Jurnal Vocational Teknik Elektronika dan Informatika
http://ejournal.unp.ac.id/index.php/voteknika/index
Vol. 9, No. 2, Juni 2021 **P- ISSN: 2302-3295, E-ISSN : 2716-3989**

Analisis Metode *Web Security* PTES (*Penetration Testing Execution And Standart*) Pada Aplikasi *E-Learning* Universitas Negeri Padang

Fadilla Yulia Fauzan[1*], Syukhri[2]
[1]Prodi Pendidikan Teknik Informatika Fakultas Teknik Universitas Negeri Padang
[2]Jurusan Teknik Elektronika Fakultas Teknik Universitas Negeri Padang
Jl. Prof. Hamka Kampus UNP Air Tawar Padang
**Corresponding author* e-mail : fadilayulia31@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk mengetahui kerentanan pada *E-Learning* Universitas Negeri Padang dengan menggunakan metode *Penetration Testing Execution Standard*. Metode *penetration testing* ini berfungsi untuk melihat hasil dan analisis dari pengujian keamanan pada *E-Learning* Universitas Negeri Padang, serta dapat menjadi bahan masukan bagi Universitas Negeri Padang dan laporan sebagai acuan untuk keamanan pada *E-Learning* Universitas Negeri Padang. Penelitian ini menggunakan pendekatan kuantitatif dengan penelitian deskriptif. Penelitian menggunakan metode *Penetration Testing* memiliki tahapan-tahapan sebagai berikut: 1. *Pre-engagement Interaction*, 2. *Intelegence Gathering*, 3. *Vulnerabillity Analysis*, 4. *Exploitation*, dan 5. *Reporting*. Hasil pengujian menggunakan *zenmap* didapatkan 6 port yang terbuka pada *elearning.unp2.ac.id*. Pada tahapan *Scanning* menggunakan *Acunetix* yang didapatkan ada beberapa kerentanan teratas yaitu *Cross-site Request Forgery, Development configuration file, Slow HTTP Denial of Service Attack, Weak Password, TLS 1.0 Enable* , dan *exploitation* menggunakan teknik *SQL Injection* dengan hasil tidak dapat melihat celah keamanan, dapat disimpulkan pada tahap *scanning* didapatkan hasil celah dari keamanan web adalah sebanyak 96 dengan disimpulkan *Acunetix Threat Level 2* yaitu pada level *Medium* yang artinya tidak terlalu berpengaruhnya dengan serangan-serangan pada website tersebut, dan pada tahapan *Exploitation* menggunakan SQLMap dengan teknik SQL Injection dimana pada tahap ini dinyatakan gagal karena *e-learning2.unp* sudah menggunakan keamanan SSL/HTTPS yang menyulitkan para hacker masuk ke sistem database web tersebut. Analisis dari tahapan *Penetration Testing* dapat menjadi dasar untuk meningkatkan kualitas keamanan website sehingga dapat mencegah kerentanan yang akan datang.

***Kata kunci** : e-learning, penetration testing, scanning, acunetix, sqlmap*

ABSTRACT

This study aims to determine the vulnerability of E-Learning Padang State University using the method Penetration Testing Execution Standard. This Method penetration testing serves to see the results and analysis of security testing at E-Learning Padang State University, and can be input for Padang State University and reports as a reference for security on E-Learning Padang State University. This research uses a quantitative approach with descriptive research. Research using the method Penetration Testing has the following stages: 1. Pre-engagement interaction, 2. Intelligence Gathering, 3. Vulnerability Analysis, 4. Exploitation, and 5. Reporting. The test results using zenmap found 6 open ports on elearning2.unp.ac.id. At the stage Scanning using Acunetix , there are several top vulnerabilities, namely Cross-site Request Forgery, Development configuration files, Slow HTTP Denial of Service Attack, Weak Password, TLS 1.0 Enable , and exploitation using techniques SQL Injection with the result that they cannot see security holes, It can be concluded at the stage scanning that the results of web security gaps are as many as 96, it is concluded that Acunetix Threat Level 2 is at the level Medium which means that it does not really affect the attacks on the website, and at the stage Exploitation uses SQLMap with the SQL Injection technique where at the This was declared a failure because elearning2.unp already uses SSL / HTTPS security which makes it difficult for hackers to enter the web database system. Analysis of the stage Penetration Testing can be the basis for improving the quality of website security so that it can prevent future vulnerabilities.

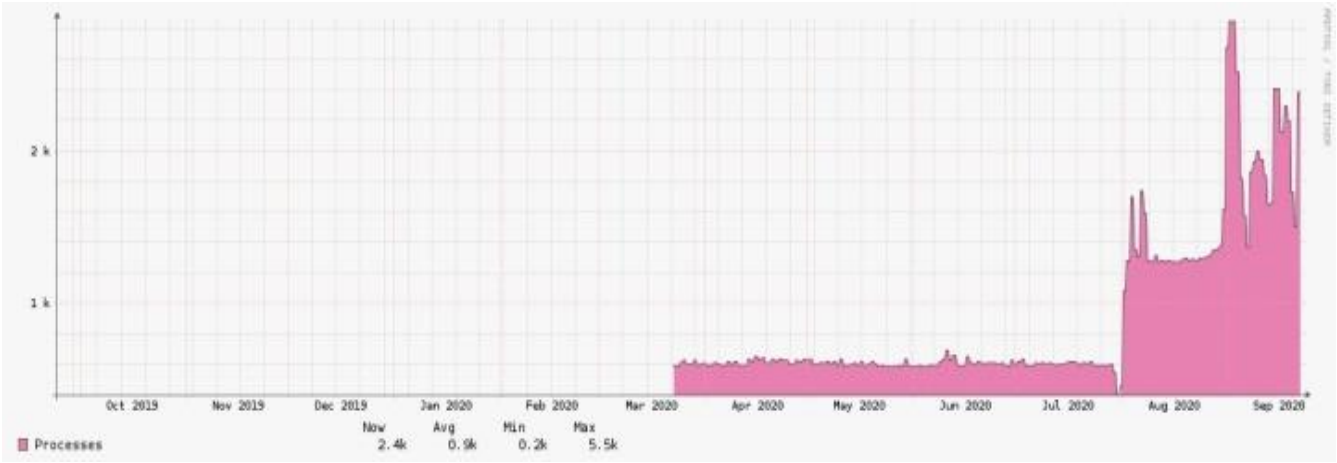
***Keywords:** e-learning, penetration testing, scanning, acunetix, sqlmap*

I. PENDAHULUAN

Perkembangan dunia Teknologi Informasi (TI) yang semakin pesat, kebutuhan akan suatu konsep dan mekanisme belajar mengajar berbasis TI menjadi tidak terelakkan lagi yang membutuhkan sebuah keamanan pada suatu sistem. Security atau keamanan merupakan hal yang sangat penting dalam membangun sebuah jaringan komputer di dalam *web server*. Konsep yang dikenal dengan *E-Learning* ini membawa pengaruh ternyadinya proses transformasi pendidikan konvensional ke dalam bentuk digital.

Banyak Universitas sudah memanfaatkan *E-learning* sebagai media pembelajaran, begitu pula dengan Universitas Negeri Padang (UNP)[1]. *E-learning* Universitas Negeri Padang mulai berfungsi semester Juli-Desember 2013 baru digunakan pertamakali di Fakultas Teknik. Kemudian awal tahun 2014 disosialisasikan ke seluruh UNP secara bertahap sesuai jadwal yang ditentukan. Setelah semua kegiatan sosialisasi selesai *E-learning* sudah dapat dimanfaatkan oleh seluruh dosen yang membina suatu mata kuliah serta mahasiswa yang terdaftar pada mata kuliah tersebut. Mahasiswa yang terdaftar pada mata kuliah tertentu secara otomatis terdaftar sebagai peserta perkuliahan dalam *E-learning*. Pembelajaran dengan media *E-learning* tentu adanya data yang tersimpan, pada proses ini membuktikan bahwa adanya kegiatan *upload* dan *download* dari hasil diskusi maupun tugas dari dosen dan mahasiswa. Mengingat pentingnya data-data tersebut maka perlu diterapkan pengujian keamanan dari *E-learning.* Pengujian ini dilakukan utuk mengetahui tingkat kerentanan agar terhindar dari serangan pihak yang tidak bertanggung jawab.

Merujuk pada hasil wawancara yang dilakukan dengan bapak Mohamad Amin, S.Kom. selaku pegelola *E-learning* UNP menyatakan bahwa penggunaan *E-learning* meningkat selama 2 semester terakhir. Dimana peningkatan terjadi pada masa pandemi yang mengharuskan kegiatan pembelajaran dilakukan secara daring. Dapat dibuktikan pada Gambar 1. *Graffict traffic access* dibawah ini:



Gambar 1. Grafik trafik akses *e-learning* UNP

Berdasarkan grafik tersebut dapat disimpulkan bahwa penggunaan *E-learning* UNP meningkat pada tahun ajaran 2019/2020 semester genap Januari-Juni, peningkatan ini terjadi semakin pesat hingga tahun ajaran 2020/2021 semester ganjil Juli-Desember. Dengan demikian peningkatan penggunaan *E-learning* harus diimbangi dengan keamanan yang baik di sisi *E-learning.* Metode yang digunakan dalam mengamankan fungsi data atau performa yang ada pada suatu sistem, dimana percobaan yang akan dilakukan untuk mengetahui apakah sebuah website aman atau tidaknya dari aksi-aksi berbahaya yang dilakukan oleh penyerang adalah dengan melakukan *Penetration Testing.*

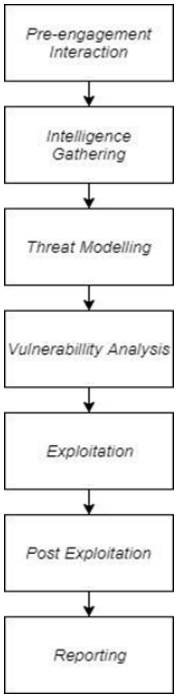
Penetration Testing mempunyai standar resmi sebagai acuan dalam pelaksanaannya. Tujuan dari *Penetration Testing* adalah untuk mengidentifikasi titik-titik lemah dalam sistem keamanan organisasi khususnya sistem komputer. Selain itu untuk mengukur kepatuhan akan pelaksanaan kebijakan keamanannya. *Penetration Testing* juga dapat memperingatkan kelemahan dalam kebijakan keamanan teknologi informasi pada sistem[2].

E-Learning Universitas Negeri Padang perlu dilakukan *Penetration Testing* untuk dapat mengetahui apakah ada serangan yang terjadi serta dapat melemahkan suatu sisi pada *web server*, dalam tujuan memudahkan pengelola e-learning dalam mengamankan data *users.*

P-ISSN: 2302-3295

II. METODE

Penetration Testing Execution Standart (PTES) merupakan penyedia servis keamanan menggunakan bahasa yang umum dengan cakupan yang dalam. Pada Gambar 2 dibawah ini ada 7 tahapan dalam melakukan *penetration testing* yaitu[3] :



Gambar 2. Tahapan PTES

1. ***Pre-Engagement Interaction*** memiliki tujuan untuk menyajikan dan menjelaskan alat da teknik yang tersedia dapat membantu langkah pre-engagement yang berhasil dari uji penetrasi. Dokumen yang terpenting adalah Izin untuk menguji.

2. ***Intelegence Gathering*** adalah melakukan pengumpulan informasi untuk digunakan dalam melakukan uji penetrasi. Informasi umum yang perlu didapatkan adalah informasi domain, IP address, host.

3. ***Threat Modelling*** adalaah bagian pendekatan pemodelan ancaman yang diperlukan untuk pelaksanaan pengujian penetrasi yang benar.

4. ***Vulnerabillity Testing*** adalah pengujian kerentanan yang memiliki proses menemukan kelemahan dalam sistem dan aplikasi yang dapat dimanfaatkan oleh penyerang. Pada kerentanan ini akan didapatkan seperti dari kesalahan konfigurasi host dan layanan, atau desain aplikasi yang tidak aman.

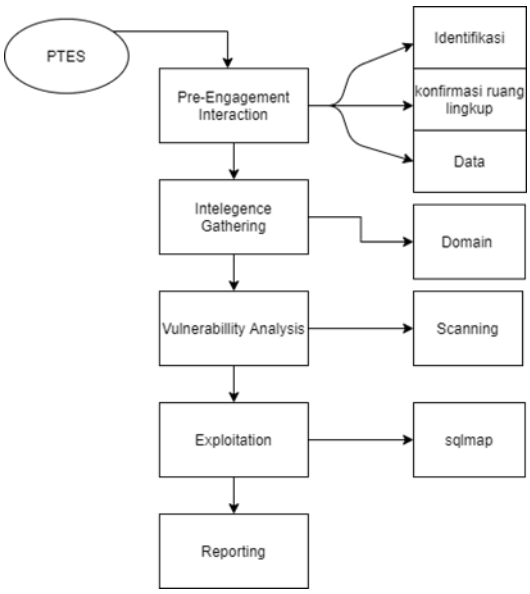
5. ***Exploitation*** adalah fase dari uji penetrasi yang berfokus pada penetapan akses ke sistem atau sumber daya dengan melewati batasan keamanan. Fokusnya pada mengidentifikasi titik masuk utama kedalam organisasi dan untuk mengidentifikasi target yang cukup memiliki nilai yang tinggi.

6. ***Post Exploitation*** mempunyai tujuan utuk menentukan nilai dari sistem guna untuk mempertahankan kontrol dari suatu sistem.

7. ***Reporting*** adalah langkah untuk menuliskan laporan yang mendiskripsikan hasil lengkap pengujian dan presentasi yang sudah dipersiapkan dengan rekomendasi dan penyelesaiannya.

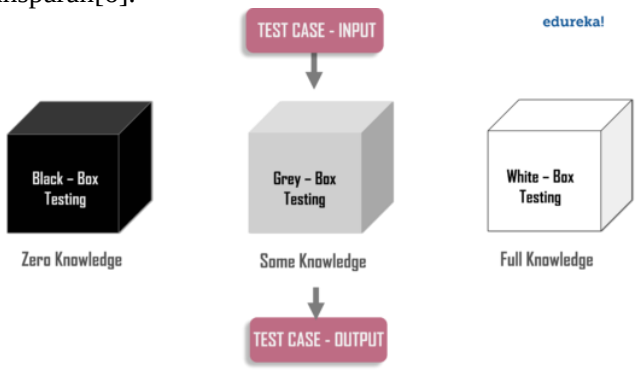
Penelitian ini menggunakan pendekatan kuantitatif dengan penelitian deskriptif[4]. Objek penelitian yaitu *E-learning* Universitas Negeri Padang. Lokasi penelitian ini dilakukan di UPT. PTIK Universitas Negeri Padang di Gedung ex Rektorat.

Variabel yang akan diuji pada Gambar 3. dibawah yaitu *PenetrationTesting* dengan tahapan sebagai berikut: 1. *Pre-engagement Interaction* (a. Identifikasi; b. Konfirmasi; c. Pengambilan Data) 2. *Intelegence Gathering* (menggunakan *tool* seperti *whois* dan *zenmap*) 3. *Vulnerabillity Analysis* (*Scanning* menggunakan *Acunetix*) 4. *Exploitation* (menggunakan *Sqlmap*) 5. *Reporting*[5].



Gambar 3. Kerangka berpikir PTES

Ada tiga strategi penetration testing seperti yang terlihat pada Gambar 4 yaitu *Black Box, Grey Box, dan White Box*. Penelitian ini dilakukan dengan menggunakan stetegi *White Box* Testing yaitu dimana penguji memiliki akses untuk mendapatkan semua informasi yang dibutuhkan dengan transparan[6].



Gambar 4. Strategi *penetration testing*

III. HASIL DAN PEMBAHASAN

1. Pre-Engagement Interaction

Tujuan dari tahapan ini adalah penyajian dan penjelasan alat beserta teknik yang akan dilakukan kepada pihak yang akan di pentest. Salah satu dokumen penting yag harus dimiliki adalah izin untuk melakukan penetrasi. Dan izin penelitian sudah didapatkan melalui BAK Universitas Negeri Padang yang ditanda tangani oleh Wakil Rektor I setelah itu baru ke UPT-PTIK Universitas Negeri Padang.

2. Intelegence Gathering

Tahapan *Intelegence Gathering* ini yang dilakukan pertama kali adalah pengecekan informasi Domain dari elearning2.unp.ac.id menggunakan *whois lookup*. Dalam pencarian informasi ini hanya menggunakan domain yaitu "***elearning.unp.ac.id***" informasi tersebut dapat dilihat pada Gambar 5. sebagai berikut :

Gambar 5. Whois lookup *elearning2.unp.ac.id*

Tabel 1. Hasil whois lookup

elearning2.unp.ac.id	
Domain ID	PANDI-DO152191
Domain Name	unp.ac.id
Created On	16/10/2001 13.32
Last Update On	17/09/2018 11.12
Expiration Date	31/10/2021 23.59
Status	ok

Mengacu pada hasil pencarian informasi domain pada Gambar 5 diatas, dapat dilihat lebih jelas pada Tabel 1. Hasil Whois Lookup dimana setelah pegecekan informasi domain, langkah selanjutya adalah pengecekan jaringan atau yang akan digunakan yaitu Nmap (*network mapper*) yang merupakan tool untuk eksplorasi jaringan yang dapat dilihat pada Tabel 2. Zenmap *elearning2.unp.ac.id* dibawah :

P-ISSN: 2302-3295

Tabel 2. Zenmap elearning2.unp.ac.id

elearning2.unp.ac.id		
Port	Status	Services
22	Open	ssh
53	Open	domain
80	Open	http
111	Open	rpcbind
443	Open	ssl/http
2049	Open	nfs_acl

3. Vulnerability Analysis

Tahapan ke tiga proses yang akan dilakukan adalah *Scanning* terhadap *elearning2.unp.ac.id*. Pada proses scanning ini bertujuan untuk menemukan kelemahan yang ada dalam sistem dengan menggunakan *Acunetix Web Vulnerability Scanner* (AVWS). Berikut Tabel 3 hasil dari scanning menggunakan AWVS :

Tabel 3. Hasil scaning dengan *Acunetix Web Vulnerability Scanner* (AWVS).

Celah	Jumlah	Level Alert
Development configuration file	5	Medium
HTML form without CSRF protection	75	Medium
Slow HTTP Denial of Service Attack	1	Medium
TLS 1.0 enabled	1	Medium
Cookie(s) without HttpOnly flag set	1	Low
Documentation file	5	Low
Login page password-guessing attack	1	Low
Possible sensitive directories	1	Low
Content Security Policy (CSP) not implemented	1	Informational
Content type is not specified	2	Informational
Password type input with auto-complete enabled	1	Informational
TLS 1.1 enabled	1	Informational

Pengujian scanning ini didapatkan lima peringatan teratas diantaranya :

a. *HTML without Cross-site Request Forgery* (CSRF/XSRF) protection. CSRF adalah kerentanan dimana penyerang dapat mempengaruhi pengguna seperti admin dari sistem. Serangan CSRF ini secara khusus menargetkan request data, bukan pada pencuria data. Idealnya penyerangan CSRF ini mengganggu integritas sesi pengguna dengan website melalui memasukkan network request lewat browser user. Rekomendasi untuk mengatasi serangan ini adalah dengan membuatkan sebuah token CSRF yang diharapkan mempu mengatasi bentuk penyerangan ini.

b. *Development configuration file* dapat memperlihatkan informasi sesitif yangn dapat membantu penyerang untuk mempersiapkan serangan yang lebih lanjut. Pada peringatan ini sebaiknya dihapus atau dibatasi akses kedalam file ini dari sistem.

c. *Slow HTTP Denial of Service Attack* pada jenis serangan ini server *elearning2.unp* cukup rentan. Serangan ini bergantung pada HTTP yang membutuhkan permintaan untuk diterima sepenuhnya oleh server sebelum diproses.

d. *Weak password (login page password-guessing attack)* adalah penyerang dapat mencoba menemukan kata sandi yang lemah dengan cara sistematis mencoba setiap kemungkinan kombinasi huruf, angka, simbol hinggamenemukan suatu kombinasi benar yang berfungsi. Pada jenis serangan ini direkomendasikan agar menerapkan beberapa jenis penguncian akun setelah sejumlah percobaan sandi yang salah.

e. *TLS 1.0 Enable* adalah *Transport Layer Security* yang mengamankan privasi data. TLS 1.0 tidak dianggap sebagai "kriptografi kuat" seperti yang didefinisikan dan diharuskan oleh Standar Keamanan Data PCI 3.2. bila digunakan

untuk melindungi informasi sensitif yang ditransfer ke atau dari situs web. Yang harus dilakukan dalam peringatan ini adalah untuk menonaktifkan SSL/TLS awal dan menerapkan protokol enkripsi yang lebih aman –TLS 1.1 atau lebih tinggi (TLS v1.2 sangat disarankan)

Tahap *exploitation* ini menggunakan teknik *SQL Injection* dengan menggunakan *toll SQLMap* yang dinyatakan gagal karena website sudah menggunakan keamanan SSL (Secure Socket Layer) yang mana tidak ada celah keamanan yang menyulitkan penyerang masuk kepada sistem database web tersebut terlihat pada Gambar 6 dibawah :

4. Exploitation

Gambar 6. SQLMap

5. Reporting

Pada tahapan ini penulis akan memberikan Top Vulnerabilities yang dilakukan dengan Acunetix Web Vulnerability Analysis yaitu : *HTML form without CSRF Protection, development configuration file, Slow HTTP Denial of Service Attack,* dan *TLS 1.0 Enable.* Berdasarkan dari hasil yang telah dilakukan, maka dapat disimpulkan dengan *Acunetix Threat Level 2 "Medium".* Pada exploitation tidak bisa dilanjutkan karena *elearning2.unp.ac.id* telah menggunakan keamanan jenis SSL (*Secure Socket Layer*).

IV. KESIMPULAN

Pengujian menggunakan metode Penetration Testing pada E-learning Universitas Negeri Padang ini disimpulkan bahwa website *elearning2.unp.ac.id* terdapat celah keamanan Lever 2 yaitu level Medium. Sehingga serangan yang terjadi tidak terlalu berpengaruh terhadap website. Dan pada exploitation menggunakan SQL Injecton gagal karena website sudah meingkatkan keamanan menggunakan SSL (Secure Socket Layer).

V. SARAN

Untuk pengujian selanjutnya diharapkan menggunakan Framework yang berbeda seperti ISSAF *(Information System Security Assesment Framework),* atau OWASP (*The Open Web Application Security Project)*. Untuk pengelola dan pengembang elearning.unp diharapkan dapat mempertahankan keamanan serta meningkatkan ke jenjang yang lebih tinggi, agar users tidak khawatir akan serangan yang akan datang nantinya.

UCAPAN TERIMA KASIH

Terimakasih kepada bapak Mohamad Amin selaku pengelola dan pegembang website *elearning2.unp.ac.id* yang telah memberikan izin untuk melakukan uji penetrasi pada E-learning UNP.

P-ISSN: 2302-3295

DAFTAR PUSTAKA

[1]. Hendriyani, Y., & Effendi, H. (2018). Persepsi Mahasiswa terhadap Penggunaan E-Learning dalam Pembelajaran Bahasa Pemograman di Fakultas Teknik UNP.

[2]. Patrick Engebretson, 2010. The Basic of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, Elsevier

[3]. Syarif, T. R. (2019). *Analisis Perbandingan Metode Web Security Ptes, Issaf Dan Owasp Di Dinas Komunikasi Dan Informasi Kota* (Doctoral dissertation, Universitas Komputer Indonesia).

[4]. Sudaryono. 2017. *Metodologi Penelitian*. Jakarta: PT Raja Grafindo Persada

[5]. *The PTES Team, February 08, 2017. The Penetration Testing Execution Standard Documentation*

[6]. A. Choudary, *What is Penetration Testing – Methodologies amd Tools*, 2020, website : https://www.edureka.co/blog/what-is-penetration-testing/ ,
diakses tanggal 12 Desember 2020.