ANALISIS KEAMANAN SISTEM INFORMASI PADA WEBSITE E-RAPORT SEKOLAH XYZ MENGGUNAKAN *INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK* (*ISSAF*)

Oleh :

DERY SYAMS AHNAF

1204200143

PROGRAM STUDI STRATA 1 SISTEM INFORMASI

FAKULTAS REKAYASA INDUSTRI

UNIVERSITAS TELKOM

2024

ABSTRAK

Kemajuan TIK telah memberikan kemudahan bagi manusia dalam mengakses dan berbagi informasi. Salah satu contoh dari kemajuan TIK dapat diblihat dari banyaknya situs web online, serta penggunaan media sosial yang semakin meningkat. Merujuk hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2021-2022, pengguna internet di Indonesia mencapai 77,02% dari populasi penduduk Indonesia atau setara 210.026.769 juta pengguna. Angka ini menunjukkan peningkatan sebesar 3,32% dibandingkan dengan tahun 2019-2020 [3].Salah satu bentuk pemanfaatan internet adalah dengan menggunakan website. Website dapat digunakan oleh individu, organisasi, maupun perusahaan untuk berbagai tujuan, salah satu pemanfaatan *website* untuk pendidikan adalah *E-Raport* merupakan aplikasi raport eletronik untuk sekolah, yang memiliki dua jenis *login*, yaitu *login* untuk admin dan *login* untuk guru sekolah. Keamanan sistem informasi aplikasi *e-raport* berbasis website menjadi hal yang penting untuk diperhatikan, mengingat sistem tersebut memuat data peserta didik dan data yang berkaitan dengan proses pembelajaran. Apabila terdapat celah keamanan, maka celah keamanan tersebut dapat dimanfaatkan oleh penyerang untuk melakukan serangan, seperti pencurian data, penyalahgunaan data, dan gangguan layanan. Penelitian ini bertujuan untuk menganalisis keamanan sistem informasi aplikasi berbasis website *e-raportt* sekolah XYZ dengan menggunakan kerangka kerja *Information System Security Assessment Framework* (ISSAF). Berdasarkan hasil pengujian menggunakan framework ISSAF ditemukan beberapa celah keamanan yaitu: 2 celah keamanan medium, 4 celah keamanan low dan 3 celah keamanan informational. Selain itu terdapat banyak port yang terbuka pada website *e raport* yang bisa diekploitasi oleh penyerang. Namun untuk database dan password pana pengujian ini tidak dapat ditembus oleh penguji. Kendati demikian website eraport tergolong secure serta penulis mencantumkan rekomendasi untuk membantu pihak sekolah untuk melakukan perbaikan terhapap website e-raport. Dengan adanya dapat membantu pengelola system sekolah XYZ untuk meningkatkan keamanan sistem tersebut.

Kata Kunci: *Aplikasi Berbasis Website, ISSAF, Keamanan Sistem Informasi, Penetration Testing*

ABSTRACT

The advancement of Information Technology (IT) has provided convenience for humans in accessing and sharing information. One example of IT advancement can be seen in the proliferation of online websites and the increasing use of social media. Referring to the survey results conducted by the Association of Indonesian Internet Service Providers (APJII) in 2021-2022, internet users in Indonesia reached 77.02% of the population or approximately 210,026,769 million users. This figure represents an increase of 3.32% compared to 2019-2020 [3]. One form of internet utilization is through the use of websites. Websites can be used by individuals, organizations, and companies for various purposes. One such application in education is E-Raport, an electronic report application for schools, which has two types of logins: one for administrators and one for school teachers. The security of the information system of the E-Raport website-based application is crucial given that it contains student data and information related to the learning process. Any security vulnerabilities could potentially be exploited by attackers for data theft, misuse, or service disruption. This study aims to analyze the security of the information system of the XYZ school's E-Raport website-based application using the Information System Security Assessment Framework (ISSAF). Based on testing using the ISSAF framework, several security vulnerabilities were identified: 2 medium-level vulnerabilities, 4 low-level vulnerabilities, and 3 informational vulnerabilities. Additionally, there are many open ports on the E-Raport website that could be exploited by attackers. However, during testing, the database and passwords were not penetrated by the tester. Nevertheless, the E-Raport website is considered secure, and the author provides recommendations to assist the school in improving the E-Raport website. This could help the management of XYZ school system to enhance the security of their system.

Keywords: Information System Security, ISSAF, Penetration Test, Website Based Application

LEMBAR PENGESAHAN

Tugas Akhir dengan judul :

ANALISIS KEAMANAN SISTEM INFORMASI PADA WEBSITE E-RAPORT SEKOLAH XYZ MENGGUNAKAN *INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF)*

Telah disetujui dan disahkan pada Sidang Tugas Akhir

Program Studi Strata 1 Sistem Informasi

Fakultas Rekayasa Industri Universitas Telkom

Oleh :

Dery Syams Ahnaf

1204200143

Surabaya, 29 Juli 2024

Disetujui oleh,

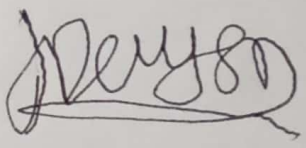
Pembimbing 1,	Pembimbing 2,
Kharisma Monika Dian Pertiwi, S.Kom., M.Kom	Adzanil Rachmadhi Putra, S.Kom., M.Kom.
20950044	22940040

LEMBAR PERNYATAAN ORISINALITAS

Nama	:	Dery Syams Ahnaf
NIM	:	1204200143
Alamat	:	Jambangan Sawah III/E no.11 Surabaya
No.Tlp	:	085784362341

Menyatakan bahwa Tugas Akhir ini merupakan karya orisinal saya sendiri. Atas pernyataan ini, saya siap menanggung risiko atau sanksi yang dijatuhkan kepada saya apabila kemudian ditemukan adanya pelanggaran terhadap kejujuran akademik atau etika keilmuan dalam karya ini, atau ditemukan bukti yang menunjukkan ketidakaslian karya ini.

Surabaya, 29 Juli 2024



Dery Syams Ahnaf

KATA PENGANTAR

Bismillahirrahmanirrahim

Dengan meneyebut nama Allah Subhanahu Wa Ta'ala Yang Maha Pengasih lagi Maha Penyayang. Puji syukur atas pertolongan-Nya penulis dapat menyelesaikan Tugas Akhir ini yang berjudul "ANALISIS KEAMANAN SISTEM INFORMASI PADA WEBSITE E-RAPORT SEKOLAH XYZ MENGGUNAKAN *INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK* (ISSAF)". Sebelum mengerjakan tugas akhir peneliti sempat kebingungan untuk memilih topik dan judul yang akan digunakan dalam penelitian. Sewaktu penulis berada dalam kelas system keamanan informasi yang dibawakan oleh Bapak Muhammad Nasrullah S.Kom., M.Kom, beliau mengatakan bahwasanya topik tentang keamanan system informasi merupakan topik yang "seksi" dan kakak tingkat kami yang mengambil topik tersebut mendapatkan nilai A dan yang terendah adalah AB. Berdasarkan alasan tersebut peneliti termotivasi dan seperti mendapatkan pencerahan untuk memilih topik tentang system keamanan informasi. Selain alasan yang telah disebutkan sebelumnya penulis mendapatkan referensi yang bersifat tekhnis untuk penyusunan tugas akhir ini. Dimana referensi tekhnis tersebut berasal dari kakak tingkat penulis yaitu saudara Mochammad Evan Wiratama S.Kom. Kemudian dalam proses penyelesaian tugas akhir ini penulis diberikan orang – orang yang selalu baik dalam memberikan doa, dukungan, kritik, dan masukan saran sehingga penelitian ini dapat berproses dengan lancar meskipun banyak sekali penulis melewati rintangan dan terkadang merasa berputus asa. Kemudian secara khusus penulis mengucapkan *jazakumullah khairan* dan terima kasih dari hati yang paling dalam kepada yang terhormat:

1. Keluarga khususnya kedua orang tua dan saudara yang selalu memberikan doa, dukungan, nasihat, serta motivasi untuk menyelesaikan Tugas Akhir ini,
2. Bapak Prof. Dr. Adiwijaya., selaku Rektor Telkom University,
3. Bapak Prof. Dr. Irfan Darmawan, S.T., M.T., selaku Dekan Fakultas Rekayasa Industri Telkom University,
4. Ibu Ully Asfari, S.Kom., M.Kom., selaku Ketua Program Studi Sistem Informasi Telkom University Surabaya,
5. Bapak Noerma Pudji Istyanto, S.Kom., M.Kom, selaku dosen wali saya di Program Studi Sistem Informasi Telkom University Surabaya,
6. Ibu Kharisma Monika Dian Pertiwi, S.Kom., M.Kom, selaku dosen pembimbing I yang telah memberi ilmu dan dengan sabar memberikan bimbingan, arahan, masukan, dan motivasi dalam pengerjaan Tugas Akhir ini,
7. Bapak Adzanil Rachmadhi Putra, S. Kom., M. Kom selaku dosen pembimbing II yang telah memberi ilmu dan dengan sabar memberikan bimbingan, arahan, masukan, dan motivasi dalam pengerjaan Tugas Akhir ini,
8. Kepala sekolah XYZ yang telah memberikan saya izin untuk melakukan penelitian analisa keamanan sistem website PPDB dalam Tugas Akhir ini,
9. Para karyawan lembaga sekolah XYZ yang bersedia diwawancarai oleh saya untuk mendapatkan data dalam penelitian Tugas Akhir ini,
10. Bapak Muhammad Nasrullah S.Kom., M.Kom. yang telah memberikan gambaran umum mengenai topik keamanan sistem informasi dan yang telah menjadi dosen penguji 1 saya

11. Mochamad Nizar Palefi Ma’ady, S.Kom., M.Kom., M.IM yang telah menjadi dosen penguji 2 saya
12. Saudara Mochammad Evan Wiratama S.Kom. yang telah memberikan referensi yang bersifat tekhnis untuk penyusunan tugas akhir ini yang mana digunakan untuk menusun bab 4 dan bab 5
13. Rekan – rekan yang bersama sama berjuang menyelesaikan Tugas Akhir dan selalu memberikan saya dukungan serta motivasi selama penyelesaian Tugas Akhir ini.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I PENDAHULUAN

I.1 Latar Belakang

Kemajuan Teknologi Informasi dan Komunikasi, atau selanjutnya bisa disebut dengan TIK telah memberikan kemudahan bagi manusia dalam mengakses dan berbagi informasi. Salah satu contoh dari kemajuan TIK dapat dilihat dari banyaknya situs *web online* serta penggunaan media sosial yang semakin meningkat. Kemudahan yang ditawarkan oleh kemajuan TIK tentunya memiliki dampak positif bagi berbagai bidang, termasuk bidang pendidikan, bisnis, dan pemerintahan. Namun, di sisi lain, kemajuan TIK juga menimbulkan berbagai risiko bahaya, seperti ancaman digital (M. Arief, 2021). Ancaman digital dapat berdampak pada sistem secara keseluruhan, khususnya website yang dapat diakses secara *online.*

Internet merupakan salah satu bentuk kemajuan dalam bidang TIK. Perkembangan internet di Indonesia yang semakin pesat telah mengubah gaya hidup masyarakat. Didalam kehidupan masyarakat Indonesia, internet telah menjadi bagian tak terpisahkan, mulai dari aktivitas pendidikan, bisnis, hingga hiburan. Merujuk hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2021-2022, pengguna internet di Indonesia mencapai 77,02% dari populasi penduduk Indonesia atau setara 210.026.769 juta pengguna. Angka ini menunjukkan peningkatan sebesar 3,32% dibandingkan dengan tahun 2019-2020 (APJII, 2022).

Salah satu bentuk pemanfaatan internet adalah dengan menggunakan *website*. *Website* adalah sebuah situs web yang menyediakan informasi kepada penggunanya. *Website* dapat digunakan oleh individu, organisasi, maupun perusahaan untuk berbagai tujuan, seperti untuk mempromosikan produk atau jasa, untuk memberikan informasi, atau untuk keperluan pendidikan. Peningkatan penggunaan *website* juga telah membawa dampak negatif, salah satunya adalah meningkatnya risiko keamanan informasi. *Website* dapat menjadi target serangan keamanan informasi, seperti peretasan, *malware*, dan *denial-of-service*. Serangan keamanan informasi tersebut dapat menyebabkan pencurian data, kerusakan sistem, atau bahkan penyebaran informasi yang tidak benar. Serangan *malware* adalah

salah satu jenis serangan keamanan informasi yang paling sering terjadi pada *website*. *Malware* adalah perangkat lunak berbahaya yang dapat digunakan untuk berbagai tujuan, seperti mencuri data, merusak sistem, atau bahkan mengendalikan komputer korban. Berdasarkan penelitian yang dilakukan oleh Dirgahayu et al. (2015), jenis serangan yang paling lazim terhadap *website* adalah serangan *malware*. Serangan *malware* tersebut dapat dilakukan dengan berbagai cara, seperti menggunakan celah keamanan pada salah satu *website*, atau dengan memanfaatkan kesalahan pengguna(Dirgahayu, 2015).

Berdasarkan informasi mengenai serangan keamanan sistem informasi pada website dan dampak yang diakibatkan oleh serangan keamanan sistem informasi pada website, maka diperlukan mitigasi celah keamanan untuk mengurangi risiko keamanan dalam sistem komputer atau jaringan. Hal ini diperkuat dengan Badan Siber dan Sandi Negera (BSSN) yang telah mempublikasikan Lanskap keamanan siber Indonesia 2023. Didalam lanskap tersebut disebutkan selama tahun 2023, total jumlah anomali trafik di Indonesia mencapai 403.990.813, dengan *Generic Trojan RAT* sebagai jenis trafik anomali yang paling dominan, menunjukkan aktivitas komunikasi backdoor ke domain malicious yang diduga sebagai command and control server milik threat actor. Selain itu, tercatat 4.001.905 aktivitas *Advanced Persistent Threat* (APT) dan 1.011.209 aktivitas ransomware. BSSN telah mengirimkan 1.762 notifikasi indikasi insiden kepada stakeholder, dengan jenis notifikasi terbanyak adalah terkait Anomali Trafik. Berdasarkan analisis BSSN, beberapa ancaman siber diprediksi akan muncul pada tahun 2024, termasuk *Web Defacement, Ransomware, Cyber Threats Based Artificial Intelligence (AI), Internet of Things (IoT) Attack, Advanced Persistent Threat (APT), Phishing, dan Distributed Denial of Service (DDoS)* (NEGARA, B. S. (2023)).

Mitigasi celah keamanan melibatkan serangkaian langkah untuk mengurangi risiko keamanan dalam sistem komputer atau jaringan. Langkah-langkahnya meliputi pembaruan perangkat lunak secara teratur, pengelolaan rentang dan izin, pengelolaan keamanan jaringan, pengujian keamanan rutin, penggunaan enkripsi data, pendidikan pengguna tentang keamanan informasi, *monitoring* dan respons keamanan yang cepat, kebijakan keamanan yang jelas, manajemen risiko terpadu, dan pemantauan keamanan secara proaktif. Untuk menganalisis keamanan

informasi terdapat banyak *framework* salah satunya adalah *Information System Security Assessment Framework* (ISSAF). *Information System Security Assessment Framework* (ISSAF) muncul sebagai suatu kerangka kerja yang kritis dalam melakukan *penetration testing* (O. S. S. I. Group, 2022).*Penetration testing* adalah metode yang digunakan untuk menguji keamanan sistem dengan mensimulasikan serangan dari pihak luar (R. Munir, 2019). ISSAF memberikan panduan yang terstruktur dan intuitif melalui serangkaian langkah-langkah kompleks, membantu organisasi untuk menjaga keutuhan dan kerahasiaan informasi mereka.

Sejak didirikannya tahun 2011, sekolah xyz mempunyai dua Kompetensi Keahlian yaitu: Multimedia dan Teknik Kendaraan Ringan. Dalam proses penyelenggaraan kegiaatan belajar dan mengajar sekolah xyz memiliki salah satu layanan yaitu E Repor. *E-Raport* adalah aplikasi raport eletronik untuk sekolah, yang memiliki dua jenis *login*, yaitu *login* untuk admin dan *login* untuk guru sekolah. Dalam layanannya sekolah XYZ mengguanakan *e-raport* untuk menunjang proses kegiatan belajar mengajar memiliki produk layanan *website learning management sistem* yang digunakan sebagai sarana untuk belajar bagi peserta didik. Apabila *user login* sebagai guru, *user* bisa mengedit nilai, merubah password. Namun apabila *user login* sebagai admin maka *user* bisa melakukan sinkronisasi (mengambil data dapodik dan mengirim data *e-raport),* referensi (melihat guru dan tenaga pendidik), mengatur hak akses, profil (mengubah email dan kata sandi) dan menu yang lain.

Berdasarkan uraian pada paragraph 4 yang membahas tentang pandangan dan informasi terkait situasi keamanan ruang siber di Indonesia sepanjang tahun 2023 ditambah dengan apabila kita melihat peristiwa kemarin pada bulan juli terdapat serangan ransomware pada pusat data nasional(PDN). Salah satu dampak dari serangan tersebut adalah tidak bisa diaksesnya layanan pada domain Kementerian, Pendidikan, Kebudayaan, Riset dan Teknologi (Kemendikbud Ristek), yang dimana Kemendikbud Ristek merupakan pengembang dari aplikasi *eraport*. Sesungguhnya keamanan sistem informasi aplikasi *e-raport* berbasis website menjadi hal yang penting untuk diperhatikan, mengingat sistem tersebut memuat data peserta didik dan data yang berkaitan dengan proses pembelajaran. Apabila terdapat celah

keamanan, maka celah keamanan tersebut dapat dimanfaatkan oleh penyerang untuk melakukan serangan, seperti pencurian data, penyalahgunaan data, dan gangguan layanan. Website *e-raport* berisi banyak data sensitif berkaitan dengan data siswa, data tentang kegiatan belajar mengajar dan lain-lain. Jika website kebobolan adalah penyerang dapat melakukan tindakan yang ilegal, seperti pencurian data, penyalahgunaan data, dan gangguan layanan Berdasarkan uraian permasalahan diatas penelitian ini bertujuan untuk menganalisis keamanan sistem informasi aplikasi website *e-raport* sekolah XYZ dengan menggunakan pendekatan *Information System Security Assessment Framework* (ISSAF). Meskipun sebelumnya belum pernah terjadi insisden pada celah keamanan pada sistem e-raport sekolah xyz, akan tetapi dengan adanya penelitian dapat membantu pengelola sistem *eraport* sekolah XYZ untuk meningkatkan keamanan sistem tersebut. Serta dengan adanya penelitian ini dapat dijadikan landasan awal untuk menilai keamanan sistem informasi *eraport* sekolah xyz. Selain itu menjadi langkah pencegahan untuk mengurangi celah keamanan sistem informasi *eraport* sekolah xyz.

I.2 Rumusan Masalah

Berdasarkan latar belakang penelitian yang ditulis pada sub-bab 1.1 diatas, maka terdapat rumusan masalah dalam penelitian sebagai berikut:

1. Bagaimana penerapan ISSAF dalam pengujian keamanan sistem informasi pada website *e-raport* sekolah XYZ?
2. Bagaimana hasil analisis keamanan sistem informasi pada website website *e-raport* sekolah XYZ berdasarkan ISSAF?
3. Bagaimana rekomendasi yang sesuai untuk meningkatkan keamanan website website *e-raport* sekolah XYZ berdasarkan hasil pengujian berdasarkan ISSAF?

I.3 Tujuan dan Manfaat

Berdasarkan rumusan masalah penelitian yang ditulis pada sub-bab I.2 diatas, maka terdapat tujuan dalam penelitian sebagai berikut:

1. Mengetahui penerapan *Information System Security Assessment Framework* (ISSAF) sebagai metode penilaian keamanan sistem informasi pada website E-Raport sekolah XYZ.

2. Mengetahui hasil analisis celah keamanan secara mendalam keadaan keamanan sistem informasi pada website website E-Raport sekolah XYZ.
3. Memberikan rekomendasi yang sesuai untuk meningkatkan keamanan system Informasi website *e-raport* sekolah XYZ berdasarkan hasil pengujian berdasarkan ISSAF.

Serta terdapat manfaat dalam penelitian ini yaitu:

1. Memberikan rekomendasi konkret untuk meningkatkan keamanan sistem informasi pada website E - Raport sekolah xyz berdasarkan hasil analisis kondisi saat ini.
2. Memberikan wawasan tentang sejauh mana ISSAF dapat digunakan secara efektif untuk mengevaluasi keamanan sistem informasi.
3. Menambah literatur kepada pihak sekolah dalam bidang keamanan sistem informasi, terutama terkait penerapan ISSAF dan evaluasi keamanan pada website E - Raport.
4. Menyediakan dasar bagi penelitian selanjutnya terkait peningkatan keamanan sistem informasi pada lembaga serupa atau pengembangan metode evaluasi keamanan lainnya.

I.4 Batasan Masalah

Berdasarkan latar belakang yang telah dipaparkan di atas, maka terdapat Batasan masalah penelitian sebagai berikut:

1. Melakukan uji keamanan sistem informasi website E - Raport sekolah XYZ berdasarkan *framework* ISSAF.
2. Metode *penetration testing* menggunaka cara *black box testing.*
3. Berdasarkan pertemuan pertama untuk memberikan surat izin, penelitian pihak sekolah memeberikan izin secara lisan agar pengujian dilakukan pada server dummy dan tidak boleh pada server utama dikarenakan akan mengganggu layanan yang dimiliki oleh sekolah
4. Menggunakan server dummy sebagai sarana untuk melakukan uji keamanan sistem informasi website E – Raport sekolah XYZ.

5. Menggunakan layanan *remote desktop* bulanan sebagai sever dummy, akibatnya setiap bulan Alamat ip selalu berganti

6. Berdasarkan pakta integritas sekolah, akses yang diberikan oleh pihak sekolah hanyalah akses untuk guru dan tidak diberikan akses *username* dan *password admin*.

I.5 Metodologi Penelitian

Pendekatan yang akan digunakan dalam penelitian ini adalah *framework*. *Information System Security Assessment Framework* (ISSAF). Pendekatan ini dipilih karena penelitian akan lebih berfokus pada pemahaman mendalam terhadap keamanan sistem informasi pada website website *e-raport* sekolah XYZ dan implementasi *Framework Information System Security Assessment* (ISSAF). Pendekatan ini dipilih karena penelitian akan lebih berfokus pada pemahaman mendalam terhadap keamanan sistem informasi pada website website *e-raport* sekolah XYZ dan implementasi *Information System Security Assessment Framework* (ISSAF).

Jenis data yang akan dikumpulkan melibatkan data primer dan sekunder. Data primer akan diperoleh melalui wawancara dengan pihak terkait, seperti administrator sistem informasi dan pengguna website. Data sekunder akan diperoleh dari dokumen-dokumen terkait keamanan sistem informasi dan hasil audit keamanan sebelumnya.

BAB II TINJAUAN PUSTAKA

II.1 Penelitian Terdahulu

Penelitian terdahulu memungkinkan peneliti untuk membandingkan temuan masa lalu dengan penelitian yang sedang dilakukan. Selain itu penelitian terdahulu memperluas dan memperdalam berbagai teori yang akan digunakan dalam penelitian. Dengan adanya penelitian terdahulu dapat memperkuat teori dan menjadi kaidah teknis untuk melakukan pengujian dalam penelitian ini. Berikut ini adalah beberapa penelitian terdahulu:

Tabel 2.1 Penelitian Terdahulu

Penelitian 1	
Judul	Analisis Keamanan Web Server *Open Journal System* (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning) (M. Guntoro, 2020)
Penulis	Guntoro, Loneli Costaner, dan Musfawati.
Tahun	2020
Metode	Menggunakan metode ISSAF dan OWASP
Hasil Penelitian	sistem OJS Universitas Lancang tergolong aman, karena tidak mampu untuk ditembus. Walaupun OJS Universitas Lancang Kuning tergolong aman, serangan bisa saja terjadi dari dalam institusi.
Perbedaan	Pada penelitian sebelumnya menggunakan metode ISSAF DAN OWASP sedangkan penelitian saat ini lebih spesifik menggunakan metode ISSAF.

Berbeda dengan penelitian 1 di atas penelitian ini lebih memfokuskan pada penerapan metode ISSAF saja menunjukkan spesifikasinya yang lebih terarah dalam mengevaluasi keamanan sistem informasi pada website *e-raport* sekolah XYZ. Perbandingan ini dapat memberikan wawasan tambahan terkait efektivitas

metode ISSAF secara tunggal dibandingkan dengan penggunaan bersamaan dengan OWASP, serta relevansinya dalam konteks keamanan sistem informasi pada lembaga pendidikan.

Penelitian 2	
Judul	Analisis Keamanan Website Menggunakan Information System Security Asessment Framework (ISSAF) (Herman, 2023)
Penulis	Herman, Imam Riadi, Yudi Kurniawan, Irhash Ainur Rafiq
Tahun	2023
Metode	*Information Systems Security Assessment Framework* (ISSAF).
Hasil Penelitian	website yang di uji masih memiliki beberapa kerentanan seperti XSS, SQL *Injection*, CSRF Token not set, dan yang lainnya. Hasil akurasi yang di dapatkan menggunakan *subgraph vega* adalah sebesar 100% untuk kerentanan *Cross Site Scrpting*, dan 77% untuk SQL *Injection.*
Perbedaan	Perbedaan penelitian saat ini dengan penelitian terdahulu adalah pada objek penelitiannya. Penelitian saat ini berfokus pada analisis keamanan website website *e-raport* sekolah XYZ sedangkan penelitian terdahulu berfokus pada analisis keamanan website secara umum.

Penelitian 2 di atas bertujuan untuk menganalisis keamanan sebuah website dengan fokus pada website pembelajaran Yayasan HSI Abdullah Roy. Pada penelitin saat ini lebih terperinci sehingga penelitian ini memberikan kontribusi yang lebih terarah dan relevan terhadap keamanan sistem informasi pada konteks lembaga pendidikan tersebut.

Penelitian 3	
Judul	Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ. (Wardhana, 2021)
Penulis	Wardhana, Andhika Wisnu, and Henki Bayu Seta
Tahun	2021
Metode	Menggunakan metode ISSAF
Hasil Penelitian	ditemukan beberapa kerentanan yakni, *Bruteforce Attack, Cross-Site Request Forgery (CSRF) Attack, Session Hijacking* melalui Cookie, maupun IDOR (*Insecure Direct Object Reference*). Hasil report dan pemberian rekomendasi akan diberikan kepada pihak administrator IT Universitas XYZ
Perbedaan	Objek penelitian saat ini adalah website website *e-raport* sekolah XYZ, sedangkan objek penelitian terdahulu adalah website pembelajaran Universitas XYZ.

Penelitian 3 diatas bertujuan untuk menganalisis keamanan sistem pembelajaran online pada website Universitas XYZ. Hasil dari penelitian akan disampaikan kepada pihak administrator IT Universitas XYZ untuk memperbaiki dan memperkuat sistem keamanan mereka.

Penelitian 4	
Judul	Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test dan ISSAF. (Silmina, 2022)
Penulis	Silmina, Esi Putri, dan Rovalia Adhella Attya Amanda
Tahun	2022
Metode	ISSAF
Hasil Penelitian	Hasil Penelitian menunjukkan bahwa Sistem Informasi Sekolah MTsN 8 Bantul aman dari celah keamanan.
Perbedaan	Metode penelitian saat ini menggunakan ISSAF, sedangkan metode penelitian terdahulu menggunakan ISSAF dan *penetration testing*.

Penelitian sebelumnya bertujuan untuk menganalisis keamanan jaringan sistem informasi di Sekolah MTsN 8 Bantul. Penelitian ini menggunakan metode *Information System Security Assessment Framework* (ISSAF). Dengan demikian, penelitian ini memberikan keyakinan bahwa keamanan jaringan sistem informasi sekolah tersebut dapat diandalkan. Perbandingan ini menunjukkan variasi dalam pendekatan analisis keamanan jaringan sistem informasi sekolah, dan dapat memberikan wawasan tambahan tentang efektivitas metode ISSAF secara tunggal dibandingkan dengan penggunaan bersamaan dengan penetration testing.

Penelitian 5	
Judul	Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. (Suta Sanjaya, 2020)
Penulis	I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, Dewa Made Sri Arsa
Tahun	2020
Metode	*penetration testing* dengan Framework ISSAF
Hasil Penelitian	diperoleh 18 celah keamanan yang terdapat pada website Lembaga X. Pemberian rekomendasi diberikan untuk meningkatkan keamanan website Lembaga X.
Perbedaan	Obyek penelitian saat ini adalah website website *e-raport* sekolah XYZ, sedangkan obyek penelitian terdahulu adalah website lembaga X.

Penelitian sebelumnya bertujuan untuk mengevaluasi keamanan website dari Lembaga X menggunakan metode *penetration testing* dengan metode ISSAF. Hasilnya menunjukkan bahwa terdapat 18 celah pada website Lembaga X. Oleh karena itu, penelitian ini memberikan pemahaman mendalam tentang kerentanan yang ada pada website tersebut. Selanjutnya, rekomendasi diberikan untuk meningkatkan tingkat keamanan website Lembaga X. Perbandingan ini memberikan wawasan tentang variasi dalam evaluasi keamanan website di berbagai konteks lembaga dan dapat menjadi dasar untuk menyusun rekomendasi dan tindakan yang lebih spesifik terkait keamanan website pembelajaran.

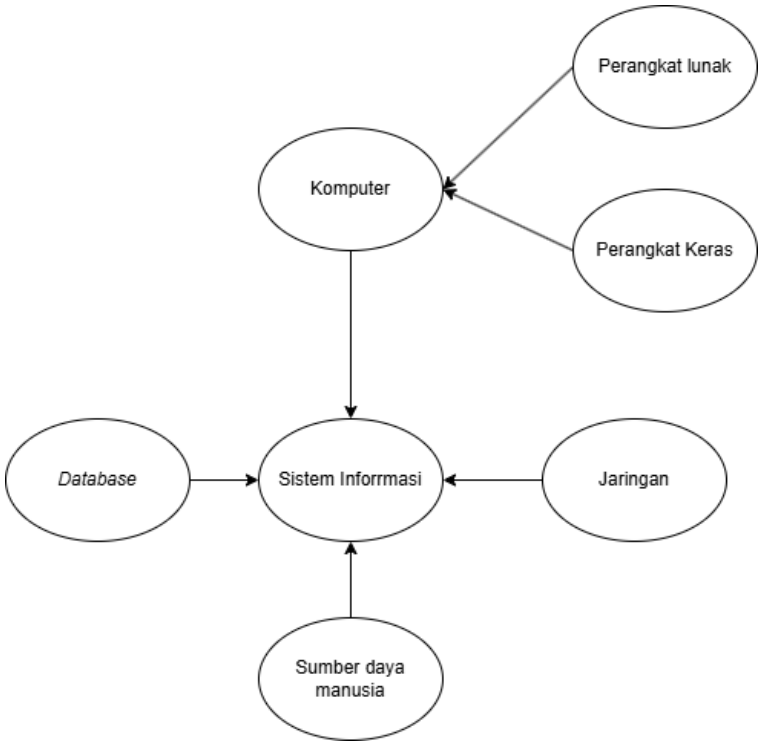
Penelitian 6	
Judul	Analisis Keamanan Sistem Informasi Akademik Berbasis *Web* Menggunakan *Framework* ISSAF (Rusydi Umar, et al, 2023)
Penulis	Rusydi Umar, Imam Riadi, Muhammad Ihya Aulia Elfatiha
Tahun	202
Metode	Framework ISSAF
Hasil Penelitian	ais.ibm.ac.id dipandang kurang aman dari serangan *Brute-force Attack* dengan nilai 7.8, kemudian pada CSRF *Attack (Cross-Site Request Forgery)* dengan nilai 7.6, *Session Hijacking* melalui *Cookies* dengan nilai 9.0, dan *Insecure Direct Object References* (IDOR) dengan nilai 6.8.
Perbedaan	Obyek penelitian saat ini adalah website website *e-raport* sekolah XYZ, sedangkan obyek penelitian terdahulu adalah website ais.ibm.ac.id.

Penelitian sebelumnya bertujuan untuk menganalisis keamanan website dari Institut Bisnis Muhammadiyah Bekasi (IBM Bekasi). Berbeda dengan penelitian 6 di atas penelitian ini lebih memfokuskan pada penerapan metode ISSAF saja menunjukkan spesifikasinya yang lebih terarah dalam mengevaluasi keamanan sistem informasi pada website *e-raport* sekolah XYZ.

Kseimpulannya adalah penelitian terdahulu memiliki fokus yang beragam, mulai dari analisis keamanan web server, sistem pembelajaran online, hingga jaringan sistem informasi sekolah. Metode yang digunakan melibatkan ISSAF, OWASP, dan kombinasi dengan *penetration testing*. Hasil penelitian menunjukkan variasi, dari keamanan yang cukup baik hingga ditemukan celah keamanan yang perlu diperbaiki. Kesimpulan ini mengindikasikan kompleksitas dan kebutuhan untuk pendekatan yang holistik dalam memastikan keamanan sistem informasi.

II.2 Dasar Teori

II.2.1 Sistem Informasi



Gambar 2.1 *Compenent* Sistem Informasi (geeksforgeeks.org. 2024.)

Sistem yang terdiri dari berbagai elemen seperti orang, prosedur, data, perangkat lunak, dan perangkat keras yang bekerja bersama-sama untuk menyediakan informasi yang digunakan sebagai pendukung dalam suatu organisasi merupakan pengertian dari sistem informasi. Sistem informasi dapat digunakan dalam berbagai konteks, seperti manajemen sekolah, rekomendasi pekerjaan untuk alumni, manajemen grosir, dan audit sistem [2].

II.2.2 Keamanan Sistem Informasi

Gambar 2.2 Keaman Sistem Informasi (learn.microsoft.com.2024)

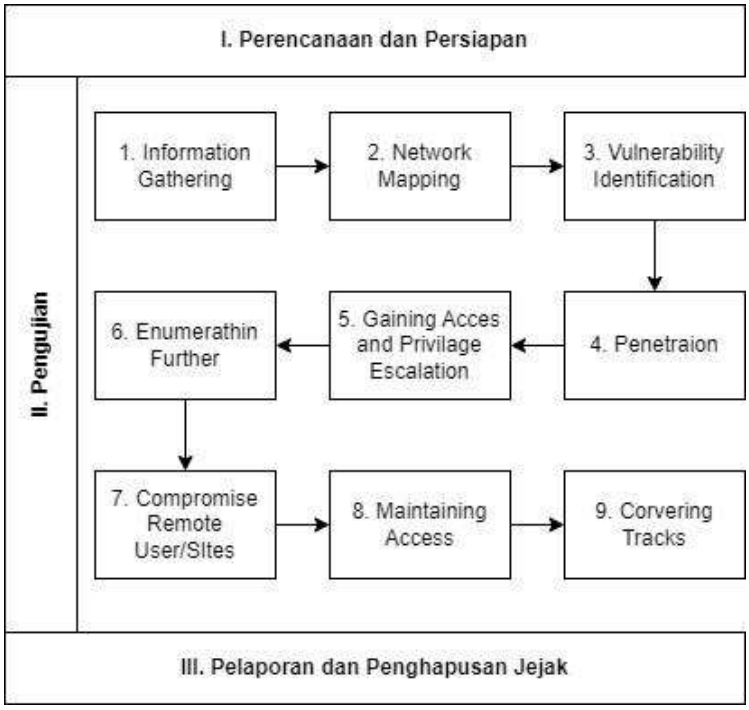
Keamanan sistem informasi berfungsi untuk melindungi sistem informasi dari berbagai ancaman, seperti serangan, kerusakan, dan penyalahgunaan. Keamanan sistem informasi meliputi tiga aspek utama, yaitu kerahasiaan, integritas, dan ketersediaan. Kerahasiaan adalah kemampuan untuk menjaga informasi dari akses yang tidak sah. Integritas adalah kemampuan untuk menjaga informasi agar tetap akurat dan utuh. Ketersediaan adalah kemampuan untuk memastikan bahwa informasi dapat diakses oleh pengguna yang berwenang ketika dibutuhkan. Sumber ancaman keamanan sistem informasi berasal dari berbagai hal, bisa berasal dari dalam atau bisa berasal dari luar. Ancaman dari dalam organisasi dapat berupa kesalahan manusia, kelalaian, atau kesengajaan. Ancaman dari luar organisasi dapat berupa serangan dari hacker, malware, atau bencana alam. Untuk melindungi sistem informasi dari berbagai ancaman, diperlukan penerapan pengendalian keamanan informasi. Pengendalian keamanan informasi dapat berupa pengendalian teknis, pengendalian administratif, dan pengendalian fisik [2].

II.2.3 SQL *Injection* menggunakan *SQLMap*

SQL *injection* menggunakan *sqlmap* adalah teknik serangan keamanan yang dilakukan dengan memanfaatkan celah keamanan pada aplikasi *website* menggunakan program sqlmap. Sqlmap adalah alat sumber terbuka yang digunakan

untuk pengujian penetrasi situs *website* dengan fokus pada serangan injeksi SQL. sqlmap dapat melakukan serangan injeksi SQL dengan secara otomatis menemukan dan mengeksploitasi lubang keamanan di aplikasi web. Beberapa fitur sqlmap termasuk kemampuan untuk mengambil data dari *database*, memperbarui tabel, dan bahkan membuka *shell* pada *host* jarak jauh jika semua persyaratan terpenuhi. sqlmap memiliki banyak fitur dan merupakan alat yang sangat berguna untuk pengujian keamanan dan menemukan kerentanan dalam aplikasi *website*

II.2.4 *ISSAF (Information System Security Assessment Framework)*



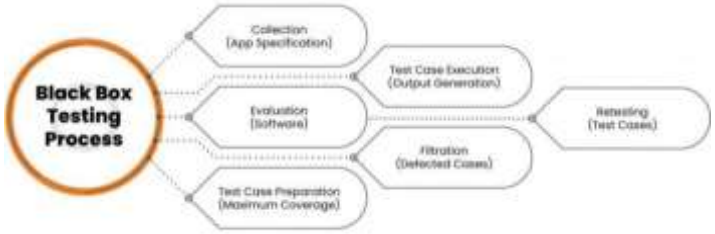
Gambar 2.4 Tahapan pada framework ISSAF (Fajaryanto, 2015)

ISSAF (Information System Security Assessment Framework) adalah sebuah struktur yang terorganisir yang mengelompokkan evaluasi keamanan sistem informasi ke dalam berbagai domain dan detail evaluasi spesifik atau kriteria pengujian untuk setiap domainnya. Tujuannya adalah untuk memberikan masukan praktis dalam penilaian keamanan yang mencerminkan situasi kehidupan nyata. ISSAF dapat digunakan untuk memenuhi kebutuhan penilaian keamanan organisasi dan juga sebagai referensi untuk memenuhi kebutuhan keamanan informasi lainnya. Kerangka kerja ini mencakup aspek penting dari proses keamanan,

penilaian, dan perkuatan untuk mendapatkan pemahaman yang komprehensif tentang potensi kerentanan yang mungkin ada (Balwant, 2006)

II.2.5 *Black Box Testing*

Black Box Testing mempunyai karakteristik dimana penguji dengan tidak mengetahui target yang akan diuji. Maka dari itu harus mencari tahu terkait semua celah pada keamanan. *Black Box Testing* bertujuan untuk mencari keamanan dari luar dengan mensimulasikan sebagai *attacker* (Guntoro, 2020) Berikut contoh struktur dalam proses *blak box testing*:



Gambar 2.5 *Proses black box testing* (Guntoro, 2020)

II.2.6 *Kali Linux*

Kali Linux adalah sistem operasi yang dibuat dari basis Debian yang ditujukan untuk mencari celah keamanan informasi. Sehingga kali linux dapat digunakan untuk para pemula dalam melakukan penetrasi pada jaringan. Kali Linux merupakan system yang lengkap, sehingga bisa digunakan dalam mencari kerentanan yang ada. Kali Linux dilengkapi dengan softwrare sebagai alat bantu yang digunakan dalam pengujian penetrasi (Hertzog et al, 2017).

II.2.7 *Shodan*

Shodan adalah platform yang mengumpulkan dan menyediakan akses ke informasi tentang perangkat yang terhubung ke Internet. Shodan dapat mencari data dan membuat profile pada setiap target perangkat secara terperinci. Fitur yang dimiliki shodan dapat berguna bagi para profesional keamanan, peneliti, dan bahkan peretas. Shodan bekerja dengan melakukan *scanning* dan mengumpulkan indeks informasi terhadap suatu perangkat yang tersambung pada internet seperti sistem pada server, webcam, router, perangkat IoT dan masih banyak lagi (O'Harrow Jr, et al 2013)

II.2.8 *Censys*

Censys merupakan penyedia layanan scanning dataset. Censys terus memindai seluruh ruang alamat IPv4 publik pada 3.592+ port menggunakan deteksi protokol otomatis. Hasilnya adalah representasi paling akurat dari keadaan Internet saat ini. *Censys* juga memanfaatkan pengalihan dan *Domain Name System* untuk menemukan dan memindai (~ 150M) alamat IPv6 yang digunakan (censys.io. 2024).

II.2.9 *NMAP*

Nmap, atau "*Network Mapper*," merupakan alat sumber terbuka untuk menjelajahi dan melakukan audit keamanan pada jaringan. Alat ini didesain khusus untuk melakukan pemindaian cepat pada jaringan yang besar, walaupun juga bisa digunakan untuk host tunggal. Nmap menggunakan paket IP mentah dengan cara yang canggih untuk mengidentifikasi host yang ada dalam jaringan, mengetahui layanan yang disediakan (termasuk nama aplikasi dan versinya), sistem operasi yang digunakan beserta versinya, jenis firewall/filter paket yang digunakan, dan berbagai karakteristik lainnya. Walaupun Nmap seringkali digunakan untuk melakukan audit keamanan, banyak administrator sistem dan jaringan yang menganggapnya bermanfaat untuk tugas-tugas sehari-hari seperti inventarisasi jaringan, mengatur jadwal peningkatan layanan, dan memonitor waktu aktif dari host atau layanan (Medeiros, et al 2009).

II.2.10 *SQL MAP*

Sqlmap merupakan sebuah perangkat lunak sumber terbuka untuk uji penetrasi yang mengotomatisasi proses penemuan dan pemanfaatan kelemahan injeksi SQL serta mengambil alih kontrol atas server basis data. Dilengkapi dengan mesin deteksi yang kuat, berbagai fitur khusus untuk pengujian penetrasi, dan berbagai pilihan termasuk identifikasi basis data, ekstraksi data dari basis data, akses ke sistem file yang mendasarinya, dan pelaksanaan perintah pada sistem operasi melalui koneksi out-of-band. Selain itu, SQLMAP juga berguna untuk mendeteksi dan memanfaatkan kerentanan injeksi SQL dalam aplikasi web (Clarke, et al 2012)

II.2.11 *Nikto*

Nikto adalah alat pemindaian kerentanan perangkat lunak gratis yang berbasis baris perintah. Alat ini digunakan untuk memeriksa server web guna menemukan

file atau CGI yang berpotensi membahayakan, perangkat lunak server yang sudah usang, serta masalah keamanan lainnya. Nikto melakukan pemeriksaan secara umum dan spesifik terhadap tipe server tertentu. Selain itu, alat ini juga mampu menangkap dan mencetak cookie yang diterima. Alat ini juga melakukan pemeriksaan terhadap konfigurasi server seperti keberadaan beberapa file indeks dan opsi server HTTP, serta mencoba mengidentifikasi server web dan perangkat lunak yang terinstal. Pembaruan item pemindaian dan plugin dilakukan secara berkala dan dapat diperbarui secara otomatis (madhusudan_soni., 2020.).

II.2.12 *Zap*

Zed Attack Proxy (ZAP) adalah alat pengujian penetrasi gratis berbasis sumber terbuka yang dikelola di bawah The Software Security Project (SSP). ZAP didesain khusus untuk melakukan pengujian pada aplikasi web dengan fleksibilitas dan kemampuan untuk dikembangkan lebih lanjut. Dalam esensinya, ZAP dapat dianggap sebagai "proxy man-in-the-middle." Alat ini berada di antara peramban pengujian dan aplikasi web yang sedang diuji, sehingga dapat menangkap dan memeriksa pesan yang dikirimkan antara keduanya, serta mengubah konten jika perlu, sebelum meneruskan paket-paket tersebut ke tujuan (Zap Development Team, 2023).

Gambar 2.4 Cara kerja zap pada website tanpa konfigurasi

Meskipun terdapat network proxy, ZAP dapat dikonfigurasi untuk terhubung kedalam proxy tersebut

Gambar 2.5 Cara kerja zap pada website tanpa konfigurasi

II.2.13 *Legion*

Legion adalah alat GUI di Kali Linux yang memungkinkan pentester untuk dengan cepat menemukan dan mengeksploitasi vektor serangan pada host Legion juga menyediakan layanan seperti pengintaian dan pemindaian otomatis dengan NMAP, whataweb, sslyzer, Vulners, webslayer, SMBenum, dirbuster, nikto, Hydra, dan hampir 100 skrip terjadwal otomatis ditambahkan ke dalamnya.Selain itu Ini memiliki fitur penyimpanan otomatis hasil dan tugas proyek secara real-time. Ini memiliki fitur penyimpanan otomatis hasil dan tugas proyek secara real-time. Fungsionalitas modular dari Legion Tool memungkinkan pengguna menyesuaikan Legion dengan mudah (lalitmohantiwari7700, 2020).

II.2.14 *Hydra*

Hydra adalah koneksi paralel yang mendukung banyak protokol serangan. *Hydra* digunakan oleh peneliti dan konsultan keamanan untuk *bruteforce attack*. *Hydra* memiliki kecepatan dan fleksibilitas yang tinggi, serta memungkinkan pengguna untuk dengan mudah menambahkan modul baru. Alat ini memperbolehkan para peneliti dan konsultan keamanan untuk menunjukkan seberapa mudahnya mendapatkan akses ilegal ke sistem secara remote (McNab, et al 2011)

II.2.15 *Wireshark*

Wireshark adalah salah *software* analisis *open source*. Software ini digunakan untuk pemecah masalah jaringan. Wireshark memungkinkan pengguna menempatkan pengontrol antarmuka jaringan ke mode promiscuous (jika didukung oleh pengontrol antarmuka jaringan), sehingga mereka dapat melihat semua lalu lintas yang terlihat pada antarmuka itu termasuk lalu lintas unicast yang tidak dikirim ke alamat MAC pengontrol antarmuka jaringan itu (Hnatyshin, et.al 2021).

II.2.16 *Cookie manager*

Cookie manager ini memungkinkan untuk melihat dan mengubah *cookie* tertentu dengan cepat. Ini dirancang agar kompatibel *dengan Chrome, Firefox* dan *Firefox* untuk *Android*. Secara *default*, *cookie manager* terbuka saat ekstensi dijalankan. Ini memungkinkan untuk menonaktifkan ekstensi sampai membutuhkannya (Cookie Manager, 2023).

II.2.17 *Vulnerability assessment*

Vulnerability assessment adalah fase pendekatan untuk mengidentifikasi kerentanan yang ada dalam system. Vulnerability atau kerentanan terbagi menjadi tiga pemberitahuan khusus. Pembagiannya meliputi high, medium, dan low. Dari beberapa hasil kategori tersebut, maka terdapat manfaat sebagaimana dapat mengetahui tingkat kerentanan pada sistem (M. Aziz, 2021).

II.2.18 *Cross-Site Request Forgery (CSRF)*

Cross-Site Request Forgery (CSRF) adalah serangan dimana kepercayaan yang diberikan oleh web browser kepada situs web yang dikunjungi oleh pengguna (S. M. R. W. Rankothge, 2020). Dalam serangan ini, peretas mengeksploitasi kepercayaan ini untuk melakukan tindakan yang tidak diinginkan oleh pengguna, seperti mengirim permintaan HTTP yang tidak sah dari situs web yang terpercaya. Serangan CSRF dapat menyebabkan aksi yang tidak diinginkan, seperti mengubah data pengguna, melakukan transaksi keuangan, atau mengirim pesan tanpa sepengetahuan pengguna. Untuk melindungi aplikasi web dari serangan CSRF, berbagai teknik mitigasi telah dikembangkan, termasuk penggunaan token CSRF, verifikasi referer, dan penggunaan header khusus dalam permintaan HTTP. Selain itu, alat-alat seperti OWASP ZAP juga digunakan untuk menemukan kerentanan CSRF dalam aplikasi web dan melakukan mitigasi yang diperlukan

II.2.19 *Session Hijacking*

Session Hijacking adalah serangan keamanan di mana individu yang tidak sah mengambil alih sesi pengguna yang valid untuk mendapatkan akses ke informasi sensitif atau melakukan tindakan jahat (I. T. Elira Hoxha, 2022). Jenis serangan ini difasilitasi dengan mengeksploitasi kerentanan dalam situs web yang dirancang dengan buruk dan kurangnya mekanisme keamanan, yang mengekspos identitas pengguna dan data sesi. Pembajakan sesi dapat menyebabkan akses tidak sah ke data rahasia dan tindakan tidak sah atas nama pengguna yang sah. Untuk mencegah pembajakan sesi, berbagai strategi pencegahan telah diusulkan, termasuk penggunaan *cookie* sekali pakai, token autentikasi tanpa kewarganegaraan, dan langkah-langkah keamanan lainnya. Strategi ini bertujuan untuk mengurangi risiko pembajakan sesi dan meningkatkan keamanan aplikasi web dan sesi penggunaan.

II.2.20 *Cross-Site Scripting (XSS)*

Cross-Site Scripting (XSS) merupakan salah satu serangan oleh peretas untuk menyerang aplikasi web dengan tujuan utama untuk mencuri informasi rahasia dari klien atau basis data webserver. Serangan XSS dapat dilakukan dengan menggunakan berbagai alat, seperti XSSer, FoxyProxy, dan Burp Suite. Penelitian juga membahas tentang kontrameasure terhadap serangan XSS untuk mencegah pengguna dari jatuh ke dalam serangan XSS dengan mudah (V. S. Voo Teck En, 2022).

II.2.21 *SQL Injection (SQLI)*

SQL Injection (SQLI) merupakan jenis serangan siber dimana penyerang memanipulasi bidang input aplikasi web untuk mengeksekusi perintah SQL yang tidak sah (D. A. S. S. A. Maha Alghawazi, 2022). Serangan ini dapat menyebabkan akses tidak sah ke data sensitif, modifikasi data, dan bahkan penghapusan data dari database yang mendasarinya. Serangan injeksi SQL termasuk yang paling merusak di antara serangan aplikasi web, karena dapat membahayakan kerahasiaan, integritas, dan ketersediaan data. Untuk mengatasi ancaman ini, berbagai teknik deteksi dan pencegahan telah dikembangkan, termasuk penggunaan model pembelajaran mesin dan pembelajaran mendalam untuk mendeteksi serangan injeksi SQL dengan akurasi tinggi. Teknik-teknik ini bertujuan untuk mengidentifikasi dan memitigasi kerentanan yang dapat dimanfaatkan oleh serangan injeksi SQL, sehingga meningkatkan keamanan aplikasi web dan basis data.

II.2.22 *Insecure Direct Object Reference (IDOR)*

Insecure Direct Object Reference (IDOR) adalah celah keamanan yang muncul saat sebuah aplikasi web tidak memvalidasi atau memberikan izin akses yang memadai terhadap objek secara langsung, seperti data atau sumber daya (I. A. K. Rio Ananda Putra, 20223). Dalam konteks keamanan aplikasi web, objek tersebut bisa berupa file, catatan database, atau sumber daya lain yang diidentifikasi melalui parameter atau referensi langsung. Dengan menggunakan teknik IDOR, seorang penyerang dapat memanipulasi parameter yang diteruskan ke aplikasi web untuk memperoleh akses yang tidak sah terhadap objek yang semestinya tidak dapat diakses. Dengan memanfaatkan celah ini, penyerang dapat mengakses, mengubah,

atau menghapus data yang seharusnya hanya dapat diakses oleh pengguna yang memiliki izin.Untuk melindungi aplikasi web dari serangan IDOR, berbagai teknik mitigasi telah dikembangkan, termasuk penggunaan token CSRF, verifikasi referer, dan penggunaan header khusus dalam permintaan HTTP. Selain itu, alat-alat seperti OWASP ZAP juga digunakan untuk menemukan kerentanan IDOR dalam aplikasi web dan melakukan mitigasi yang diperlukan

II.2.23 *Bruteforce attack*

Bruteforce attack adalah serangan yang dilakukan dengan cara mencoba berbagai kemungkinan kombinasi password mendapatkan akses ke sistem atau data yang dilindungi. Serangan ini dapat dilakukan secara manual atau dengan menggunakan program otomatis yang disebut bruteforcer.(I. K. Marco Ariano Kristyanto, 2022).

II.2.25 SSL/TLS

SSL (Secure Sockets Layer) atau TLS (Transport Layer Security) adalah protokol keamanan yang digunakan untuk melindungi koneksi antara server website dan aplikasi web. Protokol ini mengenkripsi data yang dikirim dan diterima melalui jaringan, termasuk email, sesi penjelajahan website, dan transfer file. SSL/TLS memastikan bahwa informasi antara klien dan server terenkripsi sehingga tidak dapat dibaca oleh pihak yang tidak berkepentingan. Selain itu, SSL/TLS digunakan untuk memverifikasi identitas server dan klien guna mencegah serangan yang tidak diinginkan. Protokol ini berlaku untuk semua jenis data yang dikirim dan diterima melalui jaringan, termasuk data pribadi seperti informasi login dan nomor kartu kredit. Mengaktifkan SSL/TLS di situs web dilakukan dengan menginstal sertifikat SSL/TLS di server website (Stephen A, et al 2000). SSL/TLS memberikan banyak manfaat, seperti melindungi informasi pribadi, meningkatkan kepercayaan pelanggan, dan mendukung kepatuhan terhadap regulasi.

II.2.26 *Domain Name Server*

Domain Name Server (DNS) adalah sistem yang menyimpan informasi mengenai nama-nama host. Nama domain disimpan dalam bentuk database yang tersebar di jaringan komputer. Fungsinya utama adalah untuk mengonversi nama-nama host menjadi alamat IP, dan sebaliknya. Hal ini mempermudah pengguna

internet untuk mengingat dan mengakses nama-nama tersebut (A. Fujianto and I. dfdf Waspada, 2016).

II.2.27 *Cookies*

Cookies adalah file teks yang mengandung informasi yang diperoleh saat pengguna Internet mengakses suatu situs web tertentu. Mereka muncul dalam bentuk notifikasi saat mengunjungi sebuah situs web. Cookies adalah file kecil yang berisi informasi mengenai interaksi saat menjelajahi situs web. Selain digunakan untuk mengidentifikasi dan melacak aktivitas, cookies juga membantu mengingat informasi pengguna. Dengan demikian, ketika pengguna kembali mengunjungi situs web, mereka dapat diidentifikasi secara otomatis dan tidak perlu lagi memasukkan informasi pengguna secara manual (Kristol, et al 2001)

BAB III METODOLOGI

III.1 Metode Penelitian

Pada kesempatan ini, pendekatan yang diterapkan adalah metode kualitatif melalui wawancara. Proses wawancara dilakukan dengan mengajukan pertanyaan langsung kepada pihak operator dari website *e-raport* sekolah XYZ. Tujuan dari kegiatan ini adalah untuk memperoleh izin yang diperlukan serta untuk mengidentifikasi kebutuhan pengujian keamanan sistem informasi pada website website *e-raport* sekolah XYZ Selain itu, wawancara ini juga bertujuan untuk menentukan rekomendasi perbaikan yang dapat diterapkan.

III.2 Alat dan Bahan Penelitian

Dalam melaksanakan penelitian ini, berbagai alat diperlukan untuk memastikan kelancaran proses pengumpulan dan analisis data. Adapun alat-alat yang digunakan adalah:

1. Laptop dan Perangkat Lunak

a. Laptop pribadi sebagai platform utama untuk menjalankan perangkat lunak

b. Alat dan bahan melakukan analisis keamanan sistem informasi.

Tabel III.1 Tabel alat dan bahan

No.	Kebutuhan	Spesifikasi *Tools*
1.	*Device*	*AMD Ryzen 5 5500U*.2.30GHz RAM 8GB
2.	*Operating System*	*Kali Linux*
3.	*Hosting Dummy Server*	Menggunakan jasa hosting pihak ketiga seperti aws,dan sebagianya atau menggunakan cara yang lain
4.	*Information gathering*	*Nmap, whois, wappalyzer, tools lain yang sejenis*
5.	*Network mapping*	*NMap, tools* lain yang sejenis
6.	*Vulnerability identification*	*Nessus, tools* lain yang sejenis
7.	*Penetration testing*	*SQL Map*
8.	*Gaining access and privilage escalation*	*Hydra*
9.	*Enumerating further*	*Wireshark, dan cookie manager*

10.	*Compromise remote user/sites*	Tidak sampai pada tahap ini dikarenakan gagalnya tahapan *Enumerating further*
11.	*Maintaining access*	Tidak sampai pada tahap ini dikarenakan gagalnya tahapan *Enumerating further*
12.	*Corvering track*	Tidak sampai pada tahap ini dikarenakan gagalnya tahapan *Enumerating further*

2. Software Penetration Test

Penggunaan perangkat lunak khusus untuk kegiatan *penetration testing* guna mengidentifikasi celah keamanan potensial pada website pembelajaran. Penggunaan software berada di halaman 34 pada tabel III.1

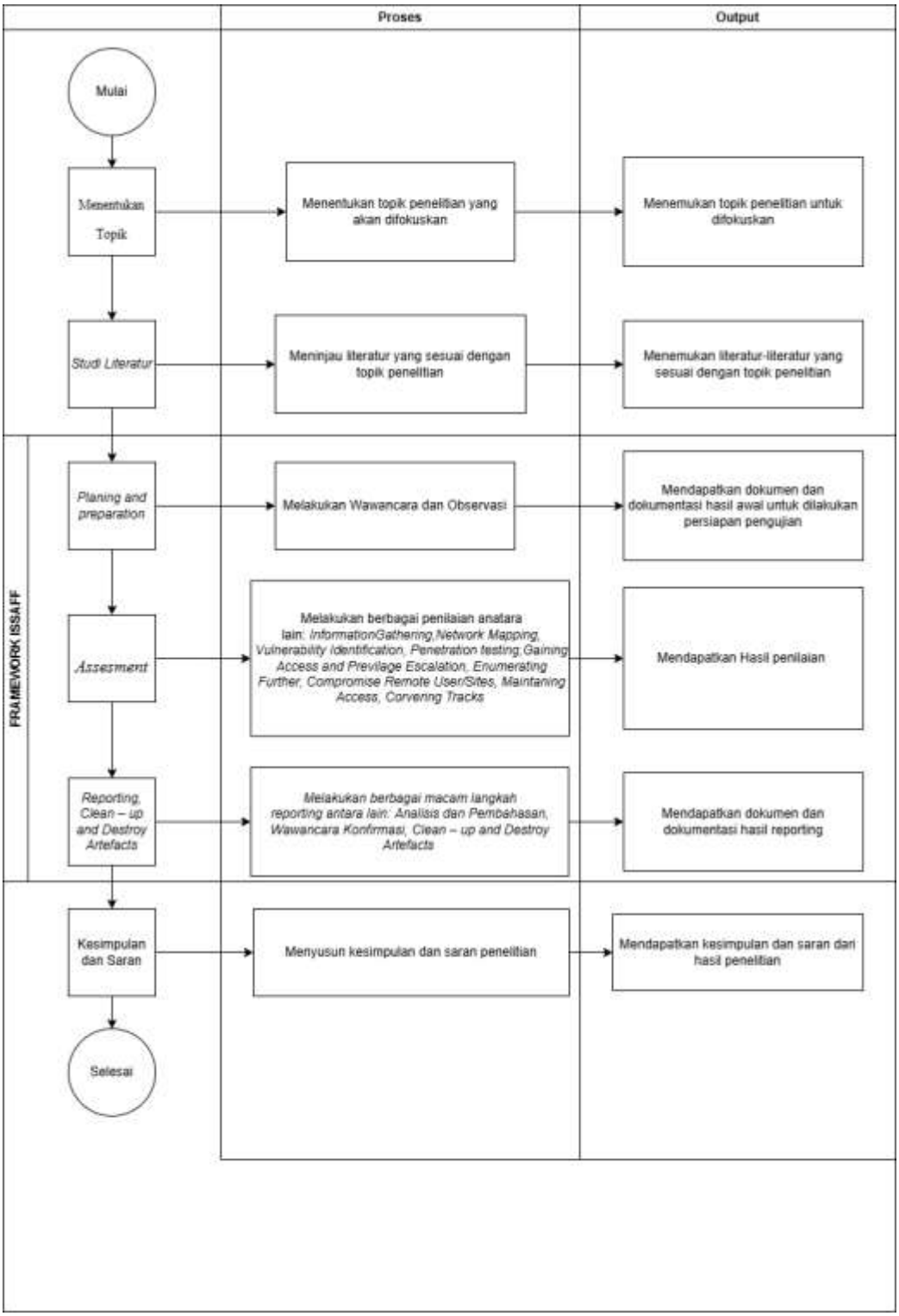
3. Server Dummy

Server Dummy dimaksudkan menyimpan database di server yang bukan aslinya. Sebelum itu server dummy harus di install sesuai dengan website aslinya. Untuk server dummy penulis berencana menggunakan server aws atau hostinga online yang lainnya

Untuk melengkapi kebutuhan penelitian, beberapa bahan menjadi fokus dalam pengumpulan data dan analisis. Bahan-bahan tersebut melibatkan:

1. Dokumentasi website *e-raport* sekolah XYZ
2. Dokumentasi terkait struktur, arsitektur, dan kebijakan keamanan yang telah ada pada website website *e-raport* sekolah XYZ.
3. Panduan Wawancara
   Dokumen panduan wawancara yang berisi kumpulan pertanyaan terstruktur untuk diarahkan kepada pihak operator dari website *e-raport* sekolah XYZ.
4. Dokumen Izin dan Persetujuan
   Dokumen formal izin yang diperlukan untuk melakukan penetration testing dan wawancara kepada pihak terkait.

III.3 Prosedur Penelitian



Gambar 3.1 *Flowchart* prosedur penelitian

Berdasarkan gambar 3.1 penelitian ini memiliki prosedur penelitian sebagai berikut:

III.3.1 Menentukan Topik

Pada tahap ini, penelitian dimulai dengan menentukan topik penelitian yang akan difokuskan, yaitu "Analisis Keamanan Sistem Informasi pada Website pihak operator dari website *e-raport* sekolah XYZ menggunakan Metode ISSAF."

III.3.2 Studi Literatur

Langkah ini melibatkan peninjauan literatur untuk memahami kerangka teoritis dan penelitian terdahulu yang relevan dengan keamanan sistem informasi, metode ISSAF, dan konteks website E - Raport.

III.3.3 *Planing and preparation*

Pada tahap perencanaan dan persiapan, langkah-langkah berikut dilakukan:

1. Wawancara

   Menyiapkan panduan wawancara untuk mendapatkan informasi dari pihak operator dari website *e-raport* sekolah XYZ.

2. Observasi

   Merencanakan kegiatan observasi untuk memahami secara langsung konteks dan keadaan sistem informasi.

III.3.4 *Assesment*

Assessment merupakan tahapan utama didalam frawemork issaf. Dimana tahapan ini berisi berbagai macam pengujian keamanan system informasi. Adapun tahapan assessment dibagi menjadi:

III.3.4.1 Information Gathering

Information Gathering adalah aktivitas untuk mencari informasi atau data tentang suatu target. Proses ini sangat penting bagi para profesional keamanan siber, serta peretas dan penjahat siber, untuk memahami kerentanan potensial dan merencanakan serangan. Tujuan dari Information Gathering dalam keamanan siber adalah untuk mengungkap informasi penting yang mungkin tidak diketahui, seperti mengamankan jaringan bisnis dan mengurangi potensi akses tidak sah ke jaringan perusahaan.

III.3.4.3 *Network Mapping*

Proses visualisasi dan pemahaman sistem jaringan yang kompleks dengan memecahnya menjadi fragmen-fragmen kecil. Ini digunakan untuk menganalisis jaringan, memahami bagaimana perangkat saling berinteraksi, dan menemukan perangkat yang terhubung ke jaringan.

III.3.4.3 *Vulnerability Identification*

Identifikasi kerentanan adalah proses penting dalam keamanan siber yang melibatkan identifikasi dan pemahaman kelemahan dalam sistem, infrastruktur, dan sistem pendukung. Hal ini penting untuk melindungi sistem TI secara proaktif dan mencegah kerusakan potensial dari serangan. Proses ini melibatkan pemeriksaan aktif jaringan untuk mengidentifikasi host, perangkat lunak, dan konfigurasi dengan kerentanan yang belum diperbaiki. Ini dapat mencakup menemukan perangkat lunak yang belum diperbarui, standar enkripsi dan keamanan yang sudah usang, atau port terbuka dan layanan jaringan yang tidak cukup dilindungi di belakang firewall

III.3.4.4 *Penetration testing*

Simulasi serangan siber yang diotorisasi dilakukan pada sistem komputer untuk mengevaluasi tingkat keamanannya. Uji penetrasi ini bertujuan untuk menemukan dan menunjukkan dampak bisnis dari kelemahan yang ada dalam suatu sistem. Para penguji penetrasi menggunakan metode, alat, dan prosedur yang serupa dengan serangan yang dilakukan oleh penyerang untuk menemukan dan menunjukkan konsekuensi bisnis dari kelemahan dalam sistem tersebut. Uji penetrasi biasanya mensimulasikan berbagai jenis serangan yang mungkin mengancam suatu bisnis. Mereka menguji apakah sistem tersebut mampu bertahan terhadap serangan dari pengguna yang terautentikasi maupun yang tidak terautentikasi, serta berbagai peran sistem. Dengan cakupan yang tepat, uji penetrasi dapat menyelidiki setiap aspek dari suatu sistem.

III.3.4.5 *Gaining Access and Previlage Escalation*

Dalam serangan privilege escalation, peretas memanfaatkan kerentanan dalam kontrol akses dan pembatasan sumber daya untuk mengesampingkan izin dan batasan dari akun pengguna target untuk mendapatkan akses yang lebih tinggi. Serangan ini biasanya bertujuan untuk memperoleh hak administratif dan

memanipulasi pengaturan keamanan sistem dengan memperluas cakupan serangan awal.

III.3.4.6 *Enumerating Further*

Setelah proses enumeration awal, penyerang dapat menggunakan informasi yang ditemukan untuk melakukan enumerating further, yaitu mengumpulkan informasi lebih lanjut tentang sistem atau jaringan. Tujuannya adalah untuk memperoleh akses ke informasi sensitif seperti kata sandi dan nama pengguna yang kemudian dapat digunakan untuk tujuan jahat seperti pencurian identitas atau pelanggaran data.

III.3.4.3 *Compromise Remote User/Sites*

"*Compromise Remote User/Sites*" dalam bahasa Indonesia dapat diartikan sebagai "Kompromi Pengguna/Situs Remote". Istilah ini merujuk pada situasi di mana pengguna atau situs remote mengalami kompromi keamanan, yang dapat mengakibatkan akses yang tidak sah atau penyalahgunaan sistem. Kompromi semacam ini dapat terjadi melalui berbagai metode, termasuk serangan siber yang bertujuan untuk mendapatkan akses yang tidak sah ke sistem atau situs remote.

III.3.4.8 *Maintaning Access*

Upaya untuk tetap terhubung ke suatu sistem atau jaringan setelah berhasil mendapatkan akses yang tidak sah. Ini dapat terjadi dalam konteks keamanan siber, manajemen akses fisik, atau pengendalian akses ke sistem komputer.

III.3.4.9 *Corvering Tracks*

Merujuk pada serangkaian tindakan yang dilakukan oleh penyerang setelah berhasil melakukan serangan untuk menghapus atau menyembunyikan jejak-jejak yang dapat digunakan untuk melacak atau mendeteksi kehadiran mereka. Tindakan ini bertujuan untuk mengurangi kemungkinan deteksi dan identifikasi penyerang serta mempersulit upaya penyelidikan.

III.3.5 Reporting, Clean – up and Destroy Artefacts

1. Analisis dan Pembahasan

Analisis dan pembahasan adalah tahap penting dalam penelitian atau studi yang dilakukan. Analisis merujuk pada proses pengumpulan, pemrosesan, dan interpretasi data untuk menjawab pertanyaan penelitian atau studi yang dilakukan.

Sedangkan pembahasan merujuk pada interpretasi hasil analisis dan penjelasan tentang implikasi temuan terhadap topik penelitian atau studi yang dilakukan.

Hasil analisis dan pembahasan tersebut dapat digunakan untuk mengidentifikasi tren, mengembangkan rekomendasi, dan membuat keputusan yang didasarkan pada data. Oleh karena itu, analisis dan pembahasan merupakan tahap penting dalam penelitian atau studi yang dilakukan dan harus dilakukan dengan hati-hati dan teliti untuk memastikan hasil yang akurat dan dapat diandalkan.

2. Wawancara Konfirmasi

Wawancara konfirmasi dapat menjadi bagian penting dalam prosedur penelitian. Wawancara konfirmasi dapat dilakukan untuk memastikan keakuratan data yang diperoleh dari responden, serta untuk memperoleh pemahaman yang lebih mendalam terkait dengan topik penelitian.wawancara konfirmasi dapat menjadi langkah yang penting dalam memvalidasi data, memperoleh pemahaman yang lebih mendalam. Hal ini dapat membantu memastikan keakuratan dan keabsahan hasil penelitian yang dilakukan.

3. *Clean – up and Destroy Artefacts*

Tahap akhir dalam proses penetration testing, yaitu tahap penghapusan semua jejak atau bukti aktivitas penetrasi. Dalam keseluruhan, "*Clean-up and Destroy Artefacts*" dapat menjadi bagian penting dalam prosedur penelitian untuk memastikan keakuratan dan keabsahan data yang digunakan serta untuk mempercepat proses analisis data.

III.4 Deskripsi Objek

Deskripsi objek merupakan urain umum mengenai objek yang *website* menggambarkan fitur-fitur dan perilaku yang diharapkan dari situs web tersebut. Pada sub bab penelitian ini berisi fitur-fitur dan perilaku yang diharapkan dari situs web *e-raport* .User *login* sebagai guru, terdapat menu referensi dengan sub menu peserta didik aktif dimana didalam detailnya terdapat semua data terkait peserta didik yaiitu NIK, Alamat, dan nama orang tua. Guru bisa melihat, mencari dan memperbahurui data terkait peserta didik. Selain itu terdapat menu kompetensi datar yang dimana guru uru bisa melihat, mencari dan memperbahurui data kompetensi datar. Selain itu terdapat menu tujuan pembelajaran yang dimana guru bisa melihat, mencari dan memperbahurui data tujuan pembelajaran. Selain itu terdapat menu tujuan pembelajaran yang dimana guru bisa melihat, mencari dan memperbahurui data tujuan pembelajaran. Selain itu terdapat bobot penilaian pembelajaran yang dimana guru bisa melihat, mencari dan memperbahurui data bobot penilaian. Selanjutnya, terdapat nilai pembelajaran yang dimana guru bisa melihat, mencari dan memperbahurui data nilai. Selain itu terdapat profil pengguna pembelajaran yang dimana guru bisa melihat, mencari dan memperbahurui data profil pengguna Namun apabila *user login* sebagai admin maka *user* bisa melakukan sinkronisasi (mengambil data dapodik dan mengirim data *e-raport),* referensi (melihat guru dan tenaga pendidik), mengatur hak akses, profil (mengubah email dan kata sandi) dan menu yang lain.

BAB IV HASIL DAN PEMBAHASAN

IV.1 *Planing and preparation*

IV.1 Wawancara dan Observasi

Wawancara persetujuan sangat penting sebelum melakukan sebuah uji kerentanan pada sistem *E- Raport* sekolah XYZ. Tahapan ini menghasilkan sebuah izin serta melakukan sesi tanya jawab kepada pihak lembaga sekolah XYZ. Tahapan ini berfungsi untuk menghindari adanya kesalahpahaman ketika sedang melakukan uji kerentanan pada website *E- Raport* sekolah XYZ. Sesi Wawanara dilakukan pada tanggal 08 bulan maret tahun 2024 jam 09;39 WIB pagi dengan narasumber adalah Bapak Moh Hisyam Fitrhony selaku salah satu operator website dan Wakil Kepala hubungan masyarakat (WAKA HUMAS) sekolah XYZ. Dokumen hasil wawancara dan dokumentasi wawancara terlampir pada lampiran 2 dan lampiran 3.

IV.1.2 Pembelian Server dummy

Dikarenakan Batasan masalah pada penelitian ini pengujian dilakukan menggunakan server dummy. Maka pada tahapan ini penguji melakukan pembelian server dummy. Untuk lebih lengkapnya bisa dilihat pada lampiran 4

IV.1.3 Instalasi e-raport pada server dummy

Setelah membeli server dummy maka selanjutnya dilakukan pemasangan *e raport* pada server dummy. Berdasarkan link official website *e raport* yaitu: Dashboard e-Raport SMK (ditpsmk.net), terdapat link langkah-langkah instalasi yaitu: Panduan e-Raport SMK V.7.pdf - Google Drive. Uraian langkah- Langkah instalasi berada pada lampiran 5-7

IV.2 Assesment

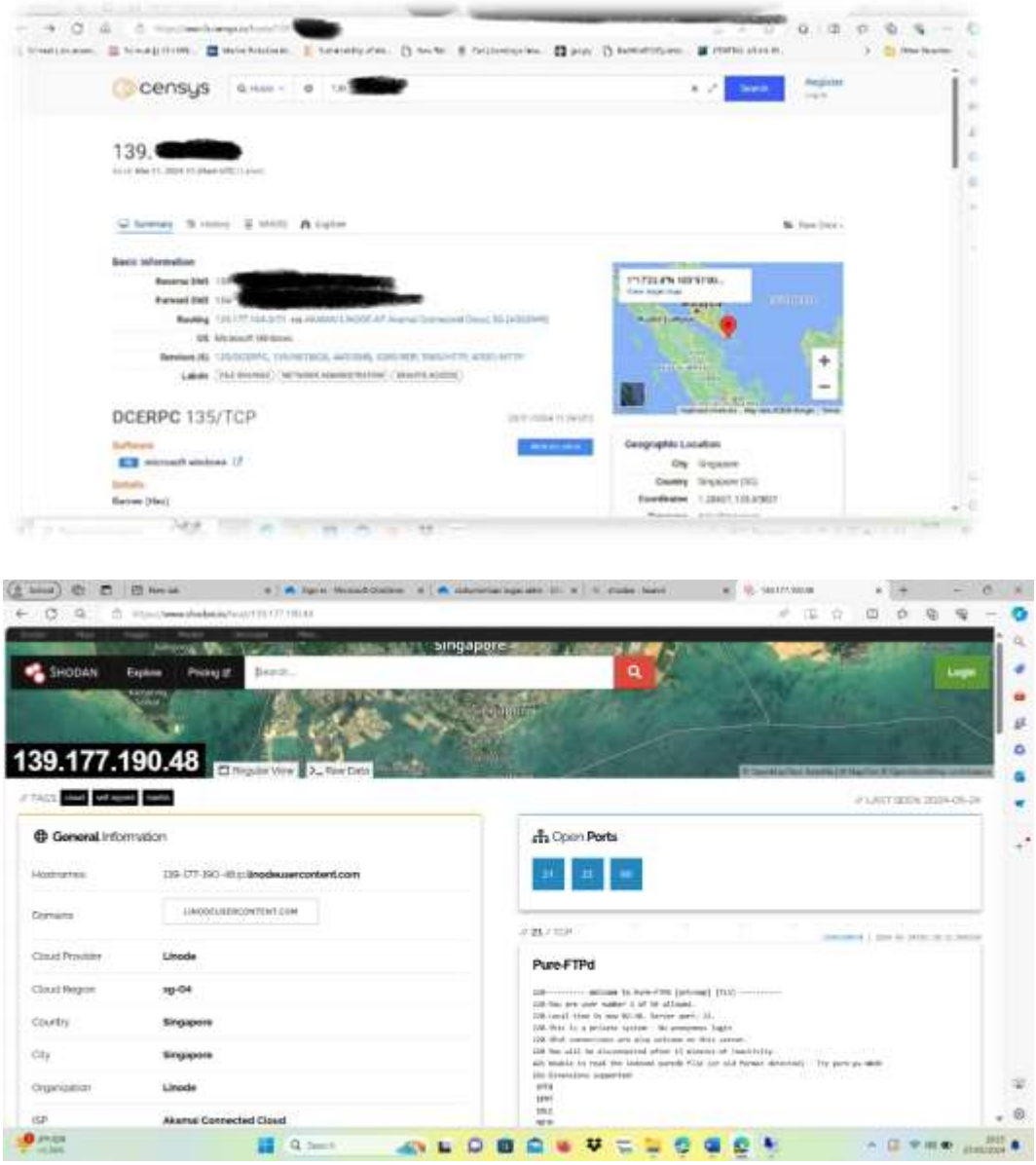
Tahap selanjutnya dari framework ISSAF yaitu assessment yang dibagi ke dalam beberapa tahap, antara lain:

IV.2.1 Information Gathering

Information Gathering yaitu tahpapan mencari data dan informasi dari berbagai sumber terbuka atau umum. Sumber informasi ini dapat mencakup internet,

publikasi, dokumentasi, serta data yang dapat diakses secara bebas.Pada tahap *Information Gathering* penguji menggunakan tools yaitu shodan dan censys

IV.2.1.1 *Hasil Information Gathering pada server dummy*



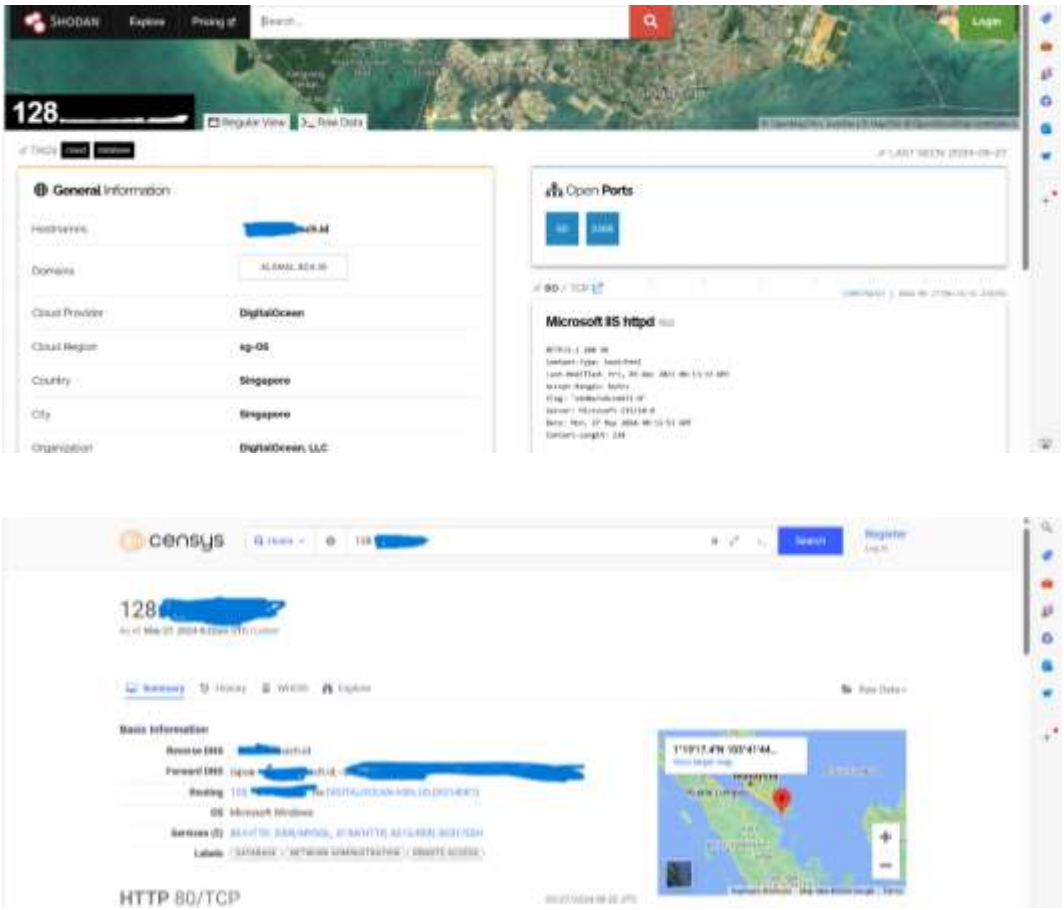
Gambar IV.1 Hasil *Information Gathering* pada server dummy

Berdasarkan gambar IV.1 hasil *Information Gathering* pada server dummy tools shodan dan censys dapat diketahui beberapa informasi yaitu:

1. Alamat ip adalah 139.xxx.xxx.xx
2. memiliki port 22, 135, 445,3389,5985,8181

3. Operating system Windows Server 2012 R2 Standard 9600

IV.2.1.2 *Hasil Information Gathering pada server production*



Gambar IV.2 Hasil *Information pada server production*

Berdasarkan gambar IV.2 hasil *Information pada server production* tools shodan dan censys dapat diketahui beberapa informasi yaitu:

1. Reverse DNS : xxx.xxxxxx.sch.id,
2. Routing: 128.xxx.xxx.x/xx via DIGITALOCEAN-ASN, US (AS14061)
3. OS: Microsoft Windows
4. Services (5): 80/HTTP, 3306/MYSQL, 8154/HTTP, 8212/RDP, 8331/SSH

IV.2.2 *Network mapping*

Network mapping adalah proses pemindaian dan pemetaan infrastruktur jaringan komputer untuk mengidentifikasi perangkat yang terhubung, konfigurasi jaringan, dan sumber daya yang ada. Ini melibatkan penggunaan perangkat lunak khusus untuk mengumpulkan informasi tentang jaringan,seperti perangkat yang

terhubung, port yang terbuka, sistem operasi yang berjalan, dan layanan yang dijalankan. Didalam network mapping penguji menggunakan berbagai macam command untuk memperbanyak hasil dari network mapping

IV.2.2.1 Identify Live Hosts

Perintah nmap -v -sn digunakan untuk mengidentifikasi host-host yang aktif atau online dalam suatu jaringan tanpa melakukan pemindaian port. Opsi -sn menginstruksikan Nmap untuk melakukan pemindaian tanpa port (Ping Scan), hanya untuk mengetahui keberadaan host yang aktif.

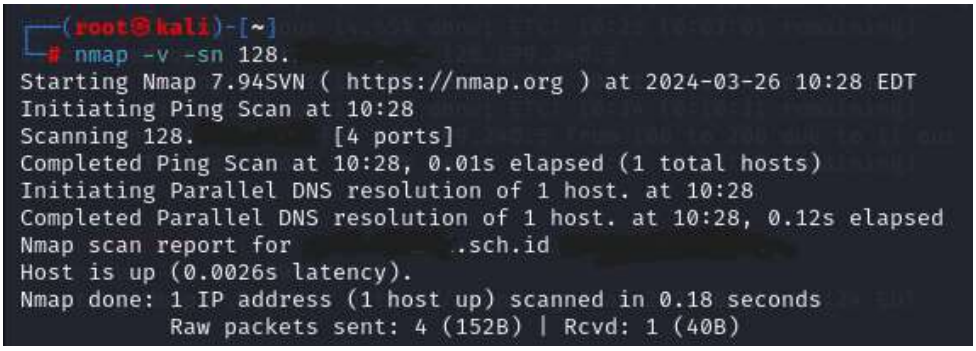
IV.2.2.1.1 Identify Live Hosts server dummy

Gambar IV.3 Hasil Identify Live Hosts di server dummy

Setelah dilakukan *scanning* pada alamat ip 139.177.190.48 yang terdapat dalam gambar IV.3 ditemukan 1 *IP addres (1 host up)* dan dilakukan scan selama 0,94 detik

IV.2.2.1.2 *Identify Live Hosts server production*

Setelah dilakukan Scanning pada situs xxxx.xxxxxx.sch.id (128.xxx.xxx.x) pada waktu 03-26-2024 yang ditukkan oleh gambar IV.4 ditemukaan bahwa host berfungsi dengan latancy 0,0026s. selain itu 1 *IP address (1 host up) di scan* selama 0,18 *seconds*



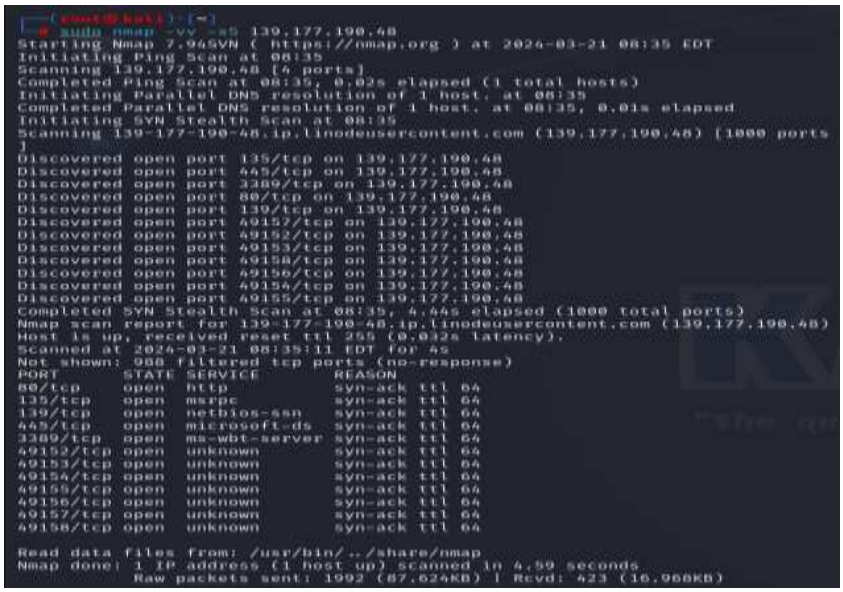
Gambar IV.4 Hasil Identify Live Hosts di server dummy

IV.2.2.2 *TCP Port Scanning*

nmap –vv -sS digunakan untuk melakukan pemindaian port menggunakan TCP SYN scan (-sS). Opsi -sS membuat Nmap menggunakan teknik SYN scan untuk menentukan port mana yang terbuka dalam target yang dipilih. Ini sering digunakan untuk pemindaian cepat dan stealthy.

IV.2.2.2.1 *TCP Port Scanning server dummy*

Hasil *TCP Port menggunakan command nmap –vv -sS Scanning* di sever dummy

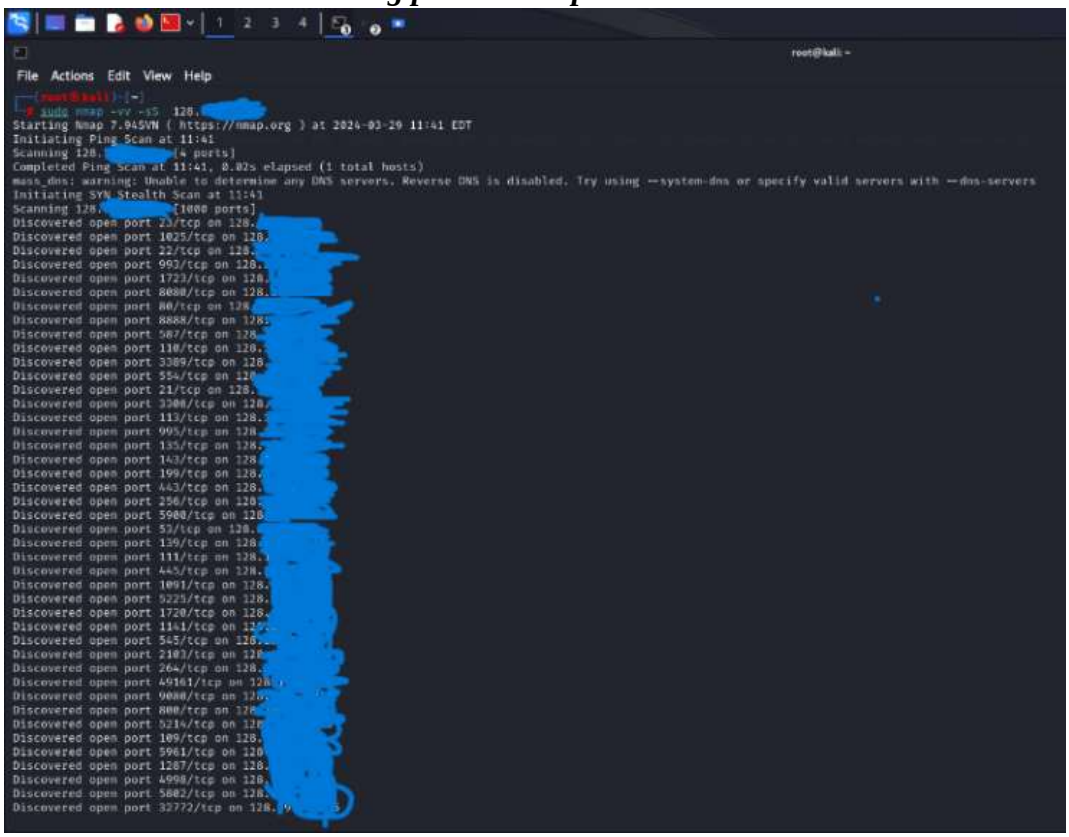


Gambar IV.5 Hasil dari TCP Port Scanning pada server dummy

Setelah dilakukan scan pada 139.177.190.48 pada gambar IV.5 yang berjumlah 1000 ports. Hasil dari scan tersebut ditemukan 988 port tidak ditunjukkan karena tidak merespons dan ditemukan beberapa *open* port dengan servicenya antara lain adalah open port 80/tcp dengan sevice http, open port 135/tcp dengan service msrpc,open port 139/tcp dengan service netbios-ssn, open port 445/tcp dengan service microsoft-ds, open port 3389/tcp dengan service ms-wbt-server. Selain itu ditemukan beberapa port dengan service uknown. Kesemua hasil memiliki reason syn attack ttl 64. Pejelasan syn attack ttl 64 adalah. Dalam tiga langkah awal TCP (TCP three-way handshake), SYN-ACK adalah respons dari server setelah menerima permintaan SYN dari klien. SYN-ACK mengakui SYN dan menandakan kesiapan server untuk membangun koneksi. Nilai TTL (Time To

Live) sebesar 64 dalam SYN-ACK menunjukkan berapa banyak “loncatan” (router) yang dapat dilalui paket sebelum dibuang. Jika lebih dari 64 loncatan terjadi, paket akan diabaikan. TTL penting untuk diagnostik jaringan dan keamanan

IV.2.2.2.2 *TCP Port Scanning pada server production*



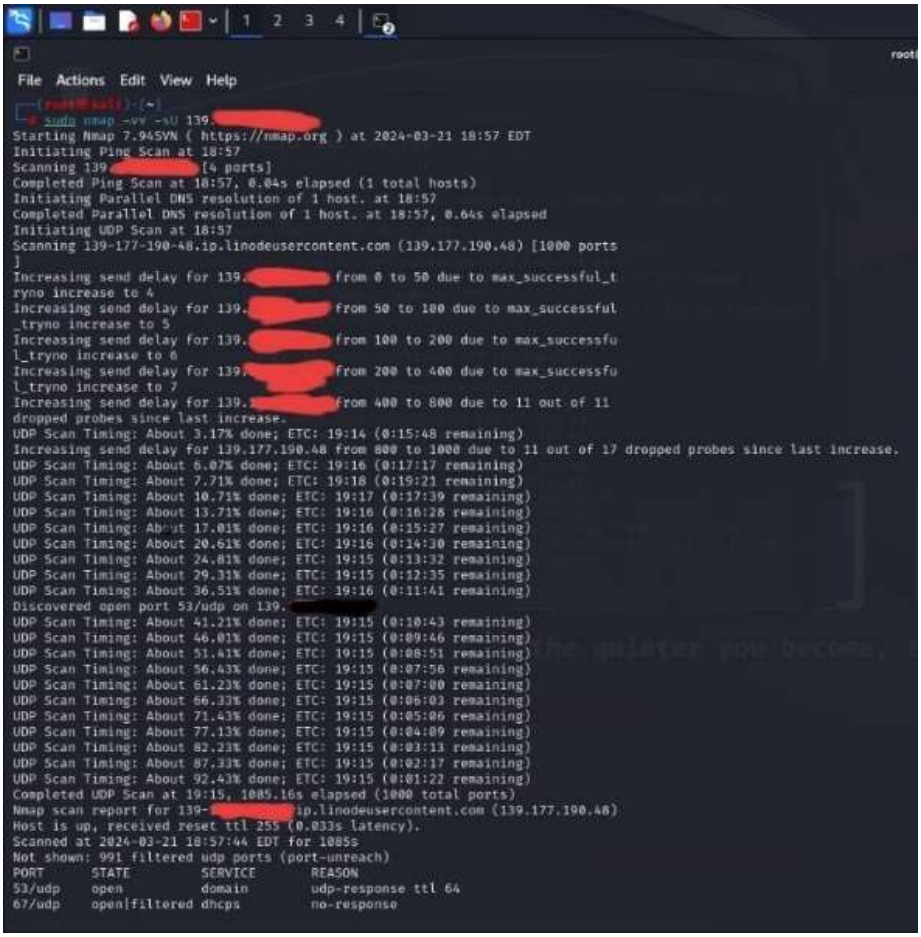
Gambar IV.6 Hasil dari TCP Port Scanning pada server production

Setelah dilakukan Scanning pada situs xxxx.xxxxxx.sch.id (128.xxx.xxx.x) pada waktu 03-26-2024. Didalam gamba IV.6 Ditemukan 1000 port yang terbuka dan merespon atara lain adalah open port 80/tcp dengan sevice http, open port 3306/tcp mysql. . Kesemua hasil memiliki reason syn attack ttl 64. Pejelasan syn attack ttl 64 adalah. Dalam tiga langkah awal TCP (TCP three-way handshake), SYN-ACK adalah respons dari server setelah menerima permintaan SYN dari klien. SYN-ACK mengakui SYN dan menandakan kesiapan server untuk membangun koneksi. Nilai TTL (Time To Live) sebesar 64 dalam SYN-ACK menunjukkan berapa banyak “loncatan” (router) yang dapat dilalui paket sebelum dibuang. Jika lebih dari 64 loncatan terjadi, paket akan diabaikan. TTL penting untuk diagnostik jaringan dan keamanan

IV.2.2.3 *UDP Port Scanning*

Perintah nmap -vv -sU menginstruksikan Nmap untuk melakukan pemindaian port menggunakan UDP (-sU).UDP scan digunakan untuk menemukan port terbuka yang berjalan pada protokol UDP. Ini penting karena UDP tidak memiliki mekanisme seperti TCP yang mengonfirmasi ketersediaan layanan.

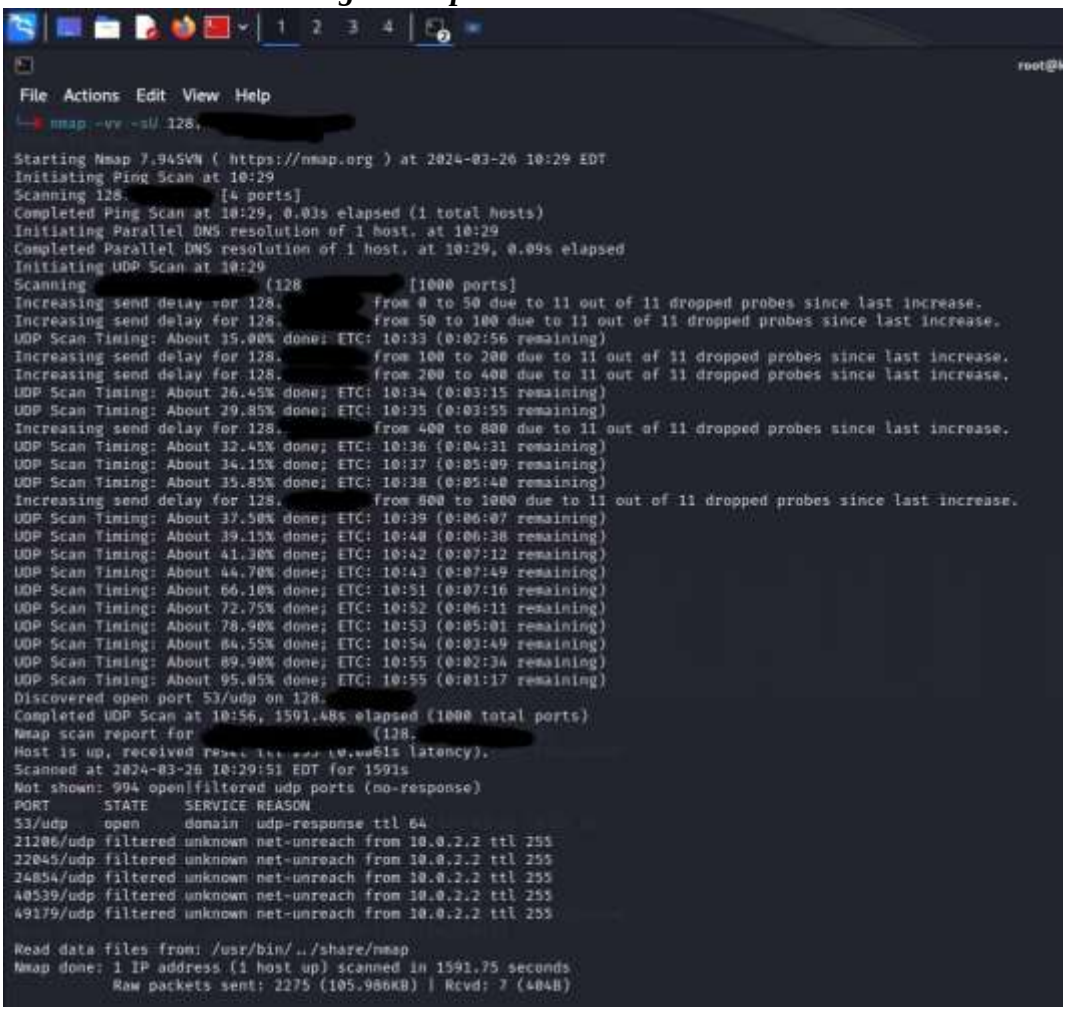
IV.2.2.3.1 UDP Port Scanning server dummy



Gambar IV.7 Hasil UDP Port Scanning pada server dummy

Setalah dilakukan scan pada gambar IV.7 ditemukan bahwasanya host memiliki 1000 port dan dari 1000 port tersebut *991 port unreach*

IV.2.2.3.2 *UDP Port Scanning server production*



Gambar IV.8 Hasil UDP Port Scanning pada server production

Setalah dilakukan scan pada gambar IV.8 ditemukan bahwasanya host memiliki 1000 port dan dari 1000 port tersebut *991 no response*

IV.2.2.4 *Banner Grabbing*

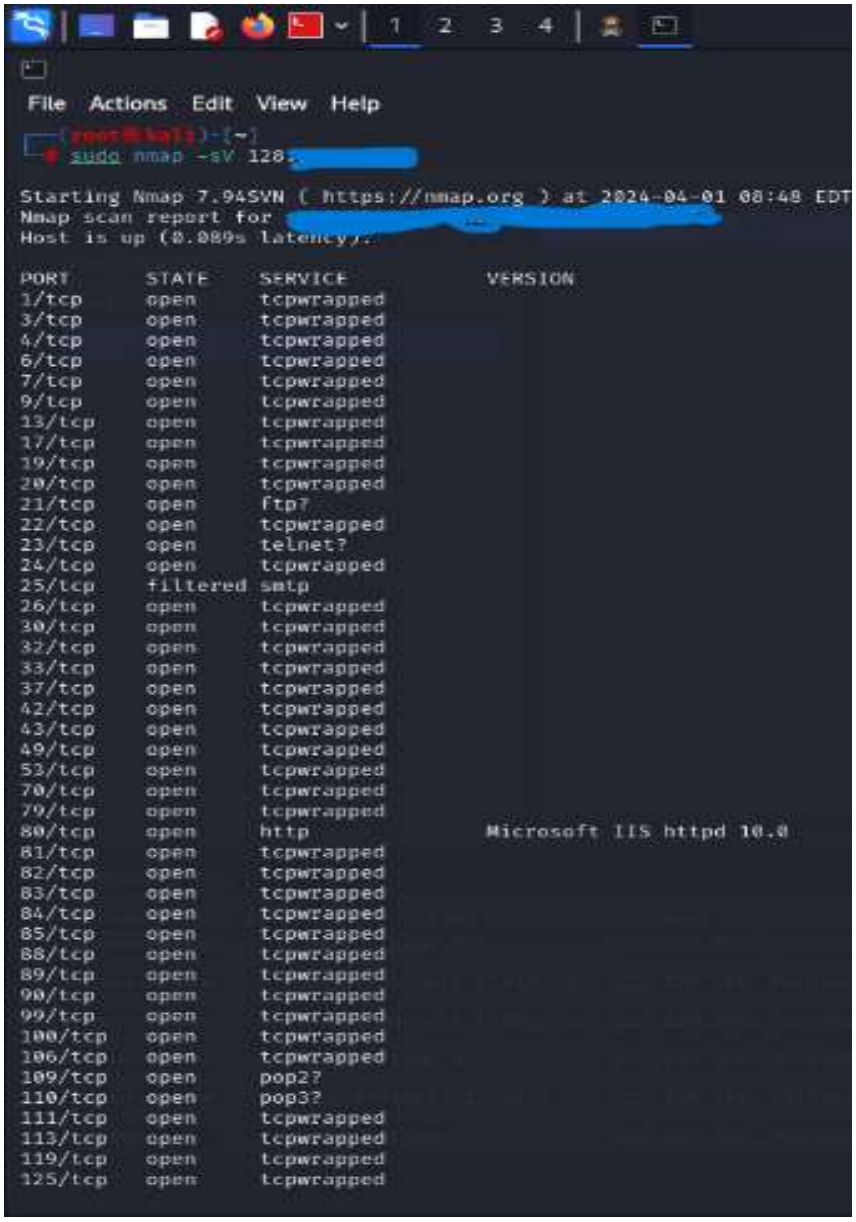
Perintah nmap -sV digunakan untuk melakukan banner grabbing. Opsi -sV memungkinkan Nmap untuk mencoba mendapatkan informasi versi dari layanan yang berjalan pada port yang dipindai. Ini membantu dalam mengetahui versi layanan yang digunakan untuk menilai keamanan dankerentanan yang terkait.

IV.2.3.4.1 *Banner Grabbing server dummy*

Gambar IV.9 Hasil Banner Grabbing pada server dummy

Setalah dilakukan scan pada gambar IV.9 ditemukan bahwasanya host memiliki 1000 port dan dari 1000 port tersebut *998 no response. Diantara port yang merespon anatara lain 445/tcp dengan state service open microsoft-ds version Microsoft Windows Server 2008 R2 - 2012 microsoft-ds dan* 139/tcp dengan state service open netbios-ssn version Microsoft Windows netbios-ssn

IV.2.3.4.2 *Banner Grabbing server production*



Gambar IV.10 Hasil Banner Grabbing pada server production

Berdasarkan banner grabbing pada server production dalam gambar IV.10 terdapat hasil antara lain, 80/tcp state open service http Version Microsoft IIS httpd 10.0 dan 3306/tcp state open service mysql version MySQL 5.5.5-10.5.4-MariaDB

IV.2.2.5 *Using TCP/IP Stack Fingerprinting*

Perintah nmap -O ini menggunakan teknik TCP/IP stack fingerprinting (-O) untuk mencoba mengidentifikasi sistem operasi dari host yang dipindai. Nmap akan mencoba menganalisis respons dari host dan membuat estimasi tentang sistem operasi yang digunakan

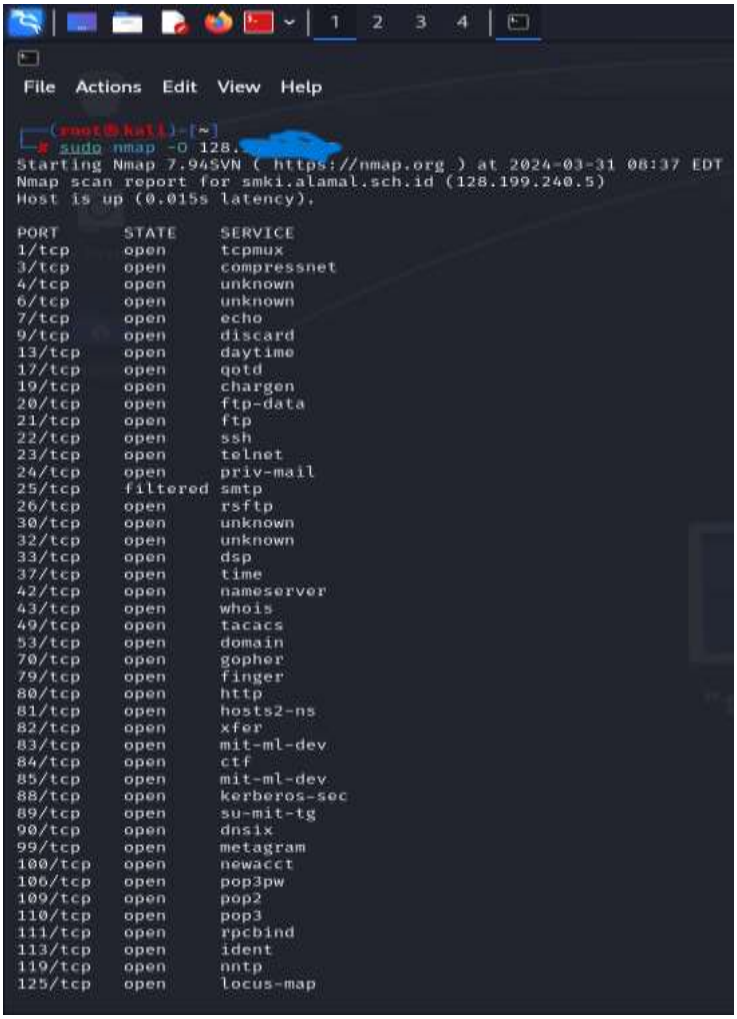
IV.2.2.5.1 *Using TCP/IP Stack Fingerprinting server dummy*

Gambar IV.11 Using TCP/IP Stack Fingerprinting pada server dummy

Berdasarkan hasil pengujian pada gambar IV.11 ditemukan 988 ports no response. Port tersebut antara *lain 80/tcp service http, 135/ tcp service msrpc, 139/tcp netbios-ssn, 445/tcp microsoft ds, 3389/tcp service ms-wbt-server dan* beberapa *port uknown* lainnya dan ditemukan presentase OS yang digunakan yaitu oracle virtual box 93%, qemu 88% bay network embedded 85%

IV.2.2.5.2 *Using TCP/IP Stack Fingerprinting server production*

sudo nmap -O 128.xxx.xxx.x



Gambar IV.12 Hasil Using TCP/IP Stack Fingerprinting pada server production

Berdasarkan hasil pengujian pada Gambar IV.12 ditemukan presentase OS yang digunakan yaitu oracle virtual box 94 qemu 91% bay network embedded 85%

IV.2.3 *Vulnerability Identification*

Vulnerability Identification adalah proses penting dalam keamanan siber yang melibatkan identifikasi dan pemahaman kelemahan dalam sistem, infrastruktur, dan sistem pendukung. Hal ini penting untuk melindungi sistem TI secara proaktif dan mencegah kerusakan potensial dari serangan. Pada pengujian kali ini *tools* yang digunakan adalah Nikto, Region dan Zap

IV.2.4.1 Nikto

IV.2.4.1.1 Penggunaan *nikto server dummy*

nikto -h 139.xxx.xxx.xx-p 8154

Nikto melakukan pemeriksaan secara umum dan spesifik terhadap tipe server tertentu. Selain itu, alat ini juga mampu menangkap dan mencetak cookie yang diterima Nikto Penggunaan nikto berfokus pada host 139.xxx.xxx.xx dan pada port 8154. Dikarenakan pada host 139.xxx.xxx.xx dan port 8154 terdapat aplikasi e raport

Gambar IV.13 Hasil Penggunaan nikto pada server dummy

Didadalam gambar IV.13 adalah + Server: Apache/2.4.55 (Win64) OpenSSL/1.1.1s PHP/8.1.23

IV.2.4.1.2 Penggunaan *nikto server production*

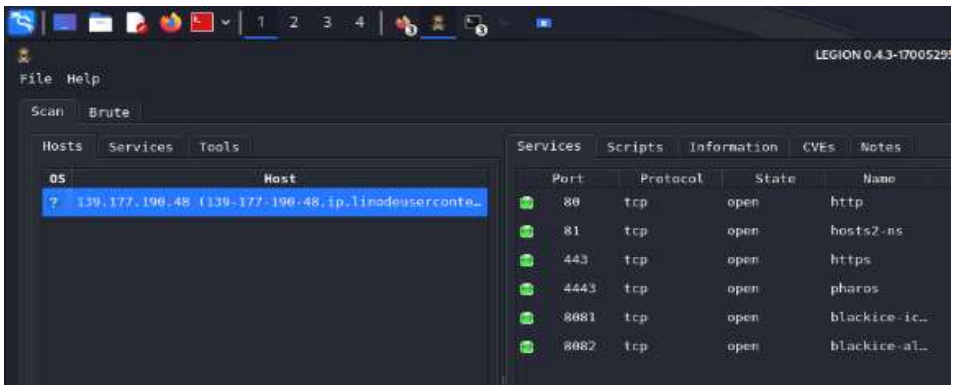
Penggunaan nikto berfokus pada host 128.xxx.xxx.x dan pada port 8154 dikarenakan pada host 8154 terdapat aplikasi e raport

Gambar IV.14 Hasil Penggunaan nikto pada server production

Hasil pada Gambar IV.14 hasil Penggunaan nikto pada server production adalah + Server: Apache/2.4.55 (Win64) OpenSSL/1.1.1s PHP/8.1.23

IV.2.4.2 Legion

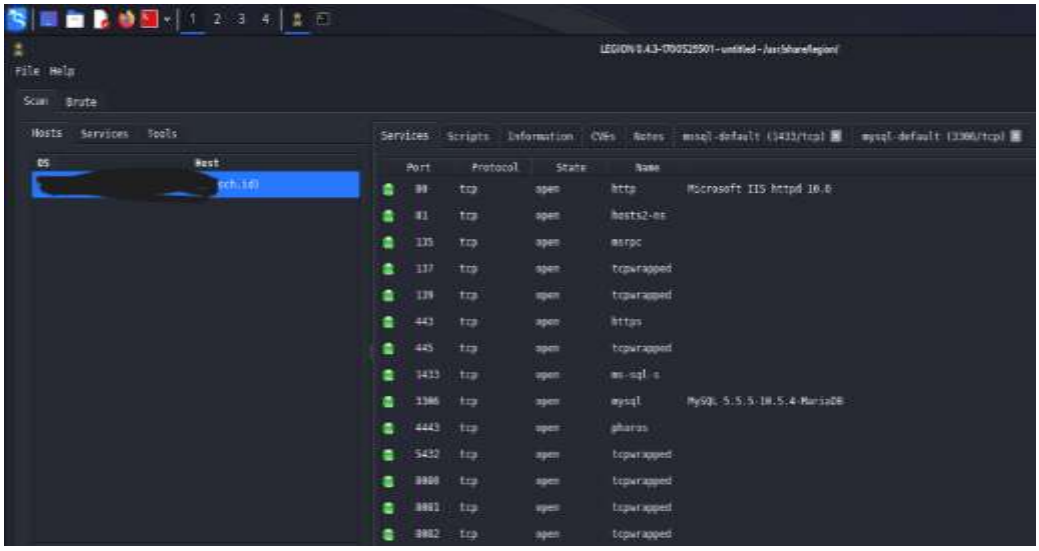
iV.2.4.2.1 *Scan region server dummy*



Gambar IV.15 Hasil Scan region pada server dummy

Setelah dilakukan *scanning* oleh tools region pada Gambar IV.15 adalah *open port* 80/tcp dengan *service http*, open port 81/tcp dengan *service host2ns*,*open port* 443/tcp dengan *service https*, *open port* 4443/tcp dengan *service pharros*. Selain itu *tools region* menemukan bahwa *operating system* yang digunakan kemungkinan adalah 3com 4500G switch dengan akurasi sebesar 93%

IV.2.4.2.1 *Scan Region Pada server Production*



Gambar IV.16 Hasil Scan Region Pada server Production

Berdasarkan scanning menggunakan region pada server production pada Gambar IV.16 terdapat hasil antara lain, 80/tcp s*tate open service http version* Microsoft IIS httpd 10.0, 3306/tcp *state open service* mysql *version* MySQL 5.5.5-

10.5.4-MariaDB, 1433/tcp *state open service* mysql. Selain itu tools region menemukan bahwa operating system yang digunakan kemungkinan adalah *oracle virtual box* dengan akurasi sebesar 92

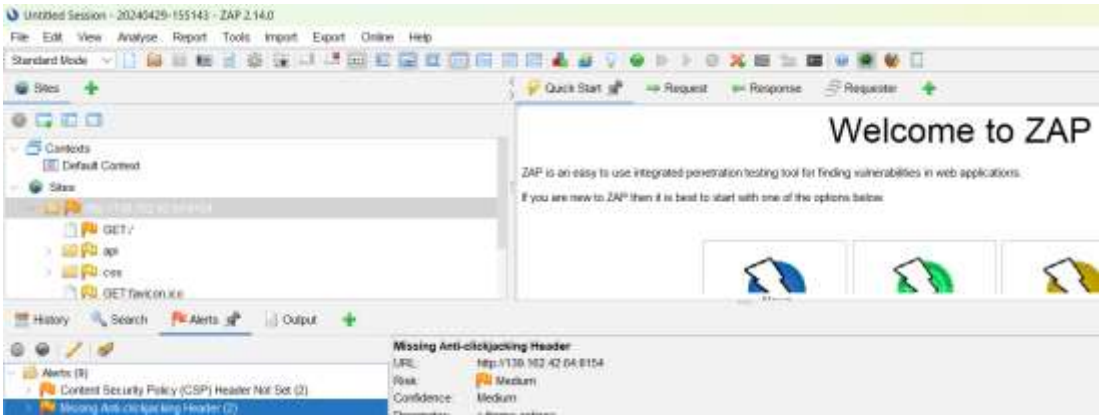
iV.2.4.3 Zap

iV.2.4.3.1 Penggunaan zap pada server dummy

IV.2.4.3.1.1 Celah keamanan medium

Gambar IV.17 Hasil Scan Zap pada server dummy

Berdasarkan Gambar IV.17 Tidak terdapat *CSP (Content-Security-Policy). CSP* adalah lapisan yang ditambahkan pada HTTP response header yang berfungsi untuk mencegah serangan tertentu termasuk XSS Solusinya adalah pastikan server web, server aplikasi, load balancer, dll. dikonfigurasi untuk mengatur header Content-Security-Policy



Gambar IV.18 Hasil Scan Zap pada server dummy

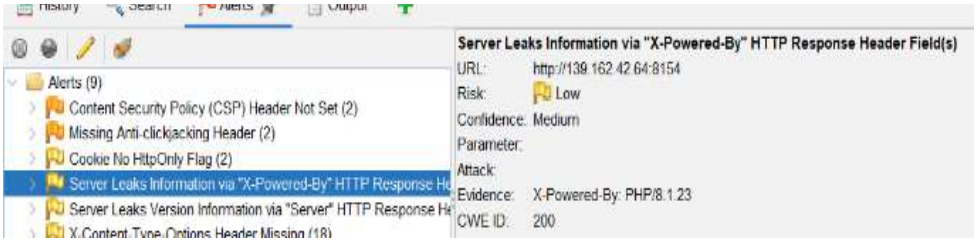
Berdasarkan Gambar IV.18 Wesite tidak ada bisa terlindungi oleh serangan *click-jacking*.Singkatnya serangan click jacking berkerja dengan cara mengelabui

pengguna dengan menyisipkan elemen transparan pada elemen HTML Solusinya adalah pastikan website telah mendukung *HTTP Content-Security-Policy dan X-Frame-*

IV.2.4.3.1.2 Celah keamanan Low

Gambar IV.19 Hasil Scan Zap pada server dummy

Berdasarkan Gambar IV.19 Wesite menerapkan cookie tanpa httponly flag yang berdungsi sebagai pelapis keamanan website, apabila tidak menginstalnya sementara browser mengisntalnya maka cookie akan diakses dari pengguna. Namun apabila sebaliknya maka cookie dari website akan diabaikan dan akan rentan terhadap serangan xss. Solusinya dengan memastikan Http only flag telah terinstal



Gambar IV.20 Hasil Scan Zap pada server dummy

Berdasarkan Gambar IV.20 Wesite membocorkan informasi melalui renspon header HTTP "X-Powered-By" HTTP “X-Powered-By” adalah bagian dari respons standar yang disertakan oleh server web dalam tanggapannya. Header ini mengandung informasi tentang teknologi atau perangkat lunak yang digunakan oleh server. Namun, masalahnya adalah header ini juga dapat mengungkapkan informasi sensitif tentang konfigurasi server, yang dapat dieksploitasi oleh penyerang. Soluinya adalah Pastikan server web, server aplikasi, load balancer, dll. dikonfigurasi

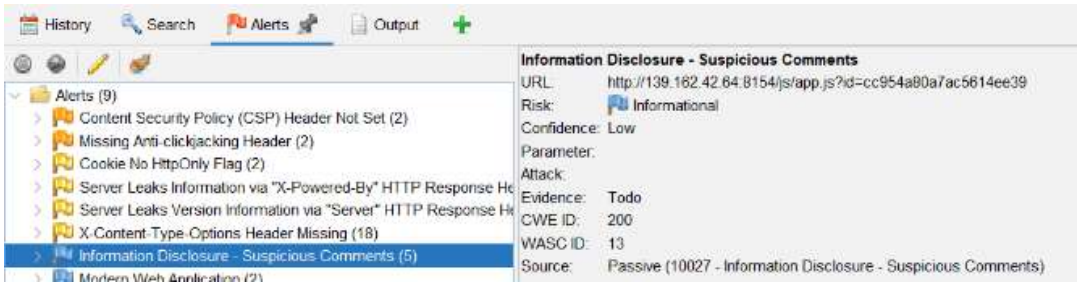
Gambar IV.21 Hasil Scan Zap pada server dummy

Berdasarkan Gambar IV.21 Website membocorkan informasi melalui http server Header respon Kode Respons HTTP adalah sekumpulan kode numerik tiga digit yang dikembalikan oleh server web sebagai respons terhadap permintaan HTTP yang dibuat oleh klien (biasanya browser web atau aplikasi lain). Kode status ini disertakan dalam header respons dari respons HTTP untuk memberikan informasi tentang hasil permintaan . Solusinya dengan konfirmasi server web, server aplikasi, load balancer, dll.

Gambar IV.22 Hasil Scan Zap pada server dummy

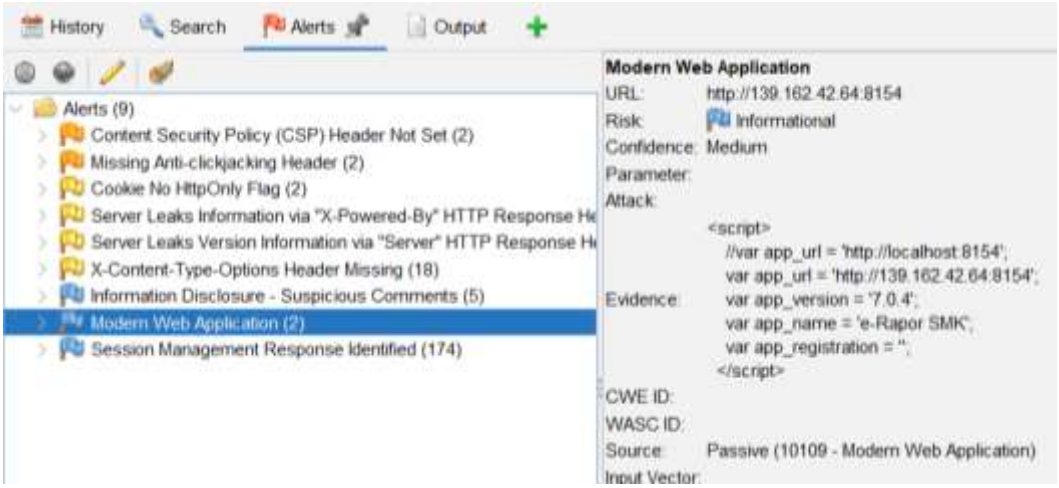
Berdasarkan Gambar IV.22 Header Anti-MIME-Sniffing X-Content-Type-Options tidak diatur ke 'nosniff'. Header respon HTTP “X-Content-Type-Options” adalah bagian dari respons yang dikirim oleh server web ke browser. Header ini memiliki nilai yang dapat diatur, salah satunya adalah “nosniff”. Dengan mengatur header ini, Anda memastikan bahwa tipe konten yang dinyatakan dalam header Content-Type benar-benar browser tidak melakukan MIME (Multipurpose Internet Mail Extensions) Dimana browser menebak paket yang dikirimkan Solusinya adalah Pastikan bahwa aplikasi/server web menetapkan header Content-Type dengan tepat, dan menetapkan header X-Content-Type-Options ke 'nosniff' untuk semua halaman web.

IV.2.4.3.1.3 Celah keamanan Informational



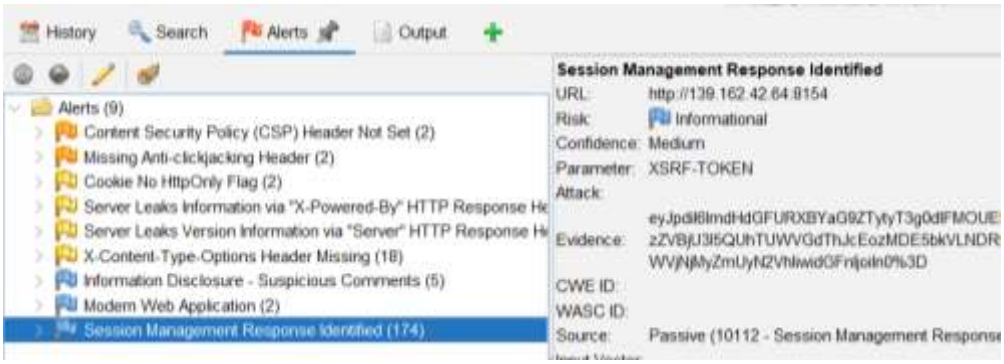
Gambar IV.23 Hasil Scan Zap pada server dummy

Berdasarkan Gambar IV.23 Respons tampaknya berisi komentar mencurigakan yang dapat membantu penyerang. Solusinya adalah Hapus semua komentar yang mengembalikan informasi yang dapat membantu penyerang



Gambar IV.24 Hasil Scan Zap pada server dummy

Berdasarkan Gambar IV.24 Merupakan hasil scan dari *tool* zap dengan alert yang bsersifat informational, Dimana risk tersebut bukan kerentanan sehingga tidak ada yang perlu diperbaiki



Gambar IV.24 Hasil Scan Zap pada server dummy

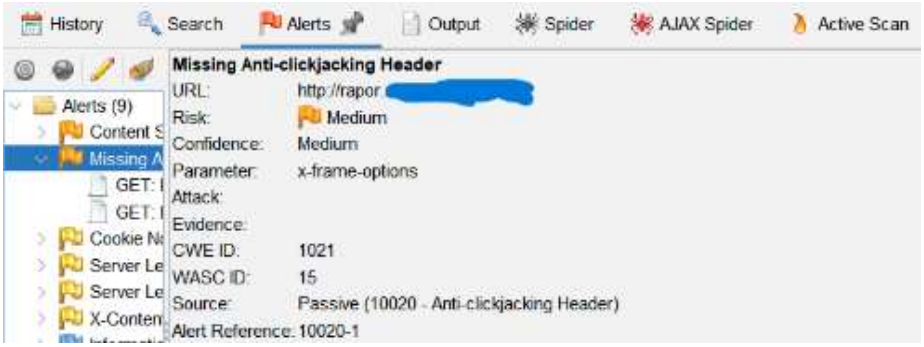
Respons tersebut tampaknya berisi komentar mencurigakan yang dapat membantu penyerang. Catatan: Kecocokan yang dibuat dalam blok skrip atau file bertentangan dengan keseluruhan konten, bukan hanya komentar. Solusinya adalah Hapus semua komentar yang mengembalikan informasi yang dapat membantu penyerang dan memperbaiki masalah mendasar yang mereka rujuk.

IV.2.4.3.2 Penggunaan zap pada server production

IV.2.4.3.2.1 Celah keamanan Medium

Gambar IV.25 Hasil Scan Zap pada server production

Berdasarkan Gambar IV.25 Tidak terdapat *CSP (Content-Security-Policy). CSP* adalah lapisan yang ditambahkan pada HTTP response header yang berfungsi untuk mencegah serangan tertentu termasuk XSS Solusinya adalah pastikan server web, server aplikasi, load balancer, dll. dikonfigurasi untuk mengatur header Content-Security-Policy



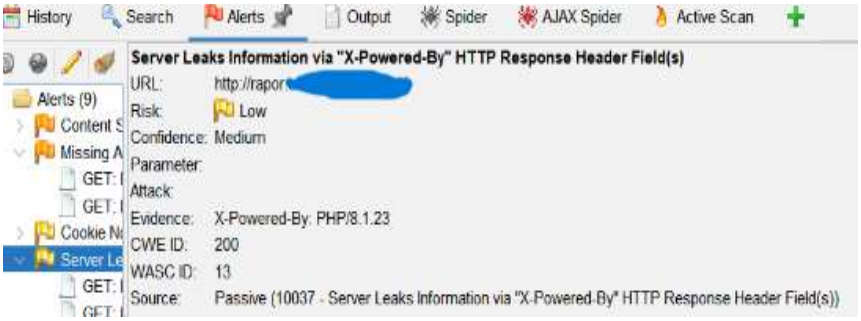
Gambar IV.35 Hasil Scan Zap pada server production

Berdasarkan Gambar IV.35 Wesite tidak ada bisa terlindungi oleh serangan *click-jacking*.Singkatnya serangan click jacking berkerja dengan cara mengelabui pengguna dengan menyisipkan elemen transparan pada elemen HTML Solusinya adalah pastikan website telah mendukung *HTTP Content-Security-Policy dan X-Frame-*

IV.2.4.3.2.2 Low

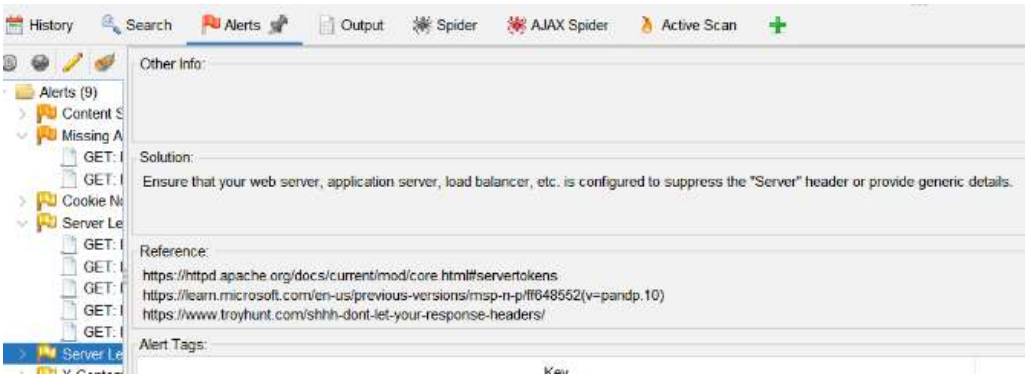
Gambar IV.26 Hasil Scan Zap pada server production

Berdasarkan Gambar IV.26 Wesite menerapkan cookie tanpa httponly flag yang berdungsi sebagai pelapis keamanan website, apabila tidak menginstalnya sementara browser mengisntalnya maka cookie akan diakses dari pengguna. Namun apabila sebaliknya maka cookie dari website akan diabaikan dan akan rentan terhadap serangan xss. Solusinya dengan memastikan Http only flag telah terinstal



Gambar IV.27 Hasil Scan Zap pada server production

Berdasarkan Gambar IV.27 Wesite membocorkan informasi melalui renspon header HTTP "X-Powered-By" HTTP “X-Powered-By” adalah bagian dari respons standar yang disertakan oleh server web dalam tanggapannya. Header ini mengandung informasi tentang teknologi atau perangkat lunak yang digunakan oleh server. Namun, masalahnya adalah header ini juga dapat mengungkapkan informasi sensitif tentang konfigurasi server, yang dapat dieksploitasi oleh penyerang. Soluinya adalah Pastikan server web, server aplikasi, load balancer, dll. Dikonfigurasi



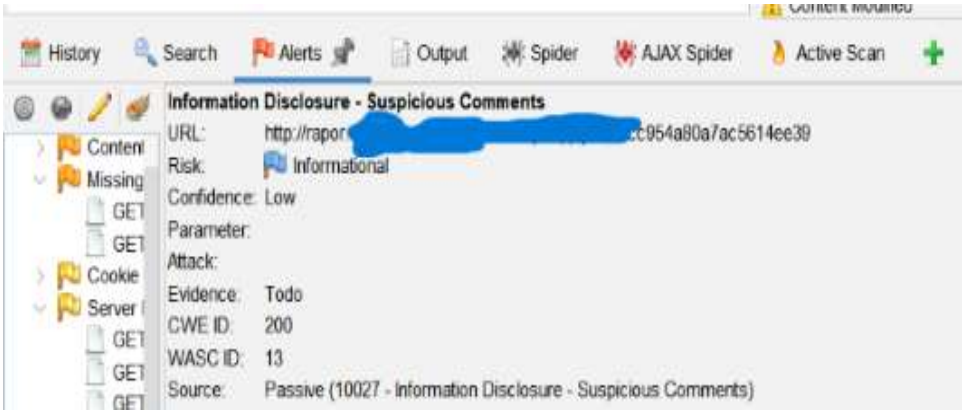
Gambar IV.28 Hasil Scan Zap pada server production

Berdasarkan Gambar IV. 28 Website membocorkan informasi melalui http server. Kode Respons HTTP adalah sekumpulan kode numerik tiga digit yang dikembalikan oleh server web sebagai respons terhadap permintaan HTTP yang dibuat oleh klien (biasanya browser web atau aplikasi lain). Kode status ini disertakan dalam header respons dari respons HTTP untuk memberikan informasi tentang hasil permintaan .Solusinya dengan konfirmasi server web, server aplikasi, load balancer, dll.

Gambar IV.29 Hasil Scan Zap pada server production

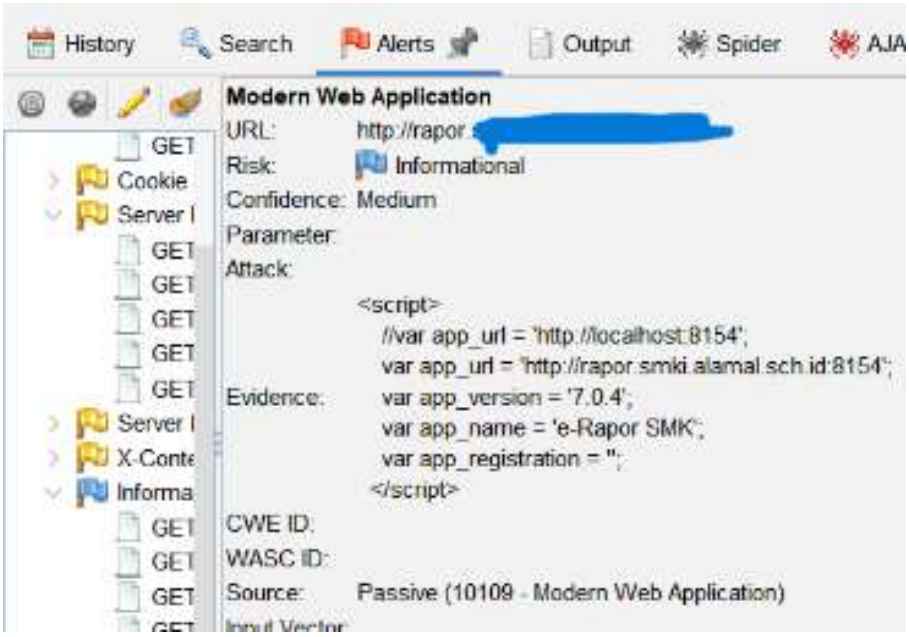
Berdasarkan Gambar IV.31 Header Anti-MIME-Sniffing X-Content-Type-Options tidak diatur ke 'nosniff'. Header respon HTTP “X-Content-Type-Options” adalah bagian dari respons yang dikirim oleh server web ke browser. Header ini memiliki nilai yang dapat diatur, salah satunya adalah “nosniff”. Dengan mengatur header ini, Anda memastikan bahwa tipe konten yang dinyatakan dalam header Content-Type benar-benar browser tidak melakukan MIME (Multipurpose Internet Mail Extensions) Dimana browser menebak paket yang dikirimkan Solusinya adalah Pastikan bahwa aplikasi/server web menetapkan header Content-Type dengan tepat, dan menetapkan header X-Content-Type-Options ke 'nosniff' untuk semua halaman web.

IV.2.4.3.2.3 Celah keamanan Informational



Gambar IV.30 Hasil Scan Zap pada server production

Berdasarkan Gambar IV.30 Respons tampaknya berisi komentar mencurigakan yang dapat membantu penyerang. Solusinya adalah Hapus semua komentar yang mengembalikan informasi yang dapat membantu penyerang

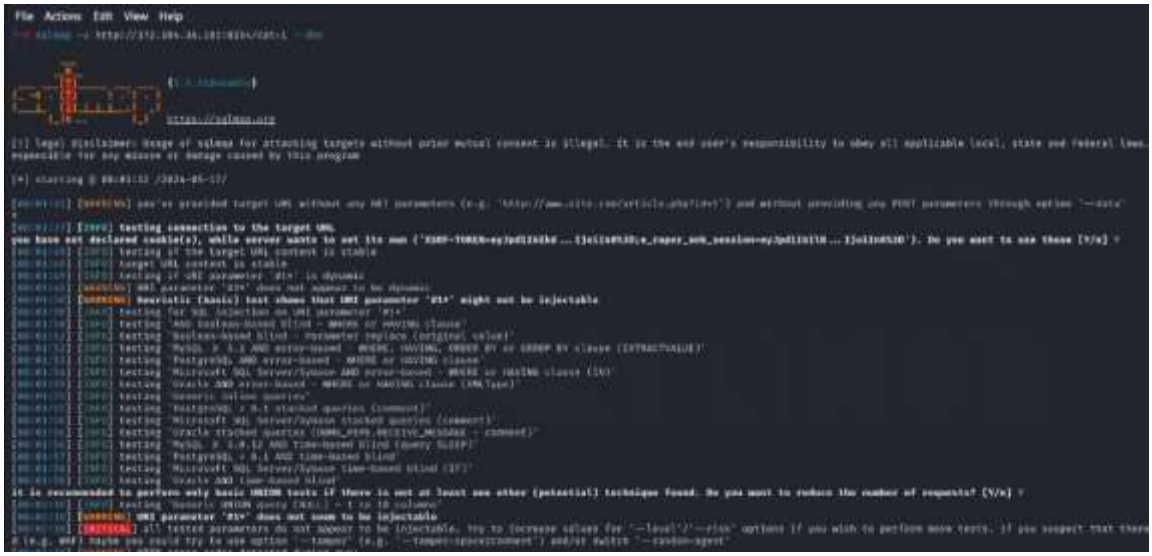


Gambar IV.31 Hasil Scan Zap pada server production

Berdasarkan Gambar IV.31 Merupakan hasil scan dari *tool* zap dengan alert yang bersifat informational, Dimana risk tersebut bukan kerentanan sehingga tidak ada yang perlu diperbaiki

IV.2.4 *Penetration Testing*

Kita harus memasukkan url web yang ingin kita periksa bersama dengan parameter -u. Kita juga dapat menggunakan parameter -tor jika kita ingin menguji situs web menggunakan proxy. Biasanya, kita ingin menguji apakah kita bisa mendapatkan akses ke database. Jadi, kita menggunakan opsi -dbs untuk melakukannya. -dbs mencantumkan semua basis data yang ada. referensi/peserta-didik-aktif?status=aktif, cat=1 dan grep=1 merupakan parameter yang akan dilakukan pengujian



Gambar IV.32 Hasil Penetration testing

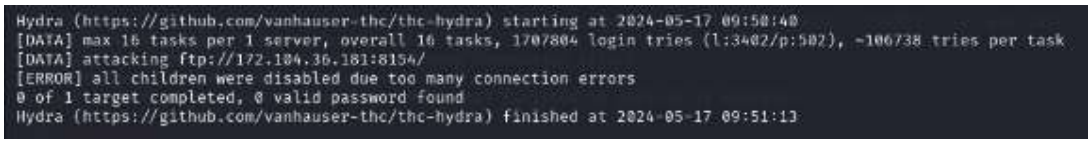
Setelah dilakukan penetration testing yang menggunakan tools sqlmap ditunjkkan pada Gambar IV.32 terdapat hasil *all parameter do not appear to be injectable.* Hasil ini terjadi dikarenakan semua database telah dilindugi dengan baik

IV.2.5 *Gaining Access and Privilege Escalation*

Dalam serangan *privilege escalation,* peretas memanfaatkan kerentanan dalam kontrol akses dan pembatasan sumber daya untuk mengesampingkan izin dan batasan dari akun pengguna target untuk mendapatkan akses yang lebih tinggi.

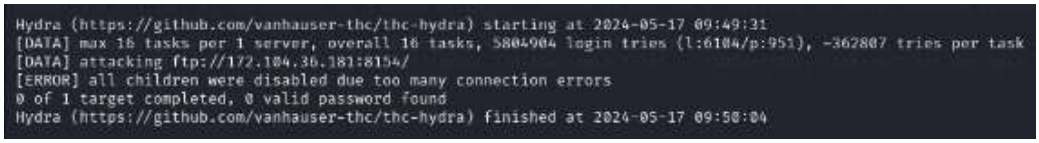
IV.2.5.1 Hydra

Tools Hydra dan penguji menggunakan 5 wordlist yang berisi gmail dan password yang bersumber dari github



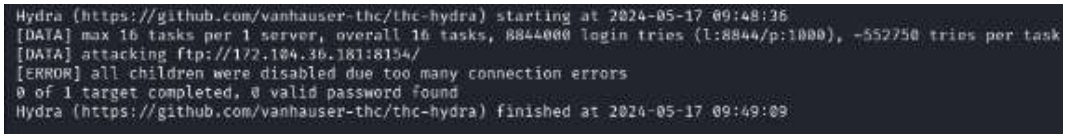
Gambar 4.33 Hasil Gaining Access and *Privilege Escalation* menggunakan Hydra

Proses Scaaning menggunakan hydra dengan mencoba berbagai dataset berupa wordlist 5 yang berisi username dan password menggunakan tool hydra sudah selesai dilakukan, Berdasarkan Gambar IV.33 hasilnya adalah tidak terdapat username dan password yang sesuai.



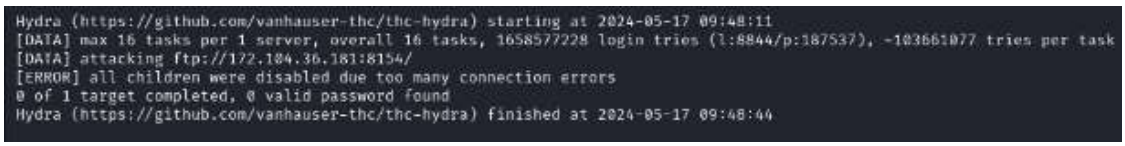
Gambar IV.34 Hasil Gaining Access and *Privilege Escalation* menggunakan Hydra

Proses Scaaning menggunakan hydra dengan mencoba berbagai dataset berupa file wordlist 4 yang berisi username dan password menggunakan tool hydra sudah selesai dilakukan, Berdasarkan Gambar IV.34 hasilnya adalah tidak terdapat username dan password yang sesuai



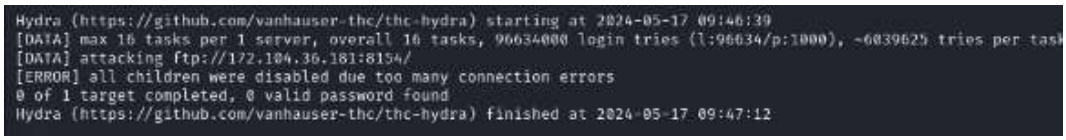
Gambar IV.35 Hasil Gaining Access and *Privilege Escalation* menggunakan Hydra

Proses Scaaning menggunakan hydra dengan mencoba berbagai dataset berupa file wordlist 3 yang berisi username dan password menggunakan tool hydra sudah selesai dilakukan, Berdasarkan Gambar IV.35 hasilnya adalah tidak terdapat username dan password yang sesuai



Gambar IV.36 Hasil Gaining Access and *Privilege Escalation* menggunakan Hydra

Proses Scaaning menggunakan hydra dengan mencoba berbagai dataset berupa file wordlist 2 yang berisi username dan password menggunakan tool hydra sudah selesai dilakukan, Berdasarkan Gambar IV.36 hasilnya adalah tidak terdapat username dan password yang sesuai.



4.37 Hasil Gaining Access and *Privilege Escalation* menggunakan Hydra

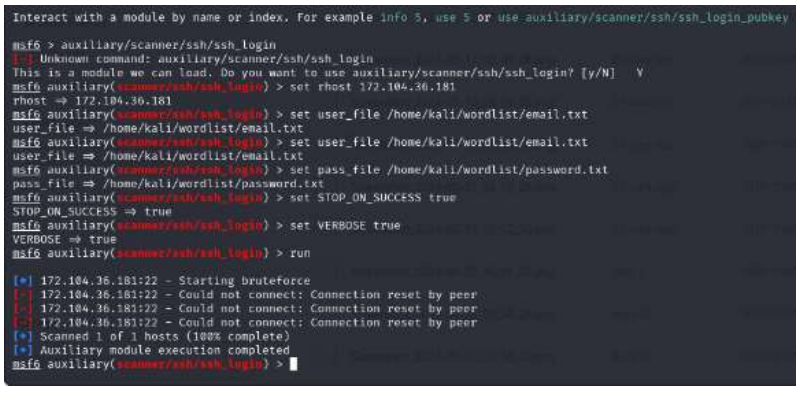
Proses Scaaning menggunakan hydra dengan mencoba berbagai dataset berupa file wordlist 1 yang berisi username dan password menggunakan tool hydra sudah selesai dilakukan, Berdasarkan Gambar IV.37 hasilnya adalah tidak terdapat username dan password yang sesuai.

IV.2.5.2 *Nmap*

Gambar IV.38 Hasil Gaining Access and *Privilege Escalation* menggunakan Nmap

Berdasarkan Gambar IV.38 hasilnya adalah menggunakan nmap tidak ada hasil atau informasi yang diperoleh

IV.2.5.1 *Metsploit*



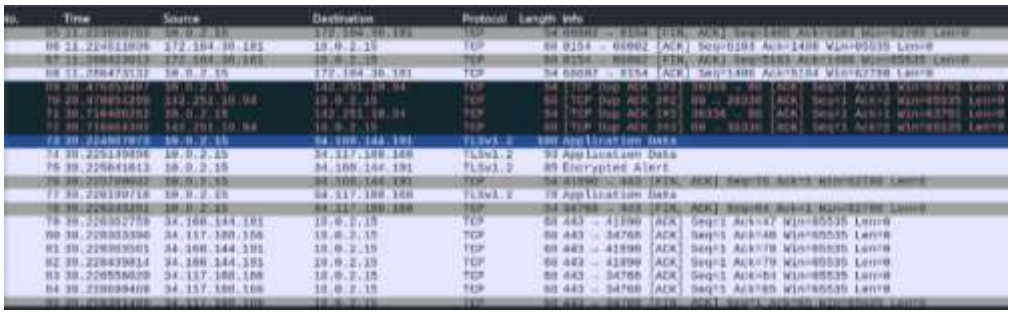
Gambar IV.39 Gaining Access and *Privilege Escalation* menggunakan metasploit

Setelah menggunakan tools Metasploit dengan mencoba berbagai dataset berupa file wordlist 1 yang berisi username dan password ynag sama dengan yang

digunakan pada tool hydra yang sudah selesai dilakukan,.Dalam Gambar IV.39 ditemukan kegagalan. Kegagalan tersebut dkarena faktor yang terhalang oleh firewall yang ada pada server

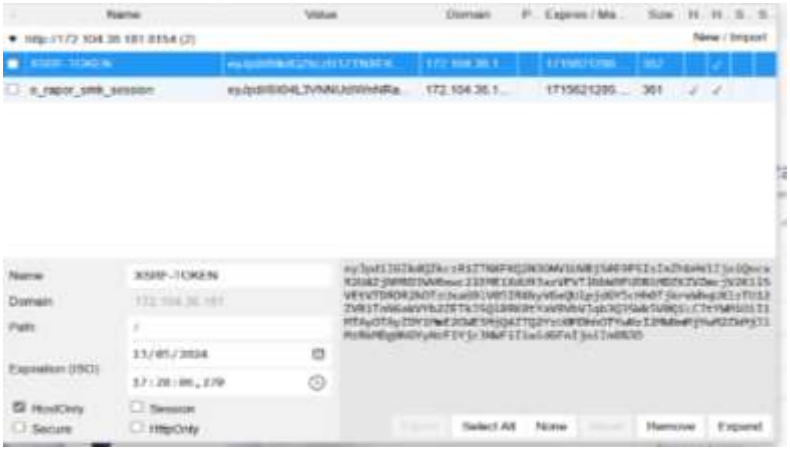
IV.2.6 *Enumerating Further*

Setelah proses enumeration awal, penyerang dapat menggunakan informasi yang ditemukan untuk melakukan enumerating further, yaitu mengumpulkan informasi lebih lanjut tentang sistem atau jaringan. Pada Pengujian ini menggunakan cookie manager dan wireshark sebagai tools untuk Enumerating Further

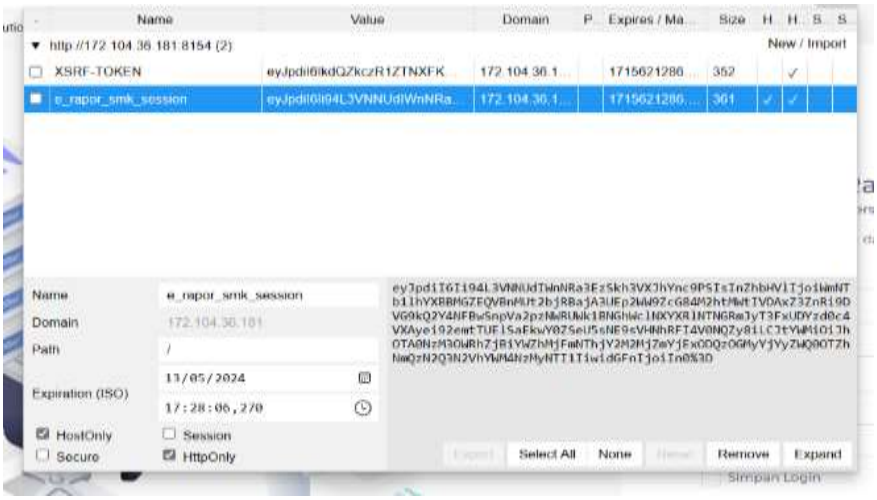


Gambar IV.40 Hasil Enmurating Futher menggunkan wireshark

Setelah melakukan login user yang ditunjukkan oleh Gambar IV.40, wireshark otomatis langsung merekam data yang dikirim melalui jaringan komputer. Namun berdasarkan hasil dari rekaman data tidak terdapat data username dan password dalam jaringan. Dikarenakan website sudah di enkripsi oleh TLS 1.3. maka tidak ada data username dan password yang terekam oleh wireshark



Gambar IV.41 a Hasil Enmurating Futher menggunkan cookie manager



Gambar IV.41 b Hasil *Enumerating Futher* menggunkan cookie manager

Dengan menggunakan tool cookie manager dalam Gambar IV.41 a dan b yang dapat menyimpan hasil cookie. Untuk Gambar IV.41 a terdapat cookie bernama XSRF token. Sedangkan untuk Gambar IV.41 b terdapat cookie bernama e_raport_smk_session. Hasil cookie tersebut tujuan mengingat informasi otentikasi seperti username dan password agar dapat untuk login dengan mudah tanpa meng-input kredensial setiap kali login. Setekah disimpan menggunakan tools cookie manager, selanjutnya mencoba login dengan hasil cookie yang disipan dan tidak bisa melakukan login menggunakan cookie yang disimpan oleh cookie manager

IV.2.7 *Compromise Remote User/Sites*

"*Compromise Remote User/Sites*" dalam bahasa Indonesia dapat diartikan sebagai "Kompromi Pengguna/Situs Remote". Istilah ini merujuk pada situasi di mana pengguna atau situs remote mengalami kompromi keamanan, yang dapat mengakibatkan akses yang tidak sah atau penyalahgunaan sistem. Kompromi semacam ini dapat terjadi melalui berbagai metode, termasuk serangan siber yang bertujuan untuk mendapatkan akses yang tidak sah ke sistem atau situs remote. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan.

IV.2.8 *Maintaning Access*

Upaya untuk tetap terhubung ke suatu sistem atau jaringan setelah berhasil mendapatkan akses yang tidak sah. Ini dapat terjadi dalam konteks keamanan siber,

manajemen akses fisik, atau pengendalian akses ke sistem komputer. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan.

IV.2.9 *Corvering Tracks*

Merujuk pada serangkaian tindakan yang dilakukan oleh penyerang setelah berhasil melakukan serangan untuk menghapus atau menyembunyikan jejak-jejak yang dapat digunakan untuk melacak atau mendeteksi kehadiran mereka. Tindakan ini bertujuan untuk mengurangi kemungkinan deteksi dan identifikasi penyerang serta mempersulit upaya penyelidikan. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan.

IV.3 Hasil Temuan dan Rekomendasi

Dari hasil dan pengujian yang telah di cantumkan pada bab 4.3 hingga bab 4.5 terdapat hasil dan rekomendasi antara lain:

IV.3.1 Hasil dan rekomendasi pada server dummy

Tabel IV.1 Hasil dan rekomendasi pada server dummy

Asesment	***Tools***	**Rangkuman Hasil**	***Impact***	**Saran**
Information Gathering	*Shodan, Censys*	Ditemukan spesifikasi *website* PPDB sekolah XYZ, seperti: Alamat ip adalah 139.xxx.xxx.xx, memiliki port 22, 135, 445,3389,5985,8181 Operating system Windows Server 2012 R2 Standard 9600	Berdasarkan informasi awal tersebut penyerang bisa melakukan ekplotasi lebih lanjut	-
Network Mapping	*Nmap*	host memiliki 1000 port dan dari 1000 port tersebut *998 no response. Diantara port yang merespon anatara lain* port 80/tcp dengan sevice http, open port 135/tcp dengan	Informasi megenai port terbuka yang diperoleh dari alat pemindaian nmap sangat berisiko karena	Menerapkan *intrusion detection system* (IDS) untuk mendeteksi adanya serangan seperti *port*

Asesment	*Tools*	Rangkuman Hasil	*Impact*	Saran
		service msrpc,open port 139/tcp dengan service netbios-ssn, open port 445/tcp dengan service microsoft-ds, open port 3389/tcp dengan service ms-wbt-server. Selain itu ditemukan beberapa port dengan service uknown. Selain itu *445/tcp dengan state service open microsoft-ds version Microsoft Windows Server 2008 R2 - 2012 microsoft-ds dan* 139/tcp dengan state service open netbios-ssn version Microsoft Windows netbios-ssn. Selanjutnya, ditemukan 988 ports no response dan ditemukan presentase OS yang digunakan yaitu oracle virtual box 93%, qemu 88% bay network embedded 85%	beberapa port tersebut dapat dimanfaatkan oleh hacker untuk melakukan serangan (Suta Sanjaya, 2020).	*scan* (Sutarti, et al 2018).

Vulnerability Identification	*Nikto*	Ditemukan spesifikasi mengenai versi server, SSL, dan PHP. Riciannya adalah Server: Apache/2.4.55 (Win64) OpenSSL/1.1.1s PHP/8.1.23	Informasi mengenai spesifikasi versi server, SSL, dan PHP, dapat dieksploitasi oleh hacker	Lakukan update terbaru untuk setiap versi server, SSL, dan PHP untuk meningkatkan keamanan dari level sebelumnya
	Region	Ditemukan detail mengenai port beserta service dan kemungkinan operating sistem yang digunakan Riciannya berada adalah *open port* 80/tcp dengan *service http*, open port 81/tcp dengan *service host2ns,open port* 443/tcp dengan *service https, open port* 4443/tcp dengan *service pharros*. Selain itu *tools region* menemukan bahwa *operating system* yang digunakan kemungkinan adalah 3com 4500G switch dengan akurasi sebesar 93%	Informasi mengenai port terbuka yang diperoleh dari alat pemindaian region sangat berisiko karena beberapa port tersebut dapat dimanfaatkan oleh hacker untuk melakukan serangan (Suta Sanjaya, 20200.	Menerapkan *intrusion detection system* (IDS) untuk mendeteksi adanya serangan seperti *port scan* (Sutarti, et al 2018).
	Zap	Ditemukan berbagai kerentanan mulai dari medium hingga informational. Riciannya dari risk medium adalah: Tidak terdapat *CSP (Content-Security-Policy).*	*CSP* adalah lapisan yang ditambahkan pada HTTP response	Solusinya adalah Solusinya

			header yang berfungsi untuk mencegah serangan tertentu termasuk XSS	adalah pastikan server web, server aplikasi, load balancer, dll. dikonfigurasi untuk mengatur header *Content-Security-Policy*
		Selanjutnya, *Website* tidak ada bisa terlindungi oleh serangan *click-jacking*	Singkatnya serangan click jacking berkerja dengan cara mengelabui pengguna dengan menyisipkan elemen transparan pada elemen HTML	Solusinya adalah pastikan website telah mendukung *HTTP Content-Security-Policy dan X-Frame-*
		Selain itu rincian dari risk low antara lain: *Website* menerapkan cookie tanpa httponly flag yang berdungsi sebagai pelapis keamanan website, apabila tidak menginstalnya sementara browser mengisntalnya maka cookie akan diakses dari pengguna. Namun apabila sebaliknya maka cookie dari website akan diabaikan dan *Website* membocorkan informasi melalui renspon header	Rentan terhadap serangan xss. Namun, masalahnya adalah header ini juga dapat	Solusinya dengan memastikan Http only flag telah terinstal Soluinya adalah Pastikan

		HTTP "X-Powered-By" HTTP "X-Powered-By" adalah bagian dari respons standar yang disertakan oleh server web dalam tanggapannya. Header ini mengandung informasi tentang teknologi atau perangkat lunak yang digunakan oleh server.	mengungkapkan informasi sensitif tentang konfigurasi server, yang dapat dieksploitasi oleh penyerang.	server web, server aplikasi, load balancer, dll. Dikonfigurasi
		Website membocorkan informasi melalui http server Header respon Kode Respons HTTP. Kode Respons HTTP adalah sekumpulan kode numerik tiga digit yang dikembalikan oleh server web sebagai respons terhadap permintaan HTTP yang dibuat oleh klien (biasanya browser web atau aplikasi lain).	Kode status ini disertakan dalam header respons dari respons HTTP untuk memberikan informasi tentang hasil permintaan	Solusinya dengan konfirmasi server web, server aplikasi, load balancer, dll.
		Header Anti-MIME-Sniffing X-Content-Type-Options tidak diatur ke 'nosniff'. Header respon HTTP "X-Content-Type-Options" adalah bagian dari respons yang dikirim oleh server web ke browser.	Dengan mengatur header ini, Anda memastikan bahwa tipe konten yang dinyatakan dalam header Content-Type benar-benar browser tidak melakukan MIME (Multipurpose Internet Mail Extensions). Dimana	Solusinya adalah Pastikan bahwa aplikasi/server web menetapkan header Content-Type dengan tepat, dan menetapkan

			browser menebak paket yang dikirimkan	header X-Content-Type-Options ke 'nosniff' untuk semua halaman web.
		Rincian dari risk *informational* adalah: Respons tampaknya berisi komentar mencurigakan yang dapat membantu penyerang. Merupakan hasil scan dari *tool* zap dengan alert yang bersifat informational, Respons tersebut tampaknya berisi komentar mencurigakan yang dapat membantu penyerang.	 Dapat membantu penyerang Dimana risk tersebut bukan kerentanan Dapat membantu penyerang	 Solusinya adalah hapus semua komentar. Tidak ada yang perlu diperbaiki Solusinya adalah hapus semua komentar.
Penetration Testing	*SQL MAP*	Berdasarkan hasil pengujian yang termuat dalam sub-bab 4.2.4 Terdapat hasil *all parameter do not appear to be injectable*	Hasil ini terjadi dikarenakan semua database telah dilindugi dengan baik.	-
Gaining Access and Privilege Escalation	*Hydra*	Berdasarkan hasil yang sudah dilakukan didalam sub bab 4.2.5.1,	-	-

		hasilnya adalah tidak terdapat username dan password yang sesuai.		
	Nmap	Berdasarkan hasil yang sudah dilakukan didalam sub bab 4.2.5.2, hasilnya adalah tidak terdapat username dan password yang sesuai	-	-
	Metasploit	Berdasarkan hasil yang sudah dilakukan didalam sub bab 4.2.5.3, hasilnya adalah tidak terdapat username dan password yang sesuai	-	-
Enumerating Further	*Wireshark*	Berdasarkan hasil pengujian yang berada pada sub bab 4.2.6 berhasil merekam data lalu lintas menggunakan wireshark. Namun tidak mendapatkan informasi username dan password karena protokol TLS yang digunakan sudah versi terbaru.	Penyerang tidak dapat langsung mengakses dengan mencuri username dan password dari paket data yang terdeteksi oleh wireshark.	
	Cookie Manager	Berdasarkan hasil pengujian yang berada pada sub bab 4.2.6 Setekah disimpan menggunakan tools cookie manager, selanjutnya mencoba login dengan hasil cookie yang disipan dan tidak bisa	Dalam konteks ini, penyerang tidak dapat masuk ke akun tanpa memasukkan informasi login, meskipun cookies telah disimpan di pengelola cookies.	

		melakukan login menggunakan cookie yang disimpan oleh cookie manager		
Compromise Remote User/Sites	-	Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik		
Maintaning Access	-	Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik		
Corvering Tracks	-	Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik		

IV.3.2 Hasil dan rekomendasi pada server production

Tabel IV.2 Hasil dan rekomendasi pada server dummy

Aseesment	*Tools*	Rangkuman Hasil	*Impact*	Saran
Information Gathering	*Shodan, Censys*	Ditemukan spesifikasi *website* PPDB sekolah XYZ, seperti: Reverse DNS : xxx.xxxxxx.sch.id, Routing: 128.xxx.xxx.x/xx via DIGITALOCEAN-ASN, US (AS14061) OS: Microsoft Windows Services (5): 80/HTTP, 3306/MYSQL, 8154/HTTP, 8212/RDP, 8331/SSH	Berdasarkan informasi awal tersebut penyerang bisa melakukan ekplotasi lebih lanjut	-
Network Mapping	*Nmap*	Ditemukan 1000 port yang terbuka dan merespon atara lain adalah open port 80/tcp dengan sevice http, open port 3306/tcp mysql. 80/tcp state open service http Version Microsoft IIS httpd 10.0 dan 3306/tcp state open service mysql version MySQL 5.5.5-10.5.4-MariaDB ditemukan presentase OS yang digunakan yaitu oracle virtual box 94 qemu 91% bay	Informasi megenai port terbuka yang diperoleh dari alat pemindaian nmap sangat berisiko karena beberapa port tersebut dapat dimanfaatkan oleh hacker untuk melakukan serangan [4].	Menerapkan *intrusion detection system* (IDS) untuk mendeteksi adanya serangan seperti *port scan* [34].

Aseesment	*Tools*	Rangkuman Hasil	*Impact*	Saran
		network embedded 85%		
Vulnerability Identification	*Nikto*	Ditemukan spesifikasi mengenai versi server, SSL, dan PHP. Riciannya adalah Apache/2.4.55 (Win64) OpenSSL/1.1.1s PHP/8.1.23	Informasi mengenai spesifikasi versi server, SSL, dan PHP, dapat dieksploitasi oleh hacker	Lakukan update terbaru untuk setiap versi server, SSL, dan PHP untuk meningkatkan keamanan dari level sebelumnya
	Region	Ditemukan detail mengenai port beserta service dan kemungkinan operating sistem yang digunakan Riciannya adalah: terdapat hasil antara lain, 80/tcp s*tate open service http version* Microsoft IIS httpd 10.0, 3306/tcp *state open service* mysql *version* MySQL 5.5.5-10.5.4-MariaDB, 1433/tcp *state open service* mysql. Selain itu tools region menemukan bahwa operating system yang digunakan kemungkinan adalah *oracle virtual box* dengan akurasi sebesar 92	Informasi mengenai port terbuka yang diperoleh dari alat pemindaian region sangat berisiko karena beberapa port tersebut dapat dimanfaatkan oleh hacker untuk melakukan serangan [39].	Menerapkan *intrusion detection system* (IDS) untuk mendeteksi adanya serangan seperti *port scan* [40].

Aseesment	*Tools*	Rangkuman Hasil	*Impact*	Saran
	Zap	kerentanan mulai dari medium hingga informational. Riciannya dari risk medium adalah:		
		Tidak terdapat *CSP (Content-Security-Policy).*	*CSP* adalah lapisan yang ditambahkan pada HTTP response header yang berfungsi untuk mencegah serangan tertentu termasuk XSS	Solusinya adalah Solusinya adalah pastikan server web, server aplikasi, load balancer, dll. dikonfigurasi untuk mengatur header *Content-Security-Policy*
		Selanjutnya, *Website* tidak ada bisa terlindungi oleh serangan *click-jacking*	Singkatnya serangan click jacking berkerja dengan cara mengelabui pengguna dengan menyisipkan elemen transparan pada elemen HTML	Solusinya adalah pastikan website telah mendukung *HTTP Content-Security-Policy dan X-Frame-*
		Selain itu rincian dari risk low antara lain: *Website* menerapkan cookie tanpa httponly flag yang berdungsi sebagai pelapis keamanan website, apabila tidak menginstalnya sementara browser	Rentan terhadap serangan xss.	Solusinya dengan memastikan Http only flag telah terinstal

Aseesment	*Tools*	Rangkuman Hasil	*Impact*	Saran
		mengisntalnya maka cookie akan diakses dari pengguna. Namun apabila sebaliknya maka cookie dari website akan diabaikan dan *Website* membocorkan informasi melalui renspon header *HTTP "X-Powered-By" HTTP "X-Powered-By"* adalah bagian dari respons standar yang disertakan oleh server web dalam tanggapannya. Header ini mengandung informasi tentang teknologi atau perangkat lunak yang digunakan oleh server. Website membocorkan informasi melalui http server Header respon Kode Respons HTTP. Kode Respons HTTP adalah sekumpulan kode numerik tiga digit yang dikembalikan oleh server web sebagai respons terhadap permintaan	Namun, masalahnya adalah header ini juga dapat mengungkapkan informasi sensitif tentang konfigurasi server, yang dapat dieksploitasi oleh penyerang. Kode status ini disertakan dalam header respons dari respons HTTP untuk memberikan informasi tentang hasil permintaan	Soluinya adalah Pastikan server web, server aplikasi, load balancer, dll. Dikonfigurasi Solusinya dengan konfirmasi server web, server aplikasi, load balancer, dll.

Aseesment	*Tools*	Rangkuman Hasil	*Impact*	Saran
		HTTP yang dibuat oleh klien (biasanya browser web atau aplikasi lain). Header Anti-MIME-Sniffing X-Content-Type-Options tidak diatur ke 'nosniff'. Header respon HTTP “X-Content-Type-Options” adalah bagian dari respons yang dikirim oleh server web ke browser.	Dengan mengatur header ini, Anda memastikan bahwa tipe konten yang dinyatakan dalam header Content-Type benar-benar browser tidak melakukan MIME (Multipurpose Internet Mail Extensions). Dimana browser menebak paket yang dikirimkan	Solusinya adalah Pastikan bahwa aplikasi/server web menetapkan header Content-Type dengan tepat, dan menetapkan header X-Content-Type-Options ke 'nosniff' untuk semua halaman web.
		Rincian dari risk *informational* adalah: Respons tampaknya berisi komentar mencurigakan yang dapat membantu penyerang. Merupakan hasil scan dari *tool* zap dengan alert yang bersifat informational, Respons tersebut tampaknya berisi komentar mencurigakan yang	Dapat membantu penyerang Dimana risk tersebut bukan kerentanan Dapat membantu penyerang	Solusinya adalah hapus semua komentar. Tidak ada yang perlu diperbaiki Solusinya adalah hapus

Aseesment	*Tools*	Rangkuman Hasil	*Impact*	Saran
		dapat membantu penyerang.		semua komentar.

IV.4 *Reporting dan Clean-up and Destroy Artefacts*

Tahap ketiga pada *framework ISSAF* yang digunakan selanjutnya yaitu reporting dan clean-up and destroy artefacts. Pada pengujian kali ini penguji hanya melakukan wawancara konfirmasi dengan Bapak Moh Hisyam Fitrhony selaku selaku salah satu operator website dan waka humas sekolah XYZ. Hasil dokumen dan dokumentasi wawancara dapat dilihat pada lampiran 8 dan lampiran 9

Tabel IV.3 Ringkasan kondisi website pada server dummy

Aseesment	Rangkuman Hasil
Information Gathering	Ditemukan spesifikasi *website eraport* sekolah XYZ, seperti Alamat ip, port yang tersedia, dan *operating sistem* yang dipakai. Detailnya berada pada tabel IV.1
Network Mapping	Ditemukan banyak port yang terbuka, lebih detailnya berada pada sub bab tabel IV.1
Vulnerability Identification	Ditemukan berbagai informasi dan kerentanan. Riciannya berada pada tabel IV.1
Penetration Testing	Berdasarkan hasil pengujian yang termuat dalam tabel IV.1 Terdapat hasil *all parameter do not appear to be injectable*
Gaining Access and Privilege Escalation	Berdasarkan hasil yang sudah dilakukan didalam sub bab tabel IV.1, hasilnya adalah tidak terdapat username dan password yang sesuai.
	Berdasarkan hasil yang sudah dilakukan didalam sub bab tabel

	IV.1, hasilnya adalah tidak terdapat username dan password yang sesuai
	Berdasarkan hasil yang sudah dilakukan didalam sub bab tabel IV.1, hasilnya adalah tidak terdapat username dan password yang sesuai
Enumerating Further	Berdasarkan hasil pengujian yang berada pada tabel IV.1 berhasil merekam data lalu lintas menggunakan wireshark. Namun tidak mendapatkan informasi username dan password karena protokol TLS yang digunakan sudah versi terbaru.
	Berdasarkan hasil pengujian yang berada pada tabel IV.1 Setekah disimpan menggunakan tools cookie manager, selanjutnya mencoba login dengan hasil cookie yang disipan dan tidak bisa melakukan login menggunakan cookie yang disimpan oleh cookie manager
Compromise Remote User/Sites	Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik
Maintaning Access	Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik

Corvering Tracks	Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik

Tabel IV.4 Ringkasan kondisi website pada *server production*

Aseesment	Rangkuman Hasil
Information Gathering	Ditemukan spesifikasi *website* PPDB sekolah XYZ, seperti Alamat ip, port yang tersedia, dan *operating sistem* yang dipakai. Detailnya berada pada tabel IV.2
Network Mapping	Ditemukan banyak port yang terbuka, lebih detailnya berada pada tabel IV.2
Vulnerability Identification	Ditemukan berbagai informasi dan kerentanan. Riciannya berada pada tabel IV.2

Dikarenakan objek pengujian kali ini menggunakan *server dummy* menggunakan *remote desktop* yang diinstal di *device* milik penguji sendiri maka sub tahapan *Clean-up and Destroy Artefacts* tidak dilakukan. Berdasarkan hasil tabel IV.1 sampai IV.4 dapat disimpulkan kondisi website ini memiliki aenyak celah keamanan yang sampai level medium oleh karena itu untuk pihak operator dapat melakukan perbaikan pada server production Selain itu sub tahapan *Clean-up and Destroy Artefacts* tidak dilakukan karena pengujian gagal dalam tahapan enumerating futher dan penguji tidak bisa mencapai tahapan *compromise user.*

BAB V KESIMPULAN DAN SARAN

V.1 Kesimpulan

Berdasarkan dari pembahasan yang telah dipaparkan sebelumnya dapat diambil kesimpulan, kesimpulan tersebut antara lain:

V.1.1 Kondisi keamanan sistem informasi

Berdasarkan pembahasan sebelumnya dalam melakukan pengujian berdasarkan framework ISSAf terdapat langkah-langkah antara lain:

1. *Planing and preparation* merupakan tahap perencanaan dan persiapan, langkah-langkah berikut dilakukan:
    a) Wawancara bisa dilakukan dengan menyiapkan panduan wawancara untuk mendapatkan informasi dari pihak operator dari website e-raport sekolah XYZ.
    b) ObservasiMerencanakan kegiatan observasi untuk memahami secara langsung konteks dan keadaan sistem informasi.
2. *Assesment, Assessment* merupakan tahapan utama didalam frawemork issaf. *Assesment* terdiri dari
    a) *Information Gathering, Information Gathering* adalah aktivitas untuk mencari informasi atau data tentang suatu target
    b) *Network Mapping, Network Mapping adalah* Proses visualisasi dan pemahaman sistem jaringan yang kompleks dengan memecahnya menjadi fragmen-fragmen kecil
    c) *Vulnerability Identification, Vulnerability Identification* adalah proses penting dalam keamanan siber yang melibatkan identifikasi dan pemahaman kelemahan dalam sistem, infrastruktur, dan sistem pendukung.

d) *Penetration Testing, Penetration Testing* merupakan simulasi serangan siber yang diotorisasi dilakukan pada sistem komputer untuk mengevaluasi tingkat keamanannya

e) *Gaining Access and Previlage Escalation, Gaining Access and Previlage Escalation* atau serangan *privilege escalation*, peretas memanfaatkan kerentanan dalam kontrol akses dan pembatasan sumber daya untuk mengesampingkan izin dan batasan dari akun pengguna target untuk mendapatkan akses yang lebih tinggi.

f) *Enumerating Further*, *Enumerating Further* merupakan proses enumeration awal, penyerang dapat menggunakan informasi yang ditemukan untuk melakukan enumerating further, yaitu mengumpulkan informasi lebih lanjut tentang sistem atau jaringan

g) *Compromise Remote User/Sites, "Compromise Remote User/Sites"* dalam bahasa Indonesia dapat diartikan sebagai "Kompromi Pengguna/Situs Remote". Istilah ini merujuk pada situasi di mana pengguna atau situs remote mengalami kompromi keamanan, yang dapat mengakibatkan akses yang tidak sah atau penyalahgunaan sistem

h) *Maintaning Access*, *Maintaning Access* merupakan upaya untuk tetap terhubung ke suatu sistem atau jaringan setelah berhasil mendapatkan akses yang tidak sah.

i) *Corvering Tracks*, Corvering Tracks merujuk pada serangkaian tindakan yang dilakukan oleh penyerang setelah berhasil melakukan serangan untuk menghapus atau menyembunyikan jejak-jejak yang dapat digunakan untuk melacak atau mendeteksi kehadiran mereka.

3. *Reporting dan Clean-up and Destroy Artefacts*, Tahap ketiga pada framework ISSAF yang digunakan selanjutnya yaitu reporting dan clean-up and destroy artefacts

V.1.2 Hasil Pengujian

Setelah melakukan pengujian menggunakan framework ISSAF antara lain

V.1.2.1 Hasil Pengujian pada server dummy

1. *Information Gathering*:Ditemukan spesifikasi website PPDB sekolah XYZ, seperti Alamat ip, port yang tersedia, dan operating sistem yang dipakai.
2. *Network Mapping*: Ditemukan banyak port yang terbuka, lebih detailnya
3. *Vulnerability Identification*: Ditemukan berbagai informasi dan kerentanan. Riciannya berada pada tabel IV.1
4. *Penetration Testing*: Berdasarkan hasil pengujian yang termuat dalam tabel IV.1 Terdapat hasil all parameter do not appear to be injectable
5. *Gaining Access and Privilege Escalation*: Hasil yang sudah hasilnya adalah tidak terdapat username dan password yang sesuai.
6. *Enumerating Further*: Berhasil merekam data lalu lintas menggunakan wireshark. Namun tidak mendapatkan informasi username dan password karena protokol TLS yang digunakan sudah versi terbaru.selain ituSetekah disimpan menggunakan tools cookie manager, selanjutnya mencoba login dengan hasil cookie yang disipan dan tidak bisa melakukan login menggunakan cookie yang disimpan oleh cookie manager
7. *Compromise Remote User/Sites*:Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap *Enumerating Further* tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik
8. *Maintaning Access* : Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap *Enumerating Further* tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik
9. *Corvering Tracks*:Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap *Enumerating Further* tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik

V.1.2.2 Hasil Pengujian pada server production

1. *Information Gathering*: Ditemukan spesifikasi website *e-raport* sekolah XYZ, seperti Alamat ip, port yang tersedia, dan operating sistem yang dipakai
2. *Network Mapping*: Ditemukan banyak port yang terbuka

3. *Vulnerability Identification*: Ditemukan berbagai informasi dan kerentanan.

V.1.3 Rekomendasi Pengujian

V.1.1.1 Rekomendasi Pengujian pada *server dummy*

1. *Information Gathering*: Terdapat beberapa informasi umum, Alamat ip, port yang tersedia, dan operating sistem yang dipakai. Dengan adanya informasi
2. *Network Mapping:* Menerapkan intrusion detection system (IDS) untuk mendeteksi adanya serangan seperti port scan
3. *Vulnerability Identification*: Lakukan update terbaru untuk setiap versi server, SSL, dan PHP untuk meningkatkan keamanan dari level sebelumnya. Menerapkan intrusion detection system (IDS) untuk mendeteksi adanya serangan seperti port scan. Selanjutnya pastikan server web, server aplikasi, load balancer, dll. dikonfigurasi untuk mengatur header Content-Security-Policy. Selain itu, pastikan website telah mendukung *HTTP Content-Security-Policy dan X-Frame-*Selanjutnya dengan memastikan Http only flag telah terinstas Soluinya adalah Pastikan server web, server aplikasi, load balancer, dll. Dikonfigurasi. Solusinya dengan konfirmasi server web, server aplikasi, load balancer, dll. Solusinya adalah Pastikan bahwa aplikasi/server web menetapkan header Content-Type dengan tepat, dan menetapkan header X-Content-Type-Options ke 'nosniff' untuk semua halaman web.
4. *Penetration Testing*: Data base tidak injectable
5. *Gaining Access and Privilege Escalation*: tidak bisa menembus karena tidak menemukan kombinasi username dan password
6. *Enumerating Further*: terhalang oleh enkripsi
7. *Compromise Remote User/Sites*: Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik
8. *Maintaning Access*; Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa

dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik

9. *Corvering Tracks:* Tidak sampai pada tahapan inu. Dikarenakan kegagalan pada tahap Enumerating Further tahapan ini tidak bisa dilakukan. Kegagalan tersebut disebabkan oleh sistem yang sudah terkonfigurasi dengan baik

V.1.1.1 Hasil Pengujian pada *server production*

1. *Information Gathering* tidak ada yang bisa direkomendasikan karena merupakan hasil scan otomatis
2. *Network Mapping* : Menerapkan intrusion detection system (IDS) untuk mendeteksi adanya serangan seperti port scan
3. *Vulnerability Identification*: Lakukan update terbaru untuk setiap versi server, SSL, dan PHP untuk meningkatkan keamanan dari level sebelumnya. Menerapkan intrusion detection system (IDS) untuk mendeteksi adanya serangan seperti port scan. Selanjutnya pastikan server web, server aplikasi, load balancer, dll. dikonfigurasi untuk mengatur header Content-Security-Policy. Selain itu, pastikan website telah mendukung *HTTP Content-Security-Policy dan X-Frame-* Selanjutnya dengan memastikan Http only flag telah terinstas Soluinya adalah Pastikan server web, server aplikasi, load balancer, dll. Dikonfigurasi. Solusinya dengan konfirmasi server web, server aplikasi, load balancer, dll. Solusinya adalah Pastikan bahwa aplikasi/server web menetapkan header Content-Type dengan tepat, dan menetapkan header X-Content-Type-Options ke 'nosniff' untuk semua halaman web.

V.2 Saran

Adapun saran untuk penelitian selanjutnya adalah sebagai berikut:

1. Melakukan pengujian system keamanan lanjutan di server production
2. Menggunakan *Framework* lain untuk melakukan pengujian, baik itu di server dummy ataupun di server production.

3. Menggunakan metode pengujian lain, seperti metode *white box* atau *grey box* untuk melakukan pengujian, baik itu di *server dummy* ataupun di *server production*.
4. Menggunakan *tools* lain untuk melakukan pengujian baik itu di server dummy ataupun di server production. Seperti menggunakan *whois, wappalyzer, Nessus, Metasploit, hydra, manual input, burpsuites*, dan *tools* lainnya
5. Mencoba memperbaiki berdasarkan rekomendasi penelitian ini yang dihasilkan melalui pengujian menggunakan *framework Information System Security Assessment Framework* (ISSAF)
    a) Menerapkan intrusion detection system (IDS) untuk mendeteksi adanya serangan seperti port scan
    b) Lakukan update terbaru untuk setiap versi server, SSL, dan PHP untuk meningkatkan keamanan dari level sebelumnya. Menerapkan intrusion detection system (IDS) untuk mendeteksi adanya serangan seperti port scan. Selanjutnya pastikan server web, server aplikasi, load balancer, dll. dikonfigurasi untuk mengatur header Content-Security-Policy. Selain itu, pastikan website telah mendukung HTTP Content-Security-Policy dan X-Frame- Selanjutnya dengan memastikan Http only flag telah terinstas Soluinya adalah Pastikan server web, server aplikasi, load balancer, dll. Dikonfigurasi. Solusinya dengan konfirmasi server web, server aplikasi, load balancer, dll. Solusinya adalah Pastikan bahwa aplikasi/server web menetapkan header Content-Type dengan tepat, dan menetapkan header X-Content-Type-Options ke 'nosniff' untuk semua halaman web

BAB VI DAFTAR PUSTAKA

M. Arief, 2021, Keamanan informasi: Konsep, ancaman, dan pengendalian., Yogyakarta: Andi.

Asosiasi Penyelenggara Jasa Internet Indonsesa. (APJII), 2022 Survei APJII: Penetrasi dan Perilaku Pengguna Internet Indonesia 2021-2022., Jakarta: APJII.

A. W. A. &. C. D, 2015 Dirgahayu, "Analisis keamanan website dengan menggunakan metode static analysis.," Jurnal Informatika, 11(2)., pp. 143-150.

R. Munir, 2019 Keamanan sistem informasi., Bandung: Informatika.

L. C. d. M. Guntoro, 2020 "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," Jurnal Ilmiah Penelitian dan Pembelajaran Informatika, vol. Volume 05, pp. 45 - 55.

I. R. Y. K.,. I. A. R. Herman, 2023 "Analisis Keamanan Website Menggunakan Information System Security Asessment Framework (ISSAF)," Jurnal Teknlogi Informatika dan Komputer MH. Thamrin, vol. Volume 9 No 1.

A. W. &. S. H. B. Wardhana, 2021 "Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ.," Informatik: Jurnal Ilmu Komputer, , Vols. 17(3), , pp. 226-237.

E. P. a. R. A. A. A. Silmina, 2022 "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test dan ISSAF.," Jurnal Transmisi 24.3: 83-91.

G. M. A. S. D. M. S. A. I Gede Ary Suta Sanjaya, 2020 "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," JURNAL ILMIAH MERPATI, Vols. VOL 8, NO. 2.

Rusydi Umar, I. R. (April 2023). Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF. *Jutisi: Vol. 12, No. 1*, 280-292.

geeksforgeeks.org, 2024. *geeksforgeeks.org*. Retrieved from geeksforgeeks.org Components Of Information System: https://www.geeksforgeeks.org/components-of-information-system/

Balwant Rathore, M. B, 2006. Information Systems Security Assessment Framework (ISSAF) draft 0.2. In M. B. Balwant Rathore, Information Systems Security Assessment Framework (ISSAF) draft 0.2 (p. 18). Open Information System Security Group .

Hertzog, Raphael; O'Gorman, Jim; Aharoni, Mati, 2017. *Kali Linux Revealed: Mastering the Penetration Testing Distribution*. Offsec Press. ISBN 978-0-9976156-0-9. Archived

O'Harrow Jr, Robert, 2012. "Cyber search engine Shodan exposes industrial control systems to new risks". *Washington Post*

Medeiros, João Paulo S.; Brito Jr., Agostinho M.; Pires, Paulo S. Motta, 2009. "A Data Mining Based Analysis of Nmap Operating System Fingerprint Database". *Computational Intelligence in Security for Information Systems*. Advances in Intelligent and Soft Computing. Vol. 63. pp. 1–8. doi:10.1007/978-3-642-04091-7_1. ISBN 978-3-642-04090-0.

Clarke, Justin, 2012. *SQL injection attacks and defense*. Waltham, MA: Elsevier. p. 282. ISBN 978-1-59749-963-7.

madhusudan_soni., 2020. *geeksforgeeks.org*. Retrieved from geeksforgeeks.org/how-to-scan-vulnerabilities-of-websites-using-nikto-in-linux/: https://www.geeksforgeeks.org/how-to-scan-vulnerabilities-of-websites-using-nikto-in-linux/

Organisation, Z. (2023). ZAP 2.15 Getting Stated Guide. In Z. D. Team, *ZAP 2.15 Getting Stated Guide* (pp. 2-3). Zap Development Team.

lalitmohantiwari7700. (2020, December 24). *geeksforgeeks.org*. Retrieved from geeksforgeeks.org /legion-tool-in-kali-linux/: https://www.geeksforgeeks.org/legion-tool-in-kali-linux/

Hnatyshin, Vasil Y.; Lobo, Andrea F, 2021. "Undergraduate Data Communications and Networking Projects Using OPNET and Wireshark Software". Rowan University..

McNab, Chris , 2011. Network Security Assessment: Know Your Network. O'Reilly Media, Inc. p. 181. ISBN 978-0-596-51933-9.

Christophe Gagnier, 2023. Cookie-Editor - A safe cookie editor for Chrome, Firefox, Safari, Edge and Opera

M. Aziz, 2021 "Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas Xyz," *Jecsit*, vol. 1, no. 1, pp. 101–109,.

V. S. Voo Teck En, 2022 "Cross-Site Scripting (XSS).," IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), 1-5., pp. 1-5, 2022.

D. A. S. S. A. Maha Alghawazi, 2022 "Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review," Journal of Cybersecurity and Security.

S. M. R. W. Rankothge, 2020 "Identification and Mitigation Tool For Cross-Site Request Forgery (CSRF)," IEEE 8th R10 Humanitarian Technology Conference (R10-HTC), , pp. 1-5.

I. T. Elira Hoxha, 2022 "Session hijacking vulnerabilities and prevention algorithms," Global Journal of Information Technology: Emerging Technologies, Vols. vol. 12, No. 1.

I. A. K. Rio Ananda Putra, 2023 "Detection and Prevention of Insecure Direct Object References (IDOR) in Website-Based Applications," Procedia of Engineering and Life Science, vol. v4i0, p. 1435.

I. K. Marco Ariano Kristyanto, 2022 "SSH Bruteforce Attack Classification using Machine Learning," 10th International Conference on Information and Communication Technology, pp. 116 - 119.

T. Dirgahayu, Y. Prayudi, and A. Fajaryanto, 2015 "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," J. Ilm. NERO, vol. 1, no. 3, pp. 190–197.

NEGARA, B. S. (2023). LANSKAP KEAMANAN SIBER INDONESIA 2023. In D. O. Siber, *LANSKAP KEAMANAN SIBER INDONESIA 2023.* BADAN SIBER DAN SANDI NEGARA.

Stephen A. Thomas 2000. SSL and TLS essentials securing the Web. New York: Wiley. ISBN 978-0-471-38354-3.

A. Fujianto and I. dfdf Waspada, 2016, "Rancang bangun sistem informasi pengelolaan DNS secara terpusat (Studi kasus Cv . Surya Putra Perkasa)," *J. Infokam*, vol. 1, pp. 9–10,.

Kristol, David M. (2001). "HTTP Cookies: Standards, Privacy, and Politics". ACM Transactions on Internet Technology. 1 (2). Association for Computing Machinery (ACM): 151–198. arXiv:cs/0105018. doi:10.1145/502152.502153. ISSN 1533-5399. S2CID 1848140.

P. G. S. Adinata, I. P. W. P. Putra, N. P. A. I. Juliantari, and K. D. A. Sutrisna, 77, 2022"Analisis Perbandingan Tools SQL Injection Menggunakan SQLmap, SQLsus dan The Mole," Inform. J. Ilmu Komput., vol. 18, no. 3, p. 286, 2022, doi: 10.52958/iftk.v18i3.5373.

learn.microsoft.com. (2024, July 1). *learn.microsoft.com*. Retrieved from learn.microsoft.com Desain arsitektur keamanan: https://learn.microsoft.com/id-id/azure/architecture/guide/security/security-

Sutarti, A. P. Pancaro, and F. I. Saputra, 2018 "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, pp. 1–8,

LAMPIRAN

Lampiran I. Surat balasan pihak sekolah

Nomor : 1168/SMKIA/XI/2023 Surabaya, 22 November 2023
Lampiran : -
Perihal : Surat balasan pengantar penelitian dan pengambilan data

Kepada Yth.
Bapak Dr. Helmy Widyantara, S.Kom., M.Eng.
Dekan Fakultas Teknologi Informasi & Bisnis
Jl. Ketintang No. 156
Surabaya 60231

Assalamualaikum w.w.

Dengan hormat,

Melalui surat ini, kami sampaikan balasan kabar mengenai Surat Pengantar Penelitian dan Pengambilan Data (No: 1451/AKD8/DEK-TI/XI/2023) dari IT Telkom Surabaya. Bahwa kami telah menerima informasi dengan baik dan berterima kasih atas peluang kerjasama yang telah diberikan kepada

Permohonan yang disampaikan melalui surat tersebut, kami terima dengan baik, serta harapan turut mensukseskan Tri Dharma Perguruan Tinggi dalam hal Penelitian. Tentu demi kenyamanan bersama, kami harap agar mahasiswa dengan data berikut:

Nama Lengkap : Dery Syam Ahnaf
NIM : 1204200143
Fak/Prodi : FTIB / Sistem Informasi

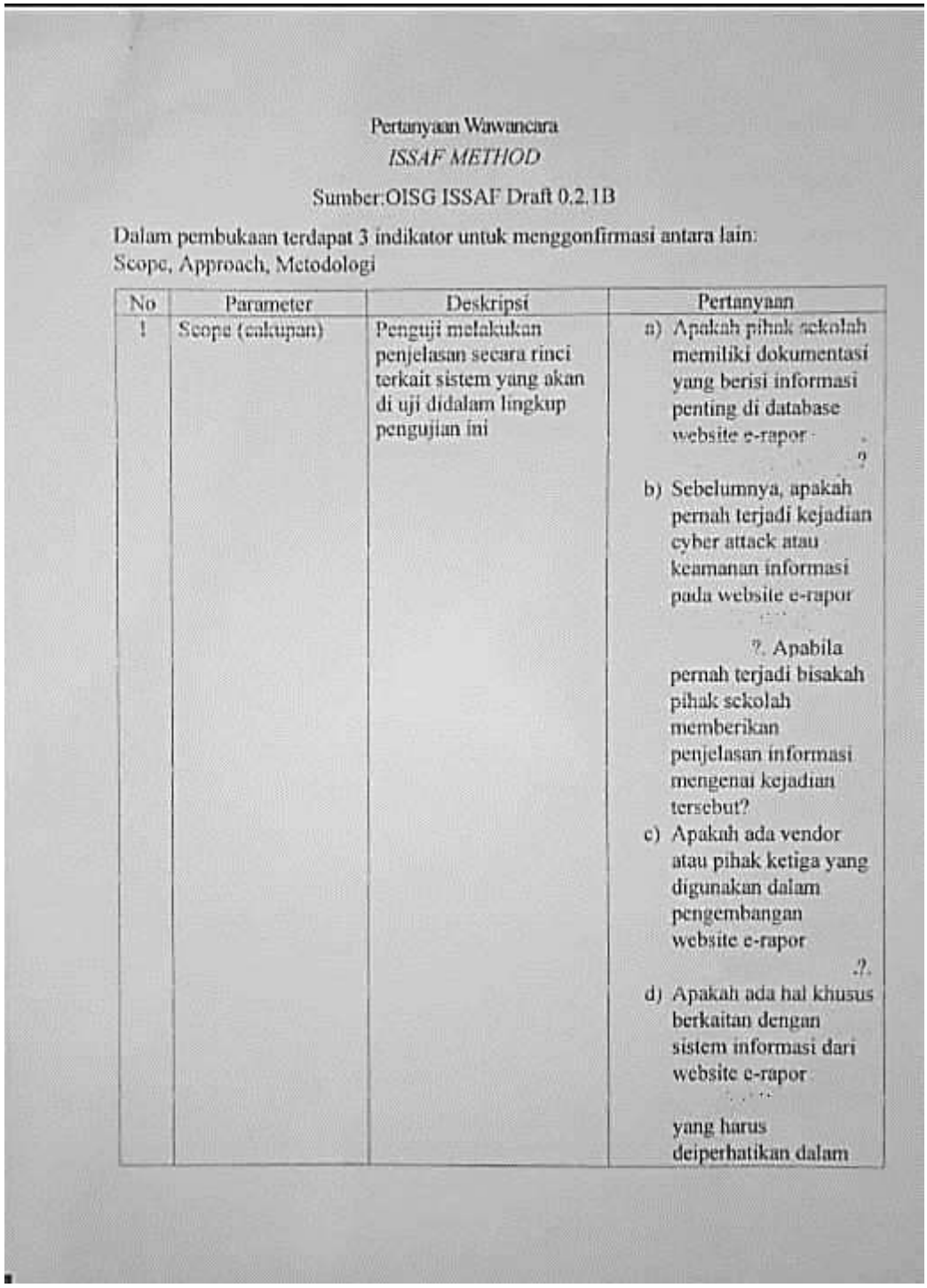
Agar tetap mengikuti aturan dan kesepakatan yang telah ada terkait penelitian di

Demikian balasan kabar kami, atas perhatian dan maklumnya disampaikan terima kasih. Mohon maaf jika ada hal yang kurang berkenan.

Wassalamualaikum w.w.

Kepala S

Lampiran II. Dokumen hasil wawancara



Pertanyaan Wawancara

ISSAF METHOD

Sumber:OISG ISSAF Draft 0.2.1B

Dalam pembukaan terdapat 3 indikator untuk menggonfirmasi antara lain: Scope, Approach, Metodologi

No	Parameter	Deskripsi	Pertanyaan
1	Scope (cakupan)	Penguji melakukan penjelasan secara rinci terkait sistem yang akan di uji didalam lingkup pengujian ini	a) Apakah pihak sekolah memiliki dokumentasi yang berisi informasi penting di database website e-rapor b) Sebelumnya, apakah pernah terjadi kejadian cyber attack atau keamanan informasi pada website e-rapor ?. Apabila pernah terjadi bisakah pihak sekolah memberikan penjelasan informasi mengenai kejadian tersebut? c) Apakah ada vendor atau pihak ketiga yang digunakan dalam pengembangan website e-rapor d) Apakah ada hal khusus berkaitan dengan sistem informasi dari website e-rapor yang harus deiperhatikan dalam

			pengujian keamanan ini? e) Apakah ada Batasan yang harus dipertimbangkan pada pengujian ini?
2	Approach (pendekatan)	Penguji menjabarkan metode yang digunakan dalam melakukan penguji keamanan sistem informasi untuk mengidentifikasi celah keamanan.	a) Apakah pihak sekolah sering melakukan pemeliharaan dan pembaruaan keamanan sistem website e-rapor ?. Apabila dilakukan pemeliharaan dan pembaruaan keamanan sistem, Berapa lama sekali sistem ini diperbarui?. b) Apakah pihak sekolah memiliki jadwal untuk sering melakukan pemeliharaan dan pembaruaan keamanan sistem website e-rapor ?. c) Kapan terakhir kali sistem ini di-update? d) Apakah pihak sekolah menggunakan jasa dari pihak ketiga untuk menambah keamanan sistem website e-rapor ?. e) Bagaimana pihak sekolah

			mendeskripsikan mengenai tingkat keamanan sistem website e-rapor ?. f) Bagaimana Langkah-langkah yang diambil oleh pihak sekolah Ketika terjadi cyber attack atau ancaman keamanan sistem website e-rapor ?.
3	Metodologi	Penguji menjelaskan langkah-langkah yang akan digunakan selama melakukan pengujian keamanan (pentest)	a) Apakah sebelumnya pihak sekolah menggunakan *framework* atau metode terentu dalam menguji keamanan sistem website e-rapor ?. b) Apakah pihak sekolah memiliki preferensi atau feedback terkait metode atau framework yang kami gunakan dalam pengujian ini? c) Apakah pihak sekolah memiliki preferensi atau feedback mengenai metode dan tools testing yang kami gunakan dalam pengujian ini?

Jawaban:

1. Scope

   a) Ya

   b) Tidak

   c) Ada

   d) Tidak disebarkan ke luar sekolah dan harus kembali semula seusai pengujian

   e) User dan Password admin tidak bisa kami berikan karena terkait pakta integritas sekolah

2. Pendekatan

   a) Ya, minimal setiap semester

   b) Ya

   c) Akhir Januari 2023

   d) Tidak

   e) Sistem keamanan masih standar, karena OS server berbasis Windows, sehingga tidak menambahkan keamanan https

   f) Take down server dan kami telusuri untuk dipulihkan, serta melakukan backup secara berkala untuk antisipasi

3. Metodologi

   a) Tidak

   b) Terkait metode atau framework yang diujikan, sudah baik, namun akan lebih tepat jika disasarkan pada portal eLearning yang lebih kompleks, karena urgensi eRapor tidak begitu krusial dan sistem sudah disiapkan dari pusat, hanya diinstal secara parsial di Satuan Pendidikan masing-masing dan tersinkronisasi

   c) belum ada

Catatan oleh dosen pembimbing, Senin 04 Maret 2024

1. Kemarin saya diminta oleh dosen saya agar menambahkan langkah-langkah dan dokumentasi penginstalan aplikasi e raport kedalam rdp. saya meminta tolong ke pak hisyam, untuk menambahkan langkah-langkah dan dokumentasi penginstalan aplikasi e raport kedalam rdp
2. Kemarin saya diminta oleh doesen pembimbing saya didalam intalasi aplikasi e raport agar ditambahkan data basenya yang terkait e raport, mulai dari nilai dan sebagainya, untuk datanya bisa 3-5 tahun data kebelakang tidak harus data saat ini. saya meminta tolong ke pak hisyam, untuk instalasi eraport selanjutnya didalam intalasi aplikasi e raport agar ditambahkan data basenya yang terkait e raport, mulai dari nilai dan sebagainya, untuk datanya bisa 3-5 tahun data kebelakang tidak harus data saat ini.

Respon catatan:

1. Silakan bisa pelajari di youtube banyak, atau official site ada di http://erapor.ditpsmk.net/pusat-unduhan
2. Terkait database rapor, semua sudah tersimpan secara otomatis dari sistem, ketika login tinggal pilih semester dan tahun ajaran. Kalaupun datanya tidak muncul, berarti memang dari pusat diprotect sampai periode tertentu, karena sistemnya hanya update versi datawebnya, bukan instal ulang setiap pembaharuannya

Surabava, 08 Maret 2024

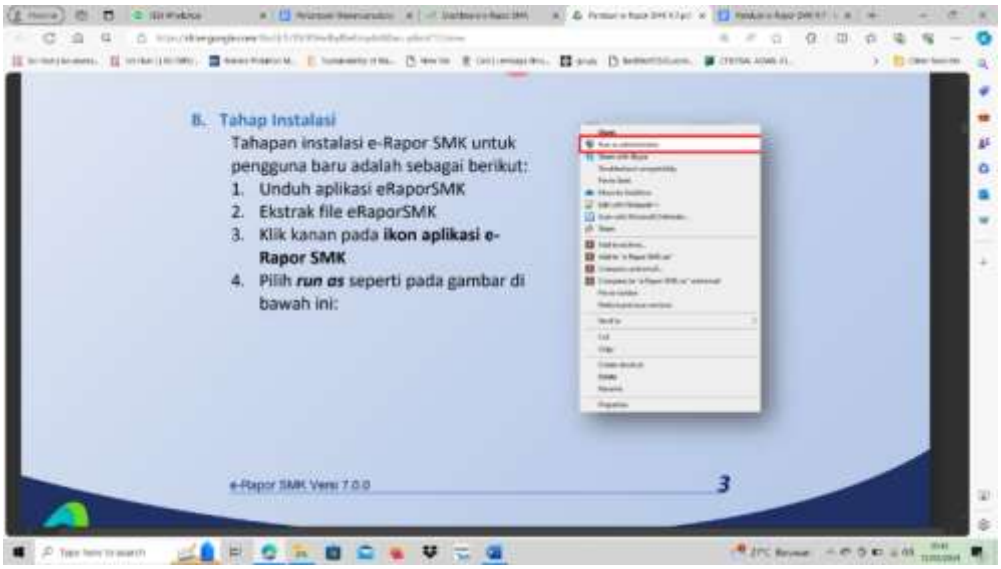
Narasumber,

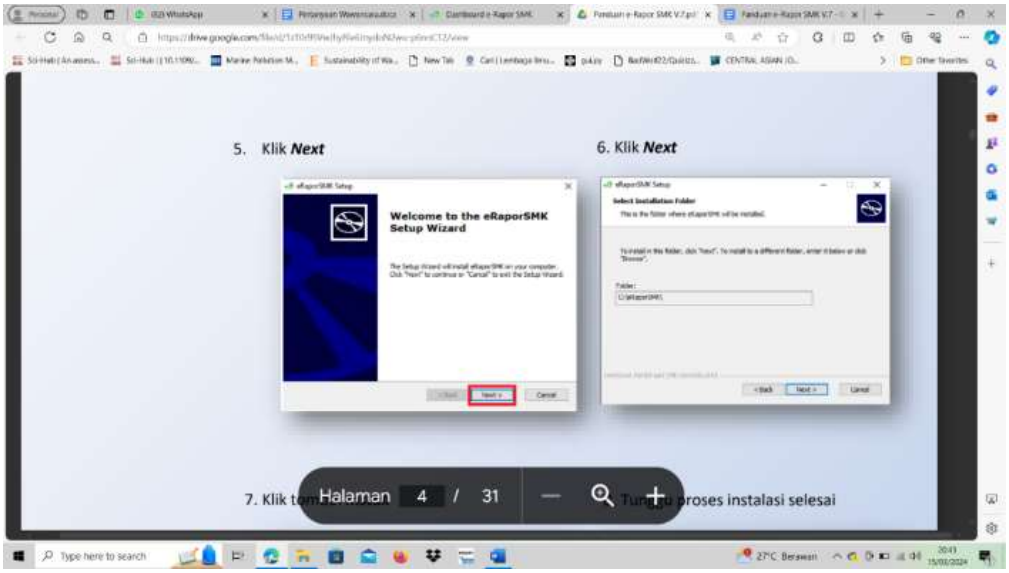
Moh. Hisyam Fithrony

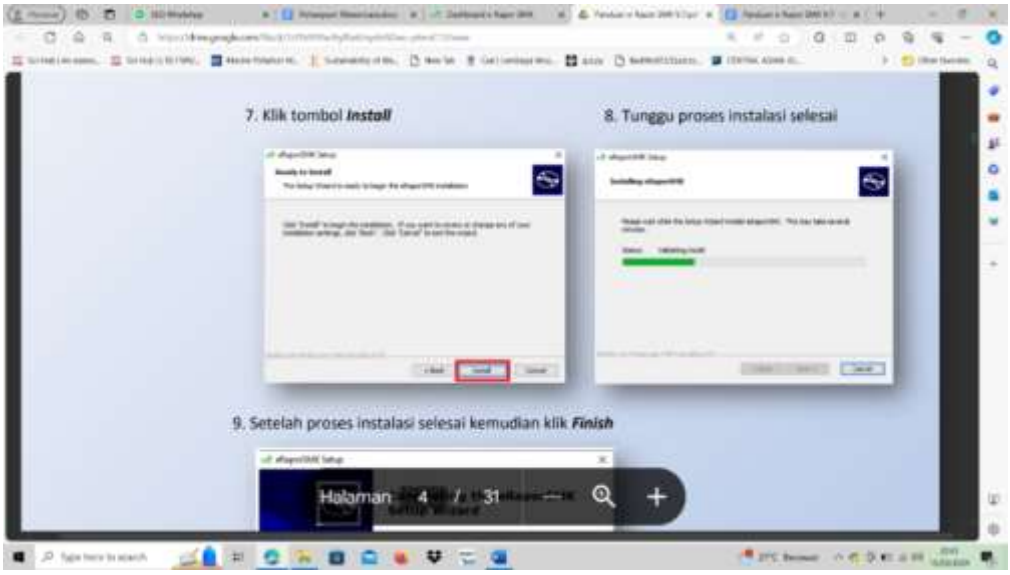
Lampiran III. Dokumentasi wawancara

Lampiran IV Spesifikasi minimum untuk eraport

Lampiran V Tahap instalasi e-raport

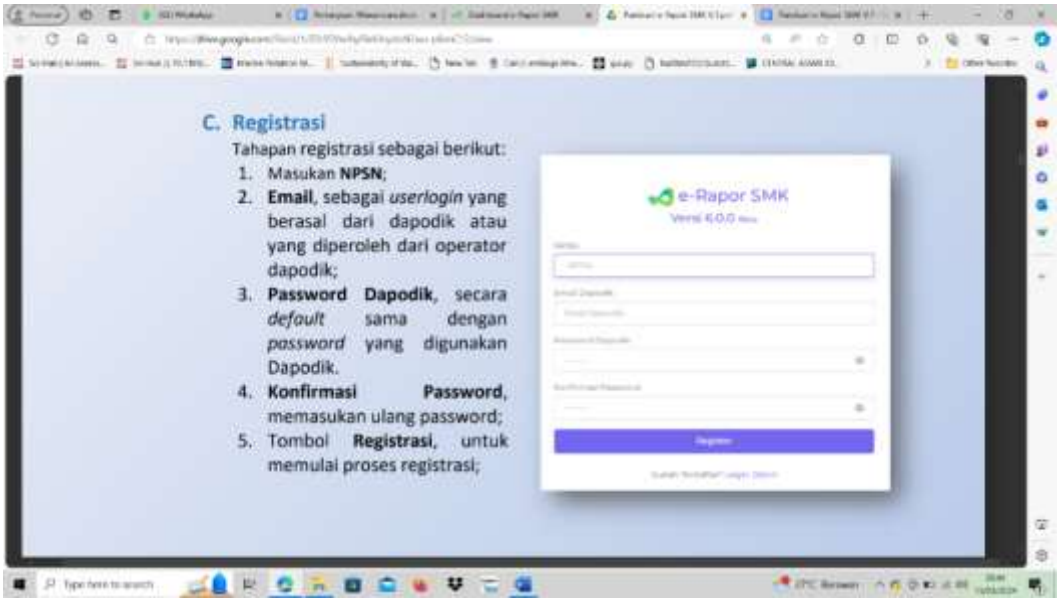



5. Klik Next
6. Klik Next
Welcome to the eRaporSMK Setup Wizard
Halaman 4 / 31

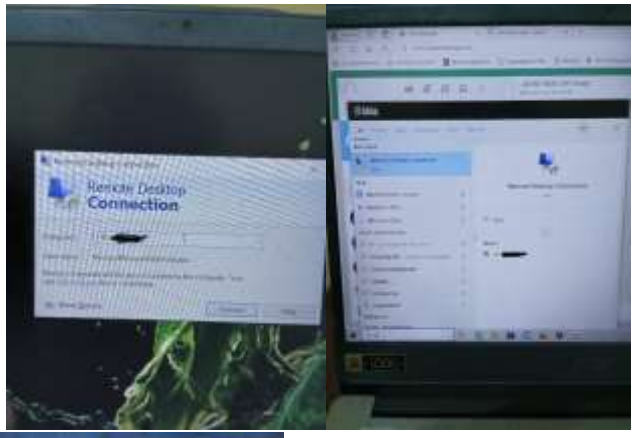

7. Klik tombol Install
8. Tunggu proses instalasi selesai
9. Setelah proses instalasi selesai kemudian klik Finish
Halaman 4 / 31


9. Setelah proses instalasi selesai kemudian klik Finish
Completing the eRaporSMK Setup Wizard
Halaman 4 / 31

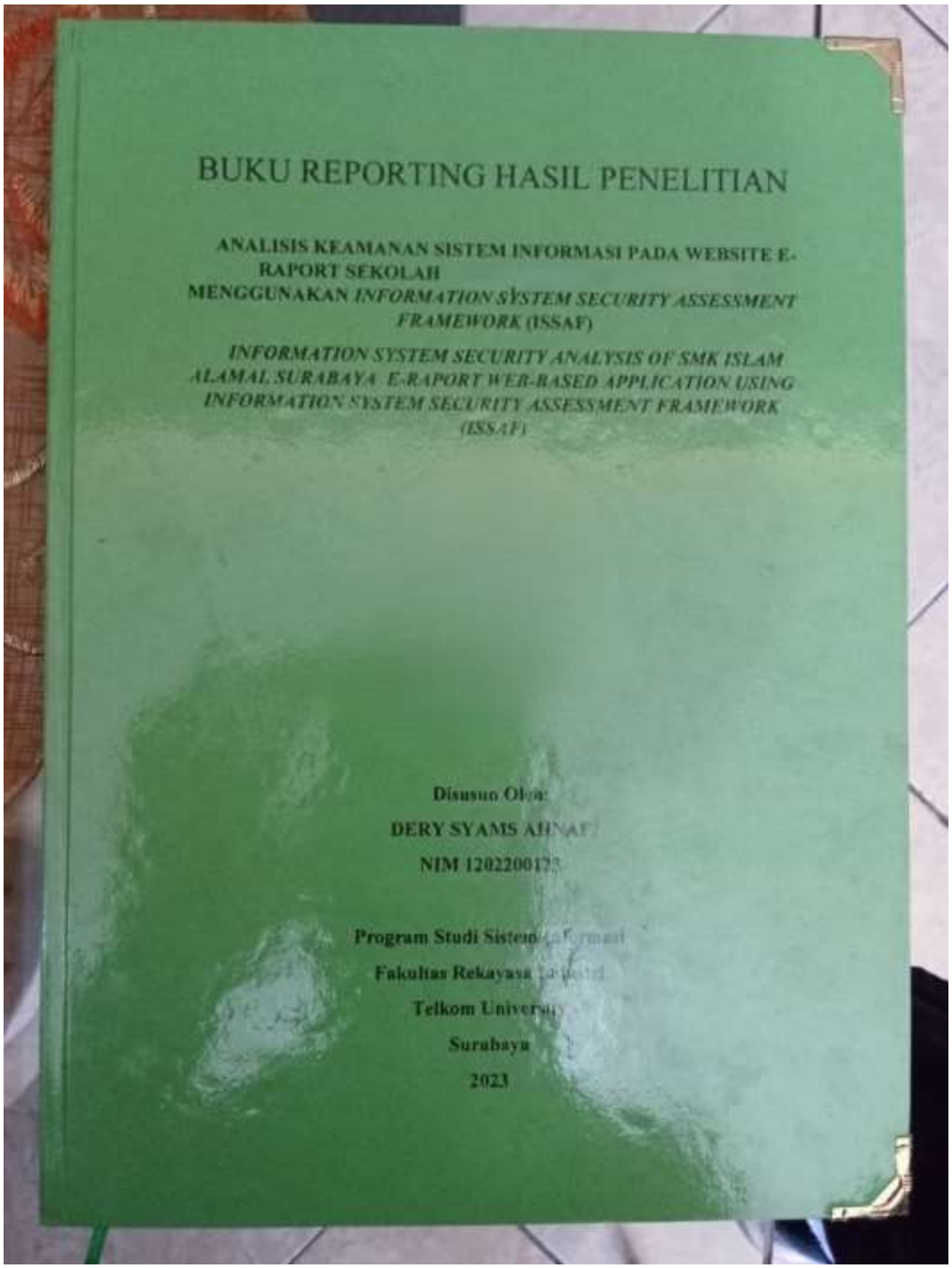
Lampiran VI Registrasi e-raport



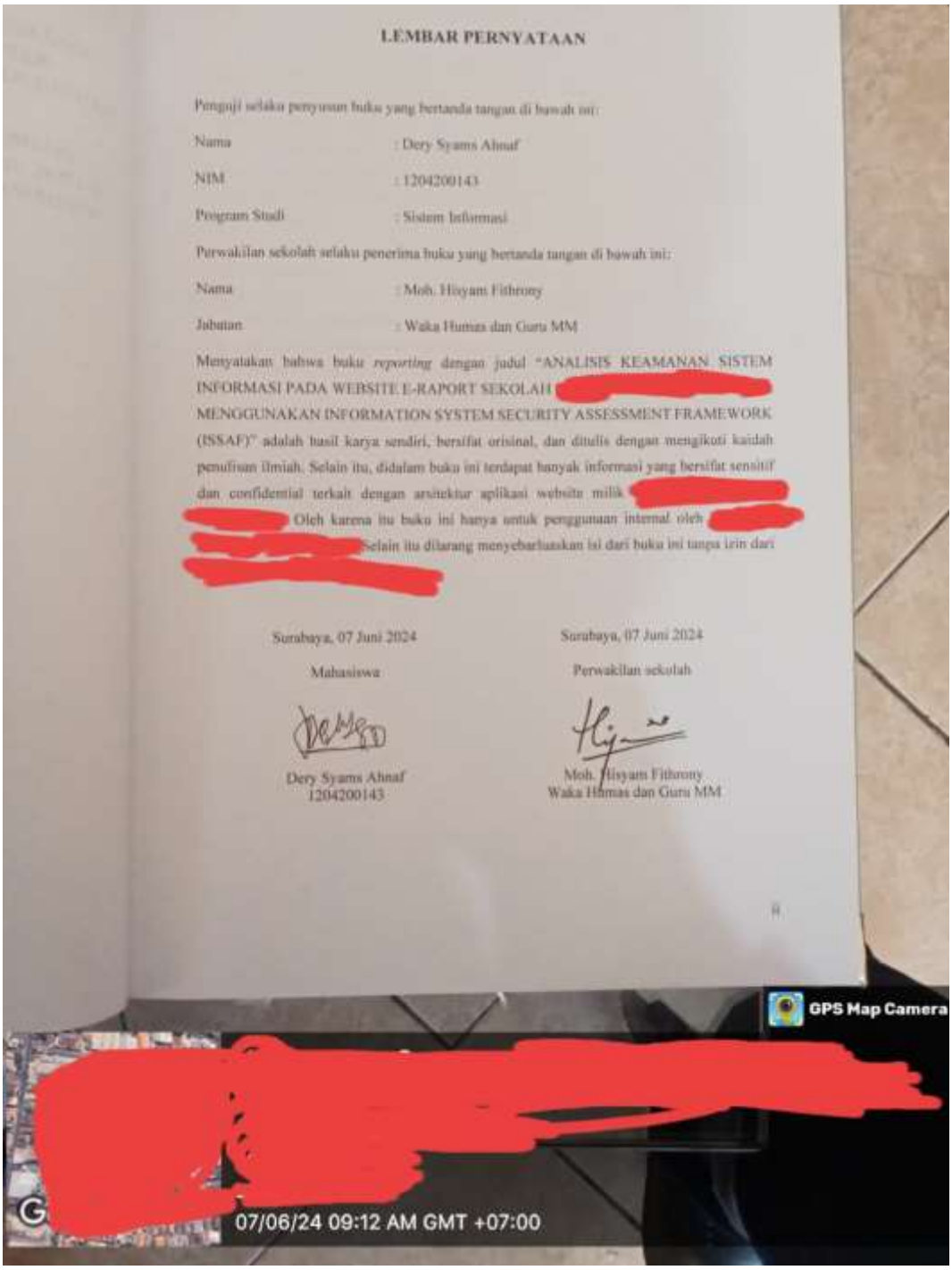
Lampiran VII Pembelian server dummy



Lampiran VIII. Dokumen hasil reporting



Lampiran X1. Dokumentasi hasil reporting



LEMBAR PERNYATAAN

Penguji selaku penyusun buku yang bertanda tangan di bawah ini:

Nama : Dery Syams Ahnaf

NIM : 1204200143

Program Studi : Sistem Informasi

Perwakilan sekolah selaku penerima buku yang bertanda tangan di bawah ini:

Nama : Moh. Hisyam Fithrony

Jabatan : Waka Humas dan Guru MM

Menyatakan bahwa buku *reporting* dengan judul "ANALISIS KEAMANAN SISTEM INFORMASI PADA WEBSITE E-RAPORT SEKOLAH [redacted] MENGGUNAKAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF)" adalah hasil karya sendiri, bersifat orisinal, dan ditulis dengan mengikuti kaidah penulisan ilmiah. Selain itu, didalam buku ini terdapat banyak informasi yang bersifat sensitif dan confidential terkait dengan arsitektur aplikasi website milik [redacted] Oleh karena itu buku ini hanya untuk penggunaan internal oleh [redacted] Selain itu dilarang menyebarluaskan isi dari buku ini tanpa izin dari [redacted]

Surabaya, 07 Juni 2024
Mahasiswa

Dery Syams Ahnaf
1204200143

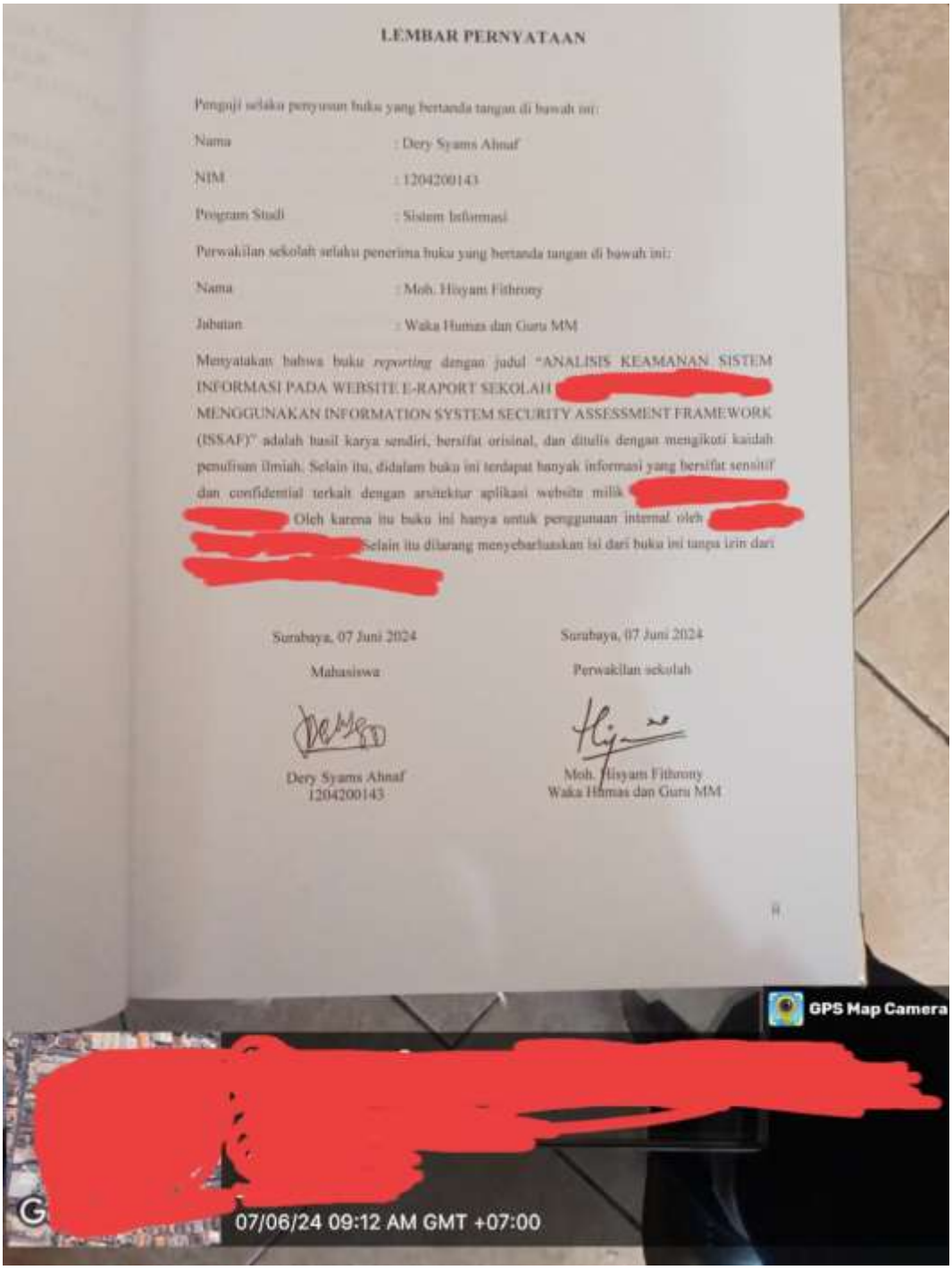
Surabaya, 07 Juni 2024
Perwakilan sekolah

Moh. Hisyam Fithrony
Waka Humas dan Guru MM

GPS Map Camera

[redacted]

07/06/24 09:12 AM GMT +07:00



LEMBAR PERNYATAAN

Penguji selaku penyusun buku yang bertanda tangan di bawah ini:

Nama : Dery Syams Ahnaf

NIM : 1204200143

Program Studi : Sistem Informasi

Perwakilan sekolah selaku penerima buku yang bertanda tangan di bawah ini:

Nama : Moh. Hisyam Fithrony

Jabatan : Waka Humas dan Guru MM

Menyatakan bahwa buku *reporting* dengan judul "ANALISIS KEAMANAN SISTEM INFORMASI PADA WEBSITE E-RAPORT SEKOLAH [redacted] MENGGUNAKAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF)" adalah hasil karya sendiri, bersifat orisinal, dan ditulis dengan mengikuti kaidah penulisan ilmiah. Selain itu, didalam buku ini terdapat banyak informasi yang bersifat sensitif dan confidential terkait dengan arsitektur aplikasi website milik [redacted] Oleh karena itu buku ini hanya untuk penggunaan internal oleh [redacted] Selain itu dilarang menyebarluaskan isi dari buku ini tanpa izin dari [redacted]

Surabaya, 07 Juni 2024
Mahasiswa

Dery Syams Ahnaf
1204200143

Surabaya, 07 Juni 2024
Perwakilan sekolah

Moh. Hisyam Fithrony
Waka Humas dan Guru MM

GPS Map Camera

[redacted]

07/06/24 09:12 AM GMT +07:00


GPS Map Camera
07/06/24 09:13 AM GMT +07:00