PENETRATION TESTING TERHADAP *WEBSITE* UNIVERSITAS PASUNDAN DENGAN METODE ZERO ENTRY HACKING (STUDI KASUS: http://www.unpas.ac.id)

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan
Program Strata 1, Program Studi Teknik Informatika,
Universitas Pasundan Bandung

oleh :

Oman Gunawan
NRP : 16.304.0111

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
AGUSTUS 2022

LEMBAR PENGESAHAN

LAPORAN TUGAS AKHIR

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari senin 22 Agustus 2022, tugas akhir dari :

Nama : Oman Gunawan Nrp

: 16.304.0111

Dengan judul :

"*PENETRATION TESTING* TERHADAP *WEBSITE* UNIVERSITAS PASUNDAN DENGAN METODE ZERO ENTRY HACKING (STUDI KASUS: http://www.unpas.ac.id)"

Menyetujui,

Bandung, 22 Agustus 2022

Pembimbing Utama,

(Doddy Ferdiansyah, S.T., M.T)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa :

1. Tugas akhir ini adalah benar-benar asli dan belum pernah diajukan untuk mendapatkan gelar akademik, baik di Universitas Pasundan Bandung maupun di Perguruan Tinggi lainnya
2. Tugas akhir ini merupakan gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain kecuali arahan dari tim Dosen Pembimbing
3. Dalam tugas akhir ini tidak terdapat karya atau pendapat orang lain, kecuali bagian-bagian tertentu dalam penulisan laporan Tugas akhir yang saya kutip dari hasil karya orang lain telah dituliskan dalam sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulisan karya ilmiah, serta disebutkan dalam Daftar Pustaka pada tugas akhir ini
4. Kakas, perangkat lunak, dan alat bantu kerja lainnya yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab saya, bukan tanggung jawab Universitas Pasundan Bandung

Apabila di kemudian hari ditemukan seluruh atau sebagian laporan tugas akhir ini bukan hasil karya saya sendiri atau adanya plagiasi dalam bagian-bagian tertentu, saya bersedia menerima sangsi akademik, termasuk pencabutan gelar akademik yang saya sandang sesuai dengan norma yang berlaku di Universitas Pasundan, serta perundang-undangan lainnya

Bandung, 22 Agustus 2022

Yang membuat pernyataan,

Oman Gunawan

NRP. 16.304.0111

ABSTRAK

Dunia siber di Indonesia sering terjadi serangan dari sumber yang tercatat atau bisa dari luar negeri yang menjadikan sumber serangan itu selaku pijakan untuk mencari kerentanan pada suatu platform. Metode penyerangan siber menggunakan *malware* tercatat paling banyak digunakan didunia, hackmagedon mencatat 39% dari distribusi teratas serangan siber dunia merupakan serangan menggunakan *malware* sehingga menduduki peringkat pertama dalam serangan siber secara global. Meskipun penyerang lebih sering melakukan penyerangan kepada Lembaga Pemerintahaan, Keuangan dan Berita, bukan berarti lembaga pendidikan seperti Universitas Pasundan menjadi aman dari serangan siber. Tujuan penelitian ini adalah untuk membantu meningkatkan sistem keamanan situs web Universitas Pasundan salah satu cara yang dilakukan adalah menggunakan metode *Penetration Testing*.

Penelitian dilakukan dengan 4 tahap pengujian yaitu: Pengintaian Sistem digunakan untuk mengumpulkan informasi sebanyak-banyaknya mengenai situs web yang diteliti, Pemindaian dilakukan untuk mencari kelemahan pada target yang diteliti, Eksploitasi celah keamanan mengacu pada standar keamanan OWASP Top 10 untuk membantu dalam memastikan ada atau tidaknya celah keamanan. dan Pada tahap terakhir yaitu menuliskan laporan mengenai hasil dari pengujian tersebut.

Hasil akhir dan kesimpulan yang dapat diambil dari penelitian ini berupa laporan celah keamanan yang berisi daftar kelemahan yang dimiliki oleh situs web Universitas Pasundan, sehingga pengelola dapat meningkatkan keamanan agar meminimalisir penyerangan dari peretas yang tidak bertanggung jawab.

Kata Kunci : Serangan siber, Situs Web, OWASP Top 10, Uji Penetrasi.

ABSTRACT

The cyber world in Indonesia often experiences attacks from recorded sources or can be from abroad, which makes the source of the attack a stepping stone to find vulnerabilities on a platform. The method of cyber-attack using malware is recorded as the most widely used in the world, hackmagedon noted that 39% of the top distribution of cyber-attacks in the world were attacks using malware so that it was ranked first in cyber-attacks globally. Although attackers often attack Government, Finance and News Institutions, it does not mean that educational institutions such as Pasundan University are safe from cyber attacks. The purpose of this study is to help improve the security system of the Pasundan University website. One way to do this is to use the Penetration Testing method.

The study was conducted with 4 testing stages, namely: System Reconnaissance is used to collect as much information as possible about the website under study, Scanning is carried out to find weaknesses in the target being studied, Exploitation of security holes refers to OWASP Top 10 security standards to assist in ascertaining whether or not there are any security gaps. and At the last stage, namely writing a report on the results of the test.

The final results and conclusions that can be drawn from this research are in the form of a security vulnerability report that lists the weaknesses of the Pasundan University website, so that managers can improve security in order to minimize attacks from irresponsible hackers.
Keywords: Cyber attack, Website, OWASP Top 10, Penetration Testing.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah subhanahu wa ta'ala, karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan tugas akhir dengan judul "*Penetration Testing* Terhadap *Website* Universitas Pasundan Dengan Metode Zero Entry Hacking (Studi Kasus: http://www.unpas.ac.id)". Adapun maksud dan tujuan dari penulisan tugas akhir ini adalah untuk memenuhi salah satu syarat untuk kelulusan Program Strata 1, Program Studi Teknik Informatika, Fakultas Teknik Universitas Pasundan.

Selama penulisan dan penelitian tugas akhir ini banyak sekali hambatan yang penulis alami, namun berkat bantuan, dorongan serta bimbingan dari berbagai pihak, tugas akhir ini dapat terselesaikan dengan baik. Maka pada kesempatan ini penulis menyampaikan ucapan terima kasih yang setulus-tulusnya kepada :

1. Kepada kedua orang tua yang selalu saya hormati, sayangi, dan banggakan, Almarhum Bapak Uwar Suwardi dan Ibu Anyi, serta kakak-kakak saya Asep Ramdani, Titi Mariah, Irmayanti, Toto, serta adik saya Melisa Silvi Yanti, serta seluruh keluarga yang telah memberikan motivasi serta do'anya dalam pembuatan tugas akhir ini.
2. Kepada Dosen Wali, Bapak Fajar Darmawan, S.T., M.Kom., yang telah membimbing penulis ketika masa perkulihahan hingga menjelang akhir masa studi.
3. Kepada Pembimbing, Bapak Doddy Ferdiansyah, S.T., M.T., yang selalu membimbing penulis sehingga laporan tugas akhir ini dapat diselesaikan.
4. Kepada dosen penguji, Bapak Sali Alas Majapahit, S.ST., M.Kom dan Bapak Miftahul Fadli Muttaqin, ST., M.T., yang telah bersedia menjadi penguji di sidang tugas akhir ini.
5. Koordinator Tugas akhir serta seluruh civitas akademika Teknik Informatika di UNIVERSITAS PASUNDAN BANDUNG, yang telah memberikan bekal ilmu selama penulis menimba ilmu.
6. Kepada teman-teman seperjuangan di Universitas Pasundan Bandung, Fajar, Irpan, Riksa, Hadi, Robi, Opik, Rizal, Thomas dan seluruh teman angkatan 2016.

Semoga kebaikan mereka mendapatkan pahala dari Allah subhanahu wa ta'ala. Penulis sadar bahwa dalam penyusunan tugas akhir ini masih jauh dari kesempurnaan. Oleh karena itu, penulis harapkan kritik dan saran dari semua pihak demi perbaikan dimasa yang akan datang. Penulis berharap tugas akhir ini bermanfaat bagi peneliti dan pihak-pihak terkait. Aamiin.

Bandung, 22 Agustus 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

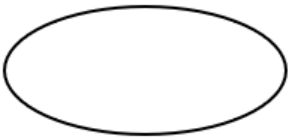
DAFTAR ISTILAH

NO	Istilah Asing	Arti
1.	Ad hoc	Sebuah istilah dari bahasa Latin yang populer dipakai dalam bidang keorganisasian atau penelitian. Istilah ini memiliki arti "dibentuk atau dimaksudkan untuk salah satu tujuan saja" atau sesuatu yang "diimprovisasi"
2.	Authorization	Proses penentuan apakah user tersebut diijinkan/ditolak untuk melakukan satu atau beberapa action atau akses terhadap resources tertentu dalam system.
3.	Blackbox	Istilah untuk pengetesan keamanan suatu jaringan atau situs web.
4.	Browser	Suatu perangkat lunak atau software yang digunakan untuk mencari informasi atau mengakses situs-situs yang ada di internet.
5.	Bug/Error	Adalah error yang menyebabkan aplikasi/software tak berjalan dengan semestinya.
6.	Cloud Computing	Merujuk pada tugas dan layanan yang disediakan atau di-hosting di internet atas dasar bayar sekali pakai.
7.	Cookie	Bagian kecil dari data yang dikirim dari sebuah situs web dan disimpan dalam komputer pengguna oleh peramban web ketika pengguna tersebut sedang membuka halaman web.
8.	Cyber	Media elektronik dalam jaringan komputer yang banyak dipakai untuk keperluan komunikasi satu arah maupun timbal-balik secara online.
9.	Database	Sekumpulan data terstruktur yang disimpan di komputer, terutama yang dapat diakses dengan berbagai cara.
10.	Delete	Dalam penggunaannya method untuk kelompok HTTP verb ini adalah untuk menghapus item/resource yang telah ada.
11.	Deserialization	Proses yang mengubah format data menjadi objek seperti klien mengirimkan permintaan sebagai format data JSON dan layanan back end mengubahnya menjadi Java Entity Class.
12.	Domain	Nama unik yang diberikan untuk mengidentifikasi nama server komputer seperti server web atau server surel di jaringan komputer ataupun internet.
13.	Email	Surat dengan format digital (ditulis dengan menggunakan komputer) dan dikirimkan melalui jaringan komputer.
14.	File	Adalah identitas dari data yang disimpan di dalam berkas sistem yang dapat diakses dan diatur oleh pengguna
15.	Firewall	Adalah suatu sistem yang dirancang untuk mencegah akses yang tidak diinginkan dari atau ke dalam suatu jaringan internal
16.	Footprinting	Teknik yang digunakan untuk mengumpulkan informasi tentang sistem komputer dan entitas di mana mereka berada.
17.	Hardware	Mesin, perkabelan, dan komponen fisik lainnya dari komputer atau sistem elektronik lainnya.
18.	Homepage	Disebut juga dengan beranda merupakan suatu halaman utama atau halaman pembuka yang ada dalam suatu website.
19.	Host	Komputer yang menggunakan sistem operasi multi user yang berada didalam suatu jaringan dan pemakainya dapat berkomunikasi dengan host lain didalam jaringan tersebut.
20.	Hypertext Transfer Protocol (HTTP)	protokol pada lapisan aplikasi untuk sistem informasi hypermedia yang terdistribusi dan kolaboratif.
21.	IP Address	Adalah label numerik yang ditetapkan untuk setiap perangkat yang terhubung ke jaringan komputer yang menggunakan Protokol Internet untuk komunikasi
22.	Node	Sistem atau perangkat apa pun yang dapat terhubung dengan jaringan, serta dapat menjalankan fungsi tertentu seperti membuat, menerima, atau mengirim informasi melalui saluran komunikasi.
23.	Login	Adalah proses untuk mengakses komputer dengan memasukkan identitas dari akun pengguna dan kata sandi guna mendapatkan hak akses menggunakan aplikasi.
24.	Malware	Perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya.
25.	Open Source	Adalah jenis perangkat lunak yang kode sumber-nya terbuka untuk dipelajari, diubah, ditingkatkan dan disebarluaskan
26.	Post	Dalam penggunaannya method untuk kelompok HTTP verb ini adalah untuk membuat (create) item/resource baru. Kelompok method ini biasanya tidak mengembalikan keluaran/output yang kadang disebut procedure.
27.	Put	Dalam penggunaannya method untuk kelompok HTTP verb ini adalah untuk mengupdate item/resource yang telah ada.
28.	Scanning	Teknik pemindaian untuk mendapatkan informasi spesifik secara cepat dan akurat dari sebuah aplikasi.
29.	Search Engines	Program komputer yang dirancang untuk melakukan pencarian atas berkas-berkas yang tersimpan dalam layanan www, ftp, publikasi milis, ataupun news group dalam sebuah ataupun sejumlah komputer peladen dalam suatu jaringan.

NO	Istilah Asing	Arti
30.	Social Engineering	Dalam konteks keamanan informasi, manipulasi psikologis adalah manipulasi psikologis orang untuk melakukan tindakan atau membocorkan informasi rahasia. Ini berbeda dengan rekayasa sosial dalam ilmu sosial, yang tidak berkenaan dengan pengungkapan informasi rahasia.
31.	Tools	Alat atau perangkat lunak yang bisa digunakan seseorang untuk melakukan suatu pekerjaan didalam komputer
32.	Traceroute	perintah untuk menunjukkan rute yang dilewati paket untuk mencapai tujuan.
33.	up to date	Artinya terkini
34.	User	Orang yang menggunakan komputer atau layanan jaringan. Seorang pengguna sering memiliki akun pengguna dan diidentifikasi ke sistem dengan nama pengguna
35.	Website	Satu set halaman informasi di internet tentang subjek tertentu, diterbitkan oleh satu orang atau organisasi
36.	White box	Dilakukan ketika perusahaan ingin mendeteksi kerentanan sekecil apapun di dalam sistem.

DAFTAR SIMBOL

I. Flow Direction

Nama	Simbol	Deskripsi
Connector		Menggambarkan alur dari satu proses ke proses lainnya
Input/output		Mengggambarkan sebuah input atau output yang saling berinteraksi dengan satu proses
Off Page Connector		Menggambarkan keluar atau masuk proses pada halaman yang berbeda
Process		Menggambarkan sebuah proses

II. Fishbone Diagram

Nama	Simbol	Deskripsi
Bone/Spine		Memetakan arah penyebab permasalahan
Head		Menggambarkan penyebab / akibat dari permasalahan

BAB 1
PENDAHULUAN

Pada bab ini menjelaskan latarbelakang persoalan, identifikasi masalah, tujuan dari tugas akhir, serta metodologi yang digunakan dalam pengerjaan tugas akhir dan sistematika penulisan laporan tugas akhir.

1.1 Latarbelakang

Dunia siber Indonesia di tahun 2019 diramaikan dengan 2 kejadian besar. Kejadian awal terpaut insiden siber yang terus menerus menghantam sistem keamanan siber nasional serta kejadian kedua terpaut usaha pemerintah menguatkan kemanan siber nasional itu sendiri. Insiden siber di Indonesia tidak lepas dengan apa yang terjalin di dunia siber global, sebab serangan dapat tiba dari mana saja bukan cuma dari Indonesia. Serangan siber pula belum pasti dicoba dari sumber serangan yang tercatat tetapi bisa jadi saja dari negeri lain yang menjadikan negeri sumber serangan itu selaku pijakan ataupun platform saja. Sistem *monitoring* nasional mata garuda BSSN misalnya mencatat sebanyak 290,3 juta serangan siber yang masuk ke Indonesia sejauh tahun 2019 ini serangan terbanyak tiba dari *IP address* berlokasi di Amerika Serikat, beralih dari keadaan tahun tadinya yang tercatat lebih banyak dari *IP address* yang terdapat di Indonesia sendiri [PUS19].

Metode penyerangan siber menggunakan *malware* tercatat paling banyak digunakan didunia siber global, *Hackmagedon* mencatat 39% dari distribusi teratas serangan siber dunia merupakan serangan menggunakan *malware*. Serangan *malware* masih menduduki peringkat pertama dalam serangan siber secara global. Tren yang sama diperlihatkan juga di Indonesia, *malware* menduduki peringkat pertama metode serangan yang sering digunakan dalam sembilan bulan dari dua belas bulan sepanjang tahun 2019. 36,2% dari distribusi teratas serangan siber ke Indonesia tercatat merupakan serangan menggunakan *malware*. *Kaspersky* juga mencatat adanya infeksi *malware* ke Indonesia setiap bulan rata rata 150 ribu infeksi [PUS19].

Meskipun penyerang lebih sering melakukan penyerangan kepada Lembaga Pemerintahaan, Keuangan dan Berita, bukan berarti lembaga pendidikan seperti Universitas Pasundan menjadi aman dari serangan siber. Universitas Pasundan sebagai salah satu lembaga pendidikan perguruan tinggi terkemuka di Indonesia memanfaatkan jaringan internet yaitu web sebagai media dalam menyampaikan informasi kepada pihak luar dan menghubungkan civitas-civitas yang ada guna memudahkan dalam penyampaian informasi. Pertukaran informasi yang terjadi dalam jaringan internet dapat berupa informasi penting atau pribadi yang hak aksesnya hanya dapat dilakukan oleh orang-orang tertentu.

Dalam wawancara dengan salah satu staff SPTIK yang bertugas mengelola *website* Universitas Pasundan, dapat diketahui bahwa *website* Universitas Pasundan pernah mendapat serangan siber berupa deface. *Web defacement* menurut BSSN adalah serangan pada *website* dengan mengubah tampilan maupun konten yang terdapat di *website* tersebut dengan cara memanfaatkan kelemahan yang terdapat pada sistem sehingga penyerang dapat mengganti atau menghapus konten

suatu *website*. Hal ini dapat mengakibatkan menganggu layanan dan menurunkan kredibilitas Universitas Pasundan.

Dengan demikian untuk mengambil topik penelitian tentang keamanan sistem informasi dengan judul penelitian "*Penetration Testing* Terhadap *Website* Universitas Pasundan" diharapkan dapat memberikan manfaat terutama bagi Universitas Pasundan.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka permasalahan yang dimunculkan pada tugas akhir ini adalah:

1. Adanya serangan siber yang mengancam sistem keamanan di *website* Universitas Pasundan

1.3 Tujuan Tugas akhir

Tujuan tugas akhir ini adalah menghasilkan sebuah laporan hasil dari pengujian/*penetration testing* yang dapat membantu pengelola mengamankan *website* Universitas Pasundan.

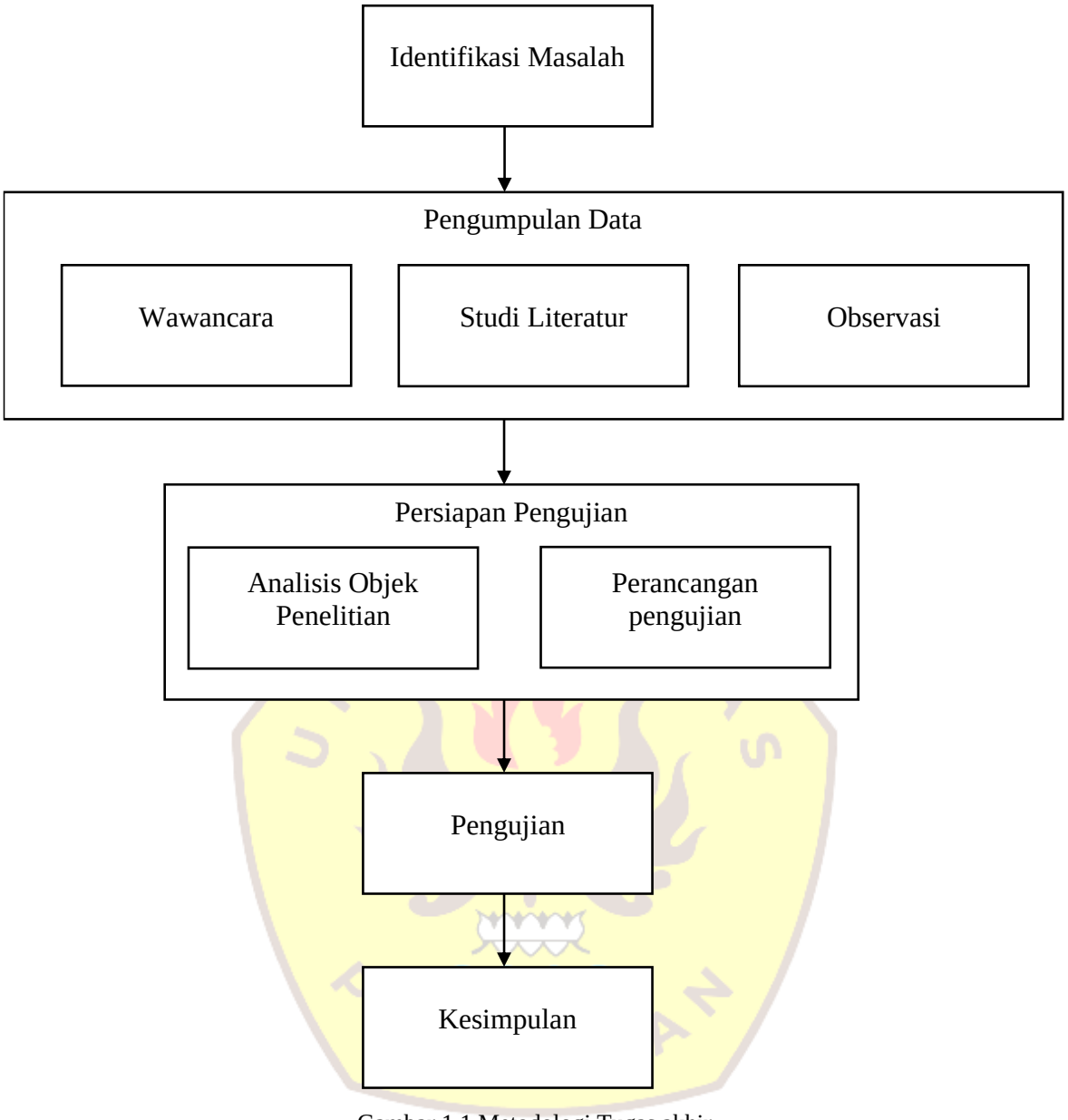
1.4 Lingkup Tugas akhir

Penyelesaian Tugas akhir dibatasi sebagai berikut:

1. *Website* yang akan diuji adalah *website* dengan domain unpas.ac.id.
2. Kategori pengujian yang dilakukan dalam melakukan *penetration testing* adalah *black box.*
3. *Penetration testing* ini mengacu pada OWASP Top 10 tahun 2017.
4. Pada tahap eksploitasi akan melakukan pengujian dengan *Sensitive Data Exposure* dan *Security Misconfiguration*.
5. *Broken Access Control* tidak diuji dikarenakan syarat ekploitasi membutuhkan akses untuk *login* sebagai admin/*user*.

1.5 Metodologi Tugas akhir

Metodologi Tugas Akhir adalah kerangka dasar tahapan penyelesaian tugas akhir. Metodologi penulisan pada tugas akhir ini mencakup seluruh kegiatan yang dilaksanakan untuk menganalisis masalah dan memecahkan kasus penelitian. Metodologi penelitian tugas akhir yang akan dilakukan untuk melakukan *Penetration Testing* Terhadap *Website* Universitas Pasundan Dengan Metode *Zero Entry Hacking* dapat dilihat pada gambar 1.1.



Gambar 1.1 Metodologi Tugas akhir

1. Identifikasi Masalah

   Pada tahap ini dilakukan identifikasi masalah yang terjadi pada aplikasi web serta solusi sementara yang diusulkan untuk menyelesaikan masalah tersebut.

2. Pengumpulan Data

   Pada tahap ini merupakan tahap yang dilakukan untuk mengumpulkan data mengenai aplikasi web yang akan diuji. Di dalam tahap ini terdapat tiga tahap yang dilakukan yaitu:

   a. Wawancara Merupakan suatu tahap yang dilakukan untuk mendapatkan informasi yang tepat dari narasumber secara langsung dengan cara penyampaian sejumlah pertanyaan dari pewawancara kepada narasumber.

b. Observasi Merupakan suatu tahap yang dilakukan untuk mencari informasi terkait hal yang dibutuhkan dengan melakukan tindakan secara langsung di lokasi penelitian.

c. Studi Literatur Merupakan pemanfaatan hasil pencarian dari referensi seperti buku, jurnal, serta internet untuk mendapatkan ilmu atau materi yang berkaitan dengan tugas akhir.

3. Persiapan Pengujian

Pada tahap ini merupakan tahap dimana penguji melakukan analisis terhadap *website* yang bertujuan untuk menganalisis kebutuhan dan membuat perancangan untuk melakukan pengujian.

4. Pengujian

Pada tahap ini merupakan tahap dimana penguji melakukan pengujian terhadap *website* dengan celah keamanan atau kerentanan yang diperoleh dari pencarian kelemahan pada *website* yang mengacu pada OWASP TOP 10 2017.

Pada tahap ini juga merupakan tahap hasil dari pengujian yang telah dilakukan terhadap *website* yang dilakukan.

5. Kesimpulan

Pada tahap ini merupakan tahap dimana akan dijelaskan mengenai kesimpulan yang telah dilakukan pada *website* yang diuji serta saran bagi penelitian selanjutnya.

1.6 Sistematika Penulisan Tugas akhir

Buku Tugas akhir ditulis dengan mengikuti sistematika sebagai berikut :

BAB 1 PENDAHULUAN

Bab pendahuluan berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan tugas akhir.

BAB 2 LANDASAN TEORI

Bab ini berisi teori-teori yang mendukung penelitian penulis, berupa literatur yang valid dan kasus yang mirip dengan topik penulis, Di bab ini terdapat teori yang digunakan dan penelitian terdahulu.

BAB 3 SKEMA PENELITIAN

Bab ini berisi penjelasan cara penulis untuk menyelesaikan tugas akhir, agar sesuai dengan pencapaian tugas akhir. Di bab ini terdapat alur penyelesaian tugas akhir, perumusan masalah, kerangka pemikiran teoritis, profile penelitian.

BAB 4 ANALISIS DAN PERANCANGAN

Bab ini berisi tentang analisis dari sistem yang meliputi analisis objek penelitian, analisis kebutuhan, dan perancangan pengujian yang akan digunakan pada pengujian pada target.

BAB 5 PENGUJIAN DAN HASIL

Bab ini berisi tentang pengujian dan hasil dari pengujian yang mengacu pada perancangan dari pengujian target.

BAB 6 PENUTUP

Bab ini berisi kesimpulan yang diperoleh dari hasil penelitian tugas akhir, saran-saran untuk penelitian selanjutnya dan rekomendasi.

DAFTAR PUSTAKA

[AND06] Andreu, A., “Professional Pen Testing for Web Apllications”, Wiley Publishing, Indianapolis, 2006.

[AUT19] Author, “Apa itu Black Box Penetration Testing?” tersedia : 20 April 2019, https://www.qtera.co.id/apa-itu-black-box-penetration-testing/, April 2019,diakses : 17 Juli 2022.

[BAC11] Bacudio, A. G., Yuan, X., Chu, B. T. B., Jones, M., ”An overview of Penetration Testing”, International Journal of Network Security & Its Applications, Vol.3, No.6, November 2011.

[BAL15] Baloch, R., “Ethical Hacking And Penetration Testing Guide”, Taylor & Francis Group, 2015.

[COL09] Cole, E., Krutz, R., Conley, J. W., ”Network Security Bible. 2nd Edition”, Jilid 2, Wiley Publishing, Indianapolis, 2009.

[DEW18] Dewanto, A. Putra., “Penetration Testing Pada Domain uii.ac.id Menggunakan OWASP 10”,

[ENG13] Engebretson, P. “The Basic Of Hacking and Penetration Testing”, Edition 2, Elsevier Inc, Waltham, 2013.

[HID21] Hidayatulloh. Syarif,. Saptadiaji, Desky., “Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)”. 2021

[IQB14] Iqbal, M., “5 Jam Belajar PHP MYSQL Dengan Dreamweaver CS3”, Deepublish, 2014.

[MEU14] Meucci, Matteo., Muller, Andrew., “OWASP Testing Guide Release”, Versi 4.0, Creative Common, 2014.

[NAG14] Nagpal, B., Chauhan, N., Singh, N., Sharma, P., ”Preventive Measures for Securing Web Applications Using Broken Authentication and Session Management Attacks: A Study”, International Journal of Computer Applications, 0975 – 8887, Tahun 2014.

[PUS19] Pusopskamsinas., “Indonesia Cyber Security Monitoring Report 2019”, Jakarta, 2019.

[ROC21] Rochman, Agus., Salam, R. Rohian., Maulana, S. Agus., “Analisis Keamanan Website Dengan Information System Security Assessment Framework (ISSAF) Dan Open Web Application Security Project (OWASP) Di Rumah Sakit XYZ”, Jurnal Indonesia Sosial Teknologi, Vol. 2, No.4, 2021.

[ROS21] Rosaliah, Y. T. Afifa, Jayanta., Hananto, Bayu., “Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10

pada Website SIM xxx", Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya, Jakarta, 2021.

[SIM06] Simarmata, J., "Pengenalan Teknologi Komputer dan Informasi", Andi, Yogyakarta, 2006.

[SOF19] Sofana, I., Primartha, R., "Network Security dan Cyber Security", Informatika, Bandung, 2019.

[VAN17] Van Der Stock, A., Glas, B., Smithline, N., Gigler, T., "Owasp Top 10 2017 The Ten Most Critical Web Application Security Risks.", Creative Commons, 2017.

[WAR19] Wardaya, Muhammad S. Sastra., "Penetration Testing Terhadap Website Asosiasi Profesional Informasi Sekolah Indonesia (APISI)", Jakarta, 2019.

[WHI06] Whitaker, A., Newman, D. P., "Penetration Testing and Network Defense", Cisco Systems Inc, Indianapolis, 2006.

UNIVERSITAS
PASUNDAN