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

Uji Keamanan Aplikasi *Website* XYZ Menggunakan Burp Suite Berdasarkan Kerangka NIST SP 800-115

Mamay Syani*[1], Ridwan Nurhakim[2], Fadhil Rifgi Pratama[3], Haisyam Maulana[4], Ali Nurdin[5]
*[1,2,3]Politeknik TEDC Bandung
[4,5]Universitas Galuh Ciamis
Email: *[1]msyani@poltektedc.ac.id, [2]ridwann690@gmail.com, [3]fadhilrifgipratama26@gmail.com, [4]haisyammaulana22@gmail.com, [5]alinurdin@unigal.ac.id

Abstract

Advancements in digital technology have prompted government institutions to adopt online services, including the provision of public information through their official websites. However, the growing reliance on digital systems has also led to an increase in cybersecurity threats. This study aims to assess potential security vulnerabilities on the XYZ website, which is managed by a regional government, using a penetration testing approach based on the NIST SP 800-115 framework and the Burp Suite tool. The testing process was carried out in four phases: planning, discovery, attack execution, and reporting. The results revealed eight vulnerabilities, including two classified as high severity: code injection and unencrypted communication (HTTP). Additionally, publicly accessible backup files and support for XML input were identified, posing risks of XML External Entity (XXE) attacks. These findings highlight the critical importance of input validation, full implementation of HTTPS protocols, and strict file management to enhance website security. The study also recommends conducting further audits related to XML vulnerabilities and implementing continuous system monitoring to address evolving cyber threats.

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

Abstrak

Perkembangan dalam teknologi digital telah mendorong instansi pemerintah untuk mengadopsi layanan online, termasuk dalam menyediakan informasi publik melalui situs resmi mereka. Namun, seiring dengan meningkatnya penggunaan sistem digital, terdapat peningkatan dalam risiko ancaman siber. Penelitian ini bertujuan untuk menilai potensi kerentanan keamanan pada situs web XYZ yang dikelola oleh pemerintah daerah dengan menggunakan metode penetration testing mengacu pada kerangka kerja NIST SP 800-115 dan alat bantu Burp Suite. Proses uji coba dilakukan melalui empat fase: perencanaan, penemuan, pelaksanaan serangan, dan penyusunan laporan. Hasil dari pengujian menunjukkan adanya delapan kerentanan, di antaranya dua yang tergolong dengan tingkat keparahan tinggi, yaitu code injection dan komunikasi yang tidak menggunakan enkripsi (HTTP). Selain itu, terdeteksi file cadangan yang dapat diakses secara publik serta dukungan input XML yang menimbulkan risiko serangan XXE. Temuan ini menyoroti kenyataan bahwa validasi input, penerapan protokol HTTPS secara menyeluruh, dan manajemen file yang ketat adalah penting untuk meningkatkan keamanan situs. Saran juga mencakup kebutuhan untuk melakukan audit lanjutan terkait potensi kerentanan XML dan menjalankan pemantauan sistem secara berkala untuk menghadapi ancaman yang terus berubah.

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

I. PENDAHULUAN

Perkembangan teknologi digital telah mendorong digitalisasi layanan publik, termasuk pada sektor pemerintahan. *Website* pemerintah menjadi sarana utama dalam menyediakan informasi dan layanan kepada masyarakat. Tiga studi terkait pengujian penetrasi dan penilaian kerentanan pada situs web di Indonesia mengungkapkan beragam

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

metode yang diterapkan secara efektif. Firdaus et al. menerapkan kerangka ISSAF bersama dengan standar ISO 31000 dalam menangani risiko teknologi informasi pada situs akademik, menekankan sinergi antara manajemen risiko dan teknik eksploitasi [1]. Zairina et al. mengevaluasi sistem *e-voting* nasional berdasarkan panduan OWASP Top 10, yang menghasilkan temuan kerentanan serius seperti SQL injection dan XSS [2]. Sementara itu, Wahyuni et al. mengkaji keamanan situs *e-commerce* milik Dapur Cokelat Indonesia dengan bantuan alat otomatis seperti Acunetix, yang berhasil mengidentifikasi kelemahan pada autentikasi dan manajemen sesi. Ketiga penelitian tersebut secara keseluruhan menunjukkan pentingnya pengujian keamanan yang rutin, adopsi standar global, serta penggabungan metode manual dan otomatis untuk memperkuat pertahanan siber situs web di Indonesia [3].

Menurut laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023, terdapat lebih dari 400 juta anomali trafik jaringan yang berpotensi sebagai serangan siber terhadap sistem pemerintah yang dapat berdampak pada penurunan peforma perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan. Oleh karena itu, diperlukan langkah proaktif dalam mengidentifikasi dan menangani celah keamanan yang ada pada sistem digital milik pemerintah.

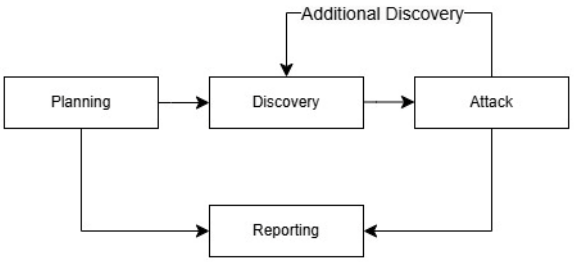
Penelitian ini bertujuan untuk mengevaluasi kerentanan pada situs XYZ dengan memanfaatkan kerangka kerja NIST SP 800-115 sebagai panduan metodologis. Kerangka tersebut menawarkan pendekatan terstruktur dalam menilai risiko yang dihadapi oleh sistem informasi.

II. METODOLOGI PENELITIAN

Penelitian ini mengimplementasikan metode *penetration testing* (Pentest) merupakan evaluasi yang dilakukan terhadap suatu perangkat lunak atau sistem untuk menemukan celah yang bisa dimanfaatkan [4]. Penggunaan pentest bertujian untuk mengidentifikasi potensi kerentanan pada sistus XYZ dengan cara mensimulasikan serangan siber secara etis dan terkendali. Proses ini dilakuakan dengan menggunakan pendekatan sistematis yang diambil dari kerangka kerja NIST SP 800-115 sebagai metodologi penelitian ini. NIST SP 800-115 adalah sebuah dokumen yang menggambarkan berbagai metode serta teknik yang diterapkan saat melakukan pengujian kerentanan pada situs selama penetration testing, berserta saran solusi untuk mengatasi kerentanan yang terdapat pada situs tersebut [5].

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

2.1. Tahapan Pengujian



Gambar 1 Tahapan Metodologi NIST

2.1.1 *Planning* (Perencanaan)

Tahap *planning*, merupakan tahapan awal dalam melakukan pengujian serta sebagai persetujuan kepada pihak yang mengelola sistem, serta melakukan penjelasan mengenai ruang lingkup dalam penelitian [6]. Dalam studi ini, penekanan pengujian terbatas hanya pada sektor publik dari situs XYZ tanpa melaksanakan tindakan merusak yang dapat mengganggu operasional.

2.1.2 *Discovery* (Penemuan)

Tahap Penemuan memiliki dua komponen, yaitu mengumpulkan data mengenai target seperti nama host dan rincian tentang alamat IP, sistem, serta layanan melalui pemindaian terhadap target. Komponen kedua adalah analisis kerentanan atau mengevaluasi kelemahan yang telah diperoleh selama proses pengumpulan data [7].

2.1.3 *Attack* (Serangan)

Tahap Attack adalah langkah dalam pendekatan NIST SP 800-115 untuk melakukan penetrasi pada Docker yang lemah yang sedang diuji untuk mengidentifikasi adanya kerentanan dengan melaksanakan skenario pengumpulan data [8]. Uji coba dilakukan dalam keadaan yang terkontrol dengan meniru serangan pada elemen input, arsip cadangan, dan jalur HTTP untuk memastikan kemungkinan terjadinya eksploitasi.

2.1.4 *Reporting* (Pelaporan)

Tahap reporting pengungkapan hasil riset dan penjelasan terkait hasil tes serta penilaian tentang aspek keamanan [9]. Temuan dirangkum dalam dokumen terstruktur berdasarkan tingkat keparahan dan digunakan sebagai acuan pembuatan visualisasi data.

2.2 Tools yang digunakan

Penelitian ini mengimplementasikan Burp Suite sebagai alat utama untuk melakukan pengujian penetrasi. Burp Suite merupakan platform untuk menguji keamanan aplikasi web yang sangat digemari oleh para profesional di bidang keamanan siber. Beragam fitur yang disediakan oleh perangkat lunak ini memungkinkan evaluasi dan analisis mendalam terhadap aplikasi web untuk mengidentifikasi potensi kelemahannya

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

dan memberikan solusi untuk perbaikannya. Burp Suite memiliki fitur-fitur utama seperti Proksi Intercepting, Pemindai, Penyerang, dan Pengulang. Semua fitur ini mampu mengelola dan menganalisis lalu lintas HTTP/HTTPS yang terjadi antara pengguna dan server [10].

III. HASIL DAN PEMBAHASAN

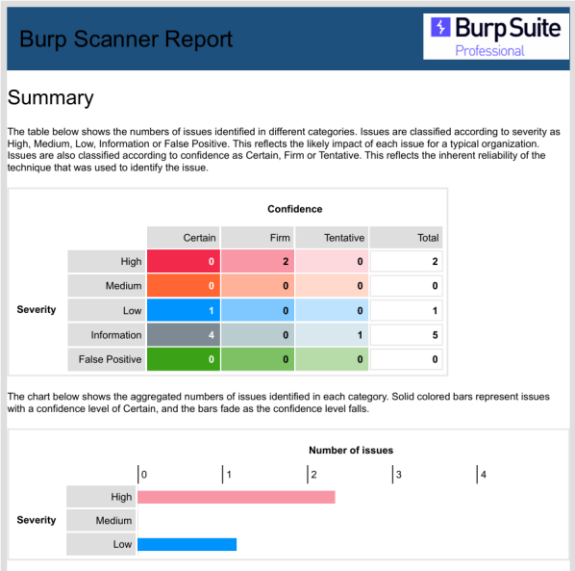
Setelah melakukan pengujian penetrasi terhadap situs XYZ, ditemukan sejumlah temuan yang diklasifikasikan

3.1. Struktur dan Fitur Situs XYZ

Situs web XYZ adalah portal layanan digital yang dikembangkan oleh pemerintah daerah untuk mempromosikan masyarakat ketika mengakses berbagai layanan manajemen *online*, dari mengelola dokumen populasi hingga mengirimkan lisensi perusahaan. Dengan menggunakan *platform* ini, pengguna dapat mengisi formulir *online*, mengunggah dokumen persyaratan, dan memantau status aplikasi dengan cara yang lebih praktis. Dengan antarmuka yang ramah pengguna dan akses satu pintu (SSO), situs web XYZ berupaya meningkatkan kemudahan, transparansi, dan kecepatan layanan.

3.2 Hasil Pemindaian situs XYZ

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



Gambar 2 hasil pemindaian Website xyz

3.3 Ringkasan temuan

Dari analisis menggunakan Burp Suite, teridentifikasi 8 celah keamanan yang dikategorikan menurut level keparahan sebagai berikut:

Tabel 1 ringkasan temuan

Tingkat kerentanan	Total temuan
High	2
Medium	0
Low	1
Informational	4

Laporan ini mengindikasikan terdapat satu kelemahan dengan tingkat keparahan yang tinggi dan kepercayaan yang kuat, bersama dengan beberapa masalah sedang dan rendah. Ini menunjukkan adanya masalah serius yang harus segera diperbaiki, meskipun mayoritas temuan bersifat kecil.

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

3.4 Jenis kerentanan yang ditemukan

Berikut beberapa jenis kerentanan utama yang berhasil diidentifikasi:

a. *Code injection*

Ditemukan bahwa *webiste* tampaknya mengeksekusi input pengguna seoelah-olah itu adalah perintah kode. Temuan ini menunjukkan bahwa *website* memiliki kerentanan *code injection*, yang merupakan salah satu jenis serangan berisiko tinggi. Karena input pengguna tidak difilter atau divalidasi dengan baik, sistem menjadi rentan terhadap eksploitasi yang dapat berakibat fatal bagi keamanan aplikasi dan data.

b. *Unencrypted communications*

Aplikasi web masih dapat diakses menggunakan HTTP (tidak aman), bukan HTTPS (aman/terenkripsi). Ini berarti data yang dikirimkan antara pengguna dan server dapat dicegat dan dibaca oleh pihak ketiga, seperti pada jaringan Wi-Fi publik atau jaringan lokal yang tidak aman.

c. *Input returned in response (reflected)*

Aplikasi mengembalikan kembali sebagian input pengguna dalam respons HTTP tanpa proses validasi atau penyaringan. Meskipun bersifat informatif, refleksi input perlu diperhatikan karena berpotensi menjadi jalur masuk bagi serangan yang lebih serius.

d. *Backup file*

Ditemukan file backup atau salinan lama seperti /robots.jar dan /robots.txt.jar yang dapat diakses secara publik melalui web server. File backup yang dibiarkan tersedia ini dapat mengungkapkan informasi sensitif seperti kode sumber, konfigurasi, atau data lain yang seharusnya tidak diketahui pihak luar.

e. *TLS certificate*

Server website XYZ menggunakan sertifikat TLS yang valid dan terpercaya. Sertifikat ini berfungsi untuk mengamankan komunikasi antara pengguna dan server dengan mengenkripsi data yang ditransmisikan serta memastikan keaslian identitas server.

f. *XML input supported*

Aplikasi pada website XYZ menerima input dengan format application/xml. Meskipun menerima input XML bukanlah masalah langsung, hal ini membuka kemungkinan kerentanan terkait pengolahan XML, terutama serangan XML External Entity (XXE).

3.5 Pembahasan

Pengujian menunjukkan bahwa situs web XYZ telah menerapkan sertifikat TLS yang valid, tetapi masih terdapat sejumlah kerentanan yang signifikan. Penggunaan injeksi kode dan akses HTTP yang tidak terenkripsi menciptakan celah bagi serangan yang berbahaya dan peretasan data. Adanya refleksi input dan file cadangan yang dapat diakses secara publik meningkatkan kemungkinan kebocoran informasi. Dukungan untuk input XML juga bisa menimbulkan ancaman serangan tertentu seperti XXE.

Peningkatan dalam validasi input, penerapan HTTPS secara menyeluruh,

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

dan pengelolaan file yang lebih ketat sangat diperlukan untuk memperkuat keamanan situs web secara drastis.

IV. KESIMPULAN

Penelitian ini berhasil melakukan evaluasi kerentanan pada situs XYZ dengan menerapkan metode penetration testing berdasarkan kerangka kerja NIST SP 800-115 dan menggunakan alat Burp Suite. Hasil dari pemindaian ini mengungkapkan beberapa kerentanan kritis, seperti injeksi kode dan penggunaan koneksi HTTP tanpa enkripsi, yang dapat mengancam keselamatan data dan aplikasi. Selain itu, temuan mengenai file cadangan publik dan input XML yang diperbolehkan juga menunjukkan adanya risiko kebocoran data dan kemungkinan serangan khusus XML. Walaupun situs tersebut telah menerapkan sertifikat TLS yang sah, perbaikan masih harus dilakukan pada aspek validasi input dan perlindungan komunikasi.

V. SARAN

Berdasarkan hasil dari penelitian ini, disarankan kepada pengelola situs XYZ untuk segera memperkuat proses validasi dan pembersihan input guna mencegah risiko tinggi terkait code injection. Selain itu, sangat penting untuk menerapkan kebijakan penggunaan HTTPS secara menyeluruh agar semua komunikasi antara pengguna dan server terjaga dengan enkripsi yang tepat, sehingga potensi penyadapan data bisa ditekan, khususnya di jaringan publik. Pengelola juga perlu menghapus atau melindungi file cadangan yang masih bisa diakses publik untuk mencegah kebocoran informasi yang sensitif. Mengingat situs tersebut mendukung input XML, perlu dilakukan audit lanjutan untuk menanggulangi ancaman XML External Entity (XXE) yang berbahaya. Terakhir, sangat dianjurkan untuk melakukan pemantauan dan pembaruan secara berkala terhadap pengaturan keamanan dan perangkat lunak agar situs selalu tahan terhadap ancaman siber yang terus berubah. Langkah-langkah ini akan membantu meningkatkan keandalan serta keamanan layanan digital yang diberikan kepada masyarakat.

DAFTAR PUSTAKA

[1] Perdianza Me, Firdaus Ma, Indah Dr, Sriwijaya U, Ilir O, Selatan S. Information Technology Risk Management Using Iso 31000 Based On The Issaf Penetration Testing Framework Menggunakan Iso 31000 Berbasis Kerangka Kerja Pengujian. 2024;9(2):839–51.

[2] Zairina Z, Huwae Rb, Jatmika Ah. Implementasi Owasp Top 10 Dalam Pengujian Penetrasi Website : Mengidentifikasi Celah Keamanan Dalam Sistem Pengelolaan Voting Indonesia (Implementation Of Owasp Top 10 In Website Penetration Testing : Identifying Security Gaps In Indonesia ' S

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

Voting Man. 2025;7(1).

[3] Wahyuni Ft, Utama Gp, Imelda I, Painem P. Analisis Vulnerability Dan Risk Assesment Terhadap Website Pt . Dapur Cokelat Indonesia Menggunakan Metode Penetration Testing Vulnerability Analysis And Risk Assesment Againts Website Pt . Dapur Cokelat Indonesia Using Penetration Testing. 2024;3(September):1134–43.

[4] Sholawati A, Setyadi Hj, Padmo A, Masa A. Implementasi Penetration Testing Pada Sistem Informasi Terpadu Layanan Prodi Menggunakan. 2024;25(2):73–86.

[5] Maherza Sa, Hananto B, Pradnyana Iww. Penetration Testing Terhadap Website Sekolah Menengah Atas Abc Dengan Metode Nist Sp 800-115. Inform J Ilmu Komput. 2023;19(1):11–27.

[6] Mambo F, Yuniarto D, Setiadi D, Informatika Ps, Teknologi F, Universitas I, Et Al. Evaluasi Keamanan Website Dengan Menggunakan Metode Nist Sp. 2024;3.

[7] Purnomo Md, Chusyairi A, Insani Ub, Jaya S, Bekasi K. Pengujian Keamanan Sistem Mengunakan Metode Penetration Testing Di Website Diskominfostandi Kota Bekasi. 2024;1(1):92–101.

[8] Astriani T. Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar Nist 800-115. JATISI (Jurnal Tek Inform Dan Sist Informasi). 2021;8(4):2041–50.

[9] Darojat EZ, Sediyono E, Sembiring I. Vulnerability Assessment Website E-Government Dengan NIST SP 800-115 Dan OWASP Menggunakan Web Vulnerability Scanner. J Sist Inf Bisnis. 2022;12(1):36–44.

[10] Dwi Agustina V, Ariyadi T, Syah Putra T, Lega A. Teknik Pengujian Penetrasi Http Menggunakan Tools Burp. 2025;4(1):16–21.

[11] 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