BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin maju, memastikan keamanan siber menjadi prioritas utama bagi layanan berbasis web guna melindungi data pengguna dan mencegah ancaman siber yang dapat merugikan masyarakat luas. Pemerintah Kabupaten Jombang melalui inovasi teknologi menghadirkan platform website "SAMBANG" sebagai sarana pelayanan publik berbasis digital. Website ini dirancang untuk mempermudah masyarakat dalam mengakses informasi dan layanan administrasi secara online. Namun, Ancaman terhadap keamanan data dan kerahasiaan informasi meningkat seiring dengan peningkatan penggunaan teknologi ini, seperti peretasan sistem, pencurian identitas, dan serangan ransomware, menjadi tantangan krusial yang harus segera diatasi. Website "SAMBANG" merupakan singkatan dari Sistem Administrasi Berbasis Digital Jombang, yang mencakup berbagai layanan seperti pengurusan dokumen administrasi, pendaftaran layanan publik, hingga penyediaan informasi umum terkait kebijakan pemerintah daerah. Website ini telah membantu ribuan warga Jombang dalam mengurangi birokrasi manual yang sering memakan waktu. Selain itu, platform ini juga mempercepat proses pelayanan, sehingga masyarakat dapat mengakses layanan dengan lebih efisien. Namun, di sisi lain, kehadiran website ini juga menjadi target potensial bagi para peretas (hacker) yang ingin mengeksploitasi celah keamanan (bug) untuk memperoleh akses tidak sah ke sistem tersebut.

Ancaman keamanan yang dihadapi website 'SAMBANG' sejalan dengan tren global di mana sistem pemerintahan kerap menjadi sasaran serangan siber yang berpotensi mengganggu layanan publik. Fenomena serangan siber yang mengancam sistem pemerintahan bukanlah hal baru. Menurut laporan Badan Siber dan Sandi Negara (BSSN) pada tahun 2023, tercatat lebih dari 1.000 insiden siber yang menyerang situs web pemerintah

di Indonesia. Mayoritas serangan ini memanfaatkan kelemahan pada sistem keamanan website, seperti injeksi SQL (SQL injection), serangan lintas situs (cross-site scripting), dan pengambilan alih sesi pengguna (session hijacking) [2]. Tidak terkecuali, potensi ancaman ini juga dapat mengancam integritas dan kerahasiaan data pada website "SAMBANG." Pada tahun 2022, sebuah insiden serangan terhadap platform serupa di daerah lain menunjukkan dampak buruk yang signifikan. Data pribadi ribuan pengguna terekspos, yang menyebabkan kerugian material maupun imaterial bagi masyarakat. Kondisi ini menimbulkan urgensi untuk memastikan bahwa sistem "SAMBANG" dirancang agar tidak terdapat kerentanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang. Oleh karena itu, diperlukan penelitian mendalam untuk menganalisis bug atau kerentanan keamanan pada website ini. Analisis terhadap bug pada website "SAMBANG" memiliki relevansi tinggi untuk mendukung keamanan sistem informasi di Kabupaten Jombang. Dengan memahami kelemahan yang ada, langkah mitigasi dapat dirancang untuk mencegah eksploitasi oleh pihak eksternal. Penelitian ini juga bertujuan untuk meningkatkan kesadaran akan pentingnya praktik keamanan siber dalam pengembangan platform layanan digital pemerintah. Tanpa upaya proaktif dalam mengidentifikasi dan memperbaiki bug, potensi ancaman seperti pencurian data pribadi, defacing website, hingga serangan *denial-of-service* (DoS) dapat berdampak serius pada kepercayaan publik terhadap layanan pemerintah [5].

```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 1. 1 *Coding SQL Injection*

Lebih lanjut, fenomena global menunjukkan bahwa ancaman terhadap keamanan siber tidak hanya datang dari individu dengan keterampilan teknis tinggi, tetapi juga dari perangkat otomatis seperti serangan botnet Mirai pada tahun 2016 berhasil mengeksploitasi kelemahan perangkat IoT dan melumpuhkan berbagai layanan internet utama, termasuk sistem pemerintahan dan perusahaan besar. Botnet semacam ini secara sistematis memindai dan menyerang celah keamanan pada website, berpotensi menyebabkan gangguan serius terhadap layanan digital [12]. Hal ini menjadikan identifikasi bug sebagai langkah penting dalam mencegah serangan yang dapat merusak sistem "SAMBANG." Dalam konteks Kabupaten Jombang, dampak dari keamanan website yang terabaikan dapat meluas hingga pada aspek sosial dan ekonomi. Sebagai contoh, jika data pribadi pengguna terekspos, hal ini tidak hanya akan merusak reputasi pemerintah daerah, tetapi juga dapat menyebabkan kerugian keuangan akibat penyalahgunaan data. Selain itu, serangan terhadap sistem dapat mengganggu operasional layanan publik yang pada akhirnya mempengaruhi kenyamanan masyarakat dalam mengakses layanan administratif.

Salah satu permasalahan utama yang dapat ditemukan adalah kerentanan terhadap serangan siber. Beberapa jenis serangan yang sering terjadi antara lain SQL Injection, yang memungkinkan penyerang menyisipkan kode berbahaya ke dalam kueri database; Cross-Site Scripting

(XSS), yang memanfaatkan celah dalam aplikasi web untuk menyuntikkan skrip berbahaya yang dapat dieksekusi di browser pengguna; serta Cross-Site Request Forgery (CSRF), yang memanipulasi pengguna agar melakukan tindakan yang tidak diinginkan tanpa sepengetahuan mereka [1]. Serangan-serangan ini terjadi karena adanya kelemahan dalam kode atau konfigurasi sistem, yang dapat dieksploitasi oleh penyerang. Selain itu, kelemahan dalam autentikasi dan otorisasi pengguna dapat menyebabkan akses tidak sah ke informasi sensitif, sehingga meningkatkan risiko kebocoran data. Kurangnya enkripsi dalam komunikasi data antara pengguna dan server juga dapat meningkatkan kemungkinan serangan man-in-the-middle, di mana peretas dapat menghentikan dan mengubah data yang dikirim [6]. Tidak adanya sistem pemantauan keamanan yang memadai dapat membuat ancaman keamanan sulit terdeteksi secara dini, sehingga memungkinkan eksploitasi berlangsung dalam jangka waktu yang lama sebelum ditemukan. Kesalahan konfigurasi pada server web, seperti penggunaan default credential atau kebijakan akses yang tidak ketat, juga menjadi faktor yang sering diabaikan namun memiliki dampak besar terhadap keamanan sistem. Penelitian ini memiliki tujuan utama untuk menganalisis bug pada celah keamanan website "SAMBANG" Kabupaten Jombang dengan pendekatan teknis dan metodologi yang komprehensif. Beberapa aspek yang akan dikaji meliputi jenis-jenis bug yang ditemukan, tingkat risiko yang ditimbulkan, serta strategi mitigasi yang dapat diterapkan untuk meningkatkan keamanan sistem. Diharapkan penelitian ini dapat membantu meningkatkan kualitas sistem informasi pemerintah daerah, khususnya dalam hal keamanan siber. Melalui kajian yang mendalam, penelitian ini diharapkan dapat menghasilkan rekomendasi praktis yang relevan bagi pengelola website "SAMBANG."

```php
<?php
// Tangkap input dari form atau URL
$name = $_GET['name'] ?? 'Tamu';
?>

<!DOCTYPE html>
<html>
<head>
    <title>Selamat Datang</title>
</head>
<body>
    <h1>Halo, <?php echo $name; ?>!</h1>
</body>
</html>
http://localhost/xss.php?name=<script>alert('XSS!')</script>
```

Gambar 1. 2 *Coding XSS Attack*

Evaluasi parameter yang diuji dalam analisis keamanan website "SAMBANG" Kabupaten Jombang melibatkan berbagai aspek teknis dan operasional. Evaluasi ini bertujuan untuk mengidentifikasi serta memperbaiki celah keamanan yang ada, sehingga sistem dapat beroperasi dengan lebih aman dan terhindar dari potensi serangan siber. Proses ini mencakup pengujian terhadap konfigurasi sistem, validasi input, enkripsi data, serta mekanisme otentikasi dan otorisasi pengguna. Salah satu parameter utama yang diuji adalah kerentanan aplikasi web, yang mencakup pengujian terhadap ancaman umum seperti SQL Injection. Penerapan serta pengembangan kebijakan keamanan yang ketat diperlukan untuk memastikan seluruh pihak terkait memahami sekaligus mematuhi standar keamanan yang telah ditetapkan [2]. Sosialisasi dan pelatihan rutin bagi staf pengelola website juga perlu dilakukan agar mereka memiliki pemahaman yang baik tentang praktik keamanan siber. Selain itu, penelitian ini juga berperan sebagai upaya preventif untuk meminimalisir risiko serangan siber yang dapat berdampak negatif pada masyarakat. Dengan demikian, keamanan website "SAMBANG" tidak hanya menjadi tanggung jawab teknis semata, tetapi juga menjadi bagian dari komitmen pemerintah Kabupaten Jombang dalam memberikan pelayanan terbaik bagi masyarakat. Secara keseluruhan, penelitian ini bermanfaat dalam tiga aspek utama: meningkatkan keamanan website "SAMBANG", memperkuat kepercayaan masyarakat terhadap layanan digital pemerintah, dan mendukung pengembangan kebijakan keamanan siber di tingkat daerah. Dengan demikian, penelitian ini tidak

hanya bersifat teknis, tetapi juga strategis dalam mendukung transformasi digital yang aman dan berkelanjutan di Kabupaten Jombang. Mengacu pada uraian latar belakang yang telah dijelaskan, peneliti merancang penelitian berjudul "*Analisis Risiko dan Strategi Perlindungan Sistem terhadap Ancaman Siber pada Website 'SAMBANG' kabupaten Jombang"*

1.2 Rumusan Masalah

Mengacu uraian latar belakang tersebut, peneliti menyusun rumusan masalah berupa:

a. Bagaimana risiko keamanan yang diakibatkan oleh bug yang ditemukan pada website 'SAMBANG' dalam konteks ancaman siber, seperti serangan SQL Injection dan Cross-Site Scripting (XSS)?
b. Langkah-langkah mitigasi apa yang dapat diterapkan untuk memperbaiki bug atau celah keamanan yang ditemukan pada website 'SAMBANG', seperti penerapan input validation untuk mencegah SQL Injection dan penggunaan Content Security Policy (CSP) untuk mengurangi risiko Cross-Site Scripting (XSS)?

1.3 Tujuan Penelitian

Mengacu rumusan masalah yang telah dirumuskan, tujuan penelitian ini meliputi:

a. Menganalisis risiko keamanan yang ditimbulkan oleh bug yang ditemukan pada website *SAMBANG* dalam konteks ancaman siber, khususnya serangan SQL Injection dan Cross-Site Scripting (XSS).
b. Mengidentifikasi dan merumuskan langkah-langkah mitigasi yang efektif untuk memperbaiki bug atau celah keamanan pada website *SAMBANG*, seperti penerapan *input validation* untuk mencegah SQL Injection dan penggunaan *Content Security Policy* (CSP) untuk mengurangi risiko Cross-Site Scripting (XSS).

1.4 Batasan Masalah

Pembatasan masalah berikut disusun guna memastikan penelitian berjalan secara terarah dan tidak meluas:

1. Ruang lingkup sistem yang dianalisis terbatas pada website *SAMBANG* milik Pemerintah Kabupaten Jombang, khususnya pada aspek keamanan aplikasi web yang berkaitan dengan akses pengguna dan pengelolaan data layanan publik digital.
2. Jenis ancaman siber yang dianalisis berfokus pada serangan umum yang terjadi pada aplikasi web, seperti:
   a) SQL Injection
   b) Cross-Site Scripting (XSS)
   c) (Opsional) Cross-Site Request Forgery (CSRF), jika ditemukan indikasi dalam proses audit keamanan.
3. Analisis keamanan hanya mencakup identifikasi bug atau celah keamanan yang dapat dimanfaatkan oleh individu yang tidak berwewenang, tanpa melakukan eksploitasi aktif atau simulasi serangan siber secara merusak (non-destructive testing).
4. Strategi perlindungan yang dikaji meliputi rekomendasi teknis dan prosedural, seperti penerapan validasi input, penggunaan header keamanan (misalnya CSP), penguatan autentikasi, serta konfigurasi sistem yang lebih aman. Namun, tidak membahas secara mendalam implementasi arsitektur keamanan jaringan (seperti firewall, IDS/IPS, atau VPN).
5. Pendekatan teknis dalam penelitian ini dilakukan melalui metode analisis kerentanan (vulnerability assessment) dan kajian literatur terkait praktik terbaik (best practices) dalam keamanan aplikasi web, dengan studi kasus terbatas pada struktur dan fitur website *SAMBANG* yang dapat diakses publik (client-side).
6. Penelitian tidak mencakup audit keamanan fisik, keamanan internal jaringan pemerintah, maupun kebijakan manajemen risiko secara

menyeluruh dalam struktur organisasi Pemerintah Kabupaten Jombang

1.5 Manfaat Penelitian

1.5.1 Manfaat Teoritis

Diharapkan penelitian ini dapat berperan dalam memperkaya literatur dan pengembangan ilmu di bidang keamanan siber, khususnya dalam konteks analisis kerentanan pada aplikasi web layanan publik. Temuan dari penelitian ini dapat memperkaya literatur ilmiah mengenai identifikasi bug dan celah keamanan, serta strategi mitigasi yang relevan untuk mencegah eksploitasi oleh pihak tidak bertanggung jawab. Penelitian ini juga diharapkan dapat dijadikan acuan dalam pengembangan teori dan penyusunan model evaluasi keamanan sistem informasi publik berbasis web, khususnya dalam penerapan prinsip-prinsip keamanan aplikasi pada instansi pemerintahan daerah.

1.5.2 Manfaat Praktis

Dari sisi praktis, penelitian ini bermanfaat bagi:

1. Pengelola sistem informasi pemerintah daerah, khususnya tim pengembang dan administrator website "SAMBANG", dalam memahami risiko keamanan yang mungkin timbul akibat bug atau celah pada sistem, serta langkah-langkah mitigasi yang dapat diterapkan untuk memperkuat perlindungan data dan layanan.
2. Pemerintah Kabupaten Jombang, sebagai referensi dalam meningkatkan kualitas dan keandalan layanan publik berbasis digital, serta dalam merumuskan kebijakan keamanan siber yang lebih komprehensif.
3. Pengembang aplikasi web dan profesional IT, sebagai acuan dalam melakukan pengujian keamanan (security testing), serta

penerapan praktik terbaik (best practices) dalam membangun sistem informasi yang aman dari ancaman siber.

4. Mahasiswa dan peneliti, sebagai sumber referensi awal untuk melakukan penelitian lanjutan dalam bidang keamanan aplikasi web, serta pengembangan sistem informasi publik yang aman, adaptif, dan berkelanjutan

UNIVERSITAS MUHAMMADIYAH MALANG