TUGAS AKHIR

PENGUJIAN PENETRASI CELAH KEAMANAN PADA APLIKASI WEB *E-LEARNING* MENGGUNAKAN METODE OWASP *TESTING GUIDE*

(Studi Kasus : elearningft.unpas.ac.id)

Untuk Penyusunan Kelengkapan Tugas Akhir
Program Studi Teknik Informatika Universitas Pasundan

Disusun Oleh :

Rezki Jabbar Mulia

NRP. 17.304.0018

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS PASUNDAN

OKTOBER 2022

UNIVERSITAS
PASUNDAN

LEMBAR PENGESAHAN
LAPORAN TUGAS AKHIR

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung,Pada hari, Kamis, 29 September 2022, tugas akhir dari:

Nama : Rezki Jabbar Mulia

NRP : 173040018

Dengan Judul:

"PENGUJIAN PENETRASI CELAH KEAMANAN
PADA APLIKASI WEB E-LEARNING
MENGGUNAKAN METODE OWASP TESTING GUIDE
(Studi Kasus : elearningft.unpas.ac.id)

Bandung, 29 September 2022
Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
(Doddy Ferdiansyah, S.T, M.T)	(Miftahul Fadli Muttaqin, S.T.,M.T)

ABSTRAK

Aplikasi web adalah sekumpulan halaman pada suatu *domain* pada internet atau *intra network* yang dibuat dengan berbagai tujuan dan dapat di akses secara luas melalui halaman *index* atau halaman utama yang menggunakan URL dalam aplikasi web. *E-learning* adalah sebuah metode pembelajaran yang menggunakan teknologi digital yang banyak di pakai oleh instansi pendidikan.

Penelitian ini dilakukan untuk melakukan evaluasi melalui pengujian penetrasi celah keamanan terhadap aplikasi web dengan tujuan mencari atau menemukan celah keamanan aplikasi web. Penelitian ini dilakukan dengan mengumpulkan informasi melalui pendeteksian aplikasi web, melakukan analisis celah keamanan dan mengeksploitasi aplikasi web terhadap celah keamanan yang ditemukan serta membuat laporan hasil pengujian penetrasi yang telah dilakukan.

Hasil akhir penelitian ini adalah dokumen hasil pengujian penetrasi aplikasi web yang dapat digunakan untuk meningkatkan sisi keamanan aplikasi web.

Kata kunci: Internet, aplikasi web, *penetration testing*, celah keamanan, OWASP *Testing Guide*

ABSTRACT

Web application is a bunch of pages on a domain of the internet or intra-network that created for many purposes and can widely accessing by way of index or or main page that uses an URL on web application. E-Learning is a learning method that uses digital technology that widely used by educational institutions.

The research are conducted to evaluate by penetration testing of vurnabilites security of web application with reconnaissance by web application, analyzing security gaps and exploiting web applications for vulnerabilities security and reporting the results of penetration testing that had been obtained.

The final results of the research is a web application penetration testing with result is a document that can be used to improve the security of web applications.

Keywords**:** *Internet, web applications, penetration testing, security holes,* OWASP *Testing Guide*

UNIVERSITAS
PASUNDAN

DAFTAR ISI

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Internet adalah suatu jaringan komunkasi yang bersifat global dan terbuka yang memiliki fungsi untuk menghubungkan antara media elektronik dengan media elektronik yang lain. Sehingga kebutuhan dalam berkomunkasi, bertukar informasi ataupun mencari informasi dapat lebih mudah didapat oleh siapapun dan kapanpun. Penggunaan internet dewasa ini semakin berkembang, internet merupakan titik singgung antara dunia fisik dan dunia maya ini semakin banyak pengunjungnya. Statistik terakhir memperhatikan bahwa penetrasi internet pada tahun 2022 awal telah mencapai kurang lebih 66.2% dari total 7,934 miliyar penduduk bumi.

WORLD INTERNET USAGE AND POPULATION STATISTICS
2022 Year-Q1 Estimates

World Regions	Population (2022 Est.)	Population % of World	Internet Users 31 Dec 2021	Penetration Rate (% Pop.)	Growth 2000-2022	Internet World %
Africa	1,394,588,547	17.6 %	601,327,461	43.1 %	13,220 %	11.5 %
Asia	4,350,826,899	54.8 %	2,790,150,527	64.1 %	2,341 %	53.1 %
Europe	841,319,704	10.6 %	743,602,636	88.4 %	608 %	14.2 %
Latin America / Carib.	663,520,324	8.4 %	533,171,730	80.4 %	2,851 %	10.1 %
North America	372,555,585	4.7 %	347,916,694	93.4 %	222 %	6.6 %
Middle East	268,302,801	3.4 %	205,019,130	76.4 %	6,141 %	3.9 %
Oceania / Australia	43,602,955	0.5 %	30,549,185	70.1 %	301 %	0.6 %
WORLD TOTAL	7,934,716,815	100.0 %	5,251,737,363	66.2 %	1,355 %	100.0 %

Gambar 1. 1 Statistik Pengguna Internet Pada Tahun 2022 (Sumber: internetworldstats.com/stats.html)

Asumsinya adalah bahwa satu dari lima individu di dunia ini adalah pengguna internet Berikut dengan ancaman yang berada, menurut BSSN (Badan Siber Sandi Negara) pada semester awal tahun 2021 Indonesia memiliki 741 miliyar anomali trafik/serangan siber dengan serangan yang terbanyak yaitu adalah *malware*.

Gambar 1. 2 Infografis Serangan Siber Pada Awal Tahun 2021 di Indonesia (Gambar: BSSN)

E-learning adalah sebuah metode pembelajaran yang menggunakan teknologi digital yang banyak di pakai oleh instansi pendidikan sebagai proses pembelajaran jarak jauh yang dipadukan antara prinsip pembelajaran dan teknologi. Perkembangan *e-learning* yang sangat pesat dari tahun 1837 hingga 2020 yang awalnya hanya sebagai *Phonographical Correspondence Society* yang hanya berupa kaset dapat diputar sebentar hingga dapat menjadi interaktif dan juga kolaboratif.

Universitas Pasundan Fakultas Teknik merupakan instansi pendidikan yang menggunakan aplikasi *website e-learning* yang digunakan untuk kegiatan belajar mengajar atau kuliah secara daring. Menurut SK Rektor Nomor 131/Unpas.R/SK/C/VIII/2020 tentang Pembelajaran Daring. Moodle adalah sebuah platform pembelajaran atau *Learning Management* System (LMS) yang digunakan oleh elearningft, elearning sendiri terdapat Moodle versi 3.9. Penggunaan elearningft pun sampai saat ini belum ada pengujian dari sisi celah keamanan untuk melindungi aset dan juga informasi penting yang berada di dalam web aplikasi tersebut. Ancaman pada *e-learning* pada umumnya memiliki 3 hal, yaitu; kerentanan privasi pengguna, kerentanan konten, dan kerentanan pada *website*. Berikut untuk gambar tipe serangan pada sistem *e-learning*:

Serangan Aktif		Serangan Pasif	
Integrity	*Authentication*	*Availability*	*Confidentiality*
Malicious code attack	*Brute force attacks*	*Denial-of-service*	*Group session eavesdropping*
Message injection	*Dictionary attack*	*Node attacks*	*Group session traffic analysis*
Traffic modification	*Login spoofing attacks*	*Link attacks*	*Group identity disclosure*
Traffic deletion	*Key management attacks*	*Network attacks*	
Traffic rerouting	*Replay attacks*		
Traffic misdelivery-rerouti	*Man-in-middle attacks*		
Forgery attacks	*Session hijacking attacks*		
Stack overflow attacks	*Non-repudiation attacks*		

Gambar 1. 3 Serangan Aktif dan Pasif Pada *e-learning*

Open Web Application Security Project atau akronimnya sebagai OWASP merupakan organisasi nirbala di Amerika Serikat yang resmi secara daring pada bulan Desember 2001. OWASP adalah komunitas terbuka yang di dedikasikan untuk memungkinkan organisasi memahami, mengembangkan, memperoleh mengoperasikan, dan memelihara aplikasi yang dapat dipercaya dari aspek keamanan.(Dwi Sumarwo, Kemendikbud)

Berdasarkan latar belakang diatas maka penulis mengajukan penulisan tugas akhir dengan melakukan pengujian keamanan pada aplikasi web elearningft berdasarkan celah keamanan yang di temukan oleh penulis dan menggunakan metode OWASP *Testing Guide*. Hasil dari penulisan ini diharapkan sebagai langkah preventif untuk menjadi mitigasi dan pertimbangan dari sisi keamanan pada aplikasi web sehingga mengurangi terjadinya eksploitasi oleh pihak yang tidak bertanggung jawab.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang sebelumnya dipaparkan, maka permasalahan yang memuat pada penelitian ini adalah:

1) Belum adanya pengujian celah keamanan.

2) Faktor-faktor celah keamanan apa saja yang bisa menjadi risiko aplikasi web elearningft.

1.3 Tujuan Penelitian

Berikut tujuan yang di teliti dalam penelitian sebagai berikut :

1) Melakukan pengujian celah keamanan terhadap aplikasi web elearningft menggunakan metode OWASP *Testing Guide* dan diharapkan sebagai acuan dalam memperbaiki keamanan aplikasi web.

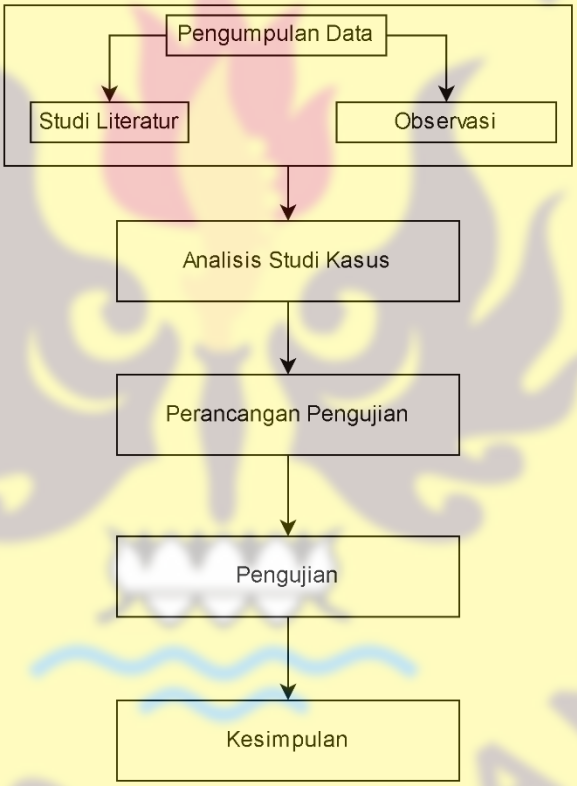
1.4 Lingkup Tugas Akhir

Berikut lingkup penyelesaian penelitian tugas akhi sebagai berikut :

1) Pengujian yang dilakukan pada aplikasi web menggunakan jenis pengujian *Grey Box Testing*.
2) Pengujian yang dilakukan menggunakan metode OWASP Testing Guide versi 4.0.
3) Pengujian hanya berupa saran dan tidak melakukan perbaikan.

1.5 Metodologi Tugas Akhir

Bagian ini menjelaskan bagaimana alur-alur metodologi penyelesaian yang dilakukan oleh penulis dalam menyelesaikan tugas akhir.



Gambar 1. 4 Metodologi Tugas Akhir

Berdasarkan gambar . Tahapan Penelitian dapat dilihat bahwa didalam penelitian tugas akhir ini dibutuhkan berberapa alur-alur penunjang. Berikut rincian dari metodologi tugas akhir, yaitu :

1. Pengumpulan Data

Pada tahap ini dilakukan pengumpulan data yang relevan dan teoritis.

a) Studi Literatur

Studi Literatur digunakan sebagai preferensi dan membantu mengumpulkan informasi-informasi yang relevan terhadap topik yang dibahas.

b) Observasi

Pada tahap ini melihat dan menjinjau perilaku dari web aplikasi dan di implementasikan dengan penulisan. yang dilakukan di Fakultas Teknik Universitas Pasundan.

2. Analisis Studi Kasus

Pada tahap ini dilakukan analisis menggunakan metode OWASP *Testing Guide* yaitu *Testing for Reflected Cross-site Scripting*(OTG-INPVAL-001), *Testing for Stored Cross-site Scripting*(OTG-INPVAL-002), *Testing for Session Management Schema*(OTG-SESS-001), *Testing for Session Fixation*(OTG-SESS-003),dan *Testing for Session Hijacking*(WTSG-SESS-09).

3. Perancangan Pengujian

Pada tahap ini dilakukan perancangan skema pengujian setelah analisis dengan menggunakan OWASP *Testing Guide* versi 4.0

4. Pengujian Sistem

Pada tahap ini melakukan pengujian keamanan informasi menggunakan standar OWASP *Testing Guide* versi 4.0 yang menghasilkan hasil pengujian.

5. Kesimpulan dan Saran

Tahap ini penulis menyimpulkan dari penelitian yang telah dilaksanakan dengan membuat poin-poin dengan masalah dari keseluruhan pengolahan data yang sudah di identifikasi, serta saran sebagai prospek penelitian lainnya.

1.6 Sistematika Penulisan Tugas Akhir

Dalam penulisan penelitian tugas akhir ini terdapat berberapa bab yang menjelaskan secara sistemastis mengenai penelitian tugas akhir secara rinci dan keterkaitan di setiap bab antara sesudah dan sebelumnya. Adapun sistematika penulisan dijelaskan sebagai berikut:

BAB 1. PENDAHULUAN

Bab ini penjelasan penulisan secara umum mengenai usulan penelitian yang akan dilakukan dalam pengerjaan tugas akhir. Berisi tentang latar belakang, identifikasi masalah, tujuan penelitian, lingkup tugas akhir, dan metodologi tugas akhir.

BAB 2. LANDASAN TEORI DAN PENELITIAN TERDAHULU

Bab ini berisi definisi, teori-teori serta konsep yang diperlukan dalam pengerjaan tugas akhir. Bab ini juga membahas mengenai jurnal-jurnal ilmiah terdahulu yang memiliki kemiripan dengan tugas akhir yang dikerjakan.

BAB 3. SKEMA PENELITIAN

Bab ini berisi penjelasan alur penyelesaian tugas akhir, analisis persoalan dan manfaat tugas akhir, kerangka pemikiran teoritis, dan profile tempat penelitian.

BAB 4. ANALISIS CELAH KEAMANAN

Bab ini berisi tahapan dalam tahapan analisis aplikasi web elearningft dengan mengumpulkan informasi-informasi proses bisnis dan sistem dari aplikasi web elearningft serta mencari celah keamanan pada aplikasi web dengan menggunakan *tools* yang ditentukan.

BAB 5. EVALUASI DAN REKOMENDASI

Bab ini menjelaskan tentang saran dan rekomendasi setelah pengujian telah dilakukan pada aplikasi web elearningft dan melakukan pengujian dengan metode OWASP *Testing Guide* dengan menggunakan *tools* yang bertujuan untuk mengetahui apakah aplikasi web elearningft rentan terhadap serangan.

BAB 6. PENUTUP

Bab ini berisi mengenai hasil penelitian serta pernyataan yang didapat berdasarkan identifikasi masalah yang dikemukakan, serta keterkaitan dari semua tahap yang dilakukan dalam penelitian. Di dalamnya terdapat pula saran yang diusulkan untuk penelitian selanjutnya terkait dengan prospek penelitian selanjutnya, serta rekomendasi penerapan di perusahaan terkait.

UNIVERSITAS
PASUNDAN

DAFTAR PUSTAKA

[ALD18] Aldo Karendra, Khoirusy Syafaat, "Audit Dan Optimalisasi Keamanan Website Pada Universitas Muhammadiyah Palembang", STMIK Palcomtech, 2018

[BAG20] Bagus Wicaksono, "Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik Penetration Testing Dan Dast (Dynamic Application Security Testing)", Institut Sains & Teknologi AKPRIND Yogyakarta, 2020

[BUD17] Budi Rahadjo. "Keamanan Informasi", PT Insan Infonesia, 2017.

[BRY91] Bryan C. William, "Manual Book Moodle for Teachers, Trainers and Administrator", Free Software Fundation. Inc. 1991

[CIO12] Ciobanu (Defta) Costinela – Lumini & Ciobanu (Iacob) Nicoleta – Magdalena. "E-learning Security Vulnerabilities", Elsavier Ltd, 2012

[COM04] Common Vurnablities Exposure, "Moodle", tersedia Juni 2004, www.cvedetails.com/product/3590/Moodle-Moodle.html?vendor_id=2105 , diakses 15 Juni 2022

[COM06] Common Weakness Enumeration, "CWE-79", tersedia Juni 2006, cwe.mitre.org/data/definitions/79.html, diakses pada 29 juli 2022

[DAM16] Damiano Distante, "The Architecture of the Moodle" tersedia Januarai 2016, researchgate.net/figure/The-architecture-of-the-TUT-LA-Moodle-plug-in_fig11_289556424, diakses pada 17 September 2022

[DEV22] Developer Mozilla, "Element.innerHTML", tersedia September 2022, developer.mozilla.org/en-US/docs/Web/API/Element/innerHTML, diakses 16 September 2022

[DWI19] Dwi Sumarwanto, "Penggunaan OWASP 4 Sebagai Standar Pengujian Kerentanan Keamanan Aplikasi Berbasis Web", tersedia Maret 2019 , solmet.kemdikbud.go.id/?p=3098 , diakses 26 Mei 2022

[FIR20] Firman Nugraha, Dedi Restendi, Agus Triyanto. "Pengembangan Sistem Pelatihan Jarak Jauh Berbasis Moodle Di Balai Diklat Keagamaan Bandung", Andragogi: Jurnal Diklat Teknis Pendidikan dan Keagamaan, 2020

[GIT22] Git Moodle, "Moodle Official Production Repository", tersedia 30 September 2022, git.moodle.org/gw?p=moodle.git;a=summary, diakses 15 Agustus 2022

[GUP20] Brij B. Gupta, "Cross-Site Scripting Attacks Classification, Attack, and Countermeassures", CRC Press, 2020

[HEG18] Hegi Septiyanto Wibowo. "Evaluasi Celah Keamanan Pada Website P3gl Dengan Penetration Testing Dan Berdasarkan Owasp Top-10 2017 (Studi Kasus: Pusat Penelitian Dan Pengembangan Geologi Kelautan)", Universitas Pasundan, 2018

[HOA21] Hoang Kein, "CVE-2020-25627", Tersedia Juni 2021, github.com/HoangKien1020/CVE-2020-25627, diakses 31 Agustus 2022

[IPG19] IP Geolocation, "elearningft.unpas.ac.id", tersedia 03 Maret 2019, ipgeolocation.io/ip-location/elearningft.unpas.ac.id, diakses pada 25 Juni 2022

[INT22] Internet Worlds Stats, "Usage and Population Statistics" Tersedia Juni 2022 www.internetworldstats.com/stats.htm , Juli 2022, Diakses 28 Mei 2022

[MAT14] Andrew Muller, "OWASP *Testing Guide* v4", The OWASP Foundation, 2014

[MIC20] Michael Hawkins, "Security announcements
MSA-20-0011: Stored XSS via moodlenetprofile parameter in user profile", tersedia 21 September 2020, moodle.org/mod/forum/discuss.php?d=410839 , diakses 30 Juni 2022

[QAT22] Qatros Teknologi Nusantara, "Apa Itu Pentest Part 1" Tersedia 12 Januari 2022, qatros.com/blog/blog-technology-1/post/apa-itu-pentest-penetration-test-part-1-24, diakses pada 16 Juni 2022

[REZ20] Reza Pramudita, Syifaul Fuada, Nuur Wachid Abdul Majid. "Studi Pustaka Tentang Kerentanan Keamanan E-Learning dan Penanganannya". Universitas Budidarma, 2020

[RIC11] Richardus Eko Indrajit. "Pengantar Konsep Keamanan Informasi di Dunia Siber", APTIKOM, 2011
Tim Hunt, "What is the structure of Moodle site?", tersedia Febuari 2009, moodle.org/mod/forum/discuss.php?d=115620&lang=et, diakses pada 17 September 2022

[THO22] Thomas Hamilton, "What is Grey Box Testing? Techniques, Example", tersedia 03 September 2022, guru99.com/grey-box-testing.html, diakses 9 Agustus 2022

[ZAP22] ZAP Dev Team, "Alerts", tersedia Juli 2022, www.zaproxy.org/docs/desktop/start/features/alerts/, diakses pada 20 September 2022