Analisis Keamanan *Website* XYZ Kabupaten M Menggunakan *Framework* Issaf

Chafidz Izzuddin Robbani
Sistem Informasi
Telkom University Surabaya
Surabaya, Indonesia
chafidzizzuddin@student.telkomuniversity.ac.id

Muhamad Nasrullah
Sistem Informasi
Telkom University Surabaya
Surabaya, Indonesia
emnasrul@telkomuniversity.ac.id

Adzanil Rachmadhi Putra
Sistem Informasi
Telkom University Surabaya
Surabaya, Indonesia
adzrachmadhip@telkomuniversity.ac.id

***Abstrak* — Penelitian ini membahas keamanan *Website* Sistem Informasi Kerjasama Media (XYZ) milik Dinas Komunikasi dan Informatika Kabupaten M. XYZ digunakan untuk mengelola kerjasama media pemerintah secara transparan dan efisien. Sistem ini menyimpan data sensitif, namun tidak pernah dilakukan pengecekan keamanan rutin, meningkatkan risiko pencurian data.**

Untuk mengatasi masalah ini, dilakukan pengujian keamanan menggunakan metode *penetration testing* berbasis *Framework ISSAF (Information Systems Security Assessment Framework). ISSAF* terdiri dari sembilan tahap, mulai dari pengumpulan informasi hingga menutupi jejak, guna mengidentifikasi kerentanan sistem.

Hasil pengujian menunjukkan bahwa *Website* XYZ memiliki celah keamanan, seperti informasi yang mudah diakses dan *port* terbuka. Meski SSL/TLS dapat membantu mencegah serangan, masih terdapat risiko dengan kategori *high, medium,* dan *low*. Oleh karena itu, diberikan rekomendasi perbaikan guna meningkatkan keamanan sistem.

Dengan implementasi langkah-langkah ini, diharapkan tingkat keamanan *Website* XYZ meningkat, risiko pencurian data berkurang, serta kepercayaan publik terhadap layanan Kominfo semakin tinggi.

Kata Kunci: Website, Penetration Testing, ISSAF, Keamanan

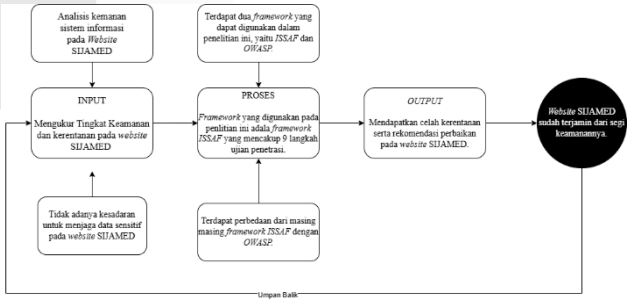
I. PENDAHULUAN

Di era digital saat ini, *Website* menjadi sarana penting bagi organisasi, termasuk instansi pemerintahan, dalam menyampaikan informasi dan layanan kepada publik (Umar, R., Riadi, I., & Elfatiha, M. I. A. (2023). Salah satu contohnya adalah Sistem Informasi Kerjasama Media (XYZ) yang dikembangkan oleh Dinas Komunikasi dan Informatika Kabupaten M. *Website* ini digunakan untuk mengelola kerja sama media dengan mitra pemerintah secara lebih transparan dan efisien.

Namun, dalam wawancara dengan Kepala Divisi Teknologi Informasi Diskominfo Kabupaten M, terungkap bahwa tidak ada pengecekan keamanan rutin terhadap *Website* XYZ. Hal ini menimbulkan risiko besar, seperti potensi pencurian data sensitif oleh pihak yang tidak bertanggung jawab. Seiring dengan meningkatnya ancaman siber, keamanan *Website* menjadi aspek yang tidak bisa diabaikan.

Penelitian ini bertujuan untuk menganalisis tingkat keamanan *Website* XYZ dengan menggunakan metode penetration testing berbasis *Information Systems Security Assessment Framework (ISSAF). Framework* ini mencakup sembilan tahap evaluasi keamanan, mulai dari pengumpulan informasi hingga mitigasi risiko. Hasil analisis diharapkan dapat mengidentifikasi potensi kerentanan dan memberikan rekomendasi untuk meningkatkan perlindungan data serta keandalan sistem informasi di sektor pemerintahan.

Kerangka berpikir merupakan pemikiran dasar peneliti yang disintesiskan dari tinjauan pustaka dan hasil penelitian yang relevan, observasi, kajian perpustakaan, atau narasi tentang kerangka bagaimana pemecahan masalah yang telah dirumuskan (Peirisal, T., & Hidayat, S. (2021, October). Pada penelitian ini terdapat flowchart kerangka berpikir, yaitu dimulai dengan menentukan topik, pada tahapan ini akan mencari masalah yang terjadi serta menghasilkan output sebuah pemberian saran perbaikan kepada objek.



Gambar 1
(*Flowchart* Alur Kerangka Berpikir)

II. KAJIAN TEORI

1. *Website* dan Keamanan Sistem Informasi

Website merupakan sistem yang berfungsi sebagai media komunikasi, promosi, serta penyedia layanan bagi pengguna secara daring (Sofyan, Sugiarto, & Akbar, 2023).

Dalam sektor pemerintahan, *Website* menjadi sarana penting dalam mendukung transparansi serta efisiensi pelayanan publik. Namun, seiring dengan berkembangnya teknologi, ancaman keamanan siber juga meningkat, sehingga diperlukan langkah-langkah pencegahan untuk melindungi data sensitif yang tersimpan dalam sistem (Umar, Riadi, & Elfatiha, 2023).

2. Ancaman Keamanan Siber

Serangan siber merupakan ancaman serius yang dapat mengakibatkan pencurian data, manipulasi informasi, hingga gangguan terhadap operasional suatu sistem. Beberapa serangan yang umum terjadi adalah *phishing, SQL injection, cross-site scripting (XSS),* serta *ransomware* (Latifah, Mawardi, & Wardhana, 2022). Di Indonesia, kasus serangan siber mengalami peningkatan yang signifikan, dengan laporan sebanyak 88 juta serangan dalam periode Oktober 2023 (Badan Siber dan Sandi Negara, 2023).

3. *Penetration Testing*

Penetration testing atau uji penetrasi merupakan teknik yang digunakan untuk menguji keamanan suatu sistem dengan mensimulasikan serangan siber. Uji ini bertujuan untuk mengidentifikasi celah keamanan serta memberikan rekomendasi perbaikan sebelum sistem tersebut diserang oleh pihak yang tidak bertanggung jawab (OISSG, 2019).

4. *Framework ISSAF (Information Systems Security Assessment Framework)*

ISSAF adalah *framework* yang dirancang untuk melakukan evaluasi keamanan sistem informasi secara sistematis. *Framework* ini mencakup sembilan tahap pengujian, yaitu:

a. *Information Gathering:* Pengumpulan informasi awal tentang sistem target.
b. *Network Mapping*: Pemetaan jaringan dan analisis arsitektur sistem.
c. *Vulnerability Identification*: Identifikasi kelemahan dalam sistem.
d. *Penetration Testing:* Simulasi serangan untuk mengukur tingkat keamanan.
e. *Gaining Access and Privilege Escalation*: Pengujian akses tidak sah terhadap sistem.
f. *Enumerating Further:* Eksplorasi lebih dalam terhadap data yang dapat diakses.
g. *Compromise Remote User/Sites:* Pengujian eksploitasi melalui akses jarak jauh.
h. *Maintaining Access:* Simulasi serangan untuk mempertahankan akses.
i. *Covering Tracks*: Upaya menghapus jejak serangan guna menghindari deteksi (Umar *et al*., 2023).

Framework ISSAF dipilih dalam penelitian ini karena mencakup aspek yang lebih luas dalam evaluasi keamanan sistem informasi dibandingkan dengan *framework* lain, seperti *OWASP (Open Web Application Security Project)* yang lebih terfokus pada keamanan aplikasi berbasis *web* (Sutarli & Kurniawan, 2023).

5. *Tools* yang Digunakan dalam Pengujian Keamanan

Untuk menguji keamanan *Website* XYZ, digunakan beberapa tools berikut:

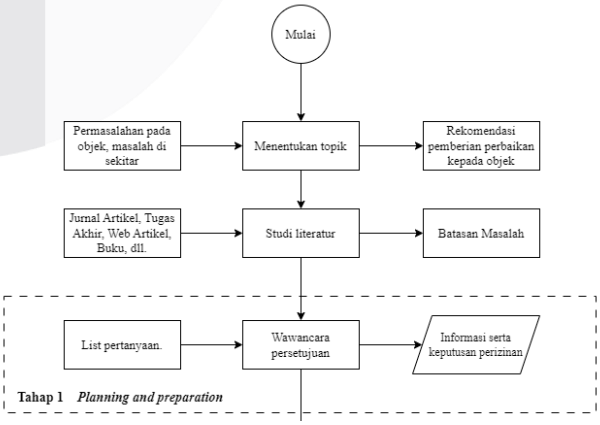
a. Nmap: Untuk memindai jaringan dan mendeteksi *port* yang terbuka (Andriyani, Sidiq, & Zen, 2023).
b. *OWASP ZAP:* Untuk mengidentifikasi kerentanan dalam aplikasi berbasis *web (OWASP,* 2024*).*
c. *Burp Suite:* Untuk menganalisis komunikasi jaringan dan mengevaluasi sistem keamanan (Haq & Khan, 2021).
d. *SQLMap*: Untuk mendeteksi dan mengeksploitasi celah keamanan *SQL Injection* (*Kali Linux*, 2024).
e. *Hydra:* Untuk melakukan uji coba serangan *brute force* terhadap sistem *login* (*Kali Linux*, 2024).

Kajian teori ini menyoroti pentingnya pengujian keamanan *Website* untuk mencegah serangan siber yang berpotensi merugikan instansi pemerintahan. *Framework ISSAF* dipilih karena cakupannya yang lebih luas dalam mengidentifikasi kelemahan sistem informasi. Dengan menggunakan berbagai *tools* pendukung, pengujian keamanan dapat dilakukan secara lebih mendalam guna meningkatkan perlindungan data dan memastikan *Website* tetap aman dari ancaman eksternal.

III. METODE

Penelitian ini bertujuan untuk menganalisis dan mengidentifikasi tingkat keamanan *Website* XYZ milik Dinas Komunikasi dan Informatika Kabupaten M. Metode ini dilakukan dengan teknik *penetration testing* berbasis *Framework ISSAF* (Information Systems Security Assessment *Framework*). Metode yang digunakan adalah metode *Black Box Testing* yang merupakan pengujian fungsionalitas sistem aplikasi yang bertujuan untuk mengidentifikasi kesalahan pada fungsi - fungsi dan menu aplikasi, termasuk kemungkinan kehilangan menu. Dalam proses pengujian ini, digunakan input data acak dengan tujuan mendapatkan hasil yang akurat dalam menunjukkan potensi kesalahan pada sistem aplikasi. Hal ini bertujuan untuk mengaudit keamanan dari luar dengan mensimulasikan sebagai attacker.

Sistematika Penelitian merupakan gambaran untuk menjelaskan tentang langkah langkah yang akan dilakukan dalam sebuah penelitian. Berikut penjelasannya.

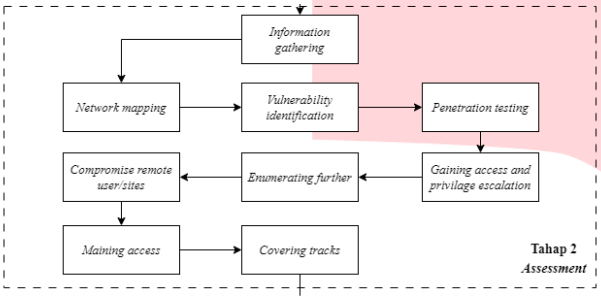


Gambar 2
(Tahap 1 *Planning and Preparation*)

a. Tahap 1. Planning and Preparation

Tahap 1 pada tahapan Planning and Preparation dimulai dari menentukan topik, selanjutnya melakukan studi literatur, serta wawancara persetujuan.

1. Menentukan Topik
Pada tahapan ini, penentuan topik dibantu dengan adanya permasalahan pada objek terkait, lalu menghasilkan sebuah rekomendasi pemberian perbaikan kepada objek.
2. Studi Literatur
Tahap berikutnya yaitu dengan melakukan studi literatur berupa jurnal, *Website* maupun buku. Dengan hal ini peneliti dapat menemukan batasan masalah penelitian.
3. Wawancara Persetujuan
Selanjutnya, dilakukan wawancara persetujuan oleh mas ini selaku pembuat atau developer dari *Website* XYZ untuk mengetahui informasi yang dibutuhkan oleh peneliti.



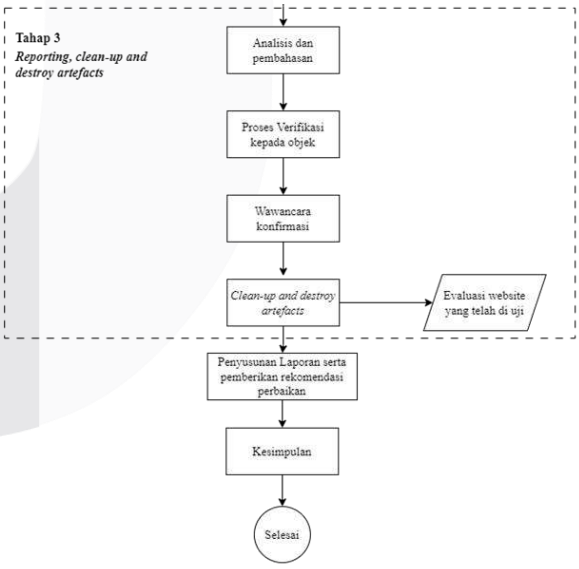
Gambar 3
(Tahap 2 *Assestment*)

1. *Information Gathering*
Pada tahap *Information Gathering* melakukan pengumpulan informasi menggunakan internet untuk menemukan seluruh informasi pada *Website* XYZ. Hal tersebut dapat dilakukan dengan pengumpulan info teknis seperti IP *address,* sistem, dan juga info non teknis dengan menggunakan media pendukung seperti *search engine*. Tahap information gathering ini menggunakan *tools ping, whois,* dan *wappalyzer.*
2. *Network Mapping*
Ketika seluruh informasi target diperoleh, maka dilakukan pendekatan secara teknis, yaitu memperoleh seluruh informasi mengenai proses *Scanning* jaringan yang diperoleh, yaitu *port open*, layanan yang digunakan, dan sistem operasi yang berjalan di server *Website* XYZ.
3. *Vulnerability Identification*
Tahap *Vulnerability Identification* yaitu melakukan Scanning untuk mengidentifikasi titik kerentanan pada *Website* XYZ. Kerentanan dapat diklasifikasikan dalam tingkat tertentu, yaitu: *low, medium, high,* dan *critical.*
4. *Penetration testing*
Pada tahap *Penetration testing* melakukan uji coba serangan untuk medapatkan hak akses ilegal dengan cara menghindari sistem keamanan dan mencoba mengambil akses sejauh mungkin. Tahap *Penetration testing* ini menggunakan teknik serangan *sql injection, XSS cross-site scripting* dan *shell upload exploitation.*
5. *Gaining Access and Privilege Escalation*
Setelah melakukan tahap *Penetration Testing,* maka dilakukan tahap *Gaining Access and Privileges Escalation*. Pada tahap ini mencoba kembali melakukan akses jarak jauh dengan cara mendapatkan hak akses *root* pada *server Website* XYZ. Pada tahap ini melakukan jenis serangan *brute force, exploitation port 80*, dan *PHP shell injection*. Hal in menggunakan *tools metasploit, hydra*, dan manual input pada *form upload.*

6. *Enumerating Further*
Pada tahap *Enumarting Further* melakukan tahapan mencari informasi lebih lanjut dari tahap sebelumnya yang meliputi *sniff traffic* dan *hacking session* untuk mengetahui kerentanan dalam rekam data yang berisikan *username, password* dan pencurian *cookies.*

7. *Compromise Remote User/Sites*
Pada tahap *Compromise Remote User/Sites* yaitu melakukan eksploitasi untuk mendapatkan akses ke dalam *user root* dengan menghubungkan *remote user* dan *enterprise user.*
8. *Maintaining Access*
Pada tahap *Maintaining Access* melakukan pengujian dengan mempertahankan hak akses dengan penanaman *backdoor.* Hal tersebut bertujuan untuk masuk kembali ke sistem dengan mudah tanpa memerlukan metode serangan awal yang rumit.
9. *Covering Tracks*
Tahap terakhir pada *Framework ISSAF* adalah *Covering Tracks* yaitu Tindakan atau strategi yang dilakukan peneliti untuk membersihkan jejak penelitian.

c. Tahap 3. *Reporting, Clean-up and Destroy Artefacts*
Pada tahap terakhir ini adalah laporan, pembersihan serta penghancuran atau memusnahkan data setelah pengujian keamanan selesai dilakukan, berikut penjelasannya:



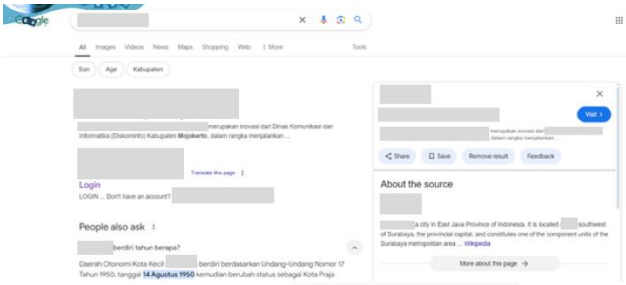
Gambar 4
(Tahap 3 *Reporting, Clean-up and Destroy Artefacts)*

1. Analisis dan Pembahasan
Setelah melakukan wawancara konfirmasi, maka dianalisis kembali hasil dari *Penetration testing* dengan *validator* yang berasal dari pihak eksternal dengan latar belakang pendidikan dan pengalaman di bidang *Cyber Security.*

IV. PENGUMPULAN DAN PENGOLAHAN DATA

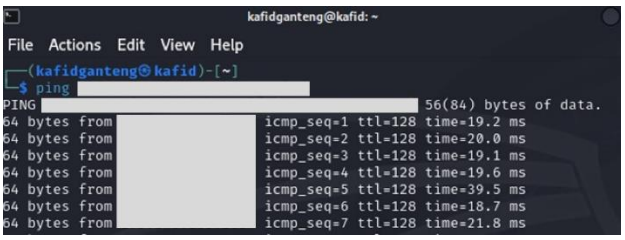
Dalam penelitian ini juga dilakukan pengumpulan informasi yang bertujuan untuk memudahkan peneliti melakukan pengete san keamanan yang didalamnya ada informasi tentang topologi, jaringan, *port,* dengan tujuan menemukan celah yang berpotensi untuk dilakukan pencurian datanya, serta informasi lainnya yang terdapat pada *Website* XYZ.Mkab.go.id atau dengan tahapan *Information Gathering* untuk mengetahui informasi secara utuh yang sedang digunakan pada *Website* XYZ.

Pada tahap ini merupakan langkah pertama dalam pelaksanaan 9 langkah pengujian keamanan. Di tahap ini peneliti melakukan pengumpulan informasi terkait *Website* XYZ. Langkah ini bertujuan untuk mengetahui data, informasi seperti lokasi, tempat, dari *Website* XYZ yang dimana bisa membantu peneliti untuk melanjutkan langkah pengujian keamanan ke tahap selanjutnya. Berikut penjelasannya.



Gambar 5
(Situs *web* XYZ)

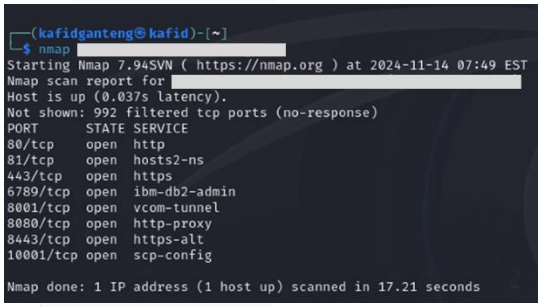
Pada Gambar 5 adalah hasil yang dilakukan dalam pencarian informasi menggunakan mesin pencari atau *search engine* untuk mencari *Website* resmi dari XYZ. Hasil dari search engine tersebut menghasilkan situs XYZ.Mkab.go.id di posisi paling atas, yang diartikan sebagai *Website* utama dari XYZ dengan berisikan informasi utama mengenai layanan yang ada pada *Website* XYZ.



Gambar 6
(Hasil *scan domain* XYZ menggunakan *ping*)

Gambar 6 menjelaskan tentang hasil dari perintah ping XYZ.Mkab.go.id. Dari hasil diatas, peneliti dapat informasi tentang ip dari domain XYZ.Mkab.go.id adalah xxx.xxx.xxx.xxx. Berikut untuk penjelasannya, hasil *ping* waktu *respons* dari *server* adalah sekitar 18-21 ms yang berarti *server* berada pada kondisi responsif dan tersedia. Sedangkan nilai TTL adalah 128 yang berarti jarak hop dalam jaringan antara pengguna dan *server*. Dengan demikian peneliti dapat melanjutkan ke tahap selanjutnya. Kemudian untuk mendapatkan informasi lebih banyak, maka peneliti melakukan *scan* menggunakan *tools whois.*

Tahap setelah *Information Gathering* adalah *Network Mapping,* merupakan tahap pencarian identifikasi dan memvisualisasikan perangkat, koneksi dan hubungan dalam suatu jaringan komputer. Tentunya langkah ini berfungsi untuk memahami struktur, topologi dan aliran data yang berjalan pada *Website* XYZ. Pada tahapan ini peneliti menggunakan *tools nmap*, yang akan mencari jaringan *port* yang sedang berjalan, *host* serta layanan. Dengan bantuan tools nmap diharapkan peneliti bisa lebih mengerti informasi detail tentang titik kerentanan pada *Website* XYZ.



Gambar 7
(Hasil identifikasi *nmap Website* XYZ)

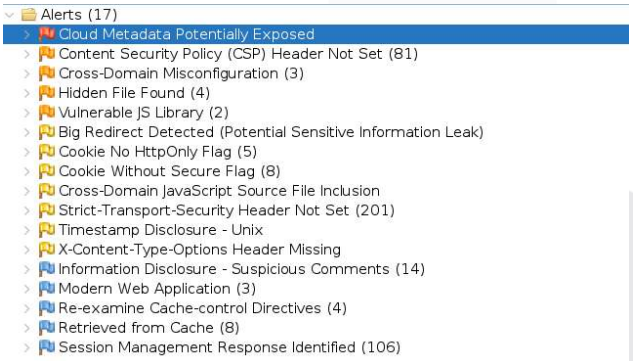
Pada Gambar 7 merupakan hasil dari identifikasi nmap pada *Website* XYZ, hal ini dilakukan supaya ditemukan ip addres *Website* XYZ adalah 103.170.105.253 dan beberapa port terbuka yang sedang menjalankan layanan *Website*. Pemindaian ini juga menemukan protokol komunikasi seperti, *HTTP, HOSTS2-NS, HTTPS, IBM-DB2-ADMIN, VCOM-TUNNEL, HTTP-PROXY, HTTPS-ALT, SCP-CONFIG.*

Kemudian tahap selanjutnya peneliti melakukan scan uji keamanan menggunakan *Secure Socket Layer (SSL)* dan *Transport Layer Security (TLS)* yang digunakan dalam *Website* XYZ dengan memakai tools sslabs.com, sehingga mendapatkan hasil sebagai berikut.

Gambar 8
(Hasil *scan* menggunakan *SSLabs*)

Gambar 8 menunjukan hasil dari *scanning* yang dilakukan pada *Website* XYZ. Dari hasil *scan* tersebut tingkat kerentanan yang dimiliki oleh *server,* secara keseluruhan *Website* XYZ mendapatkan *Overall Rating A* yang menunjukan bahwa konfigurasi *SSL/TLS server* cukup aman. Lalu, sertifikat yang digunakan oleh XYZ mendapatkan nilai yang sangat baik, yang artinya dari sertifikat tersebut *valid,* hal ini juga didukung dengan otoritas yang resmi. Dengan hal ini, sistem dari XYZ dapat dienkripsi dengan baik.

Tahap setelah *Information Gathering* adalah *Vulnerability Identification*. Pada tahap ini akan dilakukan mencari dan menemukan kerentanan yang terdapat dalam *Website* XYZ. Peneliti menggunakan *tools* OWASP ZAP dan NIKTO untuk mencari titik kerentanan. Untuk hasil dari *scanning vulnerability* adalah sebagai berikut.



Gambar 9
(Hasil *scan Website* XYZ dengan OWASP ZAP)

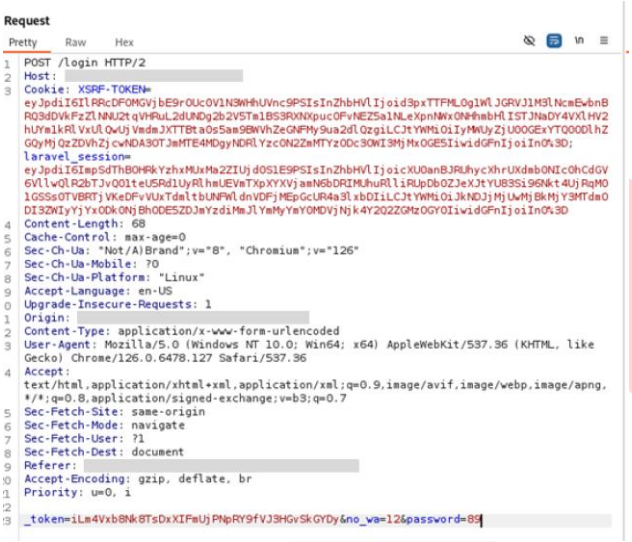
Pada Gambar 9 Menunjukan hasil dari automated scan yang menggunakan tools OWASP ZAP. Hasil menunjukan bahwa pada *Website* XYZ ditemukan titik kerentanan dengan jumlah 17 kerentanan, yang pertama *Cloud Metadata Potentially Exposed* atau metadata yang disimpan di layanan *cloud*, kemudian ada *Content Security Policy (CSP) Header Not Set yang* berarti tidak dikonfigurasi pada suatu situs *web*. *Cross-Domain Misconfiguration* yang terdapat kesalahan dalam konfigurasi lintas domain. Selanjutnya ada *Hidden File Found* atau ada file tersembunyi pada sistem atau *server,* selanjutnya ada *Vulnerable JS Library* yang memiliki kerentanan keamanan pada sisi *javascript*. *Big Redirect Detected (Potential Sensitive Information Leak)* yang terbukti bahwa ada banyak *redirect* dalam aplikasi. *Cookie No HttpOnly Flag* yang berarti *cookie* rentan terhadap serangan *XSS*. *Cookie Without Secure Flag* atau rentan terhadap pencurian di jaringan. *Cross-Domain JavaScript Source File Inclusion* yang berarti potensi masalah tehadap *XSS*. *Strict-Transport-Security Header Not Set* atau *Website* XYZ tidak mengirimkan *header HTTP*. *Timestamp Disclosure – Unix* atau penyerang dapat memanfaatkan sistem atau pola akses. *X-Content-Type-Options Header Missing* atau menebak tipe konten dari file yang diterima serta kerentanan lainnya yang bersifat informasi. Berikut untuk hasil *level* yang didapatkan.

Tahapan selanjutnya adalah *Penetration Testing*, pada tahap ini peneliti melakukan pengetesan keamanan *Website* XYZ dengan menggunakan *tools SQL Injection* dengan menggunakan *command sqlmap* pada *kali linux. SQLMap* adalah alat perangkat lunak yang digunakan untuk mengidentifikasi dan mengatasi kelebihan *eksternal* dalam aplikasi *web*. *SQLmap* adalah pada fitur *login admin* guna mengetahui apakah ada celah kerentanan dari serangan *hacker* atau tidak. Untuk itu peneliti melakukan pengetesan sebagai berikut.

Gambar 10
(Hasil *Sql Injection* pada *Website* XYZ)

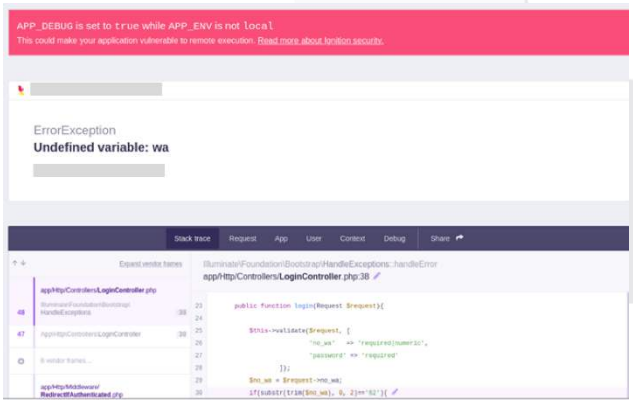
Perlu diketahui bahwa pada Gambar 10 hasil dari pengujian penetrasi pada *Website* XYZ. Pengujian dimulai dengan memasukkan perintah pada *sqlmap* pada *url login admin.* Ditemukan hasil dari pengujian diatas adalah heuristics detected that the target is protected by some kind of WAF/IPS yang berarti bahwa *Website* target telah dilindungi oleh sistem *Web Application Firewall* dan *Intrusion Prevention System*. Untuk perintah *sqlmap* peneliti menggunakan *command sqlmap -r abc.txt –dbs,* pada perintah terdapat file yang bernama abc.txt yang berisikan *request* dari *burp suite* melalui fitur *login admin.*

Kemudian, peneliti melanjutkan pengujian serangan yang menggunakan *Cross-Site Scripting (XSS).* Dalam pengujian ini dilakukan pada halaman *login admin* dengan memasukkan nomor *handphone* dan sandi secara acak. *Burpsuite* digunakan untuk menangkap aliran data dengan pengaturan *proxy* harus di konfigurasi terlebih dulu. Dengan fitur *proxy* peneliti bisa *forward* dari *proxy* ke *repeater* untuk mengirimkan *http* ataupun *https.*



Gambar 11
(*Request payload XSS* pada *Burpsuite*)

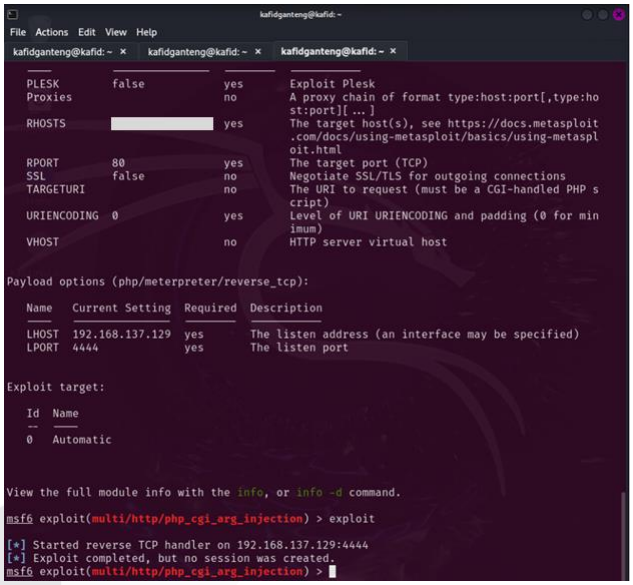
Berdasarkan pada Gambar 11 merupakan *response* dari *request* yang telah dijalankan oleh peneliti, disini *response* menjelaskan tentang *respon* dari *server laravel* yang ada pada *Website* XYZ.



Gambar 12
(*Output error* pada *Laravel*)

Pada hasil yang telah ditampilkan pada Gambar 5. 7 oleh *tools burpsuite,* itu bertuliskan *"APP_DEBUG is set to true while APP_ENV is not local".* Yang dapat dideskripsikan sebagai aplikasi yang berjalan dalam *mode debug,* dan *variabel* dari *APP_ENV* merupakan kesalahan yang tidak diatur ke jaringan lokal. Oleh karena itu, ketika peneliti mencoba menginputkan Nomor *Whatsapp* dan sandi pada halaman *login* XYZ dengan acak, maka halaman yang akan dituju adalah seperti Gambar 12 Dari hasil diatas dapat disimpulkan sebagai kesalahan dalam *file codingan laravel* dari *Website* XYZ.

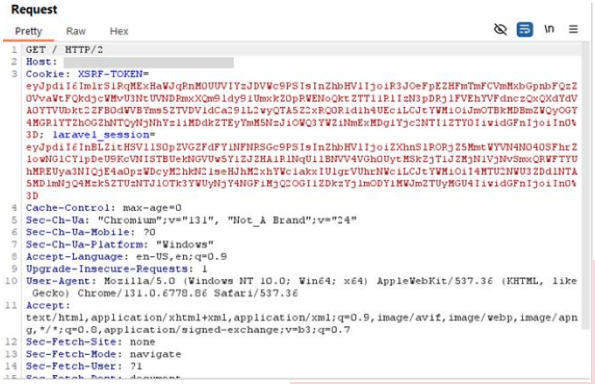
Tahap selanjutnya setelah *Penetration Testing* adalah *Gaining Accsess & Privilege Escalation*, tahap ini merupakan 2 langkah tahapan yang akan melakukan pencarian lebih tentang opsi akses untuk masuk kedalam *Website*. Kemudian peneliti melakukan serangan dengan menggunakan *brute force,* serangan ini menggunakan *tools Metasploit* untuk mencoba seluruh kata sandi untuk mencari akses melalui terminal. Jika dirasa sudah mendapatkan akses, tahap selanjutnya adalah *privilege escalation,* yang akan meningkatkan lagi dalam akses masuk ke dalam *Website*. Langkah ini diharapkan bisa mencari kelemahan dalam sistem *Website* XYZ.



Gambar 12
(*Output error* pada *Laravel*)

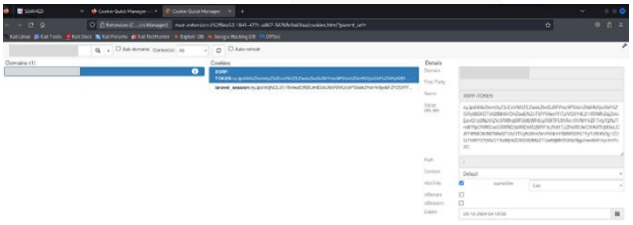
Pada Gambar 12 hasil dari uji *brute force* dengan memakai *tools* dari *Metasploit* adalah ada upaya untuk mendapatkan akses ke *Website* target, namun tugas diatas gagal dilakukan. Pada tahapan ini, peneliti menggunakan *Metasploit* dengan versi 6.4.34-dev dengan *module 'multi/http/php_cgi_arg_injection. Website* target yang diserang adalah *host* 103.170.105.253 atau XYZ.Mkab.go.id melalui *port* 80 atau http. Serangan dilakukan menggunakan kombinasi *password* yang terdapat dalam file 'password.txt'.

Hasil dari *Gaining Access & Privilege Escalation* Gagal mendapatkan akses dikarenakan *port* yang terbuka pada *Website* XYZ telah gagal dilakukan karena kendala masing masing *port* yang berbeda beda. Hal ini menyebabkan keterbatasan penelitian dalam tahapan ini.



Gambar 13
(Hasil *request* dengan *Burpsuite* untuk *cookie*)

Dapat diketahui bahwa peneliti menggunakan *tools burpsuite* berhasil menangkap *cookie* melalui hasil *request login admin* pada *Website* XYZ.



Gambar 14
(Hasil mencari *Cookie*)

Pada Gambar 14 peneliti gagal menyimpan *cookie* untuk melakukan *login* tanpa *inputan kredensial*. Hal ini terjadi karena diblokir oleh *CRSF-TOKEN* yang biasanya digunakan untuk melindungi *Website* target dari serangan *Cross-Site Request Forgery (CSRF).* Setelah itu, ada pesan tertulis bahwa *laravel_session* yang berarti *tools* yang biasa digunakan oleh *laravel* untuk melacak sesi pengguna.

Tahap selanjutnya adalah kompromi terhadap pengguna atau situs jarak jauh. Pada tahap ini, eksploitasi dilakukan untuk mencoba mendapatkan akses ke akun *root* dengan menghubungkan pengguna jarak jauh dengan pengguna enterprise atau jaringan internal pada *Website* XYZ. Namun, upaya ini tidak berhasil karena terdapat kegagalan pada tahapan *gaining access* dan *privilege escalation.* Pada tahapan ini peneliti akan melakukan pengujian dengan mempertahankan hak akses dengan penanaman *backdoor*. Hal tersebut bertujuan untuk masuk kembali ke sistem dengan mudah tanpa memerlukan metode serangan awal yang rumit. Tetapi dalam penelitian ini terkait pengetesan keamanan pada *Website* XYZ tidak dapat dilanjutkan hingga selesai. Tahapan terakhir dari ke 9 langkah pengujian adalah tahapan. *Covering Tracks* atau tahapan yang dilakukan peneliti untuk menghapus langkah langkah jejak aktivitas yang telah dilakukan. Dengan hal ini, peneliti menghapus *entry log*, menghapus folder dan juga file file sisa pengetesan.

V. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan penelitian yang sudah dilaksanakan pada *Website* XYZ dengan menggunakan *Framework* ISSAF dapat disimpulkan bahwa:

1. Proses layanan kerjasama media yang krusial yaitu, pengujian keamanan akun dan autentikasi dengan menggunakan *tools Brute Force Attack* dan pengetesan basis data yang dilakukan dengan *tools Sql Injection*.

2. Kerentanan yang ditemukan dalam *Website* XYZ yaitu, pada kategori *high* ada *Cloud Metadata Potentially Exposed*, karena tingkatan resiko paling tinggi dan terdapat data sensitif dalam *Website*. Pada kategori medium terdapat *Content Security Policy (CSP) Header Not Set, Cross-Domain Misconfiguration, Hidden File Found,* dan *Vulnerable JS Library*, karena ada masalah yang bersifat moderat seperti data sistem yang berpotensi diserang. Untuk kategori *low* terdapat *Big Redirect Detected (Potential Sensitive Information Leak), Cookie No HttpOnly Flag, Cookie Without Secure Flag, Cross-Domain JavaScript Source File Inclusion, Strict-Transport-Security Header Not Set, Timestamp Disclosure – Unix,* dan *X-Content-Type-Options Header Missing*, karena tingkatan paling rendah untuk ancaman penyerangan dan mudah untuk di selesaikan.

3. Rekomendasi perbaikan untuk meningkatkan keamanan *Website* XYZ meliputi, menyembunyikan seluruh informasi yang ada dengan teknik *Obfuscation*, rutin melakukan *update* dan audit keamanan secara berkala, dan menambahkan fitur *firewall* untuk fitur yang diperlukan.

Saran

Selain itu ada saran untuk penelitian selanjutnya agar memperhatikan keamanan pada *Website* XYZ sebagai berikut:

1. Rekomendasi meliputi pencarian *tools* pengganti untuk menggantikan proses yang gagal, seperti menggunakan *framework* OWASP dengan *tools* berbeda dari *ISSAF,* serta melakukan analisis berdasarkan tingkatan risiko dan menentukan prioritas perbaikan sesuai dengan risiko tersebut.

REFERENSI

[1] D. P. Anggraeni, B. P. Zen, and M. Pranata, *"Security analysis on websites using the information system assessment framework (ISSAF) and open web application security version 4 (OWASPv4) using the penetration testing method*," Jurnal Pertahanan, vol. 8, no. 3, pp. 497–506, 2022.

[2] N. P. Bestari, "PDN tumbang diserang hacker, Kominfo beberkan nasib data RI," CNBC Indonesia, Jun. 26, 2024. [Online].Available:https://www.cnbcindonesia.com/tech/20240626155217-37-549536/pdn-tumbang-diserang-hacker-kominfo-beberkan-nasib-data-ri

[3] F. N. Latifah, I. Mawardi, and B. Wardhana, *"Threat of data theft (phishing) amid trends in fintech users during the COVID-19 pandemic (study phishing in Indonesia),"* Perisai: Islamic Banking and Finance Journal, vol. 6, no. 1, pp. 74–86, Apr. 2022, doi: 10.21070/perisai.v6i1.1598.

[4] F. Fachri, "Optimasi keamanan *web server* terhadap serangan *brute-force* menggunakan *penetration testing,"* Jurnal Teknologi Informasi Dan Ilmu Komputer, vol. 10, no. 1, pp. 51–58, 2023.

[5] A. Fajarino, Y. N. Kunang, H. M. Yudha, E. S. Negara, and N. R. Damayanti, "Evaluasi dan peningkatan keamanan pada sistem informasi akademik Universitas XYZ Palembang," J-SAKTI (Jurnal Sains Komputer dan Informatika), vol. 7, no. 2, pp. 991–1005, 2023.

[6] G. Guntoro, L. Costaner, and M. Musfawati, "Analisis keamanan *web server Open Journal System (OJS)* menggunakan metode *ISSAF* dan *OWASP* (studi kasus OJS Universitas Lancang Kuning)," JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika), vol. 5, no. 1, pp. 45–55, 2020.

[7] I. U. Haq, T. A. Khan, and A. Akhunzada, *"A dynamic robust DL-based model for android malware detection," IEEE Access*, vol. 9, pp. 74510–74521, 2021.

[8] F. Heiding, E. Süren, J. Olegård, and R. Lagerström, "*Penetration testing of connected households," Computers & Security,* vol. 126, p. 103067, 2023.

[9] N. Herawati and V. Budiyanto, "Analisis keamanan sebuah domain menggunakan *Open Web Application Security Project (OWASP) Zap,"* Jurnal Teknologi Technoscientia, pp. 27–36, 2023.

[10] F. F. Husna and M. Mustaqim, "Pemanfaatan *electronic banking* bagi anggota di KSPPS BMT Bina Ummat Sejahtera Cabang Tayu," MALIA: *Journal of Islamic Banking and Finance, vol*. 4, no. 2, pp. 148–153, 2020.