ANALISIS KEAMANAN *WEBSITE* DI SMK WONGSOREJO GOMBONG TERHADAP SERANGAN *CROSS-SITE SCRIPTING (XSS)* MENGGUNAKAN *PENETRATION TESTING*

Rio Kuswara, Fahmi Facrhi
Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen
Jl. Kutoarjo No.Km.05, Wonoboyo, Jatisari, Kec. Kebumen, Kabupaten Kebumen, Jawa Tengah 54317
riokuswara4@gmail.com

ABSTRAK

Penelitian ini menganalisis keamanan *website* SMK Wongsorejo Gombong terhadap serangan *Cross-Site Scripting (XSS)* menggunakan metode *Penetration Testing*, yang mencakup tahapan *Information Gathering*, *Vulnerability Assessment*, *Exploit*, dan *Reporting*. Meskipun era digital memudahkan akses informasi, hal ini juga membawa tantangan baru, terutama terkait ancaman terhadap keamanan data dan privasi pengguna. Website SMK Wongsorejo Gombong, yang hingga kini belum pernah menjalani analisis keamanan, sehingga berpotensi menjadi target serangan siber. Hasil penelitian menampilkan bahwa terdapat empat kelemahan pada website yang berada di level high terdapat tiga kelemahan, level medium terdapat empat kelemahan, level low terdapat enam kelemahan, dan level Informational terdapat tiga kelemahan serta ditemukannya beberapa port yang masih terbuka dalam website. yang menyebabkan peretas dengan mudah masuk kedalam sistem untuk mengekploitasi informasi yang terdapat dalam Sistem Informasi Akademik. Untuk mengatasi kelemahan ini, direkomendasikan *mitigasi* berupa validasi input berbasis whitelist, penerapan *Content Security Policy (CSP)*, penguatan *firewall, output encoding*, serta penguatan konfigurasi server. Evaluasi keamanan secara berkala juga diusulkan untuk memantau potensi kerentanan baru. Kesimpulan Pada penelitiaan ini berhasil menemukan berbagai jenis kerentanan salah satu kerentanan yang di lakukan *exploit* adalah *xss*, dimana payload *XSS* berhasil dijalankan meskipun tidak sepenuhnya, karena terhalang sanitasi input dan eror server.

Kata kunci : *Skrip Lintas Situs, Pengujian Penetrasi, Keamanan Website*

1. PENDAHULUAN

Era digital yang terus berkembang, kita mengalami transformasi besar dalam berbagai aspek kehidupan, mulai dari sarana informasi, komunikasi, bisnis, hingga keamanan. Teknologi digital seperti *website*, media sosial, perangkat mobile, dan lain sebagainya, telah merubah cara manusia berinteraksi dan menjalankan aktivitas sehari-hari. Perkembangan teknologi yang semakin berkembang, sekarang kerja sama antar individu atau tim di lokasi yang berbeda dapat dilakukan tanpa harus bertemu langsung, memungkinkan kerja sama di tempat yang berbeda. Pekerjaan, rapat, dan presentasi dapat dilakukan secara virtual, menciptakan cara baru yang lebih mudah dan hemat waktu untuk berinteraksi dan bekerja sama [1].

Pada era yang semakin maju dampak yang paling mencolok dari perkembangan ini adalah meningkatnya kecepatan dalam mencari informasi. Dengan keberadaan teknologi digital, semua orang dapat memperoleh data dan berita secara real-time, yang sangat mendukung pengambilan keputusan yang lebih cepat dan efektif. Di tengah perkembangan ini, *website* menjadi salah satu komponen penting sebagai sarana komunikasi, informasi, dan transaksi di berbagai sektor, termasuk bisnis, pemerintahan, pendidikan, dan layanan masyarakat [2].

Ditengah perkembangan teknologi ini keberadaan *website* menjadi salah satu digital yang penting sebagai sarana informasi seperti SMK Wongsorejo Gombong telah memanfaatkan teknologi digital dengan menggunakan *website* sebagai media untuk menyampaikan berbagai informasi penting sekolah. Informasi yang disajikan melalui *website* ini mencakup jadwal penerimaan siswa baru, pengumuman kelulusan, informasi terkait program prakerin atau PKL, serta penyebaran berita tentang berbagai kegiatan sekolah dan lainnya. Dengan platform online, SMK Wongsorejo Gombong dapat menjangkau masyarakat dalam lingkup yang lebih luas dan meningkatkan interaksi dengan komunitas. Selain itu, *website* sering dimanfaatkan untuk promosi, kampanye, dan pemasaran, sehingga menjadi alat strategis yang efektif.

Namun, kemudahan akses informasi di era digital juga membawa tantangan baru di bidang siber. Salah satu tantangan utama adalah ancaman terhadap keamanan data dan privasi pengguna. Hal ini membuat keamanan *website* SMK Wongsorejo menjadi terancam akan terjadinya peretasan karena hingga saat ini belum pernah dilakukan analisis keamanan sama sekali [3].

Di era digital, *website* sering kali menjadi target utama para peretas yang berusaha melakukan *Eksploitasi* celah keamanan untuk mendapatkan akses tidak sah atau mencuri informasi sensitif. Kondisi ini menuntut adanya langkah proaktif dalam melindungi keamanan *website* agar tetap terpercaya [4].

Salah satu ancaman yang sering dijumpai pada *website* adalah kerentanan *Cross-Site Scripting (XSS)*. *XSS* merupakan jenis serangan yang memungkinkan

penyerang untuk menyisipkan kode berbahaya, biasanya dalam bentuk *JavaScript*, ke dalam halaman web yang akan dijalankan oleh pengguna lain. Serangan ini dapat menyebabkan dampak yang signifikan, seperti pencurian data sensitif, manipulasi tampilan *website*, hingga pengambilalihan sesi pengguna [5].

Kerentanan *XSS* umumnya terjadi akibat kurangnya validasi dan sanitasi input pada aplikasi web. Hal ini memungkinkan penyerang untuk menyisipkan *skrip* berbahaya melalui form, URL, atau elemen lainnya. Ketika *skrip* ini dieksekusi pada browser korban, penyerang dapat mengakses data pribadi pengguna, seperti cookie, token *otentikasi*, atau informasi penting lainnya. Selain itu, *XSS* juga dapat dimanfaatkan untuk menyebarkan malware atau mengarahkan pengguna ke situs phishing [6].

Hal ini menyoroti pentingnya menganalisi sitem keamanan secara berkala supaya sistem memiliki keamana yang kuat [7].

Pentingnya pengujian keamanan pada sistem aplikasi berbasis web menjadi semakin pokok dalam kemajuan teknologi yang pesat serta tingginya pengguna aplikasi berbasis link. Seiring dengan kondisi perkembangan yang pesat ini, berbagai serangan keamanan terus berkembang menggunakan berbagai metode ancaman yang semakin canggih [8].

Namun, masalah keamanan kerap dianggap kurang penting, sering diabaikan, dan hanya ditempatkan di posisi kedua atau bahkan terakhir dalam daftar prioritas sebuah organisas. Oleh karena itu, menjadi suatu keharusan bagi organisasi untuk secara aktif melakukan penilaian terhadap keamanan sistem *website* [9].

Perlindungan sistem yang tidak memadai akan lebih rentan menjadi sasaran serangan siber oleh para peretas yang berusaha mencuri, merusak, atau mengubah data penting. Keamanan *website* menjadi sangat penting untuk menjaga kepercayaan pengguna dan keamana data. sekarang banyak digunakan buat menangani informasi sensitif, seperti data pribadi, informasi keuangan, dan data penting lainnya. Oleh karena itu, upaya untuk mencegah terjadinya peretasan pengembang di upayakan agar selalu menganalisa keamanan sistem *website* nya dan di jadikan salah satu prioritas utama guna mendeteksi potensi kerentanan dan memahami risiko yang mungkin terjadi [10].

Berdasarkan permasalahan di atas penulis bertujuan untuk menganalisis keamanan *website* SMK Wongsorejo Gombong menggunakan metode *Penetration testing (Pentest)*. Dengan demikian, hasil dari penelitian ini diharapkan dapat membantu organisasi dalam mengidentifikasi celah keamanan serta meningkatkan ketahanan *website* terhadap ancaman serangan siber. Penelitian ini juga dapat memberikan gambaran mengenai proses pelaksanaan pentest pada sistem *website* dan mengidentifikasi jenis kerentanan yang sering ditemukan dan dapat memberikan kontribusi dalam pengembangan strategi keamanan yang lebih efektif, serta meningkatkan pemahaman akan pentingnya evaluasi berkala dalam menjaga keamanan dan integritas *website* [11].

Penelitian ini menggunakan *Penetration testing*. *Penetration testing (Pentest)* adalah metode serangan terhadap sistem yang berupaya mencari kelemahan di dalam sistem perangkat lunak, Aplikasi dan jaringan web yang rentan terhadap ancaman. Metode ini menggunakan simulasi serangan yang dijalankan oleh pihak luar untuk mendeteksi potensi celah-celah keamanan yang mungkin ada. Hasil dari pengujian ini dapat menunjukkan hasil dari analisa mengenai kelemahan sistem yang perlu ditangani [12].

Dalam Pengujian penetrasi mencakup beberapa teknik yaitu *Information Gathering*, dimana *Information Gathering* adalah langkah awal dalam peroses pengujian *Penetration testing* guna untuk mengetahui data-data mengenai situs web target yang akan diuji [13].

Vulnerability Assessment merupakan langkah yang dipakai untuk memindai kelemahan pada situs *website*, untuk mengidentifikasi jenis kerentanan yang ada pada *website* dengan melaksanakan *vulnerability scanning* yang dapat dipergunakan untuk mendeteksi celah keamanan seperti *SQL Injection*, *Cross-Site Scripting (XSS)*, dan berbagai jenis kerentanan lainnya [14].

Dalam melakukan pemindaian kerentanan, terdapat beberapa *Tools* yang dapat dimanfaatkan untuk mengoptimalkan proses kegiatan *vulnerability scanning* seperti Acunetix, OWASP ZAP, Vega, dan lainnya. Untuk tahapan Selanjutnya yang dapat dilakukan yaitu pengujian kerentanan terhadap kelemahan yang ditemukan selama proses *scanning*, melalui *Eksploitasi* untuk membuktikan dampak dari kerentanan tersebut Dengan demikian, proses pengujian penetrasi tidak hanya membantu dalam menemukan kerentanan, tetapi juga memberikan gambaran yang jelas mengenai tingkat resiko yang dapat ditimbulkan oleh celah-celah keamanan yang ada [15].

2. TINJAUAN PUSTAKA

2.1. Keamanan *Website*

Keamanan *Website* merupakan langkah atau upaya yang dilakukan untuk melindungi *website* dari Macam-macam jenis ancaman atau serangan yang dapat merusak, mencuri data, atau mengganggu aktivitas *website* tersebut. Tujuan utama dari keamanan *website* adalah memastikan bahwa data dan informasi yang ada di *website* aman, serta menjaga agar pengguna *website* tetap terlindungi [16].

Keamanan *website* sangat penting untuk menjaga kepercayaan pengguna, melindungi informasi sensitif, dan mencegah kehilangan data yang bisa menyebabkan karugian besar bagi perusahaan atau individu. Tanpa perlindungan keamanan yang memadai, *website* akan lebih rawan menghadap i serangan yang bisa mengganggu operasional bisnis, merusak reputasi, hingga menyebabkan kerugian finansial [17].

2.2. Ancaman Keamanan Pada *Website*

Seiring dengan berkembangnya teknologi, *website* yang saat ini menjadi bagian penting dari sebagian besar faktor kehidupan moderen, juga rawan terhadap berbagai macam serangan yang semakin bervariasi dan canggih untuk meng*Eksploitasi* kerentanan pada kode atau konfigurasi [5].

Cross-Site Scripting (XSS) merupakan jenis kerenganan yang sering di jumpai pada *website*, di mana peretas memasuka kode berbahaya (biasanya *JavaScript*) pada halaman web yang dikunjungi oleh pengguna lain. Tujuannya adalah untuk mencuri data sensitif seperti cookie atau informasi penguna bisa juga di manfaatkan untuk merusak halaman web [18].

2.3. *Penetration Testing*

Penetration testing adalah metode untuk mengevaluasi keamanan sistem komputer atau jaringan dengan mengidentifikasi kelemahan, kerentanan, dan kekurangan pembaruan. Proses ini mencakup identifikasi celah keamanan, konfigurasi firewall, serta titik akses nirkabel, baik melalui jaringan internal maupun jarak jauh. Tujuannya adalah untuk memahami jenis-jenis serangan yang mungkin terjadi pada sistem serta dampak yang dapat ditimbulkan akibat kelemahan tersebut. Uji penetrasi dilakukan untuk mengidentifikasi sekaligus mengeksploitasi kerentanan keamanan, sehingga dapat menilai sejauh mana langkah-langkah pengamanan yang telah diterapkan bekerja secara efektif atau justru kurang optimal. [19].

2.4. *Tools Penetrations Testing*

Tools penetrasi *testing* merupakan perangkat lunak yang dimanfaatkan para peneliti untuk membantu mengidentifikasi dan mengeksploitaasi kerentanan sebuah sistem atau jaringan. Pemilihan *Tools* yang tepat dapat mebantu saat melakukan pengujian kerentanan dan juga bisa mempengaruhi hasil dari pengujian [20].

Penelitian ini secara keseluruhan menggunakan empat *Tools* utama yaitu:

a. XSS attack
   Digunakan untuk menyisipkan skrip berbahaya pada halaman web guna menguji kerentanan XSS.
b. Owasp Zap
   Digunakan untuk memindai dan mendeteksi kerentanan yang ada pada website.
c. *Whois*
   Digunakan untuk mendapatkan informasi mengenai kepemilikan domain dan detail terkait lainnya.
d. *Nmap*
   Digunakan untuk memeriksa jaringan, seperti *host aktif*, *port* terbuka, dan sistem *operasi*.

2.5. Sitem Operasi Kali Linux

Kali linux adalah distribusi berbasis Debian GNU/Linux untuk kebutuhan forensik digital dan dimanfaatkan untuk pengujian penetrasi [21].

Fungsi utama kali linux adalah untuk melakukan pemeriksaan keamanan dan pengujian *Penetration*. Kali linux mempunyai ratusan *Tools*, untuk mendukung aktivitas terkait keamanan informasi, termasuk *Penetration testing*, security research, computer forensics, dan reverse engineering [22].

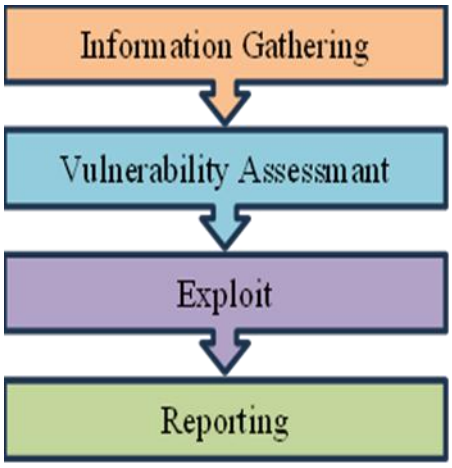
2.6. Virtual Environment

Virtual environment adalah wadah teknologi virtual yang memungkinkkan dapat berbagi sumber daya dari perangkat utama. selain itu, juga menyediakan akses ke lingkungan terdistribusi dan virtualisasi. Virtualisasi yaitu peroses pembuatan suatu model virtual dari suatu perangkat yang memiliki bentuk fisik, penelitian ini membutuhkan virtual environment untuk menjalankan skenario serangan dan menguji sistem keamanan pada *website* dengan memanfaatkan kerentanan yang berhasil ditemukan [23].

3. METODE PENELITIAN

Dalam penelitian ini, Analisis Keamanan *Website* SMK Wongsorejo Gombong terhadap serangan *Cross-Site Scripting (XSS)* dilakukan menggunakan metode *Penetration Testing* yang terstruktur. Penetration testing pada penelitian diawali dengan studi literatur mengenai pengujian yang dilakukan dan melakukan diskusi dan wawancara terhadap pihak pengelola website. Penelitian ini menggunakan laptop dengan sistem operasi Kali Linux dan beberapa *tools* untuk simulasi serangan sistem dalam melakukan *Penetration Testting*.

Metode ini dirancang untuk mengevaluasi kerentanan keamanan pada sistem dengan mensimulasikan serangan yang dilakukan oleh pihak eksternal. Adapun tahapan dalam dalam metode *Penetration testing* menurut [24] dapat dilihat pada Gambar 1.



Gambar 1. Metode *Penetration testing*

3.1. *Information Gathering*

Pengumpulan informasi (*Information Gathering*) adalah tahap awal dalam pengujian keamanan yang

bertujuan untuk mengumpulkan sebanyak mungkin data terkait target [25].

3.2. *Vulnerability* Assessmant

Penilaian Kerentan (*Vulnerability Assessment*) adalah langkah kedua dalam tahapan pengujian keamanan. Proses ini bertujuan untuk mengidentifikasi kerentanannya atau celah-celah yang ada pada sistem, yang berpotensi untuk di*Eksploitasi* oleh penyerang [26].

3.3. *Exploit.*

Pada langkah *Eksploitasi* ini, pengujian dilakukan dengan mencoba meng*Eksploitasi* sistem yang memiliki kerentanan terhadap serangan *XSS* (*Cross-Site Scripting*). Teknik yang digunakan adalah dengan menyisipkan kode *JavaScript* ke dalam parameter yang telah diidentifikasi sebagai titik lemah yang rentan terhadap *XSS* [27].

3.4. *Reporting*.

Setelah ancaman atau serangan ditemukan, tahap selanjutnya adalah pelaporan (*Reporting*). Pada tahap ini, hasil dari pengujian atau serangan yang telah dilakukan akan dirangkum dalam sebuah laporan yang mendetail [28].

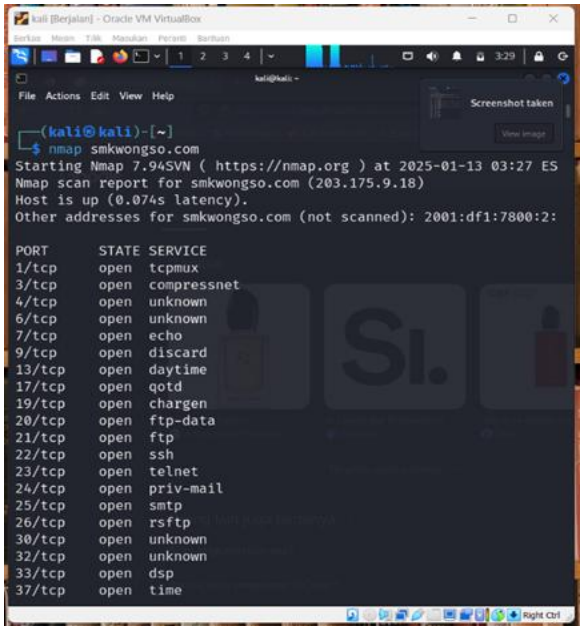
4. HASIL DAN PEMBAHASAN

pembahasan akan difokuskan pada langkah-langkah spesifik yang diambil untuk menganalisis keamanan website SMK Wongsorejo Gombong terhadap serangan Cross-Site Scripting (XSS) menggunakan metode penetration testing. Skenario pengujian meliputi:

4.1. *Information Gathering*

Pada langkah *Information Gathering* atau pengumpulan informasi dalam pengujian *Penetration testing*, peneliti berfokus untuk mendapatkan informasi secukupnya tentang sistem target, proses pengumpulan informasi sendiri di bagi menjadi dua yaitu active *Information Gathering* (pengumpulan informasi aktif) dan passive *Information Gathering* (pengumpulan informasi pasif). Pada Pengumpuan informasi menggunakan Active *Information Gathering* (Pengumpulan Informasi Aktif) peneliti menggunakan *Tools Nmap* sedangkan passive *Information Gathering* (pengumpulan informasi pasif) menggunakan tool *Whois*. Berikut adalah hasil dari active information gatering (pengumpulan informasi aktif) yang memanfaatkan tool *Nmap* dapat di lihat pada gambar 2.

Pada Gambar 2 hasil pemindaian menggunakan *Nmap* memberikan informasi bahwa pada sistem *Website* SMK Wongsorejo Gombong, terdapat banyak port yang masih terbuka salah satunya port 21 FTP (File Transfer Protocol), port 22 SSH (Secure Shell) dan port 80 HTTP (Hypertext Transfer Protocol) yang berjalan pada IP 203.175.9.18, selanjutnya langkah pengumpulan passive *Information Gathering* (pengumpulan informasi pasif) dengan menggunakan tool *Whois* dengan tujuan untuk mendapatkan informasi terkait domain. Berikut adalah Gambar 3 hasil pemindaian dari tool *Whois*.



Gambar 2. Hasil pemindaian *Nmap* pada *website*

Gambar 3. Hasil Pemindaian *Whois* Pada *Website*

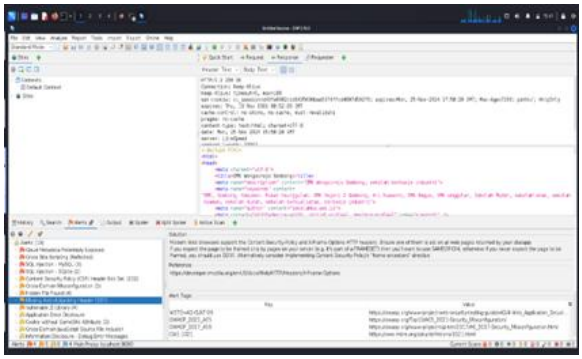
Pada Gambar 3 merupakan hasil dari pemindaian dengan menggunakan tool *Whois*, memperoleh informasi mengenai domain SMKWONGSO.COM, termasuk informasi kontak registrar, tanggal pembuatan, dan status domain. Informasi ini bisa digunakan untuk memverifikasi kepemilikan domain, mencari tahu informasi kontak pemilik, dan untuk mengetahui apakah domain tersebut dapat ditransfer ke registrar lain. Status domain "clientTransferProhibited" menunjukkan bahwa domain tersebut tidak dapat ditransfer ke registrar lain, mungkin karena alasan teknis atau kebijakan dari registrar saat ini.

4.2. *Vulnerability* Assessmant

Pada tahap ini, dilakukan penilaian terhadap keamanan *website* SMK Wongsorejo Gombong menggunakan OWASP ZAP, sebuah alat open-source

yang dirancang untuk mendeteksi kerentanan keamanan pada aplikasi web [21].

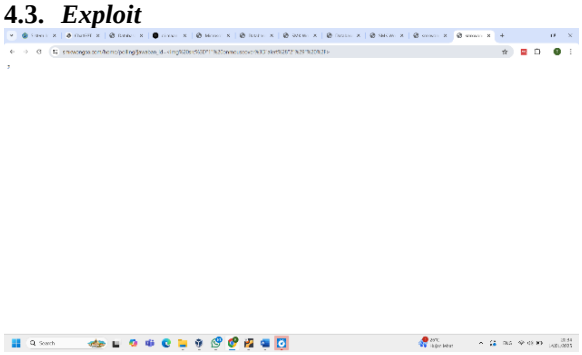
Hasil analisis menunjukkan adanya beberapa kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, Berikut adalah gambar 4 rincian hasil *scanning website* SMK Wongsorejo Gombong



Gambar 4. Hasil Penggunaan *Tool Owasp Zap*

Memberikan informasi hasil pemindaian *website* menggunakan tool Owasp zap. Hasil tersebut menunjukan adanya empat kerentanan tingkat high di antaranya *Cloud Metadata*, Cross Site Scripting, dan SQL Ijnection. Hal tersebut menunjukkan bahwa *website* SMK Wongsorejo masih memiliki banyak celah keamanan sehingga memerlukan solusi perbaikan. Berdasarkan hasil pemindaian dengan *Tools* Owasp zap, dapat disimpulkan bahwa kerentanan *website* terhadap serangan *XSS* sangat memungkinkan. Oleh karena itu, perlu dilakukan analisis untuk menjaga tingkat keamanan sistem dari serangan luar.

4.3. *Exploit*



Gambar 5 Hasil Serangan *XSS*

Serangan *XSS* meng*Eksploitasi* kerentanan sistem keamanan *website* untuk mencuri data, mengendalikan sesi pengguna, menjalankan kode jahat, atau digunakan sebagai bagian dari serangan phishing melalui script khusus. Script tersebut berisi sebuah muatan (payload) yang diinjeksi menjadi bagian dari permintaan yang dikirim ke web server. Permintaan tersebut direfleksikan kembali sedemikian rupa sehingga respon HTTP mencakup muatan permintaan HTTP dan payload *XSS* dieksekusi pada browser pengguna. Berikut adalah hasil dari serangan XSS pada website SMK Wongsorejo Gombong seperti pada gambar 5. Hasil pengujian serangan xss.

Berdasarkan pengujian yang dilakukan pada URL“smkwongso.com/home/polling?jawaban_id=<img%20src%3D'1'%20onmouseover%3D'alert(2)'>,” ditemukan adanya potensi kerentanan Cross-Site Scripting (XSS) pada parameter jawaban_id. Hasil pengujian menunjukkan bahwa kode JavaScript alert(2) berhasil dijalankan, sebagaimana terlihat dari tampilan halaman yang memunculkan angka "2". Namun, payload tidak sepenuhnya dieksekusi seperti yang diharapkan, karena adanya mekanisme sanitasi input parsial pada sisi server. Kerentanan ini mengindikasikan bahwa situs web belum sepenuhnya aman terhadap serangan XSS. Disarankan untuk melakukan validasi input secara ketat, menerapkan encoding output, serta menggunakan mekanisme keamanan tambahan seperti Content Security Policy (CSP) untuk mencegah eksploitasi lebih lanjut.

4.4. *Reporting*

Tahapan terakhir dalam metode *Penetration testing* adalah membuat laporan atau *Reporting*, yang mencakup seluruh hasil analisis dan *Eksploitasi* kerentanan pada sistem target. Dalam tahap ini, peneliti mendokumentasikan setiap proses penting yang dilakukan selama pengujian terhadap *website* smkwongso.com, termasuk hasil screening menggunakan tool OWASP ZAP. Laporan ini berfungsi sebagai referensi untuk memahami potensi ancaman dan langkah *mitigasi* yang diperlukan untuk memperbaiki kerentanan yang ditemukan. Berikut adalah hasil dari screening yang dirangkum dalam tabel 1:

Table 1. Tabel Hasil Pengujian Kerentanan Mendeteksi 11 *Sub File Vulnerability, High, Medium, Low*

Jenis	*Risk*	*Confidence*
Cloud Metadata Potentially Exposed	*High*	*Medium*
Cross Site Scripting	*High*	*Medium*
SQL Ijnection	*High*	*Medium*
Content Security Policy (CSP) Header Not Set	*Medium*	*High*
Cross-Domain Misconfiguration	*Medium*	*Medium*
Missing Anti-clickjacking Header	*Medium*	*Medium*
Vulnerable JS Library	*Medium*	*Medium*
Application Error Disclosure	*Low*	*Medium*
Cookie without SameSite Attribute	*Low*	*Medium*
Cross-Domain JavaScript Source File Inclusion Low	*Low*	*Medium*
Information Disclosure - Debug Error Messages	*Low*	*Medium*
Timestamp Disclosure - Unix	*Low*	*Low*

Jenis	*Risk*	*Confidence*
X-Content-Type-Options Header Missing	*Low*	*Medium*
Information Disclosure - Suspicious Comments	*Informational*	*Low*
Modern Web Application	*Informational*	*Medium*
Session Management Response Identified	*Informational*	*Medium*

Tabel 1 menunjukkan berbagai jenis kerentanan yang teridentifikasi pada sistem *website*, beserta tingkat risiko dan tingkat kepercayaannya. Berdasarkan hasil analisis, terdapat 16 kerentanan dengan risiko high, medium, low, dan informational seperti *Cloud Metadata* Potentially Exposed, *Cross-Site Scripting (XSS)*, dan *SQL Injection*, yang memiliki kerentanan high yang memerlukan penanganan prioritas untuk meningkatkan keamanan sistem. Selanjutnya pada Tabel 2 menyajikan rekomendasi perbaikan yang dapat diterapkan oleh pihah pengelola *website* nya.

Table 2. Rekomendasi Dari *Owasp Zap*

Jenis Kerentanan	Rekomendasi
Cloud Metadata Potentially Exposed	Batasi permintaan internal ke metadata server menggunakan *firewall*.
Cross Site Scripting	Gunakan *output encoding* pada semua data yang ditampilkan ke pengguna.
SQL Ijnection	Validasi input pengguna dengan ketat menggunakan whitelist untuk memastikan data yang diterima hanya sesuai dengan format yang diizinkan.
Content Security Policy (CSP) Header Not Set	Gunakan aturan CSP yang lebih spesifik sesuai kebutuhan, seperti membatasi sumber untuk *skrip* dan gaya.
Cross-Domain Misconfiguration	Konfigurasikan header HTTP "*Access-Control-Allow-Origin*" ke kumpulan domain yang lebih ketat, atau hapus seluruh *header CORS*, untuk memungkinkan browser web menerapkan Kebijakan Asal yang Sama (SOP) dengan cara yang lebih ketat.
Missing Anti-clickjacking Header	Perbarui atau sesuaikan konfigurasi server untuk mendukung penambahan header keamanan.
Vulnerable JS Library	Silakan tingkatkan ke versi terbaru.
Application Error Disclosure	Blokir akses langsung ke stack trace atau file debug menggunakan aturan *firewall* atau konfigurasi server.
Cookie without SameSite Attribute	Pastikan atribut SameSite disetel ke 'longgar' atau idealnya 'ketat' untuk semua cookie.
Cross-Domain JavaScript Source File Inclusion Low	Pastikan file JavaScript hanya dimuat dari sumber yang terpercaya dan tidak dapat dimanipulasi oleh pengguna akhir aplikasi.
Information Disclosure - Debug Error Messages	Nonaktifkan pesan debug sebelum mendorong ke produksi.
Timestamp Disclosure - Unix	Verifikasi secara manual bahwa data penanda waktu bersifat aman dan tidak dapat dikombinasikan untuk menghasilkan pola yang rentan terhadap *Eksploitasi*.
X-Content-Type-Options Header Missing	Gunakan browser modern yang sesuai standar dan mendukung pengaturan untuk menonaktifkan MIME-sniffing.
Information Disclosure - Suspicious Comments	Hapus seluruh komentar yang memberikan informasi yang bisa dimanfaatkan oleh penyerang dan perbaiki masalah yang disebutkan dalam komentar tersebut.
Modern Web Application	Peringatan ini bersifat informasi, sehingga tidak ada tindakan yang perlu diambil.
Session Management Response Identified	Ini adalah peringatan informasi, bukan kerentanannya, jadi tidak ada yang perlu diperbaiki.

Langkah-langkah perbaikan yang disarankan dalam tabel di atas dirancang untuk menangani setiap jenis kerentanan secara spesifik dan terarah. Misalnya, untuk kerentanan *SQL Injection*, validasi input pengguna secara ketat sangat diperlukan agar data yang dimasukkan sesuai dengan format yang telah ditentukan. Selain itu, untuk mengatasi risiko dari *Cloud Metadata* Potentially Exposed, pembatasan permintaan internal ke metadata server melalui *firewall* merupakan langkah yang efektif. Dengan menerapkan rekomendasi ini secara konsisten, risiko kerentanan dapat diminimalkan, sehingga *website* menjadi lebih aman dan terlindungi dari potensi serangan. Evaluasi dan implementasi perbaikan secara berkala juga sangat penting untuk memastikan sistem selalu berada dalam kondisi optimal.

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil mengidentifikasi 16 kerentanan pada website SMK Wongsorejo Gombong menggunakan metode *Penetration Testing*, yang meliputi tahapan *Information Gathering, Vulnerability Assessment, Exploit,* dan *Reporting*. Beberapa kerentanan dengan tingkat risiko tinggi yang ditemukan antara lain *Cloud Metadata, Cross-Site Scripting (XSS*), dan *SQL Injection*, yang memiliki potensi ancaman serius terhadap keamanan sistem. Hasil eksploitasi menunjukkan bahwa payload *XSS* berhasil dijalankan, meskipun tidak sepenuhnya, karena terhalang oleh mekanisme sanitasi input dan eror pada server. Selain itu, ditemukan sejumlah port terbuka yang berpotensi menjadi celah bagi serangan siber. Penelitian ini merekomendasikan langkah mitigasi, seperti validasi input berbasis *whitelist*, penerapan *Content Security Policy (CSP)*, penguatan *firewall*, dan *encoding output*. Evaluasi keamanan

secara berkala sangat disarankan untuk menjaga ketahanan sistem terhadap ancaman baru. Saran untuk peneliti selanjutnya adalah memanfaatkan kombinasi alat *Penetration testing* lainnya, seperti *Burp Suite* atau *Metasploit*, untuk memperluas cakupan pengujian serta meningkatkan akurasi dalam mendeteksi dan mengidentifikasi kerentanan keamanan pada sistem.

DAFTAR PUSTAKA

[1] E. Setyorini, "Efektifitas Pemanfaatan Zoom Meeting Terhadap Bekerja Dari Rumah Pada Masa Pandemi Covid-19," *Acad. J. Inov. Ris. Akad.*, vol. 2, no. 1, pp. 11–20, 2022, Accessed: Dec. 11, 2024. [Online]. Available: https://doi.org/10.51878/academia.v2i1.1076

[2] T. F. Astuti, A. Subarno, and C. D. S. Indrawati, "Pemanfaatan website sekolah sebagai sarana promosi dan informasi humas di SMK Negeri 1 Wonogiri," *JIKAP (Jurnal Inf. dan Komun. Adm. Perkantoran)*, vol. 8, no. 2, pp. 187–192, Feb. 2024, doi: 10.20961/jikap.v8i2.77776.

[3] N. S. Lubis and M. I. P. Nasution, "Perkembangan Teknologi Informasi Dan Dampaknya Pada Masyarakat," *J. Multidisiplin Saintek*, vol. 01, no. 12, pp. 21–30, 2023.

[4] M. P. Utama, K. R. Putri, A. A. E. Wirayuda, V. A. T. P. Herlambang, I. M. E. Listartha, and G. A. J. Saskara, "Analisis Perbandingan Kinerja Tool Website Directory Brute Force dengan Target Website DVWA," *J. Inform.*, vol. 18, no. 3, pp. 278–285, 2022, [Online]. Available: https://www.kali.org/get-kali/#kali-platforms,

[5] M. D. Al Vriano, "Pengujian Keamanan Web Juice Shop Dengan Metode Pentesting Berbasis Owasp Top 10," *J. Multidisiplin Saintek*, vol. 01, no. 06, pp. 81–90, 2023, Accessed: Dec. 11, 2024. [Online]. Available: https://doi.org/10.3785/kjst.v1i6.522

[6] S. Suroto and A. Asman, "ANCAMAN TERHADAP KEAMANAN INFORMASI OLEH SERANGAN CROSS-SITE SCRIPTING (XSS) DAN METODE PENCEGAHANNYA," 2021. [Online]. Available: http://www.hackers.com?yid=

[7] A. Elanda and R. L. Buana, "Analisis Keamanan Sistem Informasi Berbasis Website Dengan Metode Open Web Application Security Project (OWASP) Versi 4: Systematic Review," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 5, no. 2, pp. 185–191, 2020, Accessed: Dec. 11, 2024. [Online]. Available: https://doi.org/10.24114/cess.v5i2.17149

[8] M. O. Hoshmand and S. Ratnawati, "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity," *J. Sains dan Teknol.*, vol. 5, no. 2, pp. 679–686, 2023, doi: 10.55338/saintek.v5i2.2347.

[9] M. Tahir and M. Risky, "Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard)," *J. Tek. Inform. UNIKA St. Thomas*, vol. 09, no. 01, pp. 118–125, 2024.

[10] R. Gymnatsiar, U. Y. K. S. Hediyanto, and M. Fathinuddin, "Vulnerability Assessment And Penetration Testing (Vapt) Pada Website Layanan Akademik Universitas Xyz," *e-Proceeding Eng.*, vol. 11, no. 4, pp. 4241–4248, 2024.

[11] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritm.*, vol. 19, no. 1, pp. 77–86, 2021, [Online]. Available: http://jurnal.itg.ac.id/

[12] M. A. Nurrizki, E. I. H. Ujianto, and Rianto, "Analisis Keamanan Website Desa Budaya DIY Dengan Metode Penetration Testing (Pentest) dan OWASP ZAP," *J. Apl. Teknol. Inf. dan Manaj.*, vol. 5, no. 1, pp. 22–27, 2024, Accessed: Dec. 11, 2024. [Online]. Available: https://doi.org/10.31102/jatim.v5i1.2620

[13] F. Tinambunan, A. Junaidi, and A. M. Rizki, "PENGUJIAN SISTEM INFORMASI AKADEMIK UNIVERSITAS X MELALUI PENDEKATAN PENETRATION TESTING BERDASARKAN OWASP TOP 10," 2024.

[14] Y. Mulyanto, E. Haryanti, and Jumirah, "Analisis Keamanan Website SMK 1 Sumbawa Menggunakan Metode Vulnerability Asesement," *JINTEKS (Jurnal Inform. Teknol. dan Sains)*, vol. 3, no. 3, pp. 394–400, 2021, doi: 10.51401.

[15] D. F. Priambodo, A. D. Rifansyah, and M. Hasbi, "Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating," *Teknika*, vol. 12, no. 1, pp. 33–46, Feb. 2023, doi: 10.34148/teknika.v12i1.571.

[16] I. E. Alwi, Herdianti, and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting Dan Vulnerability Scanning," *Informatics J.*, vol. 5, no. 2, pp. 43–48, 2020, Accessed: Dec. 11, 2024. [Online]. Available: https://jurnal.unej.ac.id/index.php/INFORMAL/index

[17] A. M. Ujung and M. I. P. Nasution, "Pentingnya Sistem Keamanan Database untuk melindungi data pribadi," *JISKA J. Sist. Inf. Dan Inform.*, vol. 1, no. 2, pp. 44–47, 2023, [Online]. Available: http://jurnal.unidha.ac.id/index.php/jteksis

[18] A. Nur and D. A. Hafid, "Peranan IT Security Dalam Mengamankan Infrastruktur Dan Transaksi Di Perusahaan E-Commerce," *J. Multidisiplin Saintek*, vol. 4, no. 10, pp. 1–20, 2024.

[19] S. F. Maulana and H. Suhendi, "PENGUJIAN CELAH KEAMANAN JARINGAN KOMPUTER PT. JIONA SEJATI DENGAN NETWORK PENETRATION TESTING," *eProsiding Tek. Inform.*, vol. 2, no. 1, pp. 44–50, 2021, [Online]. Available:

https://eprosiding.ars.ac.id/index.php/pti

[20] M. Ayyas, A. Fauzi, and S. Widodo, "Studi Komparatif Teknik Analisis Keamanan Sistem Informasie-Government: Penetration Testing VS VulnerabilityAssessment," *SATIN - Sains dan Teknol. Inf.*, vol. 9, no. 2, pp. 25–34, Dec. 2023, doi: 10.33372/stn.v9i2.1000.

[21] H. S. Rosari, M. S. Al Hakim, E. Sibagariang, and A. R. Kardian, "Analisis Kecepatan MySQL dan PostgreSQL pada Windows 11 dan Kali Linux 2022," *J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 8, no. 1, pp. 231--222, 2023, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

[22] S. H. Handika, A. A. Rahman, I. Suraswati, and N. S. Neyman, "Memahami Cara Kerja Phishing Menggunakan Tools Pada Kali Linux," *J. Internet Softw. Eng.*, vol. 1, no. 2, pp. 1–11, 2024.

[23] R. Umar, I. Riadi, and R. S. Kusuma, "Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method," *IJID (International J. Informatics Dev.*, vol. 10, no. 1, pp. 53–61, Jun. 2021, doi: 10.14421/ijid.2021.2423.

[24] Y. Mulyanto, M. T. A. Zaen, Yuliadi, and S. Sihab, "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)," *J. Inf. Syst. Res.*, vol. 4, no. 1, pp. 202–209, Oct. 2022, doi: 10.47065/josh.v4i1.2335.

[25] N. Herawati, V. Budiyanto, and Uminingsih, "Analisis Keamanan Sebuah Domain Menggunakan Open Web Application Security Project (OWASP) Zap," *J. Teknol. TECHNOSCIENTIA*, vol. 15, no. 2, pp. 27–37, Mar. 2023, doi: 10.34151/technoscientia.v15i2.4013.

[26] Y. Mulyanto, Herfandi, and R. C. Kirana, "Analisis Keamanan Wireless Local Area Network (WLAN) Terhadap Serangan Brute Force Dengan Metode Penetration Testing," *J. Inform. Teknol. dan Sains*, vol. 4, no. 1, pp. 26–35, 2022.

[27] S. Andriyani, M. Fajar Sidiq, and B. Parga Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar," *J. Inform. Inf. Technol.*, vol. 2, no. 1, pp. 2–11, 2023.

[28] C. Ardiantoro and N. F. Puspitasari, "Analisis Kerentanan Website XYZ Repository Management Project," *J. Elektrosista*, vol. 11, no. 2, pp. 228–241, 2024.