JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 16 No 2]
[Agustus 2022]

IMPLEMENTASI OWASP ZAP UNTUK PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK

Gregorius Hendita Artha Kusuma
Prodi Teknik Informatika, Fakultas Teknik, Universitas Pancasila, Jakarta Selatan
gregorius@univpancasila.ac.id

ARTICLE INFO

Keywords

OWASP, website, active scan, keamanan website

ABSTRACT

Information security is an important thing that must be considered for every individual and institution in order to avoid crime. Poor information systems can threaten the critical infrastructure of an organization. Problems with system security vulnerabilities or disruptions are widely scattered on the internet. Early detection of the weakness of a system is the initial solution in securing a system. Therefore we need an analysis of the vulnerability of a system that refers to the security standardization of the Open Web Application Security Project (OWASP) by performing an active scan. Website vulnerability analysis using the OWASP ZAP technique with the help of several security tools is able to determine the security level of a website based on the results of scans and tests that have been carried out where almost every test category is able to find vulnerabilities, although there are several categories that do not have vulnerabilities. The purpose of this study is to identify the vulnerabilities contained in the University Academic Information System website and conduct testing and analysis to determine the condition of the vulnerability of the University Academic Information System website using the Open Web Application Security Project (OWASP). The research method used as a website security parameter is OWASP Top-10 2021.

I. LATAR BELAKANG

Statistik Pengguna Internet di Indonesia Berdasarkan hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada Tahun 2016. Jumlah pengguna internet telah mencapai 132,7 juta orang dari total penduduk Indonesia sebanyak 256,2 juta orang. Hal ini menunjukkan bahwa lebih dari 50% penduduk Indonesia kini telah terhubung dengan internet. Penetrasi internet mayoritas masih berada di Pulau Jawa, yaitu sekitar 65% dari total pengguna. Pengguna internet berdasarkan usia, mayoritas didominasi oleh pengguna yang berada pada rentang usia 35-44 tahun, yaitu sebesar 29,2%. Berdasarkan usia justru didominasi oleh pengguna yang berusia antara 25-34 tahun, yaitu sebesar 75,8%.

Penggunaan internet yang semakin mudah menimbulkan dampak positif dan negatif tergantung pada pemanfaatannya. ibarat pedang dengan dua sisi mata yang sama tajam jika penggunaanya benar maka akan menghasilkan informasi yang baik akan tetapi, sebaliknya jika penggunaanya salah maka akan mampu melukai diri sendiri. Informasi yang dihasilkan dari internet merupakan informasi yang menyeluruh, sebagai akibat dari

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 16 No 2]
[Agustus 2022]

meluasnya informasi ini banyak perusahaan maupun instansi berlombalomba membangun sistem informasi guna meningkatkan produktifitasnya.

Pembuatan sistem informasi dapat meningkatkan mutu dan kualitas suatu organisasi. Pentingnya nilai informasi menyebabkan informasi yang dihasilkan dari sistem harus dibatasi pengaksesan oleh orang-orang tertentu agar nilai informasi yang disampaikan terjaga integritasnya. Jatuhnya informasi ke pihak lain yang tidak berwenang dapat menimbulkan kerugian bagi organisasi sehingga sistem yang dibuat harus mampu menanggulangi dari tindakan-tindakan yang tidak diinginkan.

Keamanan informasi merupakan hal yang harus diperhatikan bagi setiap instansi agar terhindar dari gangguan atau tindakan kejahatan. Masalah keamanan atau gangguan banyak bertebaran di internet, gangguan tersebut bisa berupa serangan Malware, Eksploitasi, Injeksi database dan lain sebagainya. Badan pengawas lalu lintas internet meyimpulkan bahwa pada tahun 2016 sekitar 90% kejahatan internet dilakukan dengan menyerang aplikasi web dengan yang paling populer adalah dengan cara menginjeksi database yang mencapai 47.06 % total serangan yang popular. Pemahaman dan kesadaran yang kurang terhadap isu keamanan sistem selalu mengancam setiap saat khususnya bagi para pengembang. Kebocoran data atau perusakan dapat mengancam setiap saat seiring dengan meningkatnya sumber daya manusia. Solusi pengamanan web dari gangguan atau serangan hacker dapat dilakukan dengan cara self test yaitu pengujian yang dilakukan terhadap web server secara legal dengan aktifitas menyerupai hacker. Self test dapat dilakukan dengan beberapa metode penetration testing salah satunya adalah Information Systems Security Assessment Framework (ISSAF), Open Web Application Security Project (OWASP) versi 4 dan Open Source Security Testing Methodology Manual (OSSTMM).

OWASP versi 4 merupakan peningkatan pada versi sebelumnya. Adapun 3 kelebihan versi 4 dibanding versi 3 yaitu: versi panduan pengujian terintegrasi dengan produk dokumen, semua bab telah ditingkatkan dan uji kasus diperluas, mendorong penguji keamanan untuk mengintegrasikan penguji perangkat lunak yang lainnya. Metode OWASP bersifat terbuka dan kolaboratif, metode ini didasarkan pada pendekatan Black Box Testing dimana penguji sangat minim sekali informasi pada aplikasi yang akan diuji. Sebagai suatu metode pengamanan aplikasi. OWASP menggunakan 11 kategori pendekatan pengujian yang melibatkan analisis aktif dari aplikasi untuk setiap kelemahan. OWASP Menggunakan tools vulnerability scanner dengan kolaborasi beberapa tools security project dalam mencari celah keamanan, kemudian melakukan pengujian pada beberapa kategori untuk mengetahui keamanan suatu aplikasi.

II. STUDI PUSTAKA

2.1. Website

Website adalah kumpulan halaman dalam suatu domain yang memuat tentang berbagai informasi agar dapat dibaca dan dilihat oleh pengguna internet melalui sebuah mesin pencari. Informasi yang dapat dimuat dalam sebuah *website* umumnya berisi mengenai konten gambar, ilustrasi, video, dan teks untuk berbagai macam kepentingan.

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 16 No 2]
[Agustus 2022]

Biasanya untuk tampilan awal sebuah website dapat diakses melalui halaman utama (*homepage*) menggunakan browser dengan menuliskan URL yang tepat. Di dalam sebuah *homepage*, juga memuat beberapa halaman *web* turunan yang saling terhubung satu dengan yang lain.

2.2. OWASP ZAP

Zed Attack Proxy (ZAP) adalah aplikasi untuk melakukan pentest untuk menemukan vulnerabilities dalam suatu *web applications* dengan cara mudah, ZAP menyediakan scanner automatis sebaik bila kita menggunakan *tool* untuk menemukan *vulnerabilities* secara manual. Ketika digunakan sebagai *server proxy*, ini memungkinkan pengguna untuk memanipulasi semua lalu lintas yang melewatinya, termasuk lalu lintas menggunakan https, itu juga dapat berjalan dalam mode daemon yang kemudian dikontrol melalui REST API. ZAP telah ditambahkan ke dalam Radar Teknologi ThoughtWorks pada 30 Mei 2015 di cincin Percobaan. ZAP awalnya bercabang dari Paros, *proxy* pentesting lainnya. Simon Bennetts, pemimpin proyek, menyatakan pada tahun 2014 bahwa hanya 20% dari kode sumber ZAP masih dari Paros.

III. METODOLOGI

3.1. Teknik Pengumpulan Data/Informasi

- Studi Literatur

Teknik ini dilakukan dengan tujuan pencarian masalah apa yang masih bisa dilakukan dan pendalaman materi lebih lanjut dengan mencari tahu metode apa yang telah digunakan serta kelebihan dan kekurangan dari masing-masing metode. Sehingga diperoleh metode yang diusulkan untuk mengetahui apakah efektif juga digunakan untuk permasalahan yang diambil pada penelitian ini.

3.2. Identifikasi Website

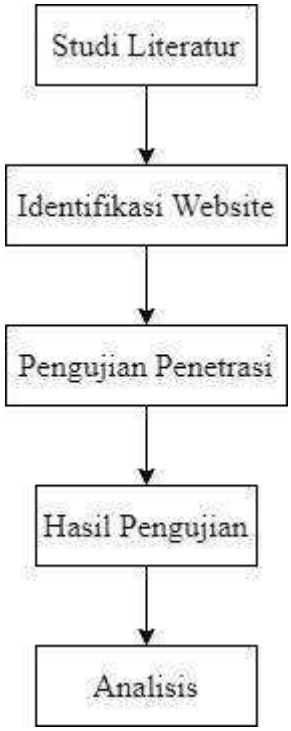
Contoh *Website* yang digunakan adalah Sistem Informasi Akademik Universitas Pancasila http://siak.univpancasila.ac.id . *Tools* yang digunakan adalah OWASP ZAP versi 2.10.0

3.3. Rancangan Penelitian

Struktur tahapan yang dilakukan peneliti untuk melakukan penelitian, dengan rancangan sebagai berikut :

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 16 No 2]
[Agustus 2022]



Gambar 1 : Diagram Alur Penelitian

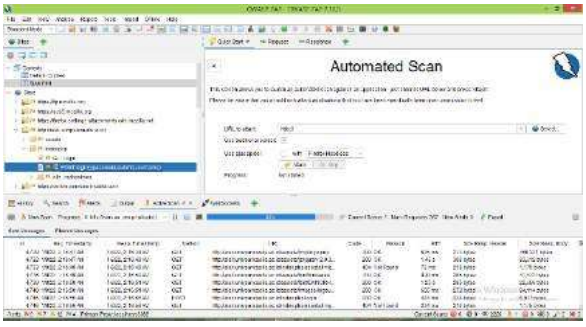
IV. HASIL DAN PEMBAHASAN

4.1. Penetrasi OWASP ZAP

Metode yang digunakan pada OWASP ZAP adalah *Active scan*, *active scan rules*, *alerts*, *Accsess control testing*, dan *passive scan rules*. Hasil scan menemukan adanya kerentanan sedang, rendah, dan informatif ,

1. HTML Form without CSRF protection termasuk dalam kerentanan : Sedang
2. Clickjacking: X-Frame-Options header missing termasuk dalam kerentanan : Rendah
3. Password type input with auto-complete enabled termasuk dalam kerentanan : Informatif

Berikut adalah hasil scan pada OWASP:



Gambar 2 : Proses Scanning

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 16 No 2]
[Agustus 2022]

Pada gambar diatas menunjukkan langkah awal dalam proses scanning menggunakan OWASP.

Gambar 3 : Hasil Scan dengan Kerentanan Sedang

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 16 No 2]
[Agustus 2022]

Gambar 4 : Hasil Scan dengan Kerentanan Rendah

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 16 No 2]
[Agustus 2022]

Berdasarkan Hasil Pengujian OWASP ZAP memiliki 19 kerentanan yaitu, :

1. Application Error Disclosure
2. CSP: Wildcard Directive
3. CSP: script-src unsafe-inline
4. CSP: style-src unsafe-inline
5. Cross-Domain Misconfiguration
6. Vulnerable JS Library
7. X-Frame-Options Header Not Set
8. Absence of Anti-CSRF Tokens
9. CSP: Notices
10. Cookie No HttpOnly Flag
11. Cookie with SameSite Attribute None
12. Cookie without SameSite Attribute
13. Cross-Domain JavaScript Source File Inclusion
14. Incomplete or No Cache-control Header Set
15. Information Disclosure - Debug Error Messages
16. Private IP Disclosure
17. Secure Pages Include Mixed Content
18. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
19. X-Content-Type-Options Header Missing

4.2. Penetrasi OWASP ZAP Berdasarkan OWASP TOP 10

Berdasarkan hasil pengujian OWASP memiliki 19 kerentanan. Dari 19 kerentanan tersebut ada yang termasuk ke dalam daftar OWASP TOP 10. Berikut hasil pengujian OWASP ZAP berdasarkan OWASP TOP 10:

Tabel 1 : Hasil Pengujian OWASP ZAP TOP 10

OWASP TOP 10	Kerentanan
A1 Broken Access Control	Sedang
A2 Cryptographic Failure	Tidak Rentan
A3 Injection	Tidak Rentan
A4 Insecure Design	Tidak Rentan
A5 Security Misconfiguration	Sedang
A6 Vulnerable and Outdated Components	Rendah
A7 Identification and Authentication Failure	Tidak Rentan
A8 Software and Data Integrity Failures	Rendah
A9 Security Logging and Monitoring Failure	Tidak Rentan

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 16 No 2]
[Agustus 2022]

A10 Server-Side Request Forgery		Tidak Rentan

Berdasarkan Tabel 1 Hasil Pengujian OWASP terdapat kerentanan di A1 Broken Access Control memiliki tingkat kerentanan sedang, A5 Security Misconfiguration memiliki tingkat kerentanan Sedang, A6 Vulnerable and Outdated Components memiliki kerentanan rendah, A8 Software and Data Integrity Failures memiliki tingkat kerentanan rendah.

IV. KESIMPULAN

Berdasarkan pengujian menggunakan OWASP ZAP versi 2.10.0 menunjukkan bahwa website Sistem Informasi Akademik Universitas Pancasila memiliki 19 kerentanan dan berdasarkan OWASP TOP 10 terdeteksi memiliki 4 kerentanan yaitu Broken Access Control, Security Misconfiguration, Vulnerable and Outdated Components, dan Software and Data Integrity Failures maka dengan dilakukannya pengujian penetration test kualitas website Sistem Informasi Akademik Universitas Pancasila berada di tingkat sedang sehingga perlu dilakukan perbaikan lebih lanjut oleh pihak pengembang Sistem Informasi Akademik Universitas Pancasila.

DAFTAR PUSTAKA

[1] Nigel Cunong,Dennis., Saputra, Muhardi., Puspitasari, Warih. (2020). Analisis Resiko Keamanan Terhadap Website Dinas Penanaman Modan dan Pelayanan Terpadu Satu Pintu Pemerintahan XYZYZ Menggunakan Standar Penetration Testing Execution Standard (PTES). e-Proceeding of Engineering, 7(1), 2090-2095.

[2] Hidayatulloh, Syarif., Saptadiaji, Desky. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). Jurnal Algoritma, 19(1), 77-86.

[3] Mayasari, Rini., Ali Ridha, Azhari., Juardi, Didi., Ahmad Baihaqi, Kiki. (2020). Analisis Vulnerability pada Website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability. SYSTEMATICS, 2(1), 33-38.

[4] Wibowo1, Feri., Harjono., Purwo Wicaksono, Agung,. Harjono. (2019). Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS. Jurnal Informatika, 6(2), 212-218.

[5] Elanda, Anggi., Lintang Buana. (2020). Analisis Sistem Keamanan Sistem Informasi Berbasis Webiste Dengan Metode Open Web Application Security Project (OWASP) Versi 4: Systematic Review. Journal of Computer Engineering System and Science, 5(2), 185-191.

[6] Yudiana., Elanda, Anggi., Lintang Buana, Robby. (2021) Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP TOP 10. Journal of Computer Engineering System and Science. 6(2), 185-191.

[7] Yulianingsih. Melindungi Aplikasi dari Serangan CrossSite Scripting (XSS) Dengan Metode Metacharacter. TEKNOSI, 3(1), 83-88.

[8] Kurniawan, A. (2020). Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi Host-Based. Jurnal Telematika, 14(1), 9-18.

https://doi.org/10.47111/JTI

[E-ISSN 2656-0321]
[Vol 16 No 2]
[Agustus 2022]

[9] Riadi, I., Rusydi Umar, R., & Lestari, T. (2020). Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP. Jurnal Informatika Sunan Kalijaga, 5(3), 146–152.

[10] Putra, Y., Yunus2, Y., & Sumijan. (2021). Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) Terhadap Seragan Cross Site Scripting. Jurnal Sistem Informasi dan Teknologi, 3(2), 56-63.

https://doi.org/10.47111/JTI