REPOSITOR, Vol. 8, No. 1, Februari 2026, Pp. 129-136
ISSN : 2714-7975
E-ISSN : 2716-1382

Analisis Risiko Dan Strategi Perlindungan Sistem Terhadap Ancaman Siber Pada Website 'SAMBANG' Kabupaten Jombang

Muhammad Rayhan Islamiah Prathama[*1], Zamah Sari[1], Denar Regata Akbi[1]
*Informatika, Universitas Muhammadiyah Malang
mrrayhankagami@webmail.umm.ac.id[*]

Abstrak

Penelitian ini bertujuan untuk menganalisis risiko keamanan serta merumuskan strategi perlindungan sistem terhadap ancaman siber pada website "SAMBANG" milik Pemerintah Kabupaten Jombang. Pendekatan penelitian yang digunakan adalah kualitatif eksploratif melalui observasi, studi literatur, serta penetration testing non-destruktif berbasis standar OWASP dan NIST. Hasil penelitian menunjukkan bahwa website "SAMBANG" masih memiliki sejumlah kerentanan dengan tingkat risiko yang tinggi, terutama pada fitur Open Data, Data Statistik, Katalog Data, dan Request Data yang rentan terhadap serangan Cross-Site Scripting (XSS), baik reflected maupun stored. Selain itu, potensi risiko SQL Injection teridentifikasi meskipun tidak tereksploitasi secara langsung, serta kelemahan autentikasi pada halaman login yang rentan terhadap brute force. Form Request Data juga ditemukan tidak memiliki mekanisme Cross-Site Request Forgery (CSRF) token, sehingga berpotensi dimanfaatkan oleh penyerang. Penelitian ini menyarankan penerapan validasi input, encoding output, Content Security Policy (CSP), prepared statement, autentikasi multi-faktor, pembatasan login, serta validasi file upload untuk meningkatkan perlindungan sistem. Dengan hasil ini, penelitian memberikan kontribusi praktis bagi pengelola sistem informasi publik daerah dalam memperkuat keamanan website pemerintahan serta membangun ketahanan siber yang lebih adaptif.

Kata Kunci: *Keamanan Siber, Analisis Risiko, Website Pemerintah, SQL Injection, XSS*

Abstract

This research aims to analyze security risks and formulate system protection strategies against cyber threats on the "SAMBANG" website owned by the Jombang Regency Government. The research approach used is exploratory qualitative through observation, literature study, and non-destructive penetration testing based on OWASP and NIST standards. The results of the study show that the "SAMBANG" website still has a number of vulnerabilities with a high level of risk, especially in the Open Data, Statistical Data, Data Catalog, and Data Request features, which are vulnerable to Cross-Site Scripting (XSS) attacks, both reflected and stored. In addition, the potential risk of SQL Injection was identified, although it was not directly exploited, as well as authentication weaknesses on the login page that were vulnerable to brute force. The Data Request form was also found to lack a Cross-Site Request Forgery (CSRF) token mechanism, making it potentially exploitable by attackers. This study recommends the implementation of input validation, output encoding, Content Security Policy (CSP), prepared statements, multi-factor authentication, login restrictions, and file upload validation to improve system protection. With these results, the study provides practical contributions for regional public information system managers in strengthening government website security and building more adaptive cyber resilience.

Keywords: *Cybersecurity, Risk Analysis, Government Websites, SQL Injection, XSS*

1. Pendahuluan

Perkembangan teknologi informasi telah mendorong pemerintah daerah untuk menyediakan layanan publik berbasis digital. Website menjadi salah satu sarana utama dalam meningkatkan efisiensi pelayanan, transparansi, dan aksesibilitas informasi bagi masyarakat [1]. Namun, dibalik manfaat tersebut, ancaman terhadap keamanan siber juga semakin meningkat, terutama pada sistem pemerintahan yang sering menjadi target serangan peretasan, pencurian identitas, maupun eksploitasi data [2].

Website SAMBANG (Sistem Administrasi Berbasis Digital Jombang) merupakan inovasi Pemerintah Kabupaten Jombang untuk mempermudah akses masyarakat terhadap layanan administrasi dan informasi publik. Meskipun telah membantu ribuan warga, keberadaannya juga menimbulkan potensi risiko keamanan. Laporan BSSN mencatat lebih dari seribu insiden siber menimpa situs pemerintah di Indonesia pada 2023, dengan serangan umum seperti SQL Injection, Cross-Site Scripting (XSS), dan session hijacking [3]. Jika tidak ditangani, kerentanan tersebut dapat berdampak pada kebocoran data pribadi, kerugian finansial, dan menurunnya kepercayaan publik [4].

Sejumlah penelitian menunjukkan bahwa kerentanan aplikasi web pemerintah masih tinggi, dengan SQL Injection dan XSS sebagai dua serangan paling dominan [5,6]. Selain itu, kelemahan autentikasi pengguna, kurangnya validasi input, serta ketiadaan mekanisme keamanan seperti Content Security Policy (CSP) dan token anti-CSRF, semakin memperbesar risiko [7]. Oleh karena itu, penting dilakukan evaluasi mendalam terhadap bug keamanan pada website pemerintahan, termasuk SAMBANG, guna mencegah eksploitasi yang dapat mengganggu layanan publik.

Penelitian ini dilakukan dengan pendekatan kualitatif eksploratif melalui observasi, studi literatur, serta penetration testing non-destruktif yang berpedoman pada standar OWASP dan NIST [8], [9]. Fokus kajian mencakup identifikasi bug pada fitur utama, analisis risiko, serta strategi mitigasi yang dapat diterapkan oleh pengelola sistem. Nilai kebaruan penelitian ini terletak pada studi kasus langsung pada website SAMBANG, yang belum pernah diteliti sebelumnya, serta penyusunan rekomendasi praktis bagi pemerintah daerah dalam meningkatkan ketahanan siber.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif eksploratif yang bertujuan untuk mengidentifikasi dan menganalisis kerentanan keamanan pada website SAMBANG Kabupaten Jombang. Pendekatan ini dipilih karena mampu memberikan pemahaman mendalam terhadap fenomena ancaman siber dalam konteks layanan publik digital [3], [4].

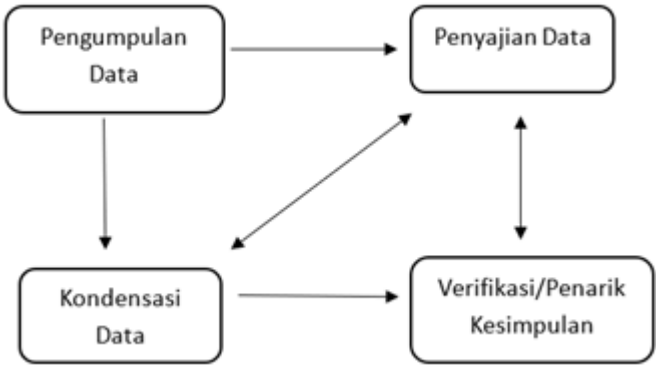
2.1 Studi Literatur

Rancangan penelitian dilakukan melalui tiga tahapan utama, yaitu:

1. Pengumpulan Data
   Melalui observasi langsung terhadap website SAMBANG, dokumentasi, serta studi literatur terkait keamanan aplikasi web.
2. Pengujian Keamanan
   Menggunakan metode penetration testing non-destruktif untuk menguji kerentanan umum pada aplikasi web, seperti SQL Injection, Cross-Site Scripting (XSS), brute force, dan Cross-Site Request Forgery (CSRF) [7], [8].
3. Analisis Risiko
   Menggunakan kerangka kerja OWASP dan NIST SP 800-30 untuk menilai tingkat kemungkinan (likelihood) dan dampak (impact) dari setiap kerentanan yang ditemukan [9], [13].

2.2 Prosedur Penelitian

Pengujian dilakukan pada beberapa fitur utama website SAMBANG, termasuk halaman login, fitur Open Data, Data Statistik, Katalog Data, serta form Request Data. Setiap fitur diuji menggunakan kombinasi manual testing dan alat bantu open-source, seperti SQLmap untuk SQL Injection dan OWASP ZAP untuk XSS. Parameter yang diuji meliputi validasi input, sanitasi output, mekanisme autentikasi, serta keamanan sesi pengguna [2], [7].



Gambar 1. Model Analisis Interaktif Miles dan Huberman

Adapun langkah-langkah dalam melakukan analisis data adalah sebagai berikut:

1. Pengumpulan Data

   Pengumpulan data merupakan langkah dalam mengumpulkan berbagai data yang diperlukan dalam penelitian. Teknik yang dilakukan yaitu wawancara dan dokumentasi data-data yang diperlukan. Data-data tersebut diperoleh dari hasil observasi peneliti dan informan mengenai bug pada celah keamanan website "SAMBANG" Kabupaten Kabupaten Jombang. Serta pengamat sebagai pemeran peneliti dan dokumentasi yang dihimpun oleh peneliti selama melakukan pengamatan di lokasi penelitian.
2. Kondensasi Data

   Kondensasi data adalah proses di mana peneliti memilih, menyederhanakan, dan mengabstraksikan data dari berbagai sumber seperti catatan lapangan, observasi, dokumen, dan materi empiris lainnya. Tujuan dari kondensasi ini adalah untuk menyusun data menjadi bentuk yang lebih fokus dan relevan dengan kebutuhan penelitian. Ini melibatkan pengumpulan data dari observasi yang telah dilakukan untuk memastikan bahwa informasi yang diperoleh sesuai dengan topik penelitian.
3. Penyajian Data

   Penyajian data yakni menyusun penyajian hasil penelitian dalam bentuk eksploratif, gambar saat melaksanakan penilitian di *website* "SAMBANG" disertai analisis awal terhadap berbagai temuan data di lapangan sebagai proses awal pengelolaan data.
4. Penarikan Kesimpulan dan Verifikasi

   Penarikan kesimpulan yaitu dilakukannya pembahasan yang berdasarkan pada hasil reduksi dan penyajian data. Dalam menarik kesimpulan, peneliti akan melakukan sesuai dengan hasil pengamatan yang dilakukan selama penelitian di *website* "SAMBANG". Peneliti akan mengeksplor dan menarik kesimpulan mengenai bug pada celah keamanan di *website* "SAMBANG" Kabupaten Jombang. Setelah menarik kesimpulan, kemudian di verifikasi yang bertujuan untuk mencari data baru yang lebih mendalam dengan persetujuan yang sama.

2.3 Perancangan Alat

Data yang diperoleh dari pengujian kemudian dianalisis secara kualitatif menggunakan model interaktif Miles & Huberman, yang meliputi tahap kondensasi data, penyajian data, serta penarikan kesimpulan [14]. Risiko keamanan dikelompokkan menggunakan matriks risiko untuk menentukan prioritas mitigasi. Untuk mempermudah tindak lanjut, seluruh risiko diprioritaskan menggunakan pendekatan Risk Matrix.

Tabel 1. Matriks Prioritas Risiko Keamanan Website SAMBANG

Risiko Keamanan	Likelihood	Impact	Kategori Risiko	Tindakan Prioritas
Stored XSS	Tinggi	Tinggi	Kritis	Segera filter dan encode input
Brute Force Login	Tinggi	Tinggi	Kritis	Terapkan rate limit & MFA

File Upload Tidak Aman	Sedang	Tinggi	Tinggi	Validasi MIME dan hash nama
Reflected XSS	Sedang	Sedang	Sedang	Implementasi CSP
CSRF pada Request Data	Sedang	Sedang	Sedang	Gunakan CSRF token
Metadata HTML Injection	Tinggi	Sedang	Tinggi	Validasi & audit metadata
IDOR File Access	Rendah	Tinggi	Sedang	Tokenisasi dan URL hash

3. Hasil Penelitian dan Pembahasan

3.1 Evaluasi Keamanan Website SAMBANG

Hasil pengujian terhadap website SAMBANG menunjukkan masih adanya kerentanan pada beberapa fitur utama. Pada halaman login, sistem tidak dilengkapi dengan mekanisme rate limiting maupun multi-factor authentication, sehingga berpotensi dieksploitasi melalui brute force. Tidak adanya fitur account lockout semakin memperbesar risiko serangan [2], [5].

Tabel 2. Hasil Pengujian Brute Force Login

Parameter	Keterangan
Titik Kerentanan	Form login, parameter pencarian
Payload Uji	' OR '1'='1, admin' --
Hasil Uji	Tidak langsung tembus, tetapi tidak ada pesan sanitasi input
Likelihood	Sedang
Dampak	Tinggi (bisa bocornya seluruh isi database)
Risiko Keseluruhan	Tinggi
Status Validasi Input	Belum sepenuhnya menerapkan prepared statement
Strategi Mitigasi	Gunakan parameterized query dan whitelist filter

Pada fitur Open Data, Data Statistik, dan Katalog Data, ditemukan kerentanan Cross-Site Scripting (XSS) dalam bentuk reflected dan stored. Kerentanan ini muncul akibat tidak adanya validasi input yang memadai serta ketiadaan output encoding, sehingga memungkinkan penyerang menyisipkan script berbahaya untuk mencuri data sesi pengguna [3], [4].

Tabel 3. Temuan Kerentanan XSS

Fitur	Jenis XSS	Payload Uji	Hasil
Open Data	Reflected	<script>alert('XSS')</script>	Skrip berhasil dijalankan
Data Statistik	Stored	HTML skrip pada metadata	Skrip tersimpan dan tereksekusi
Produsen Data	Stored	<img src=x onerror=alert(1)>	Skrip berhasil dieksekusi
Katalog Data	Stored	HTML script dalam deskripsi file	Tereksekusi saat ditampilkan

```php
<?php
// Koneksi ke database
$conn = mysqli_connect("localhost", "root", "", "test_db");

if (!$conn) {
    die("Koneksi gagal: " . mysqli_connect_error());
}

// Tangkap input dari URL
$username = $_GET['username'];

// Query rentan SQL Injection
$sql = "SELECT * FROM users WHERE username = '$username'";
$result = mysqli_query($conn, $sql);

// Tampilkan hasil
if (mysqli_num_rows($result) > 0) {
    while($row = mysqli_fetch_assoc($result)) {
        echo "Username: " . $row["username"] . " - Email: " . $row["email"] . "<br>";
    }
} else {
    echo "0 results";
}

mysqli_close($conn);
?>
```

Gambar 2. Hasil Uji XSS berupa Alert-pop

Kode di atas melakukan koneksi ke database test_db, kemudian mengambil input dari parameter URL $_GET['username'], dan langsung memasukkannya ke dalam query SQL tanpa validasi atau filter apapun. Hal ini membuka celah keamanan yang sangat besar karena penyerang dapat menyisipkan perintah SQL berbahaya.
Sebagai contoh, jika penyerang mengakses URL berikut:

```
http://example.com/script.php?username=' OR '1'='1
```

Maka nilai dari $username akan menjadi ' OR '1'='1, dan query yang dihasilkan adalah:

```
SELECT * FROM users WHERE username = '' OR '1'='1';
```

Query tersebut akan mengembalikan seluruh data dari tabel users karena kondisi 1='1' selalu benar, sehingga sistem menampilkan seluruh informasi pengguna tanpa otorisasi yang sah. Ini merupakan bentuk serangan Authentication Bypass, yang dapat berlanjut menjadi pencurian data (*data leakage*).

Sementara itu, form Request Data diketahui tidak memiliki mekanisme token Cross-Site Request Forgery (CSRF). Kondisi ini membuka peluang bagi penyerang untuk mengirimkan permintaan palsu yang tampak sah. Form upload pada fitur tersebut juga tidak dilengkapi dengan validasi ketat, sehingga berisiko menjadi sarana unggah file berbahaya [7], [11].

Tabel 4. Hasil Pengujian CSRF

Elemen Formulir	Ada CSRF Token	Validasi Referer	Risiko
Form Request Data	Tidak	Tidak	Sedang

Mitigasi:

- Gunakan CSRF token unik yang diperbarui pada setiap sesi.
- Validasi HTTP referer dan origin.
- Hindari metode GET untuk aksi-aksi perubahan data.

Beberapa fitur memungkinkan pengguna mengunggah file atau mengakses file publik tanpa validasi MIME type. Pengujian menemukan file dapat diunggah dengan ekstensi mencurigakan dan URL bisa dimodifikasi untuk mengakses file tidak sah.

Tabel 5. Evaluasi Validasi File Upload

Fitur	Masalah Ditemukan	Dampak
Katalog Data	Tidak validasi MIME type	File bisa mengandung skrip
Publikasi	Tidak ada whitelist ekstensi	PDF/EXE bisa disisipkan
Info Keuangan Daerah	URL bisa dimodifikasi oleh pengguna	Akses file tidak sah (IDOR)

Mitigasi:
- Validasi nama file dan jenis MIME yang diizinkan.
- Terapkan sistem hash atau UUID untuk nama file.
- Gunakan direktori publik terpisah dengan kontrol akses.

3.2 Analisis Risiko dan Strategi Mitigasi

Analisis risiko berdasarkan standar OWASP dan NIST menunjukkan bahwa serangan XSS dan brute force termasuk kategori tinggi, sedangkan CSRF dan kelemahan validasi upload file berada pada kategori sedang. Potensi SQL Injection terdeteksi, meskipun tidak berhasil dieksploitasi penuh karena sistem telah memiliki sanitasi parsial pada query. Namun demikian, risiko SQL Injection tetap dikategorikan berbahaya karena dampaknya yang besar apabila berhasil dimanfaatkan [6], [13].

Strategi mitigasi yang direkomendasikan antara lain validasi input dan output encoding, penggunaan prepared statement untuk mencegah SQL Injection, penambahan Content Security Policy (CSP) untuk mengurangi risiko XSS, serta penerapan token CSRF untuk mencegah pengiriman permintaan ilegal. Untuk login, disarankan implementasi multi-factor authentication, rate limiting, serta account lockout setelah percobaan gagal berulang [8]. Validasi ketat pada proses upload file juga penting dilakukan untuk mencegah penyisipan file berbahaya.

Temuan ini sejalan dengan penelitian sebelumnya yang menegaskan bahwa aplikasi web pemerintahan masih rawan terhadap serangan klasik seperti SQL Injection dan XSS [4], [10], serta menekankan pentingnya penguatan ketahanan siber di sektor publik [5], [13].

4. Kesimpulan

Penelitian ini telah berhasil mengidentifikasi kerentanan keamanan pada website SAMBANG Kabupaten Jombang melalui pendekatan kualitatif eksploratif dan penetration testing non-destruktif. Hasil pengujian menunjukkan adanya celah pada beberapa fitur, meliputi kelemahan autentikasi login yang rentan terhadap brute force, kerentanan Cross-Site Scripting (XSS) pada fitur Open Data, Statistik, dan Katalog Data, ketiadaan token Cross-Site Request Forgery (CSRF) pada form Request Data, serta validasi yang lemah pada mekanisme upload file. Potensi serangan SQL Injection juga teridentifikasi meskipun tidak berhasil dieksploitasi sepenuhnya.

Berdasarkan analisis risiko dengan standar OWASP dan NIST, kerentanan XSS dan brute force termasuk dalam kategori risiko tinggi, sementara CSRF dan validasi upload file masuk kategori sedang. Untuk memitigasi risiko tersebut, penelitian ini merekomendasikan penerapan validasi input, output encoding, penggunaan prepared statement, penambahan Content Security Policy (CSP), penerapan token CSRF, serta mekanisme autentikasi berlapis seperti multi-factor authentication dan account lockout.

Penelitian ini berkontribusi dengan memberikan rekomendasi praktis bagi pemerintah daerah dalam memperkuat ketahanan siber pada website layanan publik. Ke depan, penelitian dapat dikembangkan dengan melakukan uji keamanan yang lebih komprehensif menggunakan metode dynamic analysis atau red team testing untuk memperoleh gambaran lebih luas mengenai ancaman siber pada sistem pemerintahan.

Referensi

[1] Ali, A. A. Gani, and M. I. Zainal, "Cybersecurity Threats and Countermeasures in Digital Government: A Systematic Literature Review," Journal of Information Security, vol. 14, no. 2, pp. 45–59, 2023. doi: 10.4236/jis.2023.142004.

[2] M. S. H. Rahman, M. Hossain, and M. I. Hoque, "SQL Injection Attack Detection and Prevention Techniques: A Review," Security and Privacy, vol. 4, no. 3, pp. 1–14, 2021. doi: 10.1002/spy2.126.

[3] K. A. Mahmood, R. A. Shaikh, and M. Ahmed, "A Review of Cross Site Scripting (XSS) Attack and Defense Mechanisms," in Proc. 2020 Int. Conf. Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, pp. 145–150, 2020. doi: 10.1109/ICCWS51030.2020.00028.

[4] B. A. Latif, M. A. M. Isa, and S. M. M. Shah, "A Comparative Study on Web Application Vulnerabilities: SQL Injection and XSS," Journal of ICT Research and Applications, vol. 17, no. 1, pp. 89–104, 2023. doi: 10.5614/itbj.ict.res.appl.2023.17.1.6.

[5] Z. Alharbi and N. Khan, "Cyber Resilience: A Review and Research Agenda," Computers & Security, vol. 105, pp. 102–123, 2021. doi: 10.1016/j.cose.2021.102238.

[6] J. Smith and L. Zhang, "Understanding Cybersecurity and Cyber Resilience in Modern Information Systems," IEEE Access, vol. 9, pp. 124337–124350, 2021. doi: 10.1109/ACCESS.2021.3108698.

[7] T. T. Nguyen, "A Survey on Web Application Security: SQLi and XSS Attacks," International Journal of Advanced Computer Science and Applications, vol. 12, no. 6, pp. 398–405, 2021. doi: 10.14569/IJACSA.2021.0120648.

[8] K. A. Kurniawan, A. Nugroho, and D. Wulandari, "Implementasi Penetration Testing Metode Black Box untuk Mengetahui Keamanan Website Pemerintahan," Jurnal Ilmiah Teknologi Informasi Asia, vol. 15, no. 2, pp. 101–110, 2022. doi: 10.37253/jtia.v15i2.574.

[9] F. Yusuf, "Metode Vulnerability Assessment dalam Mengetahui Kerentanan Sistem Website: Studi Kasus E-Gov," Jurnal Teknik Informatika dan Sistem Informasi (JuTISI), vol. 9, no. 1, pp. 57–64, 2023. doi: 10.30596/jutisi.v9i1.12963.

[10] R. Anwar and S. R. Putri, "Analisis SQL Injection pada Sistem Informasi Akademik Menggunakan Metode White Box Testing," Jurnal Teknologi dan Sistem Komputer, vol. 12, no. 2, pp. 180–186, 2024. doi: 10.14710/jtsiskom.2024.180.

[11] M. Alshaer, A. Shaaban, and R. Alsaqour, "Advanced Techniques for Detecting and Preventing SQL Injection Attacks: A Comprehensive Survey," IEEE Access, vol. 10, pp. 12345–12362, 2022.

[12] S. Kumar, R. R. Singh, and P. K. Singh, "An Efficient Detection and Prevention Model for Cross-Site Scripting (XSS) Attacks," IEEE Transactions on Information Forensics and Security, vol. 17, no. 4, pp. 975–984, Apr. 2022.

[13] Y. Zhang, J. Li, and X. Liu, "Cyber Resilience Framework for Critical Infrastructure: A Survey and Future Directions," IEEE Transactions on Industrial Informatics, vol. 18, no. 2, pp. 789–799, Feb. 2022.

[14] M. G. B. Sitorus, N. Maria, and Y. N. Safa, "Tinjauan literatur manajemen risiko cyber dalam proyek: Identifikasi, evaluasi, dan mitigasi ancaman," Jurnal Manajemen Informatika (JAMIKA), vol. 14, no. 2, pp. 187–198, 2024. doi: 10.34010/jamika.v14i2.12887.