JURNAL SISTEM INFORMASI GALUH
Volume 3, Nomor 2, Juli 2025
(Mamay Syani, S.ST., M.Kom)
ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

Vulnerability Assessment Pada Situs XYZ Menggunakan *Web Vulnerability Scanner* Burp Suite

Mamay Syani*[1], Taufik Fajar Mustafa[2], Hafizh Maalik Falah[3], Tuti Rohayati[4], Usep Abdul Rosid[5]
*[1,2,3]Politeknik TEDC Bandung
[4]Universitas Galuh Ciamis
[5]Politeknik Negeri Subang
Email: *[1]msyani@poltektedc.ac.id, [2]tfajar321321@gmail.com, [3]hafizhmf23@gmail.com, [4]tutirohayati@unigal.ac.id, [5]usepabdulr@polsub.ac.id

Abstract

The increasing adoption of digital services by local governments demands greater attention to cybersecurity aspects. This study applies the penetration testing method using a Blue Teaming approach on XYZ, a web-based public service portal using Burp Suite tools, to identify potential security vulnerabilities. The testing follows the NIST SP 800-115 guidelines and reveals 16 vulnerabilities classified as low to medium severity. Findings indicate weaknesses such as cookies without Secure and HttpOnly attributes, the use of vulnerable JavaScript libraries, and the absence of HSTS policy. Recommendations are provided to help site administrators enhance overall system security resilience.

Keywords *: Website Security, Penetration Testing, NIST SP 800-115, Burp Suite, Government Website.*

Abstrak

Peningkatan adopsi layanan digital oleh pemerintah daerah menuntut perhatian yang lebih besar terhadap aspek keamanan siber. Penelitian ini menerapkan metode penetration testing *dengan pendekatan* Blue Teaming *terhadap situs XYZ, sebuah portal layanan publik berbasis web dengan tools Burp Suite, untuk mengidentifikasi potensi kerentanan keamanan. Pengujian dilakukan berdasarkan pedoman NIST SP 800-115 dan menghasilkan 16 temuan kerentanan yang diklasifikasikan dalam kategori keparahan rendah hingga sedang. Temuan menunjukkan adanya kelemahan konfigurasi seperti cookie tanpa atribut* Secure *dan* HttpOnly*, penggunaan pustaka JavaScript rentan, serta ketiadaan kebijakan HSTS. Rekomendasi perbaikan disusun agar pengelola situs dapat meningkatkan ketahanan keamanan sistem secara menyeluruh.*

Kata Kunci *: Keamanan Website, Penetration Testing, NIST SP 800-115, Burp Suite, Situs Pemerintah.*

I. PENDAHULUAN

Penerapan teknologi informasi dalam pelayanan publik terus berkembang, salah satunya dengan kehadiran layanan digital berbasis web yang memudahkan masyarakat dalam mengakses berbagai informasi dan layanan. Situs XYZ merupakan salah satu portal layanan pemerintah daerah yang dirancang untuk menyediakan akses digital terhadap berbagai layanan administrasi masyarakat. Dengan meningkatnya jumlah pengguna dan aktivitas di situs ini, penting bagi pengelola untuk memahami pola interaksi pengguna guna meningkatkan kualitas layanan.

Visualisasi data menjadi metode yang efektif untuk menganalisis aktivitas pengguna secara komprehensif dan

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

real-time. Dalam konteks situs XYZ, data yang bersumber dari log aktivitas pengguna dapat dianalisis untuk mengidentifikasi layanan yang paling banyak diakses, waktu kunjungan terbanyak, serta potensi masalah keamanan dan performa situs.

Penelitian-penelitian sebelumnya menunjukkan pentingnya evaluasi keamanan website layanan publik dengan metode *penetration testing* dan *vulnerability assessment*. Darojat dkk. (2022) mengkombinasikan panduan teknis dari NIST SP 800-115 dan parameter OWASP untuk menilai keamanan dua website e-government, dengan hasil yang menunjukkan adanya berbagai kerentanan konfigurasi dan keamanan aplikasi web yang perlu segera ditindaklanjuti [1]. Penelitian lain oleh Ary dkk. (2020) menerapkan kerangka kerja ISSAF untuk mengevaluasi celah keamanan pada website Lembaga X dan menemukan 18 kerentanan kritis yang dapat dimanfaatkan oleh penyerang jika tidak segera ditangani [2]. Sementara itu, Hidayatulloh dan Saptadiaji (2021) menggunakan OWASP Top 10 2017 dalam pengujian keamanan website Universitas ARS dan berhasil mengidentifikasi 13 kerentanan, meskipun sebagian besar berada pada tingkat ancaman rendah [3].

Studi-studi tersebut memperlihatkan bahwa meskipun banyak website pemerintahan dan institusi pendidikan telah beralih ke platform digital, aspek keamanannya masih menyimpan banyak celah yang berpotensi dieksploitasi. Oleh karena itu, penelitian ini berfokus pada penerapan metode *penetration testing* menggunakan *tools* Burp Suite terhadap situs XYZ sebagai studi kasus, dengan tujuan mengidentifikasi potensi kerentanan dan menyajikan hasil dalam bentuk visualisasi data interaktif untuk mendukung pengambilan keputusan teknis secara efektif.

II. METODE PENELITIAN

Penelitian ini menggunakan metode *penetration testing* (uji penetrasi) yang bertujuan untuk mengidentifikasi potensi kerentanan pada situs XYZ dengan cara mensimulasikan serangan terhadap sistem. Pendekatan ini meniru teknik dan alat yang umum digunakan oleh penyerang untuk mengevaluasi kekuatan dan kelemahan sistem dari sisi keamanan siber [4]. Proses ini menggunakan pendekatan dari NIST (National Institute of Standards and Technology), tepatnya NIST SP 800-115 yang merupakan panduan teknis untuk pengujian dan penilaian keamanan informasi, metodologi yang dikhususkan

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

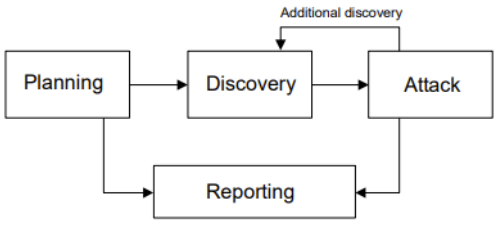
untuk membantu organisasi dalam melakukan perencaaan tes keamanan informasi [5].

2.1. Jenis Pengujian

Penelitian ini mengadopsi pendekatan *Blue Teaming,* yaitu pengujian dilakukan dengan sepengetahuan dan persetujuan dari pihak pengelola sistem situs XYZ. Pendekatan ini dipilih karena lebih hemat biaya dan lebih aman dibandingkan Red Teaming, serta dapat dilakukan tanpa menimbulkan gangguan yang berarti terhadap sistem yang diuji [4].

2.2. Tahapan Pengujian

Metode *penetration testing* dilakukan dengan 4 tahapan utama berdasarkan NIST SP 800-115 yang dapat dilihat pada Gambar 1, yaitu:



Gambar 1 Tahapan Metodologi

2.2.1. Perencanaan (Planning)

Pada fase perencanaan, ditetapkan target, tujuan, ruang lingkup, dan metode pengujian. Selanjutnya, disusun kesepakatan uji penetrasi yang terdokumentasi dalam *Rules of Engagement* [6]. Dalam konteks penelitian ini, pengujian hanya dilakukan pada subdomain publik situs XYZ, dengan batasan teknik yang tidak merusak (non-destructive), seperti pemindaian port dan analisis kerentanan pasif.

2.2.2. Penemuan (Discovery)

Tahap discovery mencakup dua bagian, yaitu pengumpulan informasi sistem target seperti *host*, *IP*, layanan, dan struktur situs menggunakan teknik seperti *port scanning, DNS interrogation*, dan *banner grabbing*, serta analisis kerentanan berdasarkan data yang diperoleh untuk mengidentifikasi potensi celah keamanan [7].

2.2.3. Serangan (Attack)

Tahap ini bertujuan untuk menguji kerentanan sistem berdasarkan informasi yang diperoleh dari proses *discovery*. Pengujian dilakukan secara pasif dan terbatas, dengan mensimulasikan serangan pada *endpoint* atau parameter yang terindikasi memiliki celah keamanan [8]. Fokus pengujian meliputi kerentanan umum seperti *cookie* tanpa atribut *Secure* dan *HttpOnly*, penggunaan *JavaScript* eksternal yang rentan, tidak diterapkannya *HTTP Strict Transport Security* (HSTS), serta ketergantungan pada pihak ketiga yang berisiko.

2.2.4. Pelaporan (Reporting)

Semua temuan dirangkum dalam bentuk laporan dengan klasifikasi berdasarkan tingkat keparahan (*high, medium, low, informational*) dan tingkat

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

keyakinan (*certain, firm, tentative*). Laporan ini digunakan sebagai dasar untuk membuat visualisasi data.

2.3. Tools yang Digunakan

Penelitian ini menggunakan Burp Suite sebagai tools utama yang digunakan untuk melakukan pemindaian dan eksploitasi terhadap situs. Burp Suite adalah salah satu alat yang paling sering digunakan dalam penetrasi testing untuk website dan aplikasi mobile. Alat ini sangat berguna bagi para profesional keamanan siber karena kemampuannya dalam menangkap dan menganalisis paket data yang dikirim dan diterima oleh aplikasi atau situs web [9].

III. HASIL DAN PEMBAHASAN

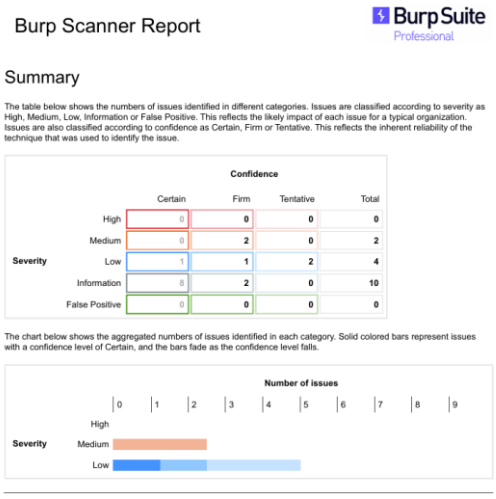
Setelah dilakukan pengujian penetrasi terhadap situs XYZ, ditemukan sejumlah temuan yang diklasifikasikan berdasarkan tingkat keparahan dan jenis kerentanan.

3.1. Struktur dan Fitur Situs XYZ

Situs XYZ merupakan *platform* digital milik pemerintah daerah yang bertujuan untuk mempermudah masyarakat dalam mengakses layanan administrasi secara daring, seperti pengajuan surat keterangan domisili, usaha, dan lainnya. Platform ini menyediakan fitur-fitur utama seperti pengisian formulir online, unggah dokumen persyaratan, pelacakan status permohonan, serta dukungan tanda tangan elektronik. Dengan tampilan antarmuka yang responsif dan integrasi ke dalam sistem pemerintahan lain seperti layanan kependudukan dan *smart city*, situs XYZ menjadi salah satu contoh penerapan teknologi untuk meningkatkan efisiensi, transparansi, dan akuntabilitas dalam pelayanan publik.

3.2. Hasil Pemindaian Situs XYZ

Pemindaian dilakukan dengan tools Burp Suite dengan pengaturan *Balance.* Tampilan hasil pemindaian dapat dilihat pada Gambar 2.


Burp Scanner Report

BurpSuite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low, Information or False Positive. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	0	0
	Medium	0	2	0	2
	Low	1	1	2	4
	Information	8	2	0	10
	False Positive	0	0	0	0

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.

Gambar 2 Hasil Pemindaian

3.3. Ringkasan Temuan

Dari hasil pemindaian dengan Burp Suite, ditemukan total 16 kerentanan, yang dikelompokkan berdasarkan tingkat keparahan sebagai berikut :

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

Tabel 1 Ringkasan Temuan

Tingkat Keparahan	Jumlah Temuan
High	0
Medium	4
Low	10
Informational	2

Visualisasi dalam Metabase menunjukkan dominasi temuan dengan tingkat keparahan *low*, yang menunjukkan bahwa meskipun tidak kritis, situs masih menyimpan sejumlah risiko keamanan yang perlu ditangani segera untuk mencegah eskalasi.

3.4. Jenis Kerentanan yang Ditemukan

Berikut beberapa jenis kerentanan utama yang berhasil diidentifikasi:

a. TLS Cookie tanpa Secure Flag

Ditemukan bahwa beberapa *cookie* seperti *session* tidak dilindungi dengan atribut *Secure*, yang memungkinkan transmisi cookie melalui koneksi HTTP tidak terenkripsi. Hal ini meningkatkan risiko pencurian sesi jika pengguna mengakses situs melalui jaringan yang tidak aman.

b. Ketergantungan pada *JavaScript* yang Rentan

Situs XYZ menggunakan pustaka *jquery-validation v1.17.0* yang telah diketahui memiliki beberapa celah keamanan seperti *Regular Expression Denial of Service (ReDoS)*. Temuan ini dikategorikan sebagai *low severity* tetapi penting untuk segera diperbarui ke versi terbaru.

c. *Cookie* tanpa *HttpOnly Flag*

Cookie XSRF-TOKEN ditemukan tidak memiliki atribut *HttpOnly*, sehingga memungkinkan akses oleh skrip sisi klien jika terjadi serangan XSS (*Cross-site Scripting*).

d. Tidak Diterapkannya *HTTP Strict Transport Security* (HSTS)

Situs belum mengaktifkan header *Strict-Transport-Security*, yang membuat browser tidak secara otomatis mengalihkan akses ke HTTPS. Hal ini membuka celah terhadap serangan *SSL stripping* pada jaringan publik.

e. *Cross-Domain Script Include*

Situs memuat skrip eksternal seperti *Google reCAPTCHA* tanpa menerapkan *Subresource Integrity* (SRI). Meskipun skrip tersebut berasal dari sumber tepercaya, tanpa SRI situs tetap rentan jika sumber tersebut disusupi.

3.5. Pembahasan

Hasil ini menunjukkan bahwa situs XYZ memiliki infrastruktur dasar yang cukup baik karena tidak ditemukan kerentanan dengan tingkat keparahan tinggi. Namun, adanya beberapa konfigurasi yang kurang optimal seperti cookie tidak aman dan pustaka rentan menunjukkan masih adanya celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, khususnya melalui serangan berbasis sesi dan injeksi skrip.

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

Dengan menerapkan rekomendasi perbaikan seperti pembaruan pustaka, pengaturan ulang cookie, dan aktivasi HSTS, maka situs XYZ dapat meningkatkan ketahanan keamanannya secara signifikan.

IV. KESIMPULAN

Penelitian ini berhasil menerapkan metode *penetration testing* dengan pendekatan *Blue Teaming* untuk mengevaluasi keamanan situs XYZ. Berdasarkan hasil pemindaian menggunakan Burp Suite dan analisis visual melalui Metabase, ditemukan total 16 kerentanan yang sebagian besar berada pada tingkat keparahan rendah. Meskipun tidak ditemukan kerentanan kritis, sejumlah konfigurasi yang kurang optimal dapat dieksploitasi untuk mencuri data sesi atau memanipulasi interaksi pengguna.

V. SARAN

Berdasarkan hasil pengujian dan analisis, disarankan agar pengelola situs XYZ segera meningkatkan konfigurasi keamanan dasar pada sistem mereka. Salah satu langkah penting adalah memastikan bahwa seluruh cookie yang digunakan untuk menyimpan data sensitif, seperti token sesi, telah dilengkapi dengan atribut *Secure* dan *HttpOnly*. Hal ini bertujuan untuk mencegah penyadapan melalui jaringan tidak aman serta menghindari potensi eksploitasi oleh skrip berbahaya di sisi klien.

Selain itu, pengelola perlu melakukan pembaruan rutin terhadap pustaka pihak ketiga, khususnya pustaka jquery-validation yang teridentifikasi memiliki sejumlah kerentanan. Pembaruan ini penting dilakukan untuk menutup celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Di samping itu, kebijakan keamanan seperti *HTTP Strict Transport Security* (HSTS) perlu diimplementasikan guna memastikan seluruh akses ke situs hanya dilakukan melalui protokol HTTPS yang terenkripsi, sehingga menutup kemungkinan terjadinya serangan downgrade seperti *SSL stripping*.

Penggunaan skrip eksternal juga perlu ditinjau kembali, dan apabila tetap diperlukan, harus disertai dengan penerapan *Subresource Integrity* (SRI) agar integritas file dapat divalidasi oleh *browser* sebelum dijalankan. Terakhir, disarankan agar audit keamanan dilakukan secara berkala dengan pendekatan yang sistematis dan terdokumentasi. Hal ini akan membantu memastikan bahwa situs selalu berada dalam kondisi aman serta dapat secara proaktif menghadapi berbagai jenis

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

ancaman yang mungkin timbul di masa mendatang.

DAFTAR PUSTAKA

[1] E. Z. Darojat, E. Sediyono, dan I. Sembiring, "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," *JURNAL SISTEM INFORMASI BISNIS*, vol. 12, no. 1, hlm. 36–44, Sep 2022, doi: 10.21456/vol12iss1pp36-44.

[2] G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, dan S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," Agu 2020.

[3] S. Hidayatulloh dan D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," Garut, Agu 2021. [Daring]. Tersedia pada: http://jurnal.itg.ac.id/

[4] K. A. Scarfone, M. P. Souppaya, A. Cody, dan A. D. Orebaugh, "Technical guide to information security testing and assessment.," Gaithersburg, MD, 2008. doi: 10.6028/NIST.SP.800-115.

[5] R. C. Silaban dan E. Wijaya, "Analisis Kerentanan Website Menggunakan Metode NIST SP 800-115 dan OWASP di Diskominfo Kabupaten Bandung," 2018.

[6] S. S. Anelia, J. Jayanta, dan B. Hananto, "Uji Penetrasi Server Universitas PQR Menggunakan Metode National Institute Of Standards And Technology (NIST SP 800-115)," *Jurnal Ilmu Teknik dan Komputer*, vol. 7, no. 1, hlm. 34, Mar 2023, doi: 10.22441/jitkom.2023.v7i1.005.

[7] M. D. Purnomo dan A. Chusyairi, "Pengujian Keamanan Sistem Mengunakan Metode Penetration Testing di Website Diskominfostandi Kota Bekasi," *Oktober*, vol. 1, no. 1, 2024, doi: 10.69533.

[8] H. Sulaeman dan A. Takwim, "Analisa Kualitas Keamanan Pada Aplikasi Slims Akasia Dengan Metode NIST SP 800-115 DAN OWASP."

[9] D. B. Hendayati, "Apa itu Burp Suite? Fitur dan Cara Menggunakannya," Digital Solusi Grup. Diakses: 16 Mei 2025. [Daring]. Tersedia pada: https://digitalsolusigrup.co.id/burp-suite-adalah/

[10] Nanda Aprillia, M., Wahyu Christanto, F., Parga Zen, B., Maulana, H., & Yudi Permana, N. (2025). Implementasi Teknologi QR Code pada Sistem Absensi Karyawan Berbasis Website. *Jurnal Sistem Informasi Galuh*, *3*(1), 39–50.https://d