Jurnal Ilmiah Wahana Pendidikan, Agustus 2022, 8 (12), 327-334
DOI: https://doi.org/10.5281/zenodo.6945632
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Blackbox Testing Sistem Informasi Absensi Pegawai Karawang Dengan Metode *Top 10 Owasp Attack*

Rona Febriana

Universitas Singaperbangsa Karawang

Received: 14 Juli 2022
Revised: 17 Juli 2022
Accepted: 20 Juli 2022

Abstract

Website-based applications have recently been widely used by the public. As a result, there are more and more data leaks in several website-based applications. In 2021 alone, there have been several cases, such as BPJS Kesehatan which experienced a population data leak of 279 million. Data leaks can occur due to various factors such as Human Error or lack of knowledge of company staff on data privacy. Then another factor is malicious software or what we usually call malware. A software that is inserted into the system to damage and steal important data. Entering malware into the system is very difficult if done manually, therefore usually this malware is entered through the internet network. In this study, the methodology used is Penetration Testing from OWASP with a specific method, namely Penetration Testing Execution Standard (PTES) which was adapted from a group of information security practitioners. After conducting tests to find vulnerabilities in the Employee Attendance Information System using the OWASP TOP 10 (2021) method, 3 categories of vulnerabilities were found, namely Identification and Authentication Failures with medium severity, Insecure Design with low severity, and Security Misconfiguration with critical severity. It is recommended that in the future attack techniques are carried out other than using available applications/tools (open source/official tools), namely social engineering, email spamming, etc.

Keywords: *Website, Malware, Pentetration Testing, OWASP, Social Engineering*
(*) Corresponding Author: rona62@gmail.com

How to Cite: Febriana, R. (2022). Blackbox Testing Sistem Informasi Absensi Pegawai Karawang Dengan Metode Top 10 Owasp Attack. *Jurnal Ilmiah Wahana Pendidikan, 8*(12), 327-334. https://doi.org/10.5281/zenodo.6945632

PENDAHULUAN

Aplikasi berbasis website belakangan banyak digunakan untuk berbagai hal seperti pendaftaran vaksin, pengecekan sertifikat vaksin, dan masih banyak lagi. Masyarakat cenderung memilih aplikasi berbasis website dibanding mobile karena pengguna tidak perlu melakukan instalasi aplikasi pada device mereka, cukup mengakses URL atau domain dari website tersebut.

Website biasanya banyak menyimpan data pengguna yang nantinya bisa diolah untuk keperluan Data Science, Statistik, dan laporan. Data ini biasanya hasil dari pendaftaran pengguna pada website tersebut ataupun dari tempat lain yang aplikasinya saling berhubungan. Terdapat beberapa website yang tidak mengharuskan penggunanya untuk melakukan pendaftaran. Namun terdapat juga beberapa website yang mengharuskan penggunanya daftar terlebih dahulu untuk menggunakan fitur-fitur yang tersedia di dalamnya.

Data pengguna yang tersimpan di database website tentunya harus dijaga dengan sebaik-baiknya oleh pengembang aplikasi tersebut. Semakin banyak data penting di website tersebut, maka semakin banyak juga ancaman penyerangan dari orang yang tidak bertanggung jawab. Penyerang atau biasa kita sebut hacker blackhat bisa dengan segala upaya untuk mencuri data privasi milik pengguna.

Belakangan ini marak terjadi kebocoran data pada beberapa aplikasi berbasis website. Pada tahun 2021 saja sudah terjadi beberapa kasus seperti BPJS kesehatan yang mengalami kebocoran data penduduk sebanyak 279 juta, yang didalamnya berisi informasi seperti NIK, nama, alamat, nomor telepon, dan email. Lalu BRI life juga mengalami kebocoran data nasabah sebesar 250 gigabyte dan dijual di situs gelap seharga Rp. 101,5 juta. Dan belum lama ini pada tahun 2022 terjadi kebocoran data pasien Kemenkes sebanyak 6 juta orang yang didalamnya terdapat beberapa informasi seperti hasil pemeriksaan radiologi, hasil CT Scan, Tes Covid-19, hingga hasil rontgen (X-ray).

Masih banyak lagi kasus kebocoran data di Indonesia selain yang disebutkan diatas, bahkan menurut Kominfo pada tahun 2021 saja terjadi 43 kasus kebocoran data pribadi. Hal ini seharusnya mendapat perhatian khusus dari pemerintah maupun perusahaan yang mengalami kebocoran data untuk meningkatkan keamanan website ataupun aplikasi yang dibuat. Karena kasus kebocoran data seperti ini sangat merugikan banyak pihak. Contoh dampak buruk bagi pembuat website ataupun perusahaan yang mengalami kebocoran data adalah hilangnya kepercayaan publik, reputasi turun, tuntutan hukum, ataupun denda. Sedangkan dampak buruk bagi pengguna yang datanya bocor adalah data tersebut dapat disalahgunakan oleh orang yang tidak bertanggung jawab untuk pinjaman online, ataupun penipuan.

Kebocoran data bisa terjadi karena berbagai faktor, pertama adalah Human Error atau kurangnya pengetahuan staf perusahaan terhadap data privasi maupun data yang dilindungi. Umumnya human error terjadi dengan kondisi staf tidak mengetahui bahwa dirinya dieksploitasi atau dimanfaatkan oleh penyerang. Seperti menjebak staf untuk menginputkan kredensial untuk login ke sistem perusahaan dengan metode social engineering, phising, bahkan clickhijacking. Link jebakan atau phising biasanya akan dikirim melalui media sosial, no handphone, dan juga email staf perusahaan tersebut. Berharap nantinya staf akan mengetuk link tersebut dan melihat halaman login palsu.

Faktor kedua yang menjadi penyebab kebocoran data adalah malicious software atau yang biasa kita sebut malware. Sebuah perangkat lunak yang dimasukan kedalam sistem untuk merusak dan mencuri data-data penting. Memasukan malware ke dalam sistem sangatlah sulit jika dilakukan secara manual, oleh karena itu biasanya malware ini dimasukan melalui jaringan internet. Selain itu, ketidakhati-hatian staf dalam menginstal aplikasi juga bisa menjadi malware masuk ke dalam sistem. Contohnya ketika staf menginstal aplikasi yang tidak jelas sumbernya darimana, bisa jadi didalamnya terdapat malware yang sangat berbahaya dan berdampak buruk untuk sistem. Malware sendiri berbeda dengan trojan ataupun virus, dari kemampuannya, malware biasanya lebih powerfull dibanding trojan dan virus. Trojan biasanya dirancang untuk mencuri informasi penting pada log komputer, sedangkan virus biasanya dirancang untuk merusak dan bahkan menghapus data-data di sebuah komputer.

Faktor selanjutnya yang menjadi penyebab kebocoran data adalah lemahnya sistem keamanan website perusahaan tersebut. Untuk masuk ke dalam server atau database website, seorang Attacker dapat melakukan serangan atau penetration testing dengan tujuan mendapatkan akses ilegal. Suatu website dapat dikatakan lemah jika memiliki celah keamanan atau vulnerabilities yang dapat dieksploitasi attacker. Untuk menghindari celah keamanan yang dapat dieksploitasi, website harus memiliki standar keamanan yang sudah ditentukan. Ada banyak standar keamanan yang bisa menjadi referensi, salah satunya adalah Open Web Application Security Project atau biasa kita sebut OWASP. Awalnya OWASP adalah sebuah organisasi yang fokus untuk keamanan website. Namun seiring berjalannya waktu, OWASP menjadi standar keamanan website yang sering digunakan.

Menurut OWASP 2021, terdapat 10 celah keamanan web yang perlu ditutupi oleh developer untuk menghindari attacker mengeksploitasi kerentanan tersebut. 10 Celah keamanan tersebut adalah Broken Access Control, Sensitive Data Exposure/Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, dan Server-Side Request Forgery (SSRF). Top 10 OWASP Attack biasanya akan diperbarui secara rutin oleh pakar keamanan website di seluruh dunia. Namun bukan berarti website 100% aman jika tidak terdapat 10 celah keamanan tersebut, karena tidak ada sebuah sistem yang benar-benar aman. Sebuah celah keamanan akan terus ada seiring berjalannya perkembangan teknologi. Tugas dari seorang Cyber Security untuk mengikuti trend serangan baru tersebut.

METODOLOGI PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah Penetration Testing dari OWASP dengan metode spesifiknya yaitu Penetration Testing Execution Standard (PTES) yang diadaptasi dari sekelompok praktisi keamanan informasi (Pentest-Standard Organization), dengan melakukan serangan dan melakukan analisa untuk mendapatkan suatu data dalam hasil berupa suatu bug atau celah yang terdapat pada website.

Penetration Testing Execution Standard (PTES) memiliki 7 tahap, akan tetapi penulis menggunakan 6 tahapan untuk mengetahui kerentanan yang ada pada website, tahapan yang sengaja tidak dipakai yaitu threat modeling nantiya bisa masuk pada proses Vulnerability Analysis.

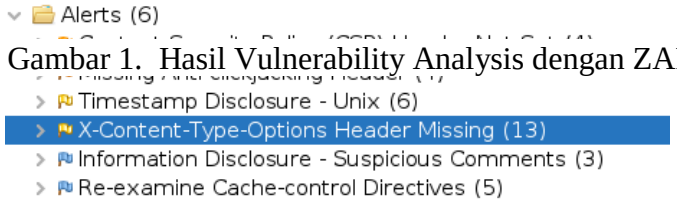
HASIL DAN PEMBAHASAN

Adapun hasil dari scanning menggunakan Builtwith pada gambar 4.2 dan gambar 4.3 diketahui bahwa Frameworks yang digunakan adalah Nuxt.js serta Web Servers Nginx 1.17. Hasilnya sama persis seperti Wappalyzer. Dengan begitu dapat disimpulkan bahwa Sistem Informasi Absensi Pegawai (SIAP) Kabupaten Karawang menggunakan bahasa pemrograman Node.js, menggunakan web server Nginx 1.17, dan web framework Nuxt.js.

Subdomain lain pada website SIAP

Untuk mencari Subdomain pada website SIAP, dapat dilakukan teknik Subdomain Enumeration yang berfungsi untuk mencari subdomain dari website SIAP. Selain itu, dapat dilakukan juga secara manual untuk menganalisa isi konten dari website SIAP. Dalam pengujian ini tools yang digunakan adalah Sudomy, yang bisa didownload pada github di link berikut https://github.com/screetsec/Sudomy.git.

Dapat dilihat hasil subdomain enumeration dengan command "./sudomy –d siap.bkpsdm.karawangkab.go.id" pada gambar 4.4.



Gambar 1. Hasil Vulnerability Analysis dengan ZAP

Diketahui bahwa terdapat 2 subdomain pada website SIAP yaitu :

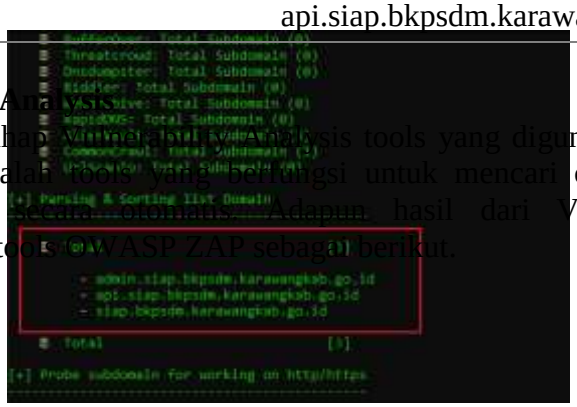
•admin.siap.bkpsdm.karawangkab.go.id

•api.siap.bkpsdm.karawangkab.go.id

Setelah melakukan proses Intelligence Gathering hasilnya dapat dibuatkan tabel agar lebih detail dan terperinci sebagai berikut :

Hasil Intelligence Gathering Sistem Informasi Absensi Pegawai Karawang

Programming Language	Node.js
Web Frameworks	Nuxt.js
Web Servers	Nginx 1.17
Subdomain	admin.siap.bkpsdm.karawangkab.go.id api.siap.bkpsdm.karawangkab.go.id



Vulnerability Analysis

Pada tahap Vulnerability Analysis tools yang digunakan adalah OWASP ZAP. ZAP adalah tools yang berfungsi untuk mencari celah keamanan pada aplikasi web secara otomatis. Adapun hasil dari Vulnerability Analysis menggunakan tools OWASP ZAP sebagai berikut.

Berdasarkan hasil scanning dari tools OWASP ZAP ditemukan 6 vulnerability pada web Sistem Informasi Absensi Pegawai Karawang. Perhitungan keparahan yang digunakan ZAP untuk menentukan severity, risk score, dan impact merujuk kepada OWASP yang memiliki metodologinya sendiri. Sedangkan untuk perhitungan tingkat keparahan yang banyak digunakan secara umum adalah CVSS V3. Agar lebih terperinci dan detail, maka dibuatkan tabel hasil Vulnerability Analysis dengan tools OWASP ZAP seperti dibawah ini.

Table 2 - Hasil Vulnerability Analysis OWASP ZAP

Vulnerability	Severity	Reference
Content Security Policy (CSP) Header Not Set	Medium	https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
Missing Anti-clickjacking Header	Medium	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
Timestamp Disclosure - Unix	Low	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
X-Content-Type-Options Header Missing	Low	https://owasp.org/www-community/Security_Headers
Information Disclosure - Suspicious Comments	Informational	-
Re-examine Cache-control Directives	Informational	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching

Exploitation

Exploitation adalah tahap dimana pentester melakukan serangan kepada target. Pada tahap exploitation ini ditemukan beberapa kerentanan dengan

kategori berdasarkan OWASP TOP 10 (2021) pada website SIAP. Ditemukan 2 kerentanan pada kategori Identification and Authentication Failures, 1 kerentanan pada kategori Insecure Design, dan 1 kerentanan pada kategori Security Misconfiguration.

A07:2021 – Identification and Authentication Failures

Berikut beberapa kerentanan dengan kategori Identification and Authentication Failures yang ditemukan pada website SIAP.

1. Improper Restriction of Excessive Authentication Attempts

Kerentanan ini terjadi karena tidak adanya pembatasan upaya otentikasi, sehingga dapat dilakukan teknik Brute Force. Brute Force adalah teknik serangan yang mencoba semua kunci yang memungkinkan secara otomatis. Tools yang digunakan untuk melakukan teknik Brute Force kali ini adalah BurpSuite.

Berdasarkan gambar diatas dapat dilihat bahwa website SIAP rentan terhadap teknik Brute Force. BurpSuite melakukan serangan percobaan Login dengan mencoba 99 kunci secara otomatis tanpa ada pembatasan upaya oleh sistem. Agar lebih detail dan terperinci terkait kerentanan ini, maka dibuatkan tabel seperti dibawah.

Tabel 3 - Vulnerability Details

Reference	**https://cwe.mitre.org/data/definitions/307.html**
Base Score	5.3 Medium

Weak Password Requirements

Kerentanan ini terjadi karena tidak adanya persyaratan dalam membuat password. Menurut National Institute of Standards and Technology (NIST), password memerlukan paling sedikit 8 karakter untuk standarnya.

KESIMPULAN

1. Berdasarkan pengujian yang dilakukan dengan mengikuti tahapan dari metode Penetration Testing Execution Standard beserta menggunakan beberapa tools open source dan beberapa referensi dari Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE) dapat disimpulkan bahwa Sistem Informasi Absensi Pegawai masih memiliki celah keamanan yang dapat dieksploitasi.
2. Setelah melakukan pengujian untuk mencari kerentanan pada Sistem Informasi Absensi Pegawai dengan metode OWASP TOP 10 (2021) ditemukan 3 kategori kerentanan yaitu Identification and Authentication Failures dengan severity medium, Insecure Design dengan severity low, dan Security Misconfiguration dengan severity critical.

DAFTAR PUSTAKA

Anggi Elanda, R. L. (2020). ANALISIS KEAMANAN SISTEM INFORMASI BERBASIS WEBSITE DENGAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) VERSI 4: SYSTEMATIC REVIEW. *CESS (Journal of Computer Engineering System and Science)* , 185-191.

Bekti. (2022, May 8). *Pengertian Website – Sejarah, Jenis, Manfaat, Unsur, Tahapan, Fungsi, Para Ahli*. Retrieved from gurupendidikan: https://www.gurupendidikan.co.id/pengertian-website/

Devi Rizky Septani, N. W. (2016). Investigasi Serangan Malware Njrat Pada PC . *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, 123.

Febiharsa, D. (2018). UJI FUNGSIONALITAS (BLACKBOX TESTING) SISTEM INFORMASI LEMBAGA SERTIFIKASI PROFESI (SILSP) BATIK DENGAN APPPERFECT WEB TEST DAN UJI BATIK DENGAN APPPERFECT WEB TEST DAN UJI . *Journal of Informatics Education*, 117-126.

Guntoro, L. C. (2020). ANALISIS KEAMANAN WEB SERVER OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING). *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 46.

I Gede Ary Suta Sanjaya, G. M. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF . *JURNAL ILMIAH MERPATI VOL. 8*, 113.

Kuncoro, A. W. (2022). *Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review*. Yogyakarta.

M. Sidi Mustaqbal, R. F. (2015). PENGUJIAN APLIKASI MENGGUNAKAN BLACK BOX TESTING BOUNDARY VALUE ANALYSIS (Studi Kasus : Aplikasi Prediksi Kelulusan SNMPTN). *Jurnal Ilmiah Teknologi Informasi Terapan*, 31-36.

OWASP. (2021). *A01:2021 – Kerusakan Akses Kontrol*. Retrieved from OWASP TOP 10:2021: https://owasp.org/Top10/id/A01_2021-Broken_Access_Control/

OWASP. (2021). *A04:2021 – Insecure Design*. Retrieved from OWASP: https://owasp.org/Top10/id/A04_2021-Insecure_Design/

RINALDY GUNAWAN, D. F. (2016). ANALISIS SERANGAN MALWARE PADA KEAMANAN JARINGAN KOMPUTER. *Institutional repositories & scientific journals*.

Technology, N. I. (2021, September 24). *NIST Password Guidelines: The New Requirements You Need to Know*. Retrieved from AUDITBOARD: https://www.auditboard.com/blog/nist-password-guidelines/

Umi Salamah, F. N. (2017). Pengujian Sistem Informasi Penjualan Undangan Pernikahan Online Berbasis Web Menggunakan Black Box Testing. *INFORMATION MANAGEMENT FOR EDUCATORS AND PROFESSIONALS*, 35-46.

Yudiana, A. E. (2021). ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10. *CESS (Journal of Computer Engineering System and Science)*, 185.

Yudiana, A. E. (2021). ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10. *CESS (Journal of Computer Engineering System and Science)*, 188.

Yuhefizar. (2022, May 8). *Pengertian Website – Sejarah, Jenis, Manfaat, Unsur, Tahapan, Fungsi, Para Ahli*. Retrieved from gurupendidikan: https://www.gurupendidikan.co.id/pengertian-website/

Organization, P.-S. (2014, Agustus 16). *Main Page : High Level Organization of the Standard*. Dipetik Juni 25, 2019, dari The Penetration Testing

Fatmawati, Irviani, R., Septiana, E., Sinthiya, I. P., & Kristina, M. (2016). Tata Kelola Teknologi Informasi Sebagai Implementassi E-Government pada Kabupaten Pemekaran untuk Meningkatkan Potensi Daerah. *Prosiding Seminar Nasional Pendidikan Teknik Informatika*, 249-257.

Nimda. (2019, Januari 1). *Keamanan Web*. Diambil kembali dari Universitas Pasundan: http://www.unpas.ac.id/keamanan-web/

Stuttard. (2012). Celah Keamanan Pada Aplikasi Website, 3. *Vulnerability Bugs*.