OPEN ACCESS

Volume 9 (3), July-September 2025, 981-990

E-ISSN:2580-1643

Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

DOI: https://doi.org/10.35870/jtik.v9i3.3692

Analisis Keamanan Website Berbasis *WordPress* melalui *Penetration Testing* untuk Meningkatkan Keamanan Digital

Bagus Setya Putra [1*], Dwi Budi Santoso [2]

[1*,2] *Sisten Informasi, Fakultas Teknologi Informasi dan Industri, Universitas Stikubank, Kota Semarang, Provinsi Jawa Tengah, Indonesia.*

a r t i c l e i n f o

Article history:
Received 20 December 2024
Received in revised form
10 January 2025
Accepted 15 February 2025
Available online July 2025.

Keywords:
Penetration; WordPress; PTES; Burpsuite; Nmap; OwasZap; Wpscan.

a b s t r a c t

The development of information technology has made the security and integrity of digital information exchange on websites extremely important. Many websites utilize Content Management Systems CMS like WordPress as an alternative choice. This research aims to conduct penetration testing on the WordPress based website teknoblog.top using the Penetration Testing Execution Standard PTES method and provide recommendations for improving existing vulnerabilities. The analysis results on teknoblog.top using the WPScan tool found 6 informational findings, which do not indicate vulnerabilities. Meanwhile, OWASP ZAP identified vulnerabilities with a total of 3 medium level alerts, 5 low level alerts, and 6 informational alerts. The vulnerability successfully exploited in this research was the Missing Anti Clickjacking Header with a medium level severity. This finding was confirmed using the BurpSuite Scanner tool. The vulnerability was caused by the website not properly configuring the security header. To verify the accuracy of the Missing Anti Clickjacking Header vulnerability findings on the OWASP ZAP scanning tool, exploitation was carried out manually using a simple HTML script and through the clickjacker.io website. It is important to address this issue to prevent web pages from being loaded in iframes on other websites. The recommended fix for this vulnerability is the addition of the X Frame Options header to protect the website from clickjacking attacks.

Kata Kunci:
Penetrasi; WordPress; PTES; Burpsuite; Nmap; OwasZap; Wpscan.

a b s t r a k

Perkembangan teknologi informasi menjadikan keamanan dan integritas dari pertukaran informasi digital pada sebuah situs web menjadi sangat penting. Banyak situs web memanfaatkan Content Management System CMS seperti WordPress sebagai pilihan alternatif. Penelitian ini bertujuan untuk melakukan pengujian penetrasi pada situs web berbasis WordPress yaitu teknoblog.top dengan menggunakan metode Penetration Testing Execution Standard PTES dan memberikan rekomendasi saran perbaikan terhadap kerentanan yang ada. Hasil analisis pada teknoblog.top menggunakan tool WPScan menghasilkan 6 temuan bersifat informational, temuan informasi ini tidak menunjukkan kerentanan. Sedangkan OWASP ZAP menemukan kerentanan dengan total 3 medium level, 5 low level, dan 6 informational. kerentanan yang berhasil di eksploitasi pada penelitian ini yaitu Missing Anti clickjacking Header dengan tingkat keparahan medium level. Temuan ini terkonfirmasi menggunakan alat BurpSuite Scanner. Kerentanan disebabkan situs web tidak melakukan konfigurasi keamanan pada header dengan benar. untuk membuktikan keakuratan temuan dari kerentanan Missing Anti clickjacking Header pada alat pemindaian OWAS ZAP, Exploitasi pada kerentanan dilakukan secara manual menggunakan script HTML sederhana dan melalui situs web clickjacker.io. Penting untuk memperbaiki masalah ini agar mencegah halaman situs web dimuat dalam iframe pada situs web lain. Perbaikan yang disarankan untuk kerentanan ini adalah penambahan header X Frame Options untuk melindungi situs web dari serangan clickjacking.

Corresponding Author. Email: bagussetya0002@mhs.unisbank.ac.id [1].

ACM Computing Classification System (CCS)
EBSCOhost
Communication and Mass Media Complete (CMMC)

1. Pendahuluan

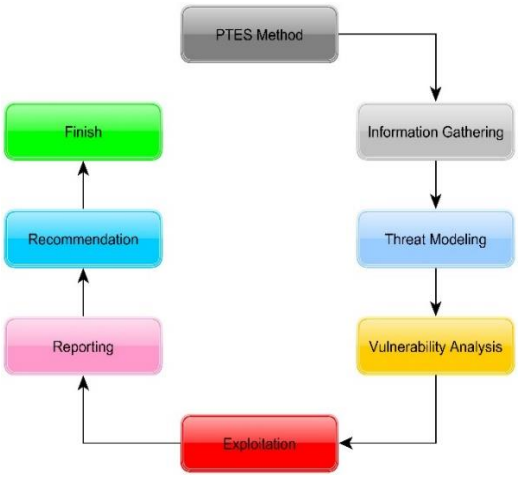
Penyebaran Informasi melalui teknologi memberikan kemudahan bagi kehidupan untuk mengetahui dan mencari informasi sesuai dengan kebutuhan (Zahwa dkk., 2022). Salah satu media yang secara *real-time* memberikan informasi terbaru adalah situs web berjenis blog, dimana informasi dipublikasi kepada masyarakat luas secara mudah dan efisien, begitupun juga sebaliknya masyarakat dengan mudah untuk mengakses informasi hanya dengan menggunakan sebuah smartphone yang terhubung pada internet. Namun seperti halnya jenis situs web lain, blog juga rentan terhadap berbagai ancaman serangan pada kemanan (Burhani & Priyawati, 2024). Menurut Asosiasi Penyelenggara Jasa Internet Indonesia APJII, pengguna internet di Indonesia mengalami peningkatan 1,4% dari priode sebelumnya, mencapai 221.563.479 jiwa dari total hasil populasi 278.696.200 jiwa penduduk Indonesia tahun 2023 (Kurniawan, H., & Christianto, E. 2024). Sebagai salah satu platform situs web yang sering digunakan, WordPress rentan untuk menjadi target serangan siber karena banyaknya pengguna dan plugin yang tersedia (Pratiwi dkk., 2020) . Analisis keamanan pada situs berbasis WordPress melalui pengujian penetrasi adalah langkah penting untuk menjaga data tetap aman dan utuh (Mamuriyah dkk., 2024). Upaya pengujian penetrasi pada situs web difokuskan untuk menemukan kerentanan dengan menembus sistem menggunakan alat penyerangan siber, hal ini diperuntukkan agar situs web memiliki rekomendasi perbaikan sistem dalam meningkatkan keamanannya (Wen & Katt, 2023).

PTES adalah metode pengujian penetrasi yang memberikan panduan secara teratur dan lengkap untuk melakukan pengujian penetrasi mencakup semua langkah penting, dari perencanaan hingga pelaporan hasil indentifikasi (Dasmen dkk., 2022). Proses pengujian penetrasi menggunakan metode *Penetration Testing Execution Standart* PTES pada umumnya memiliki beberapa tahapan yang terdiri dari pengumpulan informasi, pemodelan serangan, identifikasi kelemahan atau pemindaian kerentanan, dan eksploitasi. Pada tahap pengumpulan informasi, peneliti mengumpulkan data dari situs web yang akan diuji, termasuk *paltform* CMS yang digunakan, plugin yang terpasang, dan pengaturan server (Laksmiati, D. 2023). Setelah data terkumpul, penguji dapat menentukan pemodelan serangan berdasarkan hasil temuan kerentenan pada situs web. Dalam menetukan pemodelan serangan pada celah keamanan yang teridentifikasi peneliti menggunakan alat pemindaian OWAS ZAP. ZAP merupakan alat sumber terbuka yang berfungsi untuk melakukan pemindaian secara otomatis pada situs atau aplikasi web. ZAP juga memiliki kemampuan dalam memodifikasi lalu lintas prtokol jarigan pada situs web (Darojat dkk., 2022). alat pemindaian otomatis seperti WP*Scan* juga digunakan pada penelitian ini untuk mendeteksi kerentanan situs web yang diketahui menggunakan CMS berbasis WordPress (Ramadhani dkk., 2024). Biasanya WP*Scan* secara *default* telah terinstal dan dapat langsung dijalankan pada *operating system* kali linux. Setelah ditemukannya celah keamanan dan model serangan yang sesuai dengan kerentanan, langkah berikutnya adalah tahap eksploitasi, pada tahap ini penguji mencoba memanfaatkan hasil temuan dari kerentanan untuk melakukan simulasi serangan pada situs web (Aziz, 2021). Tools yang digunakan untuk eksploitasi dapat bervariatif sesuai jenis temuan yang dihasilkan oleh alat pemindaian. Hasil pengujian penetrasi akan memberikan gambaran yang jelas tentang tingkat keamanan situs web dan area yang perlu diperbaiki.

Menurut penelitian yang dilakukan oleh (Riyanti dkk., 2024). Pendekatan lain pada penelitian pengujian penetrasi menggunakan metode *National Institute of Standards and Technology* NIST. Penelitian berhasil mengidentifikasi dan mengeksploitasi celah keamanan menggunakan alat SQL*map* yang terdapat pada sistem operasi kali linux, penelitian mengungkapkan bahwa situs web memiliki kerentanan terhadap jenis serangan SQL Injection dan berhasil dieksploitasi. Temuan utama mencakup keberhasilan dalam memperoleh data autentikasi penting, struktur tabel, kolom, dan isi data dari database target. Platform WordPress sangat populer di dunia, perkiraan pengguna lebih dari 493 juta termasuk di negara Indonesia. Berdasarkan statistik laporan dari Akamai perusahaan penyedia layanan keamanan *cyber*, *cloud*, dan *Content Delivery Network* CDN Rata-rata serangan siber di Indonesia pada tahun 2023 mencapai 22 serangan perdetik. Jumlah serangan tebanyak berjenis *Distributed Denial of Service* DDoS dengan total 260 miliar selama priode januari 2023 hingga juni 2024. Laporan dari statistik

menunjukkan pentingnya pemeliharaan keamanan pada sebuah situs web berbasis WordPress dan platform situs web lainnya. Penelitian ini menggunakan *Penetration Testing Execution Standart* PTES sebagai metode pengujian penetrasi yang bertujuan untuk meminimalisir kerentanan pada situs web teknoblog.top dan meningkatkan keamanan dari potensi serangan siber di masa depan.

2. Metodologi Penelitian



Gambar 1. Tahapan Penelitian

1) *Information Gathering*
   Tahap ini bertujuan untuk mengumpulkan berbagai informasi terkait situs web teknoblog.top, termasuk alamat IP dan data terkait lainnya. Proses ini penting untuk mengetahui karakteristik dasar dari situs web yang akan diuji, sehingga pengujian lebih lanjut dapat dilakukan dengan lebih terarah.
2) *Threat Modeling*
   Pada tahap ini, peneliti menentukan model ancaman yang teridentifikasi dengan menggunakan alat *OWASP ZAP*. *OWASP ZAP* merupakan alat sumber terbuka yang dilengkapi dengan antarmuka grafis yang intuitif, memudahkan pengguna dalam menjalankan pemindaian keamanan aplikasi dan situs web secara otomatis. Alat ini memiliki keunggulan dalam melakukan pemindaian aktif dan pasif, serta fitur spidering yang memungkinkan penelusuran struktur situs web untuk memberikan informasi tentang lokasi kerentanan yang ada.
3) *Vulnerability Analysis*
   Pemindaian keamanan pada tahap ini bertujuan untuk menganalisis potensi celah keamanan serta jenis serangan yang dapat terjadi pada sistem. Peneliti menggunakan *WPScan* untuk mendeteksi kerentanan pada situs berbasis WordPress. *WPScan* dipilih karena merupakan alat yang khusus didesain untuk mengidentifikasi daftar plugin, tema, serta potensi kerentanan pada situs yang menggunakan platform WordPress.
4) *Exploitation*
   Pada tahap eksploitasi, peneliti melakukan simulasi serangan terhadap situs web untuk mencari celah yang dapat dieksploitasi. *BurpSuite* digunakan sebagai alat untuk mendeteksi dan menguji kerentanan yang ditemukan dalam penelitian ini, yaitu Missing Anti-Clickjacking Header. *BurpSuite* Scanner secara otomatis mendeteksi apakah situs web menggunakan header HTTP yang sesuai, seperti *X-Frame-Options*, untuk mengurangi risiko serangan.
5) *Reporting*
   Laporan disusun berdasarkan hasil temuan dan analisis kerentanan yang berhasil ditemukan. Laporan ini mencakup demonstrasi *Proof of Concept* (PoC) untuk menunjukkan keberhasilan eksploitasi yang telah dilakukan pada kerentanan yang ditemukan.
6) *Recommendation*
   Pada tahap ini, peneliti memberikan rekomendasi untuk memperbaiki sistem yang diuji. Rekomendasi tersebut mencakup pembaruan perangkat lunak situs web guna meminimalkan potensi risiko serangan di masa depan. Perbaikan yang diajukan bertujuan untuk memperkuat keamanan situs web secara menyeluruh.

3. Hasil dan Pembahasan

Hasil

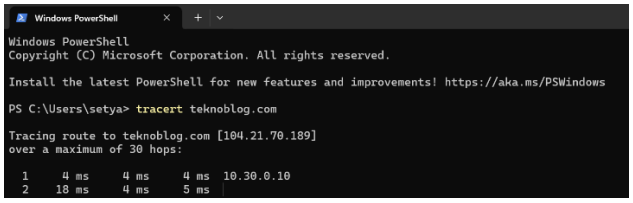
Sebelum melakukan pengujian pada sebuah situs web diperlukan persiapan kebutuhan alat untuk melakukan penetrasi, diantaranya *software* dan *hardware*. Berikut pada tabel 1. Dijelaskan beberapa hasil analisis dari alat yang digunakan dalam penelitian.

Tabel 1. Alat kebutuhan penelitian

No	Parameter Pengujian	Spesifikasi
1	Perangkat	Lenovo
2	RAM	8 GB
3	Jaringan	Wifi, Selular
4	Sistem Operasi	Windows 11
5	*Virtual Machine*	Oracle Vbox
6	Sitem Operasi VM	Kali Linux
7	*Information Gathering*	Nmap, Whois, *Lookup*
8	*Threat Modeling*	OWAS ZAP
9	*Vulnerability Analysis*	WP *Scan*
10	*Exploitation*	Burpsuite Profesional, clickjack.io

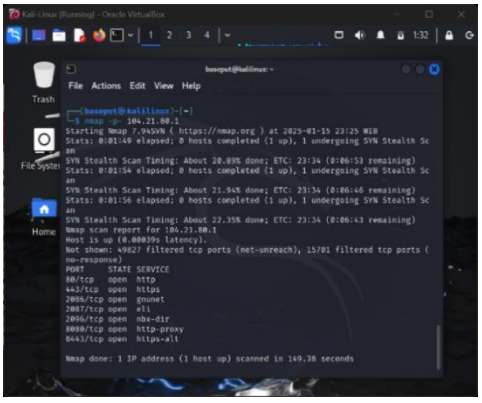
Information Gathering

Pada tahapan ini peneliti mengumpulkan data dari target website teknoblog.top berupa informasi situs web, teknologi yang digunakan dan IP *Internet Protocol address*. Peneliti menggunakan CMD *command prompt* dengan perintah tracert teknoblog.top.



Gambar 2. Pengecekan IP pada *command prompt*

Setelah menemukan ip target selanjutnya melakukan scan port menggunakan Nmap. Nmap *Network Mapper* merupakan alat *open source* yang digunakan untuk eksplorasi jaringan dan audit keamanan.

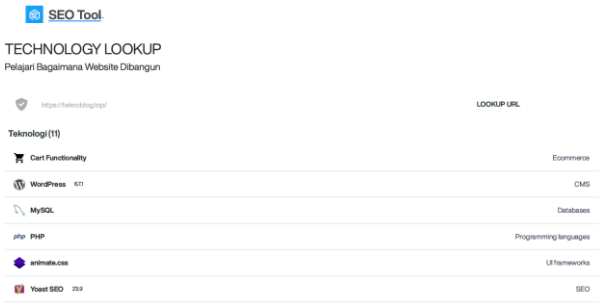


Gambar 3. Scanning port menggunakan Nmap

Tael 2. Hasil *Scan Port* menggunakan Nmap

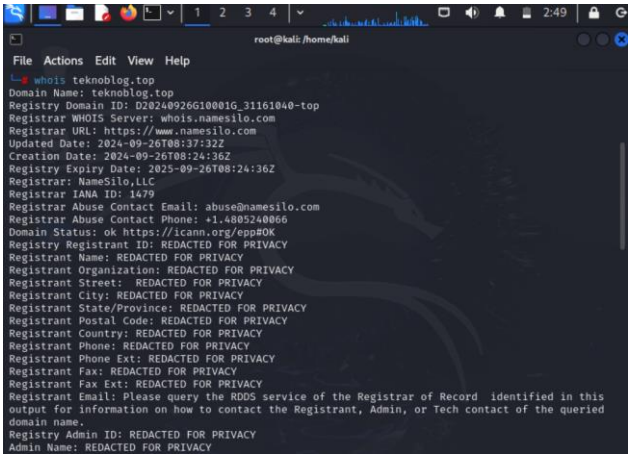
No	Port aktif	Status
1	80/tcp http	Open
2	443/tcp https	Open
3	2086/tcp gnunet	Open
4	2087/tcp eli	Open
5	2096/tcp nbx-dir	Open
6	8080/tcp http-proxy	Open
7	8443/tcp https-alt	Open

Untuk mengetahui dan mengkonfirmasi apakah situs web benar menggunakan CMS WordPress, peneliti menggunakan aplikasi web dari *TechnologyLookup* https://tools.co/id/technology-lookup.



Gambar 4. Pengecekan teknologi dari situs web

Whois adalah sebuah situs web yang difungsikan untuk menemukan informasi terkait domain. Berdasarkan informasi yang diperoleh situs web tersebut hanya menggunakan domain name teknoblog.top informasi ditampilkan pada Gambar 5.

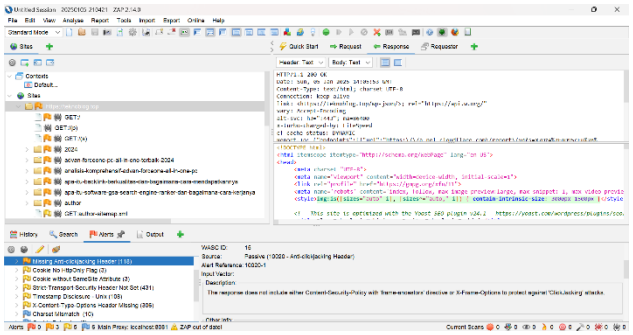


Gambar 5. Informasi menggunakan situs web whois

Threat Modeling

Pada tahapan ini peneliti menganalisis kerentanan menggunakan OWASP ZAP versi 2.14.0 untuk

memodelkan jenis ancaman pada situs web. Berdasarkan analisis, peneliti menemukan 8 jenis kerentanan dan 6 jenis informasi dengan 3 jenis level berbeda diantaranya: 3 *medium level alerts*, 5 *low level alerts*, dan 6 *informational alerts*.



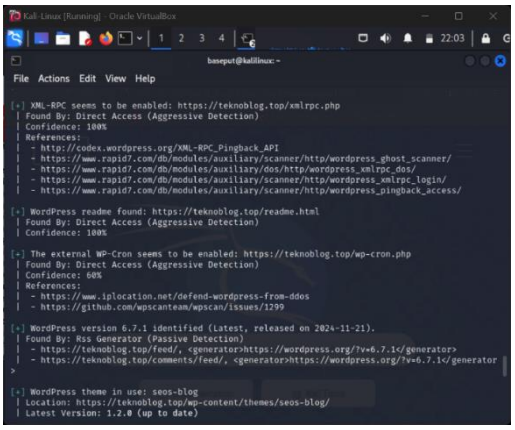
Gambar 6. Analisis ZAP temuan model ancaman

Tabel 3. Identifikasi Model Ancaman OWAS ZAP

No	Jenis Kerentanan	Level
1	*Absence of Anti*-CSRF *Tokens*	Medium
2	*Content Security Policy* (CSP) *Header Not Set*	Medium
3	*Missing Anti-clickjacking Header*	Medium
4	*Cookie No* HttpOnly *Flag*	Low
5	*Cookie without SameSite Attribute*	Low
6	*Strict-Transport-Security Header Not Set*	Low
7	*Timestamp Disclosure – Unix*	Low
8	*X-Content-Type-Options Header Missing*	Low
9	*Charset Mismatch*	Info
10	*Cookie Poisoning*	Info
11	*Information Disclosure - Suspicious Comments*	Info
12	*Modern Web Application*	Info
13	*Re-examine Cache-control Directives*	Info
14	*Session Management Response Identified*	Info

Vulnerability Analysis

Pada tahap ini peneliti menggunakan tool WP*Scan* untuk menganalisis kelemahan, tool ini dapat langsung dijalankan menggunakan *Operating System* Kali Linux pada *Virtual Machine* Vbox. WP*Scan* merupakan tool yang dirancang khusus untuk mengidentifikasi celah kelemahan pada situs web yang menggunakan CMS berbasis Wordpress.

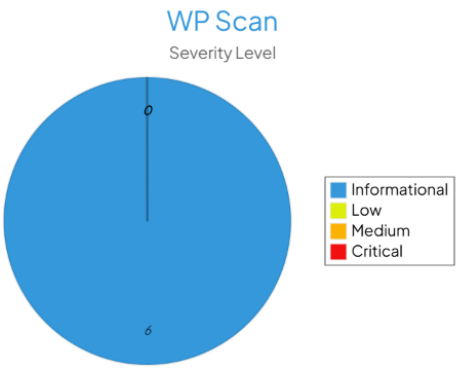


Gambar 7. Hasil scan menggunakan WPScan

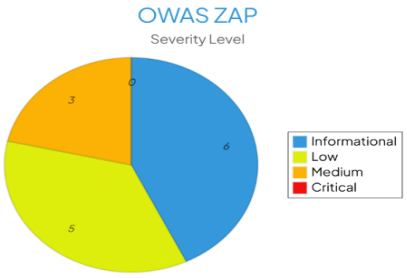
Hasil pemindaian dari WP*Scan* menunjukkan bahwa tidak ditemukannya kerentanan yang berarti seperti level critical maupun medium vulnerability pada situs web teknblog.top. Beberapa temuan hanya bersifat Informational dengan detail temuan terlihat pada tabel 4. Temuan informational pada WP*Scan* memberikan informasi tentang kerentanan di situs WordPress, tetapi tidak secara langsung menunjukkan adanya eksploitasi yang berhasil.

Tabel 4. Hasil *Scan* menggunakan WP*Scan*

No	Jenis Kerentanan	Level
1	robots.txt found	Info
2	XML-RPC seems to be enabled	Info
3	WordPress readme found	Info
4	The external WP-Cron seems to be enabled	Info
5	WordPress version 6.7.1 identified	Info
6	WordPress theme in use: seos-blog	Info



Gambar 8. WPScan Severity level

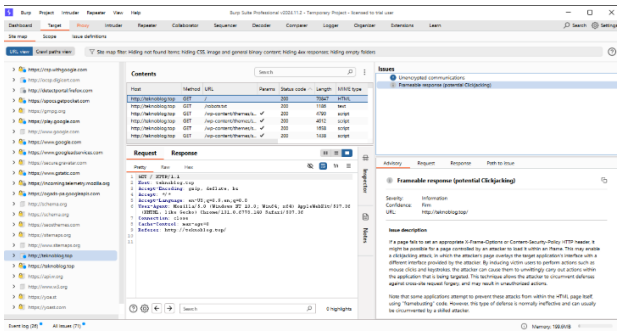


Gambar 9. OwasZap severity level

Tidak semua hasil temuan pada penelitian ini dilakukan eksploitasi. Tantangan terjadi ketika alat pemindaian dan eksploitasi yang dijalankan dengan agresif memicu pemblokiran IP *Address* oleh sistem keamanan *Firewall* pada *platform* Wordpress secara otomatis. Jenis serangan yang dapat memicu pemblokiran IP *Address* seperti, *Distributed Denial of Service* DDoS, *Brute Force Attack*, SQL *Injection*, XSS *Cross Site Scripting*, dan *Spoofing* atau aktivitas penyamaran.

Exploitation

Pada tahap eksploitasi batasan yang ditentukan dalam penelitian ini terjadi ketika temuan mencapai tingkat keparahan *medium dan critical vulnerabilities.* Hasil kerentanan yang ditemukan dari WP*Scan* hanya bersifat *informational.* Sedangkan kerentanan lain yang ditemukan pada OWAS ZAP yaitu *Missing Anti-clickjacking* dengan tingkat keparahan *medium level.* Dampak dari keamanan *firewall* pada *platfrom* WordPress menyebabkan pengujian dan eksploitasi dibatasi pada temuan *Missing Anti-clickjacking.* Peneliti akan membuat simulasi serangan pada hasil temuan *Missing Anti-clickjacking Header* dan melakukan validasi dalam bentuk PoC *Proof of Concept.* Penggunaan burpsuite *scanner* dapat difungsikan secara otomatis untuk megidentifikasi adanya potensial kerentanan *Missing Anti-clickjacking Header* pada situs web.

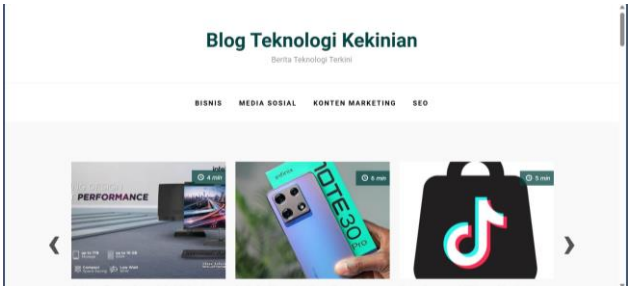


Gambar 10. Burpsuite scanner potensial clickjacking

Dari gambar diatas pada konten HTML terlihat jika *header* dari situs web berpotensi pada serangan *clickjacking.* Perubahan dari *frame header* dan modifikasi elemen tidak sah dapat terjadi pada kelemahan sperti ini. Penyebab dari kerentanan ini adalah situs web tidak menggunakan keamanan pada *header* seperti *X Frame Options* atau *Content Security Policy* untuk menghindari potensi serangan *clickjacking* yang dapat merugikan pengguna dan pengembang situs web. Pengujian yang pertama pada kerentanan *Missing Anti-clickjacking* disimulasikan dengan cara manual melalui *browser* untuk memastikan pengujian tidak berdampak 986ystem986e pada 986ystem. Oleh karena itu peneliti menulis script HTML sederhana menggunakan teks editor yang bertujuan untuk merubah frame pada halaman situs web.

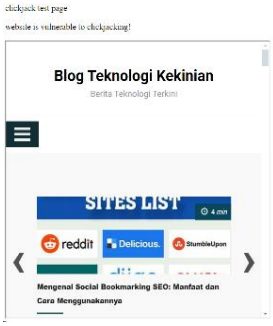
```
<html>
<head>
<tittle>clickjack test page</tittle>
</head>
<body>
<p>website is vulnerable to clickjacking!</P>
<iframe src="https://teknoblog.top/" width="500" height="500"></iframe>
</body>
</html>
```

Gambar 11. Script Alternatif pengujian manual *Missing Anti-clickjacking Header*



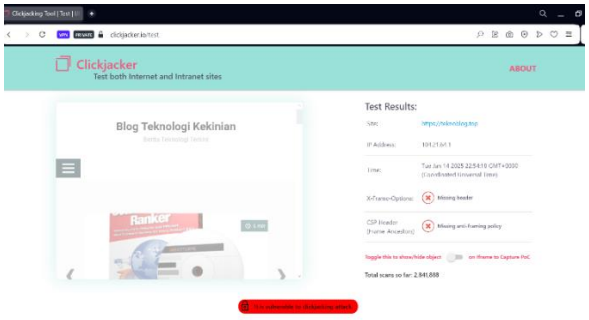
Gambar 12. Halaman sebelum pengujian

Pada gambar 12. Terlihat bahwa situs web masih dapat diakses sesuai dengan isi halaman asli.



Gambar 13. Halaman setelah pengujian Clickjacking

Pada gambar 13. Ukuran *frame* dari halaman situs web berhasil dirubah dengan penggunaan modifikasi script HTML sederhana. Situs web yang tidak memiliki kerentanan *Missing Anti clickjacking* akan memberikan *response blocked* kepada akses penelusuran terhadap situs web ketika *sciprt* diujikan melalui browser dengan format html. Setelah melakukan pengujian secara manual, tahap selanjutnya peneliti melakukan pengujian melalui situs web clickjacker.io untuk menguji akurasi temuan kerentanan *Missing Anti clickjacking Header* yang sebelumnya ditemukan dari alat pemindaian OWAS ZAP.



Gambar 14. Pengujian melalui Clickjacker.io

Pada gambar 14. Terlihat bahwa situs web tidak memiliki keamana pada *header* yang menyebabkan kerentanan berhasil dibuktikan. Implikasi terhadap pengelolaan keamanan situs web setelah melakukan perbaikan terkait temuan *Missing Anti ClickJacking* adalah peningkatan keamanan pengunjung situs web dalam mengakses informasi yang dimuat pada blog. Implementasi proteksi *anti clickjacking* secara signifikan mampu menjaga integritas dan keakuratan informasi yang akan berdampak pada kualitas dan kepuasan pengunjung pada situs web. Berdasarkan temuan kerentanan dengan tingkat keparahan rendah dan menengah yang dihasilkan dari pemindaian menggunakan *OWASP ZAP*, beberapa rekomendasi perbaikan dapat diberikan untuk meningkatkan keamanan situs web. Pertama, untuk mengatasi *Absence of Anti-CSRF Tokens*, disarankan untuk menambahkan token Anti-CSRF yang disimpan dalam formulir sebagai field yang tersembunyi. Kedua, untuk menangani *Content Security Policy CSP Header Not Set*, perlu ditambahkan header *Content-Security-Policy* ke dalam respons HTTP. Selanjutnya, untuk mengatasi *Missing Anti-clickjacking Header*, disarankan untuk menambahkan header *X-Frame-Options* atau menggunakan *Content-Security-Policy* (*CSP*). Untuk *Cookie No HttpOnly Flag*, atribut *HttpOnly* perlu ditambahkan saat mengatur cookie dari sisi server. Begitu juga dengan *Cookie without SameSite Attribute*, yang membutuhkan penambahan atribut *SameSite* pada cookie sensitif. Untuk *Strict-Transport-Security Header Not Set*, disarankan untuk menambahkan header *Strict-Transport-Security* (HSTS). Terkait dengan *Timestamp Disclosure – Unix*, akses terhadap data yang mengandung informasi waktu, seperti timestamp, dalam respons HTTP harus dikendalikan dan timestamp yang terlihat di file yang diunduh serta header pada log perlu dihilangkan atau disamarkan. Terakhir, untuk mengatasi *X-Content-Type-Options Header Missing*, disarankan untuk menambahkan header *X-Content-Type: nosniff* untuk mencegah browser mencoba menebak tipe MIME dari respons. Implementasi rekomendasi ini akan memperkuat keamanan situs web dan mengurangi potensi kerentanannya terhadap serangan.

Pembahasan

Berdasarkan hasil pemindaian yang dilakukan dengan menggunakan alat *OWASP ZAP*, sejumlah kerentanannya ditemukan pada situs web teknoblog.top yang perlu segera ditangani untuk meningkatkan tingkat keamanannya. Penemuan ini sesuai dengan temuan sebelumnya yang menunjukkan bahwa pengujian penetrasi merupakan langkah penting dalam mengidentifikasi dan menanggulangi kerentanan situs web (Aziz, 2021). Kerentanan yang ditemukan, seperti *Absence of Anti-CSRF Tokens*, memerlukan penanganan segera, karena dapat membuka peluang bagi serangan *Cross-Site Request Forgery* (CSRF) yang dapat merusak integritas data. Menambahkan token Anti-CSRF sebagai field tersembunyi dalam formulir, seperti yang disarankan oleh Burhani & Priyawati (2024), dapat mengurangi potensi serangan ini dengan memastikan bahwa hanya permintaan yang sah yang diterima oleh situs web. Selain itu, temuan terkait dengan *Content Security Policy (CSP) Header Not Set* juga menjadi perhatian serius. Sejalan dengan penelitian oleh Darojat *et al.* (2022), CSP berfungsi untuk melindungi aplikasi web dari serangan *Cross-Site Scripting* (XSS) dengan membatasi sumber daya yang dapat dimuat oleh halaman web. Dengan menambahkan header *Content-Security-Policy* ke dalam respons HTTP, situs web dapat lebih terproteksi dari serangan yang memanfaatkan celah XSS.

Kerentanan *Missing Anti-clickjacking Header* yang ditemukan juga menandakan bahwa situs web rentan terhadap serangan *Clickjacking*. Menambahkan header *X-Frame-Options* atau menggunakan *Content-Security-Policy* (*CSP*) adalah langkah yang tepat untuk mencegah situs web dimuat dalam iframe di situs yang tidak sah, sebagaimana yang telah dibahas oleh Mamuriyah *et al.* (2024) dalam penelitiannya mengenai perlindungan terhadap serangan siber. Langkah ini penting untuk melindungi pengalaman pengguna dan mencegah eksploitasi celah keamanan ini. Pada *Cookie No HttpOnly Flag dan Cookie without SameSite Attribute*, penambahan atribut *HttpOnly* dan *SameSite* pada cookie dapat mengurangi risiko serangan, seperti yang dijelaskan oleh Wen & Katt (2023), yang mengemukakan bahwa pengaturan ini membantu mencegah pencurian cookie melalui skrip berbahaya dan serangan *Cross-Site Request Forgery* (CSRF). Perlindungan terhadap cookie sangat penting karena mereka sering kali menyimpan informasi sensitif yang dapat dimanfaatkan oleh penyerang. *Strict-Transport-Security Header Not Set* merupakan temuan lain yang menunjukkan bahwa situs web tidak memaksa penggunaan HTTPS, yang bisa memungkinkan serangan *Man-in-the-Middle* (MITM). Menambahkan header *Strict-Transport-Security* (HSTS) akan mengarahkan browser untuk hanya mengakses situs web melalui HTTPS, yang penting untuk melindungi data dari pemantauan atau perubahan yang dilakukan oleh pihak ketiga (Riyanti *et al*., 2024).

Temuan *Timestamp Disclosure – Unix* menunjukkan bahwa situs web membocorkan informasi waktu yang dapat dimanfaatkan oleh penyerang untuk merancang serangan lebih lanjut. Sebagaimana dianjurkan oleh Laksmiati (2023), pengontrolan akses terhadap data timestamp dalam respons HTTP sangat diperlukan untuk mencegah penyalahgunaan informasi ini. Terakhir, *X-Content-Type-Options Header Missing* menunjukkan bahwa situs web memungkinkan browser untuk menebak tipe MIME, yang bisa mengekspos situs web terhadap serangan. Menambahkan header *X-Content-Type: nosniff* dapat mencegah browser menebak tipe MIME dan memastikan bahwa hanya tipe yang benar-benar ditentukan oleh server yang digunakan (Dasmen *et al*., 2023). Perbaikan terhadap kerentanan yang ditemukan pada situs web teknoblog.top sangat diperlukan untuk meningkatkan keamanannya. Langkah-langkah perbaikan yang disarankan, seperti menambahkan header keamanan yang tepat dan mengatur atribut cookie, akan memperkuat perlindungan situs web terhadap berbagai ancaman siber. Implementasi rekomendasi ini sejalan dengan penelitian yang menunjukkan bahwa pengujian penetrasi dan pemantauan rutin terhadap situs web dapat membantu mengidentifikasi dan mengatasi potensi kerentanannya sebelum dieksploitasi oleh penyerang (Ramadhani *et al*., 2024).

4. Kesimpulan dan Saran

Berdasarkan hasil dari penelitian disimpulkan bahwa tidak semua tools vulnerability dapat menemukan kerentanan yang sama pada sebuah situs web. WP*Scan* tidak menemukan kerentanan yang berarti sedangkan OwasZap menemukan beberapa kerentanan yang bahkan dapat dieksploitasi seperti *Missing Anti-clickjacking Header*. Kerentanan keamanan yang tidak terdeteksi dari situs web memberikan dampak buruk pada kehilangan data sensitif, gangguan operasional dan kerusakan reputasi pada situs web. Bahkan risiko dari serangan siber dapat mencapai kerugian finasial akibat pengeluaran biaya, perbaikan sistem, pemulihan data dan kehilangan aset berharga. Penelitian ini memberikan manfaat bahwa dengan melakukan pengujian penetrasi secara rutin pada situs web akan membantu pengelolaan keamanan yang lebih efektif untuk mengetahui celah keamanan yang sebelumnya tidak terdeteksi pada sebuah situs web. Pengembang situs dapat lebih mampu memitigasi risiko kerugian serangan siber yang tidak terduga dimasa depan dengan melakukan pengujian penetrasi yang ditujukan untuk perbaikan keamanan sistem. Rekomendasi perbaikan pada temuan *Missing Anti-clickjacking Header* pada situs web yaitu dengan menambahkan header *X Frame Options* dengan pengaturan pilihan yang sesuai seperti *deny*, ini adalah pilihan kemanan ketat dimana halaman web tidak dapat dimuat pada *iframe* manapun termasuk situs yang sama. Pilihan lain, *sameorigin* pilihan ini memberikan fleksibilitas untuk memuat *iframe* halaman pada situs web yang sama namun mencegah dimuat pada situs lain. Saran untuk penelitian selanjutnya menggunakan alat pemindaian kerentanan yang berbeda seperti Nessus dan Arachni atau *tools*

lainnya untuk mengidentifikasi celah keamanan yaitu kelemahan pada situs atau aplikasi web. Pengujian penetrasi pada platform *content management system* CMS lainnya juga penting untuk diuji.

5. Ucapan Terima Kasih

Dengan segala kerendahan hati dan rasa hormat, penulis ingin menyampaikan rasa terima kasih yang tulus kepada Orangtua, untuk semua dukungan moral dan materi selama proses penelitian ini. Tanpa doa yang tiada henti disujudkan, penulis merasa tidak akan bisa mencapai pencapaian ini. Terimakasih kepada Anisatul Asiyah berkat motivasi dan inspirasi serta perhatian dan kesetiaan yang diberikan dengan tulus sehingga penelitian ini berlangsung dengan sebagaimana mestinya. Terimakasih kepada Bapak Dwi Budi yang telah membimbing proses penelitian dan memberikan ruang juga waktu untuk berdiskusi dalam penelitian ini. Semoga Allah SWT senantiasa melimpahkan berkah dan rahmat-Nya kepada mereka.

6. Daftar Pustaka

Aziz, M. (2021). Vulnerability assesment untuk mencari celah keamanan web aplikasi e-learning pada Universitas XYZ. *Jecsit*, *1*(1), 101-109.

Burhani, L. F., & Priyawati, D. (2024). Analisis Pengujian Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode Penetration Testing Execution Standard (Ptes). *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, *9*(1), 307-319. https://doi.org/10.29100/jipi.v9i1.4455.

Darojat, E. Z., Sediyono, E., & Sembiring, I. (2022). Vulnerability assessment website e-government dengan NIST SP 800-115 dan OWASP menggunakan web vulnerability scanner. *Jurnal Sistem Informasi Bisnis, 12*(1), 36–44. https://doi.org/10.21456/vol12iss1pp36-44.

Dasmen, R. N., Rasmila, R., Widodo, T. L., Kundari, K., & Farizky, M. T. (2023). Pengujian penetrasi pada website eLearning2.binadarma.ac.id dengan metode PTES (Penetration Testing Execution Standard). *Jurnal Komputer dan Informatika, 11*(1), 91–95. https://doi.org/10.35508/jicon.v11i1.9809.

Dharmawan, A. (2022). Penetration testing menggunakan OWASP top 10 pada domain xyz. ac. id. *Electro Luceat*, *8*(1), 100-108. https://doi.org/10.32531/jelekn.v8i1.455.

Kurniawan, H., & Christianto, E. (2024). Analysis Vulnerability Website Baleomolcreative dengan Metode Penetration Testing Execution Standard & Vulnerability Assessment Pada Http Response Header Field. *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, *8*(3), 734-745. https://doi.org/10.35870/jtik.v8i3.2202.

Laksmiati, D. (2023). Vulnerability assessment with network-based scanner method for improving website security. *Journal of Computer Networks, Architecture and High Performance Computing, 5*(1), 38–45. https://doi.org/10.47709/cnahpc.v5i1.1991.

Mamuriyah, N., Prasetyo, S. E., & Sijabat, A. O. (2024). Rancangan sistem keamanan jaringan dari serangan DDoS menggunakan metode pengujian penetrasi. *Jurnal Teknologi Dan Sistem Informasi Bisnis, 6*(1), 162–167. https://doi.org/10.47233/jteksis.v6i1.1124.

Pratiwi, D., Santoso, G. B., Mardianto, I., Sediyono, A., & Rochman, A. (2020). Pengelolaan pengelolaan konten web menggunakan WordPress, Canva dan Photoshop untuk guru-guru wilayah Jakarta. *Abdihaz: Jurnal Ilmiah Pengabdian pada Masyarakat, 2*(1), 11. https://doi.org/10.32663/abdihaz.v2i1.1093.

Ramadhani, G. T. A., Steyer, M. R. R., Maulidan, M. H., & Setiawan, A. (2024). Analisis kerentanan WordPress dengan WPScan dan teknik mitigasi. *Journal of Internet and Software Engineering, 1*(4), 15. https://doi.org/10.47134/pjise.v1i4.2613.

Riyanti, A., Rahmanto, B. M., Hardianto, D. R., Yuristiawan, R. D. A., & Setiawan, A. (2024). Uji penetrasi injeksi SQL terhadap celah keamanan database website menggunakan SQLmap. *Journal of Internet and Software Engineering,* *1*(4), 9. https://doi.org/10.47134/pjise.v1i4.2623.

Utama, D. A., Khairil, K., & Supardi, R. (2024). Analisis Keamanan Website Menggunakan PTES (Penetration Testing Execution And Standart). *Jurnal Media Infotama*, *20*(1), 106-112. https://doi.org/10.37676/jmi.v20i1.5367.

Wen, S. F., & Katt, B. (2023). A quantitative security evaluation and analysis model for web applications based on OWASP application security verification standard. *Computers and Security,* *135*. https://doi.org/10.1016/j.cose.2023.103532.

Zahwa, F. A., & Syafi'i, I. (2022). Pemilihan pengembangan media pembelajaran berbasis teknologi informasi. *Equilibrium: Jurnal Penelitian Pendidikan Dan Ekonomi*, *19*(01), 61-78. https://doi.org/10.25134/equi.v19i01.3963.