Jurnal Pendidikan dan Konseling
Volume 4 Nomor 4 tahun 2022
E-ISSN: 2685-936X dan P-ISSN: 2685-9351
Universitas Pahlawan Tuanku Tambusai

Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode *Vulnerability Assessment*

Alif Muhammad Akmal[1], Nono Heryana[2], Arip Solehudin[3]
[1,2,3] Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang
Email: alifmuhammad18212@student.unsika.ac.id[1], nono@unsika.ac.id[2]
arip.solehudin@unsika.ac.id[3]

Abstrak

Saat ini, teknologi informasi memiliki peranan yang sangat penting di segala bidang dan aspek kehidupan, baik dalam dunia bisnis, ekonomi, dan politik. Hal ini disebabkan karena teknologi sistem informasi yang ada saat ini dapat memenuhi kebutuhan masyarakat secara instan. Sehingga, kita dapat melakukan pengolahan data dan menghasilkan suatu informasi yang dibutuhkan dengan lebih mudah, akurat, efektif dan efesien. Meskipun demikian, tidak sedikit pihak yang memanfaatkan perkembangan teknologi secara tidak bertanggung jawab. Mulai dari kasus peretasan, penipuan, bahkan kasus – kasus Cybercrime yang tidak hanya menyerang individu, namun juga perusahaan/korporasi dan instansi pemerintah. Di Indonesia, kasus kejahatan yang umum terjadi melalui jaringan internet di dunia komputer adalah serangan Virus, Worm, Dorm, Web Deface, hingga masalah pencurian data pribadi, pinjaman online, dan kartu kredit. Berdasarkan latar belakang diatas, penelitian ini bertujuan untuk menganalisis dan melakukan pengujian keamanan website Universitas Singaperbangsa Karawang menggunakan metode Vulnerability assessment dan website vulnerability scanning yang digunakan adalah Owasp ZAP, Nmap, Nikto dan Acunetix.
Kata Kunci: Teknologi Informasi, *Cyber Crime*, Owasp, *Vulnerability assessment*

Abstract

Currently, information technology has a very important role in all fields and aspects of life, both in the world of business, economics, and politics. This is because the current information system technology can meet the needs of the community instantly. Thus, we can perform data processing and produce the required information more easily, accurately, effectively and efficiently. However, not a few parties take advantage of technological developments irresponsibly. Starting from hacking cases, fraud, and even Cybercrime cases that not only attack individuals, but also companies/corporations and government agencies. In Indonesia, common crime cases that occur through the internet network in the computer world are Virus, Worm, Dorm, Web Deface attacks, to the problem of personal data theft, online loans, and credit cards. Based on the above background, this study aims to analyze and test the website security of Singaperbangsa Karawang University using the Vulnerability assessment method and the website vulnerability scanning used is Owasp ZAP, Nmap, Nikto and Acunetix.
Keyword: *Technology Information, Cyber Crime, Owasp, Vulnerability assessment*

PENDAHULUAN

Saat ini, teknologi informasi memiliki peranan yang sangat penting di segala bidang dan aspek kehidupan, baik dalam dunia bisnis, ekonomi, dan politik. Hal ini disebabkan karena teknologi sistem informasi yang ada saat ini dapat memenuhi kebutuhan masyarakat secara instan. Sehingga, kita dapat

melakukan pengolahan data dan menghasilkan suatu informasi yang dibutuhkan dengan lebih mudah, akurat, efektif dan efesien.

Meskipun demikian, tidak sedikit pihak yang memanfaatkan perkembangan teknologi secara tidak bertanggung jawab. Mulai dari kasus peretasan, penipuan, bahkan kasus – kasus *Cybercrime* yang tidak hanya menyerang individu, namun juga perusahaan/korporasi dan instansi pemerintah. Di Indonesia, kasus kejahatan yang umum terjadi melalui jaringan internet di dunia komputer adalah serangan *Virus, Worm, Dorm, Web Deface*, hingga masalah pencurian data pribadi, pinjaman online, dan kartu kredit.

Cybercrime secara umum merupakan suatu aktivitas kejahatan dunia maya dengan memanfaatkan jaringan komputer sebagai alat dan jaringan internet sebagai medianya. *Cybercrime* dalam pengertian luas merupakan semua tindakan ilegal yang dilakukan melalui jaringan komputer dan internet untuk mendapatkan keuntungan dengan merugikan pihak lain, sedangkan *Cybercrime* dalam pengertian sempit semua tindakan ilegal yang ditunjukan untuk menyerang sistem keamanan komputer dan data yang diproses oleh suatu sistem komputer (Ayu Rifka Sitoresmi, 2021).

Kasus *Cybercrime* Pertama kali terjadi di Amerika Serikat pada tahun 1960an, pada tahun 1970 di Amerika Serikat terjadi kasus manipulasi data nilai akademik mahasiswa di Brooklyn New York, kasus penyalahgunaan komputer perusahaan untuk kepentingan karyawan, kasus pengkopian data untuk sarana kejahatan penyelundupan narkotika, kasus penipuan melalui kartu kredit. Selain itu terjadi pula kasus akses tidak sah terhadap database *Security Pacific National Bank* yang mengakibatkan kerugian sebesar $10.2 juta US pada tahun 1978. Selanjutnya kejahatan serupa terjadi pula disejumlah negara antara lain, Jerman, Australia, Inggris, Finlandia, Swedia, Austria, Jepang, Belanda, dan Indonesia. Kejahatan tersebut menyerang terhadap harta kekayaan, kehormatan sistem dalam jaringan komputer (Meinarni, 2019).

Sebuah laporan yang di sponsori oleh *McAfee* memperkirakan bahwa kerusakan tahunan yang disebabkan oleh *cybercrimes* mencapai $445 miliar. Namun, sebuah laporan dari *Microsoft* menunjukan bahwa perkiraan berbasis survei semacam itu “sangat tidak sempurna” dan membesar-besarkan kerugian yang sebenarnya. Sekitar $1,5 miliar hilang pada tahun 2012 untuk penipuan lartu kredit dan debit online di Amerika Serikat. Pada tahun 2016 sebuah studi oleh juniper Research memperkirakan bahwa biaya *Cybercrime* bisa mencapai 2,1 triliun pada tahun 2008 (Gani, 2014).

Keamanan sistem informasi perlu diwaspadai dari ancaman yang bersifat internal dan eksternal yaitu baik dari dalam sistem maupun diluar sistem yang akan berdampak pada ketidakstabilan sistem. Pemicu keamanan sistem informasi yang mengakibatkan terganggunya sistem dan dapat terjadi kerusakan pada informasi berasal dari mekanisme, organisasi, kelompok, dan individu. Upaya dalam keamanan sistem informasi terlebih dahulu perlu mengetahui dan memprediksi ancaman yang akan terjadi sebab tidak ada serangan sebelum adanya ancaman, sehingga ketidakstabilan sistem akibat serangan yang terjadi akan diminimalisirkan dengan upaya yang telah di perkirakan sebelumnya, yaitu dengan memprediksi ancaman sebelum terjadinya serangan.

Perhitungan untuk meminimalisir ancaman tersebut melalui metode-metode pada suatu penilaian resiko (Marakas dan O’Brien (2017, 2018). Menurut G. J. Simons mengemukakan bahwa keamanan informasi adalah usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik (Febrianto, 2020). Menurut John D. Howard dalam bukunya "An Analysis of Security Incidents On The Internet" menyatakan bahwa keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Sedangkan menurut Gollman pada tahun 1999 dalam bukunya "Computer Security" menyatakan bahwa keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan penganggu

yang tidak dikenali dalam sistem komputer. Sedangkan menurut Garfinkel dan Spafford sebagai ahli keamanan komputer menyatakan bahwa komputer dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan (Rahim, 1999).

Universitas Singaperbangsa Karawang adalah perguruan tinggi yang sudah memanfaatkan *website* dalam melakukan proses pengolahan data. Seluruh informasi yang berkaitan dengan kampus telah dimuat pada *website*. Hal ini tentunya akan sangat efektif dalam melakukan proses pengolahan data, karena mahasiswa ataupun dosen akan dimudahkan untuk mengakses dan mendapatkan informasi. Tetapi, banyak resiko yang akan terjadi apabila *website* yang digunakan oleh Universitas Singaperbangsa tidak memiliki keamanan yang baik, banyak ancaman dari pihak yang tidak bertanggung jawab yang bisa memanfaatkan celah keamanan untuk merugikan Universitas Singaperbangsa Karawang.

Vulnerabilty assessment adalah proses mendefiniskan, mengidentifikasi, dan mempriotaskan kerentanan dalam sistem komputer, aplikasi, dan infrastruktur jaringan da memberikan organisasi melakukan penilaiandengan pengetahuan, kesadaran, dan latar belakang risiko yang diperlukan untuk memahami ancaman terhadap lingkungannya dan bereaksi dengan tepat. Proses *vulnerability assessment* yang dimaksudkan untuk mendefinisikan ancaman dan risiko yang ditimbulkannya biasanya melibatkan penggunaan alat penguji otomatis, seperti pemindaian keamanan jaringan, yang hasilnya terdaftar dalam laporan *vulnerability assessmen*t (Alwi & Ilmawan, 2021).

Berdasarkan latar belakang diatas, penelitian ini bertujuan untuk menganalisis dan melakukan pengujian keamanan *website* Universitas Singaperbangsa Karawang menggunakan metode *Vulnerability assessment* dan *website vulnerability scanning* yang digunakan adalah *Owasp ZAP, Nmap, Nikto* dan *Acunetix*. Hasil dari penelitian diharapkan menjadi informasi sekaligus evaluasi bagi Perguruan Tinggi Universitas Singaperbangsa Karawang dalam menjaga dan mengembangkan *website* Universitas Singaperbangsa Karawang.

METODE

Metodologi penelitian yang dilakukan menggunakan metode *Vulenerability Assessment*. Pada proses metode *Vulnerability Assessment* ini terdiri dari 4 tahapan yaitu, *Footprinting, Vulnerability Scanning,, Vulnerability Analysis,* dan *Result*.

HASIL DAN PEMBAHASAN

Proses yang dilakukan untuk menemukan celah keamanan pada website meliputi footprinting, vulnerability scanning, vulnerability analysis, dan result. Pada proses vulnerability analysis menggunakan tools OpenVAS dalam menemukan celah keamanan pada website unsika.ac.id. Sehingga pada proses vulnerability assessment dilakukan dengan berdasarkan kerentanan yang ditemukan pada tahap vulnerability scanning. Hasil dari penelitian ini yaitu result atau hasil yang ditemukan pada saat pengujian vulnerability scanning berdasarkan kerentanan yang dimiliki OpenVAS.

Footprinting

Footprinting adalah kegiatan mengunpulkan informasi sebanyak – banyaknya yang terkait dengan target, seperti perangkat yang digunakan, merek, tipe, nomor versi OS, topologi fisik network, perangkat security network address, subnetting, dan lain – lain. Adapun tools footprinting yang digunakan pada penelitian ini yaitu aplikasi.

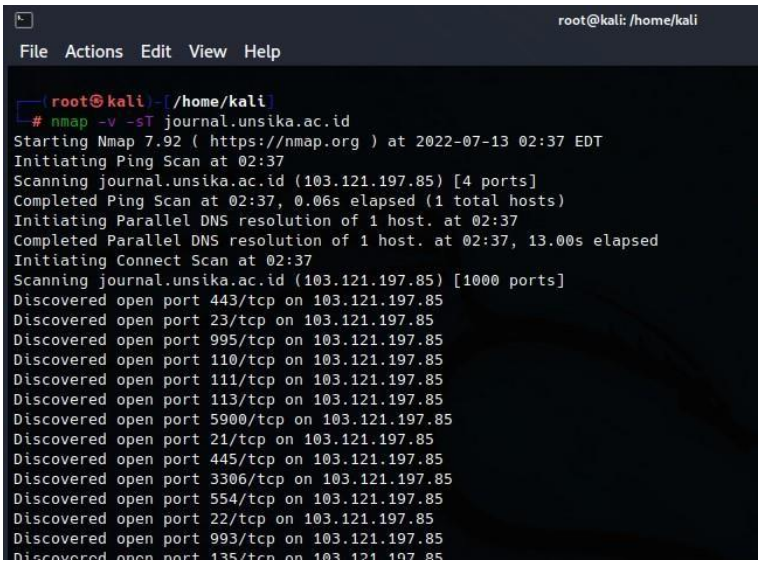
Nikto

Gambar 4. 1 *Pengujian Nikto*

Gambar 4.1. merupakan hasil dari *scanning footprinting* yang dilakukan dengan menggunakan *tools nikto* untuk mencari informasi mengenai *website* perpus.unsika.ac.id yang dijalankan pada sistem Kali Linux. *Tools Nikto* yang dijalankan pada proses *information gathering*, dengan menuliskan perintah *nikto -h perpus.unsika.ac.id -o result.html*. setelah perintah dilakukan, maka akan menghasilkan informasi seperti pada Gambar 4.1. menunjukan bahwa *website* perpus.unsika.ac.id adalah sebuah *website* yang dibangun menggunakan server *Apache*/2.4.25 (Win32) *OpenSSL*/1.0.2j dengan alamat IP 103.121.197.89. Selain itu ditemukan juga *Cookie* SenayanAdmin atau *cookie* telah disetel tanpa tanda *HttpOnly* yang berarti *cookie* dapat diakses oleh *JavaScript*. Jika skrip berbahaya dapat dijalankan di halaman ini, maka *cookie* akan dapat diakses dan dapat dikirim ke situs lain. Jika ini adalah *cookie* sesi, maka pembajakan sesi mungkin bisa terjadi.

Nmap

Dalam melakukan *footprinting*¸ menggunakan *tool NMAP* v.7.9, menggunakan objek *domain* perpus.unsika.ac.id. dengan menuliskan perintah nmap -v -sT perpus.unsika.ac.id.



Gambar 4. 2. *Nmap* perpus.unsika.ac.id

Informasi yang di dapatkan setelah melakukan pemindaian menggunakan nmap yang telah di ringkas adalah sebagai berikut :

1. **IP (*Internet Protocol*) *Address***
   - IP yang digunakan perpus.unsika.ac.id yaitu 103.121.197.89
2. ***Port* yang terbuka dan *Service* yang berjalan**

Adapun ringkasan dari beberapa *ports* yang terbuka pada *website* journal.unsika.ac.id sebagai berikut :

Tabel 4. 1. *Ports* yang terbuka

No	*Ports*	*Protokol*	Status	*Service*	Keterangan
1	25	TCP	*Filtered*	*Simple Mail Transfer Protocol (SMTP)*	*SMTP* adalah suatu protocol untuk berkomunikasi dengan server yang bergunakan untuk mengirimkan email dari lokal email ke server, sebelum akhirnya dikirimkan ke server email penerima.
4	53	TCP	*Open*	*Domain*	Port 53 atau sebutanya adalah *domain name server* (*DNS*). Digunakan untuk mencari mencari nama *domain* atau *Domain Name Server*.
5	80	TCP	*Open*	*HTTP*	Port ini digunakan untuk *Hypertext Transfer Protocol* (*HTTP*). Port ini dibuka agar *website* dapat diakses.
6	443	TCP	*Open*	*HTTPS*	Port ini digunakan untuk *Hypertext Transfer Protocol* dengan tambahan *SSL* (*HTTPS*). Port ini dibuka agar *website* dapat diakses

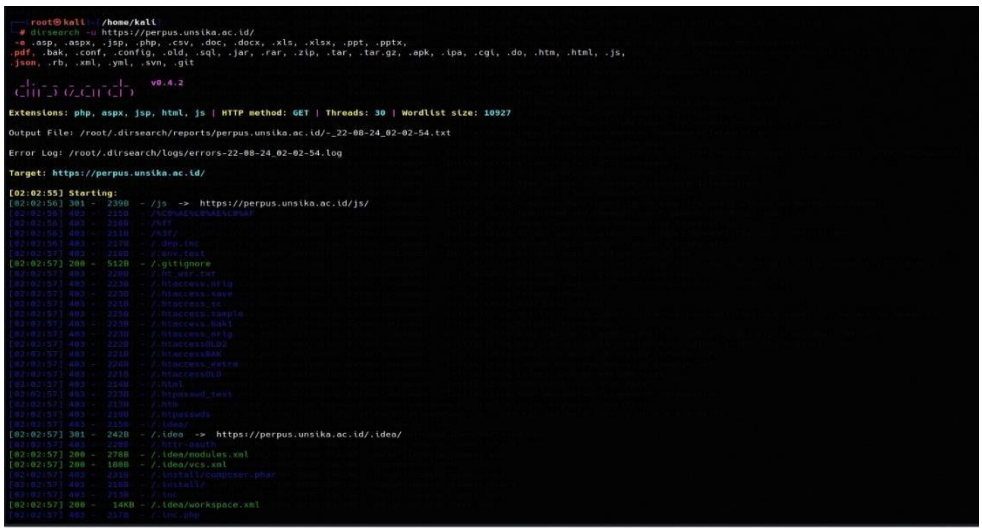
7	1723	TCP	*Open*	*PPTP*	*PPTP* digunakan untuk mengenkripsi mengontentikasi dan menogosiasi setiap data yang melewati atau merangkum data dalam bungkus IP.
8	2000	TCP	*Open*	*Cisco-sccp*	Digunakan untuk berkomunikasi antara perangkat IP dan Cisco CallManager
9	5678	TCP	*Filtered*	*RRAC*	-
10	8291	TCP	*Open*	*Winbox*	Service yang mengijinkan koneksi aplikasi winbox ke router.

Vulnerability Scanning

Vulnerability scanning merupakan proses memperoleh informasi dengan memanfaatkan *tools vulnerability scanning(OwaspZAP* dan *Openvas)* pada domain unsika.ac.id. Pada proses ini bertujuan untuk menemukan kelemahan yang ada dalam sistem. Proses ini menggunakan bantuan *tools vulnerability scanner* yang melakukan pemindaian aplikasi secara otomatis mencari celah keamanan yang mungkin bisa dimanfaatkan untuk pengembangan sistem ataupun kepentingan yang tidak baik. Pada pencarian celah keamanan, menggunakan aplikasi *vulnerability scanner* yaitu *Owasp Zap*. Hasil dari pencarian celah keamanan akan dibahas pada sub bab berikut :

Hasil Pemindaian menggunakan dirsearch

Sistem kontrol yang yang dapat mengakses informasi tanpa adanya proses *autorisasi* dan dapat menyebabkan bocornya informasi sensitif. Pengujian *broken access control* pada *website* journal.unsika.ac.id menggunakan *tools dirsearch*, dengan menuliskan perintah *dirsearch -u perpusl.unsika.ac.id -e <extensions>*.



Gambar 4. 3 Pengujian *Disearch*

Tabel 4. 2 Hasil Pengujian *Dirsearch*

No	URL
1	https://perpus.unsika.ac.id/js/
2	https://perpus.unsika.ac.id/.idea/
3	https://perpus.unsika.ac.id/ADMIN/
4	https://perpus.unsika.ac.id/Admin/
5	https://perpus.unsika.ac.id/INSTALL/
6	https://perpus.unsika.ac.id/Install/
7	https://perpus.unsika.ac.id/UPGRADE/
8	https://perpus.unsika.ac.id/admin/
9	https://perpus.unsika.ac.id/admin./
10	https://perpus.unsika.ac.id/admin/default/
11	https://perpus.unsika.ac.id/api/
12	https://perpus.unsika.ac.id/api/v1/
13	https://perpus.unsika.ac.id/config/
14	https://perpus.unsika.ac.id/files/
15	https://perpus.unsika.ac.id/help/
16	https://perpus.unsika.ac.id/images/
17	https://perpus.unsika.ac.id/install/
18	https://perpus.unsika.ac.id/lib/
19	https://perpus.unsika.ac.id/m/
20	https://perpus.unsika.ac.id/sample/

21	https://perpus.unsika.ac.id/upgrade/

Hasil pemindaian menggunakan OwaspZAP

Pencarian celah keamanan dengan menggunakan tools OpenVAS menghasilkan beberapa temuan celah yang terdapat pada alamat domain unsika.ac.id yang akan dijelaskan pada sub bagian berikut :

Gambar 4. 4 Hasil Pemindaian OwaspZAP

Vulnerability Analysis

Pada tahap ini akan dilakukan analisis celah keamanan yang terjadi pada bagian vulnerability scanning yaitu berupa tabel dibawah ini

Tabel 4. 3 Hasil Pengujian

Vulnerability Scanning	***Alert***	***Risk Assessment***
OwaspZAP	*Cross Site Scripting*	*High*
	SQL Injection	*High*
	Absence of antiCSRF tokens	*Medium*
	Content Security y(CSP) Header Not Set	*Medium*
	ulnerable JS Library	*Medium*
	e No HttpOnly Flag	*Low*
	Cookie Without Samesite Attribute	*Low*
	Cross-Domain lavaScript Source File Inclusion	*Low*
	Timestamp Disclosure - Unix	*Low*

	X-content-Type - ption Header Missing	*Low*
	Content- Type Header Misiing	*Informational*
	Information Disclosure – Suspicious Comments	*Informational*

Result

Tahap terakhir dalam melakukan vulnerability assessment adalah *result*.. Berdasarkan hasil pengujian pada tahap *vulnerability scanning website* perpus.unsika.ac.id memiliki 12 kerentanan yang telah diuji. Terdapat 2 risiko *High*, 3 *Medium*, 5 *low* dan 2 *Informational*. Berikut hasil pengujian yang akan disajikan pada tabel berikut

Tabel 4. 4 Hasil Analisis

Vulnerability Scanning	***Alert***	***Risk Assessment***	**Keterangan**
OwaspZAP	*Cross Site Scripting*	*High*	serangan injeksi kode pada sisi klien dengan menggunakan sarana halaman website atau web aplikasi ,dampaknya yaitu Serangan ini mengeksploitasi kerentanan XSS untuk mencuri data, mengendalikan sesi pengguna, menjalankan kode jahat, atau digunakan sebagai bagian dari serangan phishing.
	SQL Injection	*High*	Penyerang menggunakan kelemahan ini untuk menjalankan *query* khusus dalam *database*, yang membuatnya mampu mengambil-alih *database*.dampak nya itu *Database* bisa terekspos, bisa menampilkan informasi yang tidak semestinya, dan penyerang bisa memanipulasi *database* tersebut.

	Absence of anti-CSRF tokens	*Medium*	Celah ini dapat menyebabkan serangan *Cross-Site Request Forgery,* dampaknya yaitu Tidak adanya token Anti-CSRF dapat menyebabkan serangan *Cross-Site Request Forgery Attack* yang dapat mengakibatkan eksekusi Tindakan aplikasi tertentu sebagai pengguna lain yang masuk, misalnya mencuri akun dan mengubah informasi pribadi dari pemilik akun.
	Content Security Policy(CSP)	*Medium*	*Content Security Policy* atau CSP adalah pengaturan tambahan yang diteraplan melalui respon *HTTP Headers,* dampaknya yaitu *Cross Site Scripting*
	Header Not Set		*(XSS)* maupun serangan dengan kode injection lainnya.
	Vulnerable JS Library	*Medium*	Aplikasi menggunakan library JQuery rentan terhadap serangan XSS
	Coockie No HttpOnly Flag	*Low*	Celah ini mengindikasikan bahwa *cookies* rentan akan diakses dan dikirim ke lain. Dampak nya yaitu *Session Hijacking*
	Cookie Without Samesite Attribute	*Low*	*Atribut "SameSite"* memungkinkan untuk mendeklarasikan apakah *cookie* harus dibatasi pada konteks pihak pertama atau situs yang sama.dampaknya adalah *Cookie without SameSite Attribut* dapat menyebabkan serangan *Cross-Site Request Forgery (CSRF)*.
	Cross-Domain JavaScript Source File Inclusion	*Low*	Halaman berisi satu atau beberapa file skrip dari domain pihak ketiga.dampaknya yaitu Jika pihak ketiga secara sengaja atau tidak sengaja menyimpan konten berbahaya, konten tersebut dapat ditambahkan dan dieksekusi pada aplikasi web korban. Pastikan file sumber *Javascript* dimuat hanya dari sumber terpercaya.

Timestamp Disclosure - Unix	*Low*	Kerentanan yang disebabkan oleh tampilnya informasi *timestamp unix* pada browser. Dampaknya yaitu Kerentanan ini dapat dimanfaatkan sebagai sarana pengumpulan informasi
X-content-Type Option Header Missing	*Low*	Celah ini merupakan celah dimana *"Anti MIME-Sniffing header X-Content-TypeOptions"* tidak di *set "nosniff"*. Namun browser baru cenderung sudah tidak dapat mengakses celah ini. Dampaknya yaitu Rentan untuk *MIME-Type sniffing*.
Content-Type Header Misiing	*Informational*	Anti MIME sniffing x-content tidak 'nonsniff' sehingga browser versi lama dapat melakukan MIME-sniffing pada response body
Information Disclosure-Suspicious Comment	*Informational*	Kerentanan yang disebabkan oleh *comment out* pada *coding* yang di anggap mencurigakan atau mengandung data sensitif. Dampaknya yaitu Kerentanan ini dapat dimanfaatkan sebagai sarana pengumpulan informasi

SIMPULAN

Pengujian yang dilakukan untuk mencari celah keamanan *website dengan* melakukan proses *scanning vulnerability analysis* menggunakan *tools OWASP-ZAP*. Ditemukan 2 kerentanan dengan tingkat risiko *high*, 3 kerentanan dengan tingkat risiko *medium*, 5 kerentanan dengan tingkat risiko *low*, dan 2 kerentanan dengan tingkat risiko *informational*. Dan berdasarkan hasil dari proses *vulnerability analysis*, dilakukan proses pengujian celah keamanan antara lain, *Cross Site Scripting*, *SQL Injection*, *Absence of anti-CSRF tokens, Content Security Policy(CSP) Header Not Set, Vulnerable JS Library, Coockie No HttpOnly Flag, Cookie Without Samesite Attribute, Cross-Domain JavaScript Source File Inclusion, Timestamp Disclosure – Unix, X-content-Type -Option Header Missing, Content- Type Header Misiing, Information Disclosure – Suspicious Comments*.

DAFTAR PUSTAKA

N., Ibrahim, A., & Ambarita, A. (2018). Sistem Informasi Pengaduan Pelanggan Air Berbasis Website Pada Pdam Kota Ternate. *IJIS - Indonesian Journal On Information System*, *3*(1). https://doi.org/10.36549/ijis.v3i1.37

Adani, M. R. (2020). *Apa Itu Internet dan Apa Saja Dampaknya Bagi Kehidupan Sehari-hari?* Sekawanmedia.Co.Id.

Alwi, E. I., & Ilmawan, L. B. (2021). Analisis Keamanan Sistem Informasi

Aka. Hot.Liputan6.Com. demik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment. *INFORMAL: Informatics Journal*, *6*(3), 131.

https://doi.org/10.19184/isj.v6i3.27053
Ayu Rifka Sitoresmi. (2021). *Cyber Crime adalah Kejahatan Dunia Maya, Pahami Jenis-jenis dan Kerugiannya*
Dewi Laksmiati. (2020). Vulnerability Assessment Pada Situs www.hatsehat.com Menggunakan Openvas. *Jurnal Akrab Juara*, *5*(3), 240–246.
Febrianto, *KEPUTUSAN PEMBELIAN ONLINE DI LAZADA. CO. ID DAN BLIBLI. COM SURVEI PADA MAHASISWA STIE MALANGKUÇEÇWARA*. STIE MALANGKUCECWARA.