TUGAS AKHIR

EVALUASI KEAMANAN WEBSISTE TERHADAP KERENTANAN SERANGAN *HACKER* DENGAN METODE *PENETRATION TEST* MENGGUNAKAN OWASP ZAP
(STUDI KASUS : SIPA FAKULTAS TEKNIK)

MUHAMMAD ALHAQI
173510022

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2024

HALAMAN PENGESAHAN TUGAS AKHIR

Nama : Muhammad Alhaqi

NPM : 173510022

Kelompok Keahlian : Pemograman

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata Satu (S1)

Judul TA :Evaluasi Keamanan *Website* Terhadap Kerentanan Serangan *Hacker* dengan Metode *Penetration Test* Menggunakan OWASP ZAP

Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam tugas akhir ini telah dipelajari dan dinilai relatif telah memenuhi ketentuan-ketentuan dan kriteria- kriteria dalam metode penelitian ilmiah. Oleh karena itu tugas akhir ini dinilai layak dapat disetujui untuk disidangkan dalam ujian **Seminar Tugas Akhir.**

Pekanbaru, 2 Januari 2024

Di sahkan oleh :

Penguji I	Penguji II
Dr. Ir. Evizal Abdul Kadir, M.Eng	**Hendra Gunawan, ST, M.Eng**
NIDN. 1029027601	**NIDN. 1003087703**

Ketua Program Studi Teknik Informatika	Dosen Pembimbing
Dr. Apri Siswanto, S.Kom., M.kom	**Yudhi Arta, ST, M.Kom**
NIDN. 1016048502	**NIDN. 1029078701**

HALAMAN PENGESAHAN

DEWAN PENGUJI TUGAS AKHIR

Nama	: Muhammad Alhaqi
NPM	: 173510022
Kelompok Keahlian	: Platform
Program Studi	: Teknik Informatika
Jenjang Pendidikan	: Strata Satu (S1)
Judul TA	:Evaluasi Keamanan *Website* Terhadap Kerentanan Serangan *Hacker* Dengan Metode *Penetration Test* Menggunakan OWASP ZAP (Studi Kasus: SiPA Fakultas Tenik Universitas Islam Riau)

Tugas Akhir ini secara keseluruhan dinilai telah memenuhi ketentuan-ketentuan dan kaidah-kaidah dalam penulisan penelitian ilmiah serta telah diuji dan dapat dipertahankan dihadapan dewan penguji. Oleh karena itu, Tim Penguji Ujian Tugas Akhir Fakultas Teknik Universitas Islam Riau menyatakan bahwa mahasiswa yang bersangkutan dinyatakan Telah Lulus Mengikuti Ujian Tugas Akhir Pada Tanggal 22 Februari 2024 dan disetujui serta diterima untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Strata Satu Bidang Ilmu Teknik Informatika.

Pekanbaru, 22 Februari 2024

Dewan Penguji

1. Pembimbing : Yudhi Arta, S.T, M.Kom ( )
2. Penguji 1 : Hendra Gunawan, ST., M.Eng ( )
3. Penguji 2 : Dr. Evizal, ST., M.Eng ( )

Disahkan Oleh :

Ketua Program Studi
Teknik Informatika

Dr.Apri Siswanto, S.Kom., M.Kom
NIDN 1016048502

PERNYATAAN KEASLIAN TUGAS AKHIR

Dengan ini saya menyatakan bahwa tugas akhir ini merupakan karya saya sendiri dan semua sumber yang tercantum didalamnya baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar sesuai ketentuan. Jika terdapat unsur penipuan atau pemalsuan data maka saya bersedia dicabut gelar yang telah saya peroleh.

Pekanbaru, 14 Maret 2024

MUHAMMAD ALHAQI
NPM 173510022

KATA PENGANTAR

Assalamu'alaikum warahmatullahi wabarakatuh

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa Allah SWT yang telah melimpahkan rahmat, taufik serta hidayah-Nya sehingga penulis dapat membuat tugas akhir skripsi dengan judul dengan judul "**Evaluasi Keamanan Websiste Terhadap Kerentanan Serangan *Hacker* Dengan Metode *Penetration Test* Menggunakan *Open Web Application Security Project* (OWASP) ZAP"** sebagai salah satu syarat wajib untuk menyelesaikan program sarjana strata satu (S1) pada fakultas teknik program studi Teknik informatika Universitas Islam Riau.

Dalam pengusunan laporan skripsi ini, penulis sadar bahwa berhasilnya studi dan penyusunan laporan skripsi tidak lepas dari bantuan dan bimbingan dari berbagai pihak. Untuk itu dalam kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar – besarnya kepada:

1. ALLAH Subhanahu Wa Ta'ala dengan segala rahmat dan karunia-NYA yang memberikan kekuatan bagi penulis dalam menyelesaikan skripsi ini.
2. Nabi Muhammad Sallallahu'Alaihi Wa Salam yang menjadi panutan penulis dalam menjalani hidup.
3. Dewi Hastuti & Azkari Amin selaku orang tua penulis yang selalu mendoakan dan memberi motivasi kepada penulis.
4. (Alm) Hj. Badariah selaku nenek penulis yang menjadi motivator seumur hidup bagi penulis.
5. Prof. Dr. H. Nurman, S.Sos., M.Si selaku paman penulis yang selalu memberikan motivasi dan dorongan dalam masa perkuliahan.
6. H. Masud, S.Pd selaku paman penulis yang selalu memberikan motivasi dan bimbingan dalam masa perkuliahan.
7. Seluruh Keluarga Besar yang memberikan doa dan semangat kepada penulis dalam menjalani kehidupan.
8. Bapak Dr. Eng. Muslim, S.T., MT selaku Dekan Fakultas Teknik Universitas Islam Riau.

9. Ibu Dr. Mursyidah, M.Sc selaku Wakil Dekan I, Bapak Dr. Anas Puri, S.T., M.T selaku Wakil Dekan II dan Bapak Akmar Efendi, S.Kom., M.Kom selaku Wakil Dekan III.
10. Bapak Dr. Apri Siswanto,S.Kom., M.Kom selaku Ketua Program Studi Teknik Informatika.
11. Seluruh Dosen Program Studi Teknik Informatika yang mendidik serta memberi arahan.
12. Tata Usaha yang telah membantu dan mempermudah dalam pengurusan administrasi.
13. Teman – teman Angkatan 17 Teknik Informatika UIR yang selalu memberikan dukungan kepada penulis.
14. Wirda Aprilia Ningsih, S.Hut selaku pasangan penulis yang selalu memberikan motivasi, semangat serta doanya dan juga aktor dibalik layar dalam segala kesulitan bagi penulis.

Penyusun menyadari bahwa dalam penyusunan laporan skripsi ini masih banyak kekurangan, untuk itu dengan segala kerendahan hati penulis mengharapkan saran dan kritik yang sifatnya membangun guna memperbaiki laporan skripsi ini.

Akhir kata semoga laporan skripsi ini dapat menambah ilmu pengetahuan khususnya bagi penulis dan bermanfaat bagi semua pihak yang membacanya.

Pekanbaru, 30 Januari 2024

Muhammad Alhaqi

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

Evaluasi Keamanan Websiste Terhadap Kerentanan Serangan *Hacker* Dengan Metode *Penetration Test* Menggunakan OWASP ZAP (Studi Kasus : SiPA Fakultas Teknik)

Muhammad Alhaqi

Laboratorium Teknik Informatika
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Riau

ABSTRAK

Keamanan informasi merupakan hal yang harus diperhatikan bagi setiap pengguna website agar terhindar dari gangguan atau tindakan kejahatan. Masalah keamanan atau gangguan banyak bertebaran di internet, gangguan tersebut bisa berupa serangan Malware, Eksploitasi, Injeksi database dan lain sebagainya. Informasi yang paling sering dicuri adalah data pribadi (36%) dan kekayaan intelektual (11%). Individu lebih cenderung memiliki kredensial dan data pribadi yang dicuri, masing-masing sebesar 41% dan 24%, diperlukan sebuah evaluasi pada sebuah website dalam upaya untuk melindungi website dari serangan atau aksi yang tidak diinginkan yang dapat merusak atau mencuri data dari website tersebut. Evaluasi Keamanan Websiste Terhadap Kerentanan Serangan Hacker Dengan Metode *Penetration Test* Menggunakan *Open Web Application Security Project* (OWASP) ZAP agar dapat membantu pengembang website dalam menjaga keamanan website tersebut dari serangan pihak luar yang tidak bertanggung jawab dan menyalahgunakan data yang ada pada website tersebut. Pengujian menggunakan metode penetration test terhadap beberapa serangan rentan akan penyadapan dari user tidak bertanggungjawab. Celah yang didapat adalah XSS *Injection, Absence of Anti-CSRF tokens, Missing anti-clickjacking, Cross-Domain JavaScript Source File Inclusion*.

Kata Kunci : *Penetration Testing*, OWASP ZAP, *Cyber Security*.

Evaluation of Website Security Against Vulnerability to Hacker Attacks With the Penetration Test Method Using OWASP ZAP (Case Study: SiPA Faculty of Engineering)

Muhammad Alhaqi

Informatics Engineering Laboratory
Informatics Engineering Study Program, Faculty of Engineering, Riau Islamic **University**

ABSTRACT

Information security is something that every website user must pay attention to in order to avoid interference or criminal acts. There are many security problems or disturbances scattered on the internet, these disturbances can be in the form of Malware attacks, exploits, database injections and so on. The information most frequently stolen is personal data (36%) and intellectual property (11%). Individuals are more likely to have their credentials and personal data stolen, at 41% and 24% respectively, requiring an evaluation of a website in an effort to protect the website from attacks or unwanted actions that could damage or steal data from the website. Evaluation of Website Security Against Vulnerability to Hacker Attacks Using the Penetration Test Method Using the Open Web Application Security Project (OWASP) ZAP in order to assist website developers in maintaining the security of the website from attacks by irresponsible external parties who misuse the data on the website. The test uses the penetration test method against several attacks that are vulnerable to eavesdropping from irresponsible users. The gaps found are XSS Injection, Absence of Anti-CSRF tokens, Missing anti-clickjacking, Cross-Domain JavaScript Source File Inclusion.

Keywords: Penetration Testing, OWASP ZAP, Cyber Security.

BAB I
PENDAHULUAN

1.1 Latar Belakang

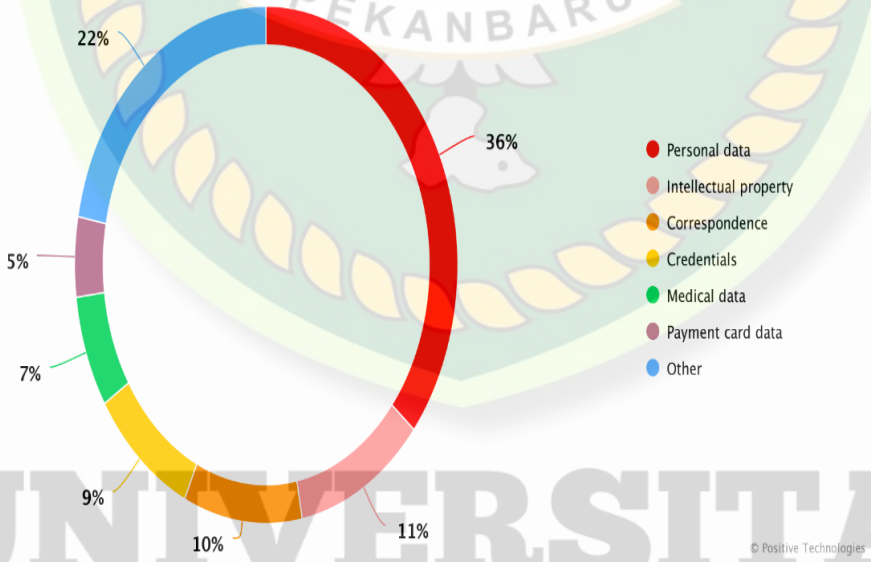
Sejarah website dimulai pada tahun 1991, ketika Tim Berners-Lee, seorang ilmuwan di CERN, mengembangkan *World Wide Web* (WWW) sebagai sarana untuk berbagi informasi di internet. Sejak saat itu, website telah mengalami perkembangan yang pesat, mulai dari website sederhana yang hanya berisi teks, hingga website yang kompleks dengan fitur interaktif dan multimedia. Sebuah situs web biasanya ditempatkan pada sebuah server web yang dapat diakses melalui jaringan seperti Internet, ataupun jaringan wilayah lokal (LAN) melalui alamat Internet yang dikenali sebagai *Unerversal Resource Locator* (URL)

Dalam pengembangan website, teknologi juga berperan penting. Pada awalnya, website dibuat dengan menggunakan HTML (*Hypertext Markup Language*) dan CSS (*Cascading Style Sheets*), tetapi seiring berkembangnya teknologi, bahasa pemrograman seperti JavaScript dan PHP juga mulai digunakan dalam pembuatan website. Selain itu, teknologi seperti *Content Management System* (CMS) dan framework seperti Ruby on Rails dan AngularJS juga digunakan dalam pengembangan website.

Fakultas Teknik Universitas Islam Riau (UIR) menyediakan beberapa fitur yang menjadi sarana bagi mahasiswa salah satunya adalah website Sistem Pelaporan Akademik Fakultas Teknik atau SiPA FT UIR. Website tersebut disediakan oleh fakultas untuk mempermudah mahasiswa dalam pengurusan administrasi yang berkaitan dengan kegiatan Kerja Praktek mulai dari pengurusan izin kerja praktek hingga pengurusan SK pembimbing kerja praktek. Pada website tersebut memiliki beberapa informasi penting yang dijaga kerahasiaannya. Oleh

karena itu pengembang website harus selalu melakukan maintenance terhadap security website sehingga meminimalisir pencurian data dari pihak yang tidak bertanggung jawab.

Keamanan informasi merupakan hal yang harus diperhatikan bagi setiap pengguna website agar terhindar dari gangguan atau tindakan kejahatan. Masalah keamanan atau gangguan banyak bertebaran di internet, gangguan tersebut bisa berupa serangan Malware, Eksploitasi, Injeksi database dan lain sebagainya. Berdasarkan survey yang dilakukan oleh media Cyber Security diketahui bahwa lebih dari sepertiga serangan terhadap website di kuratal kedua 2022 mengakibatkan kebocoran informasi rahasia, lebih sedikit dibandingkan kuartal sebelumnya. Informasi yang paling sering dicuri adalah data pribadi (36%) dan kekayaan intelektual (11%). Individu lebih cenderung memiliki kredensial dan data pribadi yang dicuri, masing-masing sebesar 41% dan 24%.



Gambar 1. 1 Data Kebocoran Informasi Menurut Cybersecurity

Peretasan website adalah tindakan yang dilakukan oleh peretas untuk menemukan dan mengeksploitasi kerentanan dalam website untuk melakukan aksi yang tidak diinginkan, seperti mencuri data, menyebarluaskan malware, atau mengubah konten website. Ada beberapa jenis peretasan website yang sering terjadi, di antaranya: *SQL injection, Cross-Site Scripting (XSS), Distributed Denial of Service (DDoS), File Inclusion Vulnerabilities, Phishing, Website Defacement*.

Dari permasalahan diatas, maka diperlukan sebuah evaluasi pada sebuah website dalam upaya untuk melindungi website dari serangan atau aksi yang tidak diinginkan yang dapat merusak atau mencuri data dari website tersebut sehingga penulis membuat penelitian tentang "Evaluasi Keamanan Websiste Terhadap Kerentanan Serangan Hacker Dengan Metode *Penetration Test* Menggunakan *Open Web Application Security Project* (OWASP) ZAP " agar dapat membantu pengembang website dalam menjaga keamanan website tersebut dari serangan pihak luar yang tidak bertanggung jawab dan menyalahgunakan data yang ada pada website tersebut.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang dikemukakan diatas, maka masalah dapat di identifikasi sebagai berikut :

1. Adanya celah keamanan yang memungkinkan akses data untuk pihak yang tidak bertanggung jawab.
2. Timbulnya kerugian terhadap pengguna website SiPA FT UIR terhadap kebocoran data.

1.3 Rumusan Masalah

Dari penjelasan latar belakang diatas, dapat dihasilkan suatu perumusan masalah yaitu :

1. Bagaimana identifikasi risiko celah keamanan yang dapat ditimbulkan dengan adanya eksploitasi celah keamanan tersebut ?
2. Bagaimana analisa risiko dari hasil identifikasi risiko yang dilakukan ?

1.4 Batasan Masalah

1. Penelitian dilakukan pada website SiPA Fakultas Teknik Universitas Islam Riau.
2. *Penertastion Testing* dilakukan dengan menggunakan Aplikasi OWASP ZAP.
3. Tes yang dilakukan hanya untuk menganalisis celah website agar dapat dijadikan bahan pertimbangan untuk evaluasi pengembangan website.
4. Hasil akhir berupa laporan tentang celah website SiPA FT UIR.

1.5 Tujuan dan Manfaat Penelitian

1.5.1 Tujuan Penelitian

Adapun tujuan yang dapat diperoleh dari penelitian ini adalah sebagai berikut :

1. Melakukan analisis celah keamanan dengan metode *penetration test* untuk memastikan ada atau tidaknya celah keamanan yang memungkinkan akses data untuk pihak yang tidak berhak.

2. Memperoleh informasi dari metode *penetration test*, sebagai pertimbangan pengembang untuk menutup celah keamanan pada website tersebut.

1.5.2 Manfaat Penelitian

Penelitian ini diharapkan dapat membantu pengembang website dalam mengevaluasi website dari perspektif keamanan informasi. Selain itu, penelitian ini juga dapat diharapkan sebagai bahan pertimbangan dalam pengembangan website terkait dengan keamanan informasi, baik secara teknis maupun non teknis.

BAB II

LANDASAN TEORI

2.1. Tinjauan Pustaka

Penelitian yang dilakukan oleh Syarif & Desky (2021) tentang " *Penetration Testing* pada Website Universitas ARS Menggunakan *Open Web Application Security Project* (OWASP) " mendapatkan kesimpulan bahwa jumlah kerentanan website Universitas ARS yang berhasil dipindai adalah 13 kerentanan yang dapat di uji. Dari 13 kerentanan tersebut ada 1 kerentanan yang berada pada tingkat ancaman yang sedang, yaitu X-Frame-Options Header Not Set dan 12 kerentanan yang berada pada tingkat ancaman yang rendah. Sehingga keamanan website Universitas ARS sudah baik karena berdasarkan aspek keamanan informasi CIA TRIAD yaitu confidentiality, integrity dan availability terpenuhi, tetapi hanya pada aspek keamanan integration sedikit kurang terpenuhi karena Header X-Frame-Options tidak diatur pada kelima subdomain sehingga frame dapat mudah dimuat di dalam website lain yang mengganggu keutuhan informasi.

Berdasarkan penelitian yang dilakukan oleh Guntoro, Loneli & Musfawati (2020) berjudul "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)" dapat disimpulkan bahwa sistem OJS Universitas Lacang Kuning tergolong aman. Tetapi terdapat beberapa kelemahan yaitu sistem tidak bisa memblokir ketika user melakukan berkali-kali kesalahan dalam proses login. Berdasarkan pengujian menggunakan OWASP Zap tergolong ke dalam level medium. Dikarenakan sistem yang digunakan adalah menggunakan Open Source OJS. Tetapi walaupun tergolong aman, serangan bisa saja terjadi dari berbagai

pihak, baik dari dalam kampus sendiri atau serangan dari virus.

Berikutnya penelitian yang dilakukan oleh Yum Thurfah (2021) tentang "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx" dapat disimpulkan bahwa dapat disimpulkan bahwa metode OWASP TOP 10 efektif dijadikan sebagai standard keamanan untuk melakukan uji penetrasi terhadap suatu website. Hal itu disebabkannnya dengan standard keamanan yang dimiliki OWASP lengkap dan detail dilihat dari konfigurasi halaman website maupun konfigurasi server. Banyak hasil temuan yang mengacu pada 10 standard keamanan OWASP tersebut. Maka dari itu metode OWASP TOP 10 menjadi rekomendasi untuk para pentester dalam melakukan uji penetrasi menggunakan Metode OWASP Top 10 2017. Adapun celah keamanan yang ditemukan adalah *Broken Authentication, Sensitive* Data *Exposure*, dan Security *Misconfiguration*. Adapun celah lain yang ditemukan namun tidak termasuk dalam TOP 10 keamanan OWASP yaitu *Clickjacking*.

Dalam penelitian Moh Yunus (2019) tentang "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4" dapat ditarik kesimpulan ahwa analisis kerentanan aplikasi berbasis web dengan teknik OWASP versi 4 mampu mengetahui keamanan suatu aplikasi. Metode OWASP versi 4 dapat dijadikan sebagai standar penilaian keamanan aplikasi berbasis web berdasarkan hasil pengujian kerentanan pada website yang beralamat di www.xyz.com dari beberapa tahapan kategori yaitu pada tahap *Authentication Testing Authorization, Session Management Testing, Input Validation Testing, dan Error Handling*.

Berdasarkan penelitian yang dilakukan oleh Dimas, Asep & Muhammad Hasbi (2023) yang berjudul "Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating" ditemukan 9 jenis kerentanan dengan tingkat high, medium, dan low. Kerentanan tersebut terdiri dari 2 jenis kerentanan dengan tingkat high, 1 jenis kerentanan dengan tingkat medium, dan 6 jenis kerentanan dengan tingkat low. Setelah melakukan uji penetrasi sebagai bentuk validasi kerentanan, dari 9 jenis kerentanan terdapat dua yaitu Shell Injection dan Timestamp Disclousure tidak dapat dilakukan pengujian karena adanya proses maintenance dan patching sehingga tidak ditemukan lagi kerentanan tersebut.

Dalam penelitian Kasamuddin (2012) yang berjudul "Dampak Sniffing Pada Keamanan Data Di Jaringan LAN" menjelaskan bahwa kelemahan atau celah yang ada pada system keamanan di dalam jaringan bisa digunakan oleh penyusup pencurian data yang dilakukan menggunakan teknik sniffing atau teknik pencurian data lainnya. Berdasarkan penelitian yang dilakukan sangat penting untuk pengguna komputer khususnya yang sering terkoneksi ke jaringan komputer untuk melakukan pengiriman dan penerimaan data, sangat perlu mengetahui hal-hal apa saja yang perlu dilakukan akan dapat melakukan transaksi data dengan aman, sehingga tidak terjadi hal yang merugikan pada dirinya sendiri.

Berdasarkan penelitian Khairunnisa & Muklas (2021) mendapatkan bahwa Tinjauan pengujian keamanan sistem informasi, khususnya yang berkaitan dengan aplikasi situs web, disediakan dalam penelitian ini. Pengujian keamanan sangat penting dalam memberikan keamanan dan kenyamanan kepada klien kerangka kerja. Ada sejumlah kelemahan dan kerentanan dalam sistem yang dapat

ditemukan dengan mencari lubang keamanan dan menguji lubang keamanan. Karena pihak yang tidak memiliki akses dapat memanfaatkan kelemahan ini.

Dalam penelitian ini dilakukan pengujian penetrasi menggunakan metode ISSAF dan OWASP versi 4 yang bertujuan untuk menguji tingkat keamanan sistem OJS journal.unilak.ac.id. dan didapat bahwa OJS tersebut masih dalam kategori aman tidak mampu ditembus oleh kedua aplikasi yang digunakan, tetapi serangan bisa saja terjadi dengan menggunakan cara lain, sehingga perlu ditingkatkan lagi untuk keamanan website tersebut (Guntoro, 2020).

Berdasarkan penelitian dari Desi & Kadek (2021) ditemukan sebuah celah pada sistem login yaitu tidak menerapkan *Rate limiting* pada bagian Login sehingga memungkinkan untuk serangan *brute force attack*. Kerentanan *rate limiting* akan memberikan resiko adanya *request* yang berlebihan pada suatu fungsi yang harusnya dibatasi. Kemudian kerentanan XSS yang memungkinankan melakukan injeksi kode berbahaya pada sistem, terlebih lagi kerentanan ijeksi ini merupakan rangking pertama pada OWASP.

Berdasarkan pengujian keamanan website menggunakan metode *Vulnerability Assessment* dapat disimpulkan bahwa setelah dilakukan serangkaian pengujian, terdapat dua pengujian yang memiliki status tidak aman diantaranya XML-RPC dan Port 80 Service *HTTP (Hyper Text Transfer Protocol).* Adanya kerentanan tersebut dapat mengancam keamanan website jika tidak dilakukan perbaikan, oleh karna itu peneliti telah merekomendasikan solusi perbaikan. Setelah solusi perbaikan yang disarankan sudah selesai dikerjakan lalu dilakukan pengujian ulang serta nilai kerentanan dihitung Kembali (Ari Marta, 2019).

2.2. Dasar Teori

2.2.1. Website

Web merupakan kumpulan dokumen-dokumen multimedia yang saling terhubung satu sama lain yang menggunakan protokol HTTP dan untuk mengaksesnya menggunakan browser (Charolina, 2017).Sejarah web sendiri dimulai pada tahun 1989 ketika Tim Berner Lee Fisikawan CERN (Consei European pour la Recherce Nuclaire) mengajukan protokol sistem distribusi informasi internet yang digunakan untuk berbagai informasi diantara para fisikawan. Protokol inilah yang selanjutnya dikenal sebagai Protokol *World Wide Web* dan dikembangkan oleh World Wide Web Consortium.

Pada mulanya aplikasi web dibangun hanya dengan menggunakan bahasa yang disebut HTML (Hyper Text Markup Language) dan protokol yang digunakan dinamakan HTTP (HyperText Transfer Protokol). Pada perkembangan berikut, sejumlah skrip dan objek dikembangkan untuk memperluas kemampuan HTML, antara lain PHP . Dengan memperluas kemampuan HTML, yakni dengan menggunakan perangkat lunak tambahan, perubahan informasi dalam halaman-halaman web dapat ditangani melalui perubahan data, bukan melalui perubahan program. Sebagai implementasinya, aplikasi web dikoneksikan ke basis data. Dengan demikian perubahan informasi dapat dilakukan oleh operator atau yang bertanggung jawab terhadap kemutakhiran data, dan tidak menjadi tanggung jawab programer atau webmaster.

2.2.2. Keamanan Website

Keamanan website adalah upaya untuk melindungi website dari serangan atau aksi yang tidak diinginkan yang dapat merusak atau mencuri data dari website tersebut. Ada beberapa hal yang perlu dipertimbangkan dalam menjaga keamanan website, diantaranya:

1. Keamanan server: Pastikan server yang digunakan untuk menjalankan website dikonfigurasi dengan aman dan diperbarui secara reguler.
2. Proteksi dari serangan DDoS: Distributed Denial of Service (DDoS) adalah serangan yang dilakukan dengan menghabiskan sumber daya server dengan membuat permintaan yang berlebihan. Beberapa teknik yang dapat digunakan untuk melindungi website dari serangan DDoS adalah menggunakan firewall, Content Delivery Network (CDN), dan Proxies.
3. Enkripsi data: Enkripsi digunakan untuk melindungi data yang dikirim dan diterima oleh website dari pihak yang tidak berwenang. HTTPS adalah salah satu contoh dari enkripsi yang digunakan dalam website.
4. Autentikasi dan otorisasi: Pastikan hanya pengguna yang sah yang dapat mengakses website dan informasi yang ada di dalamnya.
5. Keamanan aplikasi: Pastikan aplikasi yang digunakan dalam website diperbarui secara reguler dan dikonfigurasi dengan aman.
6. Keamanan input: Pastikan untuk melakukan validasi input yang masuk ke website, untuk mencegah serangan SQL injection dan Cross-site scripting (XSS)

7. Analisa log: Analisa log dapat digunakan untuk mengetahui aktivitas yang tidak diinginkan pada website dan membantu dalam deteksi serangan.
8. Penetration Testing : Uji penetrasi digunakan untuk mengetahui kelemahan yang ada pada website, dan memungkinkan untuk mengambil tindakan untuk mengatasi masalah tersebut.
9. Penyimpanan data : Pastikan data yang disimpan dalam website aman dari akses yang tidak sah dan dapat dipertahankan.

Keamanan website merupakan hal yang sangat penting karena website menyimpan banyak informasi penting yang dapat digunakan oleh peretas untuk melakukan aksi yang tidak diinginkan. Oleh karena itu, perlu dilakukan tindakan pencegahan dan deteksi untuk menjaga keamanan website.

2.2.3. SSL (*Secure Socket Layer*)

Secure Socket Layer adalah salah satu metode keamanan dalam bentuk sebuah protokol yang berada di atas Transmission Control Protocol/Internet Protocol (TCP/IP) yang berfungsi untuk mengamankan browsing web, mengelola keamanan transmisi dan juga dapat menjamin keamanan dalam pengiriman data dan pengaksesan informasi pada saat client dan server sedang melakukan pertukaran informasi lewat internet SSL memungkinkan informasi sensitif seperti data kartu kredit, *username*, *password* dan informasi penting ditransmisikan cari server ke client atau sebaliknya dengan aman karena data yang dikirim akan diaca (dienkripsi).(catur Iswahyudi 2019).

2.2.4. *Penetration Testing*

Penetration testing adalah alat penilaian jaminan bernilai yang menguntungkan baik bisnis dan operasinya. Dari segi operasional, penetration testingmembantu membentuk strategi keamanan informasi melalui identifikasi kerentanan yang cepat dan akurat. Penetration testingmembagikan informasi rinci tentang ancamanan keamanan secara aktual, yang dapat dieksploitasi jika tercakup dalam aliran dan proses keamanan organisasi. Hal ini akan membantu organisasi untuk mengidentifikasi dengan cepat dan akurat, potensi kerentanan yang nyata

2.2.5. *Vulnerability*

Vulnerability adalah Kelemahan dari sebuah aset atau sekumpulan aset yang dapat dimanfaatkan oleh satu atau lebih ancaman (ISO 27005). Sedangkan menurut definisi dari IETF (Internet Engineering Task Force) melalui RFC 2828 *vulnerability* adalah sebuah celah atau kelemahan dalam sebuah system, baik dalam desain, implementasi, atau operasional dan manajemen yang dapat dimanfaatkan untuk menyerang sebuah system informasi.

2.2.6. *Injection Attack*

Injection Attack adalah jenis serangan keamanan di mana penyerang menyisipkan atau menyuntikkan kode berbahaya ke dalam input atau data yang diterima oleh aplikasi. Tujuannya adalah untuk memanfaatkan kelemahan dalam pengolahan data tersebut dan mengakibatkan eksekusi kode yang tidak sah atau mendapatkan akses tidak sah ke sistem. Ada beberapa jenis serangan injection yang umum, termasuk:

1. SQL *Injection* (SQLi): Ini adalah jenis serangan di mana penyerang memasukkan instruksi SQL yang tidak sah ke dalam input aplikasi yang berinteraksi dengan basis data. Jika input tidak dikelola dengan benar, instruksi SQL palsu dapat dijalankan, memberikan penyerang akses ke data yang seharusnya tidak dapat diakses atau bahkan memungkinkan mereka untuk menghapus atau mengubah data.
2. *Cross-Site Scripting* (XSS): Pada serangan XSS, penyerang menyisipkan skrip berbahaya (biasanya JavaScript) ke dalam halaman web yang kemudian dijalankan oleh browser pengguna yang mengakses halaman tersebut. Ini memungkinkan penyerang untuk mencuri informasi, sesi login, atau bahkan mengarahkan pengguna ke situs palsu.
3. LDAP Injection: Dalam serangan ini, penyerang memasukkan input yang merusak ke dalam permintaan LDAP (*Lightweight Directory Access Protocol*) untuk mendapatkan akses ke direktori atau data yang diinginkan.
4. XML Injection: Penyerang memasukkan data berbahaya ke dalam input XML yang kemudian dapat mengganggu pemrosesan XML atau mengungkapkan informasi sensitif.
5. *Command Injection*: Pada serangan ini, penyerang menyuntikkan perintah sistem operasi yang berbahaya ke dalam input yang kemudian dijalankan oleh sistem. Ini dapat mengakibatkan eksekusi perintah yang tidak sah dan memberikan kontrol kepada penyerang atas sistem.

2.2.7. *Cross-Site Request Forgery* (CSRF)

Cross-Site Request Forgery (CSRF) adalah jenis serangan keamanan di dunia web di mana penyerang memanfaatkan kredensial otentikasi yang sah

dari pengguna yang sudah terautentikasi untuk melakukan tindakan yang tidak diinginkan atau tidak disengaja pada suatu situs web, tanpa sepengetahuan atau izin pengguna yang terpengaruh. Serangan CSRF melibatkan meyakinkan pengguna untuk melakukan tindakan tertentu, seperti mengklik tautan atau mengirim permintaan HTTP, yang tanpa disadari akan memicu tindakan di situs web yang mereka sudah otentikasi sebelumnya. Ini dapat menyebabkan perubahan status, pengiriman data pribadi, atau bahkan tindakan yang merugikan.

Contoh sederhana serangan CSRF:

1. Seorang penyerang membuat tautan palsu yang mengirimkan permintaan HTTP untuk mengubah kata sandi pengguna di situs target.
2. Penyerang kemudian mengirim tautan ini ke pengguna yang sudah terautentikasi di situs target.
3. Jika pengguna mengklik tautan tanpa curiga, permintaan HTTP akan diizinkan oleh server karena kredensial otentikasi yang sah dimiliki oleh pengguna.
4. Akibatnya, kata sandi pengguna diubah oleh penyerang tanpa sepengetahuan pengguna.

2.2.8. XML *Injection*

XML Injection adalah jenis serangan keamanan di mana penyerang menyisipkan atau memodifikasi data berbahaya ke dalam dokumen XML yang diolah oleh aplikasi atau sistem. Tujuannya adalah untuk memanipulasi pemrosesan XML dan mengakibatkan tindakan yang tidak sah atau mendapatkan akses yang tidak diinginkan ke sistem.

Dalam XML Injection, penyerang mencoba memanfaatkan celah dalam pemrosesan XML, yang biasanya terjadi ketika aplikasi tidak memvalidasi atau membersihkan input XML dengan benar sebelum memprosesnya. Hasilnya, data yang tidak aman dapat diintegrasikan ke dalam dokumen XML dan dieksekusi oleh aplikasi, yang dapat mengakibatkan sejumlah masalah keamanan. Jika aplikasi tidak memvalidasi input dengan benar, dan mengizinkan kode JavaScript dieksekusi dalam output XML yang dihasilkan, maka pengguna yang melihat laporan ini dapat menjadi korban serangan *Cross-Site Scripting* (XSS).

2.2.9. *Insecure Deserialization*

Insecure Deserialization adalah kerentanan keamanan yang muncul saat data yang diserialisasi (biasanya dalam format seperti JSON atau XML) tidak dikelola dengan benar saat didekode kembali menjadi objek oleh suatu aplikasi atau sistem. Serangan terhadap celah ini dapat memungkinkan penyerang untuk menyusupkan objek yang berbahaya atau kode berbahaya ke dalam data yang diserialisasi, yang kemudian dapat diaktifkan saat didekode. Proses deserialisasi penting dalam banyak aplikasi yang berinteraksi dengan data yang diterima dari luar, seperti data yang diterima dari pengguna atau data yang diterima melalui jaringan. Jika data ini tidak divalidasi, disaring, atau dikelola dengan benar sebelum deserialisasi, maka penyerang dapat memanfaatkan celah ini untuk merusak, mengambil alih, atau merusak sistem.

2.2.10. OWASP ZAP

OWASP merupakan sebuah komunitas online yang memiliki berbagai proyek untuk memproduksi artikel, metodologi, dokumentasi, aplikasi, serta

teknologi yang berbasis *Free* dan *Open Source* di bidang keamanan aplikasi web. Berbagai proyek tersebut antara lain adalah:

1. **OWASP Top 10**, yang merincikan sepuluh kelemahan utama dalam aplikasi web saat ini
2. **OWASP Proactive Controls**, yang merincikan sepuluh teknik keamanan aplikasi web yang efektif
3. **OWASP Application Security Verification Standard (ASVS)**, yang merupakan sebuah standar untuk melakukan verifikasi keamanan aplikasi web
4. **OWASP Software Assurance Maturity Model (SAMM)**, yang merupakan framework dan *toolkit* asesmen untuk membantu organisasi merumuskan serta menerapkan strategi keamanan aplikasi sesuai dengan risiko yang dihadapinya
5. **OWASP Zed Attack Proxy (ZAP)**, yang merupakan *tool* yang dapat digunakan untuk menemukan berbagai lubang keamanan aplikasi web saat pengembangan dan pengujian aplikasi web
6. **OWASP ModSecurity Core Rule Set (CRS)**, yang dapat digunakan dalam penerapan *Web Application Firewall* (WAF) untuk melindungi aplikasi serta server web dari berbagai serangan terhadapnya

Melalui penerapan berbagai proyek OWASP tersebut, suatu organisasi atau perusahaan akan mampu meningkatkan dan menjaga keamanan aplikasi web yang mereka gunakan sehingga risiko dapat diminimalisir secara efektif.

BAB III

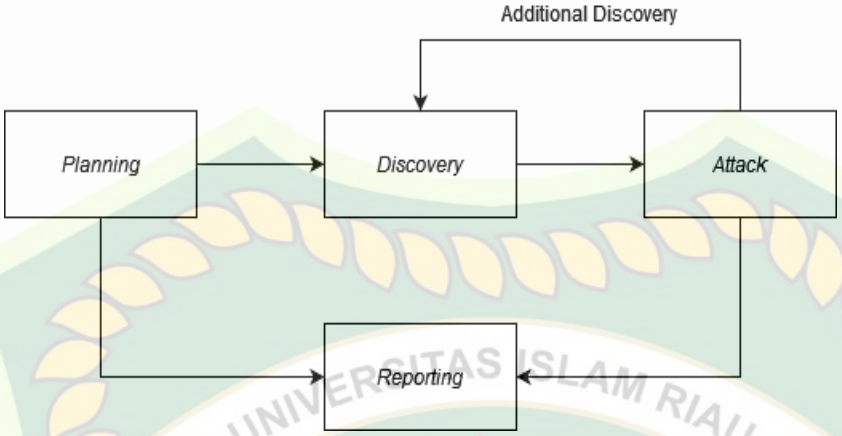
METODOLOGI PENELITIAN

3.1 Metode Penelitian

Adapun metoda yang diterapkan dalam penelitian ini adalah *Penetration Testing*. *Penetration Testing* juga dikenal sebagai *pentest* atau *ethical hacking* adalah proses yang dilakukan untuk menguji keamanan sistem komputer, jaringan, atau aplikasi dengan tujuan mengidentifikasi dan mengeksplorasi kerentanan serta menguji keefektifan kontrol keamanan yang ada. Penetration test dilakukan oleh profesional keamanan informasi yang disebut sebagai *pentest* atau *ethical hacker*.

Tujuan utama dari penetration test adalah untuk menemukan kelemahan atau celah dalam sistem yang dapat dimanfaatkan oleh penyerang. Dalam proses ini, pen tester mencoba melakukan serangan yang sebenarnya menggunakan teknik-teknik yang sama yang dapat digunakan oleh penyerang jahat. Tujuan akhirnya adalah untuk memberikan rekomendasi dan langkah-langkah mitigasi guna meningkatkan keamanan sistem.

Dalam menjalankan pengujian, terdapat 4 tahapan yang dijalankan dalam Penetration Testing yaitu tahap (Perencanaan), *Discovery* (Penemuan), *Attack* (Serangan), dan *Reporting* (Pelaporan) seperti yang dijelaskan pada Gambar 3.1.



Gambar 3. 1 Tahapan Pentest

Berdasarkan gambar 3.1, dapat dijelaskan ada beberapa proses yang dilalui dalam *penetration test* sebagai berikut :

1. *Planning*

   Tahap Perencanaan, Pada tahapan untuk mengidentifikasi target yang akan diuji, tujuan pengujian, batasan, dan lingkup pengujian. Tahap ini juga melibatkan pemahaman dan pemetaan infrastruktur yang akan diuji, termasuk sistem, jaringan, dan aplikasi yang terlibat

2. *Discovery*

   Tahap penemuan, pada tahapan ini bisa terjadi perulangan proses karna sifatnya yang dinamis. Pada tahapan pertama ini dilakukan pengumpulan semua informasi tentang sistem target. Pada tahapan kedua, jika terdapat celah setelah melakukan penyerangan, maka akan masuk Kembali pada tahap ini.

3. *Attack*

   Tahap Penyerangan, pada tahapan ini adalah percobaan mengeksploitasi kerentanan yang ada dalam sistem menggunakan berbagai teknik

serangan yang sesuai. Tujuannya adalah untuk mendapatkan akses yang tidak sah atau mengungkap informasi sensitif.

4. *Reporting*

   Setelah pengujian selesai, pentes menyusun laporan lengkap yang berisi hasil temuan, tingkat kerentanan, dan rekomendasi untuk perbaikan. Laporan ini disampaikan kepada pihak yang meminta untuk mengambil tindakan yang diperlukan.

3.2 Metode Pengumpulan Data

Proses pengumpulan data adalah untuk mendapatkan data yang benar dan menyakinkan, agar hal yang dicapai tidak menyimpang dari tujuan yang telah ditetapkan sebelumnya, penulis melakukan langkah-langkah sebagai berikut :

1. Studi Literatur

   Pada tahapan ini akan dilakukan studi literatur. Studi literatur bertujuan untuk menjelaskan kajian pustaka berdasarkan teori-teori penunjang yang digunakan sebagai bahan penelitian. Adapun studi literatur ini didapatkan dari membaca buku, jurnal, artikel maupun dari internet.

2. Pengumpulan Data

   Pada tahapan ini dilakukan pengumpulan data dengan cara mengumpulkan data target yang akan dilakukan pengujian dengan menggunakan alat yang sudah disiapkan. Adapun pengumpulan data dilakukan dengan mengidentifikasi web SiPA Fakultas Teknik dengan menggunakan aplikasi OWASP ZAP.

3.3 Alat dan Bahan Penelitian

Adapun spesifikasi *Hardware* minimal yang digunakan untuk melakukan simulasi jaringan dan spesifikasi *software* minimal yang dibutuhkan untuk sistem yang akan dibangun adalah sebagai berikut :

3.4.1 Spesifikasi Perangkat Keras *(Hardware)*

Spesifikasi perangkat keras (*Hardware)* minimal yang digunakan dalam pembangunan simulasi sistem ini adalah sebagai berikut :

1. *Processor Intel Core i5-5005U*
2. RAM 4.00 GB
3. *HDD* 300 GB
4. *Operation System Windows 10 Pro x64bit*

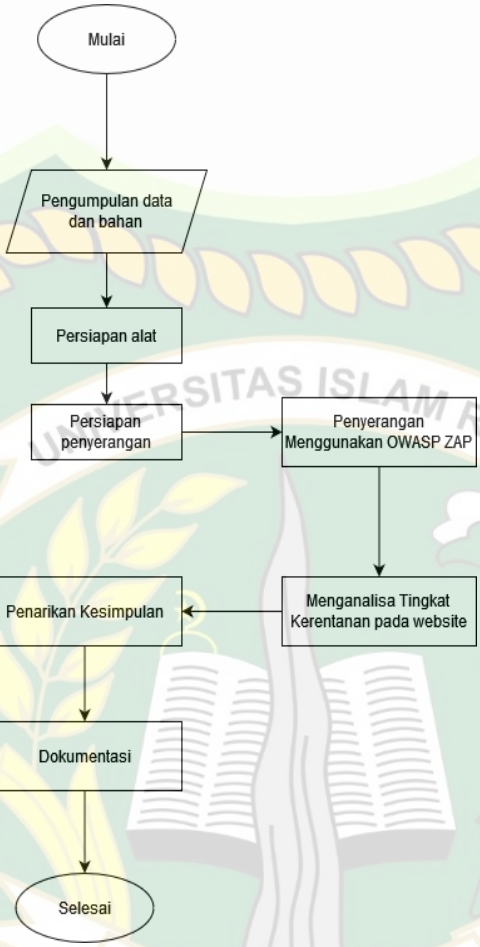
3.4.2 Spesifikasi Perangkat Lunak *(Software)*

Spesifikasi perangkat lunak *(Software)* minimal yang digunakan dalam pembangunan simulasi sistem ini adalah sebagai berikut :

1. Sistem Operasi *Windows 10 pro x64 bit*
2. *OWASP ZAP* digunakan untuk melakukan uji kerentanan terhadap website.

3.4 Alur Penelitian

Dalam menjelaskan sebuah permasalahan alur penelitian disajikan untuk mempermudah pemahaman dalam penelitian tersebut. Metode tersebut tersaji dalam diagram alur penelitian.



Gambar 3. 2 Alur Penelitian

Sesuai dengan alur penelitian pada Gambar 3.2, penelitian ini dilakukan dalam beberapa tahapan.

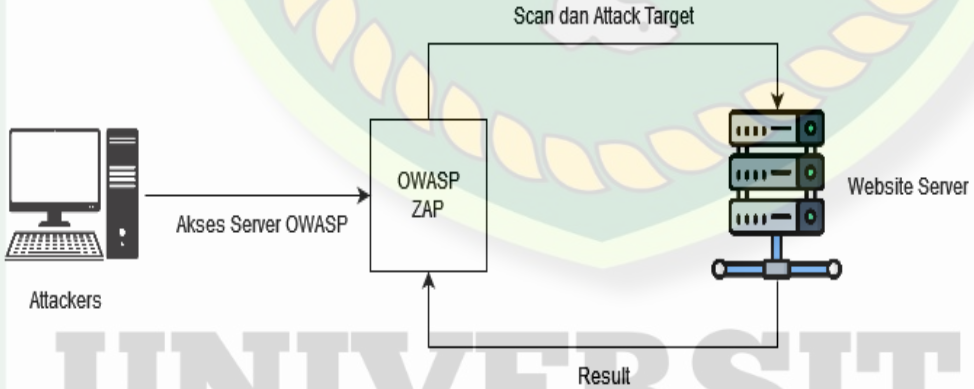
1. Mengumpulkan data dan bahan dengan mempelajari literatur, buku-buku, ebook dan artikel untuk menunjang penelitian.
2. Menyiapkan alat yang dibutuhkkan seperti *hardware dan software* untuk menunjang pelaksanaan penelitian.
3. Melakukan penyerangan terhadap website SiPa Fakultas Teknik untuk mendapatkan informasi kerentanan.

4. Menganalisis data yang diperoleh dari penyerangan menggunakan OWASP ZAP untuk mendapatkan informasi lebih lanjut mengenai kerentanan yang terdapat pada website tersebut.
5. Menarik kesimpulan untuk memutuskan sebuah saran yang bisa digunakan untuk mengamankan website terhadap kerentanan yang ada.

3.5 Pengujian Keamanan

Sebelum penelitian diimplementasikan, perlu dibangun sebuah perencanaan yang nantinya membantu memudahkan jalannya proses pelaksanaan identifikasi pada penelitian. Kegiatan ini biasanya disebut sebagai analisa desain alur *penetration test*.

Pada analisa ini terlibat komponen perangkat yang saling berhubungan, yaitu: jaringan internet, website target, dan perangkat penyerang. Untuk lebih jelasnya dapat dilihat pada gambar berikut.



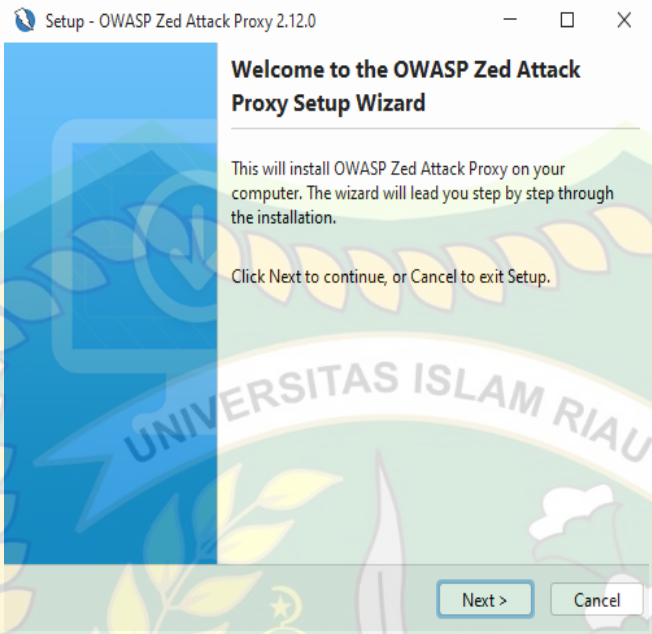
Gambar 3. 3 Desain alur *penetration test*

Setelah mengetahui skema yang ditunjukkan pada Gambar 3.3, maka langkah selanjutnya yaitu pengujian keamanan bertujuan untuk memperoleh kesadaran akan permasalahan terhadap keamanan pada *website* tersebut. Berikut penjelasan dari skema diatas.

1. Penyerang mengakses *software* yang terkoneksi langsung ke server yaitu OWASP ZAP.
2. Setelah masuk kedalam *software* penyerang memasukkan alamat domain dari website yang akan di Analisa kerentanan nya.
3. Proses pertama yang dilakukan oleh OWASP ZAP adalah melakukan *scanning dan attack* terhadap website yang dituju.
4. Setelah melakukan proses *scanning dan attacking* , OWASP ZAP akan memberikan hasil berupa kerentanan dari website tersebut pada halaman result.

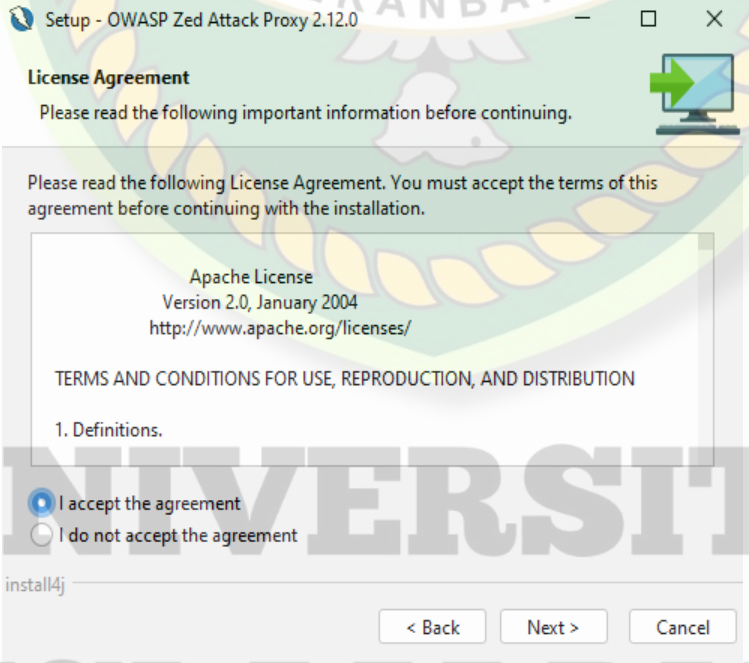
Cara melakukan instalasi OWASP ZAP adalah sebagai berikut.

Pada tahap ini, akan dilakukan instalasi OWASP ZAP yang akan digunakan sebagai *software attacks*. Berikut adalah tahapan-tahapan instalasi OWASP ZAP.



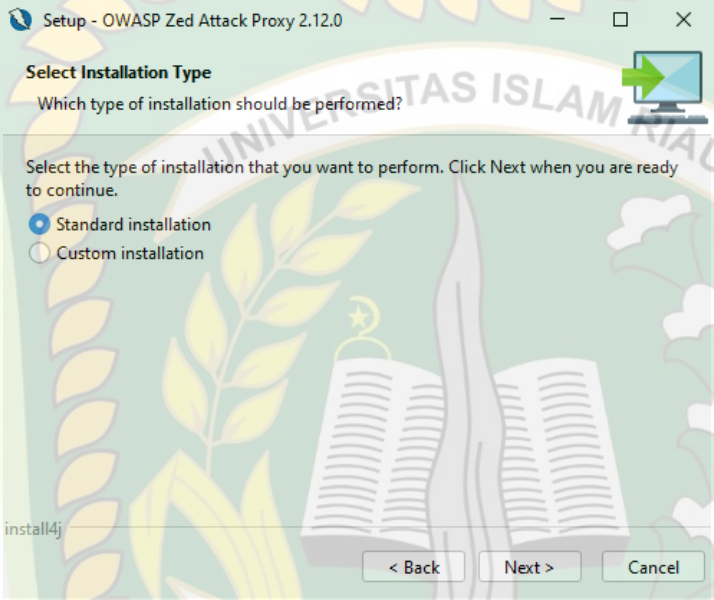
Gambar 3. 4. Langkah Awal Instalasi

Pada ilustrasi di atas, yang disebut sebagai Gambar 4.1, menampilkan tahap awal dalam proses instalasi OWASP ZAP. Pada tahap awal ini, pengguna diminta untuk memilih next untuk melanjutkan Langkah instalasi.



Gambar 3. 5. *License Agreement*

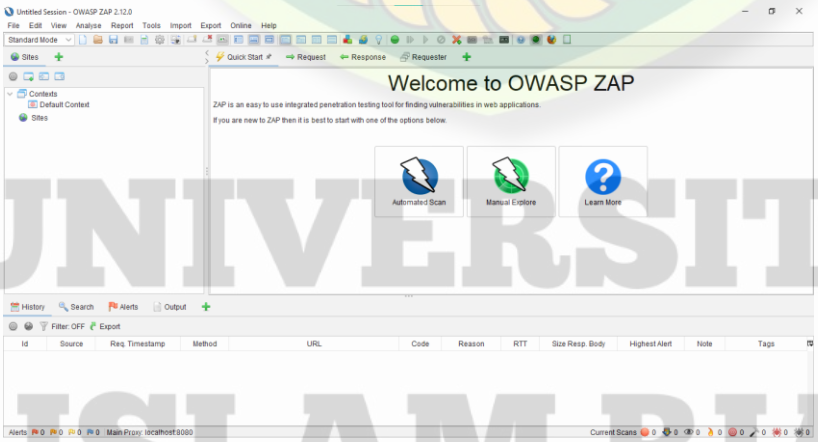
Berdasarkan gambar 3.5 pengguna diharuskan untuk memilih "*I accept the agreement*" agar dapat melanjutkan ke langkah selanjutnya. Setelah itu pilih *standart installation* seperti gambar dibawah ini. Kemudia pilih Instal dan tunggu hingga proses instalasi selesai.



Gambar 3. 6. Tipe Instalasi

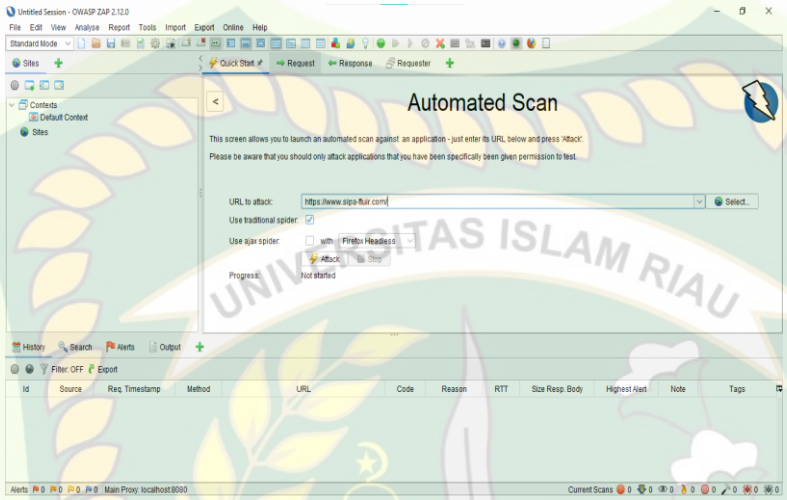
Adapun Langkah-langkah yang dilakukan adalah sebagai berikut :

1. Mengkoneksikan laptop dengan sebuah jaringan internet. Kemudian membuka *software* OWASP ZAP. Berikut tampilan awal aplikasi OWASP ZAP.



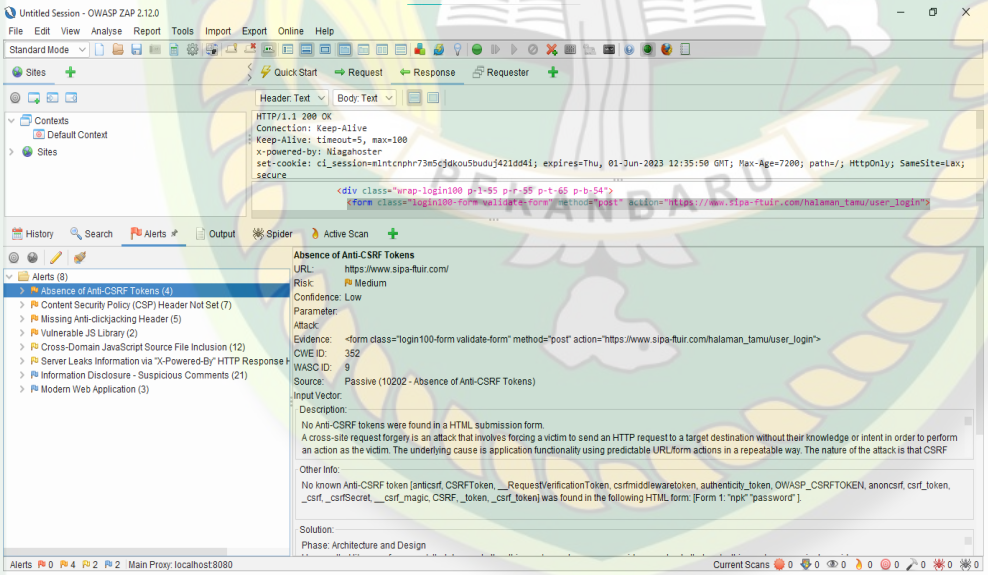
Gambar 3. 7 Tampilan Awal OWASP ZAP

2. Lalu pilih Automated Scan dan masukkan url atau website target. Kemudian Attack



Gambar 3. 8 Konfigurasi OWASP ZAP

3. Tunggu hingga hasil muncul seperti gambar dibawah ini.



Gambar 3. 9 Hasil Scanning Menggunakan OWASP ZAP

Berdasarkan gambar diatas, didapat beberapa kerentanan yang ada pada website target, kerentanan yang dimaksud dapat dilihat pada tabel berikut.

BAB IV

HASIL DAN PEMBAHASAN

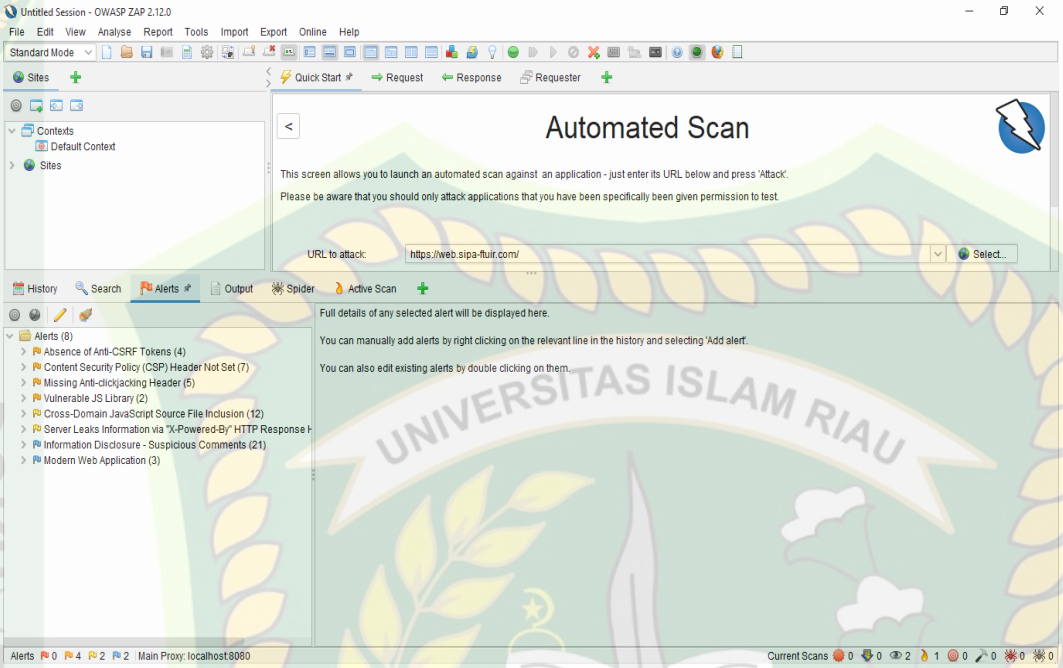
Tahapan terakhir dalam sebuah penelitian yaitu melakukan analisis hasil yang memberikan suatu keluaran penelitian. Berdasarkan metodologi yang telah ditentukan, kegiatan penelitian dianalisis menjadi laporan sederhana yang mudah untuk dimengerti.

4.1. Hasil dan Pembahasan

Analisis ini perlu dilakukan agar dapat mengetahui kerentanan website SiPA Fakultas Teknik Universitas Islam Riau. Seperti umumnya tingkat keamanan bukan berasal dari hardware dan software yang sudah ada namun terdapat peran penting dari manusia / pengguna jaringan yang melakukan kontak atau koneksi dari perancangan jaringan itu sendiri. Hasil dan pembahasan dari penelitian ini akan dilakukan penetration testing pada analisa website SiPA Fakultas Teknik Universitas Islam Riau.

4.1.1. Hasil OWASP ZAP Pada SiPA FT

Pada tahap ini akan dilakukan monitoring terhadap celah yang ada pada website target. Misalnya, celah terhadap *Injection Attack, CSRF* dan lainnya. Pada pengujian ini menggunakan software OWASP ZAP. Cara kerjanya dengan melakukan scanning yang telah dirancang oleh *software* tersebut, sehingga pengguna hanya menunggu hasil akhir dari scanning tersebut.



Gambar 4. 1. Hasil Scanning OWASP ZAP

Berdasarkan gambar diatas, didapat beberapa kerentanan yang ada pada website target, kerentanan yang dimaksud dapat dilihat pada tabel berikut.

Tabel 4. 1. Hasil Uji OWASP ZAP

No	Ancaman	Tingkat Ancaman
1	Content-Security-Policy Header Not Set	Medium
2	Absence of Anti-CSRF tokens	Medium
3	Missing anti-clickjacking	Medium
4	Cross-Domain JavaScript Source File Inclusion	Medium

Berdasarkan tabel diatas, diketahui beberapa celah kerentanan terhadap serangan pada website SiPA. Berikut adalah penjelasan lengkap mengenai ancaman diatas.

1. *Content-Security-Policy Header Not Set*

   Deskripsi : Celah ini berupa code injection atau metode XSS serta memungkinkan SQL Injection.

   Dampak : Penyerang dapat mem-bypass keamanan di sisi klien, mendapatkan informasi sensitif, atau menyimpan aplikasi berbahaya pada website SiPA FT UIR

   Solusi :

   1. Konfigurasikan header HTTP "Content-Security-Policy" dengan kebijakan yang ketat dan hanya memperbolehkan sumber daya yang diperlukan
   2. Perbarui dan uji secara berkala kebijakan CSP untuk memastikan keberlanjutan dan keefektifannya terhadap perkembangan keamanan

2. Absence of Anti-CSRF tokens

   Deskripsi : Tidak ada keamanan terhadap CSRF (Cross-Site Request Forgery)

   Dampak : Penyerang dapat memaksa pengguna yang sudah terautentikasi untuk melakukan tindakan tertentu (misalnya, mengirim formulir, mengubah kata sandi, atau melakukan transaksi keuangan) tanpa persetujuan mereka

   Solusi :

   1. Implementasikan Anti-CSRF Tokens pada formulir dan permintaan aksi yang membutuhkan otentikasi (biasanya terdapat pada laravel)

2. Berikan validasi server-side pada token yang dikirimkan oleh klien untuk memastikan keaslian dan integritasnya.

3. Missing anti-clickjacking

Deskripsi : Clickjacking adalah teknik penipuan di mana penyerang mencoba menyembunyikan elemen-elemen situs web

Dampak : Dapat memanipulasi tindakan pengguna dengan menempatkan elemen situs web yang sebenarnya di bawah elemen-elemen lain yang tampak tidak berbahaya, sehingga mengelabui pengguna untuk melakukan klik tanpa sepengetahuan mereka

Solusi :

1. Evaluasi dan terapkan Content Security Policy (CSP) yang sesuai untuk membatasi penggunaan elemen iframe secara tidak sah
2. Lakukan uji validasi secara berkala untuk memastikan keberlanjutan dan efektivitas perlindungan anti-clickjacking

4. Cross-Domain JavaScript Source File Inclusion

Deskripsi : Sistem web memungkinkan penyisipan (inclusion) berkas JavaScript

Dampak : Dapat menyebabkan eksekusi kode berbahaya pada pengguna akhir, karena berkas JavaScript dari domain yang tidak terpercaya dapat dimuat dan dijalankan pada halaman web

Solusi :

1. Terapkan kebijakan Content Security Policy (CSP) untuk membatasi sumber-sumber yang diizinkan untuk memuat berkas JavaScript.
2. Hindari penggunaan "wildcard" (*) dalam header CORS (Cross-Origin Resource Sharing) dan tentukan dengan tepat domain sumber daya yang diizinkan.

4.1.2. Hasil Penetration Testing Menggunakan Tools Lainnya

Berikut adalah hasil pengujian menggunakan tools lainnya.

Tabel 4. 2 Celah pada *jQuery 3.2.1-3.3.1*

jQuery 3.2.1-3.3.1		
CVSSv3.1 Score	**Vulnerability CVE-IDCVE**	**Vulnerability Type**
5.5 Medium	CVE-2020-11022	CWE-79- Cross Site Scripting
4.8 Medium	CVE-2019-11358	CWE-400- Prototype Pollution
4.1 Medium	CVE-2020-11023	CWE-79- Cross Site Scripting

Kesimpulan dan Saran : Komponen versi jQuery 3.2.1-3.3.1 sudah usang dan dapat menyebabkan kerentanan Cross-Site Scripting – or XSS yang berdampak pada pengguna situs web dengan menyuntikan konten berbahaya dan memungkin pelaku mengeksploitasi identitas pengguna yang disimpan dalam aplikasi dan mengalihkan lalu lintas situs web, untuk meminimalisir kerantanan komponen jQuery harus segera diupdate ke versi yang lebih baru 3.7.1.

Tabel 4. 3 Celah pada *Moment.js 2.13.0*

Moment.js 2.13.0		
CVSSv3.1 Score	**Vulnerability CVE-ID CVE**	**Vulnerability Type**
6.5 Medium	CVE-2022-24785	CWE-22 – Path Traversal

Kesimpulan dan Saran : Komponen Moment.js 2.13.0 sudah usang dan rentan terhadap penjelajahan jalur berdampak pada pengguna npm(server) moment.js terutama jika string lokal yang disediakan pengguna secara langsung digunakan untuk mengganti moment lokal, dalam meminimalisir kerantanan komponen Momen.js harus segera diupdate ke versi yang lebih baru 2.30.1

Tabel 4. 4 Celah Pada SSL/TLS

SSL/TLS: Cipher Suites Rentan Untuk HTTPS		
CVSS Score	**Vulnerability CVE-ID CVE**	**Vulnerability Type**
7.5 High	CVE-2016-2183	Blok Cipher 64-bit 3DES

Kesimpulan dan Saran : Hasil dari penetration test ini memberikan informasi bahwa semua cipher suite SSL/TLS yang diterima oleh layanan dimana vektor serangan hanya ada pada layanan HTTPS aturan- aturan ini diterapkan untuk evaluasibrangkaian sandi yang rentan. Konfigurasi layanan ini harus diubah sehingga tidak lagimenerima cipher suite yang terdaftar.

Tabel 4. 5 Celah Pada Login Cleartext

Login Cleartext Tidak Terenkripsi FTP	
CVSS Score	**Vulnerability Type**
4.8 Medium	FTP Unencrypted Cleartext Login

Kesimpulan dan Saran : Host jarak jauh menjalakan layanan FTP yang memungkinkan login teks jelas melalui koneksi tidak terenkripsi. Penyerang dapat mengungkapkan nama login dan kata sandi dengan melacak lalu lintas kelayanan FTP. Aktifkan FTPS atau terapkan koneksi melalui perintah AUTH TLS.

Tabel 4. 6 Celah pada Login IMAP

Login Cleartext IMAP Tidak Terenkripsi	
CVSS Score	**Vulnerability Type**
4.8 Medium	IMAP Unencrypted Cleartext Login

Kesimpulan dan Saran : Host jarak jauh menjalakan daemon IMAP yang memungkinkan login teks akan melalui koneksi yang tidak terengkripsi. Kredensial yang valid perlu diberikan pada pengaturan OID 'Konfigurasi Login':1.3.6.1.4.1.25623.1.0.10870. Penyerang dapat mengungkapkan nama pengguna dan kata sandi dengan melacak lalu lintas daemon IMAP jika mekanisme otentikasi kurang aman (misalnya, perintah LOGIN,AUTH). Lakukan konfigurasi server jarak jauh untuk selalu menerapkan koneksi terenkripsi melalui SSL/TLS dengan perintah 'STARTTLS'.

Tabel 4. 7 Hasil Celah pada Transmisi HTTP

Transmisi Cleartext Informasi Sensitif melalui HTTP	
CVSS Score	**Vulnerability Type**
4.8 Medium	Cleartext Transmission of Sensitive Information via HTTP

Kesimpulan dan Saran : Host/aplikasi mengirimkan informasi sensitif (nama pengguna, kata sandi) dalam bentuk teks jelas melalui HTTP. Penyerang dapat menggunakan situasi ini untuk berkompromi/menguping komunikasi HTTP antara klien dan server menggunakan serangan man-in-the-middle untuk mendapatkan akses ke data sensitif seperti nama pengguna atau kata sandi. Menerapkan transmisi data sensitif melalui koneksi SSL/TLS terenkripsi, pastikan host/aplikasi mengarahkan semua pengguna ke koneksi SSL/TLS yang aman sebelum mengizinkan memasukan data sensitif kedalam fungsi yang disebutkan.

Tabel 4. 8 Hasil Celah Pada TLSv1.1

SSL/TLS: Deteksi Protokol TLSv1.1 dan TLSv1.1 yang tidak digunakan lagi		
CVSS Score	**Vulnerability CVE-ID CVE**	**Vulnerability Type**
4.3 Medium	- CVE-2011-3389 - CVE-2015-0204	- Browser Exploit Against SSL/TLS (BEAST) - RSA-Export Keys

Kesimpulan dan Saran : Penggunaan protokol TLSv1.0 dan TLSv1.1 yang tidak digunakan lagi dalam sistem ini dapat dideteksi. Protokol TLSv1.0 dan TLSv1.1 memiliki kelemahan kriptografi yang memungkinkan penyerang dapat menggunakan kelemahan kriptografi yang diketahui untuk menguping koneksi anatara klien dan layanan guna mendapatkan akses data sensitif yang ditransfer dalam koneksi aman, kerentanan berikut nya yang ditemukan dalam protokol ini adalah tidak akan menerima pembaruan keamanan lagi. Disarankan untuk menonaktifkan protocol TLSv1.0 dan/atau TLSv1.1 yang tidak digunakan lagi dan mendukung protokol TLSv1.2+.

Tabel 4. 9 Hasil Celah Pada Exim

Exim – 4.96.2 libspf2 kerentanan RCE	
CVSS Score	**Vulnerability Type**
6.8 Medium	RCE vulnerability in libspf2

Kesimpulan dan Saran : Exim rentan terhadap eksekusi kode jarak jauh (RCE) di libspf2. Kecacatan spesifik ada dalam penguraian makro SPF, saat mengurai makro SPF, proses tidak memvalidasi data yang disediakan pengguna dengan benar, yang dapat mengakibatkan kekurangan bilangan bulat sebelum menulis ke memori. Penyerang dapat memanfaatkan kerentanan ini untuk mengeksekusi kode dalam

konteks akun layanan.

Tabel 4. 10 Hasil Celah Pada Waktu ICMP

Pengungkapan Informasi Balasan Stempel Waktu ICMP	
CVSS Score	**Vulnerability Type**
2.1 Low	ICMP Timestamp

Kesimpulan dan Saran : Host jarak jauh merespon permintaan stempel waktu ICMP, balasan stempel waktu adalah pesan ICMP yang membalas respon stempel waktu. Ini terdiri dari sumber stempel waktu yang dikirm oleh pengirim stempel waktu serta stempel waktu penerimaan dan pengiriman. Informasi ini secara teoritis dapat digunakan untuk mengeksploitasi generator nomor acak berbasis waktu yang lemah dilayanan lain. Berbagai mitigasi dapat dilakukan dengan cara menonaktifkan dukungan sepenuhnya untuk stempel

waktu ICMP pada host jarak jauh dan lindungi host jarak jauh dengan firewall, kemudia blokir paket ICMP yang melewati firewall dikedua arah.

Tabel 4. 11 Hasil Celah Informasi Software

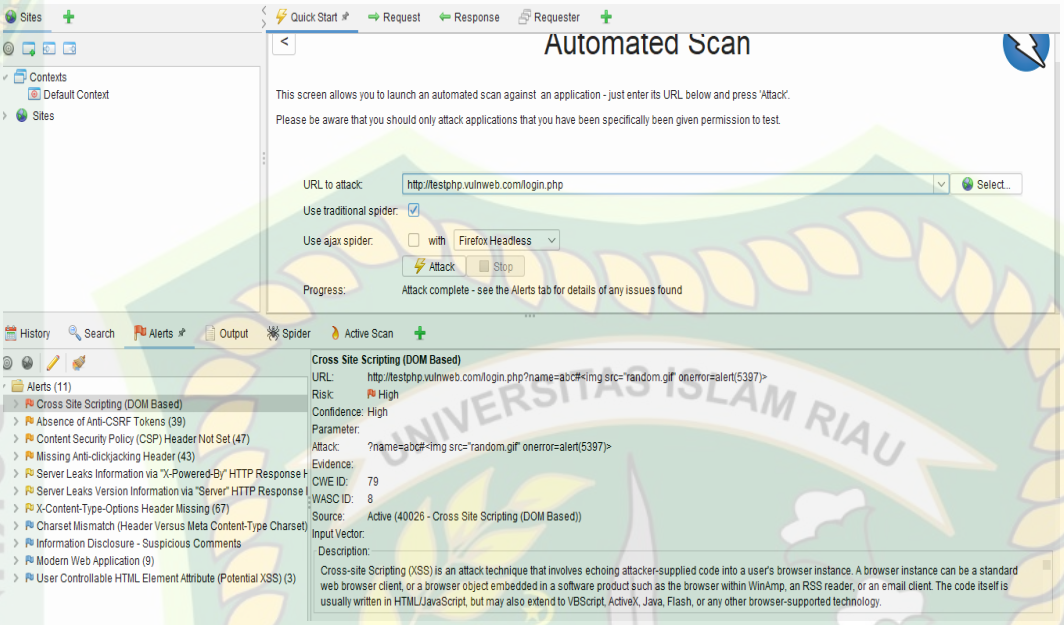
Perangkat Lunak dan Teknologi Server Terdeteksi	
Perangkat Lunak	**Kategori**
CodeIgniter	Kerangka Web
DataTables	Perpustakaan JavaScript
Google Font API	Skrip Font
LiteSpeed	Server Web
PHP	Bahasa Pemograman
Cloudflare	CDN
Cdnjs	CDN
jQuery CDN	CDN
Boostrap 4.0.0-beta	Kerangka UI
HTTP/3	Versi HTTP
jQuery 3.2.1	Perpustakaan JavaScript
Moment.js 2.13.0	Perpustakaan JavaScript
Niagahoster	Web Hosting
Popper 1.14.7	Alat/Mesin Permosisian tooltip dan popover
Select2	Perpustakaan JavaScript
HSTS	Keamanan

Kesimpulan dan Saran : Perangkat lunak dan teknologi server dapat terdektesi hal ini dapat dimanfaatkan penyerang untuk menggunakan informasi ini dalam melakukan serangan spesifik terhadap jenis dan versi perangkat lunak yang teridentifikasi. Disarankan untuk menghilangkan informasi yang memungkinkan identifikasi platform perangkat lunak, teknologi, server dan sistem operasi: header server HTTP,Informasi Meta HTML dan lain – lain.

Selain itu, File Security.txt Tidak Ditemukan sehingga Kesimpulan dan Saran adalah Sistem mendeteksi bahwa server tidak memiliki file security.txt. Tidak ada resiko khusus apabila tidak membuat file security.txt yang valid untuk server, namun file ini penting karena menawarkan saluran khusus untuk melaporkan kerentanan dan masalah keamanan. Sangat disarankan untuk menerapkan file security.txt sesuai standar , agar peneliti atau pengguna dapat melaporkan masalah keamanan apapun yang ditemukan, sehingga dapat meningkatkan mekanisme pertahanan server.

4.1.3. Hasil OWASP ZAP Pada Website Lainnya

Pada tahap ini akan dilakukan monitoring terhadap celah yang ada pada website target lainnya. Misalnya, celah terhadap *Injection Attack, CSRF* dan lainnya. Pada pengujian ini menggunakan software OWASP ZAP. Cara kerjanya sama dengan pengujian sebelumnya. Berikut hasil pengujian terhadap website http://testphp.vulnweb.com.



Gambar 4. 2. Hasil Scanning Website Lainnya

Berdasarkan gambar diatas, didapat beberapa kerentanan yang ada pada website target, salah satu celah pada website tersebut memiliki tingkat ancaman yang high, sehingga sangat rentan untuk diserang oleh pihak yang tidak bertanggung jawab. kerentanan yang dimaksud dapat dilihat pada tabel berikut.

Tabel 4. 12. Hasil Uji OWASP ZAP Website Lainnya

No	Ancaman	Tingkat Ancaman
1	Cross Site Scripting (DOM Based)	High
2	Content-Security-Policy Header Not Set	Medium
3	Absence of Anti-CSRF tokens	Medium
4	Missing anti-clickjacking	Medium
5	Cross-Domain JavaScript Source File Inclusion	Medium

1. Cross Site Scripting (DOM Based)

   Ancaman yang mungkin terjadi adalah Cross Site Scripting (DOM Based), dimana ancaman tersebut menyerang pada celah *code injection* yang menanamkan kode/skrip berbahaya di *website*. *Cross-site scripting* memanfaatkan kerentanan pada aplikasi *web* berupa *input* dan *output* yang tidak divalidasi atau dikodekan.

2. *Content-Security-Policy Header Not Set*

   Ancaman yang mungkin terjadi adalah Content-Security-Policy Header Not Set. Ancaman ini bisa terjadi dengan menggunakan metode XSS atau serangan code injection pada website. Adapun dampak yang timbul pada Penyerang dapat mem-*bypass* keamanan di sisi klien, mendapatkan informasi sensitif, atau menyimpan aplikasi berbahaya pada website.

3. *Absence of Anti-CSRF token*s

   Ancaman yang ditimbulkan adalah Absence of Anti-CSRF tokens. Ancaman ini memiliki celah pada Eksplotasi yang sifatnya berbahaya bagi para pengguna. Sedangkan dampak yang mungkin timbul Ketika ancaman ini terjadi adalah Kredensial pengguna akan didapatkan oleh penyerang, seperti ID Session, Cookie dan lain sebagainya.

4. *Missing anti-clickjackin*g

   Ancaman ini disebut Missing anti-clickjacking, celah dari ancaman ini biasanya terjadi pada website melalui Ads On yang ditambahkan contohnya tombol “Klik Di Sini”. Dampak yang mungkin dihasilkan dari celah ini adalah Ketika diklik ternyata memicu fungsi jahat yang telah

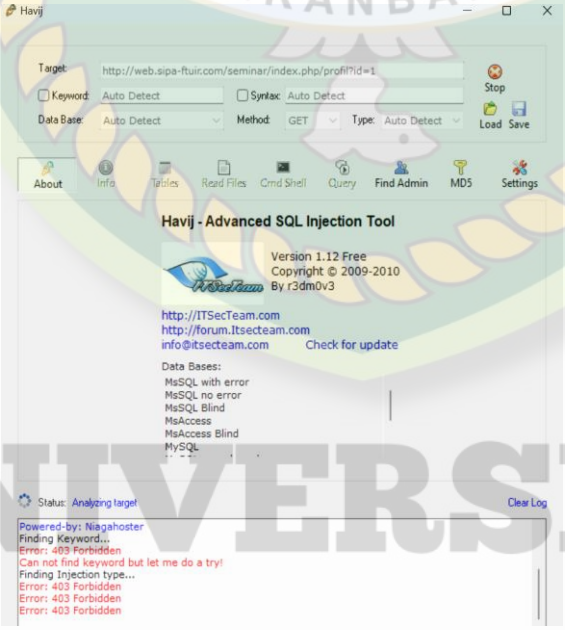
dibuat oleh penyerang, mulai dari memalsukan atau mengikuti di media sosial hingga mengambil uang dari akun bank pengguna.

5. Cross-Domain JavaScript Source File Inclusion

   Ancaman Cross-Domain JavaScript Source File Inclusion terjadi karena terdapat celah karena penyerang dapat melakukan upload file script yang tidak dikenal dari domain eksternal kedalam website. Sehingga Memungkinkan penyerang untuk menambahkan script jahat agar dapat memanipulasi data dan melakukan perubahan fungsionalitas dan pengalihan data.

4.1.3. Hasil Percobaan SQL Injection SIPAFT UIR

Berdasarkan hasil pengujian menggunakan OWASP ZAP, didapat salah satu ancaman yaitu SQL Injection. Berikut adalah perocbaan melakukan serangan terhadap website tersebut menggunakan tools havij.

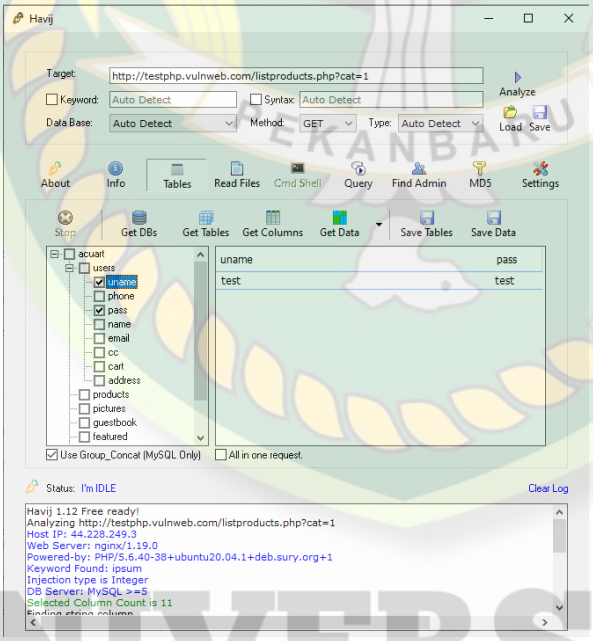


Gambar 4. 3 Hasil SQL Injection SIPAFT UIR

Berdasarkan gambar diatas, menggunakan tools havij untuk percobaan SQL Injection tidak dapat dilakukan karna akses *forbidden*. Akan tetapi, tidak menutup kemungkinan dapat dilakukan dengan tools yang lebih *advance*.

4.1.4. Hasil Percobaan SQL Injection Website

Pada tahap ini dilakukan percobaan serangan SQL Injection terhadap website http://testphp.vulnweb.com. Secara sederhana serangan SQL Injection dilakukan untuk mendapatkan tabel database yang ada pada sistem. Pada pengujian ini menggunakan software Havij. Havij sangat mudah digunakan. User hanya perlu mengisikan alamat target baik berupa url atau alamat IP dan langsung melakukan serangan. Dengan demikian maka database target bisa didapatkan. Konfigurasi Hajiv dapat dilihat pada gambar 4.4.



Gambar 4. 4 Hasil SQL Injection Website Lain

Berdasarkan gambar diatas, serangan sql injection berhasil dilakukan dan diperoleh sebuah database bernama acuart beserta denga isi data didalamnya yang bisa digunakan untuk login kedalam website tersebut.

BAB V

KESIMPULAN

5.1. Kesimpulan

Berdasarkan pengujian yang dilakukan menggunakan *software* OWASP ZAP untuk mendapatkan celah dari sistem SIPA FT Universitas Islam Riau dapat disimpulkan sebagai berikut :

1. Dengan analisis tersebut, penyerang dapat menemukan beberapa celah dari sistem tersebut. Sehingga penyerang mampu mendapatkan informasi berupa celah dan jenis serangan yang dapat dilakukan. Selain itu juga dapat mengetahui dampak dari celah tersebut
2. Pengujian menggunakan metode penetration test terhadap beberapa serangan rentan akan penyadapan dari user tidak bertanggungjawab. Celah yang didapat adalah XSS *Injection, Absence of Anti-CSRF tokens, Missing anti-clickjacking, Cross-Domain JavaScript Source File Inclusion.*

5.2. Saran

Adapun saran yang diberikan demi pengembangan website adalah:

1. Menutup celah yang sudah terdeteksi terlebih dahulu.
2. Untuk setiap form perlu adanya validasi terlebih dahulu sebelum di proses oleh website untuk menghindari XSS Injection.
3. Melakukan *maintenance* secara berkala untuk melihat file-file mencurigakan yang ada didalam sistem.

DAFTAR PUSTAKA

A. Kerentanan Keamanan, W. Menggunakan, D. Aryanti, N. Dan, And J. N. Utamajaya, "Metode Owasp (Open Web Application Security Project) Pada Dinas Tenaga Kerja," 2021.

Adhiguna, M. A. (2023). Pengujian Celah Keamanan Input Validation Pada Aplikasi Website Menggunakan Framework Owasp. Jupik: Jurnal Penelitian Ilmu Komputer, 1(4).

Al Zulfi, F. A., & Suyatno, D. F. (2023). Pengujian Fungsionalitas dan Celah Keamanan Website Kampoeng Sinaoe Menggunakan Equivalence Partition, Boundary Value Analysis, Fuzzing, dan Penetration Testing. Journal of Emerging Information System and Business Intelligence (JEISBI), 4(3), 139-146.

A. Hermawan1, T. Hartati2, And Y. A. Wijaya3, "Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi Cia Triad," Vol. 7, No. 3, 2022.

A. Elanda And R. Lintang Buana, "Analisis Keamanan Sistem Informasi Berbasis Website Dengan Metode Open Web Application Security Project (Owasp) Versi 4: Systematic Review," 2020.

A. W. Kuncoro, J. Informatika, F. Rahma, And M. E. Jurusan Informatika, "Analisis Metode Open Web Application Security Project (Owasp) Pada Engujian Keamanan Website: Literature Review."

A. Elanda And R. Lintang Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada Stmik Rosma Dengan Menggunakan Owasp Top 10," 2021.

Andriyani, S., Sidiq, M. F., & Zen, B. P. (2023). Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar. LEDGER: Journal Informatic and Information Technology, 2(1), 1-13.

Ashari, I. F., & Denira, S. T. (2023). Analisis Celah Keamanan dan Mitigasi Website E-learning Itera Menggunakan Owasp Zed Attack Proxy. Dinamika Rekayasa, 19(1).

B. Subana And A. Fadlil, "Web Server Security Analysis Using The Owasp Mantra Method," 2020.

D. Hariyadi And F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy Dan Owasp Zap Di Universitas Duta Bangsa Surakarta," Jurnal Komtika (Komputasi Dan Informatika), Vol. 5, No. 1, Pp. 35–42, Jul. 2021, Doi: 10.31603/Komtika.V5i1.5134.

I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (Owasp) Menggunakan Penetration Testing Pada Keamanan Website Absensi," Jurnal Informasi Dan Teknologi, Oct. 2022, Doi: 10.37034/Jidt.V4i3.236.

Idi, A. N., Leiwakabessy, A. Y., & Tentua, B. G. (2023). SURVEI CELAH KEAMANAN WEBSITE SISMIK FAKULTAS KEDOKTERAN UNIVERSITAS PATTIMURA MENGGUNAKAN METODE SNIFFING. Jurnal ISOMETRI, 2(1), 83-111.

I. M. Edy Listartha, I. M. A. Premana Mitha, M. W. Aditya Arta, And I. Km. W. Yuda Arimika, "Analisis Kerentanan Website Sma Negeri 2 Amlapura Menggunakan Metode Owasp (Open Web Application Security Project),"

Kestina, L., Yuhandri, Y., & Nurcahyo, G. W. (2023). Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di Bkpsdmd Kabupaten Kerinci). INNOVATIVE: Journal Of Social Science Research, 3(4), 9192-9203.

L. Costaner And Dan Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)."

T. Revolino Syarif And D. Andri Jatmiko, "Analisis Perbandingan Metode Web Security Ptes, Issaf Dan Owasp Di Dinas Komunikasi Dan Informasi Kota Bandung."

Rafeli, A. I., Seta, H. B., & Widi, I. W. (2022). Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ. Informatik: Jurnal Ilmu Komputer, 18(2), 97-103.

Rosallah, Y. T. A. (2021). Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing Dan Metode OWASP (Open Web Application Security Project) Top 10 Pada Website Sistem Informasi Manajemen (SIM) Universitas Pembangunan Nasional Veteran Jakarta.

SURAT KEPUTUSAN DEKAN FAKULTAS TEKNIK UNIVERSITAS ISLAM RIAU
NOMOR : 0139/KPTS/FT-UIR/2023
TENTANG PENGANGKATAN TIM PEMBIMBING PENELITIAN DAN PENYUSUNAN SKRIPSI

DEKAN FAKULTAS TEKNIK

Membaca : Surat Ketua Program Studi Teknik Informatika Nomor : 021/TA-TI/FT/2023 tentang persetujuan dan usulan pengangkatan Tim Pembimbing penelitian dan penyusunan Skripsi.

Menimbang : 1. Bahwa untuk menyelesaikan perkuliahan bagi mahasiswa Fakultas Teknik perlu membuat Skripsi.

2. Untuk itu perlu ditunjuk Tim Pembimbing penelitian dan penyusunan Skripsi yang diangkat dengan Surat Keputusan Dekan.

Mengingat : 1. Undang - Undang Nomor 12 Tahun 2012 Tentang Pendidikan Tinggi
2. Peraturan Presiden Republik Indonesia Nomor 8 Tahun 2012 Tentang Kerangka Kualifikasi Nasional Indonesia
3. Peraturan Pemerintah Republik Indonesia Nomor 37 Tahun 2009 Tentang Dosen
4. Peraturan Pemerintah Republik Indonesia Nomor 66 Tahun 2010 Tentang Pengelolaan dan Penyelenggaraan Pendidikan
5. Peraturan Menteri Pendidikan Nasional Nomor 63 Tahun 2009 Tentang Sistem Penjaminan Mutu Pendidikan
6. Peraturan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor 49 Tahun 2014 Tentang Standar Nasional Pendidikan Tinggi
7. Statuta Universitas Islam Riau Tahun 2018
8. Peraturan Universitas Islam Riau Nomor 001 Tahun 2018 Tentang Ketentuan Akademik Bidang Pendidikan Universitas Islam Riau

MEMUTUSKAN

Menetapkan : 1. Mengangkat saudara-saudara yang namanya tersebut dibawah ini sebagai Tim Pembimbing Penelitian & penyusunan Skripsi Mahasiswa Fak. Teknik Program Studi Teknik Informatika.

No	Nama	Pangkat	Jabatan
1.	Yudhi Arta, S.T, M.Kom	Lektor	Pembimbing

2. Mahasiswa yang akan dibimbing :

Nama : Muhammad Alhaqi
NPM : 173510022
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata Satu (S1)
Judul Skripsi : Evaluasi Keamanan Website Terhadap Kerentanan Serangan Hacker Dengan Metode Penetration Test Menggunakan Open Web Application Security Project (OWASP) ZAP (Studi Kasus : SIPA Fakultas Teknik)

3. Keputusan ini mulai berlaku pada tanggal ditetapkannya dengan ketentuan bila terdapat kekeliruan dikemudian hari segera ditinjau kembali.

Ditetapkan di : Pekanbaru
Pada Tanggal : 8 Sya'ban 1444 H
01 Maret 2023 M

Dekan,

Dr. Eng. Muslim, ST., MT
NPK : 09 11 02 374

Tembusan disampaikan :
1. Yth. Bapak Rektor UIR di Pekanbaru.
2. Yth. Sdr. Ketua Program Studi Teknik Informatika FT-UIR
3. Arsip

**Surat ini ditandatangani secara elektronik*

YAYASAN LEMBAGA PENDIDIKAN ISLAM (YLPI) RIAU
UNIVERSITAS ISLAM RIAU
Jalan Kaharuddin Nasution No. 113 P. Marpoyan Pekanbaru Riau Indonesia – Kode Pos: 28284
Telp. +62 761 674674 Fax. +62 761 674834 *Website*: www.uir.ac.id *Email*: info@uir.ac.id

F.A.3.10

KARTU BIMBINGAN TUGAS AKHIR
SEMESTER GANJIL TA 2023/2024

NPM : 173510022
Nama Mahasiswa : MUHAMMAD ALHAQI
Dosen Pembimbing : 1. YUDHI ARTA ST., M.Kom 2.
Program Studi : TEKNIK INFORMATIKA
Judul Tugas Akhir : Evaluasi Keamanan Websiste Terhadap Kerentanan Serangan HackerDenganMetodePenetration Test Menggunakan OWASP ZAP (Studi Kasus : SiPA Fakultas Teknik)
Judul Tugas Akhir (Bahasa Inggris) : Evaluation of Website Security Against Vulnerability of Hackerwith Methodepenetration Test using OWASP ZAP (Case Study : SIPA Faculty of Engineering)
Lembar Ke : .....

NO	Hari/Tanggal Bimbingan	Materi Bimbingan	Hasil / Saran Bimbingan	Paraf Dosen Pembimbing
1.	02/04/2023	Bimbingan Proposal & Program		
2.	04/04/2023	Revisi 1	Lengkapi Bab 3	
3.	01/06/2023	Revisi 2	Lengkapi Bab 3 & Bab 4	
4.	11/08/2023	Demo Program & Alur Program		
5.	25/08/2023	Revisi 3	Lanjut Seminar Proposal	
6.	02/10/2023	ACC Seminar Proposal		
7	04/01/2024	Revisi Seminar Proposal	Lanjut Sidang Komprehensif	
8	31/01/2024	ACC Sidang Komprehensif		

Pekanbaru,.....
Wakil Dekan I/Ketua Departemen/Ketua Prodi

MTCZNTEWMDIY

( )

Catatan :
1. Lama bimbingan Tugas Akhir/ Skripsi maksimal 2 semester sejak TMT SK Pembimbing diterbitkan
2. Kartu ini harus dibawa setiap kali berkonsultasi dengan pembimbing dan HARUS dicetak kembali setiap memasuki semester baru melalui SIKAD
3. Saran dan koreksi dari pembimbing harus ditulis dan diparaf oleh pembimbing
4. Setelah skripsi disetujui (ACC) oleh pembimbing, kartu ini harus ditandatangani oleh Wakil Dekan I/ Kepala departemen/Ketua prodi
5. Kartu kendali bimbingan asli yang telah ditandatangani diserahkan kepada Ketua Program Studi dan kopiannya dilampirkan pada skripsi.
6. Jika jumlah pertemuan pada kartu bimbingan tidak cukup dalam satu halaman, kartu bimbingan ini dapat di download kembali melalui SIKAD

SURAT KEPUTUSAN DEKAN FAKULTAS TEKNIK UNIVERSITAS ISLAM RIAU
NOMOR : 0162/KPTS/FT-UIR/2024
TENTANG PENETAPAN DOSEN PENGUJI SKRIPSI MAHASISWA FAK. TEKNIK UNIV. ISLAM RIAU

DEKAN FAKULTAS TEKNIK

Menimbang : 1. Bahwa untuk menyelesaikan studi S.1 bagi mahasiswa Fakultas Teknik Univ. Islam Riau dilaksanakan Ujian Skripsi/Komprehensif sebagai tugas akhir. Untuk itu perlu ditetapkan mahasiswa yang telah memenuhi syarat untuk ujian dimaksud serta dosen penguji.

2. Bahwa penetapan mahasiswa yang memenuhi syarat dan dosen penguji yang bersangkutan perlu ditetapkan dengan Surat Keputusan Dekan.

Mengingat : 1. Undang - Undang Nomor 12 Tahun 2012 Tentang Pendidikan Tinggi
2. Peraturan Presiden Republik Indonesia Nomor 8 Tahun 2012 Tentang Kerangka Kualifikasi Nasional Indonesia
3. Peraturan Pemerintah Republik Indonesia Nomor 37 Tahun 2009 Tentang Dosen
4. Peraturan Pemerintah Republik Indonesia Nomor 66 Tahun 2010 Tentang Pengelolaan dan Penyelenggaraan Pendidikan
5. Peraturan Menteri Pendidikan Nasional Nomor 63 Tahun 2009 Tentang Sistem Penjaminan Mutu Pendidikan
6. Peraturan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor 49 Tahun 2014 Tentang Standar Nasional Pendidikan Tinggi
7. Statuta Universitas Islam Riau Tahun 2018
8. Peraturan Universitas Islam Riau Nomor 001 Tahun 2018 Tentang Ketentuan Akademik Bidang Pendidikan Universitas Islam Riau

MEMUTUSKAN

Menetapkan : 1. Mahasiswa Fakultas Teknik Universitas Islam Riau yang tersebut namanya dibawah ini :

Nama	: Muhammad Alhaqi
NPM	: 173510022
Program Studi	: Teknik Informatika
Jenjang Pendidikan	: Strata Satu (S1)
Judul Skripsi	: Evaluasi Keamanan Website Terhadap Kerentanan Serangan Hacker Dengan Metode Penetration Test Menggunakan OWASP ZAP (Studi Kasus : SIPA Faculty of Engineering).

2. Penguji Skripsi/Komprehensif mahasiswa tersebut terdiri dari :

1. Yudhi Arta, S.Kom., M.Kom	Sebagai Ketua Merangkap Penguji
2. Hendra Gunawan, ST.,M.Eng	Sebagai Anggota Merangkap Penguji
3. Dr. Evizal, S.T., M.Eng.	Sebagai Anggota Merangkap Penguji

3. Laporan hasil ujian serta berita acara telah sampai kepada Pimpinan Fakultas selambat-lambatnya 1(satu) bulan setelah ujian dilaksanakan.

4. Keputusan ini mulai berlaku pada tanggal ditetapkannya dengan ketentuan bila terdapat kekeliruan dikemudian hari segera ditinjau kembali.

KUTIPAN : Disampaikan kepada yang bersangkutan untuk dapat dilaksanakan dengan sebaik-baiknya.

Ditetapkan di : Pekanbaru
Pada Tanggal : 12 Sya'ban 1445 H
22 Februari 2024 M

Dekan,

Prof. Dr. Eng. Ir. Muslim.,ST.,MT.,IPU
NPK : 1016047901

Tembusan disampaikan :
1. Yth. Rektor UIR di Pekanbaru.
2. Yth. Ketua Program Studi Teknik Informatika FT-UIR
3. Yth. Pembimbing dan Penguji Skripsi
3. Mahasiswa yang bersangkutan
5. Arsip

**Surat ini ditandatangani secara elektronik*

YAYASAN LEMBAGA PENDIDIKAN ISLAM (YLPI) RIAU
UNIVERSITAS ISLAM RIAU
FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK INFORMATIKA
Jalan Kaharuddin Nasution No. 113 P. Marpoyan Pekanbaru Riau Indonesia – Kode Pos: 28284
Telp. +62 761 674674 *Website*: www.eng.uir.ac.id *Email*: fakultas_teknik@uir.ac.id

BERITA ACARA UJIAN SKRIPSI

Berdasarkan Surat Keputusan Dekan Fakultas Teknik Universitas Islam Riau, Pekanbaru, tanggal 21 Februari 2024, Nomor: 0162 /KPTS/FT-UIR/2024, maka pada hari Kamis, tanggal 22 Februari 2024, telah dilaksanakan Ujian Skripsi Program Studi Teknik Informatika Fakultas Teknik Universitas Islam Riau, Jenjang Studi S1, Tahun Akademik 2023/2024 berikut ini.

1. Nama : Muhammad Alhaqi
2. NPM : 173510022
3. Judul Skripsi : Evaluasi Keamanan Website Terhadap Kerentanan Serangan Hacker Dengan Metode Penetration Test Menggunakan OWASP ZAP (Studi Kasus : SIPA Faculty of Engineering).
4. Waktu Ujian : 08.00 WIB s.d. Selesai
5. Tempat Pelaksanaan Ujian : Ruang Sidang Fakultas Teknik UIR

Dengan keputusan Hasil Ujian Skripsi:

~~Lulus~~*/ Lulus dengan Perbaikan*/ ~~Tidak Lulus~~*

** Coret yang tidak perlu.*

Nilai Ujian:

Nilai Ujian Angka =81,8 Nilai Huruf = (A)

Tim Penguji Skripsi.

No	Nama	Jabatan	Tanda Tangan
1	Yudhi Arta, S.Kom., M.Kom	Ketua	1.
2	Hendra Gunawan, ST.,M.Eng	Anggota	2.
3	Dr. Evizal, S.T., M.Eng.	Anggota	3.

Panitia Ujian
Ketua,

Yudhi Arta, S.Kom., M.Kom
NIDN. 1029078701

Pekanbaru, 21 Februari 2024
Mengetahui,
Dekan Fakultas Teknik

Prof. Dr. Eng. Ir. Muslim, S.T., M.T., IPU.
NIDN. 1016047901

UNIVERSITAS ISLAM RIAU
FAKULTAS TEKNIK
الجامعة الإسلامية الريوية
Alamat: Jalan Kaharuddin Nasution No.113, Marpoyan, Pekanbaru, Riau, Indonesia - 28284
Telp. +62 761 674674 Email: fakultas_teknik@uir.ac.id Website: www.eng.uir.ac.id

SURAT KETERANGAN BEBAS PLAGIAT

Nomor: 055/A-UIR/5-T/2024

Fakultas Teknik Universitas Islam Riau menerangkan bahwa Mahasiswa/i dengan identitas berikut:

Nama	:	**MUHAMMAD ALHAQI**
NPM	:	173510568
Program Studi	:	Teknik Informatika
Jenjang Pendidikan	:	Strata Satu (S1)
Judul Skripsi TA	:	EVALUASI KEAMANAN WEBSISTE TERHADAP KERENTANAN SERANGAN *HACKER* DENGAN METODE *PENETRATION TEST* MENGGUNAKAN OWASP ZAP (STUDI KASUS : SIPA FAKULTAS TEKNIK)

Dinyatakan **Bebas Plagiat,** berdasarkan hasil pengecekan pada Turnitin menunjukkan angka **Similarity Index < 30%** sesuai dengan peraturan Universitas Islam Riau yang berlaku.

Demikian surat keterangan ini dibuat untuk dapat dipergunakan sebagaimana mestinya.

Mengetahui,

Kaprodi. Teknik Informatika

Apri Siswanto, S.Kom., M.Kom., Ph.D

Pekanbaru, 15 February 2024 M
05 Syaban 1445 H

Staff Pemeriksa

Ahmad Pandi, S.Kom.