan Sistem Perangkat Lunak dengan Secure Software Development Lifecycle," *J. Ilmu Komput. dan Bisnis*, vol. 12, no. 1, pp. 88–101, 2021, doi: 10.47927/jikb.v12i1.95.

Submitted: **28/04/2022**; Accepted: **24/06/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1468-1475
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.4099

[10] W. Agustiara, A. Pratama, S. Junaidi, K. Padang, and S. Barat, "Analisis Keamanan Protokol Secure Socket Layer Terhadap Serangan Packet Sniffing Pada Website Portal," vol. 6, no. 1, 2022.
[11] S. Nurul, S. Anggrainy, and S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review SIM)," vol. 3, no. 5, pp. 564–573, 2022.
[12] I. G. A. S. Sanjaya, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *J. Ilm. Merpati*, vol. 8, no. 2, pp. 113–124, 2020.
[13] R. Umar, I. Riadi, and E. Handoyo, "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)," *J. Sist. Inf. Bisnis*, vol. 9, no. 1, p. 47, 2019, doi: 10.21456/vol9iss1pp47-54.
[14] dan S. A. M. Agus Rochman, Rizal Rohian Salam, "Analisis Keamanan Website Dengan Information System Security Assessment Framework (ISSAF) Dan Open Web Application Security Project (OWASP) Di Rumah Sakit XYZ," vol. 2, no. 4, pp. 506–519, 2021.
[15] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 6, no. 2, p. 185, 2021, doi: 10.24114/cess.v6i2.24777.
[16] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *J. Komtika (Komputasi dan Inform.*, vol. 5, no. 1, pp. 35–42, 2021, doi: 10.31603/komtika.v5i1.5134.
[17] A. Elanda and R. L. Buana, "Analisis Keamanan Sistem Informasi Berbasis Website Dengan Metode Open Web Application Security Project (OWASP) Versi 4: Systematic Review," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 5, no. 2, p. 185, 2020, doi: 10.24114/cess.v5i2.17149.
[18] J. J. B. H. Yum Thurfah Afifa Rosaliah, "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM," *Senamika*, vol. 2, no. September, pp. 752–761, 2021.
[19] I. Journal, E. I. Alwi, and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," vol. 5, no. 2, pp. 43–48, 2020.
[20] I. Riadi, A. Yudhana, and Y. W, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 4, p. 853, 2020, doi: 10.25126/jtiik.2020701928.
[21] Y. Muhyidin, M. H. Totohendarto, E. Undamayanti, and C. N. Salsabilla, "Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking Comparison of Website Security Levels Using Nmap and Nikto With Ethical Hacking Methods," pp. 1–10, 2022.
[22] Pramono, A. Sunyoto, and E. Pramono, "Deteksi Serangan SQL Injection Menggunakan Hidden Markov Model," *J. Tecnoscienza*, vol. 5, no. 2, p. 243, 2021, doi: 10.51158/tecnoscienza.v5i2.432.
[23] S. P. Sitorus and R. A. Habibi, "Teknik Pencegahan Penetrasi SQL Injeksi Dengan Pengaturan Input Type Number dan Batasan Input Pada Form Login Website," *U-NET J. Tek. Inform.*, vol. 4, no. 2, pp. 26–33, 2020, doi: 10.52332/u-net.v4i2.303.
[24] S. Rheno Widianto and I. Abdullah Azzam, "Analisis Upaya Peretasan Web Application Firewall dan Notifikasi Serangan Menggunakan Bot Telegram pada Layanan Web Server," *Elektra*, vol. 3, no. 2, pp. 19–28, 2018.
[25] R. Riska and H. Alamsyah, "Penerapan Sistem Keamanan Web Menggunakan Metode Web Aplication Firewall," *J. Amplif. J. Ilm. Bid. Tek. Elektro Dan Komput.*, vol. 11, no. 1, pp. 37–42, 2021, doi: 10.33369/jamplifier.v11i1.16683.
[26] S. U. Sunaringtyas and D. S. Prayoga, "Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada," *Edu Komputika J.*, vol. 8, no. 1, pp. 48–56, 2021.

Submitted: **28/04/2022**; Accepted: **24/06/2022**; Published: **25/07/2022**

1. HASIL CEK_60960140

ORIGINALITY REPORT

12%	11%	3%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas International Batam Student Paper	8%
2	Submitted to University of Hertfordshire Student Paper	3%

Exclude quotes	On	Exclude matches	< 3%
Exclude bibliography	On		