P-ISSN: 2963-4008
E-ISSN: 2963-430X

# PENGUJIAN KEAMANAN DENGAN METODE OWASP TOP 10 PADA WEBSITE EFORM HELPDESK

**Rangga Renaldi Yusuf[1], Teguh Nurhadi Suharsono[2]**
**[1, 2] Teknik Informatika, Universitas Sangga Buana**

**[1] korespondensi: ranggarenaldi@gmail.com**

## ABSTRACT

*The development of modern technology has had a significant positive impact on various aspects of life. However, along with this progress, the threat from hackers is also increasing. Hackers are individuals or groups with the ability to breach computer systems or networks, whether for illegal purposes, stealing data, or spreading malware. To avoid this, there is a method called penetration testing. Penetration Testing is a series of methods carried out to test the security of a system. The penetration testing process involves analyzing a system to identify potential security vulnerabilities such as system configuration errors, flaws in software or hardware development, and weaknesses in the logic of a process. After conducting a penetration test using the OWASP TOP 10 2021 method on the Eformhelpdesk website, there were six security vulnerabilities identified in the OWASP TOP 10 2021 category, and one vulnerability that did not fall into that category*.

*Keywords: Information Security, Penetration Testing, OWASP TOP 10 2021*

## ABSTRAK

*Perkembangan teknologi modern telah membawa dampak positif besar dalam berbagai aspek kehidupan. Namun, seiring dengan kemajuan ini, ancaman dari para hacker juga semakin meningkat. Hacker merupakan individu atau kelompok yang memiliki kemampuan untuk meretas sistem komputer atau jaringan, baik untuk tujuan ilegal, mencuri data, atau menyebarkan malware. Untuk menghindari hal tersebut terdapat sebuah metode yang disebut penetration tesing. Penetration testing merupakan serangkaian cara yang dilakukan untuk menguji keamanan pada sebuah sistem. Proses penetration testing dengan melibatkan proses analisis kepada sebuah sistem untuk mencari potensi celah keamanan seperti kesalahan konfigurasi sistem, cacat dalam pengembangan software maupun hardware dan kelemahan dalam logika dari sebuah proses. Setelah melakukan uji penetrasi menggunakan metode OWASP TOP 10 2021 terhadap website Eformhelpdesk, terdapat 6 celah keamanan dalam kategori OWASP TOP 10 2021 dan 1 celah tidak termasuk dalam kategori tersebut.*

*Kata Kunci: Keamanan informasi, Penetration testing, OWASP TOP 10 2021*

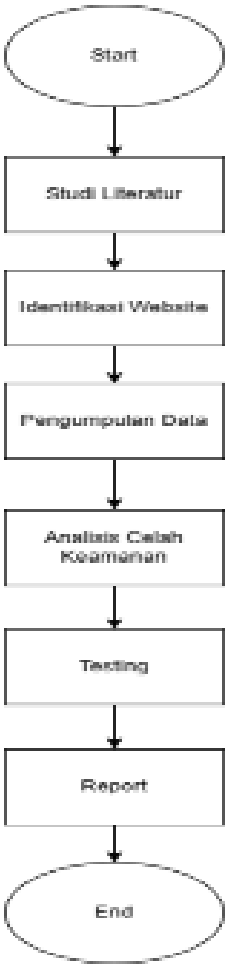
## PENDAHULUAN

Perkembangan teknologi saat ini berkembang pesat dari berbagai bidang seperti muncul aplikasi-aplikasi untuk pengelolaan data yang biasa digunakan di bidang transportasi, medis, perbankan, pendidikan, e-commerce, asuransi, dan kebersihan yang tentunya sangat memudahkan manusia dalam melakukan kegiatan dalam bidang-bidang tersebut. Perkembangan teknologi tersebut pun memiliki ancaman yang besar pada sisi security bila dibandingkan dengan dahulu. Karena tools-tools untuk mendeteksi kelamahan tersebut semakin berkembang, belum adanya ancaman lain yang disebabkan oleh malware atau virus bisa merugikan perorangan ataupun Perusahaan. Oleh sebab itu pengembang-pengembang aplikasi seperti developer harus memerhatikan hal tersebut agar aplikasi-aplikasi yang dibuat bisa terhindar dari kejahatan siber. Studi kasus yang akan menjadi objek pada penelitan ini adalah Website EformHelpdesk. Adanya kesalahan developer dalam pembuatan aplikasi ini diperlukan penelitian yang dapat

digunakan sebagai referensi atau solusi yang bisa dipakai untuk developer agar aplikasi yang dibuat bisa terhindar dari kejatan siber. Untuk mengetahui kesalahan atau kerentanan pada website tersebut, pada penelitian ini akan menggunakan standar keamanan pada OWASP TOP 10 2021. Hasil dari penelitian ini yaitu dapat mengetahui kerantanan-kerentanan yang terdapat pada website eformhelpdesk serta rekomendasi yang dapat diberikan dari hasil kerentanan-kerentanan yang telah ditemukan.

## METODE

Metodelogi penelitian ini dilakukan secara sistematis untuk mendapatkan pedoman dalam melaksanakan penelitian agar mencapai tujuan yang diinginkan.




**Gambar 1: Flowchart tahapan penelitian**

### 1. Studi Literatur

Tujuan dari tahap ini adalah untuk mendeskripsikan tinjauan pustaka terhadap teori-teori yang mendukung penelitian, diantaranya mengenai penetration testing, website, vulnerability, OWASP, OWASP Top 10, zed attack proxy (ZAP). Kegiatan ini dilakukan melalui membaca buku, majalah, laporan penelitian dan website di internet.

***Penetration Testing***

*Penetration* testing merupakan serangkaian cara yang dilakukan untuk menguji keamanan

pada sebuah sistem. Proses *penetration testing* dengan melibatkan proses analisis kepada sebuah sistem untuk mencari potensi celah keamanan seperti kesalahan konfigurasi sistem, cacat dalam pengembangan *software* maupun *hardware* dan kelemahan dalam logika dari sebuah proses(1)

Rafay Baloch(2) menjelaskan bahwa penetration testing dibagi menjadi tiga, yaitu:

*Black Box testing* merupakan jenis penetration dimana penguji penetrasi harus menemukan semua informasi yang mereka perlukan untuk menguji sistem, karena pengujian ini dilakukan oleh pihak yang tidak memiliki pengetahuan tentang sistem operasi, versi server, atau jaringan yang dikandung sistem tersebut.

*White box testing* merupakan jenis penetration dimana penguji penetrasi mengetahui semua informasi tentang sistem operasi, versi server, atau jaringan yang digunakan, dengan tujuan menemukan kerentanan yang ada dan memungkinkan administrator di organisasi dapat segera memperbaikinya

*Gray box testing* merupakan jenis penetration dimana penguji penetrasi hanya mengetahui sebagian informasi sistem, sebagai contoh diinformasikan mengenai nama aplikasi yang berjalan di background tapi tidak diinformasikan mengenai versi dari aplikasi yang dipakai.

***Website***

*Website* merupakan sekumpulan informasi atau kumpulan page yang biasa diakses menggunakan internet dan informasi tersebut berupa teks, gambar, film, ataupun suara. Setiap orang dapat mengakses dapat mengakses informasi dalam website dimanapun dan kapanpun selama terhubung dengan akses internet. Dan secara teknis website merupakan kumpulan dari page-page yang tergabung kedalam suatu domain atau subdomain tertentu(3).

***Vulnerability***

*Vulnerability* adalah suatu titik lemah atau suatu kelemahan dalam suatu prosedur keamanan control administratif, kontrol internet dan lain-lain sebagai yang dapat dieksploitasi melalui suatu trik untuk memperoleh akses yang tidak valid terhadap informasi atau untuk mengganggu proses secara kritis(4).

**OWASP**

OWASP adalah singkatan dari "*Open Web Application Security Project*". OWASP adalah sebuah organisasi nirlaba yang berfokus pada peningkatan keamanan aplikasi web dan perangkat lunak.(5) Tujuan utama dari OWASP adalah untuk meningkatkan pemahaman tentang risiko keamanan dalam pengembangan perangkat lunak, serta menyediakan sumber daya dan alat untuk membantu para profesional keamanan dan pengembang mengidentifikasi dan mengatasi kerentanan dalam aplikasi web. Salah satu hasil yang paling terkenal dari OWASP adalah daftar "OWASP Top Ten".

**OWASP Top 10**

OWASP Top 10 adalah sebuah panduan bagi para developers dan security team tentang kelemahan-kelemahan pada web apps yang

mudah diserang dan harus segera disiasati. Kelemahan-kelemahan ini memudahkan hacker untuk menanam malware, mencuri data, atau mengambil alih sepenuhnya website atau komputer(6).

***Zed Attack Proxy (ZAP)***

*Zed Attack Proxy* (ZAP) merupakan aplikasi yang digunakan untuk membantu pengembang maupun pentester dalam analisi kerentanan. Aplikasi ini memiliki dua kategori scan yang dapat dilakukan yaitu automated dan manual scan(7).

**Identifikasi Website**

Website Eformhelpdesk adalah suatu sistem yang dibuat sebagai sarana untuk pencatatan mengenai data spesifikasi, rekomendasi, dan list IP address computer yang ada diperusahaan dan juga digunakan untuk form peminjaman barang IT diperusahaan.

**Pengumpulan Data**

Pengumpulan data atau sering disebut information gathering merupakan tahapan pengumpulan informasi secara umum yang dilakukan pada target. Informasi yang dikumpulkan meliputi informasi mengenai IP target, port yang tersedia, spesifikasi CMS atau framework dan server yang digunakan, dan berbagai informasi penting lainnya yang digunakan oleh sistem.(8)Tools yang dipakai pada penelitian ini yaitu Whatweb, Nmap, CMSeek, CMSDetect, dan HTTPprint digunakan selama fase ini.

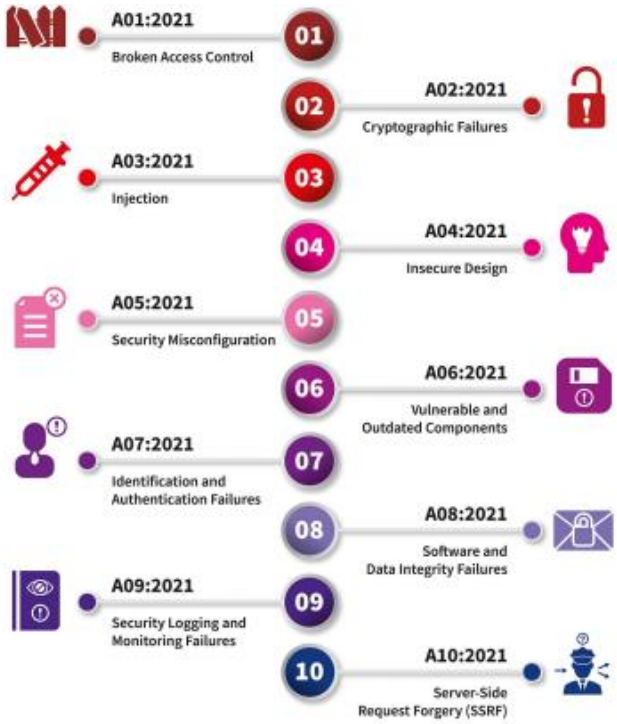
**Analisis Celah Keamanan**

Analisis kerentanan atau proses scanning merupakan proses mendefinisikan, mengidentifikasi, dan memprioritaskan kerentanan dalam sistem komputer, aplikasi, dan infrastruktur jaringan serta memberikan organisasi melakukan penilaian dengan pengetahuan, kesadaran, dan latar belakang risiko. (9)Alat yang digunakan dalam penelitian ini adalah tools bawaan dari OWASP yaitu ZAP (Zed Attack Proxy). Kemudian hasil pemindaian tools tersebut selanjutnya akan dilakukan pengecekan kebenerannya pada tahap testing.

***Testing***

Tujuan dari tahap ini yaitu untuk melakukan pengujian penetrasi berdasarkan OWASP TOP 10 2021 di situs web Eformhelpdesk dengan menggunakan berbagai macam tools untuk menguji kerentanan pada sisi keamanan website "eformhelpdesk" Berikut adalah daftar kerentanan yang diterapkan oleh OWASP Top 10 2021(10), yang dapat dilihat pada Gambar 2

P-ISSN: 2963-4008
E-ISSN: 2963-430X




**Gambar 2: OWASP Top 10 2021**

**Report**

Tahapan ini berisi tentang gambaran laporan hasil penetration testing yang dilakukan dan dapat digunakan sebagai panduan untuk memperbaiki website Eformhelpdesk.

## HASIL DAN PEMBAHASAN

### *Information Gathering*

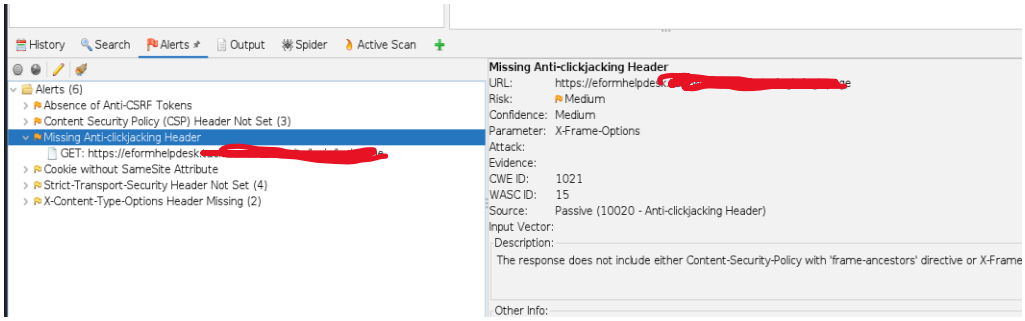
Hasil dari proses *information gathering*, dapat dilihat pada Tabel 1.

**Tabel 1: Hasil information gathering**

| No | Tools | Hasil Scanning |
|---|---|---|
| 1 | Netcraft | IP Address, yaitu 103.10.xxx.xxx |
| 2 | Whois | Alamat Server, Hosting, Email,dan informasi yang lainnya mengenai wabsite eformhelpdesk, yaitu di Jl xxxx, Bandung xxxx, xxxxx co.id |
| 3 | CMSeek dan CMS Detector | Tidak terdeteksi |
| 4 | HttPrint | Tidak terdeteksi |
| 5 | Nmap | Open Port:<br>Port 22 ssh openssh versi 7.6,<br>Port 80 apache httpd versi 2.4.29,<br>Port 3306 mysql versi 5.7.42-ubuntu 18.04<br>Sistem Operasi:<br>linux ubuntu 18.04 |

***Scanning***

Berikut merupkan hasil dari proses scanning, dapat dilihat pada Gambar 3. Hasil Scanning OWASP ZAP yang diambil yaitu yang medium risk dengan keterangan "Missing Anti-clickjacking Header" dalam respons HTTP untuk melindungi dari serangan Clickjacking oleh atacker sehingga serangan Clickjacking dapat saja dilakukan dari luar terhadap website Eformhelpdesk.



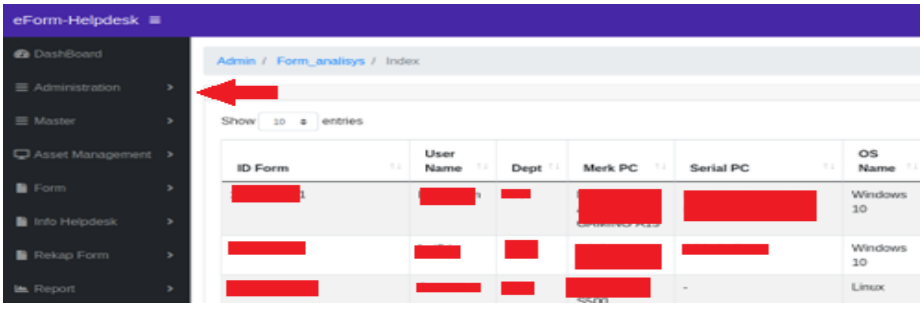

**Gambar 3: Hasil Scanning**

***Testing***

Berikut merupakan hasil penemuan pada proses testing yang telah dilakukan pada website eformhelpdesk berdasarkan standar keamanan OWASP Top 10 2021.

***Broken Access Control***

Untuk pengencekan Broken Access Control dilakukan secara manual dikarenakan Tools OWASP ZAP tidak mendeteksi kerentanan dari broken access control, disini akan dilakukan percobaan menggunakan view page source dari web eformhelpdesk, lalu ditemukan link untuk role admin. Setelah dilakukan perubahan url dari user menjadi url admin, role user dapat mengakses menu dari role admin, dapat dilihat pada Gambar 4.

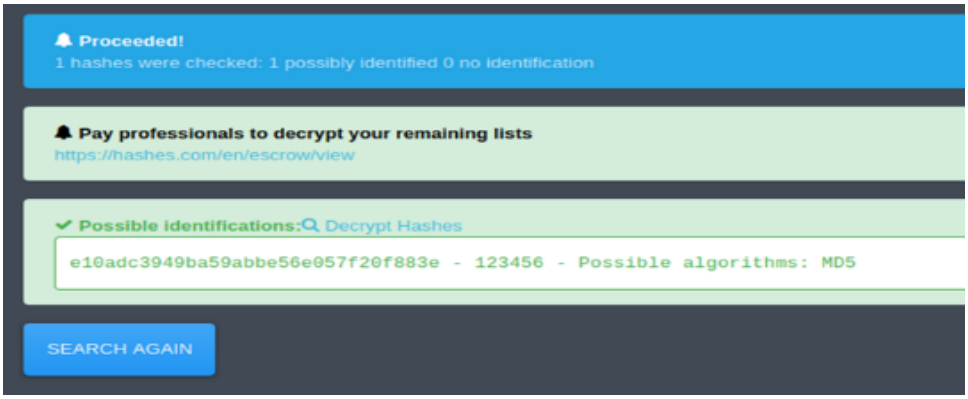



**Gambar 4: Gambar 4: Menu Role Admin**

***Cryptographic Failures***

Kerentanan ini berfokus pada pengungkapan data sensitif yang telah telah terkena serangan siber. oleh karena itu untuk kerentanan ini akan dilakukan pengecekan terkait penggunaan kriptografi pada data sensitif, untuk data sensitif yang diuji pada website eformhelpdesk yaitu

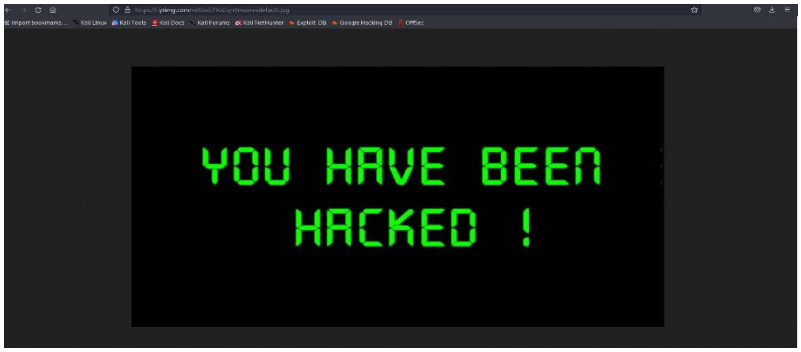
pada penggunaan hashing yang digunakan. Langkah pertama lakukan ambil salah satu data username dan password pada tabel database web Eformhelpdesk, kemudian dicek type hash serta cek kualitas hash yang digunakan, dengan dengan menggunakan tools online pada link "https://hashes.com/en/tools/hash_identifier" hasil pengecekan dapat dilihat pada Gambar 5.




**Gambar 5: Decrypt Hash**

**XSS (cross site scripting)**

Pengujian XSS dilakukan secara manual dengan menginput script alert sederhana dan script untuk meredirect halaman web eformhelpdesk pada salah satu inputan form web Eformhelpdesk dan ditemukan kerentanan dengan jenis XSS stored, untuk hasilnya dapat dilihat pada Gambar 6.

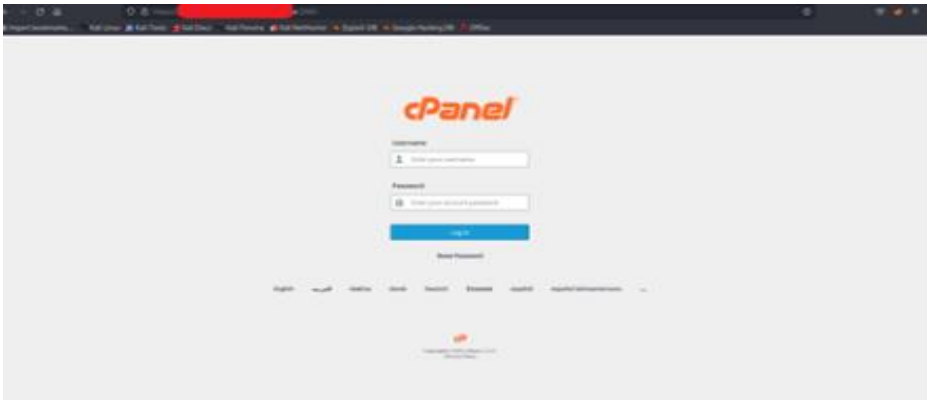



**Gambar 6: XSS Stored**

***Security Misconfiguration***

Pengecekan kerentanan ini dilakukan dengan cara melakukan scanning directory listing menggunakan tools dirb, gunakan wordlist directory listing agar proses scanning bisa lebih maksimal. Setelah dilakukan scanning terdapat dua url yang terdeteksi yaitu url untuk akses boostrap dan akses cpanel seperti pada Gambar 7.

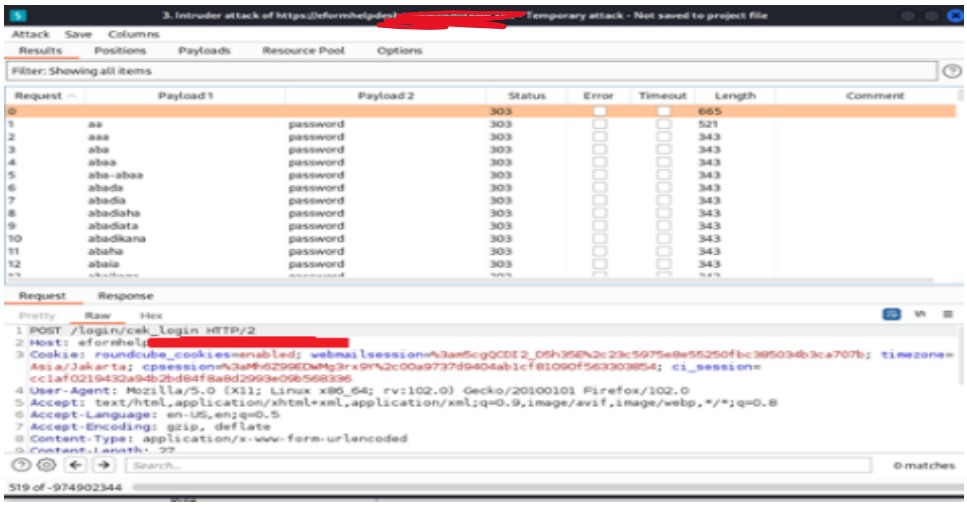
P-ISSN: 2963-4008
E-ISSN: 2963-430X




**Gambar 7: Akses Cpanel**

***Identification and Authentication Failures***

Pengujian kerentanan identification and Authentication failures dilakukan dengan cara melalukan teknik bruteforce login page, tools yang digunakan yaitu burpsuite, Pengecekan dilakukan secara manual dengan mengecek semua menu di website, setelah dilakukan Proses penyerangan dengan teknik bruteforce ini cukup memakan waktu yang lama, pada percobaan ini telah dilakukan percobaan sebanyak 519 kali tanpa adanya limit login, hasil percobaan tersebut dapat dilihat pada Gambar 8.

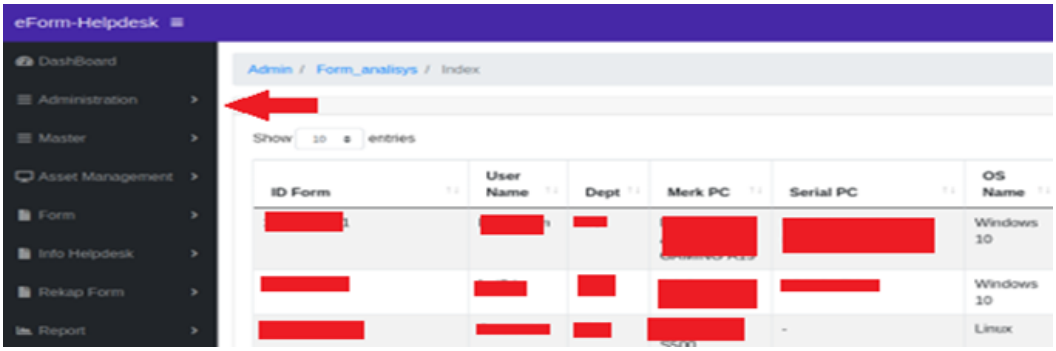



**Gambar 8: Penyerangan dengan Teknik Bruteforce**

***Security Logging and Monitoring Failures***

Pengecekan dilakukan secara manual dengan mengecek semua menu di website, setelah dilakukan pengecekan terdapat kerentanan ini dikarenakan tidak ada menu website yang mencatat semua aktifitas website. Dapat dilihat list menunya pada Gambar 9.

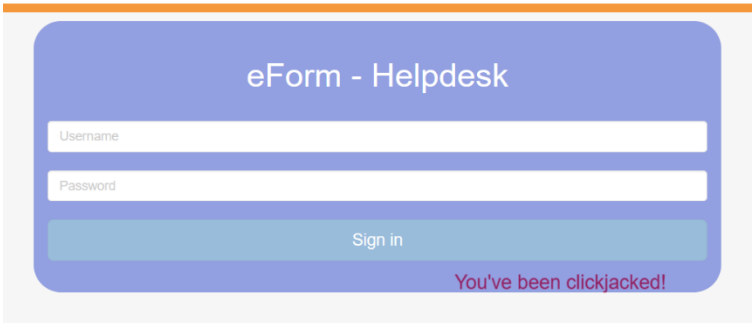
P-ISSN: 2963-4008
E-ISSN: 2963-430X




**Gambar 9: Menu Admin Website Eformhelpdesk**

***Clickjacking***

Pengujian kerentanan ini dilakukan dengan menggunakan script dari tools burpsuite. Hasil dari tahap ini hasilnya sama dengan scanning tools ZAP pada tahap sebelumnya, clickjacking yang dikategorikan medium warning. Untuk hasil dari tahap ini dapat dilihat pada Gambar 10.




**Gambar 10: Hasil *Clickjaking***

***Report***

Berdasarkan hasil semua analisis kerentanan yang dilakukan sebelumnya, dapat dilihat pada Tabel 2.

**Tabel 2: Report**

| Level Risk/Score | Metode | Status | Hasil Testing |
|---|---|---|---|
| High 7.5/10 | Broken Access Control | Dapat Ditemukan | Dapat menggunakan hak akses role admin pada autentikasi role user dengan mengubah url dari "/user" menjadi "/admin" |
| High 7.25/10 | Cryptographic Failures | Dapat Ditemukan | Menggunakan Hashing MD5 |

| Level Risk/Score | Metode | Status | Hasil Testing |
|---|---|---|---|
| High 8.25/10 | Injection (XSS) | Dapat Ditemukan | Dapat menjalankan script javascript dan XSS yang ditemukan merupakan jenis XSS Stored |
| | Injection SQL Injection | Tidak dapat ditemukan | All tested parameter do not appear to be injectable |
| - | Insecure Design | Tidak dapat ditemukan | - |
| Medium 4.75/10 | Security Misconfiguration | Dapat Ditemukan | Direktory : *https://Alamat_ website/cpanel *https://Alamat_ Website/js/ |
| - | Vulnerable and Outdated Components | Tidak dapat ditemukan | Not Vulnerable |
| High 7/10 | Identification and Authenticaion Failures | Dapat Ditemukan | Dapat melakukan Brutoforce, Percobaan yang Dilakukan sebanyak 519 kali |
| - | Software and Data Integrity Failures | Tidak dapat ditemukan | - |
| Medium 3.5/10 | Security Logging and Monitoring Failures | Dapat Ditemukan | Tidak ada menu untuk melihat aktifitas user |
| - | Server-Side Request Forgery | Tidak dapat ditemukan | Tidak ada HTTP header Request ke server lain |
| Medium | Clickjacking from vulnerability scanning | Dapat Ditemukan | You've been clickjacked |

Ancaman-ancaman terbaru pada website sudah dilakukan survey oleh OWASP (Open Web Application Security Project) dan sudah tercatat pada OWASP Top 10 2021. Pada OWASP Top 10 2021, terdapat beberapa ancaman dan tingkat resiko berserta persentase kejadian pada ancaman-ancaman terbaru terhadap website. Untuk perhitungan tingkat ancaman terhadap penemuankerentanan dapat menggunakan kalkulator OWASP risk rating yang sudah otomatis menggunakan CVSS (Common Vulnerability Scoring System) dengan rentang score 0.0 sampai 10.0, hasil perhitungan dari kerentanan yang telah diteliti dapat dilihat pada Tabel 3.

**Tabel 3: Klasifikasi ancaman-ancaman yang ditemukan**

| No | Ancaman | CVSS Score | Persentasi yang sering Terjadi | Status |
|---|---|---|---|---|
| 1 | Broken Access Control | 7.5 | 56% | Ditemukan |
| 2 | Cryptographic Failures | 7.3 | 46% | Ditemukan |
| 3 | Injection | 8.3 | 19% | Ditemukan |
| 4 | Insecure Design | - | 24% | Tidak ditemukan |

| No | Ancaman | CVSS Score | Persentasi yang sering Terjadi | Status |
|---|---|---|---|---|
| 5 | Security Misconfiguration | 4.8 | 20% | Ditemukan |
| 6 | Vulnerable and Outdated Components | - | 28% | Tidak ditemukan |
| 7 | Identification and Authenticaion Failures | 7.0 | 15% | Ditemukan |
| 8 | Software and Data Integrity Failures | - | 17% | Tidak ditemukan |
| 9 | Security Logging and Monitoring Failures | 3.5 | 19% | Ditemukan |
| 10 | Server-Side Request Forgery | - | 3% | Tidak ditemukan |

## SIMPULAN

Proses pengujian celah keamanan website Eformhelpdesk melalui beberapa tahap yaitu studi literatur, identifikasi website, pengumpulan data (information gathering), analisis celah kemanan (scanning), testing dengan berfokus pada OWASP TOP 10 2021 dan terakhir melalukan reporting pada hasil yang telah ditemukan dan dianalisis. Adapun celah keamanan yang ditemukan pada tahap pengujian yaitu Broken Access Control, Crytogrphic Failures, Injection, Security Misconfiguration, indentifiation Failures dan Security Logging and Monitoring Failures, dan celah lain yang ditemukan namun tidak termasuk dalam TOP 10 keamanan OWASP yaitu Clickjacking. Setelah selesai melakukan uji penetrasi menggunakan metode OWASP TOP 10 2021 pada website Eformhelpdesk, memiliki 6 celah keamanan yang perlu untuk dilakukan perbaikan berikut saran rekomendasi dari 6 celah tersebut yaitu, Broken Access Control melakukan Penambahan filter hak akses agar menu yang diakses sesuai dengan role, Cryptographic Failures disarankan menggunakan Hashing terbaru seperti salt, Injection (XSS) Melakukan filtering terhadap karakter-karakter khusus seperti “<”,”>” dan karakter khusus lainnya, Security Misconfiguration dengan melakukan penutupan Akses login cpanel ke public, Identification and Authenticaion Failures dengan melakukan konfigurasi unutk menambah limit login dan terakhir Security Logging and Monitoring Failures dengan Membuat menu log untuk melihat aktifitas user

## DAFTAR PUSTAKA

1. Bacudio AG, Yuan X, Bill Chu BT, Jones M. An Overview of Penetration Testing. International Journal of Network Security & Its Applications. 2011 Nov 30;3(6):19–38.

2. Baloch R. Ethical Hacking And Penetration Testing Guide.

3. Hamdan Romadhon M, Yudhistira Y. Sistem Informasi Rental Mobil Berbsasis Android Dan Website Menggunakan Framework Codeigniter 3 Studi Kasus : CV Kopja Mandiri [Internet]. Vol. 2, Jurnal Sistem Informasi dan Teknologi Peradaban (JSITP). 2021. Available from: www.journal.peradaban.ac.id

4. Elu AM. Rancang Bangun Aplikasi Pendeteksian Vulnerability Structured Query Language (Sql) Injection Untuk Keamanan Website.

5. Oleh D. (Universitas Islam Indonesia) Tugas Akhir.

6. Dewa Web. OWASP: Standar Keamanan Web App Dunia [Internet]. [cited 2023 Sep 29]. Available from: https://www.dewaweb.com/blog/owasp-standar-keamanan-web-app-dunia/

7. Arafat Amalana A. Penetration Testing Pada Website Registar Pengelola Nama Domain Internet Indonesia (PANDI).

8. Ary G, Sanjaya S, Made G, Sasmita A, Made D, Arsa S. Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF.

9. Jurnal H, Putu N, Rainita A, Agung A, Callysta Athalia I, Ananta P, et al. Jurnal Informatika Dan Tekonologi Komputer Analisis Perbandingan Vulnerability Scanning Pada Website Dvwa Menggunakan Owasp Nikto Dan Burpsuite. 2023;3(Juli).

10. OWASP. OWASP Top 10 2021 [Internet]. 2021 [cited 2023 Oct 1]. Available from: https://owasp.org/Top10/