CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 7, No. 1, Mei 2024,, hlm. 25-33

Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing

Ade Gustiyono[1], Erick Irawadi Alwi[2], Syahrul Mubarak Abdullah[3]

[1,2,3]Teknik Informatika, Fakultas Ilmu Komputer, UniversitasMuslim Indonesia
Email:[1]13020200217@umi.ac.id, [2]erick.alwi@umi.ac.id, [3]syahrul.mubarak@umi.ac.id

Abstrak

Serangan *cross-site scripting (XSS)* merupakan salah satu jenis serangan *web* yang berbahaya. Serangan ini dapat digunakan untuk mencuri data pengguna, melakukan *phising*, atau menjalankan *skrip* berbahaya di browser pengguna. Penelitian ini bertujuan untuk: Menganalisis dan mengidentifikasi kerentanan *XSS* pada situs website dengan menggunakan metode *Penetration Testing* serta memberikan rekomendasi kepada pihak PT. Tricon Metalindo Perkasa dari hasil *pentest* yang telah dilakukan. Metode yang digunakan adalah metode *penetrasi testing* dengan menggunakan *tools OWASP Zap* dan *Hackbar*. Hasil penelitian menemukan alert dianataranya *Vulnerable JS Library, X-Frame-Options Header Not Set, Absence Of Anti-CSRF Tokens, Cross-Domain JavaScript Source File Inclusion, Incomplete or No Cache-Control and Pragma HTTP Header Set dan X-Content-Type-Options-Header Missing* dengan *Risk* tingkat menengah (*medium*) sebanyak 2 temuan, tingkat rendah (*low*) sebanyak 4 dan *condifence* tingkat menengah (*medium*) sebanyak 6 dan menunjukkan bahwa terdapat kerentanan *XSS* pada website PT. Tricon Metalindo Perkaasa, kerentanan tersebut berupa *Reflected XSS* yang terletak pada kolom input pencarian dengan tingkat *risk medium*, kerentanan ini dapat di *exsploitation* oleh penyerang untuk menampilkan *pop-up*, melakukan *phising*, atau mencuri data pengguna.

Kata kunci: *cross-site scripting (XSS), reflected XSS, OWASP Zap, Penetration Testing*

Analyze Website Vulnerability To Cross-Site Scripting (XSS) Attacks Using Penetration Testing

Abstract

Cross-site scripting (XSS) attacks are a malicious form of web attacks. These attacks can be used to steal user data, perform phishing, or run malicious scripts in the user's browser. This study aims to: Analyze and identify XSS vulnerability on websites using Penetration Testing method and provide recommendations to PT. Tricon Metalindo Mighty from the results of the pentest that has been carried out. The method used is penetration testing using OWASP Zap and Hackbar tools. The research findings revealed several alerts, including Vulnerable JS Library, X-Frame-Options Header Not Set, Absence of Anti-CSRF Tokens, Cross-Domain JavaScript Source File Inclusion, Incomplete or No Cache-Control and Pragma HTTP Header Set, and Missing X-Content-Type-Options-Header. There were 2 findings categorized as medium risk, 4 findings as low risk, and 6 findings with medium confidence level. These findings indicate the presence of XSS vulnerabilities on the PT. Tricon Metalindo Perkasa website, specifically in the form of reflected XSS located in the search input column with a medium-risk level. This vulnerability can be exploited by attackers to display pop-ups, carry out phishing attempts, or steal user data.

***Keywords**: cross-site scripting (XSS), reflected XSS, OWASP Zap, Penetration*

1. PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat saat ini, membuat teknologi berperan sangat penting dalam kehidupan sehari-hari, dengan adanya jaringan komputer kita dapat dengan mudah mengakses suatu informasi dan data. Di era saat ini hampir seluruh manusia mengandalkan jaringan komputer untuk menyimpan data dan informasi (Ilham, Alwi dan Fattah, 2023). *Website* merupakan salah satu situs yang ada di internet yang dapat menyimpan dan menyebarkan segala informasi. Teknologi informasi menjadi kebutuhan mutlak, bagi seluruh lapisan masyrakat terlebih pemerintah untuk mendukung memperoleh informasi yang cepat, mudah, akuntabel, serta layanan yang perima. Jaringan komputer yang digunakan dalam pertukaran informasi pada ranah ruang publik (Rodianto, Idham, Yuliadi Zaen dan Ramadhan, 2022). Internet bagian dari kemajuan teknologi informasi menjadi media informasi yang pertumbuhannya sangat cepat tanpa terkendala ruang dan waktu. Salah satu bagian dari internet yang pertumbuhannya sangat cepat adalah *WWW* adalah teknologi yang perkembangan cepat sebagai mediakomunikasi berisi informasi berupa suara, gambar, animasi, text, dan programperangkat lunak yang menyusunnya menjadi dokumen yang dinamis (Situmorang, 2012).

Berdasarkan fungsinya website sebagai media yang menyampaikan informasi, membutuhkan sebuah keamanan agar informasi utuh diterima oleh penerima informasi. Bila pemilik *website* mengabaikan keamanan tersebut, maka seorang *cracker* mampu membuat suatu program bagi kepentingan dirinya sendiri dan bersifat merusak informasi tersebut. Beberapa contoh kasus yang dilakukan oleh cracker meliputi Virus, Pencurian Kartu Kredit, Pembobolan Rekening Bank, Pencurian Password *E-mail/Web Server*. *Cracker* mengambil data-data penting pada suatu website dan bahkan pula mengacak-acak tampilan web tersebut di website disebuah organisasi, instansi, dan sekolah (Sehaffudin, Indrihastuti dan Gunawan, 2017). Banyaknya data dan informasi yang tersebar di internet juga diiringi dengan tingginya serangan keamanan. *Website* yang memiliki sistem keamanan yang lemah akan rentan oleh serangan-serangan ancaman yang dapat terjadi sewaktu-waktu. Sering terjadi permasalahan keamanan sistem yang kadang terabaikan dan bahkan malah terletak diurutan kedua atau urutan terakhir dalam daftar yang dianggap penting (Sehaffudin, Indrihastuti dan Gunawan, 2017). Salah satu masalah pada aplikasi berbasis web adalah serangan *cross site scripting (XSS)* dan Menurut laporan digital *OWASP Top* 10 adalah dokumen yang tersedia di situs web mereka. Laporan ini mencakup 10 resiko keamanan aplikasi web teratas yang diberi peringkat secara sistematis, dengan mempertimbangkan aspek-aspek tertentu seperti ukuran dampak, tingkat kerentanan, dan frekuensi kelemahan yang ditemukan seperti pada Gambar 1.

Gambar 1. OWASP TOP 10 Vulnerability

PT. Tricon Metalindo Perkasa salah satu perusahaan di jakarta yang memanfaatkan kemajuan teknologi dalam menyediakan supply berbagai barang dan material dengan menggunakan website. Situs *website* PT. Tricon Metalindo Perkasa yang menerima input dari pengguna berpotensi rentan terhadap serangan *Cross-Site Scripting (XSS)*. Apabila website PT. Tricon Metalindo Perkasa rentan terhadap serangan *Cross Site Scripting* dapat berdampak buruk pada *commerce*, hubungan antara klien dan nama baik perusahaan.

Maka dari permasalahan tersebut penulis menawarkan solusi yaitu dengan menganalisa keamanan website terhadap serangan *Cross-Site Scripting (XSS)* menggunakan metode Penetration Testing. Dalam analisa tersebut akan diperoleh kerentanan *XSS* yang memungkinkan penyerang dapat menyisipkan kode *JavaScript* ke dalam *website* PT. Tricon Metalindo Perkasa. Kemudian peneliti akan memberikan laporan hasil *pentes* dari website PT. Tricon Metalindo Perkasa yang dapat dipahami.

Dengan dilakukan analisis kerentanan keamanan website PT. Tricon Metalindo Perkasa, diharapkan hasil dari pengujian penetrasi ini dapat menjadi acuan bagi perusahaan dalam meningkatkan langkah-langkah keamanan pada website mereka. Kajian ini juga diharapkan memberikan pemahaman yang lebih mendalam mengenai risiko serangan XSS serta rekomendasi yang spesifik dan implementatif untuk mengurangi potensi risiko tersebut di masa mendatang.

2. TINJAUAN PUSTAKA

2.1. Keamanan *Website*

Keamanan suatu website merupakan salah satu prioritas yang sangat utama bagi seorang pengololah atau pengguna situs. Kebanyakan pengguna hanya mengutamakan design tampilan dan konten supaya menarik pengunjung sebanyak banyaknya. Jika seorang pengolah atau pengguna mengabaikan keamanan suatu website maka yang dirugikan adalah pengguna itu sendiri karena seseorang dapat mengambil data-data penting pada suatu website dan bahkan pula dapat dapat mengacak-acak tampilan website tersebut. Paling utama keamanan sebuah situs adalah melindungi komputer, aplikasi dan jaringannya dengan tujuan mengamankan informasi yang berada didalamnya (Mulyanto, Haryanti dan Jumirah, 2021).

2.2. Cross-Site Scripting (XSS)

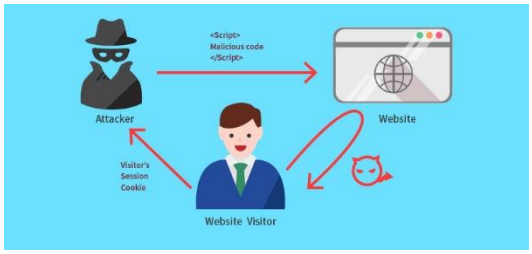
Cross site scripting (XSS) adalah jenis kerentanan yang dapat membahayakan aplikasi web dengan memasukkan kode berbahaya, yang disingkat XSS untuk membedakan *cascading style sheets (CSS)*. Kerentanan *XSS* adalah kerentanan yang sangat umum dan lazim terjadi dalam kerentanan *web*. Dengan memanfaatkan adanya kerentanan *XSS* dapat menyebabkan timbulnya banyak masalah yang serius. Penyerang membuat sejumlah situs besar *URL* yang berisi kode berbahaya dan memikat pengguna untuk mengklik situs *URL* tersebut. Ketika korban mengklik *URL* ini, penyerang bisa mendapatkan *cookie* dari pengguna dan menggunakan cookie ini untuk login ke akun korban (Liu, Zhan, Chen dan Zhang, 2019). Ada beberapa serangan XSS yang antara lain :

1. *Reflected XSS* adalah serangan di mana pengguna mengirimkan input ke aplikasi yang kemudian dipantulkan kembali ke pengguna yang sama. Serangan ini memanfaatkan permintaan yang

tidak cukup disaring oleh sistem, sehingga skrip berbahaya dapat dieksekusi saat mengirimkan permintaan ke situs web rentan (Suroto dan Asman, 2021).

2. *Stored XSS* adalah serangan di mana kode berbahaya disuntikkan secara permanen ke server target, misalnya, dalam database. Serangan terjadi ketika korban meminta informasi yang disimpan dari server dan menerima skrip berbahaya dari server, misalnya melalui pesan atau kolom komentar(Hussain, Hasan, Taimoor, Chughtai, Taimoor dan Chughtai, 2017).
3. *DOM-based XSS* (XSS Berbasis DOM) adalah serangan di mana payload serangan mengubah "lingkungan" *DOM* di browser korban, yang digunakan oleh skrip sisi klien asli. Akibatnya, kode sisi klien berjalan secara tak terduga tanpa mengubah halaman itu sendiri, karena modifikasi berbahaya telah terjadi di lingkungan *DOM* (Suroto dan Asman, 2021).

Serangan *cross-site scripting (XSS)* berbeda dari serangan lapisan aplikasi karena mereka menyerang pengguna aplikasi, bukan server atau aplikasi. Dengan membuat permintaan, web server mengumpulkan data dari web client, yang termasuk protokol seperti *POST*, *GET*, dan *COOKIES* (Liu, Zhan, Chen dan Zhang, 2019). Sehingga malicious user dapat menyerang dengan menyuntikkan kode (biasanya script sisi klien seperti JavaScript) ke dalam output aplikasi Web, contohnya dapat dilihat pada Gambar 2.



Gambar 2. Pola Serangan Cross Site Scripting.

2.3. Open Web Application Security Project

Open Web Application Security Project (OWASP) adalah komunitas terbuka yang didedikasikan untuk memungkinkan organisasi mengembangkan, membeli, dan memelihara aplikasi yang dapat dipercaya. *OWASP* adalah jenis organisasi baru. Kebebasan kami dari tekanan komersial memungkinkan kami memberikan informasi terkait keamanan aplikasi yang tidak bias, praktis, efektifbiaya. *OWASP* tidak terafiliasi dengan perusahaan teknologi manapun, meskipun kami mendukung penggunaan teknologi keamanan komersial. Serupa dengan banyak proyek *software* open source, *OWASP* menghasilkan beragam jenis materi dengan cara kolaborasi dan terbuka (OWASP, 2010).

2.4. Penetration Testing

Penetration testing adalah cara untuk mengevaluasi sistem untuk kerentanan, konfigurasi yang buruk, dan kelemahan perangkat keras dan perangkat lunak serta masalah teknis sistem informasi yang sedang diuji (Hussain, Hasan, Taimoor, Chughtai, Taimoor dan Chughtai, 2017).. Tujuan utama penetration testing adalah untuk menemukan dan mengatasi kerentanan dalam infrastruktur jaringan, sehingga dapat menunjukkan betapa rentannya jaringan tersebut (Stiawan, Idris, Abdullah, Aljaber dan Budiarto, 2017).. Pengujian penetrasi langsung telah terbukti dapat meningkatkan keamanan situs web. Selain itu, pengujian penetrasi juga dapat digunakan untuk menilai kebijakan keamanan suatu organisasi, tingkat kesadaran karyawan tentang persyaratan keamanan, dan kemampuan organisasi untuk menemukan dan menangani masalah keamananRiadi Sunardi dan Handoyo, 2019) .Tahapan penetration testing dapat dilihat pada gambar 3.

Gambar 1. Tahapan *Penetration Testing*

2.5. Kali Linux

Kali Linux merupakan sistem operasi yang bersifat terbuka atau open source, artinya siapa pun bisa mengembangkan sistem operasi ini. Sistem operasi ini diciptakan oleh hacker Linus Benedict Torvolds, yang mana beliau ini adalah seorang *hacker*. Kali Linux merupakan salah satu jenis Linux. Kali Linux banyak digunakan untuk pengujian penetrasi baik pada *website* maupun jaringan computer (Andria, 2020).

2.6. *Scanning Tools*

Scanning merupakan fase dimana mengumpulkan seluruh informasi spesifik yang berkaitan dengan jaringan korban. Scanning juga dapat diartikan sebagai suatu bentuk pendeteksian terhadap sistem yang masih hidup dan dapat diakses melalui internet atau layanan yang disediakan. Tahap ini merupakan resiko tinggi. Jika penyerang dapat menemukan kerentanan pada sistem anda, mereka dapat meng *exsploitation* jaringan anda (Fathur, 2020).

2.6. OWASP Zap tools

OWASP Zap adalah tools vulnerability scanner yang dibuat oleh organisasi *OWASP tools* in adalah proyek dari *OWASP* yang paling aktif karena terus dikembangkan dan tools ini bersifat opensource sehingga siapapun dapat mengembangkan tools ini (*The Open Web Application Security Project*, 2013). Fitur yang ada dalam *OWASPZap* antara lain Intercepting Proxy,Active and Passive Scanners,

spider scan, report Generation, Brute Force(using *OWASP* dirbuster code), Fuzzing(using fuzzdb & *OWASP* JBrosfuzz), Extensibility,Auto tagging,Port scanner, Parameter analysis, Smart card support, Session comparison, invoke external apps, Api +headless mode, Dynamis SSL Certificates, Anti CSRF token handling.

2.8 *Uniform Resource Locator*

URL atau Uniform Resource Locator adalah sebuah alamat situs web (website). URL terdiri dari beberapa bagian, termasuk nama domain untuk memberitahu browser web bagaimana dan di mana mengambil informasi yang diperlukan. Selanjutnya, URL berfungsi sebagai alamat menuju situs web yang Anda inginkan. Anda perlu untuk memasukkan alamat tersebut di dalam adres bar untuk menuju halaman yang ingin Anda lihat (Drs. Taufiqqurrachman, M.Si, 2022).

2.7. JavaScript

JavaScript adalah bahasa pemrograman yang berjalan di sisi klien, di mana komputer pengguna memproses kode secara mandiri. Bahasa ini sering digunakan untuk menambahkan animasi dan elemen interaktif lainnya pada halaman web. Banyaknya library JavaScript yang tersedia memungkinkan pengembang membuat halaman web lebih interaktif. Untuk menjalankan JavaScript, diperlukan browser yang mendukung bahasa ini. (Sinlae *et al.*, 2024, p. 2).

2.8. Hacker

Hacker adalah seseorang yang memiliki keahlian dalam pemrograman dan mampu melakukan peretasan terhadap sistem keamanan komputer atau jaringan untuk mencapai tujuan tertentu. Biasanya, seorang hacker memiliki pengetahuan mendalam tentang komputer, pemrograman, jaringan, serta perangkat keras.(Indah Sari, 2014, p. 5)

3. METODOLOGI

Dalam melakukan penelitian ini metode yang digunakan adalah *Penetrasi testing* yang merupakan metode penelitian yang bertujuan untuk menemukan dan mengeksploitasi kerentanan keamanan dalam suatu sistem atau jaringan komputer. Metode ini dilakukan dengan mensimulasikan serangan yang dilakukan oleh *hacker* atau *cracker*, sehingga dapat diketahui kelemahan-kelemahan yang ada dalam sistem website PT. Tricon Metalindo Perkasa.
Adapun penjelasan tahap-tahap *penetrasion testing*:

1. *Information Gathering*

Tahap awal dalam melakukan identifikasi target yaitu dengan cara mengumpulkan segala bentuk informasi mengenai *website* berdomain *https://tricon-metalindo.com/* yang akan menggunakan bantuan tools *OWASP Zap* untuk mengumpulkan informasi tentang target, termasuk *URL*, fitur yang tersedia, dan jenis input yang diterima. *fitur active scanning* dan *spider* pada *OWASP Zap* memfasilitasi pengumpulan informasi tentang target.

2. *Vulnerability Analysis*

Tahap selanjutnya setelah melakukan tahap *Information Gathering*, Selanjutnya melakukan analisis celah serangan *XSS* terhadap hasil scanning yang telah dilakukan pada tahap information gathering untuk mengidentifikasi kerentanan *XSS* yang ada pada target. Dengan mengidentifikasi kerentanan *XSS* kita dapat menentukan metode serangan *XSS* yang paling efektif.

3. *Exsploitation*

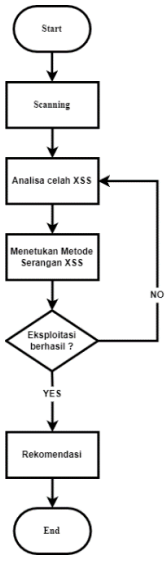
Tahap selanjutnya setelah menentukan metode serangan *XSS* yang paling efektif, kita dapat melanjutkan ke tahap *exsploitation*. Tahap ini bertujuan untuk melakukan *exsploitation* kerentanan *XSS* untuk membuktikan kerentanan dapat dimanfaatkan seorang *cracker*, dengan metode *exsploitation XSS* menggunakan bantuan *tools HACKBAR*.

4. *Report*

Proses deskripsi dan interpretasi hasil pengujian yang dilakukan dengan *framework OWASP* TOP 10 melibatkan penentuan solusi yang sesuai dengan metode pengujian tersebut.

5. Kesimpulan

Proses ini bagian penting dalam penetrasion testing, dimana hasil pengujian dianalisis dan disimpulkan untuk menghasilkan laporan yang komprehensif. Laporan ini memungkinkan organisasi untuk memahami dan mengatasi kelemahan keamanan mereka. Laporan dan presentasi yang dihasilkan dari tahap ini akan menjadi dokumen penting bagi organisasi untuk meningkatkan postur keamanan mereka.



Gambar 3. Alur Penelitian

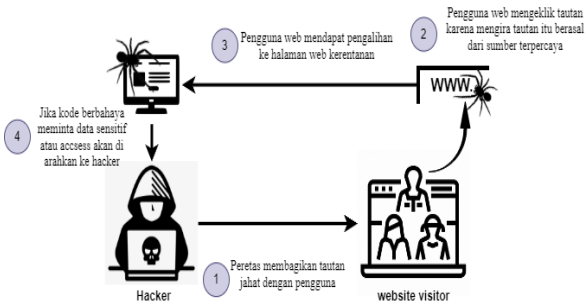
Gambar 3 merupakan alur penelitian yang diigunakan penulis dalam melakukan penelitian ini. Alur penelitian merupakan suatu alur diagram yang menjelaskan proses berjalannya sebuah penelian.

Pada tahap pengujian sistem pada suatu *website* ada beberapa tahapan mulai dari *Scanning* hingga melakukan memberikan rekomendasi.

4. PEMBAHASAN

4.1. Skenario

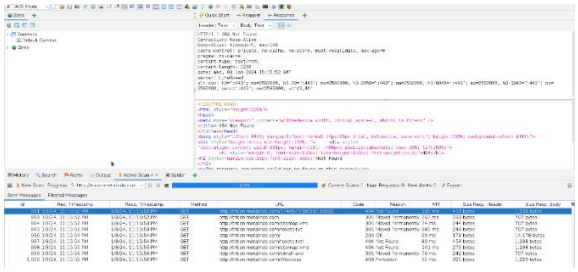
Skenario *Cross-Site Scripting (XSS)*, penyerang berinteraksi dengan korban dengan mengirimkan *URL* mereka. Setelah korban mengeksekusi *URL*, maka halaman web korban akan *exsploitation*. Dapat dilihat pada gambar 4, merupakan skenario serangan *Cross-Site Scripting (XSS)*.



Gambar 4. Skenario *Cross-Site Scripting (XSS)*

4.2 *Information Gathering*

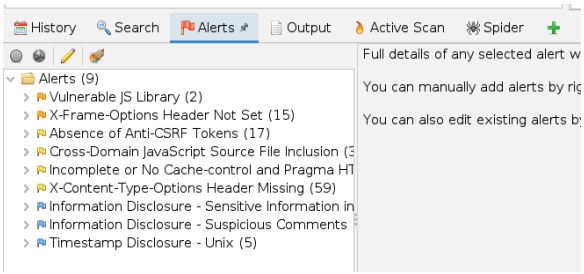
Pada tahapan ini dilakukan sebuah pengumpulan segala bentuk infomasi *web* seperti informasi umum, *website* yang ditargetkan mempunyai nama PT Tricon Metalindo Perkasa dengan domain *https://tricon-metalindo.com/* dan alamat Jl Pluit Selatan Raya No 1 Penjaringan, Jakarta Utara 1444. Kemudian infomasi teknologi yang digunakan oleh target, *website* dibuat dengan php, nama serve LiteSpeed, dan *website* ip 131.153.77.183



Gambar 5. Proses *Scanning Tools OWASP Zap*

Gambar 5 memperlihatkan proses *scanning* dengan menggunakan *OWASP Zap* untuk membantu mengidentifikasi jenis kerentanan dan jenis risiko (tinggi, sedang atau rendah).

Aplikasi ini juga memberikan informasi tentang tingkat kepercayaan keberadaan kerentanan, dari proses *scanning* yang telah dilakukan menggunakan *tools* otomatis *OWASP Zap*, memberikan informasi yang berisi tentang alert kerentanan pada *website* terdiri dari kerentanan kerentanan hasil scanning dapat dilihat pada 6



Gambar 6. Hasil *Scanning dari* Tools *OWASP Zap*

4.3. *Vulnerability Analysis*

Tahap selanjutnya akan dilakukan analisis celah serangan *XSS* terhadap hasil *scanning* yang telah dilakukan pada tahap information gathering. Analisis ini bertujuan untuk mengidentifikasi kerentanan *XSS* yang ada pada target. Berdasarkan hasil scanning *OWASP ZAP* maka ditemukan beberapa alert dianataranya *Vulnerable JS Library*, *X-Frame-Options Header Not Set*, *Absence Of Anti-CSRF Tokens*, *Cross-Domain JavaScript Source File Inclusion*, *Incomplete or No Cache-Control and Pragma HTTP Header Set dan X-Content-Type-Options-Header Missing* dengan tingkat keparahan pada celah serangan dapat dilihat pada tabel 4.

Tabel 1. Kerentanan *Website* PT. Tricon Metalindo

Kerentanan *Website* PT. Tricon Metalindo

Jenis	URL	Risk	Condifence
Vulnerable JS Librar	https://tricon-metalindo.com/js/jquery.js	Medium	Medium
X-Frame-Options Header Not Set	https://tricon-metalindo.com	Medium	Medium
Absence Of Anti-CSRF Tokens	https://tricon-metalindo.com	Low	Medium
Cross-Domain JavaScript Source File Inclusion	https://tricon-metalindo.com	Low	Medium
Incomplete or No Cache-Control and Pragma HTTP Header Set	https://tricon-metalindo.com	Low	Medium
X-Content-Type-Options-Header Missing	https://tricon-metalindo.com	Low	Medium

Pada tahap ini dilakukan analisa berdasarkan informasi dari *OWASP ZAP*, berikut ini merupakan penjelasan dari seluruh kerentanan yang ada pada *website* PT. Tricon Metalindo Perkasa:

1. *Vulnerable JS Library* Peretas dapat menyisipkan kode *JavaScript* berbahaya ke dalam aplikasi web yang menggunakan pustaka JS yang rentan. Kode ini kemudian dapat dieksekusi di *browser* pengguna, memungkinkan *peretas* untuk mencuri data, mengendalikan *browser*, atau melakukan tindakan lain yang tidak diinginkan.
2. *X-Frame-Options Header Not Set* memungkinkan pengembang *web* untuk mengontrol apakah halaman *web* mereka dapat

ditampilkan dalam frame atau iframe. Jika header ini tidak diatur, peretas dapat menjebak halaman *web* Anda dalam frame dan menampilkannya bersama dengan konten berbahaya. Hal ini dapat memungkinkan peretas untuk melakukan serangan *ClickJacking*, di mana pengguna ditipu untuk mengklik tombol atau tautan yang berbahaya.

3. *Absence of Anti-CSRF Tokens*, token acak yang digunakan untuk melindungi pengguna dari serangan *CSRF*. Serangan *CSRF* terjadi ketika peretas menipu pengguna untuk mengirimkan permintaan *HTTP* yang tidak diinginkan ke situs *web* yang tepercaya. Ketidakhadiran token Anti-CSRF dapat memungkinkan peretas untuk melakukan berbagai tindakan atas nama pengguna tanpa sepengetahuan atau persetujuan mereka.
4. *Cross-Domain JavaScript Source File Inclusion*, kerentanan yang memungkinkan peretas untuk memasukkan file *JavaScript* berbahaya dari domain lain ke dalam halaman web. Hal ini dapat memungkinkan peretas untuk mencuri data, mengendalikan browser, atau melakukan tindakan lain yang tidak diinginkan.
5. *Incomplete or No Cache-Control and Pragma HTTP Header Set* memungkinkan pengembang web untuk mengontrol bagaimana browser pengguna menyimpan dan mengakses konten *web*. Jika *header* ini tidak diatur dengan benar, *peretas* dapat mencegat konten *web* dan memodifikasinya sebelum ditampilkan kepada pengguna. Hal ini dapat memungkinkan peretas untuk melakukan berbagai serangan, seperti *phishing* dan *malware*.
6. *X-Content-Type-Options-Header Missing* memungkinkan pengembang web untuk mencegah browser pengguna menebak jenis konten halaman *web*. Hal ini dapat membantu mencegah serangan *XSS*. Jika header ini tidak diatur, peretas dapat menebak jenis konten halaman *web* dan menyuntikkan kode berbahaya ke dalamnya.

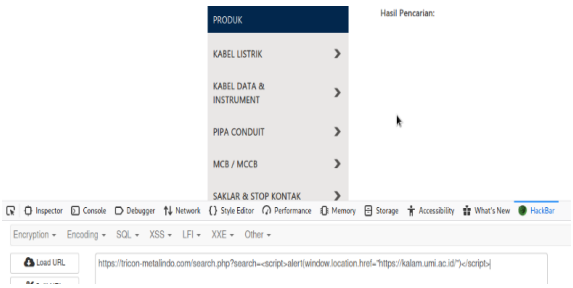
4.4. *Eksploitasi*

Tahap *eksploitasi* bertujuan untuk membuktikan bahwa kerentanan *XSS* yang ditemukan pada tahapan *Vulnerability Analysis* dapat dieksploitasi, maka dilakukanlah sebuah uji coba serangan yang dapat terjadi pada website. Untuk menemukan kerentanan *XSS* maka akan dilakukan beberapa teknik dengan cara: telusuri target dan temukan kode *javascrip*t ke dalam halaman. Metode lain adalah dengan mencoba menyuntikkan pada textbox, parameter, atau *URL* apa pun. Uji coba dapat dilihat pada Gambar 7, 8 dan 9.

Gambar 7. Menampikan pop-up

Pada gambar 7, menyuntikan kode ke searchbar yang berhasil mampilakan *pop-up* dengan menggunakan teknik *Simple injection* code *javascript* yang digunakan yakni,

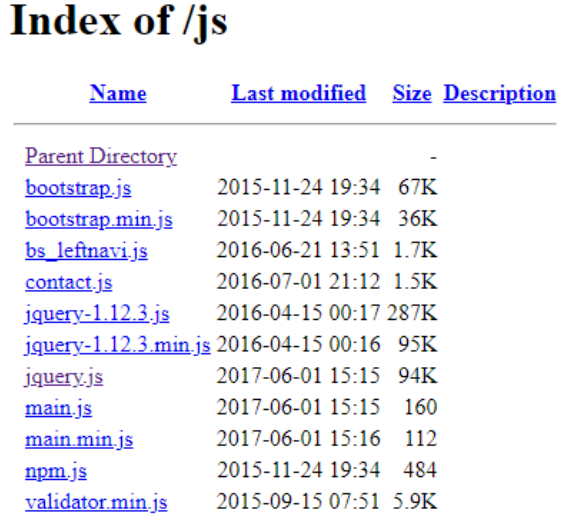
```
<script>alert(1);</script>
```



Gambar 8. Mengarahkan ke halaman lain

Pada gambar 8, menyuntikan kode ke searchbar yang yang dapat mengarahkan pengguna ke halaman berbahaya, code yang digunakan pada uji coba ini yaitu,

```
<script>alert(window.location.href="")</script>
```



Index of /js

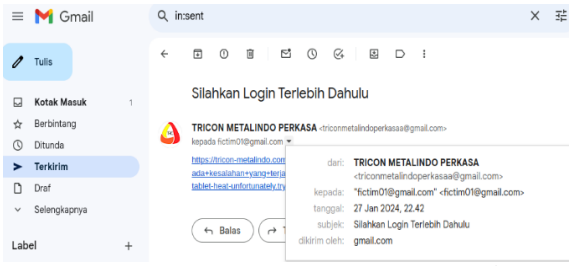
Name	Last modified	Size	Description
Parent Directory		-	
bootstrap.js	2015-11-24 19:34	67K	
bootstrap.min.js	2015-11-24 19:34	36K	
bs_leftnavi.js	2016-06-21 13:51	1.7K	
contact.js	2016-07-01 21:12	1.5K	
jquery-1.12.3.js	2016-04-15 00:17	287K	
jquery-1.12.3.min.js	2016-04-15 00:16	95K	
jquery.js	2017-06-01 15:15	94K	
main.js	2017-06-01 15:15	160	
main.min.js	2017-06-01 15:16	112	
npm.js	2015-11-24 19:34	484	
validator.min.js	2015-09-15 07:51	5.9K	

Gambar 9. Membuka file melalui URL

Kemudian melakukan uji coba terhadap *URL* secara manual, pada pengujian ini ditemukan kerentanan yang dimana seorang *cracker* atau penyerang dapat mengintip melalui *URL* yang ada dalam *system*, sehingga seorang penyerang dari luar

dapat mengakses file direktory pada website. Dapat dilihat pada gambar 9.

Berdasarkan *scanning* dan uji coba yang dilakukan sebelumnya selanjutnya melakukan simulasi serangan berdasarkan Skenario yang dibuat, skenaraio pada website PT. Tricon Metalindo Perkasa tahap pertama *Eksploitasi* dapat dilihat pada gambar 10.

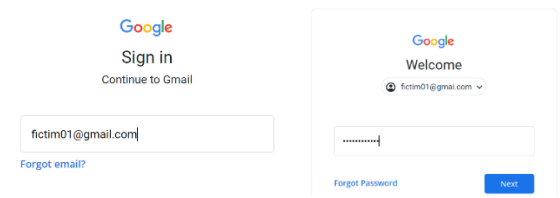


Gambar 10. Hacker mengirim link yang telah dimodifikasi

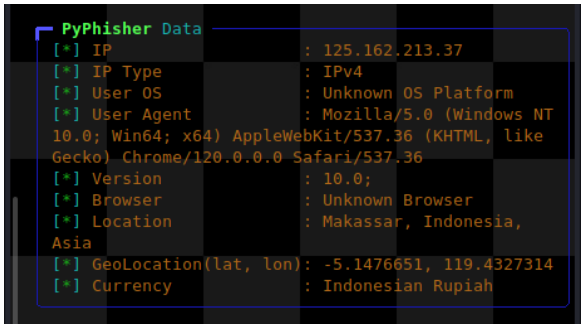
Pada gambar 10. menunjukan seorang penyerang atau hacker mengirimkan link yang telah dimofikasi kepada korban dengan nama dan logo PT. Tricon Metalindo Perkasa. Kemudian pada tahap kedua, apabila korban mengklik tautan tersebut maka korban akan diarahkan ke website asli yang telah dimodifikasi tampilnya oleh hacker dapat dilihat pada gambar 11.

Gambar 11. Halaman website yang dimodifikasi

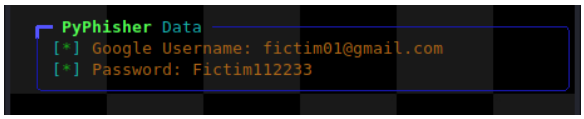
Kemudian pada tahap 4, apabila *hacker* membuat sebuah kode *skrip* dimana dia mengincar data sensitif korban dengan cara mengarahkan korban ke halaman lain apabila korban menekan tombol "*login*" yang ada korban akan di arahkan ke halaman *phising*, dimana apabila korban mengisi semua data yang ada maka data-data tersebut akan dikirim ke *hacker* dapat dilihat pada gambar 12, 13 dan 14.



Gambar 12. Korban memasukan gmail & password



Gambar 13. Informasi sensitif korban



Gambar 14. Informasi data yang dimasukan korban

4.5. Pembahasan

Hasil dari *Penetration Testing* yang telah dilakukan pada *website* PT. Tricon Metalindo Perkasa berdomain https://tricon-metalindo.com/ menemukan 2 celah kerentanan yang di antaranya *Cross-Site Scripting (XSS)* dengan tipe *Reflekted XSS* dan *Broken Access Control* dapat dilihat pada tabel 2.

Tabel 2. Rangkuman kerentanan

Kerentanan PT. Tricon Metalindo Perkasa				
Jenis	Lokasi	Inpact	RIsk	Condifence
Cross-site scripting	Searchbar	Perngarahan ke situs web berbahaya	Medium	Medium
Broken access control	URL	File system dapat intip	Low	Hight

Berdasarkan framework *OWASP* yang mencantumkan 10 kerentanan kemanan aplikasi *web* yang paling umum dan berpotensi merugikan, berikut adalah penjelasan singkat tentang resiko dan rekomendasi pada kerentanan yang ditemukan berdasarkan framework *OWASP Top* 10 *Vulnerability* dapat dilihat pada tabel 7.

Tabel 3. Jenis kerentanan

Jenis Kerentanan	**Resiko**	**Rekomendasi**
Cross-Site Scripting (XSS)	Kerentanan ini terjadi ketika aplikasi tidak memvalidasi atau memfilter input pengguna dengan benar dan memungkinkan injeksi kode skrip jahat. Serangan XSS dapat memungkinkan penyerang mencuri data pengguna atau menjalankan skrip berbahaya di browser pengguna.	Selalu validasi dan sanitasi input pengguna dengan benar pada kolom input pencarian. Pastikan hanya karakter yang diharapkan yang diterima, dan hindari menerima atau mengeksekusi input yang mengandung kode skrip.

Jenis Kerentanan	Resiko	Rekomendasi
Broken Acces Control	Kerentanan ini terjadi ketika kontrol akses tidak diterapkan dengan benar, sehingga pengguna mendapatkan akses yang tidak sah ke sumber daya yang seharusnya tidak dapat mereka akses. Ini dapat memungkinkan akses ke data sensitif atau fungsionalitas yang seharusnya terbatas.	Selalu lakukan pengecekan otorisasi di sisi server sebelum memberikan akses ke sumber daya atau fitur tertentu. Jangan hanya mengandalkan kontrol akses yang ada di sisi klien, karena ini dapat diakali oleh penyerang sehingga dapat mengakses file sensitif melalui path url.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis kerentanan website PT. Tricon Metalindo Perkasa menggunakan tools OWASP ZAP dan Hackbar, ditemukan beberapa kerentanan keamanan yang signifikan. Hasil scanning menunjukkan adanya 5 kerentanan severity high, 5 kerentanan severity medium, 11 kerentanan severity low, dan 7 kerentanan informational. Kerentanan utama yang ditemukan meliputi Reflected XSS pada kolom input pencarian, Vulnerable JS Library, X-Frame-Options Header Not Set, Absence of Anti-CSRF Tokens, serta beberapa kerentanan terkait konfigurasi header keamanan.

Pengujian eksploitasi pada kerentanan XSS berhasil dilakukan dengan beberapa skenario seperti menampilkan pop-up alert, mengarahkan pengguna ke halaman berbahaya, mengakses file directory melalui URL, serta potensi phishing dan pencurian data sensitif. Hasil pengujian ini membuktikan bahwa website masih memiliki celah keamanan yang dapat dimanfaatkan oleh penyerang untuk melakukan serangan yang dapat membahayakan pengguna maupun sistem. Oleh karena itu, diperlukan langkah-langkah perbaikan segera seperti implementasi validasi input, sanitasi data, pembaruan komponen, serta peningkatan kebijakan dan prosedur keamanan untuk mencegah potensi serangan di masa mendatang.

Beberapa perbaikan teknis yang perlu diimplementasikan segera meliputi penerapan validasi input yang ketat pada sisi server, sanitasi data untuk mencegah injeksi kode berbahaya, serta pembaruan komponen dan library JavaScript ke versi terbaru yang lebih aman. Konfigurasi header keamanan juga perlu diperbaiki dengan mengimplementasikan X-Frame-Options, Content Security Policy, dan pengaturan Cache-Control yang tepat.

Untuk penelitian selanjutnya, dapat dilakukan analisis kerentanan yang lebih mendalam dengan cakupan yang lebih luas, termasuk pengujian otomatisasi dan integrasi dengan pipeline CI/CD, serta studi kasus pada multiple website untuk mendapatkan pemahaman yang lebih komprehensif tentang pola kerentanan XSS dan metode mitigasinya.

DAFTAR PUSTAKA

Andria (2020) ‘Analisa Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux’, Gener.j, 4(2), pp. 69–79.

Fathur, M. (2020) ‘Tanggung jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen’, Jurnal Hukum, 2(1), pp. 43–60.

Hussain, M.Z. et al. (2017) ‘Penetration Testing In System Administration’, International Journal of Science and Technology Research, 6(6), pp. 275–278.

Ilham, K.F., Alwi, E.I. and Fattah, F. (2023) ‘Penerapan dan analisis network security Snort menggunakan intrusion detection system pada serangan UDP flood’, INFORMAL: Informatics Journal, 8(1), pp. 94–100.

Kals, S. et al. (2006) ‘Secubat: a web vulnerability scanner’, in Proceedings of the 15th international conference on World Wide Web. ACM, pp. 247–256.

Liu, M. et al. (2019) ‘A Survey of Exploitation and Detection Methods of XSS Vulnerabilities’, IEEE Access, 7, pp. 182004–182016.

Mulyanto, Y., Haryanti, E., and Jumirah (2021) ‘ANALISIS KEAMANAN WEBSITE SMAN 1 SUMBAWA MENGGUNAKAN METODE VULNERABILITY ASESEMENT’, JINTEKS (Jurnal Informatika Teknologi dan Sains, 3(3), pp. 394–400.

Nagendran, K. et al. (2019) ‘Web application penetration testing’, International Journal of Innovative Technology and Exploring Engineering, 8(10), pp. 1029–1035.

O.W.A.S.P. (2010) ‘The ten Most Critical Web Application Security Risk’, The Open Web Application Security Project [Preprint].

Riadi, I., Sunardi, S. and Handoyo, E. (2019) ‘Analisis Keamanan Jaringan Grr Rapid Response Menggunakan Kerangka Kerja COBIT 5. Lontar Komput’, Jurnal Ilmiah Teknologi Informasi, 10(1), p. 29.

Rodianto, R. et al. (2022) ‘Penerapan Network Development Life Cycle (NDLC) Dalam Pengembangan Jaringan Komputer Pada Badan Pengelolaan Keuangan dan Aset Daerah (BPKAD) Provinsi NTB’, Jurnal Ilmiah FIFO, 14(1), p. 35.

Sehaffudin, M.R., Indrihastuti, N. and Gunawan, E. (2017) ‘Pengisi Air Minum Otomatis Dengan Gelas Khusus Berbasis Arduino

Uno', Cahaya Bagaskara Jurnal Ilmiah Teknik Elektronika, 2(1), pp. 17–23.

Situmorang, J.R. (2012) 'Pemanfaatan Internet Sebagai New Media Dalam Bidang Politik, Bisnis, Pendidikan dan Sosial Budaya', Jurnal Administrasi Bisnis, 8(1), pp. 77–91.

Stiawan, D. et al. (2017) 'Cyber-attack penetration test and vulnerability analysis', International Journal of Online Engineering, 13(1), pp. 125–132.

Suroto, S. and Asman, A. (2021) 'Ancaman Terhadap Keamanan Informasi Oleh Serangan Cross-Site Scripting (XSS) dan Metode Pencegahannya', Jurnal Informatika, 11(1).

The Open Web Application Security Project (2013). The OWASP Foundation.

Drs. Taufiqqurrachman, M.Si (2022) PENGERTIAN URL. Available at: https://saintekmu.ac.id/myblog/taufiqqurrachman/pages/pengertian-url (Accessed: 30 October 2024).

Indah Sari (2014) 'MENGENAL HACKING SEBAGAI SALAH SATU KEJAHATAN DI DUNIA MAYA', JURNAL SISTEM INFORMASI UNIVERSITAS SURYADARMA, 10(2). Available at: https://doi.org/10.35968/jsi.v10i2.1086.

Sinlae, F. et al. (2024) 'Pengenalan Pemrograman Web: Pembuatan Aplikasi Web Sederhana Dengan PHP dan MYSQL'.