CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 2, November 2025, hlm. 106-115

Pengujian Kerentanan Website Menggunakan Metode Penetration Testing Dengan OWASP (Studi Kasus : Pemerintah Kabupaten Semarang)

Reynanda Al Ridwan Bintang Firdaus[1], Tri Ismardiko Widyawan[2]

[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul
Email: [1]reynandaukk@gmail.com, [2]ismardiko@esaunggul.ac.id

Abstrak

Keamanan website merupakan aspek krusial dalam menjaga integritas, ketersediaan, dan kerahasiaan data, khususnya pada instansi pemerintahan yang mengelola informasi publik serta data sensitif. Seiring meningkatnya kompleksitas serangan siber, risiko kebocoran data, peretasan sistem, dan gangguan layanan dapat berdampak serius terhadap kepercayaan masyarakat terhadap layanan digital pemerintah. Penelitian ini bertujuan untuk menguji tingkat keamanan website Pemerintah Kabupaten Semarang dengan menggunakan metode penetration testing berbasis standar OWASP Top 10 tahun 2021, yang mencakup tahapan perencanaan dan pengumpulan informasi, analisis kerentanan, eksploitasi, hingga penyusunan laporan hasil beserta rekomendasi mitigasi. Pengujian dilakukan melalui simulasi berbagai serangan siber yang umum terjadi sesuai kategori OWASP, sehingga dapat mengidentifikasi celah keamanan yang berpotensi dimanfaatkan oleh penyerang. Hasil penelitian menunjukkan secara kuantitatif bahwa terdapat kerentanan dengan tingkat risiko tinggi, yaitu SQL Injection dan Cross-Site Scripting (XSS), yang ditemukan pada beberapa subdomain website Pemerintah Kabupaten Semarang. Kedua kerentanan ini memungkinkan penyerang untuk mencuri, memanipulasi, atau menyalahgunakan data penting, serta mengganggu keberlangsungan layanan publik. Temuan tersebut mengindikasikan perlunya langkah mitigasi melalui penguatan validasi input, peningkatan konfigurasi keamanan aplikasi, serta penerapan pemantauan sistem secara berkelanjutan. Implementasi rekomendasi yang dihasilkan diharapkan dapat meningkatkan ketahanan website Pemerintah Kabupaten Semarang terhadap ancaman siber, mencegah kebocoran data, menjaga ketersediaan layanan digital, dan memperkuat kepercayaan masyarakat terhadap keamanan sistem pemerintahan berbasis teknologi informasi.

Kata kunci: *Cybersecurity, Penetration Testing,* OWASP*,* Keamanan Website*,* Pemerintah Kabupaten Semarang

Website Vulnerability Testing Using the Penetration Testing Method with OWASP (Case Study: Semarang Regency Government)

Abstract

Website security is an important aspect in maintaining the integrity, availability, and confidentiality of data, particularly for government institutions that manage public information and sensitive records. With the increasing complexity of cyberattacks, the risks of data breaches, system intrusions, and service disruptions may significantly undermine public trust in digital government services. This study aims to assess the security level of the official website of the Semarang Regency Government by applying the penetration testing method based on the OWASP Top 10 standard of 2021, which involves several stages, including planning and information gathering, vulnerability analysis, exploitation, and reporting of findings with corresponding mitigation recommendations. The testing process was conducted by simulating various cyberattacks categorized under OWASP Top 10 to identify exploitable vulnerabilities. The results quantitatively revealed the presence of high-risk vulnerabilities, namely SQL Injection and Cross-Site Scripting (XSS), identified across several subdomains of the government website. These vulnerabilities may allow attackers to steal, manipulate, or misuse critical data, as well as disrupt the continuity of public services. Based on these findings, this research provides technical recommendations such as strengthening input validation, enhancing application security configuration, and implementing continuous monitoring. The application of these mitigation steps is expected to improve the resilience of the Semarang Regency Government website against cyber threats, prevent data breaches, ensure service availability, and reinforce public trust in digital government systems.

Keywords*: Cybersecurity, Penetration Testing, OWASP, Website Security, Semarang Regency Government*

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah mendorong transformasi digital di berbagai sektor, termasuk sektor pemerintahan. Digitalisasi ini diwujudkan dalam berbagai bentuk, salah satunya adalah pemanfaatan website sebagai sarana utama dalam menyampaikan informasi serta memberikan layanan publik kepada masyarakat. Pemerintah daerah, termasuk Pemerintah Kabupaten Semarang, menggunakan website sebagai media komunikasi resmi untuk menyediakan berbagai layanan administratif, informasi kebijakan, dan interaksi dengan masyarakat secara daring. Namun, seiring dengan meningkatnya ketergantungan pada sistem berbasis web, ancaman keamanan siber terhadap website pemerintahan juga mengalami peningkatan yang signifikan (Prasetyo, Sukarno en Musthofa Jadied, 2021). Serangan siber telah menjadi salah satu ancaman utama bagi keberlangsungan layanan digital, terutama bagi instansi pemerintah yang mengelola data sensitif. Berbagai serangan seperti *SQL Injection*, *Cross-Site Scripting (XSS)*, *Distributed Denial of Service (DDoS*, dan *Remote Code Execution (RCE)* menjadi tantangan besar dalam menjaga keamanan sistem informasi (Purnomo et al., 2024). Jika tidak ditangani dengan baik, serangan ini dapat menyebabkan kebocoran data, manipulasi informasi, pencurian identitas, hingga gangguan terhadap layanan publik yang berakibat pada menurunnya kepercayaan masyarakat terhadap pemerintah. Oleh karena itu, penting bagi pemerintah daerah untuk menerapkan strategi keamanan siber yang efektif guna mengidentifikasi dan mengatasi potensi kerentanan yang terdapat pada sistem mereka.

Salah satu metode yang umum digunakan untuk menguji tingkat keamanan sistem berbasis web adalah penetration testing. Metode ini merupakan simulasi serangan terhadap sistem dengan tujuan untuk mengidentifikasi celah keamanan dan mengevaluasi sejauh mana sistem mampu bertahan terhadap ancaman eksternal maupun internal. Penetration testing dapat membantu organisasi dalam memahami kelemahan yang terdapat dalam sistem mereka dan mengambil langkah-langkah pencegahan yang sesuai sebelum celah keamanan tersebut dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab (Natanael, 2024). Dalam penelitian ini, pengujian keamanan dilakukan menggunakan standar OWASP (Open Web Application Security Project), yang merupakan referensi utama dalam mengidentifikasi dan menganalisis kelemahan keamanan aplikasi web. OWASP menyediakan berbagai pedoman dan framework keamanan, termasuk OWASP Top 10 (2021), yang memuat daftar sepuluh jenis kerentanan keamanan web yang paling umum dan berbahaya seperti contoh *Injection, Cryptographic Failures,* dan *Broken Access Control* (Nurelasari en Gumilang Al Farabi, 2024). Dengan menggunakan OWASP sebagai acuan, penelitian ini dapat mengungkap berbagai celah keamanan yang berpotensi menjadi titik masuk bagi penyerang dalam mengakses atau merusak sistem website yang diuji.

Berdasarkan temuan awal, website milik Pemerintah Kabupaten Semarang juga tidak terlepas dari potensi kerentanan keamanan. Seperti pada domain website arpusda.semarangkab.go.id, teridentifikasi memiliki kelemahan seperti SQL Injection, serta potensi injeksi skrip berbahaya melalui Cross-Site Scripting (XSS) yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Kondisi ini menunjukkan adanya gap antara meningkatnya implementasi layanan digital dengan kesiapan pengelolaan keamanan siber di tingkat pemerintah daerah. Website yang berfungsi sebagai portal layanan publik masih rentan terhadap ancaman, sementara literatur maupun implementasi nyata terkait strategi pengujian keamanan website pemerintah daerah masih terbatas. Hal ini mempertegas perlunya penelitian yang lebih mendalam untuk mengidentifikasi kerentanan aktual pada website pemerintahan daerah serta menyusun langkah mitigasi yang sistematis.

Penelitian ini diharapkan mampu memberikan kontribusi nyata bagi Pemerintah Kabupaten Semarang dalam mengatasi kerentanan keamanan pada website resmi serta mencegah terulangnya permasalahan serupa di masa depan. Selain meningkatkan kesadaran mengenai urgensi keamanan siber di sektor pemerintahan, penelitian ini juga menyajikan rekomendasi dan mitigasi kerentanan yang dapat dijadikan acuan, seperti mencegah kebocoran data melalui SQL Injection, menanggulangi injeksi skrip berbahaya melalui Cross-Site Scripting (XSS), pembaruan sistem secara berkala, penerapan konfigurasi keamanan yang tepat, dan monitoring aktif terhadap potensi serangan. Temuan ini juga mendukung pemerintah daerah dalam merumuskan kebijakan keamanan siber yang lebih ketat, sistematis, dan selaras dengan standar internasional, sehingga mampu melindungi data serta layanan digital dari ancaman eksternal. Mengingat kompleksitas ancaman siber yang terus berkembang, pengujian keamanan melalui penetration testing perlu dilaksanakan secara rutin sebagai langkah preventif. Dengan demikian, penelitian ini berperan strategis dalam membantu Pemerintah Kabupaten Semarang meningkatkan ketahanan keamanan website pemerintahan secara berkelanjutan sekaligus menjaga kepercayaan publik.

2. KAJIAN PUSTAKA

2.1 OWASP TOP 10

OWASP Top 10 merupakan daftar yang disusun oleh Open Web Application Security Project (OWASP) yang berisi sepuluh risiko keamanan web paling kritis serta daftar ini diperbarui secara berkala setiap beberapa tahun berdasarkan hasil pengujian keamanan dan survei dari para profesional industri (Dewi, 2022). Metode ini memungkinkan perusahaan atau programmer untuk mengembangkan website

yang aman dan berorientasi ke masa depan. Salah satu pedoman keamanan yang dapat digunakan adalah OWASP Top 10 tahun 2021, yang mencakup beberapa kategori utama, seperti kelemahan kontrol akses, kegagalan kriptografi, injeksi, kekurangan dalam desain, kelemahan konfigurasi keamanan, penggunaan komponen yang rentan dan usang, kegagalan dalam identifikasi serta autentikasi, gangguan terhadap integritas perangkat lunak dan data, kurangnya pencatatan serta pemantauan keamanan, dan serangan pemalsuan permintaan dari sisi server (SSRF) (Ramdani, Heryana en Irawan, 2022).

Gambar 1 List OWASP Top 10 (2021)

2.2 Kali Linux

Kali Linux adalah sistem operasi berbasis Debian yang dirancang khusus untuk penetration testing dan forensik digital, dilengkapi dengan berbagai alat seperti Nmap, Wireshark, dan lain-lain (Prana Walidin, Pebiana Putri en Kiswanto, 2025). Alat-alat ini penting untuk mengevaluasi keamanan sistem dengan mensimulasikan serangan dunia nyata. Kali Linux digunakan untuk mengidentifikasi kerentanan, dan mengambil langkah-langkah mitigasi.Penetration testing dengan Kali Linux membantu organisasi memahami risiko dan mengambil langkah-langkah mitigasi yang sesuai

2.3 Information Gathering

Information Gathering adalah tahap awal di mana tester mengumpulkan sebanyak mungkin informasi tentang target sistem sebelum melakukan eksploitasi dalam memperoleh data penting, seperti alamat IP, domain, port, serta jenis sistem website yang digunakan (Khan et al., 2023). Proses ini bertujuan untuk memahami arsitektur, teknologi yang digunakan, serta potensi celah keamanan untuk membantu peretas etis dalam merancang strategi serangan yang lebih efektif.

2.4 Vulnerability Assessment

Vulnerability Assessment adalah proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi kelemahan dalam sistem, jaringan, aplikasi, atau infrastruktur teknologi informasi yang dapat dieksploitasi oleh ancaman keamanan (Manaek, Richardus Eko Indrajit en Erick Dazki, 2023). Proses ini mencakup pemindaian otomatis maupun analisis manual terhadap celah keamanan yang ada, seperti kesalahan konfigurasi, perangkat lunak yang tidak diperbarui, atau kelemahan dalam kode aplikasi. Hasil dari asesmen ini digunakan untuk memberikan rekomendasi mitigasi, meningkatkan keamanan sistem, dan mengurangi risiko eksploitasi oleh penyerang sebelum celah tersebut dapat dimanfaatkan dalam serangan nyata.

2.5 Penetration Testing

Penetration Testing adalah metode pengujian yang dilakukan terhadap suatu sistem atau jaringan komputer dengan tujuan menilai tingkat keamanannya (Dharmawan, Prihati en Listijo, 2022). Pengujian ini dilakukan melalui simulasi serangan terhadap sistem atau jaringan untuk mengidentifikasi celah keamanan yang mungkin timbul akibat kelemahan sistem, konfigurasi yang tidak tepat, atau kekurangan dalam proses operasional teknis. Hasil dari pengujian ini disajikan dalam bentuk laporan yang memberikan informasi kepada pemilik sistem mengenai potensi kerentanan yang ada. Laporan tersebut dapat digunakan sebagai dasar evaluasi guna memperbaiki dan menutup celah keamanan yang ditemukan, sehingga langkah pencegahan dapat dilakukan lebih awal.

2.6 Cross Site Scripting (XSS)

Cross-Site Scripting (XSS) merupakan ancaman signifikan terhadap keamanan web karena berpotensi merusak kinerja situs web, mencuri informasi sensitif pengguna, dan bahkan mengambil kendali penuh atas situs web. Serangan XSS terjadi dengan menyisipkan kode berbahaya ke dalam halaman web, yang kemudian dieksekusi di sisi klien (browser), memungkinkan penyerang untuk mencuri data, mengendalikan sesi pengguna, atau menjalankan kode berbahaya (Riadi, Umar en Lestari, 2020). Strategi keamanan yang direkomendasikan termasuk validasi input untuk mencegah injeksi skrip berbahaya. Dampak XSS sangat signifikan, karena dapat merusak integritas dan kerahasiaan data pengguna, serta mengganggu fungsionalitas dan reputasi situs web.

2.7 SQL Injection

SQL Injection adalah teknik peretasan yang memanfaatkan kerentanan keamanan dalam aplikasi web untuk menyisipkan perintah SQL berbahaya, sehingga mendapatkan akses tidak sah ke database (Nugraha, Kautsar en Fitrani, 2024). Dengan memanipulasi query SQL melalui input dari pengguna, penyerang dapat melewati langkah-langkah keamanan dan berinteraksi langsung dengan database . Hal ini dapat mengakibatkan pencurian data sensitif pengguna, manipulasi data, atau bahkan kendali penuh atas situs web. Pengembang web harus memvalidasi dan membersihkan input pengguna untuk mencegah serangan semacam itu. Pengujian penetrasi dengan alat seperti SQLMap dan penggunaan parameterized queries dapat membantu mengidentifikasi dan mencegah kerentanan SQL injection.

2.8 Cross Site Request Forgery

Cross-Site Request Forgery (CSRF) adalah kerentanan web yang signifikan di mana penyerang mengeksploitasi sesi pengguna yang terotentikasi untuk melakukan tindakan yang tidak diinginkan pada aplikasi web (Rusdiana, Cut en Sanusi, 2019). Dengan menipu pengguna agar mengklik tautan berbahaya atau mengunjungi situs web yang disusupi, penyerang dapat mengirim permintaan yang tidak sah ke server target, yang berpotensi menyebabkan kompromi akun, pencurian data, atau perubahan yang tidak sah (Mahdi Maulana Lubis, Handoko en Wulan, 2022). Serangan CSRF secara khusus menargetkan permintaan yang mengubah status, bukan pencurian data, karena penyerang tidak dapat melihat respons terhadap permintaan yang dipalsukan. Teknik mitigasi sering melibatkan penggunaan token rahasia, yang dapat bersifat statis atau dinamis, untuk memvalidasi permintaan pengguna dan mencegah pengiriman yang tidak sah.

3. METODOLOGI

3.1 Identifikasi Masalah

Keamanan website menjadi perhatian utama karena serangan siber yang semakin kompleks mengancam data sensitif dan reputasi organisasi. Penelitian berfokus pada evaluasi kerentanan (*vulnerability assessment*) dan identifikasi celah keamanan pada website pemerintah, seperti contoh pada Pemerintah Kabupaten Semarang, yang berpotensi dieksploitasi oleh pihak tidak bertanggung jawab. Metode *penetration testing* dengan kerangka kerja OWASP (Open Web Application Security Project) Top 10 digunakan untuk menganalisis dan memberikan rekomendasi perbaikan, sehingga meningkatkan standar keamanan website dan melindungi informasi penting (Fauzi et al., 2024). OWASP Top 10 dipilih sebagai kerangka kerja keamanan aplikasi web karena menawarkan keunggulan yang lebih relevan dibandingkan framework lain seperti NIST, ISO 27001, atau SANS, khususnya dalam konteks perlindungan aplikasi web.

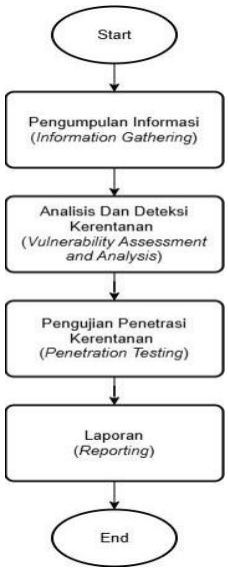
OWASP Top 10 dianggap mampu merepresentasikan ancaman keamanan terkini secara lebih realistis dengan fokus pada kerentanan web yang paling sering dijumpai (Petranović en Žarić, 2023). Keunggulan OWASP terletak pada spesialisasinya terhadap aplikasi web, sementara NIST Cybersecurity Framework dan ISO 27001 lebih berorientasi pada keamanan organisasi secara umum, dan SANS lebih menekankan pada aspek pelatihan serta sertifikasi (Deepa en Thilagam, 2016). Efektivitas OWASP dibuktikan secara empiris, misalnya melalui penerapan panduannya yang mampu menurunkan tingkat kerentanan sebesar 68,75% pada portal Division Head, 63,63% pada portal Recruiter, dan 12,5% pada portal Candidates dalam studi terhadap 70 aplikasi web (Khanum, Qadir en Jehan, 2023). Penelitian lain juga menunjukkan bahwa OWASP Top 10 mencakup kerentanan yang dilaporkan dalam National Vulnerability Database (NVD) selama sepuluh tahun terakhir (Sane, 2020). Selain itu, OWASP menyediakan perangkat praktis seperti Zed Attack Proxy untuk pengujian otomatis dan analisis kerentanan secara real-time (Sunardi, Riadi en Ananda, 2019), berbeda dengan framework lain yang cenderung konseptual serta membutuhkan implementasi tambahan untuk penerapan spesifik pada aplikasi web.

3.2 Teknik Pengumpulan Data

Dalam upaya menguji keamanan dan kerentanan website terhadap serangan siber guna meningkatkan standar perlindungan pada website Pemerintah Kabupaten Semarang, data dikumpulkan melalui tiga metode utama. Observasi dilakukan untuk mengamati langsung sistem serta infrastruktur website, sementara wawancara dengan pihak perwakilan Diskominfo Kabupaten Semarang yang mengelola website milik Pemerintah Kabupaten Semarang, bertujuan memperoleh informasi mendalam mengenai konfigurasi, kebijakan keamanan, serta riwayat insiden keamanan. Selain itu, studi literatur digunakan untuk mengumpulkan referensi teoritis dan relevan dari berbagai sumber, termasuk buku, artikel ilmiah, dan publikasi daring yang membahas metode penetration testing, standar keamanan OWASP, serta ancaman siber terkini. Pendekatan analisis keamanan sumber terbuka (OSINT) turut diterapkan guna memperoleh informasi strategis mengenai target melalui sumber-sumber publik yang tersedia secara daring.

3.3 Tahapan Penetration Testing

Tahapan penetration testing (uji penetrasi) merupakan langkah-langkah sistematis untuk mengidentifikasi, mengeksploitasi, dan menilai kerentanan keamanan dalam sistem atau jaringan. Berikut adalah tahapan umum dalam penetration testing:



Gambar 2 Alur Penelitian

Berlandaskan kerangka teoretis terpadu, penelitian ini memadukan OWASP Top 10, NIST Cybersecurity Framework (CSF), Information Security Theory, serta Government Digital Security Model. OWASP Top 10 berperan sebagai taksonomi kerentanan dan panduan prioritisasi skenario uji berisiko tinggi seperti, Broken Access Control, Cryptographic Failures, Injection, dan Cross-Site Scripting yang menstrukturkan rancangan uji pada tahap asesmen dan pengujian penetrasi. NIST CSF memetakan alur kerja, Identify untuk information gathering, Protect and Detect untuk penetapan baseline pengamanan sekaligus deteksi kelemahan pada vulnerability assessment, Respond untuk validasi dampak melalui penetration testing dan penetapan tindakan korektif; serta Recover untuk pelaporan, rencana mitigasi, dan perbaikan berkelanjutan. Dari sisi teori keamanan informasi, penelitian ini mengacu pada prinsip CIA TRIAD (confidentiality, integrity, and availability), manajemen risiko (impact vs likelihood), defense-in-depth, dan least privilege sebagai landasan pengambilan keputusan teknis. Dalam konteks pemerintahan, Government Digital Security Model menekankan tata kelola, kepatuhan regulasi, klasifikasi dan perlindungan data layanan publik, auditability, serta continuity of government services termasuk koordinasi dengan CSIRT instansi. Integrasi keempat kerangka ini memastikan setiap tahap bersifat terukur, dapat ditelusur (traceable), dan berorientasi pada penurunan risiko yang nyata terhadap aset informasi pemerintah

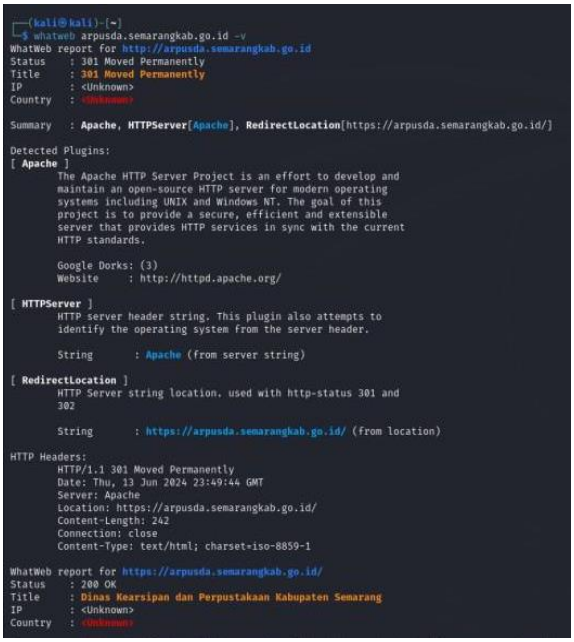
4. PEMBAHASAN

4.1 Information Gathering

Gambar 3. Hasil Scanning Port Website dengan NMAP

Pada tahap ini, akan melakukan *information gathering* sebagai bagian dari *penetration testing* terhadap salah satu website milik Pemerintah Kabupaten Semarang menggunakan NMAP dan WhatWeb. NMAP digunakan untuk memindai layanan yang berjalan pada server serta mendeteksi informasi terkait *port* yang terbuka, sistem operasi, dan keamanan, sedangkan WhatWeb digunakan untuk mengidentifikasi teknologi *web* yang digunakan. Hasil pemindaian NMAP menunjukkan bahwa *website* ini menggunakan *server* Apache HTTPD dengan layanan yang berjalan pada beberapa *port*, termasuk port 21 (FTP), port 80 (HTTP) yang melakukan redirect ke HTTPS, port 443 (HTTPS) dengan enkripsi SSL, port 554 (RTSP), serta port 1723 (PPTP).

Sementara itu, hasil pemindaian WhatWeb menunjukkan bahwa website telah mengimplementasikan enkripsi HTTPS dan memiliki pengalihan permanen 301 Moved Permanently, tetapi layanan FTP yang terbuka dapat menjadi celah keamanan yang perlu ditutup atau diamankan lebih lanjut. Dengan melakukan proses information gathering ini, dapat menekankan pentingnya melakukan pengamanan tambahan terhadap layanan atau teknologi web yang tidak diperlukan atau sudah usang agar mengurangi risiko eksploitasi terhadap sistem



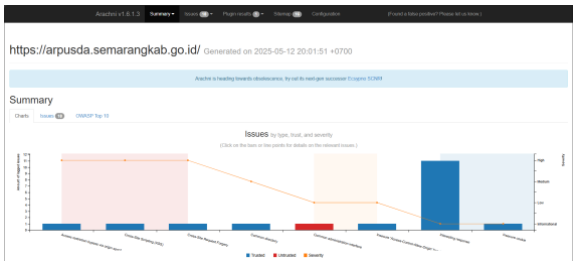
Gambar 4 Hasil Scanning Teknologi Website dengan WhatWeb

Tahapan information gathering dilakukan untuk mengumpulkan sebanyak mungkin informasi mengenai target sistem sebelum dilakukan pengujian lebih lanjut. Informasi yang diperoleh, seperti alamat IP, nama domain, layanan yang berjalan, serta sistem operasi yang digunakan sehingga menjadi dasar penting untuk mengidentifikasi potensi celah keamanan. Tahapan ini bersifat krusial karena keberhasilan pengujian kerentanan sangat bergantung pada kelengkapan dan ketepatan data yang dikumpulkan pada tahap awal.

4.2 Vulnerability Assessment

Vulnerability Assessment dilakukan dengan metode manual dan menggunakan tools otomatis seperti, Arachni yang secara otomatis memindai berbagai potensi kerentanan pada sistem web. Hasil pemindaian menunjukkan adanya beberapa kerentanan dengan tingkat keparahan tinggi, termasuk File Inclusion, Cross-Site Scripting (XSS), Blind SQL Injection (Timing Attack), dan Cross-Site Request Forgery (CSRF), yang berpotensi memungkinkan akses tidak sah, pencurian data, atau

eksekusi kode berbahaya. Selain itu, ditemukan kelemahan tingkat menengah hingga rendah, seperti direktori umum yang dapat diakses secara publik, serta insecure cookies, yang meskipun memiliki dampak lebih kecil tetap memerlukan perhatian dalam pengelolaan keamanan sistem. Berdasarkan temuan ini, penelitian merekomendasikan langkah-langkah mitigasi seperti penerapan validasi input yang ketat, penggunaan prepared statements untuk mencegah SQL Injection, implementasi token CSRF untuk mencegah serangan Cross-Site Request Forgery, serta konfigurasi security headers guna memperkuat perlindungan terhadap serangan siber.



Gambar 5 Hasil Scanning Kerentanan Website

Adapun rincian Kerentanan yang berhasil teridentifikasi adalah sebagai berikut :

Tabel 1 Daftar Kerentanan

CVSS Base Score v3	Kerentanan	Severity	Jumlah
8.6	Blind SQL Injection	High	1
6.3	Cross-Site Request Forgery	Medium	1
6.1	Cross-Site Scripting (XSS)	Medium	1
5.3	Common Directory	Medium	1
3.1	Insecure ‘Access-Control-Allow-Origin’ Header	Low	1
-	Common Administration Interface	Informational	1
-	Interesting Response	Informational	11
-	Insecure Cookie	Informational	1

4.3 Penetration Testing

Pada tahap penetration testing ini, dilakukan proses identifikasi serta eksploitasi terhadap celah keamanan yang terdapat pada website milik Pemerintah Kabupaten Semarang. Dari hasil pengujian tersebut, ditemukan dua jenis kerentanan yang terkonfirmasi atau *True Positive*, yaitu kerentanan SQL Injection dan Cross-Site Scripting (XSS). Adapun hasil dari eksploitasi terhadap kerentanan tersebut pada website Pemerintah Kabupaten Semarang disajikan sebagai berikut:

4.3.1 SQL Injection

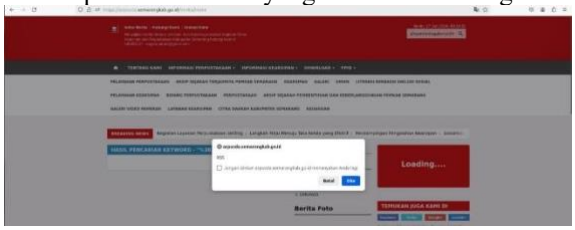
Hasil pengujian menunjukkan bahwa kerentanan SQL Injection berhasil mengeksploitasi celah keamanan pada sistem basis data menggunakan tools SQLMap, yang memungkinkan penyerang untuk mengekstrak informasi sensitif, termasuk kredensial pengguna yang telah dienkripsi. Serangan ini terjadi karena kurangnya validasi input dan absennya penggunaan prepared statements atau parameterized queries pada database.

Gambar 6 Hasil SQL Injection Dump Username dan Password

Berdasarkan gambar di atas, dapat dijelaskan bahwa terdapat dua akun pengguna yang teridentifikasi, yaitu *admin* dan *kreator*. Namun, informasi kata sandi untuk masing-masing akun masih dalam bentuk terenkripsi, dan hingga tahap pengujian ini, *SQLmap* belum berhasil mendekripsi nilai *hash* dari kata sandi tersebut.

4.3.2 Cross-Site Scripting (XSS)

Hasil pengujian Cross-Site Scripting (XSS), menunjukkan bahwa website rentan terhadap penyisipan skrip berbahaya yang dapat dieksekusi oleh browser pengguna, berpotensi digunakan untuk mencuri informasi sesi, melakukan phishing, atau memodifikasi tampilan situs. Hasil ini menunjukkan perlunya penerapan validasi input yang ketat, penggunaan mekanisme escaping pada output, penerapan Content Security Policy (CSP), serta penerapan Web Application Firewall (WAF) untuk mencegah eksploitasi lebih lanjut. Selain itu, audit keamanan berkala dan pembaruan sistem menjadi langkah krusial untuk memastikan ketahanan website terhadap ancaman siber yang terus berkembang.



Gambar 7 Hasil Pengujian Cross-Site Scripting (XSS)

Mengacu pada gambar di atas, terlihat bahwa sebuah *alert* dengan pesan “XSS” berhasil ditampilkan melalui penyisipan script `<script>alert('XSS-Reynanda')</script>`. Hasil pengujian menggunakan script tersebut menunjukkan bahwa website milik Pemerintah Kabupaten Semarang memiliki celah keamanan berupa kerentanan *Cross-Site Scripting* (XSS).

4.4 Risk Matrix Analysis: Impact vs Likelihood

Berdasarkan hasil eksploitasi kerentanan pada website Pemerintah Kabupaten Semarang, dilakukan analisis lanjutan dengan menggunakan *risk matrix* yang mengacu pada parameter *impact* dan *likelihood* sebagaimana disajikan berikut

Tabel 2 Risk Matrix Impact vs Likelihood

	Impact				
Likelihood	1-Sangat Rendah	2-Rendah	3-Sedang	4-Tinggi	5-Kritis
5-Hampir Pasti	Rendah (5)	Sedang (10)	Tinggi (15)	Ekstrim (20) (XSS)	Ekstrim (25) (SQLi)
4-Kemungkinan Besar	Rendah (4)	Sedang (8)	Sedang (12)	Tinggi (16)	Ekstrim (20)
3-Mungkin	Sangat Rendah (3)	Rendah (6)	Sedang (9)	Sedang (12)	Tinggi (15)
2-Jarang	Sangat Rendah (2)	Sangat Rendah (4)	Rendah (6)	Sedang (8)	Sedang (10)
1-Sangat Jarang	Sangat Rendah (1)	Sangat Rendah (2)	Sangat Rendah (3)	Rendah (4)	Rendah (5)

Berdasarkan hasil analisis risk matrix *impact* dan *likelihood* pada tabel 2, ditemukan bahwa kerentanan SQL Injection (SQLi) memperoleh skor risk rating sebesar 25 atau ekstrim, sedangkan Cross-Site Scripting (XSS) memperoleh skor 20 atau ekstrim. Perbedaan skor tersebut disebabkan oleh tingkatan dampak (*impact*) yang dihasilkan dari masing-masing serangan. SQL Injection dikategorikan memiliki dampak kritis karena potensi eksploitasi yang dapat memberikan akses langsung terhadap basis data, sehingga memungkinkan pencurian, manipulasi, bahkan penghapusan data penting. Hal ini mengancam tiga aspek fundamental keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan sistem, sehingga impact ditempatkan pada level tertinggi. Sementara itu, Cross-Site Scripting (XSS) meskipun sama-sama mudah dieksploitasi (*likelihood* hampir pasti), dikategorikan memiliki dampak tinggi karena serangan ini lebih berfokus pada sisi pengguna (*client-side*), seperti pencurian sesi, injeksi skrip berbahaya, atau pengalihan ke situs tidak sah. Dengan demikian, meskipun kedua kerentanan sama-sama memiliki probabilitas eksploitasi yang tinggi, SQL Injection dinilai lebih berbahaya karena implikasinya langsung terhadap *backend system* dan basis data inti, sedangkan XSS terutama berdampak pada pengguna akhir atau client.

4.5 Laporan

Bagian ini menjelaskan langkah-langkah mitigasi terhadap kerentanan yang ditemukan dengan hasil *True Positive* berdasarkan hasil pengujian, dengan tujuan meningkatkan keamanan pada website milik Pemerintah Kabupaten Semarang. Pada temuan SQL Injection, sudah berhasil terdeteksi sehingga sistem memiliki potensi kebocoran data walaupun sudah dienkripsi. Berdasarkan hasil penelitian, bahwa perbaikan kerentanan SQL Injection dilakukan dengan menerapkan praktik pengkodean yang aman, seperti menggunakan *prepared statements* atau *parameterized queries* untuk memastikan bahwa data input dari pengguna tidak dieksekusi sebagai perintah SQL (Christina Sari et al., 2024). Selain itu, penting untuk melakukan validasi dan *sanitasi* input secara ketat dengan membatasi jenis data yang diperbolehkan, serta menghindari penggunaan query dinamis yang langsung menyisipkan input pengguna ke dalam perintah SQL. Penerapan mekanisme keamanan tambahan seperti Web Application Firewall (WAF) dan pembaruan sistem secara berkala juga disarankan guna mencegah eksploitasi lebih lanjut terhadap celah keamanan serupa di masa mendatang.

Pada temuan Cross Site Scripting (XSS), sudah terdeteksi adanya eksploitasi XSS, sehingga sistem memiliki potensi risiko apabila proses sanitasi input tidak berjalan secara optimal. Berdasarkan hasil penelitian, penambahan header *Content Security-Policy* (CSP) terbukti mampu mencegah serangan XSS. Oleh karena itu, disarankan untuk mengimplementasikan header CSP seperti Content-Security-Policy: default-src 'self'; script-src 'self'; object-src 'none'; frame-ancestors 'none'; base-uri 'self';, serta memanfaatkan report-uri untuk pelaporan pelanggaran kebijakan, dan melakukan audit input secara rutin guna mencegah potensi celah keamanan (Kamaly, Septo en Widjajarto, 2024).

Tabel 3 Hasil Penelitian

Kerentanan	Teknik/Tools Pengujian	Rekomendasi
SQL Injection	Menggunakan tools SQLMap dengan perintah seperti sqlmap -u "*https://arpusda.semarangkab.go.id/berita/index" –method=POST –time-sec=10 –dbms=mysql –risk=3 –level 5 –tamper=space2comment –batch -D d4t4_arpusda –tables user –columns*"	Menerapkan *prepared statements* atau *parameterized queries* serta Web Application Firewall (WAF) sebagai tambahan untuk memastikan bahwa data input dari pengguna tidak dieksekusi sebagai perintah SQL
Cross-Site Scripting (XSS)	Melakukan penyisipan *payload* seperti *<script>alert('XSS')</script>*, *<img src="x" onerror="alert('XSS')">*, dan * XSS * ke dalam kolom input *form* maupun parameter pada URL.	Menerapkan header *Content Security-Policy* (CSP) untuk membatasi akses terhadap sumber daya yang dapat dieksekusi oleh browser.

4.6 Saran Prioritas Mitigasi Risiko Kerentanan

Berdasarkan hasil analisis terhadap kerentanan SQL Injection dan Cross-Site Scripting pada website Pemerintah Kabupaten Semarang, strategi mitigasi perlu diprioritaskan dalam tiga tingkatan tindakan. Pada tahap segera (0–30 hari), langkah yang direkomendasikan meliputi penerapan Web Application Firewall (WAF), penggunaan parameterized queries untuk mencegah SQL Injection, serta implementasi output encoding dengan dukungan Content Security Policy (CSP) headers dalam upaya meminimalisasi risiko XSS, dengan estimasi kebutuhan biaya sebesar Rp 100–200 juta (Yaswanthraj et al., 2024).

Selanjutnya, pada jangka pendek (1–3 bulan), organisasi disarankan untuk melaksanakan vulnerability assessment secara komprehensif menggunakan OWASP ZAP, menerapkan validasi input di sisi server, menyelenggarakan program pelatihan keamanan bagi tim teknologi informasi, serta mengimplementasikan sistem monitoring 24/7, dengan perkiraan investasi sebesar Rp 300–500 juta. Sementara itu, pada jangka panjang (3–12 bulan), fokus diarahkan pada modernisasi arsitektur keamanan menuju konsep Zero Trust, penerapan Secure Development Lifecycle (SDLC), serta upaya memperoleh sertifikasi ISO 27001 sesuai ketentuan Peraturan BSSN No. 11 Tahun 2018 (Prasetiyo, Huwae en Jatmika, 2024). Estimasi biaya yang dibutuhkan pada tahap ini mencapai Rp 1–2 miliar, dengan potensi return on investment (ROI) berupa pengurangan risiko data breach hingga 90% serta efisiensi biaya incident response sebesar Rp 2–5 miliar per insiden. Dengan demikian, strategi mitigasi ini tidak hanya berfungsi untuk melindungi data pribadi masyarakat, tetapi juga meningkatkan tingkat kepercayaan publik terhadap layanan digital pemerintah daerah.

4.7 Pengembangan Metodologi Penetration Testing

Metodologi pengujian keamanan website yang dapat dikembangkan serta diadopsi pemerintah daerah lain disusun secara terstruktur dengan mengacu pada standar OWASP Top 10 dan prinsip analisis risiko impact vs likelihood untuk memastikan hasil yang terukur. Tahapan yang dilakukan mencakup information gathering untuk memetakan aset digital, vulnerability assessment dengan kombinasi tools otomatis dan analisis manual, serta penetration testing terbatas guna memverifikasi kerentanan kritis seperti SQL Injection dan Cross-Site Scripting (XSS). Hasil uji kemudian dianalisis melalui risk matrix untuk menentukan prioritas mitigasi yang dibagi ke dalam tiga tingkatan, yaitu penerapan Web Application Firewall, parameterized queries, dan Content Security Policy, asesmen kerentanan menyeluruh, pelatihan SDM, dan implementasi monitoring 24/7, serta adopsi Zero Trust Architecture, penerapan Secure Development Lifecycle, dan sertifikasi ISO 27001. Metodologi ini bersifat modular sehingga dapat disesuaikan dengan kapasitas sumber daya tiap daerah, sekaligus memungkinkan penerapan secara berkelanjutan melalui audit berkala serta integrasi dengan Gov-CSIRT, sehingga mampu memperkuat ketahanan siber pemerintah daerah dan menjaga kepercayaan publik terhadap layanan digital.

4.8 Keterbatasan Penelitian

Keterbatasan dari penelitian ini terletak pada pengujian yang tidak dilakukan secara menyeluruh terhadap semua komponen sistem seperti aplikasi backend, sistem autentikasi multi-faktor, maupun integrasi pihak ketiga yang juga berpotensi menjadi titik masuk serangan. Beberapa kerentanan juga mungkin tidak teridentifikasi karena keterbatasan alat uji yang digunakan dan celah keamanan hanya dapat dimunculkan dalam kondisi tertentu yang tidak dapat disimulasikan dalam skenario pengujian ini. Keterbatasan ini menimbulkan kendala dalam penerapan langsung langkah-langkah mitigasi serta menghambat proses pengujian terhadap perbedaan kondisi sebelum dan sesudah mitigasi diterapkan sehingga analisis yang dilakukan hanya terbatas pada pemberian rekomendasi secara teoritis tanpa disertai dengan pengujian implementasi mitigasi pada sistem yang dianalisis.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa website milik Pemerintah Kabupaten Semarang masih mengandung beberapa kerentanan keamanan kritis, seperti SQL Injection dan Cross-Site Scripting (XSS), yang teridentifikasi melalui tahapan penetration testing berbasis standar OWASP. Temuan tersebut menunjukkan perlunya peningkatan sistem keamanan melalui penerapan validasi input, penggunaan prepared statements, serta pengaturan kebijakan keamanan seperti Content Security Policy (CSP). Berdasarkan hasil tersebut, disarankan agar pihak pengelola segera menerapkan langkah-langkah mitigasi yang direkomendasikan, melakukan audit keamanan secara berkala, serta memperbarui sistem dan plugin secara rutin untuk mencegah potensi eksploitasi. Selain itu, pengembangan kebijakan keamanan siber yang komprehensif dan pelatihan kepada personel teknis juga penting untuk meningkatkan kesiapsiagaan terhadap ancaman siber. Untuk penelitian selanjutnya, disarankan agar cakupan pengujian diperluas ke lebih banyak domain dan komponen sistem guna memperoleh gambaran yang lebih menyeluruh terhadap tingkat keamanan infrastruktur digital pemerintahan..

DAFTAR PUSTAKA

Christina Sari, N., Solichan, A., Ansor, B., Putra Ramdani, A., Zainudin Al Amin, M., Khaira, M. en Rohman Riquelme Al Ubaidah, A., 2024. Deteksi Kerentanan SQL Injection pada Website Menggunakan Vulnerability Assessment Info Artikel. Journal of Data Insights, [online] 2(1), bll9–17. https://doi.org/10.26714/jodi.

Deepa, G. en Thilagam, P.S., 2016. Securing web applications from injection and logic vulnerabilities: Approaches and challenges. Information and Software Technology, [online] 74, bll160–180. https://doi.org/10.1016/j.infsof.2016.02.005.

Dewi, B.T.K.& M.A.S., 2022. Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web.

Automata, [online] 3(1), bll1–8. Available at: <https://journal.uii.ac.id/AUTOMATA/article/view/21883/12030>.

Dharmawan, A., Prihati, Y. en Listijo, H., 2022. Penetration testing menggunakan OWASP top 10 pada domain xyz.ac.id. Jelc, 8(1), bll1–9.

Fauzi, R.M., Hermawan, R., Adhy, D.R. en Maesaroh, S., 2024. Analisis Kerentanan Keamanan Web Menggunakan Metode Owasp Dan Ptes Di Web Pemerintahan Desa Xyz. Power Elektronik : Jurnal Orang Elektro, 13(2), bll225–231. https://doi.org/10.30591/polektro.v13i2.6711.

Kamaly, A.D., Septo, U. en Widjajarto, A., 2024. Analisis Security Mitigation Terhadap Website Akademik Penunjan Administrasi di Institusi XYZ Mengunakan Metode Penetration Testing Execution Standard (PTES). In: eProceedings of Engineering. [online] bll3773–3781. Available at: <https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/23729>.

Khan, Z.A., Safaat, N., Irsyad, M. en Darmizal, T., 2023. Penetration Testing Information System Security Assessment Framework (ISSAF). Kajian Ilmiah Informatika dan Komputer, 4(3), bll1593–1601. https://doi.org/10.30865/klik.v4i3.1503.

Khanum, A., Qadir, S. en Jehan, S., 2023. OWASP-Based Assessment of Web Application Security. In: 2023 18th International Conference on Emerging Technologies (ICET). [online] IEEE. bll240–245. https://doi.org/10.1109/ICET59753.2023.10374730.

Mahdi Maulana Lubis, M., Handoko, D. en Wulan, N., 2022. Analisis Implementasi Laravel 9 Pada Website E-Book Dalam Mengatasi N+1 Problem Serta Penyerangan Csrf dan Xss. Januari, [online] 2023(2), bll173–187. Available at: <https://jurnal.unity-academy.sch.id/index.php/jirsi/index%0Ahttp://creativecommons.org/licenses/by-sa/4.0/>.

Manaek, R., Richardus Eko Indrajit en Erick Dazki, 2023. Arsitektur Perusahaan Untuk Infrastuktur Telekomunikasi Di Daerah Pedalaman Indonesia. SATIN - Sains dan Teknologi Informasi, 9(2), bll01–11. https://doi.org/10.33372/stn.v9i2.1000.

Natanael, N., 2024. Web Penetration Testing Dalam Mencari Kerentanan Sql Injection. JATI (Jurnal Mahasiswa Teknik Informatika), 7(6), bll3135–3138. https://doi.org/10.36040/jati.v7i6.7992.

Nugraha, L.A., Kautsar, I.A. en Fitrani, A.S., 2024. SQL Injection: Analisis Efektivitas Uji Penetrasi dalam Aplikasi Web. Smatika Jurnal, 14(01), bll111–123. https://doi.org/10.32664/smatika.v14i01.1224.

Nurelasari, E. en Gumilang Al Farabi, D., 2024. Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project (Owasp) Pada Simantep.Id. JATI (Jurnal Mahasiswa Teknik Informatika), 8(3), bll3049–3054. https://doi.org/10.36040/jati.v8i3.9314.

Petranović, T. en Žarić, N., 2023. Effectiveness of Using OWASP TOP 10 as AppSec Standard. In: 2023 27th International Conference on Information Technology (IT). [online] IEEE. bll1–4. https://doi.org/10.1109/IT57431.2023.10078626.

Prana Walidin, A., Pebiana Putri, F. en Kiswanto, D., 2025. KALI LINUX SEBAGAI ALAT ANALISIS KEAMANAN JARINGAN MELALUI PENGGUNAAN NMAP, WIRESHARK, DAN METASPLOIT. JATI (Jurnal Mahasiswa Teknik Informatika), 9(1), bll1188–1196.

Prasetiyo, N.A., Huwae, R.B. en Jatmika, A.H., 2024. AUDIT DAN ANALISIS WEBSITE PEMERINTAH MENGGUNAKAN PENGUJIAN PENETRASI SQL INJECTION DAN CROSS SITE SCRIPTING (XSS). Jurnal Teknologi Informasi, Komputer, dan Aplikasinya (JTIKA), [online] 6(2), bll525–533. https://doi.org/10.29303/jtika.v6i2.425.

Prasetyo, E., Sukarno, P. en Musthofa Jadied, E., 2021. Klasifikasi SQL Injection Menggunakan Algoritma Naïve Bayes. Jurnal Tugas Akhir Fakultas Informatika, 8(5), bll10605–10620.

Purnomo, M.D., Chusyairi, A., Insani, U.B., Jaya, S. en Bekasi, K., 2024. Pengujian Keamanan Sistem Mengunakan Metode Penetration Testing di Website Diskominfostandi Kota Bekasi. 1(1), bll92–101.

Ramdani, M.R., Heryana, N. en Irawan, Y.S.A., 2022. Penetration Testing pada Website Universitas Singaperbangsa Karawang Menggunakan Open Web Application Security Project (OWASP). Jurnal Pendidikan dan Konseling, [online] 4(3), bll5522–5529. Available at: <http://journal.universitaspahlawan.ac.id/index.php/jpdk/article/view/6353>.

Riadi, I., Umar, R. en Lestari, T., 2020. Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP. JISKA (Jurnal Informatika Sunan Kalijaga), 5(3), bll146–152. https://doi.org/10.14421/jiska.2020.53-02.

Rusdiana, Cut, B. en Sanusi, 2019. Analisa Keamanan Website Terhadap Serangan Cross-Site Request Forgery (CSRF). Kandidat : Jurnal Riset dan Inovasi Pendidikan, [online] 1(1), bll21–29. Available at: <http://jurnal.abulyatama.ac.id/index.php/kandidat>.

Sane, P., 2020. Is the OWASP Top 10 List Comprehensive Enough for Writing Secure Code? In: Proceedings of the 2020 International Conference on Big Data in Management. [online] New York, NY, USA: ACM. bll58–61. https://doi.org/10.1145/3437075.3437089.

Sunardi, Riadi, I. en Ananda, P., 2019. Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework. International Journal of Advanced Computer Science and Applications, [online] 10(11). https://doi.org/10.14569/IJACSA.2019.0101118.

Yaswanthraj, S., M, A., S, K. en R, J., 2024. SQL Injection and Prevention. International Journal of Research Publication and Reviews, [online] 5(6), bll1308–1317. https://doi.org/10.55248/gengpi.5.0624.1438.