VULNERABILITY ANALYSIS ON SEMARANG CITY ROAD SECTION INFORMATION SYSTEM WEBSITE USING VAPT METHOD

ANALISIS KERENTANAN PADA WEBSITE SISTEM INFORMASI RUAS JALAN KOTA SEMARANG MENGGUNAKAN METODE VAPT

Hanif Setia Nusantara[1], L. Budi Handoko[2], Maulana Ikhsan[3], Chaerul Umam[4]
[124]Universitas Dian Nuswantoro, Jl. Imam Bonjol No.207, Kota Semarang
[3]Dinas Pekerjaan Umum Kota Semarang, Jl. Madukoro Raya No.7, Kota Semarang
haniftara18@gmail.com[1], handoko@dsn.dinus.ac.id[2], maulanaikhsan1995@gmail.com[3], chaerul@dsn.dinus.ac.id

Abstract *- Web-based public service applications in the digital governance era are increasingly vulnerable to cyber threats. This study analyzes the vulnerability of the Semarang City Road Information System website quantitatively using the Vulnerability Assessment and Penetration Testing (VAPT) method to evaluate its effectiveness in identifying security gaps. This system is part of an e-government service providing road infrastructure information but, like other technology-based systems, is susceptible to exploitation. The VAPT method used includes two main stages: Vulnerability Assessment to identify weaknesses and Penetration Testing to simulate attacks. The study identified 5 potential vulnerabilities: SQL Injection, Credit Card Number Disclosure, Insecure Direct Object Reference (IDOR), Cross-Site Scripting (XSS), and Error Message on Page. However, 80% of these were false positives, effectively filtered by Alibaba Cloud's Web Application Firewall (WAF). The IDOR vulnerability was confirmed as valid, allowing unauthorized access to sensitive data through manipulation of the ID parameter in the URL. The original contribution of this research is the specific recommendation for implementing Indirect Object References mechanisms such as ID encryption, as well as emphasizing the need for comprehensive routine testing to improve security and prevent potential data misuse.*

Keywords *– Cybersecurity, Vulnerabilities, Information System, VAPT, e-Government*

Abstrak - Aplikasi layanan publik berbasis web di era tata kelola digital semakin rentan terhadap ancaman siber. Penelitian ini bertujuan untuk menganalisis kerentanan website Sistem Informasi Ruas Jalan Kota Semarang secara kuantitatif menggunakan metode Vulnerability Assessment and Penetration Testing (VAPT) untuk menilai efektivitasnya dalam identifikasi kerentanan. Sistem ini merupakan bagian dari layanan e-government yang menyediakan informasi mengenai kondisi infrastruktur jalan, namun seperti halnya sistem berbasis teknologi lainnya, sistem ini rentan dieksploitasi pihak yang tidak bertanggung jawab. Metode VAPT yang digunakan dalam penelitian ini mencakup dua tahap utama, yaitu Vulnerability Assessment untuk mengidentifikasi kerentanan, dan Penetration Testing untuk mensimulasikan serangan terhadap sistem. Hasil penelitian menujukkan 5 potensi kerentanan: SQL Injection, Credit Card Number Disclosed, Insecure Direct Object Reference (IDOR), Cross Site Scripting (XSS), dan Error Message on Page. Namun, 80% di antaranya adalah *false positive* yang efektif difilter oleh Web Application Firewall (WAF) Alibaba Cloud. Kerentanan IDOR terkonfirmasi valid dan krusial, memungkinkan akses ke data sensitif melalui manipulasi parameter ID pada URL. Kontribusi orisinal dalam penelitian ini adalah rekomendasi spesifik penerapan mekanisme *Indirect Object References* seperti enkripsi ID, serta penekanan pada pengujian rutin secara komprehensif terhadap sistem untuk memperbaiki keamanan dan mencegah potensi penyalahgunaan data.

Kata Kunci – Keamanan Siber, Kerentanan, Sistem Informasi, VAPT, e-Government

I. PENDAHULUAN

Era digital membawa transformasi besar dalam tata kelola pemerintahan dan pelayanan publik. Penggunaan teknologi informasi khususnya melalui penerapan e-government, telah meningkatkan efisiensi, aksesibilitas, dan kualitas pelayanan publik[1]. Pemerintah Kota Semarang misalnya, telah mengimplementasikan sistem informasi ruas jalan sebagai bagian dari e-government untuk menyediakan data infrastruktur jalan kepada masyarakat. Namun, meskipun menawarkan kemudahan dan transparansi, sistem berbasis web ini juga memiliki kelemahan, khususnya terhadap ancaman siber yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab[2]. Kondisi ini menyebabkan rawannya pencurian data sensitif yang dapat diakses oleh pihak luar yang tidak berkepentingan. Untuk mengatasi permasalahan ini, diperlukan identifikasi dan analisis kerentanan secara mendalam pada Sistem Informasi Ruas Jalan Kota Semarang. Penelitian dilakukan dengan menggunakan metode VAPT (Vulnerability Assessment and Penetration Testing). VAPT dipilih karena kemampuannya dalam menyajikan evaluasi dalam dua dimensi. Vulnerability Assessment (VA) untuk mengidentifikasi kerentanan secara sistematis, Penetration Testing (PT) untuk simulasi serangan secara nyata, guna menguji keamanan suatu sistem.

Salah satu gap yang ingin diisi oleh penelitian ini adalah belum adanya studi secara spesifik dalam mengidentifikasi kerentanan pada sistem e-government dengan fokus pada infrastruktur jalan, khususnya di kota besar Indonesia. Penelitian-penelitian sebelumnya lebih banyak berfokus pada website universitas atau perusahaan, seperti yang dilakukan oleh[3] yang berjudul "Analisis Celah Keamanan Pada Aplikasi Web E-Learning Universitas ABC Dengan Menggunakan Metode VAPT menunjukkan bahwa metode VAPT diterapkan dalam proses menganalisis celah keamanan pada lingkup universitas. Selain itu penelitian yang dilakukan oleh[4] berjudul "Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode VAPT yang merupakan penerapan metode VAPT dalam analisis keamanan pada tingkat perusahaan. Meskipun demikian, aplikasi sistem informasi e-government memiliki karakteristik yang lebih kompleks karena melibatkan data publik dan interaksi dengan masyarakat luas. Penelitian ini memberikan kontribusi yang berbeda dengan menyoroti sistem informasi yang digunakan untuk mengelola data infrastruktur jalan kota besar, yang belum banyak diteliti sebelumnya.

Tujuan dari penelitian ini adalah untuk memberikan kontribusi nyata dalam mengevaluasi tingkat kerentanan keamanan pada website Sistem Informasi Ruas Jalan milik Pemerintah Kota Semarang dengan pendekatan VAPT. Penelitian ini berfokus pada upaya mengidentifikasi kerentanan yang mungkin dimanfaatkan oleh pihak tidak bertanggung jawab, serta menyusun rekomendasi mitigasi secara spesifik yang dapat diterapkan. Dengan demikian, diharapkan sistem informasi tersebut dapat lebih aman, menjaga integritas data penting milik pemerintah, serta memastikan pelayanan publik berbasis digital tetap berjalan dengan aman dan nyaman. Temuan dalam penelitian ini juga diharapkan menjadi bahan evaluasi yang berguna bagi tim pengembang dalam memperkuat keamanan sistem informasi pemerintah, khususnya yang menyangkut infrastruktur strategis dan layanan publik, di tengah ancaman siber yang semakin kompleks.

II. SIGNIFIKASI STUDI

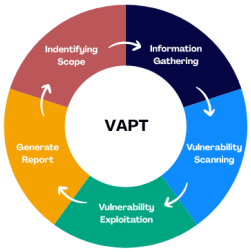
A. Studi Literatur

Penelitian terdahulu oleh [3] menunjukkan bahwa aplikasi e-learning Universitas ABC memiliki sejumlah kerentanan yang teridentifikasi melalui VAPT. Penelitian ini menggunakan alat pemindaian kerentanan Nessus untuk melakukan vulnerability scanning, yang menghasilkan daftar kerentanan dengan berbagai tingkat keparahan, mulai dari rendah, sedang, hingga kritis. Namun, peneliti hanya menganalisis dan melakukan penlilaian pada kerentanan tersebut secara garis besar, tanpa ada validasi manual secara mendalam terhadap kerentanan yang ditemukan. Selanjutnya penelitian lainnya oleh[4] menunjukkan bahwa website CV. Kazar Teknologi Indonesia memiliki sejumlah kerentanan yang teridentifikasi melalui metode VAPT. Penelitian ini menggunakan alat pemindaian seperti Nessus, OpenVAS, OWASP ZAP, dan WPScan, yang menghasilkan total 42 kerentanan dengan rincian berbagai tingkat keparahan, seperti kerentanan kritis (High), sedang (Medium), dan rendah (Low). Namun, peneliti juga tidak melakukan validasi manual secara mendalam melainkan hanya memberikan solusi secara umum terhadap kerentanan tersebut, tidak secara spesifik. Oleh karena itu, penelitian ini dilakukan guna mengisi kekurangan dari penelitian terdahulu dengan melakukan validasi manual pada setiap kerentanan yang terdeteksi, selanjutnya penelitian ini juga memberikan mitigasi secara spesifik seperti penerapan *Indirect Object References* dengan cara enkripsi ID, sehingga id tidak mudah ditebak oleh pihak luar yang tidak berkepentingan.

Berdasarkan penelitian terdahulu, dapat disimpulkan bahwa penelitian ini penting karena fokus pada keamanan sistem informasi yang mengelola data publik dan infrastruktur kritis yang sering kali terabaikan dalam studi-studi sebelumnya yang lebih mengutamakan sektor swasta atau aplikasi yang lebih terbatas. Penelitian ini memberikan implikasi praktis yang jelas, terutama bagi kebijakan Dinas Pekerjaan Umum dengan menawarkan solusi mitigasi yang dapat diterapkan untuk memperkuat sistem dan mencegah potensi ancaman siber yang dapat mengganggu kelancaran layanan publik. Selain itu, penelitian oleh[5] menyoroti bahwa meskipun banyak penelitian e-government berfokus pada adopsi dan pengembangan, aspek keamanan siber internal dalam layanan e-government masih kurang diperhatikan. Hal ini menunjukkan bahwa penelitian ini mengisi kekosongan dalam literatur yang ada, di mana sebagian besar studi sebelumnya lebih berfokus pada keamanan data internal pada sistem perusahaan atau aplikasi e-learning. Dengan demikian, penelitian ini menjawab kebutuhan untuk mengkaji kerentanannya dalam konteks e-government, yang memiliki dampak jauh lebih besar terhadap keamanan data publik dan operasional pemerintahan.

B. Metode Penelitian

VAPT adalah metodologi dengan proses bertahap untuk melakukan pengujian keamanan suatu sistem aplikasi atau jaringan [6]. VA merupakan proses scanning suatu sistem aplikasi atau jaringan untuk mengetahui adanya kelemahan dan celah didalamnya, sedangkan Penetration Testing (PT) yaitu langkah setelah dilakukannya VA)untuk melakukan percobaan mengeksploitasi sistem atau jaringan secara resmi bertujuan mengetahui kemungkinan eksploitasi dalam sistem [7]. VAPT juga dapat melacak langkah-langkah keamanan apa yang sudah ada dan memindai jaringan untuk kerentanan berdasarkan tujuan[8]. VAPT memiliki 5 tahapan diantaranya *Identifying Scope, Information Gathering, Vulnerability Scanning, Vulnerability Exploitation,* dan *Generate Report* [3] Gambaran dari metode penelitian ini akan ditunjukkan pada Gambar 1.



Gambar 1. Metode VAPT

1. Identifying Scope

Identifying scope merupakan langkah fundamental dan pertama dalam metode VAPT, berfungsi untuk menentukan ruang lingkup pengujian yang bertujuan untuk membatasi objek yang akan diuji agar fokus dan terarah [9]. Peran utamanya adalah untuk menetapkan batasan atau ruang lingkup pengujian keamanan secara jelas dan sistematis.

2. Information Gathering

Information gathering ini merupakan tahapan untuk mengumpulkan data secara sistematis terkait sistem target, yang menjadi dasar bagi identifikasi kerentanan selanjutnya. Information Gathering adalah proses mencari informasi atau mengumpulkan data dari berbagai sumber untuk tujuan tertentu, seperti analisis, investigasi, atau perencanaan[10]. Informasi yang terkumpul ini membentuk fondasi bagi semua tahapan penelitian berikutnya.

3. Vulnerability Scanning

Vulnerability Scanning dilakukan dengan teknik *Automated Scanning*. Teknik ini dipilih karena untuk memudahkan proses penelitian dalam efisiensi waktu serta mendapatkan akurasi yang baik. Dalam proses ini tools yang digunakan adalah Acunetix Vulnerability Scanner, merupakan sebuah tools yang dapat membantu mengidentifikasi kerentanan aplikasi web dengan akurasi tinggi [11].

4. Vulnerability Exploitation

Vulnerability Exploitation merupakan suatu tahapan pada *Penetration Testing* yang bertujuan untuk menguji kerentanan yang telah ditemukan benar-benar dapat di eksploitasi oleh penyerang berdasarkan hasil dari daftar kerentanan yang diberikan pada proses sebelumnya [12]. Tahap ini juga berfungsi untuk memvalidasi kerentanann yang digunakan untuk melihat apakah kerentan tersebut dapat dieksploitasi untuk mendapatkan informasi data sensitif.

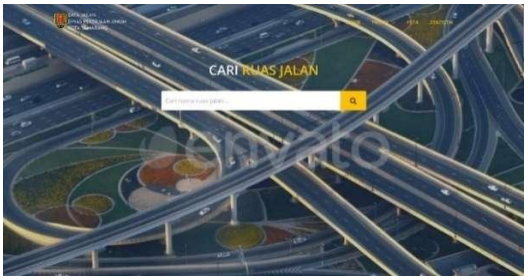
5. Generate Report

Tahap terakhir dalam metode ini adalah melakukan Generate Report, merupakan proses pembuatan laporan yang berisi tentang kerentanan pada aplikasi Website Sistem Informasi Ruas Jalan Kota Semarang [13].

III. HASIL DAN PEMBAHASAN

1. Identifying Scope

Pada penelitian ini pengujian akan difokuskan pada Aplikasi Website Sistem Informasi Ruas Jalan Kota Semarang, dimana website ini digunakan oleh Masyarakat Kota Semarang untuk mencari informasi terkait detail ruas jalan, kondisi jalan, serta ujung jalan dan pangkal jalan. Lingkup dari pengujian ini adalah berbagai kerentanan yang ada pada aplikasi website tersebut. Berikut merupakan tampilan dari aplikasi website tersebut.

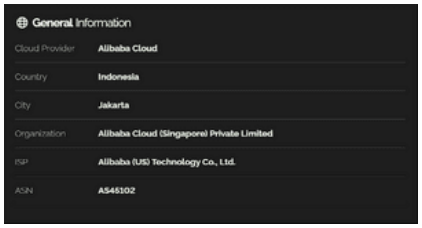


Gambar 2. Tampilan Halaman Utama Website

Dalam konteks penelitian ini, ruang lingkup pengujian akan terbatas pada analisis kerentanan yang ada pada aplikasi web tersebut. Fokus utama dari pengujian ini adalah untuk mengevaluasi kerentanan yang berpotensi di salah gunakan oleh pihak yang tidak bertanggung jawab untuk mendapatkan akses tidak sah atau merusak data sensitif.

2. Information Gathering

Information Gathering merupakan proses yang cukup penting dalam menggali informasi secara umum terkait target yang akan di uji. Pada tahap ini tools yang digunakan ada 3 diantaranya Shodan.io, NsLookup, dan Wappalyzer.



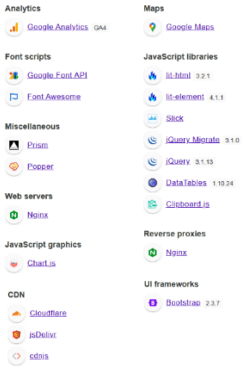
Gambar 3. Tools Shodan.io

Pada gambar diatas Shodan.io memberikan beberapa informasi seperti cloud provider yang digunakan, negara, kota, organisasi, ISP (Internet Service Provider), dan ASN (Autonomous System Number). Informasi diatas merupakan informasi yang penting untuk mengetahui target yang sedang diuji.

Gambar 4. Tools NsLookup

Selanjutnya NsLookup memberikan beberapa informasi penting diantaranya, domain utama jalanpu.semarangkota.go.id diarahkan ke layanan Aliyun WAF (Web Application Firewall) milik Alibaba Cloud dengan caonical name (CNAME) all.semarangkota.go.id.e.aliyunwaf.com yang merupakan subdomain khusus untuk layanan Alibaba Cloud WAF yang bertujuan untuk melindungi

dari serangan seperti DDoS, SQL Injection dan lain-lain. Selanjutnya kita dapat memperoleh informasi mengenai IP Adress yaitu 8.215.155.8 yang merupakan ip publik milik Alibaba Cloud.

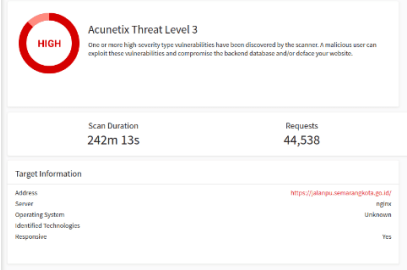


Gambar 5. Tools Wappalyzer

Tools Wappalyzer merupakan sebuah tools yang dapat memberikan informasi terkait teknologi-teknologi yang digunakan dalam sebuah website. Beberapa informasi yang dapat diperoleh adalah seperti pada gambar diatas.

3. Vulnerability Scanning

Pada tahap ini dilakukan Vulnerability Scanning untuk mencari beberapa kerentanan pada Website Sistem Informasi Ruas Jalan Kota Semarang dengan teknik Automated Scanning menggunakan tools Acunetix Vulnerability Scanner. Dimana hasil dari Vulnerability scanning pada aplikasi website tersebut dapat dilihat pada Gambar.



Gambar 6. Vulnerability Scanning dengan Tools Acunetix

Vulnerability Scanning berjalan selama 242 menit 13 detik dengan memproses 44.538 request. Proses ini menghasilkan beberapa daftar kerentanan yang terdeteksi oleh Acunetix Vulnerability Scanner pada teknik Automated Scanning, diantaranya seperti pada tabel dibawah.

TABEL I
DAFTAR KERENTANAN WEBSITE

No	Vulnerability	Base Score	Vulnerability Level
1.	SQL Injection	10	Critical
2.	Credit Card Number Disclosed	7.5	High
3.	Insecure Direct Object Reference (IDOR)	7.3	High
4.	Cross Site Scripting (XSS)	5.3	Medium
5.	Error Message on Page	5.3	Medium

Setelah dilakukan proses Vulnerability Scanning beberapa kerentanan yang ada pada Website Sistem Informasi Ruas Jalan Kota Semarang diantaranya, SQL Injection, Insecure Direct Object Reference (IDOR), Credit Card Number Disclosed, Cross Site Scripting (XSS), dan Error Message on Page.

Tujuan dari Vulnerability Scanning ini adalah untuk mengidentifikasi kerentanan-kerentanan yang ada pada Website Sistem Informasi Ruas Jalan Kota Semarang. Dengan adanya proses vulnerability scanning maka dapat ditemukannya kerentanan yang beresiko tinggi atau mungkin bahkan sebuah *false positive* [14].

4. Vulnerability Exploitation

Pada daftar kerentanan yang telah didapatkan dari hasil Vulnerability Scanning, tahap ini merupakan proses untuk melakukan penetration testing dan validasi terhadap daftar kerentanan yang telah didapatkan. Proses ini merupakan sebuah identifikasi dan analisis secara mendalam guna memvalidasi suatu kerentanan atau termasuk kerentanan false *positive*. Berikut identifikasi yang dilakukan pada setiap kerentanan:

SQL Injection: Merupakan salah satu jenis serangan keamanan yang dilakukan dengan menyisipkan kode SQL berbahaya ke dalam input yang dimasukkan ke dalam aplikasi, yang kemudian dijalankan oleh server database [15]. Kerentanan SQL Injection terdapat pada bagian **“Cookie input acw_tc was set to 1À§Àȼ%2527%2522”** yang berarti Acunetix mencoba memasukkan payload **1À§Àȼ%2527%2522** pada cookie yang terdapat pada aplikasi website tersebut.

Gambar 7. Validasi SQL Injection

Percobaan injeksi payload kedalam aplikasi diterima, namun aplikasi langsung memutuskan koneksi dan mengembalikan return cookies seperti semula. Artinya, payload tidak berhasil dijalankan karena request tersebut telah di filter oleh WAF (Web Application Firewall) milik Alibaba Cloud. Hal ini mencegah SQL Injection berjalan. Ini disebabkan oleh, request hanya akan berjalan ketika input cookies **acw_tc** dimasukkan sesuai format dan tidak terdapat payload. Jadi, kerentanan SQL Injection pada aplikasi web tersebut merupakan sebuah kerentanan yang false positive.

Credit *Card Number Disclosed:* Merupakan suatu kerentanan dimana pada sebuah aplikasi terdapat informasi terkait nomor kartu kredit seseorang, baik secara sengaja maupun tidak sengaja. Kerentanan ini ditemukan pada **“The vulnerability affects https://jalanpu.semarangkota.go.id/jalan/detail/12142”** dengan keterangan **“Credit Card number found: 4355069220001”**. Setelah dilakukan analisa lebih mendalam untuk memvalidasi kerentan tersebut, ternyata kerentanan tersebut merupakan suatu *false positive.*

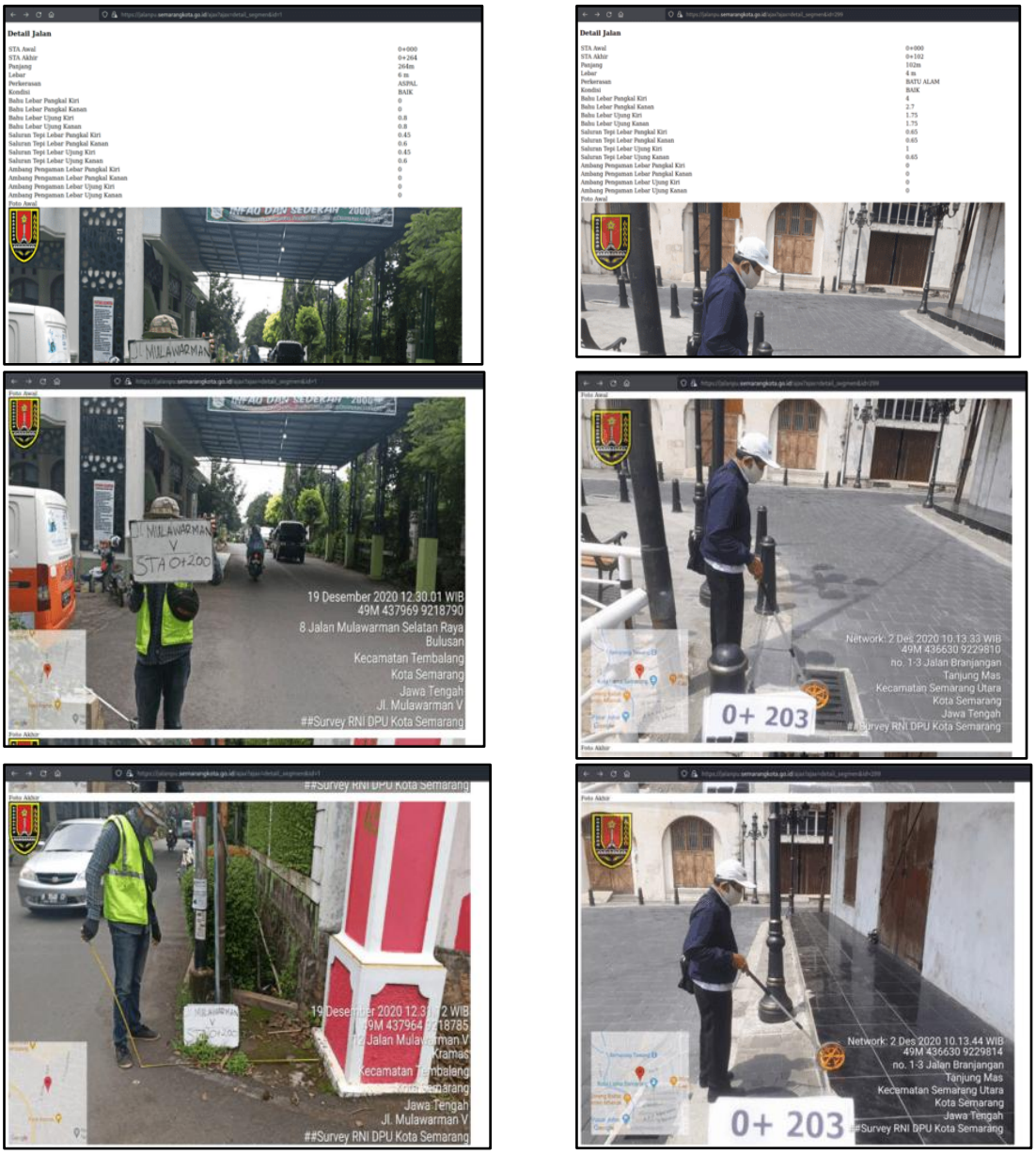
```
bounds = new google.maps.LatLngBounds();
                                    var i;

                                    var polygonCoords = [new
google.maps.LatLng(-7.012409312999978, 110.4355069220001),new
google.maps.LatLng(-7.012398084999973, 110.435534911),new
google.maps.LatLng(-7.012228512999969, 110.4356890810001),new
google.maps.LatLng(-7.012043801999937, 110.4358986220001),new
google.maps.LatLng(-7.011998264999932, 110.435949866),new
google.maps.LatLng(-7.011931459999971, 110.436014743),new
google.maps.LatLng(-7.011924381999961, 110.436018565),new
google.maps.LatLng(-7.01194161099994, 110.43647622200001),new
google.maps.LatLng(-7.011924381999961, 110.436018565),
                                    ];
```

Gambar 8. Validasi Credit Card Number Disclosed

Angka “4355069220001” yang dibaca oleh Acunetix Vulnerability Scanner sebagai kerentanan Credit Card Number Disclosed nyatanya bukan merupakan informasi sensitif terkait nomor kartu kredit, melainkan titik koordinat yang ada pada Google Maps API. Kode tersebut mendefinisikan koordinat-koordinat geografis (lintang dan bujur) yang membentuk poligon atau area tertutup pada suatu peta digital.

Insecure Direct Object Reference (IDOR): Merupakan suatu kerentanan yang terjadi ketika aplikasi web menggunakan input pengguna secara langsung untuk mengakses objek atau data sensitif, tanpa adanya kontrol akses yang memadai [16]. Kerentanan ini terdapat pada url **https://jalanpu.semarangkota.go.id/ajax?ajax=detail_segmen&id=1**. Memungkinkan pengguna mengakses data sensitif melalui manipulasi parameter id pada suatu url. Kerentanan ini merupakan kerentanan yang sah, dimana data sensitif yang seharusnya tidak ditampilkan kepada pengguna dapat di akses dengan mudah melalui url yang dapat dimanipulasi parameter id nya. Sebagai contoh ketika menuliskan id=1 maka data sensitif terkait detail jalan akan muncul, begitu pula dengan id yang lain. Berikut merupakan tampilan dari kerentanan IDOR yang terdapat pada aplikasi website sistem informasi ruas jalan kota semarang.



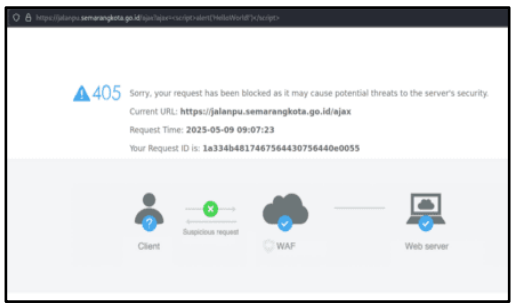
Gambar 9. (a) Kerentanan IDOR id=1 (b) Kerentanan IDOR id=299

Gambar diatas merupakan contoh kerentanan Insecure Direct Object Reference (IDOR) dimana pengguna bisa bebas mengakses data sensitif yang digunakan oleh website, yang seharusnya tidak ditampilkan pada sisi client. Url diatas merupakan salah satu data yang ditampilkan berdasarkan kita menuliskan id=1 dan id=299. Pada kerentanan Insecure Direct Object Reference (IDOR) yang ditemukan. Data tersebut berisi terkait detail jalan, foto jalan, informasi lokasi, dan tanggal pengambilan foto jalan.

Cross Site Scripting (XSS): Merupakan sebuah kerentanan di mana penyerang dapat menyisipkan skrip berbahaya (biasanya JavaScript) ke dalam aplikasi web yang akan dijalankan oleh pengguna lain [17]. Serangan ini dapat menyebabkan pencurian data, manipulasi konten, atau pengalihan pengguna ke situs web jahat [18]. Kerentanan XSS ditemukan pada bagian **"The vulnerability affects https://jalanpu.semarangkota.go.id/ajax"** dengan keterangan **"URL encoded GET input ajax was set to detail_segmen<WAVTAN>NBW6S[!+!]</WAVTAN>".** Acunetix Vulnerability Scanner mencoba menyisipkan payload XSS kedalam aplikasi web, namun web tersebut menampilkan respon seperti berikut

Gambar 10. (a) Validasi XSS 1 (b) Validasi XSS 2

Pada gambar diatas menunjukkan bahwa payload dari Acunetix Vulnerability Scanner tidak menghasilkan output kerentanan XSS, namun hanya menampilkan pesan error. Selanjutnya saya mencoba menyisipkan variasi payload lain dengan menggunakan payload XSS yang sangat umum seperti <script>alert('HelloWorld!')</script> menampilkan hasil seperti berikut



Gambar 11. Validasi XSS Payload 2

Aplikasi tersebut memunculkan pesan seperti di gambar, menunjukkan bahwa kita tidak dapat menyisipkan payload javascript ke dalam aplikasi website tersebut dikarenakan upaya upaya tersebut telah di filter oleh WAF (Web Application Firewall) milik Alibaba Cloud. Jadi, kerentanan Cross Site Scripting (XSS) pada Aplikasi Website Sistem Informasi Ruas Jalan merupakan *false positive*.

Error Message on Page: Error Message on Page adalah kondisi dimana aplikasi web menampilkan pesan kesalahan (error message) yang secara tidak sengaja mengandung informasi sensitive [19]. Pada kerentanan Error Message on Page Sistem Informasi Ruas Jalan Kota Semarang, ditemukan pada **"The vulnerability affects https://jalanpu.semarangkota.go.id/jalan/"** dengan keterangan **"Pattern found: Table 'jalanpu.tr_jalan' doesn't exist"** pesan tersebut menunjukkan bahwa Acunetix Vulnerability Scanner mencoba memanggil data pada tabel 'jalanpu.tr_jalan' namun, server merespons dengan 'Table 'jalanpu.tr_jalan' doesn't exist'

Gambar 12. Validasi Error Message on Page

Respons diatas menunjukkan bahwa tabel dengan nama 'jalanpu.tr_jalan' tidak ada. Oleh karena itu, kerentanan ini juga merupakan *false positive*.

Validasi manual menunjukkan bahwa IDOR adalah kerentanan yang paling berisiko, karena memungkinkan akses langsung ke data sensitif seperti detail jalan dan foto tanpa kontrol akses yang memadai. Sementara itu, meskipun pemindaian otomatis mendeteksi SQL Injection dan XSS, pengujian lebih lanjut menunjukkan keduanya sebagai *false positive*, dengan WAF yang memblokir eksploitasi terhadap SQL Injection dan XSS yang hanya menghasilkan pesan kesalahan. Selain itu, Credit Card Number Disclosure ternyata mengidentifikasi koordinat pada Google Maps API, bukan nomor kartu kredit, dan Error Message on Page mengungkap informasi sensitif seperti struktur tabel yang seharusnya tidak ditampilkan kepada publik. Temuan ini menunjukkan bahwa sistem WAF mampu mengurangi banyak *false positive*, sehingga pengujian sistem harus dilakukan lebih mendalam dengan validasi manual untuk memastikan hasil yang lebih akurat dan relevan.
Dibandingkan dengan penelitian sebelumnya seperti oleh [3] yang lebih mengandalkan pemindaian otomatis, penelitian ini menunjukkan pentingnya validasi manual untuk memberikan analisis yang lebih mendalam terhadap kerentanan yang terdeteksi. Hal ini mengarah pada hasil yang lebih akurat, karena penelitian sebelumnya cenderung tidak melakukan analisis manual yang memadai. Tabel berikut menunjukkan perbandingan antara *false positive* dan *true positive* yang ditemukan.

TABEL II
PERSENTASE *FALSE POSITIVE VS TRUE POSITIVE*

Kerentanan	False Positive	True Positive	Validasi Manual
SQL Injection	100%	0%	Tidak valid
XSS	100%	0%	Tidak valid
IDOR	0%	100%	Valid
Credit Card Disclosure	100%	0%	Tidak valid
Error Message	100%	0%	Tidak valid

5. Generate Report

Generate Report merupakan tahapan akhir dari metode Vulnerability Assessment and Penetration Testing (VAPT) dimana pada proses ini, penulis membuat laporan CVSS Base Score dari kerentanan telah divalidasi, laporan tersebut berisikan tentang jenis kerentanan, level cvss base score, URL Vulnerability, impact, dan rekomendasi untuk memperbaiki kerentanan.

TABEL III
LAPORAN HASIL KERENTANAN

Report	Hasil
Vulnerability	Insecure Direct Object Reference (IDOR)
Level CVSS Base Score	7.3 (High)
Vulnerability URL	https://jalanpu.semarangkota.go.id/ajax?ajax=detail_segmen&id=1
Impact	Memungkinkan penyerang bisa mendapatkan informasi data sensitif yang seharusnya tidak ditampilkan
Mitigation	Menerapkan implementasi Indirect Object References yaitu melakukan implementasi enkripsi pada id sehingga tidak mudah ditebak.

IV. KESIMPULAN

Penelitian ini berhasil menunjukkan bahwa metode VAPT efektif dalam mengidentifikasi dan mengurangi kerentanannya pada Website Sistem Informasi Ruas Jalan Kota Semarang. Meskipun pemindaian otomatis berhasil mendeteksi kerentanan seperti SQL Injection, XSS, dan Credit Card Number Disclosure, validasi manual mengungkap bahwa sebagian besar temuan tersebut adalah false positive, dikarenakan WAF milik Alibaba Cloud memblokir eksploitasi terhadap beberapa kerentanannya. Hanya IDOR yang terkonfirmasi valid, memungkinkan akses langsung ke data sensitif tanpa kontrol akses yang memadai. Untuk mitigasi, penelitian ini merekomendasikan penerapan IDOR dengan enkripsi parameter ID guna mencegah akses tidak sah, misalnya enkripsi ID dengan menggunakan Algoritma AES (Advanced Encryption Standard) dengan proses mengambil parameter ID yang akan digunakan dalam URL atau permintaan API, lalu mengenkripsi ID menjadi ciphertext yang tidak dapat dikenali oleh pihak luar, sehingga menghindari manipulasi langsung oleh pengguna. Kontribusi penelitian ini mencakup pengisian gap literatur terkait kerentanan dalam sistem e-government, khususnya pada aplikasi yang mengelola data infrastruktur kota, serta berkontribusi dalam memberikan mitigasi secara spesifik yang dapat diadaptasi pada sistem serupa di lingkungan pemerintah. Temuan ini menekankan pentingnya membangun ekosistem digital pemerintahan yang aman dan tangguh, yang dapat merespons ancaman siber yang semakin kompleks dan melindungi data publik yang sensitif.

REFERENSI

[1] Rifdan, Haerul, H. Sakawati, and M. Nur Yamin, "ANALISIS PENERAPAN E-GOVERNMENT DALAM MENINGKATKAN KUALITAS PELAYANAN PUBLIK DI KECAMATAN TALLO KOTA MAKASSAR," vol. 4, no. 1, pp. 49–61, 2024.

[2] B. A. Iswandari, "Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance," *Jurnal Hukum Ius Quia Iustum*, vol. 28, no. 1, pp. 115–138, 2021, doi: 10.20885/iustum.vol28.iss1.art6.

[3] A. Budiman, S. Ahdan, and M. Aziz, "ANALISIS CELAH KEAMANAN APLIKASI WEB E-LEARNING UNIVERSITAS ABC DENGAN VULNERABILITY ASSESMENT," *Jurnal Komputasi*, vol. 9, no. 2, pp. 1–10, 2021.

[4] A. Maliq Ibrahim, T. Defisa, H. Bayu Seta, and I. P. Wayan Widi, "Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assesment and Penetration Testing (VAPT)," *Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA) Jakarta-Indonesia*, pp. 312–325, 2022.

[5] S. Mushtaq and M. Shah, "Mitigating Cybercrimes in E-Government Services: A Systematic Review and Bibliometric Analysis," *Digital*, vol. 5, no. 1, 2025, doi: 10.3390/digital5010003.

[6] I. M. Raazi, I. Dwitawati, and P. Nabila, "UJI VULNERABILITY ASSESSMENT DALAM MENGETAHUI TINGKAT," *JINTECH: Journal of Information Technology*, vol. 4, no. 1, [Online]. Available: https://journal.ar-raniry.ac.id/index.php/jintech

[7] A. Maliq Ibrahim, T. Defisa, H. Bayu Seta, and I. P. Wayan Widi, "Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assesment and Penetration Testing (VAPT)," 2022.

[8] A. Almaarif and M. Lubis, "Vulnerability Assessment and Penetration Testing (VAPT) Framework : Case Study of Government ' s Website," vol. 10, no. 5, pp. 1874–1880, 2020.

[9] C. Darmawan, J. P. Naibaho, and A. De Kweldju, "Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021," *Edumatic: Jurnal Pendidikan Informatika*, vol. 8, no. 1, pp. 272–281, 2024, doi: 10.29408/edumatic.v8i1.25834.

[10] N. A. Zahra, F. H. Zidane, and N. R. Kuslaila, "Analisis Keamanan Sistem Informasi Pada Website Pt Sentra Vidya Utama (Sevima) Menggunakan Metode Owasp," *Prosiding Seminar Nasional Teknologi dan Sistem Informasi*, vol. 3, no. 1, pp. 384–393, 2023, doi: 10.33005/sitasi.v3i1.564.

[11] S. Prabandari, "Vulnerablity Scanning Website PMB Menggunakan Open Web Application Security Project (OWASP)," *Jurnal Lentera ICT*, vol. 9, no. November, pp. 79–90, 2024.

[12] M. I. Fadillah, U. Yunan, K. S. Yanto, and M. Fathinuddin, "Analisis Security Mitigation dengan Metode Vulnerability Assesment and Penetration Testing (VAPT) (Kasus Website Kerja Praktek dan Pengabdian Masyarakat)," *Jurnal Sains Komputer & Informatika (J-SAKTI*, vol. 7, no. 2, pp. 753–764, 2023.

[13] R. Efendi, T. Wahyono, and I. R. Widiasari, "Uji Kerentanan Keamanan pada Web Sistem Informasi Akademik Satya Wacana Menggunakan Metode Vulnerability Assessment," *Aiti*, vol. 21, no. 1, pp. 44–57, 2024, doi: 10.24246/aiti.v21i1.44-57.

[14] M. A. Aziz, "Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas Xyz," *Journal of Engineering, Computer Science and Information Technology (JECSIT)*, vol. 2, no. 1, 2023, doi: 10.33365/jecsit.v1i1.13.

[15] Y. Natanael, R. Felicia, E. Malays, and S. Sakti, "Analisis Keamanan Informasi Bagi Pengguna Website Menggunakan Kalilinux Melalui Teknik SQL Injection," *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, vol. 25, no. 1, pp. 123–132, 2024, doi: 10.37817/tekinfo.v25i1.

[16] R. Ananda Putra and I. Alnaurus Kautsar, "Detection and Prevention of Insecure Direct Object References (IDOR) in Website-Based Applications Deteksi dan Pencegahan Insecure Direct Object References (IDOR) Pada Aplikasi Berbasis Website," *Seminar Nasional & Call Paper Fakultas Sains dan Teknologi*, vol. 4, 2023.

[17] M. A. Y. Putranda, I. K. A. Mogi, I. G. N. A. C. Putra, and I. M. Widiartha, "Analisis Serangan Cross Site Scripting (XSS) Pada Website OASE Menggunakan Metode OWASP," *Jurnal Elektronik Ilmu Komputer Udayana*, vol. 13, 2024.

[18] A. Gustiyono, E. I. Alwi, and S. M. Abdullah, "Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing," *CyberSecurity dan Forensik Digital*, vol. 7, no. 1, pp. 25–33, 2024.

[19] L. Kestina, Yuhandri, and G. W. Nurcahyo, "Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di Bkpsdmd Kabupaten Kerinci)," *INNOVATIVE: Journal Of Social Science Research*, no. 4, pp. 9192–9203, 2023.