Jurnal Pendidikan dan Teknologi Indonesia (JPTI)
Vol. 5, No. 1, Januari 2025, Hal. 155-166
DOI: https://doi.org/10.52436/1.jpti.609
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Analisis Kerentanan Pada Aplikasi Web Menggunakan Metode PTES

Farhan Widianto[*1], Ermadi Satriya Wijaya[2], Harjono[3], Agung Purwo Wicaksono[4]

[1,2,3,4]Teknik Informatika, Fakultas Teknik dan Sains, Universitas Muhammadiyah Purwokerto, Indonesia
Email: [1]farhanwidi27@gmail.com, [2]ermadi_satriya@ump.ac.id

Abstrak

Aplikasi web seringkali memiliki berbagai kerentanan yang dapat mengancam keamanan dan integritas sistem. Salah satu masalah yang ditemukan pada website cobaupgradediri.com adalah terdapat celah kerentanan *Missing Anti-clickjacking Header* yang berpotensi mengakibatkan serangan *clickjacking* yang dapat mengganggu fungsi operasional serta keamanan website. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan yang dapat dieksploitasi pada kerentanan *Missing Anti-clickjacking Header* pada website cobaupgradediri.com. Untuk mengatasi permasalahan ini, maka dilakukan identifikasi kerentanan yang dapat dieksploitasi menggunakan metode *Penetration Testing Execution Standard* (PTES). Hasil pengujian menunjukan bahwa website cobaupgradediri.com rentan terhadap serangan *clickjacking*. Solusi yang dilakukan untuk mengatasi permasalahan pada penelitian ini adalah dengan menambahkan *Anti-clickjacking Header* pada konfigurasi server yang akan memberikan instruksi kepada browser untuk membatasi penayangan halaman dalam *iframe*. Urgensi pada penelitian ini terletak pada meningkatnya jumlah serangan siber terhadap aplikasi web, terutama serangan *clickjacking* yang seringkali diabaikan oleh pengembang karena sifatnya yang tersembunyi. Penelitian ini memberikan wawasan penting tentang pentingnya perlindungan terhadap kerentanannya guna menjaga keamanan dan integritas aplikasi web.

Kata kunci: *Aplikasi Web, Keamanan Siber, Metode PTES, Penetration Testing*

Vulnerability Analysis on Web Applications Using the PTES Method

Abstract

Web applications often have various vulnerabilities that can threaten the security and integrity of the system. One of the problems found on the cobaupgradediri.com website is that there is a Missing Anti-clickjacking Header vulnerability that has the potential to cause clickjacking attacks that can interfere with operational functions and website security. This research aims to identify and analyze vulnerabilities that can be exploited in the Missing Anti-clickjacking Header vulnerability on the website cobaupgradediri.com. To overcome this problem, identification of exploitable vulnerabilities using the Penetration Testing Execution Standard (PTES) method is carried out. The test results show that the website cobaupgradediri.com is vulnerable to clickjacking attacks. The solution to overcome the problems in this research is to add an Anti-clickjacking Header to the server configuration which will instruct the browser to limit page views in the iframe. The urgency of this research lies in the increasing number of cyberattacks against web applications, especially clickjacking attacks which are often overlooked by developers due to their hidden nature. This research provides important insights into the importance of vulnerability protection to maintain the security and integrity of web applications.

Keywords: *Cyber Security, Penetration Testing, PTES Method, Web Application*

1. PENDAHULUAN

Di era kemajuan teknologi informasi, perkembangan website mengalami kemajuan secara signifikan dapat dilihat dari meningkatnya jumlah pengguna layanan internet setiap tahunnya[1]. Keamanan informasi bagi pengguna web merupakan aspek yang sangat penting dengan fakta menunjukkan bahwa situs web sering kali menyimpan data sensitif pengguna, seperti data pribadi, informasi keuangan, dan berbagai informasi lainnya[2]. Seringkali ditemukan berbagai kerentanan pada aplikasi web. Kerentanan ini, yang sering disebut sebagai *vulnerability*, membuka peluang bagi penyerang untuk melancarkan serangan dengan tujuan yang tidak sah[3]. Salah satu elemen utama dalam keamanan siber adalah kemampuan untuk mengenali dan mengevaluasi kerentanan pada sebuah website[4].

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Permasalahan muncul karena ditemukannya celah kerentanan pada website cobaupgradediri.com sehingga menyebabkan potensi serangan siber yang dapat menggangu fungsi operasional pada website. Mengingat cobaupgradediri.com adalah platform teknologi pendidikan yang menyimpan data sensitif pengguna. Banyak cara untuk menyelesaikan permasalahan tersebut yang dapat mengurangi risiko terjadinya serangan siber, salah satunya yaitu analisis kerentanan dan exploitasi sesuai dengan metode PTES. Untuk mengurangi risiko kejahatan siber perlu dilakukan simulasi serangan guna mengukur tingkat keamanan suatu sistem, yang dikenal dengan *penetration testing*. *Penetration testing* merupakan simulasi serangan terhadap sistem komputer untuk mengidentifikasi kerentanan, ancaman, dan potensi risiko dalam sistem, aplikasi perangkat lunak, jaringan, atau aplikasi web yang dapat dieksploitasi oleh penyerang[5]. *Penetration testing* pada penelitian ini bertujuan untuk melakukan pengujian serangan yang berfungsi untuk memvalidasi atas celah kerentanan yang didapat. Tahapan *penetration testing* ini cocok digunakan untuk menyelesaikan permasalahan yang terjadi pada penelitian ini. Pada penelitian ini ditemukan celah kerentanan *Missing Anti-clickjacking Header* yang beresiko terjadinya serangan *clickjacking* yang dapat mengganggu fungsi dan keamanan integritas pada sistem. Masalah itulah yang menjadi pilihan mengapa harus melakukan penelitian ini. Urgensi pada penelitian ini terletak pada meningkatnya jumlah serangan siber terhadap aplikasi web, terutama serangan *clickjacking* yang seringkali diabaikan oleh pengembang karena sifatnya yang tersembunyi. *Clickjacking* adalah tipe serangan pada aplikasi web yang memanipulasi korban agar tanpa sengaja mengklik elemen halaman web yang sebenarnya tidak mereka niatkan untuk diklik. Kerentanan ini memungkinkan penyerang untuk memanfaatkan situs web sebagai sarana untuk melakukan *phishing*[6]. Serangan *clickjacking* yang diujikan ini menunjukkan bahwa website target masih memiliki celah kerentanan dan belum sepenuhnya terlindungi dari ancaman pihak luar.

Penelitian ini sebagai solusi untuk mengatasi permasalahan mengenai kerentanan *Missing Anti-clickjacking Header* yang beresiko terjadinya serangan *clickjacking* yang terdapat pada website target. Dengan tujuan untuk mengevaluasi keamanan aset teknologi informasi dengan mengidentifikasi kerentanan yang dapat di exploitasi sesuai dengan tahapan metode *Penetration Testing Execution Standard* (PTES). Penelitian ini menerapkan metode PTES untuk menganalisis kerentanan secara sistematis. Metode PTES dipilih karena tahapannya memungkinkan proses identifikasi dan validasi kerentanan dilakukan secara mendalam, sehingga mampu menghasilkan solusi yang praktis dan dapat diterapkan. Meskipun telah banyak penelitian sebelumnya yang membahas penerapan PTES, pendekatan dalam penelitian ini memiliki perbedaan mendasar dibandingkan dengan studi-studi terdahulu.

Penelitian sebelumnya hanya berfokus pada identifikasi kerentanan tanpa validasi eksploitasi langsung. Sebagai contoh, penelitian oleh[7] *penetration testing* memberikan informasi mendalam dan terkini mengenai ancaman keamanan yang berpotensi dieksploitasi jika tidak dikelola dengan baik dalam alur dan proses keamanan organisasi. Proses ini memungkinkan organisasi untuk mengidentifikasi potensi kerentanan nyata dengan lebih cepat dan tepat. Menurut peneliti[8] dapat disimpulkan bahwa analisis kerentanan aplikasi website SMKN 1 Cibatu menggunakan metode *Penetration Testing Execution Standard* (PTES) dapat mengidentifikasi kerentanannya pada sistem informasi. Penelitian lain menurut[9] artikel ini membahas penerapan metode PTES dalam melakukan pengujian pada sebuah website untuk mengidentifikasi berbagai celah keamanan, termasuk kerentanan terhadap serangan *clickjacking.* Menurut penelitian[10] jurnal ini menjelaskan analisis keamanan website melalui metode PTES serta evaluasi kerentanan yang telah ditemukan. Penelitian ini pada tahap penilaian kerentanannya, ditemukan kelemahan dalam konfigurasi keamanan situs web yang dikenal sebagai *security misconfiguration*. Kelemahan ini seharusnya dapat mencegah serangan seperti *clickjacking*[11]. Penelitian ini mengisi kekosongan yang ada pada penelitian sebelumnya yang meliputi, verifikasi kerentanan yang terbukti dimana banyak penelitian hanya mengidentifikasi kerentanan tanpa memastikan apakah celah tersebut bisa dieksploitasi dalam kondisi nyata, fokus pada kerentanan secara spesifik dimana pada penelitian hanya membahas kerentanan secara umum, namun tidak fokus pada masalah khusus seperti *Missing Anti-clickjacking Header* yang dapat membuka potensi serangan *clickjacking,* pengujian eksploitasi yaitu berbeda dengan penelitian sebelumnya, penelitian ini tidak hanya mengidentifikasi kerentanannya, tetapi juga menguji apakah kerentanannya dapat dieksploitasi, memberikan solusi mitigasi yang tepat dimana pada penelitian ini memberikan solusi yang lebih praktis dan terarah, seperti implementasi *Anti-clickjacking Header*, untuk mencegah potensi serangan yang tidak dibahas dalam penelitian lain. Dengan demikian, penelitian ini memberikan pendekatan yang lebih fokus dan aplikatif dalam mengatasi kerentanannya. Penelitian ini mengisi *gap* tersebut dengan menyoroti kerentanan spesifik yaitu *Missing Anti-clickjacking Header*, serta melakukan uji eksploitasi untuk memastikan apakah celah ini benar-benar dapat dimanfaatkan dalam aplikasi web yang diteliti**.**

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan *Missing Anti-clickjacking Header* pada situs web cobaupgradediri.com, serta melakukan uji eksploitasi terhadap kerentanannya untuk memastikan apakah celah tersebut dapat dimanfaatkan dalam serangan terhadap aplikasi web. Selain itu, penelitian ini bertujuan untuk memberikan solusi mitigasi yang praktis, seperti penerapan *Anti-clickjacking Header*, guna meminimalkan risiko serangan *clickjacking* dan memperkuat keamanan aplikasi web.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

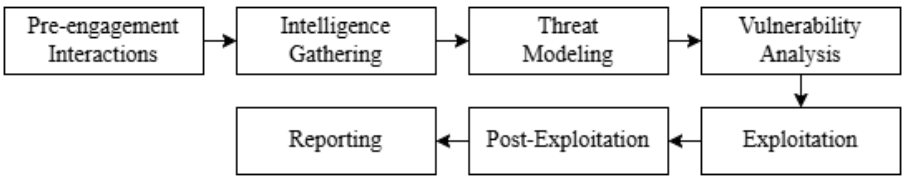
Dengan demikian penelitian ini tidak hanya memberikan kontribusi terhadap pemilik sistem pada website target, tetapi juga memberikan solusi yang baik yang dapat dipahami oleh pemilik website dalam melakukan perbaikan sistem didalamnya agar menjadi lebih aman dari serangan oleh pihak yang tidak bertanggung jawab, contohnya *hacker*. Aktivitas ini hanya dapat dilakukan dengan izin resmi dari pemilik sistem.

Ruang lingkup pada website cobaupgradediri.com batasan yang akan difokuskan pada pengujian satu kerentanan terhadap web aplikasi yang memiliki fungsi operasional penting bagi organisasi, konfirmasi terkait pendekatan metode *Penetration Testing Execution Standard* (PTES) dan dalam melakukan pengujian kerentanan sistem, menggunakan sistem operasi Kali Linux. Kali Linux adalah distribusi Linux tingkat lanjut yang dirancang khusus untuk *penetration testing* dan audit keamanan[12]. Perangkat lunak yang digunakan dalam pengujian untuk mendukung langkah-langkah penelitian menggunakan metode PTES yaitu sistem operasi Kali Linux, dan *tools* yang berjalan diatasnya yatu *tools* Whois, Whatweb, Nmap, Nikto, OWASP-ZAP dan Burp Suite.

2. METODE PENELITIAN

Isi dari metode penelitian adalah memformulasikan permasalahan yang diteliti dengan lebih rinci (sedapat mungkin ditulis secara matematis) dan menjelaskan metode yang diusulkan. Apabila menggunakan sebuah algoritma, dapat dijelaskan di bagian

Pengujian *penetration testing* adalah metode untuk mengevaluasi keamanan aset teknologi informasi dengan mengidentifikasi kerentanan yang dapat dimanfaatkan oleh pihak tidak berwenang. Proses ini dapat dilakukan secara manual oleh penguji keamanan atau diotomatisasi menggunakan perangkat lunak khusus [13]. Metode yang digunakan adalah *Penetration Testing Execution Standard* (PTES) yaitu metodologi yang dirancang untuk memberikan panduan sistematis dan komprehensif dalam melaksanakan uji. Metode PTES dikembangkan pada tahun 2010 oleh para profesional di bidang keamanan informasi. Tujuannya adalah untuk menetapkan standar yang dapat memberikan panduan kepada klien dan penguji terkait penggunaan alat, teknik, serta berbagai elemen yang terlibat dalam proses uji penetrasi secara menyeluruh. Dalam pelaksanaannya, PTES terdiri dari 7 tahap, sebagaimana ditunjukkan pada Gambar 1 yaitu.



Gambar 1. Tahap metode PTES

1. *Pre-Engagement Interaction* bertujuan untuk mengidentifikasi serta menentukan alat dan teknik yang dapat digunakan untuk memastikan keberhasilan tahap awal uji penetrasi. Proses ini mencakup pengumpulan informasi awal dan salah satu dokumen terpenting dalam proses ini adalah izin resmi untuk melakukan pengujian[14].
2. *Intelligence Gathering* adalah proses mengumpulkan informasi yang diperlukan untuk mendukung pengujian penetrasi. Informasi biasanya mengenai situs web, alamat *Internet Protocol* (IP), server, layanan hosting, jenis domain, sistem *Domain Name System* (DNS), *port* yang terbuka, serta informasi lain yang relevan untuk mendukung proses pengujian kerentanan dari website cobaupgradediri.com menggunakan Kali Linux dengan *tools* yaitu Whois, Whatweb, dan Nmap[15]. Penggunaan Kali Linux pada penelitian ini sebagai platform utama yang mendukung berbagai *tools* yang digunakan pada rangkaian penelitian ini.
3. *Threat Modeling* merupakan tahap yang menentukan pendekatan terhadap model ancaman yang diperlukan untuk memastikan tindakan eksekusi yang sesuai dalam pengujian penetrasi. Dalam standar PTES, tidak ada model khusus yang ditentukan[9]. Pendekatan ini membantu dalam mengidentifikasi, menganalisis, dan memitigasi potensi ancaman yang dapat mempengaruhi keamanan sistem yang diuji [14].
4. *Vulnerability Analysis* adalah proses pengujian untuk mengidentifikasi kelemahan dalam sistem dan aplikasi yang berpotensi dieksploitasi oleh penyerang. Proses ini bertujuan untuk menemukan celah kerentanan yang nantinya kerentanan tersebut akan dilakukan uji pentesting, sehingga memungkinkan perbaikan sebelum dieksploitasi [14]. Kerentanan yang didapatkan yaitu *Missing Anti-clickjacking Header* yang beresiko terjadinya serangan *clickjacking. Tools* yang digunakan adalah Nikto dan OWASP-ZAP. *Tools* Nikto digunakan untuk mencari kerentanan pada *port* terbuka yang didapatkan. Nikto merupakan sebuah web server sekaligus alat untuk menilai aplikasi web guna mendeteksi masalah keamanan dan kerentanannya. Nikto dapat memeriksa hingga 6700 file atau program yang berpotensi membahayakan [1].

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Kemudian *Zed Attack Proxy* (ZAP) *tools* yang digunakan untuk mencari kerentanan website secara keseluruhan, kemudian hasilnya akan dilakukan analisa dan pengujian di tahap *exploitasu.* ZAP adalah aplikasi yang dirancang untuk melakukan pengujian penetrasi guna mengidentifikasi kerentanan pada aplikasi web dengan cara yang sederhana. ZAP menawarkan pemindai otomatis sekaligus alat untuk membantu menemukan kerentanan secara manual [16].

5. *Exploitation* adalah tahap dalam pengujian ini berfokus pada pengujian kerentanan yang didapatkan pada tahap *vulnerability analysis* berupa serangan *clickjacking* pada target. *Tools* yang digunakan yaitu Burp Suite sebagai pengujian *penetration testing* dari hasil kerentanan yang didapat. Burp Suite digunakan sebagai langkah pembuktian terhadap celah kerentanan dimana tidak hanya menyebutkan kerentanan tetapi juga melakukan uji cobanya. Burp suite merupakan salah satu alat yang paling banyak digunakan oleh profesional keamanan informasi dan peretas etis untuk melakukan pengujian penetrasi pada aplikasi web dan jaringan komputer [17].
6. *Post Exploitation* bertujuan untuk menilai pentingnya sistem yang berhasil dieksploitasi sekaligus memastikan kendali atas sistem tersebut tetap terjaga. Penilaian nilai sistem dilakukan berdasarkan tingkat sensitivitas data yang tersimpan di dalamnya serta fungsi sistem tersebut dalam jaringan yang menjadi target [9]. Tujuan utamanya adalah untuk mempertahankan akses yang telah diperoleh dan memanfaatkan kontrol tersebut demi tujuan lebih lanjut, seperti pengumpulan data atau perencanaan serangan lebih lanjut [14].
7. *Reporting* adalah tahap di mana hasil pengujian disusun dalam bentuk laporan yang mendetail, mencakup seluruh temuan dari proses uji serta presentasi yang telah disiapkan. Laporan ini juga menyertakan rekomendasi perbaikan dan solusi untuk masalah yang ditemukan selama pengujian [14].

Dengan mengikuti tahapan-tahapan yang juga dapat dilihat pada Tabel 1 dibawah, pengujian *penetration testing* yang disebutkan memenuhi kriteria metodologi PTES, menjadikannya pendekatan yang sistematis dan terstruktur untuk mengevaluasi keamanan sistem.

Tabel 1. Tabel Tahap PTES

Tahap	Tujuan	Alat yang Digunakan	Deskripsi
Pre-Engagement	Identifikasi alat dan teknik yang digunakan dalam pengujian	-	Proses pengumpulan infromasi dan izin untuk uji penetrasi
Intelligence Gathering	Pengumpulan informasi mengenai target	Whois, Whatweb, Nmap	Mengumpulkan data terkait situs web, IP, dan port terbuka
Threat Modeling	Menentukan model ancaman yang relevan	-	Mengidentifikasi ancaman yang dapat memengaruhi sistem
Vulnerability Analysis	Mengidentifikasi kelemahan yang dapat dieksploitasi	Nikto, OWASP-ZAP	Memindai dan menganalisis kerentanan aplikasi web
Exploitation	Menguji apakah kerentanan dapat dieksploitasi	Burp Suite	Pengujian eksploitasi, seperti serangan clickjacking
Post-Exploitation	Menilai kontrol yang diperoleh setelah eksploitasi	-	Mengevaluasi kontrol dan pentingnya sistem yang berhasil dieksploitasi
Reporting	Menyusun laporan pengujian dan rekomendasi perbaikan	-	Laporan akhir yang menyertakan hasil, analisis, dan rekomendasi

3. HASIL DAN PEMBAHASAN

Berikut ini adalah laporan beserta gambar dan tabel yang memaparkan hasil *Penetration Testing* menggunakan Kali Linux pada website target cobaupgradediri.com.

3.1. *Pre-engagement Interaction*

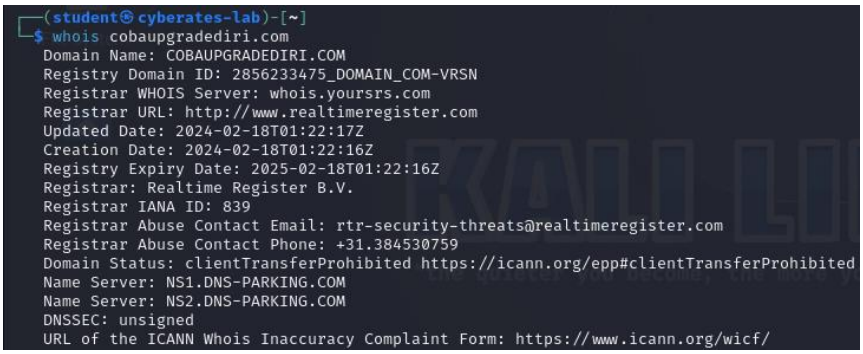
Pre-Engagement Interaction bertujuan untuk menentukan alat yang digunakan dalam tahap awal uji penetrasi. Alat yang digunakan diantaranya sistem operasi Kali Linux, Whois, Whatweb, Nikto, Nmap, OWASP-ZAP dan Burp Suite. Kemudian izin resmi sebagai dokumen dalam proses ini sudah didapatkan dari pemilik website cobaupgradediri.com beserta team didalamnya.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

3.2. *Intellegence Gathering*

3.2.1. Whois

Tahap Intellegence Gathering, fungsi Whois tetap berguna untuk mengumpulkan informasi lebih lanjut tentang domain, meskipun nama domain sudah didapatkan. Dengan perintah ”whois cobaupgradediri.com” didapatkan nama domain beserta informasi lainnya yang terlihat pada Gambar 2 dibawah yaitu ”COBAUPGRADEDIRI.COM”.



Gambar 2. Whois cobaupgradediri.com

Informasi dari hasil Whois bermanfaat untuk keamanan siber pada penelitian ini. Data seperti nama domain, registrasi, tanggal pembuatan, status, dan server DNS membantu mengidentifikasi asal-usul domain, memastikan keamanan, mendeteksi ancaman seperti DNS *hijacking*, dan melaporkan aktivitas mencurigakan. Hal ini penting untuk analisis kerentanan dan mitigasi ancaman. Hasil pencarian informasi domain dengan *tools* Whois dalam bentuk Tabel seperti terlihat pada Tabel 2 berikut:

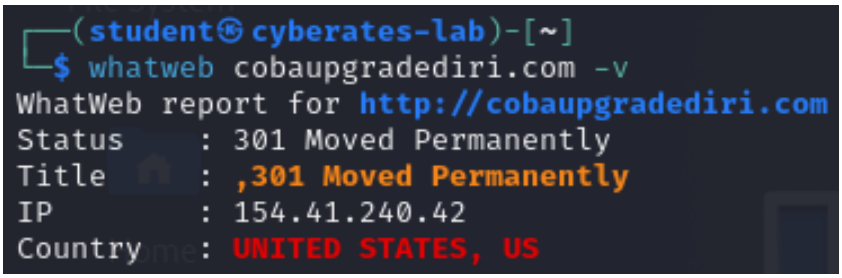
Tabel 2. Hasil Whois

	cobaupgradediri.com
Domain ID	2856233475_DOMAIN_COM-VRSN
Domain Name	COBAUPGRADEDIRI.COM
Creation Date	2024-02-18T01:22:16Z
Registry Expired Date	2025-02-18T01:22:16Z
Server Name	NS1.DNS-PARKING.COM, NS2.DNS-PARKING.COM
Domain Type	.COM

Berdasarkan hasil pencarian informasi domain yang ditampilkan pada Gambar 2, dan pada Tabel 2. Setelah melakukan pencarian informasi domain menggunakan Whois, langkah berikutnya adalah melakukan pemeriksaan jaringan dengan menggunakan Whatweb yang bertujuan mencari alamat *IP* target dan *plugin* pada web.

3.2.2. Whatweb

Penggunnaan *tools* Whatweb pada penelitian ini digunakan untuk mencari *IP* target dan mengetahui *plugin* yang digunakan pada pembuatan websitenya. Dengan perintah ”whatweb cobaupgradediri.com -v” pada Gambar 3 dibawah, maka akan didapatkan *IP* ”154.41.240.42” dan *plugin* yang digunakan pada pembuatan website tersebut.



Gambar 3. Whatweb cobaupgradediri.com

p-ISSN: 2775-4227
e-ISSN: 2775-4219

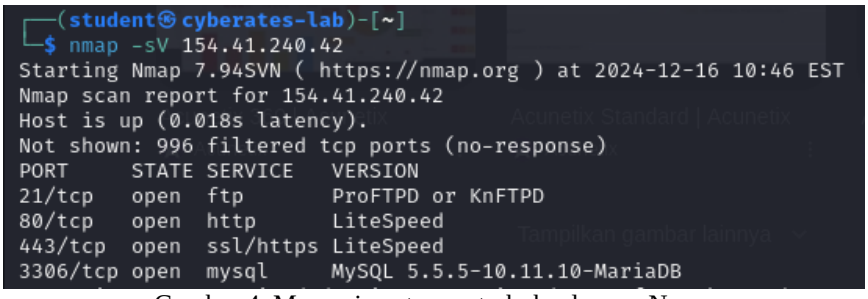
Setelah mendapatkan alamat *IP*, langkah selanjutnya adalah penggunaan *IP* untuk mencari *port* yang terbuka dan menganalisis layanan yang berjalan pada *port* tersebut menggunakan *tools* Nmap. Dengan mengetahui *port* terbuka, pengujian keamanan dapat menganalisis potensi kerentanan yang mungkin terdapat pada layanan atau aplikasi yang berjalan. Analisis ini membantu memahami lebih jauh tentang paparan target, mengidentifikasi titik lemah, serta merencanakan langkah mitigasi atau eksploitasi yang relevan. Hasil *plugin* menggunakan *tools* Whatweb. Pada Tabel 3, penggunaan Whatweb menunjukkan bahwa *platform* target menggunakan CMS WordPress, yang menjadi fokus analisis lebih lanjut.

Tabel 3. *IP* dan *Plugin*

Tools	Result IP	Web Technology	Plugin
Whatweb	154.41.240.42	Html	Html
		Http Server	Litespeed
		Platform (CMS)	Wordpress
		Jquery	JavaScript
		Script	Php
		Web Server	Litespeed

3.2.3. Nmap

Penggunaan *tools* Nmap untuk mencari *port* yang terbuka pada *IP* dari website target beserta layanannya. Dengan perintah ”nmap -sV 154.41.240.42” hasil yang didapatkan berupa 4 *port* yang terbuka yaitu *port ”21/tcp open”, ”80/tcp open”, ”443/tcp open” dan port ”3306/tcp open”* hasil ini memberikan gambaran *port* yang terbuka yang dilihat pada Gambar 4 dibawah, batasan penggunaan *port* yang terbuka hanya akan dilakukan *scanning* kerentanan yaitu pada *port* 80. Alasan hanya *port* 80 yang dilakukan *scaning*, karena *port* ini biasa dimanfaatkan dalam pencarian kerentanan karena berfungsi sebagai *port* default untuk komunikasi menggunakan HTTP (*Hypertext Transfer Protocol*), yang merupakan protokol utama dalam berbagai aplikasi web. Solusi untuk mencegah penyalahgunaan *port* yang terbuka pada aplikasi web oleh pentester atau pihak tidak bertanggung jawab, diperlukan langkah-langkah pengamanan dan pengelolaan akses yang ketat, diantaranya seperti penggunaan *firewall* untuk menyaring lalu lintas masuk dan keluar pada aplikasi, kemudian membatasi akses ke *port* dan layanan hanya untuk pengguna atau sistem yang benar-benar membutuhkan akses, melakukan pemantauan untuk mendeteksi aktivitas mencurigakan pada *port* yang terbuka, implementasi HTTPS, dan pembaruan sistem operasi secara rutin. Hasil dari *port* 80 yang terbuka akan dilakukan *vulnerability scanning* untuk mengetahui celah kerentanan didalamnya.



Gambar 4. Mencari *por*t yang terbuka dengan Nmap

Hasil dari pencarian informasi *port* yang terbuka menggunakan Nmap dalam bentuk Tabel 3 dibawah:

Tabel 3. Hasil pencarian *port* menggunakan Nmap

Tools	Target IP	TCP/UDP	Port
Nmap	154.41.240.42	tcp	21/open
		tcp	80/open
		tcp	443/open
		tcp	3306/open

3.3. *Threat Modeling*

Pengujian website cobaupgradediri.com, data yang diperoleh selama tahap *Intelligence Gathering* digunakan untuk mengidentifikasi potensi ancaman yang mungkin terjadi. Pendekatan ini memungkinkan tim

p-ISSN: 2775-4227
e-ISSN: 2775-4219

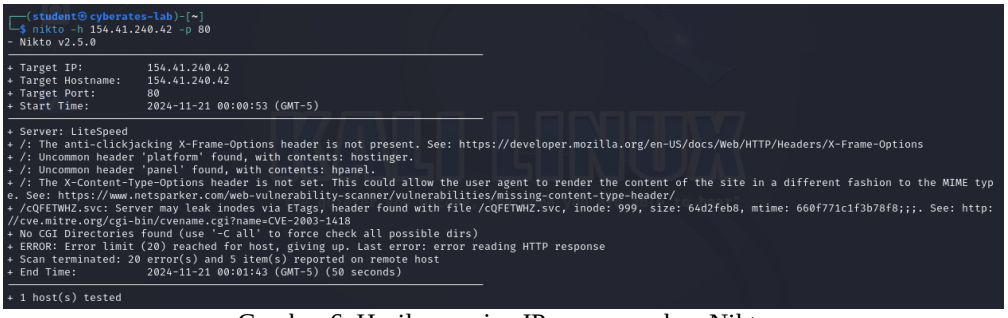
untuk menemukan kelemahan dalam sistem yang dapat dimanfaatkan oleh penyerang. Melalui permodelan ancaman, tim pengujian dapat merancang strategi mitigasi yang lebih optimal untuk mengurangi risiko pada sistem.

3.4. *Vulnerability Analysis*

3.4.1. Nikto

Scanning vulnerability analysis pada website cobaupgradediri.com menggunakan 2 *tools* yaitu Nikto dan OWASP-ZAP. Telah ditentukan batasan hanya akan dilakukan analisis kerentanan pada *port* 80, dimana *port* 80 (HTTP) sering menjadi prioritas dalam proses *port scanning* karena berfungsi sebagai default *port* untuk protokol HTTP yang digunakan oleh berbagai layanan web server seperti Apache, Nginx, atau IIS. Fokus pada *port* ini dilakukan karena banyak aplikasi web beroperasi di atasnya dan cenderung rentan terhadap serangan *clickjacking.*

Seperti ditunjukkan pada Gambar 6 dilakukan *scanning* menggunakan alamat *IP* target pada target *port* 80 yang bertujuan untuk menemukan kerentanan yang terdapat dalam sistem menggunakan *tools* Nikto dengan perintah "nikto -h 154.41.240.42 -p 80".

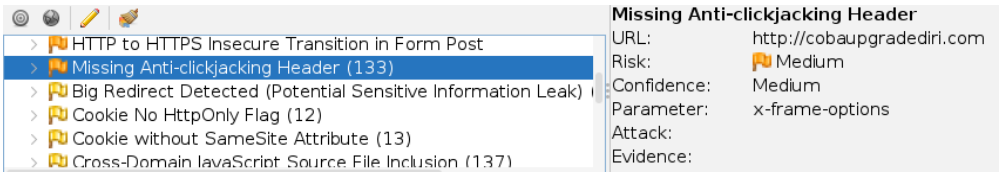


Gambar 6. Hasil *scanning* IP menggunakan Nikto

Hasil *scanning* menggunakan *tools* Nikto didapatkan berupa beberapa peringatan kerentanan pada website tetapi pada penelitian ini hanya difokuskan pada satu kerentanan yaitu Tidak adanya *header X-Frame-Options*. Dari kerentanan tersebut dimana *Header* ini berfungsi untuk mencegah situs situs lain yang dapat digunakan untuk melakukan serangan *clickjacking*. Kerentanan ini nantinya akan dilakukan pengujian *exploitasi* menggunakan *tools* Burp Suite untuk membuktikan apakah risiko benar terjadi serangan *clickjacking*. *Clickjacking* sendiri adalah teknik serangan di mana penyerang mengecoh pengguna untuk mengklik elemen tertentu di halaman web tanpa disadari, biasanya dengan cara menyembunyikan konten asli menggunakan frame transparan.

3.4.2. OWASP-ZAP

Scanning menggunakan *tools* OWASP-ZAP dengan perintah "http://cobaupgradediri.com" dengan meng-klik *attack* kemudian hasil dari *scanning* seperti terlihat pada Gambar 7 dibawah. Seperti yang sudah ditentukan diatas bahwa batasan hasil dari *scanning* uji kerentanan hanya akan diambil salah satu kerentanan yaitu *Missing Anti-clickjacking Header* dengan tingkat *alert Medium* dimana kerentanan ini beresiko terjadi serangan *clickjacking.* Hasilnya website ini belum menerapkan *header anti-Clickjacking*, yang berfungsi melindungi aplikasi dari serangan *clickjacking* dengan tujuan mencegah halaman dimuat dalam *iframe* oleh situs lain. Hasil kerentanan ini akan dilakukan pengujian eksploitasi pada serangan *clickjacking* untuk membuktikan apakah kerentanan yang dihasilkan terbukti rentan terhadap serangan *clickjacking*.



Gambar 7. *Scanning tools* ZAP

Pada Tabel 4, hasil *scanning* menggunakan OWASP-ZAP menunjukkan bahwa *Missing Anti-clickjacking Header* memiliki tingkat *alert Medium*.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Tabel 4. Hasil *Scanning* Menggunakan OWASP-ZAP

Vulnerability Analysis		
Tools	**Jenis Kerentanan**	**Level Alert**
OWASP-ZAP	Missing Anti-clickjacking Header	Medium

Penjelasan hasil kerentanan OWASP-ZAP dari jenis kerentanan yang didapat pada *scanning* menggunakan OWASP-ZAP *yaitu Missing Anti-clickjacking Header* terdapat pada Tabel 5 dibawah.

Tabel 5. Penjelasan hasil Kerentanan OWASP-ZAP

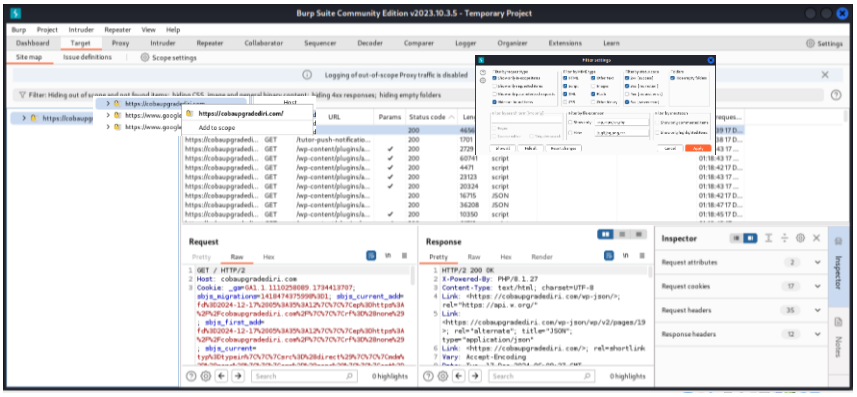
Jenis Kerentanan	Risiko	Solusi
Missing Anti-clickjacking Header	OWASP-ZAP mendeteksi respon tersebut tidak memberikan perlindungan terhadap serangan clickjacking. Untuk mengatasi hal ini, perlu ditambahkan Content-Security-Policy dengan direktif frame-ancestors atau menggunakan X-Frame-Options.	Web modern mendukung penggunaan Header HTTP seperti Content-Security-Policy dan X-Frame-Options. Pastikan salah satu Header diatur pada setiap halaman web yang dikirimkan oleh situs atau aplikasi. Jika halaman web hanya diizinkan untuk ditampilkan dalam bingkai (frame) oleh server yang sama (misalnya halaman bagian dari FRAMESET), gunakan opsi SAMEORIGIN. Namun, jika halaman tidak diizinkan untuk dibingkai sama sekali, gunakan opsi DENY. Alternatif lain, Anda bisa menerapkan kebijakan "frame-ancestors" melalui Content-Security-Policy untuk kontrol yang lebih fleksibel.

3.5. *Exploitation*

3.5.1. *Exploitation* dengan Burp Suite

Berdasarkan hasil analisa kerantanan pada website cobaupgradediri.com, ditemukan adanya kerentanan berupa *Missing Anti Clickjacking Header*. Kerentanan ini terjadi karena tidak adanya konfigurasi *X-Frame-Options* pada respon *server*. Padahal, konfigurasi ini berperan penting dalam melindungi situs dari serangan *clickjacking.* Pengujian exploitasi dari kerentanan *Missing Anti-clickjacking Header* menggunakan *tools* Burp Suite. Pengujian ini akan membuktikan apakah kerentanan yang dihasilkan terbukti rentan terhadap serangan *clickjacking*. Sehingga pengujian ini difokuskan pada uji coba serangan menggunakan konfigurasi *clickjacking* pada Burp Suite.

Langkah pengujian dengan setting pada Burp Suite yang dapat dilihat pada Gambar 8, kemudian menginputkan nama website pada menu *target* yang akan diarahkan pada *browser* yang berada didalam Burp Suite, kemudian setelah berhasil menginputkan targetnya, klik kanan url website target *"add to scope"* dan ceklis *"only scope items"* kemudian klik *apply*.

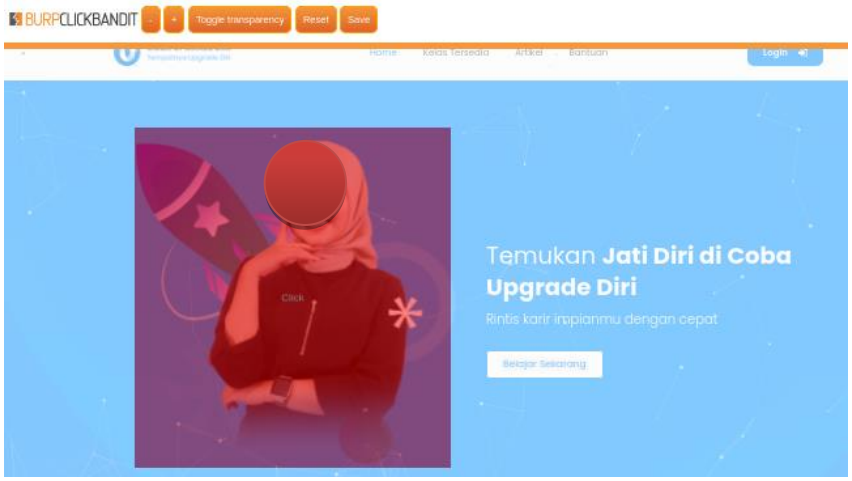


Gambar 8. *Settings* Burp Suite

Setelah berhasil menyelesaikan proses *settings*, kemudian menginputkan *plugin* Burpclickbandit digunakan untuk membuat skrip serangan *clickjacking*. Skrip tersebut diimplementasikan pada situs web target dengan memanfaatkan fitur *developer tools* pada *browser*, khususnya melalui *console*. Kemudian memilih *elements*

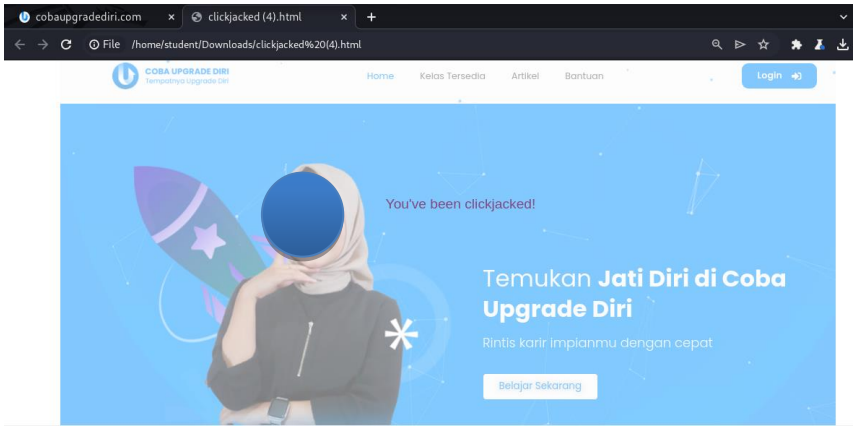
p-ISSN: 2775-4227
e-ISSN: 2775-4219

dapat dilihat pada Gambar 9 akan diletakan *button clickjacking* dari untuk melanjutkan uji coba eksploitasi *clickjacking* pada website.



Gambar 9. *Elements button clickjacking*

Setelah melakukan *settings* pada *elements* Burpclickbandit hasilnya terlihat *alert* "You've been clickjacked!" hasil eksploitasi dapat dilihat pada Gambar 10, artinya website cobaupgradediri.com berhasil dilakukan *clickjacking*, dimana ketika *users* melakukan klik secara tidak sadar pada daerah yang telah di atur elemen *clickjacking.* Hasil pengujian exploitasi mengungkap bahwa kerentanan yang diujikan berupa *Missing Anti-clickjacking Header* pada website cobaupgradediri.com terbukti rentan terhadap serangan *clickjacking* yang sudah di ujikan langsung pada penelitian ini, risiko dari serangan *clickjacking* di mana penyerang dapat memanipulasi tindakan pengguna tanpa disadari oleh mereka hasil *clickjacking*. Maka dari itu pengujian exploitasi pada kerentanan yang dihasilkan dinyatakan terbukti rentan terhadap serangan *clickjacking.*



Gambar 10. Hasil eksploitasi serangan *clickjacking*

Setelah proses pengujian *exploit* dengan Burp Suite didapatkan hasil temuannya yang mengindikasikan bahwa tidak adanya *Header X-Frame-Options* pada konfigurasi website target yang dapat meningkatkan risiko serangan *clickjacking*. Solusi dilakukannya yaitu dengan ditambahkan *Header* pada Apache (di file .htaccess) yang berfungsi untuk memberi instruksi kepada browser terkait izin penayangan suatu halaman di dalam *iframe*. Terdapat 3 langkah opsi konfigurasi yang tersedia:

- *DENY* berfungsi untuk melarang halaman dimuat dalam *iframe*.
- *SAMEORIGIN* bertujuan untuk memungkinkan halaman dimuat dalam *iframe*, tetapi hanya dari domain yang sama.
- *ALLOW-FROM* [URL] untuk mengizinkan halaman dimuat dalam *iframe*, namun terbatas pada domain tertentu (opsi ini tidak kompatibel dengan beberapa browser, seperti Chrome).

Kerentanan ini memungkinkan penyerang mengeksploitasi celah tersebut untuk memanipulasi interaksi pengguna di situs web.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

3.6. *Post-Exploitation*

Pada tahap ini dilakukan penilaian profil risiko terhadap sistem yang memiliki potensi kerentanan setelah pengujian dilakukan pada tahap sebelumnya. Beberapa jenis kerentanan berhasil diidentifikasi pada aplikasi web cobaupgradediri.com, seperti yang ditunjukkan pada Tabel 6 penilaian risiko terhadap celah kerentanan berikut.

Tabel 6. Penilaian Risiko Terhadap Celah Kerentanan

Post-Exploitation		
Nama Aset	**Jenis Kerentanan**	**Profil Risiko**
Web Aplikasi	Missing Anti-clickjacking Header	Medium

Berdasarkan hasil pengujian, ditemukan kerentanan dengan profil risiko tingkat *Medium*. Pada web aplikasi, kerentanan tersebut berupa *Missing Anti-clickjacking Header* dengan *level alert Medium* yang berpotensi membuka peluang terjadinya serangan *clickjacking*.

Kemudian mempertahankan akses dalam tahap *post-exploitation* untuk memastikan kontrol atas sistem yang telah dieksploitasi tetap terjaga. Contohnya dengan dibuat *backdoor*, yang memungkinkan akses ke sistem dapat dipulihkan di masa mendatang, bahkan jika tindakan mitigasi telah diterapkan. Langkah ini memberikan jaminan bagi penguji keamanan atau penyerang untuk tetap memiliki kemampuan mengeksplorasi sistem yang telah ditembus. Tujuan utama dari upaya mempertahankan akses ini adalah untuk memberikan waktu yang cukup bagi eksplorasi lebih lanjut, pengumpulan data, atau implementasi serangan tambahan.

Setelah akses didapat, langkah berikutnya adalah menggunakan kontrol untuk mencapai tujuan tertentu, seperti mengumpulkan data sensitif, menambahkan *tools* untuk eksploitasi lanjutan, atau membuka jalur akses baru. Setelah melewati langkah-langkah ini, pengujian dapat dilakukan secara sistematis dan terorganisir. Ini akan memberikan gambaran lengkap tentang tingkat keamanan sistem yang diuji serta tindakan apa yang perlu dilakukan untuk memperbaiki dan meningkatkan keamanan tersebut.

3.7. *Reporting*

Berdasarkan tahap penelitian yang telah dilakukan, terbukti bahwa website cobaupgradediri.com memiliki celah kerentanan terutama pada *port* yang terbuka dan kerentanan *Missing Anti-clickjacking Header* yang beresiko terjadinya serangan *clickjacking.* Berdasarkan hasil pengujian *penetration testing* dapat disimpulkan bahwa kerentanan ini menggunakan teknik serangan *clickjacking* terbukti berhasil sehingga kerentanannya beresiko terhadap serangan *clickjacking.* Solusinya melakukan perbaikan dan meningkatkan keamanan terdahap website seperti memfilter *port* yang terbuka dan menggunakan *Header X-Frame-Options*.

3.8. Diskusi

3.8.1. Perbandingan dengan Studi Sebelumnya

Penelitian ini menunjukkan bahwa website cobaupgradediri.com memiliki kerentanan berupa *"Missing Anti-clickjacking Header"* dengan tingkat risiko *Medium*, sebagaimana terlihat pada Tabel 6 diatas. Temuan ini sejalan dengan hasil penelitian sebelumnya oleh[7] hasil analisis menunjukkan bahwa ketiadaan konfigurasi *X-Frame-Options* pada server web UTM meningkatkan potensi serangan *Clickjacking*. Kondisi ini memungkinkan penyerang memanfaatkan kerentanan tersebut untuk memanipulasi interaksi pengguna di website. Untuk mengurangi risiko ini, disarankan agar server web UTM segera mengimplementasikan *X-Frame-Options* yang sesuai.

Studi ini mendukung hasil penelitian sebelumnya dengan menunjukkan bahwa penerapan header keamanan, seperti *X-Frame-Options* atau *Content-Security-Policy (CSP)*, adalah langkah krusial untuk mengurangi risiko serangan *clickjacking*. Selain itu, penggunaan alat seperti OWASP-ZAP dan Burp Suite dalam penelitian ini menyediakan bukti eksploitasi praktis yang sejalan dengan temuan dalam literatur terkait.

3.8.2. Implikasi Keamanan Aplikasi Web di Sektor Lain

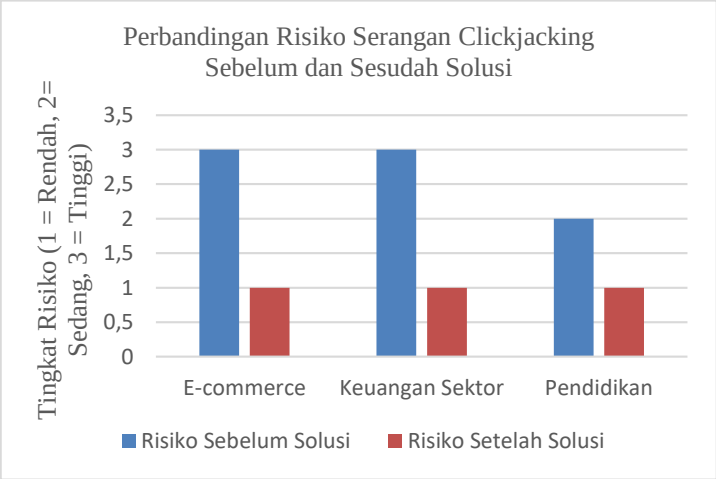
Kerentanan yang teridentifikasi pada website cobaupgradediri.com juga memiliki dampak yang relevan terhadap aplikasi web di berbagai sektor, seperti:

- E-commerce, serangan *clickjacking* berpotensi digunakan untuk mencuri data pelanggan atau menyelesaikan transaksi tanpa sepengetahuan mereka.
- Keuangan, aplikasi perbankan daring rentan terhadap manipulasi klik, yang dapat mengancam keamanan data atau dana pengguna.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

- Pendidikan, platform pembelajaran online bisa dimanfaatkan untuk menipu pengguna agar tanpa sadar memberikan informasi pribadi.

Hal ini menunjukkan pentingnya penerapan langkah mitigasi yang disarankan, seperti implementasi *header* keamanan. Grafik berikut pada Gambar 11, mengilustrasikan perbandingan risiko dan dampak solusi yang diberikan pada masing-masing sektor aplikasi web.



Gambar 11. Perbandingan Risiko dan Dampak Solusi

4. KESIMPULAN

Analisis kerentanan menggunakan metode PTES pada website cobaupgradediri.com mengidentifikasi adanya celah kerentanan *Missing Anti-clickjacking Header* dengan tingkat *medium.* Penelitian ini menunjukkan pentingnya penerapan konfigurasi keamanan seperti *X-Frame-Options* untuk mengurangi risiko *clickjacking*. Pengujian eksploitasi terhadap kerentanan *Missing Anti-clickjacking Header* terbukti bahwa website ini rentan terhadap serangan *clickjacking*. Oleh karena itu, langkah mitigasi yang efektif, seperti pemanfaatan *firewall*, pembatasan akses *port*, penerapan protokol keamanan seperti HTTPS, serta pemeliharaan sistem dengan pembaruan rutin, sangat diperlukan untuk meminimalisir potensi ancaman tersebut. Langkah mitigasi ini tidak hanya mengurangi risiko dari serangan spesifik, tetapi juga meningkatkan ketahanan sistem secara menyeluruh. Oleh karena itu, rekomendasi ini memiliki pengaruh signifikan dalam mengatasi kerentanannya dan memperkuat keamanan sistem dan melindungi data pengguna dari potensi ancaman siber.

Rekomendasi untuk penelitian selanjutnya meliputi perluasan fokus pada eksplorasi kerentanannya lainnya yang mungkin berhubungan dengan masalah serupa, seperti *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF), atau *Remote Code Execution* (RCE). Pengujian dan analisis lebih mendalam mengenai bagaimana kerentanan dapat dimanfaatkan dalam serangan berantai, yang dapat memberikan pemahaman lebih luas tentang profil kerentanannya secara keseluruhan. Selain itu, pengembangan sistem deteksi dini yang mampu secara otomatis mengenali potensi risiko serangan *clickjacking* juga merupakan area penelitian yang relevan. Penelitian ini bisa mencakup penggunaan teknik pembelajaran mesin (*machine learning*) atau analisis heuristik untuk memantau interaksi pengguna dan mendeteksi pola serangan *clickjacking* pada aplikasi web.

DAFTAR PUSTAKA

[1] Y. Muhyidin, M. Hafid Totohendarto, E. Undamayanti, and S. Tinggi Teknologi Wastukancana, "Perbandingan Tingkat Keamanan Website Menggunakan Nmap dan Nikto Dengan Metode Ethical Hacking," *J. Teknol.*, pp. 1–10, 2020.

[2] Y. Natanael, R. Felicia, and E. M. S. Sakti, "Analisis Keamanan Informasi Bagi Pengguna Website Menggunakan Kalilinux Melalui Teknik SQL Injection," *J. Ilm. Tek. Inform. ...*, vol. 25, no. 1, pp. 123–132, 2024, [Online]. Available: https://ojs.upi-yai.ac.id/index.php/TEKINFO/article/download/3903/2967

[3] Mira Orisa and M. Ardita, "Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web," *J. Mnemon.*, vol. 4, no. 1, pp. 16–19, 2021, doi: 10.36040/mnemonic.v4i1.3213.

[4] PuskoMedia Indonesia, "Mengidentifikasi dan Menilai Kerentanan Website: Panduan PraktisNo Title," 2024. https://www.puskomedia.id/blog/mengidentifikasi-dan-menilai-kerentanan-website-panduan-

p-ISSN: 2775-4227
e-ISSN: 2775-4219

praktis/

[5] I. W. Ardiyasa and A. T. Ndok, "Penetration Testing Keamanan Sistem Informasi Berbasis Web dengan Metode OSSTMM," *Semin. Nas. Corisindo*, pp. 348–353, 2023, [Online]. Available: https://stmikpontianak.org/ojs/index.php/corisindo/article/view/197

[6] Widi Linggih Jaelani, Y. Yanto, and F. Khoirunnisa, "Penetration Testing Website Dengan Metode Black Box Testing Untuk Meningkatkan Keamanan Website Pada Instansi (Redacted)," *Naratif J. Nas. Riset, Apl. dan Tek. Inform.*, vol. 5, no. 1, pp. 1–8, 2023, doi: 10.53580/naratif.v5i1.180.

[7] D. Supriadi, E. Suryadi, R. Muslim, L. D. Samsumar, and U. T. Mataram, "Implementasi Vulnerability Assessment Owasp (Open Web Application Security Project) Pada Website," vol. 1, no. 4, pp. 232–240, 2024.

[8] M. Hasibuan and A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box," *sudo J. Tek. Inform.*, vol. 1, no. 4, pp. 171–177, 2022, doi: 10.56211/sudo.v1i4.160.

[9] S. Utoro, B. A. Nugroho, M. Meinawati, and S. R. Widianto, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," *Multinetics*, vol. 6, no. 2, pp. 169–178, 2020, doi: 10.32722/multinetics.v6i2.3432.

[10] B. Kurniawan and I. Ruslianto, "Implementation of Penetration Testing on the Website Using the Penetration Testing Execution Standard (PTES) Method," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 8, no. 2, p. 518, 2023, doi: 10.24114/cess.v8i2.47096.

[11] Muhammad Risky Ardiansyah *et al.*, "Analisis Kerentanan Keamanan Website Menggunakan Metode PTES (Penetration Testing Execution And Standart)," *Nuansa Inform.*, vol. 18, no. 2, pp. 145–153, 2024, doi: 10.25134/ilkom.v18i2.119.

[12] F. Septian, M. H. Arfian, J. S. Asri, and B. Tjahjono, "Pengujian Keamanan Website dengan Metode Penetration Testing (Studi Kasus : Universitas Esa Unggul)," vol. 4, pp. 3629–3647, 2024.

[13] M. D. Purnomo, A. Chusyairi, U. B. Insani, S. Jaya, and K. Bekasi, "Pengujian Keamanan Sistem Mengunakan Metode Penetration Testing di Website Diskominfostandi Kota Bekasi," vol. 1, no. 1, pp. 92–101, 2024.

[14] F. Y. Fauzan and Syukhri, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang dari keamanan web adalah sebanyak 96 dengan disimpulkan Acunetix Threat Level 2 yaitu pada level Medium yang artinya tidak," *J. Vocat. Tek. Elektron. dan Inform.*, vol. 9, no. 2, 2021, [Online]. Available: http://ejournal.unp.ac.id/index.php/voteknika/article/download/111778/105248

[15] R. N. Dasmen, R. Rasmila, T. L. Widodo, K. Kundari, and M. T. Farizky, "Pengujian Penetrasi Pada Website Elearning2.Binadarma.Ac.Id Dengan Metode Ptes (Penetration Testing Execution Standard)," *J. Komput. dan Inform.*, vol. 11, no. 1, pp. 91–95, 2023, doi: 10.35508/jicon.v11i1.9809.

[16] G. Kusuma, "Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik," *J. Teknol. Inf. J. Keilmuan dan Apl. Bid. Tek. Inform.*, vol. 16, no. 2, pp. 178–186, 2022, doi: 10.47111/jti.v16i2.3995.

[17] Rizki M Farhan, "Pengertian Tentang Burp Suite ?," 2024, [Online]. Available: https://www.roombelajar.com/2024/04/pengertian-tentang-burp-suite.html.