ANALISIS PENGUJIAN KEAMANAN JARINGAN FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM UNIVERSITAS LAMPUNG MENGGUNAKAN METODE *BRUTE FORCE*

(Skripsi)

Oleh

Darra Deandra Modesta

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2021

ABSTRACT

ANALYSIS OF NETWORK SECURITY TESTING AT FACULTY OF MATHEMATICS AND NATURAL SCIENCES LAMPUNG UNIVERSITY USING BRUTE FORCE METHOD

By

Darra Deandra Modesta

The Faculty of Mathematics and Natural Science, University of Lampung has a website that serves as a medium of information about the Faculty of Mathematics and Natural Sciences, University of Lampung and academic services for students. As a website based on academic services, this website contains crucial data about the academic community of the Faculty of Mathematics and Natural Sciences, University of Lampung, from names to telephone numbers. However, the security problem on the website is still not getting priority by the admin, which should be addressed immediately so that data leakage does not occur. The purpose of this research is to conduct an analysis in terms of security on the website of the Faculty of Mathematics and Natural Sciences, University of Lampung and prove the vulnerabilities found. This study uses the VAPT (Vulnerability Assessment and Penetration Testing) framework to analyze and test potential vulnerabilities on the website. As a result, there are several accounts that have been successfully obtained by using the Brute Force technique. The duration of the Brute Force in revealing the target account varies depending on how complicated the combination of passwords used by the victim is. The final results of this test were assessed using a CVSS calculator. As a result, this website has a Medium vulnerability level with a score of 6.3.

Keywords: Brute Force, CVSS, Vulnerability, Website.

ABSTRAK

ANALISIS PENGUJIAN KEAMANAN JARINGAN FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM UNIVERSITAS LAMPUNG MENGGUNAKAN METODE *BRUTE FORCE*

Oleh

Darra Deandra Modesta

Website FMIPA Universitas Lampung adalah *website* yang berfungsi sebagai media informasi seputar Fakultas MIPA Universitas Lampung dan layanan akademik untuk mahasiswa. Sebagai *website* berbasis pelayanan akademik, *website* ini mengandung data-data krusial tentang civitas akademik FMIPA Universitas Lampung dari nama hingga nomor telepon. Namun, masalah keamanan pada *website* tersebut masih kurang mendapat prioritas oleh admin yang seharusnya segera ditangani agar tidak terjadi kebocoran data. Tujuan dari penelitian ini adalah untuk melakukan analisis dari segi keamanan pada *website* Fakultas MIPA Universitas Lampung dan membuktikan kerentanan yang ditemukan. Penelitian ini menggunakan *framework* VAPT (*Vulnerability Assessment and Penetration Testing*) untuk menganalisa dan menguji potensi kerentanan pada *website*. Hasilnya, terdapat beberapa akun yang berhasil didapatkan dengan memanfaatkan teknik *Brute Force*. Durasi *Brute Force* dalam mengungkap akun target berbeda-beda tergantung tingkat kerumit an kombinasi *password* yang digunakan korban. Hasil akhir dari pengujian ini dinilai menggunakan kalkulator CVSS. Hasilnya, *website* ini memiliki tingkat kerentanan *Medium* dengan skor 6.3.

Kata kunci: *Brute Force*, CVSS, Kerentanan, *Website*.

ANALISIS PENGUJIAN KEAMANAN JARINGAN FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM UNIVERSITAS LAMPUNG MENGGUNAKAN METODE *BRUTE FORCE*

Oleh

DARRA DEANDRA MODESTA

SKRIPSI

Sebagai Salah Satu Syarat untuk Memperoleh Gelar
SARJANA KOMPUTER

Pada

Jurusan Ilmu Komputer
Fakultas Matematika dan Ilmu Pengetahuan Alam

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2021

Judul Skripsi	: **ANALISIS PENGUJIAN KEAMANAN JARINGAN FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM UNIVERSITAS LAMPUNG MENGGUNAKAN METODE *BRUTE FORCE***
Nama Mahasiswa	: Darra Deandra Modesta
Nomor Pokok Mahasiswa	: 1657051021
Program Studi	: S1 Ilmu Komputer
Fakultas	: Matematika dan Ilmu Pengetahuan Alam

MENYETUJUI

1. Komisi Pembimbing

Aristoteles, S.Si., M.Si.
NIP 19810521 200604 1 002

Dewi Asiah Shofiana, S.Komp., M.Kom.
NIP 19950929 202012 2 030

2. Ketua Jurusan Ilmu Komputer

Didik Kurniawan, S.Si., M.T.
NIP 19800419 200501 1 004

MENGESAHKAN

1. Tim Penguji

Ketua : **Aristoteles, S.Si., M.Si.** .....

Sekretaris : **Dewi Asiah Shofiana, S.Komp., M.Kom.** .....

Penguji
Bukan Pembimbing : **Dr. Ir. Kurnia Muludi, M.S.Sc.** .....

2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

Dr. Eng. Suripto Dwi Yuwono, M.T.
NIP 19740705 200003 1 001

Tanggal Lulus Ujian Skripsi : **28 Juli 2021**

PERNYATAAN

Saya yang bertanda tangan di bawah ini, menyatakan bahwa skripsi saya yang berjudul **"Analisis Pengujian Keamanan Jaringan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung Menggunakan Metode *Brute Force*"** merupakan karya saya sendiri dan bukan karya orang lain. Semua tulisan yang tertuang dalam skripsi ini telah mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila di kemudian hari terbukti skripsi saya merupakan hasil penjiplakan atau dibuat orang lain, maka saya bersedia menerima sanksi berupa pencabutan gelar yang telah saya terima.

Bandar Lampung, 28 Juli 2021

DARRA DEANDRA MODESTA

NPM 1657051021

RIWAYAT HIDUP

Penulis dilahirkan pada tanggal 21 September 1998 di Bandar Lampung sebagai anak tunggal dari Ayah bernama Ir.Simon Abdurrahman dan Ibu bernama Destina. Penulis mengawali pendidikan formal pertama kali di TK Al-Bustan dan lulus pada tahun 2004. Melanjutkan pendidikan di SD Al-Kautsar Bandar Lampung dan lulus pada tahun 2010, lanjut ke SMP Al-Kautsar Bandar Lampung dan lulus pada tahun 2013, kemudian lanjut ke SMA Al-Kautsar Bandar Lampung dan lulus pada tahun 2016.

Pada tahun 2016, penulis terdaftar sebagai mahasiswa Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung. Selama menempuh studi di Universitas Lampung, penulis pernah mengikuti berbagai kegiatan, organisasi kampus, dan beberapa kejuaraan pada cabang olahraga Pencak Silat. Berikut kegiatan dan raihan prestasi yang dilakukan penulis selama menjadi mahasiswa:

1. Mengikuti kegiatan Karya Wisata Ilmiah (KWI) di Desa Margosari, Kecamatan Pagelaran Utara, Kabupaten Pringsewu pada bulan Januari tahun 2017.
2. Melaksanakan Kerja Praktik (KP) di Balai Karantina Ikan dan Pengendalian Mutu Hasil Perikanan (BKIPM) Provinsi Lampung pada bulan Januari-Februari tahun 2019.
3. Melaksanakan Kuliah Kerja Nyata (KKN) di Desa Sukamaju Kecamatan Lumbok Seminung Kabupaten Lampung Barat selama 40 hari pada bulan Juli-Agustus tahun 2019.
4. Anggota Badan Khusus HIMAKOM tahun 2017.
5. Anggota Departemen 1 Kaderisasi UKM-U Tapak Suci Universitas Lampung tahun 2017.

6. Asisten Dosen dan Praktikum mata kuliah Dasar-Dasar Pemrograman Semester Ganjil tahun ajaran 2017/2018.
7. Asisten Dosen dan Praktikum mata kuliah Pengantar Organisasi Komputer (POK) Semester Genap tahun ajaran 2018/2019.
8. Asisten Dosen dan Praktikum mata kuliah Pemrograman Web prodi D3 Manajemen Informatika Semester Genap tahun ajaran 2019/2020.
9. Mengikuti kompetisi *Cyber Security Born to Protect* yang diadakan oleh Badan KOMINFO dan lolos sebagai Top 1.000 pada tahun 2018.
10. Mengikuti Pekan Olahraga Mahasiswa Daerah (POMDA) cabang olahraga Pencak Silat yang diselenggarakan di UIN Raden Intan pada tahun 2019.
11. Meraih medali perak pada *Open* Kejuaraan Pencak Silat ke-1 IPSI Lampung Tengah kategori tanding kelas A putri tahun 2018.
12. Meraih medali perak pada kejuaraan Pencak Silat *National Open* Lampung *Championship* III kategori tanding kelas A putri tahun 2019.
13. Meraih medali perunggu pada kejuaraan Tapak Suci *International Open* Universitas Lampung kategori tanding kelas B putri tahun 2019.
14. Memiliki sertifikasi bidang Jaringan komputer MTCNA yang berhasil diperoleh pada tahun 2018.
15. Pada bulan November tahun 2019 penulis mengikuti ujian sertifikasi bidang keamanan komputer dan berhasil mendapatkan sertifikasi *Certified Secure Computer User* (CSCU) yang diselenggarakan oleh Badan KOMINFO pada acara *Born To Protect* di Palembang.
16. Pada bulan Agustus tahun 2020, penulis mengikuti ujian Sertifikasi Profesi yang diadakan oleh BNSP dan memperoleh sertifikasi kompetensi *Junior Network Administrator*.

PERSEMBAHAN

Puji dan syukur ku-ucapkan kepada Allah Subhanahu Wa Ta'ala atas segala rahmat dan ridho-Nya yang selalu memberikan keyakinan, kekuatan, kesabaran serta kelancaran sehingga skripsi ini dapat diselesaikan.

Kupersembahkan karya ini untuk:

Papa dan Mama yang selalu memberikan segalanya kepadaku. Terima kasih atas doa, kasih sayang, perhatian, dukungan, pengorbanan, serta hal lainnya yang kalian berikan dan tak akan terbalaskan.

Saudara-saudaraku, serta keluarga besar yang selalu memberikan doa dan dukungan semangat kepadaku.

Sahabat-sahabatku, terima kasih telah menemaniku, mendukungku, dan selalu memberikan kebahagiaan dalam hidupku.

Keluarga Ilmu Komputer 2016

Almamater Tercinta, Universitas Lampung

MOTTO

"Boleh jadi kamu membenci sesuatu, padahal ia amat baik bagimu, dan boleh jadi (pula) kamu menyukai sesuatu, padahal ia amat buruk bagimu; Allah mengetahui, sedang kamu tidak mengetahui"

(Q.S Al-Baqarah:216)

"Maka nikmat Tuhanmu yang manakah yang kamu dustakan?"

(Q.S Ar-Rahman:13)

"Sesungguhnya setelah kesulitan ada kemudahan, setelah kesulitan ada kemudahan"

(Q.S Al-Insyirah:5-6)

"Ada pepatah yang mengatakan 'kencangkan helm perangmu setelah menang', setelah menang, orang biasanya akan lengah."

(Imayoshi Shouichi-Kuroko no Basuke)

"Jika tidak kulakukan sekarang, maka kapan lagi?!"

(Kagami Taiga- Kuroko no Basuke)

"Seekor ikan jenis apapun, baik yang tinggal di air jernih ataupun air kotor, selama dia terus berenang ke depan, dia akan tumbuh dengan indah"

(Koro-Sensei-Ansatsu Kyoushitsu 1)

SANWACANA

Alhamdulillahirabbil'alamin, puji syukur kehadirat Allah *Subhanahu wa ta'ala,* yang telah melimpahkan segala rahmat, hidayah dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Pengujian Keamanan Jaringan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung Menggunakan Metode *Brute Force*" dengan baik. Shalawat serta salam semoga senantiasa tercurahkan kepada Nabi Muhammad *Shalallahu 'alaihi wa sallam*, keluarganya, sahabatnya, dan mudah-mudahan kita adalah umat yang diberikan syafa'atnya di hari akhir kelak, aamiin.

Dalam proses penyusunan skripsi ini penulis banyak mendapat bimbingan, dukungan, dan motivasi dari berbagai pihak yang dengan tulus telah membantu penulis agar dapat menyelesaikan skripsi ini. Penulis sangat bersyukur dan mengucapkan terima kasih sedalam-dalamnya kepada:

1. Allah SWT, yang telah memberikan rahmat, pertolongan, dan karunia-Nya sehingga penelitian ini dapat terselesaikan dengan baik.
2. Kedua orangtua tercinta, Papa, Mama, beserta keluarga besar yang tak henti-hentinya berdoa, memberikan dorongan dan dukungan baik berupa materiil maupun moril, semangat, kasih sayang kepada penulis.
3. Bapak Aristoteles, S.Si., M.Si selaku pembimbing utama yang telah sabar membimbing penulis, memberikan arahan, semangat, dan dorongan kepada penulis sehingga penelitian ini dapat terselesaikan dengan baik.
4. Ibu Dewi Asiah Shofiana, S.Komp., M.Kom, selaku pembimbing kedua yang telah membimbing penulis dalam menyelesaikan penulisan *draft* skripsi, memberikan bantuan, kritik, saran, dan dukungannya sehingga penulis dapat menyelesaikan skripsi dengan baik.

5. Bapak Dr. Ir. Kurnia Muludi,. M.S.Sc., selaku dosen pembahas atas kritik dan saran yang bermanfaat untuk perbaikan selama proses penyelesaian skripsi.
6. Bapak Ardiansyah, S.Kom., M.Kom yang telah memberikan izin bagi penulis untuk melaksanakan penelitian ini serta bersedia untuk mendampingi penulis di fase ujian skripsi.
7. Bapak Dr. Eng. Suripto Dwi Yuwono, M.T. selaku Dekan FMIPA Universitas Lampung.
8. Bapak Didik Kurniawan, S.Si., MT., selaku Ketua Jurusan Ilmu Komputer FMIPA Universitas Lampung.
9. Ibu Astria Hijriani, S.Kom., M.Kom., selaku Sekretaris Jurusan Ilmu Komputer FMIPA Universitas Lampung.
10. Bapak dan Ibu Dosen Jurusan Ilmu Komputer Universitas Lampung yang telah mendidik, memberikan ilmu dan pengetahuan selama penulis menjadi mahasiswa.
11. Ibu Ade Nora Maela, Bang Zai, dan Mas Nofal yang turut memudahkan segala urusan administrasi penulis di Jurusan Ilmu Komputer.
12. Teman-teman, kakak-kakak dan adik-adik dari UKM Tapak Suci Unila yang telah menemani, melatih, membimbing dan memberikan penulis kesempatan agar bisa berkontribusi untuk menyumbangkan prestasi untuk organisasi dan kampus, terima kasih atas pengalaman yang diberikan, semoga kita tidak putus tali silahturahmi.
13. Putra Pribowo dan M. Bella Buay Nunyai yang telah meluangkan waktu di tengah kesibukannya untuk membagi ilmunya tentang *cyber security* dan membantu penulis dalam menyelesaikan penelitian ini.
14. Sahabat semasa sekolah: Nabella, Fadilla, Rizki Tika, Riyanti, Dhea, Febri, Nur Auliya, Ellen, semoga silaturahmi kita tetap terjaga walau sudah berbeda tempat dan kehidupan.
15. Teman-teman seperbimbingan: Anggie, Sarifah, Trio, Putra Saut, Refina, Novi, Ajijah, Anesca, dan Elva yang telah menemani dan saling *sharing* ilmu baik penulisan maupun pengalaman dalam menyelesaikan skripsi.

16. Tim kesebelasan S.Kom: Maya Akhriza, Zakiatun Nufus, Mela Rahmadani, Nur Shabrina, Irmaya Kartika, Travitha Ikka Rahmawati, Yeni Rosandi, Anita Dwi Maharani, Sisda Amalia Utrujah, dan Fanni Lufiana, beserta aliansi: Antis, Tetra, Emes, Oka, Ade, Rachel, Ajijah, terimakasih atas kebersamaan kalian selama masa perkuliahan hingga lulus, semoga kita tidak putus tali silaturahmi, tak hanya sekedar kenangan semasa kuliah saja.
17. Sahabat lintas jurusan: kak Nikmah, Evin, Azizah Dewi, terimakasih telah memberikan penulis *circle* pertemanan yang lebih luas semasa kuliah.
18. Teman-teman Jurusan Ilmu Komputer angkatan 2016 yang tidak bisa disebutkan satu persatu.
19. Mohon maaf jika ada yang merasa nama kalian tidak tertulis disini ketika membaca sanwacana ini. Harap diingat ini skripsi, bukan daftar nama aktor atau staf yang biasa muncul di *credit* film, drakor, atau sejenisnya.

Penulis menyadari bahwa dalam penulisan skripsi ini masih terdapat banyak sekali kekurangan karena terbatasnya pengetahuan, pengalaman, dan kemampuan penulis. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang dapat membangun dan diharapkan penelitian ini dapat dijadikan refrensi untuk penelitian yang akan datang. Semoga skripsi ini dapat bermanfaat bagi semua pihak.

Bandar Lampung, 28 Juli 2021

Darra Deandra Modesta
NPM. 1657051021

DAFTAR ISI

Halaman

DAFTAR TABEL

Tabel Halaman

DAFTAR GAMBAR

Gambar Halaman

I. LATAR BELAKANG

1.1 Latar Belakang

Website menurut (Cinderatama & Amini, 2016) merupakan layanan yang menyediakan informasi bagi pemakai komputer yang terhubung ke internet, mulai dari informasi biasa hingga informasi yang komersial. *Website* dapat diartikan sebagai kumpulan halaman yang digunakan untuk menampilkan informasi berupa teks, gambar, dokumen animasi, suara, atau gabungan dari itu semua yang dapat diakses melalui *web browser*. Dalam kehidupan sehari-hari, pemanfaatan *website* banyak diimplementaskan dalam proses bisnis dalam berbagai instansi, salah satunya adalah perguruan tinggi negeri, salah satu perguruan tinggi yang memanfaatkan *website* adalah Universitas Lampung (Unila). Beberapa contoh manfaat *website* bagi civitas akademik Unila yaitu mempermudah proses bisnis, sebagai media informasi universitas seperti sejarah perguruan tinggi, prestasi perguruan tinggi, fakultas, program studi, hingga pelayanan akademik, contohnya informasi jadwal perkuliahan dan publikasi jurnal.

Universitas Lampung adalah salah satu perguruan tinggi negeri (PTN) yang berada di Provinsi Lampung, Indonesia. Universitas Lampung memiliki 8 fakultas, yaitu Fakultas Pertanian, Fakultas Teknik, Fakultas Ekonomi dan Bisnis, Fakultas Ilmu Sosial dan Politik, Fakults Hukum, Fakultas Keguruan dan Ilmu Pendidikan, Fakultas Matematika dan Ilmu Pengetahuan Alam, dan Fakultas Kedokteran. Setiap fakultas memiliki *website* untuk membantu kelancaran proses bisnis bagi civitas akademik, salah satu Fakultas yang memanfaatkan *website* adalah Fakultas Matematika dan Ilmu Pengetahuan

Alam, fakultas ini memiliki *website* dengan nama domain fmipa.unila.ac.id. yang berfungsi sebagai media informasi tentang fakultas dan sarana informasi untuk mahasiswa Fakultas MIPA Universitas Lampung, mulai dari berita seputar Fakultas MIPA, profil tiap jurusan, pengumuman untuk mahasiswa MIPA hingga pelayanan akademik mahasiswa sebagai konten utamanya. *Website* ini menggunakan *Wordpress* dalam pembuatan, pengaturan *interface* hingga pengaturan konten yang disajikan oleh *website* FMIPA.

Dalam penggunaannya, *website* FMIPA Universitas Lampung masih memiliki kelemahan pada aspek keamanan yang dapat disalahgunakan pihak luar untung kepentingan pribadi. Berbagai macam penyalahgunaan informasi oleh pihak luar seperti mengubah informasi, mengambil data hingga mengubah tampilan *website*. Namun, masalah keamanan pada *website* masih kurang mendapat prioritas oleh admin *website* universitas. Apabila kelemahan-kelemahan tersebut tidak segera ditangani dengan serius, maka civitas akademik akan mengalami kerugian.

Pada penelitian yang dilakukan oleh Irwansyah & Purwanto (2016) dilakukan evaluasi keamanan sistem informasi pada sistem informasi lembaga pemerintahan Provinsi Sumatera Selatan. Penelitian ini dilakukan dengan memperhatikan aspek-aspek keamanan sistem informasi seperti *Confidentially*, *Integrity*, *Autentication*, serta *Availability*. *Confidentially* mencakup kerahasiaan informasi yang berhubungan dengan data-data yang bersifat pribadi seperti nama, alamat, nomor telepon, *email*,nomor identitas, dan sebagainya, *Integrity* mencakup integritas informasi yang berarti infromasi yang tersedia tidak boleh diubah oleh pihak lain selain administrator atau orang lain yang menyamar sebagai administrator, *Authentication* adalah aspek yang memastikan bahwa informasi yang terdapat pada sistem informasi adalah asli, maksudnya pengguna sistem informasi yang memberikan atau membuat informasi tersebut benar pengguna resmi dari sistem informasi pemprov Sumatera Selatan, sedangkan *Availability* mencakup ketersediaan informasi yang dibutuhkan pengguna. Objek yang

diteliti adalah sistem informasi *monitoring* dan *reporting* SPSE dan sistem informasi penataan ruang (SIPR) Kota Lubuklinggau. Hasil penelitian tersebut menunjukkan bahwa pada sistem informasi SPSE dan SIPR ditemukan beberapa kerentanan berbahaya seperti *SQL Injection, ClearText Password Over HTTP, Password AutoComplete in browser, Cross-Site Scripting (XSS)*.

Penelitian serupa juga dilakukan oleh Zulfi (2017) yang dilakukan untuk mengevaluasi Sistem Informasi Terpadu Universitas Jember (SISTER). Penelitian tersebut menggunakan *framework Vulnerability Assesment & Penetration Testing* (VAPT) dalam melakukan simulasi penyerangan. Kerangka VAPT terdiri dari gabungan dua aktivitas, yaitu *Vulnerabilty Assesment* dan *Penetration Testing*. *Vulnerability Assessment* adalah aktivitas memeriksa celah keamanan dari suatu sistem informasi, sedangkan *Penetration Testing* adalah aktivitas menguji kelemahan yang telah ditemukan berdasarkan hasil analisa menggunakan *Vulnerability Assessment*. Pada tahap pengujian keamanan, peneliti menggunakan *Black Box Testing* dengan bantuan lima *tools* dalam melakukan analisis dan pengujian kelemahan, seperti Acunetix, Burp Suite, OWASP ZAP, W3af, dan Nessus. Hasil penelitian menunjukkan terdapat lima jenis celah keamanan yang ditemukan pada SISTER Universitas Jember.

Penelitian terbaru mengenai keamanan sistem informasi dilakukan oleh Alwi dkk (2020) dengan judul "Analisis Keamanan Website Menggunakan *Teknik Footprinting* dan *Vulnerability Scanning"*. Penelitian tersebut dilakukan dengan menggunakan dua metode analisis yaitu *footprinting* dan *vulnerability scanning*. Target penelitian adalah *website* salah satu universitas di Indonesia dengan bantuan beberapa tools seperti Zenmap, Acunetix, OWASP-ZAP dan beberapa *tools online* seperti Pentest-tools.com. Hasilnya terdapat beberapa kerentanan dengan masing-masing tingkat risiko dari *low* sampai *high*. Penelitian ini hampir sama dengan penelitian sebelumnya yang menggunakan

metode *Vulnerability Assessment* karena hasil dari *vulnerability scanning* tidak dieksploitasi oleh peneliti.

Sebagai *website* yang berbasis pelayanan akademik, *website* ini mengandung data-data krusial tentang civitas akademik FMIPA Universitas Lampung, seperti identitas pribadi berupa *e-mail*, alamat tempat tinggal, nomor pokok, hingga nomor telepon. Sayangnya, identitas mahasiswa merupakan jenis data yang sangat rentan menjadi sasaran untuk dieksploitasi oleh pihak luar.

Berdasarkan latar belakang tersebut, maka solusi dari permasalahan tersebut adalah melakukan analisis keamanan *website* menggunakan *Vulnerability Analysis* dan *Pentetration Testing* terhadap *website* FMIPA.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini yaitu:

1. Apakah *website* FMIPA Universitas Lampung memiliki kerentanan terhadap serangan siber?
2. Bagaimana langkah-langkah yang dilakukan untuk mengetahui kelemahan pada *website* FMIPA Universitas Lampung?
3. Apa saja solusi yang tepat untuk menutupi kelemahan yang ditemukan pada *website* FMIPA Universitas Lampung?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk melakukan analisis dari segi keamanan pada *website* Fakultas MIPA Universitas Lampung dan membuktikan kerentanan yang ditemukan.

1.4 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Metode serangan yang dipakai adalah serangan *Brute Force*.
2. Proses pengujian menggunakan *framework* VAPT dengan bantuan sistem operasi Kali Linux.

3. Penelitian yang dilakukan hanya bertujuan untuk menganalisis kelemahan pada *website* Fakultas MIPA bukan untuk memperbaiki kelemahan yang ada.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah dapat mengetahui mekanisme serangan pada *website* FMIPA Universitas Lampung dan diharapkan dapat dijadikan referensi oleh administrator *website* FMIPA Universitas Lampung dalam menentukan langkah-langkah pencegahan berdasarkan hasil analisis yang telah dilakukan.

II. TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian terdahulu yang menjadi rujukan dalam penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Penelitian Terdahulu

No	Peneliti	Judul Penelitian	Hasil
1	(Irwansyah, Purwanto, Timur Dali 2016)	Evaluasi Keamanan Sistem Informasi Pada Lembaga Pemerintahan Sumatera Selatan	Pada *website* SPSE dan SIPR ditemukan beberapa kerentanan sebagai berikut: 1) *SQL Injection* yang disebabkan karakter-karakter seperti (‘) atau (-) tidak difilter sehingga dapat diinjeksi pada *URL* yang rentan. *2) Clear Text Password Over HTTP* dan *Password Auto Complete in Browser* yang disebabkan otentikasi *login admin* yang tidak memanfaatkan

No	Peneliti	Judul Penelitian	Hasil
			fitur HTTPS. 3) *Session Cookie Without Secure Flag* dan *Session Cookie Without HttpOnly Flag* merupakan *cookie* yang didapat dari hasil interaksi *client* dan *server* yang memungkinkan terdapat informasi admin. *Cookie* tersebut dapat dimanfaatkan untuk melancarkan serangan injeksi seperti *XSS*. Solusi yang diberikan berupa *filtering* karakter dengan menambahkan fungsi *integer* untuk menutupi celah *SQL Injection*, menggunakan *HTTPS* dan menghapus fitur *AutoComplete* pada *web server*, memasang *firewall*, *filtering* karakter seperti (<) dan(>) hingga meninjau ulang *script coding* pada *website*.

No	Peneliti	Judul Penelitian	Hasil
2	(Zulfi, 2017)	Evaluasi Keamanan Aplikasi Sistem Informasi Mahasiswa Menggunakan *Framework* VAPT (Studi Kasus: Sister Universitas Jember)	Terdapat beberapa celah keamanan yang ditemukan pada dua *domain web* SISTER yang diuji, yaitu sebagai berikut •Sso.unej.ac.id: *-Application Error Message* *-Cross Site Scripting* (*content sniffing*) *-X-Frame-Option Header Not Set* *-Possible Username or Password Disclosure* *-Incomplete or No Cache-Control and Pragma HTTP Header Set* • Sister.unej.ac.id: *-Cross Site Scripting (verified)* *-Application Error Message* *-HTML Form without CSRF Protection* *-X-Frame-Option Header Not Set* *-Incomplete or No Cache-Control and Pragma HTTP Header Set*

No	Peneliti	Judul Penelitian	Hasil
	(Alwi dkk, 2020)	Analisis Keamanan *Website* Menggunakan Teknik *Footprinting* dan *Vulnerability Scanning*	Penelitian berfokus pada dua teknik pada *ethical hacking*, yaitu *Footprinting* dan *Vulnerability Scanning*. Penelitian hanya berfokus pada pencarian potensi kelemahan dan tidak bertujuan untuk dieksploitasi. Hasilnya terdapat beberapa kelemahan dengan tingkat kerentanan dari *low* sampai *high* seperti *CORS (Cross-Origin Resource Sharing) origin validation failure (high), X-Frame-Options Header Not Set (Medium), Directory listing is enabled (Medium), HTML form without CSRF protection (Medium), WordPress username enumeration (Medium), dan Cookie No HttpOnly Flag (Low)*.

2.2. *Penetration Testing*

Penetration Testing adalah kegiatan pengujian keamanan sistem informasi secara legal dengan tujuan untuk meningkatkan kualitas keamanan dari sebuah sistem. *Penetration testing* biasanya dilakukan oleh tenaga profesional bidang keamanan jaringan untuk mengidentifikasi risiko keamanan dan kerentanan dalam sistem dan jaringan. Tujuan dilakukannya *penetration testing* adalah agar tindakan pencegahan dapat dilakukan dan risiko terjadinya serangan dapat dikurangi hingga tingkat tertentu. Dalam hal ini, peran seorang peretas etis atau *ethical hacker* dibutuhkan dalam bisnis peretasan dan karena itu perlu berperilaku profesional (Graves, 2010).

Penetration Testing bertujuan untuk menunjukkan sejauh mana seorang penyerang dapat masuk ke dalam sistem yang dimiliki suatu instansi. Biasanya skenario peretasan yang dilakukan adalah mencari kemungkinan kerentanan, menyerang kerentanan tersebut agar bisa masuk ke dalam sistem, dan mengambil data-data penting seperti dokumen instansi, atau informasi sensitif seperti nama, alamat, nomor telepon, *e-mail*, hingga *username* dan *password* ketika penyerang dapat mengambil alih hak akses administrator.

Ada tiga jenis pengujian pada *penetration testing*, yaitu sebagai berikut (Zulfi, 2017).

2.2.1. *Black box testing*

Black box testing adalah teknik yang menggunakan keahlian dari penguji untuk melakukan serangkaian penyerangan terhadap suatu sistem. Pada skenario teknik pengujian ini, penguji bertindak sebagai *hacker* yang melakukan penyerangan dari dalam maupun luar jaringan sistem. Dalam hal ini, penguji tidak memiliki informasi apapun tentang sistem yang akan diserang, baik itu akses, topologi jaringan, konfigurasi sistem dan informasi tentang sistem lainnya. *Black box testing* dapat dilakukan di luar ataupun dari dalam wilayah sistem berada.

2.2.2. *White box testing*

White box testing adalah teknik yang membutuhkan informasi tentang sistem yang akan diuji. Informasi tersebut berupa infrastruktur, arsitektur jaringan, kode sistem, dan sebagainya. Pada umumnya pengujian ini dilakukan di dalam wilayah sistem yang diuji berada.

2.2.3. *Grey box testing*

Grey box testing adalah kombinasi dari kedua teknik yang telah disebutkan sebelumnya. Pada pelaksanaannya, penguji diberikan informasi secara terbatas, serta memiliki hak akses yang sama dengan pengguna sistem pada umumnya.

2.3. *Vulnerability Assesment*

Vulnerability atau yang biasa disebut celah pada keamanan sistem didefinisikan sebagai cacat atau kelemahan pada sebuah sistem yang dapat dimanfaatkan untuk mendapatkan akses tidak sah ke dalam sebuah sistem. Pemanfaatan celah keamanan yang berhasil dapat memungkinkan penyerang melakukan manipulasi data, mengubah hak akses, dan lain-lain (Baloch, 2017).

Biasanya *vulnerability* adalah kelemahan yang disebabkan oleh kesalahan pengaturan sistem ataupun kelalaian oleh administrator sistem (*human error*). Adanya *vulnerability* memunculkan berbagai upaya untuk melakukan ekploitasi bagaimana mengetahui kerentanan sebuah sistem komputer. Untuk itulah ada istilah yang disebut dengan *Exploit*. *Exploit* adalah sebuah aktivitas untuk menyerang keamanan komputer secara spesifik. *Exploit* banyak digunakan untuk kegiatan penetrasi baik secara legal ataupun ilegal untuk mencari kelemahan pada komputer (Zulfi, 2017).

Vulnerability Assessment adalah proses identifikasi secara menyeluruh dan mendalam pada suatu sistem informasi terkait keamanan dokumen, informasi, pemindaian jaringan, konfigurasi sistem, kesadaran orang-orang yang terlibat dalam penggunaan sistem, hingga cara pengelolaan sistem untuk mengetahui seluruh potensi kerentanan yang terdapat pada sistem. *Vulnerability Assessment* lebih fokus untuk mencari tahu berbagai macam kerentanan pada jaringan target, kemudian mengidentifikasi kemungkinan kerentanan dari sisi aplikasi, sistem operasi, hingga infrastruktur jaringan.

Perbedaan dari tahap *penetration testing* adalah kerentanan yang telah ditemukan tidak perlu dieksploitasi namun memiliki potensi untuk dieksploitasi oleh penyerang sehingga harus segera ditutup oleh pihak administrator. Setelah kerentanan berhasil diidentifikasi, maka dilakukan evaluasi berdasarkan hasil analisis kerentanan yang ditemukan untuk menentukan tingkat risiko yang mungkin terjadi. Hasil dari identifikasi tersebut nantinya akan dilakukan penghitungan tingkat kerentanan menggunakan *framework* atau suatu persamaan untuk memberikan peringkat seberapa parah kerentanan yang telah ditemukan. Hasil dari *Vulnerability Assessment* ini dikategorikan menjadi empat tingkatan kelemahan, yaitu:

2.3.1. Sangat Tinggi (*Critical*)

Pada *level* ini, terdapat kerentanan yang berpotensi tinggi untuk menjadi ancaman dan harus segera diatasi. Namun upaya pencegahan dan penanganan kerentanan tidak memadai.

2.3.2. Tinggi (*High*)

Pada *level* ini, tingkat ancaman yang terdapat pada kerentanan lebih kecil dibandingkan level *critical* dan bersifat lokal, namun upaya pencegahan masih belum memadai.

2.3.3. Sedang (*Medium*)

Pada *level* ini, tingkat kerentanan bersifat lokal dan upaya pencegahan dan penanganan juga bersifat lokal dan cukup memadai.

2.3.4. Rendah (*Low*)

Pada *level* ini, tingkat kerentanan yang terdapat pada sistem rendah sehingga dampaknya tidak begitu buruk dan upaya pencegahan dan penanganan kelemahan sudah memadai.

2.4. *Brute Force Attack*

Istilah *Brute Force* dipopulerkan oleh Kenneth Lane Thompson dengan mottonya "*When in doubt, use brute force*" (jika ragu, gunakan *brute force*). *Brute Force Attack* adalah sebuah metode serangan yang sering digunakan peretas untuk mencuri *password* (*password cracking*) dengan cara mencoba semua kemungkinan kombinasi karakter, kata kunci atau simbol. Metode ini memungkinkan peretas menemukan *password* yang diinginkan, namun tingkat keberhasilan metode ini tergantung dari seberapa panjang kombinasi karakter dari *password* yang ingin diretas. Semakin panjang kombinasi karakter, semakin lama proses pencarian dapat berjalan. Metode ini awalnya merujuk pada program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia, contohnya untuk menyelesaikan persamaan kuadrat seperti $x^2+7x-44=0$ dengan variabel x sebagai *integer*, dengan menggunakan *brute force*, pengguna hanya perlu membuat program yang mencoba semua nilai *integer* yang mungkin untuk variabel x sehingga jawaban dari persamaan tersebut muncul (Irwansyah & Purwanto, 2016).

Brute Force Attack merupakan salah satu jenis serangan *password* yang dapat dilakukan secara *offline* sehingga teknik ini dapat dilakukan di mana saja dari jarak target yang ingin diretas. Kelebihan dari metode ini adalah metode ini berguna untuk menjebol semua jenis *password*, bahkan enkripsi *password* seperti MD5, SHA1, AES, dan sebagainya, sedangkan kekurangan

dari metode *Brute Force Attack* adalah metode serangan ini paling banyak menghabiskan waktu karena tergantung dari banyaknya kemungkinan kombinasi karakter yang terdapat pada *password* sehingga kinerja komputer menjadi lambat (Pramudita, 2011).

Hal-hal yang perlu diperhatikan dalam menggunakan metode *Brute Force Attack* adalah sebagai berikut.

2.4.1. Asumsikan *password* diketik dengan format karakter *lowercase* (huruf kecil)

Pada kasus ini, waktu yang dibutuhkan untuk mendapatkan *password* cenderung sama, tetapi jika *password* yang ingin dicari mengandung karakter *uppercase* (huruf besar), cara ini tidak akan berhasil.

2.4.2. Coba semua kemungkinan

Sebagai contoh, jika *password* mengandung tujuh karakter *lowercase*, maka dibutuhkan waktu sekitar 4 jam untuk mendapatkan *password* yang diinginkan, tetapi jika mencoba kemungkinan kombinasi antara *lowercase* dan *uppercase*, akan memakan waktu hingga sekitar 23 hari untuk mendapatkan *password*.

2.4.3. Gunakan metode *Trade-off*

Cara ini dapat dilakukan dengan menggunakan kombinasi-kombinasi *password* yang mungkin, seperti contoh “kamualay”, “KAMUALAY” dan “Kamualay”. Kombinasi yang terdiri dari karakter dan simbol-simbol yang rumit seperti “kAmUaLaY” atau “K4mU@LaY” tidak dimasukkan dalam proses pencarian. Dengan cara ini, lambatnya performa komputer dalam proses *brute force* dapat teratasi, namun ada kemungkinan *password* tidak akan ditemukan karena belum tentu *password* yang ingin diambil memiliki kombinasi yang rumit.

2.5. Nikto

Nikto adalah *tools* yang berfungsi untuk melakukan pemindaian pada situs *website* dan melaporkan kerentanan yang ditemukannya yang dapat digunakan untuk melakukan pengujian celah keamanan. Nikto juga dapat digunakan untuk memindai beberapa *file* pada *server* seperti *file index*, versi *plugin* yang terpasang pada *server* dan direktori *server* (Purbo, 2018).

Namun pada penggunaannya, tidak semua informasi yang ditampilkan oleh Nikto adalah informasi kerentanan pada sistem, terkadang beberapa informasi yang ditampilkan hanya sekedar informasi mengenai *server* saja dan tidak memiliki *value* tentang keamanan sistem seperti lokasi direktori, versi *web server* yang digunakan dan informasi *header* pada *website*.

Contoh perintah Nikto antara lain:

```
nikto –host https://test.com/

nikto –C –all –host 127.0.0.1
```

2.6. Nmap

Nmap adalah *tool* yang berfungsi untuk melakukan *port scanning* pada *website* serta mencari tau *port* yang terbuka yang dapat digunakan untuk mencari tau metode yang potensial untuk melakukan eksploitasi. Selain informasi tentang *port* jaringan, Nmap dapat menemukan informasi tentang layanan yang digunakan oleh sistem (nama layanan dan versi yang digunakan), sistem operasi yang digunakan, *firewall*, dan beberapa informasi lain mengenai jaringan.

Nmap tersedia secara *default* pada sistem operasi Kali Linux. *Tools* ini dapat di *install* pada distro Linux yang lain atau sistem operasi lain seperti Windows dan Mac-OS. Nmap juga tersedia dalam bentuk *Graphic User Interface* (GUI) dengan nama produk Zenmap (Purbo, 2018).

Beberapa contoh perintah Nmap antara lain:

nmap –v –A 127.1.1.0

nmap –v –O –Pn 80, 443 test.com

2.7. WpScan

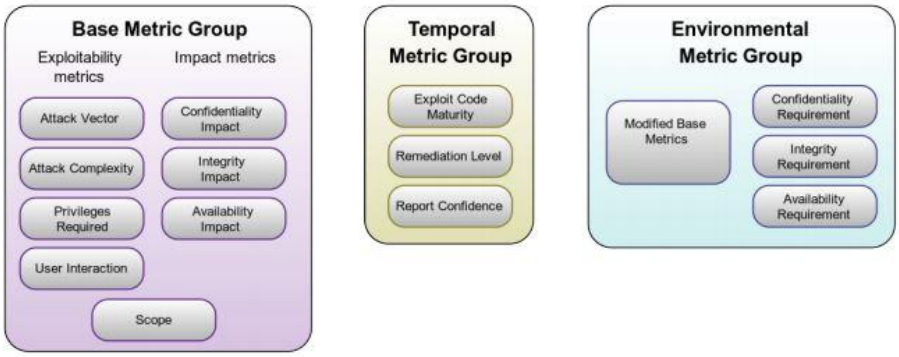
WpScan adalah *tools vulnerability scanning* untuk *website* yang menggunakan CMS *Wordpress*.

Fungsi WpScan secara umum yaitu dapat memindai daftar *Plugin*, jenis *theme* yang digunakan hingga melihat kemungkinan kerentanan pada *website*. Kerentanan yang ditemukan biasanya dapat ditemukan pada versi *plugin* atau *theme* yang biasanya sudah kadaluarsa dan belum di-*upgrade* oleh pemilik *website* (Dewanto, 2018). Beberapa fungsi WpScan antara lain sebagai berikut:

1. Daftar *plugin* yang terpasang.
2. Jenis *theme* yang digunakan.
3. Potensi kerentanan yang terdapat pada sistem.
4. Melancarkan serangan *Brute Force* pada beberapa *user*.

2.8. Common Vulnerability Scoring System

Common Vulnerability Scoring System (CVSS) adalah kerangka kerja (*framework*) yang dibangun secara terbuka yang bertujuan untuk mengomunikasikan tingkat keparahan dan dampak yang ditimbulkan dari suatu kerentanan. Hasil dari CVSS adalah skor numerik yang menunjukkan tingkat keparahan dari sebuah kerentanan yang ditemukan dan relatif terhadap kerentanan lain (FIRST, 2019). CVSS terdiri dari tiga kelompok metrik, yaitu Basis (*Base*), Temporal, dan Lingkungan (*Environment*). Tiap kelompok metrik memiliki nilai faktor masing-masing sesuai kebutuhan, seperti pada Gambar 1.



Gambar 1.Kelompok metrik CVSS.

Kelompok metrik *Base* merepresentasikan keparahan berdasarkan karakter intrinsik yang konstan seiring waktu dan mengasumsikan dampak terburuk di berbagai lingkungan yang diterapkan. Metrik ini memiliki dua sub-metrik, terdiri dari metrik eksploitasi (*Exploitability metrics*), metrik eksploitasi terdiri dari empat faktor penilaian, yaitu *Attack Vector*, *Attack Complexity*, *Privileges Required*, dan *User Interaction*, dan metrik dampak (*Impact metric*) yang terdiri dari tiga faktor penilaian, yaitu *Confidentially Impact*, *Integrity Impact*, dan *Availability Impact*. Metrik dampak juga memiliki faktor penilaian tambahan, yaitu *Scope*.

Setelah skor basis didapat, hasil dari persamaan metrik ini dapat disempurnakan dengan menghitung nilai metrik temporal dan nilai metrik lingkungan untuk mendapatkan nilai yang lebih akurat dalam menggambarkan tingkat keparahan dari sebuah kerentanan terhadap lingkungan pengguna. Namun, pada umumnya, menghitung nilai kedua metrik tersebut tidak terlalu dibutuhkan, tetapi disarankan jika ingin mendapatkan hasil yang lebih sempurna.

Kelompok temporal menyesuaikan tingkat keparahan yang dihasilkan oleh metrik basis berdasarkan faktor-faktor yang berubah dari waktu ke waktu, seperti ketersediaan kode eksploitasi. Kelompok Lingkungan menyesuaikan

keparahan Basis dan Temporal ke lingkungan komputasi tertentu. Biasanya skor dari kelompok metrik basis yang akan dipublikasikan karena skor dari kelompok ini tidak berubah seiring waktu dan sifatnya umum untuk semua lingkungan.

Setiap sub-kelompok memiliki nilai faktor masing-masing, nilai-nilai faktornya dapat dilihat pada Tabel 2 sampai dengan Tabel 9 berikut.

Tabel 2. *Attack Vector* (AV).

Nilai Metrik	Penjelasan
Network **(N)**	Komponen yang rentan terikat pada jaringan internet dan dapat dieksploitasi dari jarak jauh dan dapat dianggap sebagai serangan yang dapat dieksploitasi pada tingkat protokol satu atau lebih jaringan *hop* (misalnya, di satu atau lebih *router*). Contoh serangan jaringan adalah *Denial of Service* (DoS) dengan mengirimkan paket TCP yang dibuat khusus melalui jaringan area yang luas. .
Adjacent **(A)**	Komponen yang rentan terikat pada jaringan, tetapi serangan yang dilancarkan terbatas pada tingkat protokol ke topologi yang berdekatan secara logis. Ini berarti serangan harus diluncurkan dari jaringan fisik bersama yang sama (misalnya, *Bluetooth* atau IEEE 802.11) atau logis (misalnya, subnet IP lokal), atau dari dalam domain administratif yang aman atau terbatas (misalnya, MPLS, VPN aman ke zona jaringan administratif). Contoh serangan adalah *ARP flood* (IPv4) yang mengarah ke penolakan layanan pada segmen LAN .
Local **(L)**	Komponen yang rentan tidak terikat pada jaringan dan jalur penyerang melalui kemampuan *read*/*write*/*execute* dengan keadaan sebagai berikut: • penyerang mengeksploitasi kerentanan dengan mengakses sistem target secara lokal (misalnya, *keyboard*, konsol), atau dari jarak jauh (misalnya, SSH); atau • penyerang bergantung pada interaksi pengguna untuk melakukan tindakan yang diperlukan untuk mengeksploitasi kerentanan (misalnya, menggunakan teknik rekayasa sosial untuk mengelabui pengguna

	yang sah agar membuka dokumen berbahaya).
***Physical* (P)**	Serangan tersebut mengharuskan penyerang untuk secara fisik menyentuh atau memanipulasi komponen yang rentan. Interaksi fisik mungkin singkat (misalnya, serangan *evil maid*) atau terus-menerus. Contoh serangan semacam itu adalah serangan *cool boot* di mana penyerang memperoleh akses ke kunci enkripsi *disk* setelah mengakses sistem target secara fisik. Contoh lain termasuk serangan periferal melalui *FireWire* atau *USB Direct Memory Access* (DMA).

Tabel 3. *Attack Complexity* (AC).

Nilai metrik	Penjelasan
***Low* (L)**	Kondisi akses khusus atau keadaan khusus tidak ada. Seorang penyerang dapat mengharapkan kesuksesan yang berulang ketika menyerang komponen yang rentan.
***High* (H)**	Sebuah serangan yang berhasil tergantung pada kondisi di luar kendali penyerang. Artinya, serangan yang berhasil tidak dapat dilakukan sesuka hati, tetapi memerlukan sejumlah upaya yang terukur dalam persiapan atau eksekusi terhadap komponen yang rentan sebelum serangan berhasil dilancarkan. Misalnya, serangan yang berhasil mungkin bergantung pada penyerang yang mengatasi salah satu dari kondisi berikut: • Penyerang harus mengumpulkan pengetahuan tentang lingkungan di mana target/komponen yang rentan berada. Misalnya, persyaratan untuk mengumpulkan detail tentang pengaturan konfigurasi target, nomor urut, atau data rahasia. •Penyerang harus menyiapkan lingkungan target untuk meningkatkan keandalan eksploitasi. Misalnya, eksploitasi berulang, atau mengatasi teknik mitigasi eksploitasi tingkat lanjut. • Penyerang harus menyuntikkan serangan ke jalur jaringan logis antara target dan sumber daya yang diminta oleh korban untuk membaca dan/atau memodifikasi komunikasi jaringan (misalnya, serangan *man in the middle*).

Tabel 4. *Privileges Required* (PR)

Nilai Metrik	Penjelasan
***None* (N)**	Penyerang tidak sah sebelum menyerang, karena itu tidak memerlukan akses apa pun ke pengaturan atau *file* dari sistem yang rentan untuk melakukan serangan.
***Low* (L)**	Penyerang membutuhkan hak istimewa yang menyediakan kemampuan pengguna dasar yang biasanya hanya dapat memengaruhi pengaturan dan *file* yang dimiliki oleh pengguna. Atau, penyerang dengan hak istimewa rendah hanya memiliki kemampuan untuk mengakses sumber daya yang tidak sensitif.
***High* (L)**	Penyerang memerlukan hak istimewa yang dapat memberikan kontrol signifikan (misalnya, administratif) atas komponen rentan yang memungkinkan akses ke pengaturan dan *file* di seluruh komponen.

Tabel 5. *User Interaction* (UI)

Nilai Metrik	Penjelasan
***None* (N)**	Sistem yang rentan dapat dieksploitasi tanpa interaksi dari pengguna mana pun.
***Required* (R)**	Eksploitasi kerentanan yang berhasil memungkinkan penyerang untuk mengambil beberapa tindakan sebelum kerentanan dapat dieksploitasi..

Tabel 6. *Confidentially* (C).

Nilai metrik	Penjelasan
***High* (H)**	Adanya kehilangan kerahasiaan total, yang mengakibatkan semua sumber daya di dalam komponen dibocorkan kepada penyerang. Atau, akses ke hanya beberapa informasi terbatas, tetapi informasi yang diungkapkan memberikan dampak langsung dan serius. Misalnya, penyerang mencuri kata sandi administrator,

	atau kunci enkripsi pribadi dari *server web*.
***Low* (L)**	Ada beberapa kehilangan kerahasiaan. Akses ke beberapa informasi terbatas dapat diperoleh, tetapi penyerang tidak memiliki kendali atas informasi yang diperoleh. Pengungkapan informasi tidak menyebabkan kerugian langsung yang serius pada komponen yang terkena dampak.
***None* (N)**	Tidak ada kehilangan kerahasiaan dalam komponen yang terkena dampak

Tabel 7. *Integrated* (I).

Nilai Metrik	Penjelasan
***High* (H)**	Adanya kehilangan integritas total, atau hilangnya perlindungan sepenuhnya. Misalnya, penyerang dapat memodifikasi semua *file* yang dilindungi oleh komponen yang terpengaruh. Atau, hanya beberapa *file* yang dapat dimodifikasi, tetapi menimbulkan konsekuensi langsung dan serius pada komponen yang terpengaruh.
***Low* (L)**	Modifikasi data dimungkinkan, tetapi penyerang tidak memiliki kendali atas konsekuensi modifikasi, atau jumlah modifikasi terbatas. Modifikasi data tidak berdampak serius pada komponen yang terkena dampak.
***None* (N)**	Tidak ada kehilangan integritas dalam komponen yang terdampak.

Tabel 8. *Availability* (A).

Nilai Metrik	Penjelasan
***High* (H)**	Ada kehilangan total ketersediaan, sehingga penyerang dapat sepenuhnya memiliki akses ke sumber daya di komponen yang terkena dampak; kerugian ini dapat bertahan (sementara penyerang terus melakukan serangan) atau persisten (kondisi tetap ada bahkan setelah serangan selesai). Penyerang memiliki

	kemampuan untuk menolak beberapa ketersediaan, tetapi hilangnya ketersediaan data menghadirkan konsekuensi langsung yang serius terhadap komponen yang terkena dampak (misalnya, penyerang tidak dapat mengganggu koneksi yang ada, tetapi dapat mencegah koneksi baru; penyerang dapat berulang kali mengeksploitasi kerentanan bahwa, dalam setiap serangan yang berhasil, hanya membocorkan sejumlah kecil memori, tetapi setelah eksploitasi berulang-ulang menyebabkan layanan menjadi tidak tersedia sama sekali).
***Low* (L)**	Performa berkurang atau adanya gangguan dalam ketersediaan sumber daya. Penyerang tidak memiliki kemampuan untuk sepenuhnya menolak layanan kepada pengguna yang sah. Sumber daya dalam komponen yang terkena dampak tersedia sebagian sepanjang waktu, atau tersedia sepenuhnya hanya beberapa waktu, tetapi secara keseluruhan tidak ada konsekuensi langsung dan serius terhadap komponen yang terkena dampak.
***None* (N)**	Tidak ada dampak terhadap ketersediaan dalam komponen yang terpengaruh.

Tabel 9. *Scope* (S).

Nilai Metrik	Penjelasan
***Unchanged* (U)**	Kerentanan yang dieksploitasi hanya dapat memengaruhi sumber daya yang dikelola oleh otoritas keamanan yang sama. Dalam hal ini, komponen yang rentan dan komponen yang terkena dampak adalah sama, atau keduanya dikelola oleh otoritas keamanan yang sama.
***Changed* (U)**	Kerentanan yang dieksploitasi dapat memengaruhi sumber daya di luar cakupan keamanan yang dikelola oleh otoritas keamanan komponen rentan. Dalam hal ini, komponen rentan dan komponen yang terkena dampak berbeda dan dikelola oleh otoritas keamanan yang berbeda.

Dalam menghitung skor menggunakan CVSS, perlu diperhatikan bahwa semua metrik harus diberi skor dengan asumsi bahwa penyerang telah menemukan dan mengidentifikasi kerentanan dari sebuah sistem. Artinya, analis tidak perlu meninjau cara penyerang mengidentifikasi kerentanan tersebut.

III. METODOLOGI PENELITIAN

3.1 Waktu dan Tempat Penelitian

Penelitian dilaksanakan pada semester genap tahun ajaran 2019/2020, bertempat di Jurusan Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.

3.2. Alat Pendukung

3.2.1. Perangkat Keras (*Hardware*)

Laptop ASUS model X442UR dengan spesifikasi sebagai berikut.

a. *Processor* Intel (R) Core (TM) i7-7500U CPU @ 2.70GHz (4 CPUs), ~2.9GHz.
b. RAM: 4 GB.
c. HDD: 1 TB.

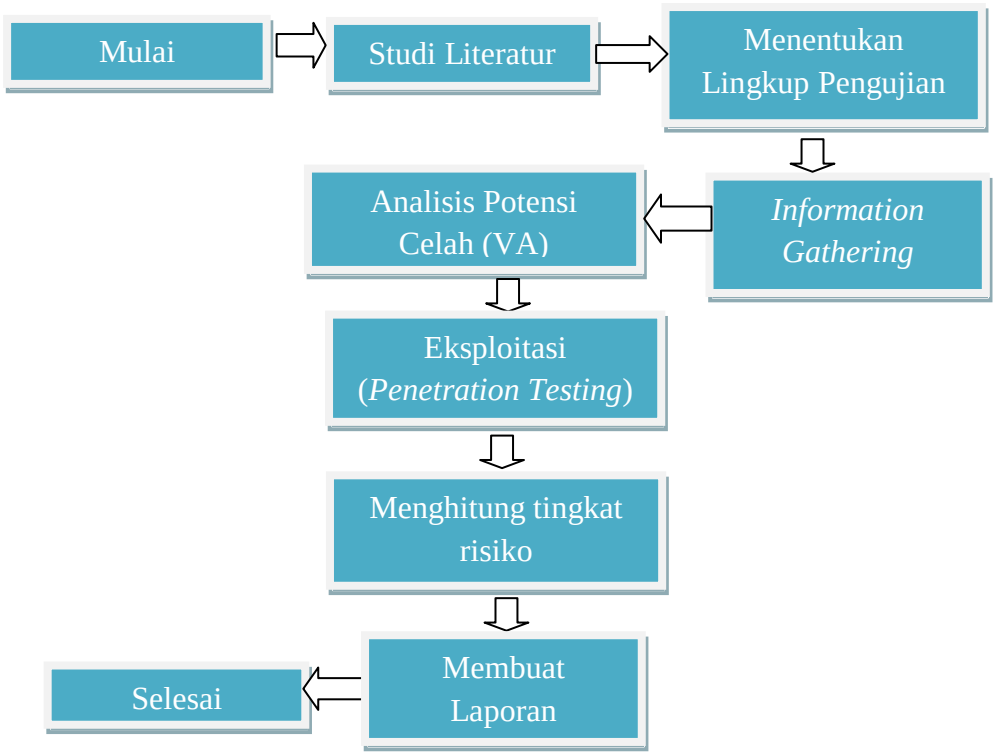
3.2.2. Perangkat Lunak (*Software*)

Perangkat lunak yang digunakan untuk pengujian keamanan adalah sebagai berikut:

a. Sistem Operasi Windows 10 *Home Single Language* 64 bit (10.0, *Build* 18362)
b. Oracle Virtual Box versi 6.1.
c. Sistem Operasi Kali Linux 2020.4 amd64.
d. *Web Browser* (*Google Chrome* dan *Mozilla Firefox*).
e. Nikto.
f. Nmap.
g. WpScan.

3.3 Metode Penelitian

Metode penelitian yang digunakan terdiri dari beberapa tahap. Gambaran alur penelitian yang dilakukan dapat dilihat pada Gambar 2.



Gambar 2. Alur penelitian.

3.3.1. Studi Literatur

Langkah awal yang dilakukan dalam penelitian ini adalah studi literatur dan fiksasi studi kasus. Studi literatur bertujuan untuk menentukan kerangka kerja dan tahapan-tahapan pengujian yang dilakukan.

3.3.2. Menentukan Lingkup Pengujian

Pada tahap ini pengujian berfokus pada pencarian celah dari *website* Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung yang meliputi struktur jaringan pada *server*, *firewall*, *database*, *website*, dan hal lain yang berhubungan dengan target yang akan diuji.

3.3.3. *Information Gathering*

Pada tahap ini, dilakukan *information gathering*, yaitu mengumpulkan informasi terkait dengan sistem yang akan diuji seperti sistem operasi yang digunakan, alamat IP, struktur jaringan pada *server*, *database*, hingga *port* yang dibuka pada sistem. Setelah informasi yang dibutuhkan telah terkumpul, dilanjutkan dengan pencarian celah pada sistem yang diuji. Dalam pelaksanaannya menggunakan bantuan *tools* yang digunakan untuk mendeteksi berbagai celah dari sistem yang diuji. Hasil pencarian celah akan digunakan sebagai bahan perencanaan untuk lanjut ke tahap berikutnya.

3.3.4. Analisis Potensi Celah (*Vulnerability Assessment*)

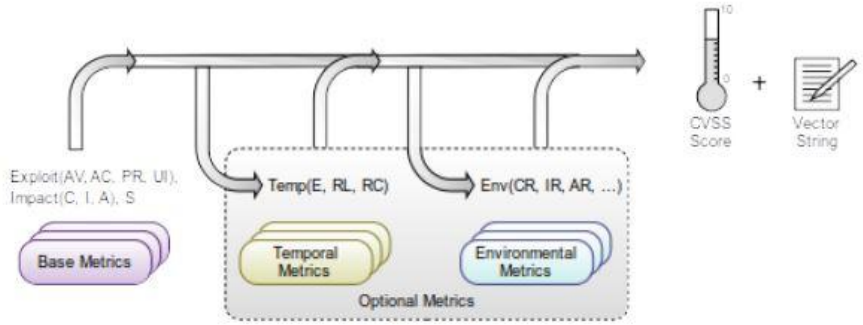
Tahap ini merupakan bagian dari *Vulnerability Assessment* (VA). Pada tahap ini, dilakukan analisis kerentanan berdasarkan informasi yang telah dikumpulkan dari tahap sebelumnya, informasi yang telah dikumpulkan tersebut akan dibuat rencana pengujian untuk tahap *penetration testing* dengan cara mengidentifikasi komponen atau direktori apa saja yang berpotensi memiliki kerentanan, apa saja kerentanan yang ditemukan, kerentanan tersebut ditemukan dan bagaimana tahap pengujian kerentanan yang dilakukan berdasarkan kerentanan yang telah ditemukan.

3.3.5. Eksploitasi Celah (*Penetration Testing*)

Tahap eksploitasi merupakan bagian dari *penetration testing* yang bertujuan untuk membuktikan bahwa kerentanan yang ditemukan dari tahap sebelumnya dapat dieksploitasi secara nyata. Pada tahap ini, dilakukan percobaan eksploitasi untuk mendapatkan hak akses, mengubah informasi yang ada, mengambil informasi, hingga dokumen yang tersedia dari *website* yang diuji. Setelah eksploitasi dilakukan, akan dilakukan penghitungan risiko yang disebabkan oleh kerentanan yang terdapat pada sistem yang diuji.

3.3.6. Menghitung Tingkat Risiko

Setelah tahap eksploitasi selesai, selanjutnya adalah menghitung tingkat risiko dari kerentanan yang telah dieksploitasi. Metode penghitungan yang digunakan adalah metode CVSS (*Common Vulnerability Scoring System*) menggunakan perhitungan dari kelompok metrik *base* untuk mengetahui skala *level* kerentanan yang ditemukan. Persamaan dari metrik basis akan menghitung nilai dari 0.0 hingga 10.0 seperti yang diilustrasikan pada Gambar 3.



Gambar 3. Proses penghitungan metrik CVSS

Hasil akhir dari perhitungan CVSS akan diakumulasikan dengan angka dari nilai 0.0 sampai dengan 10.0. semakin tinggi hasilnya, maka semakin berbahaya kerentanan tersebut. Setiap nilai merepresentasikan tingkat kerentanan yang dapat dilihat pada Tabel 10.

Tabel 10. Nilai kualitatif kerentanan.

Keterangan	**Nilai CVSS**
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

3.3.7. Penulisan Laporan Akhir

Pada tahap ini, hasil pengujian yang telah dilakukan disusun dalam bentuk laporan. Laporan ini berisi dokumentasi pengujian, tingkat kelemahan pada sistem berdasarkan dampak dari celah yang telah ditemukan, dan saran perb sistem.

V. SIMPULAN

5.1 Simpulan

Berdasarkan hasil penelitian yang dilakukan pada *website* FMIPA Universitas Lampung, dapat disimpulkan sebagai berikut:

1. *Website* FMIPA Universitas Lampung rentan terhadap serangan *Brute Force* dan dibuktikan dengan melancarkan serangan tersebut kepada *user* yaitu mahasiswa FMIPA Universitas Lampung yang terdaftar secara resmi.
2. Pada versi PhpMyAdmin yang terpasang, terdapat potensi kerentanan *Cross-site Request Forgery (CSRF)*.
3. *Brute Force* dapat dilancarkan berkali-kali tanpa batas dan dapat diserang kapanpun dan dimanapun.
4. Beberapa *plugin* yang terpasang merupakan versi lama yang belum diperbarui, apabila tidak segera diperbarui maka akan membuka peluang bagi pihak luar yang ingin menyerang *website* FMIPA melalui celah dari versi yang terpasang.

5.2 Saran

Berdasarkan hasil dari penelitian tersebut, berikut saran yang dapat diterapkan untuk perbaikan keamanan sistem FMIPA:

1. Gunakan *password* dengan kombinasi huruf besar, huruf kecil, angka, dan simbol dengan jumlah karakter maksimal 8 karakter.
2. Aktifkan fitur *captcha* untuk memvalidasi pengguna. Fitur ini dapat ditemukan di pengaturan *hosting* atau memasang *plugin* khusus untuk fitur *captcha*.
3. Selalu *update* versi *Wordpress* dan *plugin* yang terpasang pada *website*.
4. Membuat *limit* akses direktori yang memuat data-data sensitif *user*, atau *hide* direktori yang rentan sehingga *hacker* tidak mudah mencuri informasi pengguna.

DAFTAR PUSTAKA

Alwi, E. I., Herdianti, H., & Umar, F. (2020). Analisis Keamanan *Website* Menggunakan Teknik Footprinting dan Vulnerability Scanning. *INFORMAL: Informatics Journal*, *5*(2), 43.

Baloch, R. (2017). Ethical Hacking and Penetration Testing Guide. United States. CRC Press Taylor & Francis Group.

Cinderatama, & Amini. (2016). Pembuatan Sistem Informasi Lowongan Kerja. *01*(02), 1–6.

Dewanto, A. P. (2018). Penetration Testing pada Domain uii.ac.id Menggunakan OWASP 10.Yogyakarta.*Universitas Islam Indonesia*.

FIRST. (2019). Common Vulnerability Scoring System version 3.1 Specification Document Revision 1. 1, 1–22. https://www.first.org/cvss/v3.1/specification-document (diakses 5 April 2021).

Graves, K. (2010). Certified Ethical Hacking v6 study guide. Canada. Wiley Publishing, Inc., Indianapolis, Indiana.

Irwansyah, & Purwanto, T. D. (2016). Evaluasi Keamanan Sistem Informasi

Pada Lembaga Pemerintahan Provinsi Sumatera Selatan. 115(777), 40–40. *Universitas Bina Darma*.

Pramudita, K. E. (2011). Brute Force Attack dan Penerapannya pada Password Cracking. *Makalah IF3051 Strategi Algoritma – Sem. I Tahun 2010/2011, I*(2011).

Purbo, O. W. (2018). Belajar Hacking / Attack. https://lms.onnocenter.or.id/pustaka/docs/sec/XIT-belajar-hacking.pdf (diakses 16 Juli 2021).

Zulfi, A. F. (2017). Evaluasi Keamanan Aplikasi Sistem Informasi Mahasiswa Menggunakan Framework VAPT (Studi Kasus: Sister Universitas Jember). 159. *Institut Teknologi Sebelas November*.