ANALISIS CELAH KEAMANAN WEB AKADEMIK UNIVERSITAS PASUNDAN DENGAN METODE PENETRATION TESTING

TUGAS AKHIR

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

oleh :

Fahmi Farhan Husin
NRP : 16.304.0083

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG

NOVEMBER 2020

LEMBAR PENGESAHAN

LAPORAN TUGAS AKHIR

Telah disetujui dan disahkan laporan Tugas Akhir, dari :

Nama : Fahmi Farhan Husin
Nrp : 16.304.0083

Dengan judul :

"**ANALISIS CELAH KEAMANAN WEB AKADEMIK UNIVERSITAS PASUNDAN DENGAN METODE PENETRATION TESTING**"

Mengetahui,
Bandung, 4 November 2020

Koordinator TA,

(Ade Sukendar, S.T, M.T)

Pernyataan Kesediaan Pembimbing :

Bandung, _____
Pembimbing Utama

(Ferry Mulyanto, S.T,M.Kom)

ABSTRAK

Celah keamanan merupakan hal yang harus diperhatikan dalam menjaga keamanan informasi. Adanya celah keamanan akan memudahkan *cyber attack* pada aplikasi web. Perlunya analisis celah keamanan web akademik Universitas Pasundan, karena adanya akses yang tidak berhak serta gangguan pada pengelolaan pada web akademik, salah satu cara yang dilakukan adalah dengan metode *penetration testing*.

Penelitian ini membantu dalam memastikan ada atau tidaknya celah keamanan dengan melakukan analisis celah keamanan, dilakukan dengan melakukan studi literatur, yang mendukung tahapan analisis dengan memanfaatkan metode *penetration testing.*

Hasil akhir dari penelitian ini berupa celah keamanan , yang merupakan kelemahan yang dimiliki oleh web akademik, sehingga pengelola dapat meningkatkan keamanan dan agar ruang *attacker* dalam membobol aplikasi web semakin kecil

Kata Kunci : keamanan informasi, aplikasi web, celah keamanan, *cyber attack, penetration testing.*

ABSTRACT

Vulnerability is something that must be considered in maintain information security. The existence of a vulnerability will facilitate cyber attacks on web applications. The need for vulnerability analysis on the Universitas Pasundan, cause of unauthorized access and interference with the management of the academic web, one step to do is by penetration testing method.

This research helps to ensure the presence or absence of vulnerability by conducting a vulnerability analysis, carried out by conducting a literature study, which supports the analysis phase by utilizing the penetration testing method.

The final result of this research is the vulnerability, which is a weakness that is owned by the academic web, so that developers can increase security and prevent attackers break to the web applications.

Keyword : information security, web application, vulnerability, cyber attack, penetration testing.

KATA PENGANTAR

Ucapan dan rasa syukur penulis layangkan ke hadirat Ilahi Robbi, yang telah berkenan menguatkan penulis untuk membuat Laporan Tugas Akhir dengan judul "Analisis Celah Keamanan Web Akademik Universitas Pasundan dengan Metode Penetration Testing".

Adapun penulisan laporan ini bertujuan untuk memenuhi salah satu syarat untuk kelulusan Program Strata 1, di Program Studi Teknik Informatika Universitas Pasundan.

Penulis menyadari laporan ini dapat terwujud berkat bantuan dan dorongan dari berbagai pihak. Maka pada kesempatan ini penulis sampaikan terima kasih yang sebesar-besarnya atas segala bantuan yang penulis terima baik secara moril maupun materil, sehingga penulis dapat menyelesaikan laporan ini kepada :

1. Kepada pembimbing, Pak Ferry Mulyanto, S.T,M.Kom.
2. Kepada Orang Tua tersayang, dan keluarga yang selalu memberikan motivasi serta do'anya dalam pembuatan tugas akhir ini.
3. Koordinator Tugas Akhir dan Ketua Kelompok Keilmuan serta seluruh civitas akademika Teknik Informatika di UNIVERSITAS PASUNDAN BANDUNG, yang telah memberikan bekal ilmu selama penulis menimba ilmu.
4. Kepada Fitriyani, yang selalu memberikan dorongan serta do'a nya dalam pembuatan tugas akhir.
5. Kepada teman-teman seperjuangan Universitas Pasundan Bandung yang tidak bisa semua penulis sebutkan.

Tiada gading yang tak retak, tiada gelombang tanpa ombak, segala kesalahan merupakan kelemahan dan kekurangan penulis. oleh karena itu, penulis harapkan kritik dan saran dari semua pihak demi perbaikan di masa yang akan datang.

Akhir kata, semoga penulisan laporan ini dapat bermanfaat bagi penulis dan bagi perkembangan ilmu Teknologi dimasa yang akan datang.

Bandung, 4 November 2020

Penulis

DAFTAR ISI

BAB 1
Pendahuluan

Pada bab ini menjelaskan latar belakang, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi yang akan digunakan dalam pengerjaan tugas akhir, dan sistematika penulisan tugas akhir.

1.1 Latar Belakang

Isu keamanan web masih menjadi hal yang paling populer pada ranah teknologi informasi, lebih dari 25% aplikasi web memiliki setidaknya satu celah keamanan dengan tingkat keparahan tinggi [ACU20], selain itu *cyber attacks* juga masih banyak terjadi. Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat, 88.414.296 *cyber attack* telah terjadi sejak 1 Januari hingga 12 April 2020 [BSS20]. *Cyber attacks* dapat mengganggu aktivitas jaringan informasi serta data digital suatu negara yang menggunakannya sebagai alat pengontrol infrastruktur vital, seperti: suplai listrik, komando militer, kontrol radioaktif nuklir, pelepasan limbah beracun industri kimia, pengaturan lalu lintas, pengaturan bursa saham dan berbagai aktivitas lainnya [PUT17].

Keamanan informasi menjadi hal yang perlu diperhatikan untuk menjamin keamanan aplikasi web. [PAR08] memaparkan, keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan. Masalah tersebut penting karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan.

Adanya akses oleh orang yang tidak berhak pernah terjadi pada Web Akademik Universitas Pasundan. Pengguna yang tidak berhak dapat mengakses data kelulusan tes masuk calon mahasiswa baru melalui percobaan penyusupan, kemudian melakukan penipuan melalui telepon dengan meminta kepada calon mahasiswa yang lulus untuk mengirim sejumlah uang ke nomor rekeningnya. Kasus lain juga terjadi pada mahasiswa yang bisa melihat informasi pribadi mahasiswa lain yang ada di Universitas Pasundan. Menurut ketua SPTIK Universitas Pasundan, pengecekan keamanan dilakukan dengan melihat log transaksi yang ada. Walaupun dikatakan tergolong sudah aman, tidak menutup kemungkinan adanya celah-celah keamanan yang masih belum diketahui.

Dari permasalahan tersebut penulis tertarik untuk melakukan analisis celah keamanan dengan metode uji penetrasi (penetration testing) pada Web Akademik Universitas Pasundan, untuk memastikan ada atau tidaknya celah keamanan. Sesuai dengan pernyataan [SYA18], dengan metode-metode dan simulasi uji penetrasi yang dilakukan oleh *pentester* diharapkan dapat menjadi

pertimbangan pihak *developer* untuk menutup celah pada *website* sehingga ruang bagi *attacker* untuk membobol *website* semakin kecil.

1.2 Identifikasi Masalah

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

1. Adanya celah keamanan yang memungkinkan akses data untuk pihak yang tidak berhak.

1.3 Tujuan Tugas Akhir

Tujuan tugas akhir ini adalah :

1. Melakukan analisis celah keamanan dengan metode uji penetrasi untuk memastikan ada atau tidaknya celah keamanan yang memungkinkan akses data untuk pihak yang tidak berhak.
2. Memperoleh informasi dari metode uji penetrasi, sebagai pertimbangan pihak pengembang untuk menutup celah keamanan pada Web Akademik Universitas Pasundan.

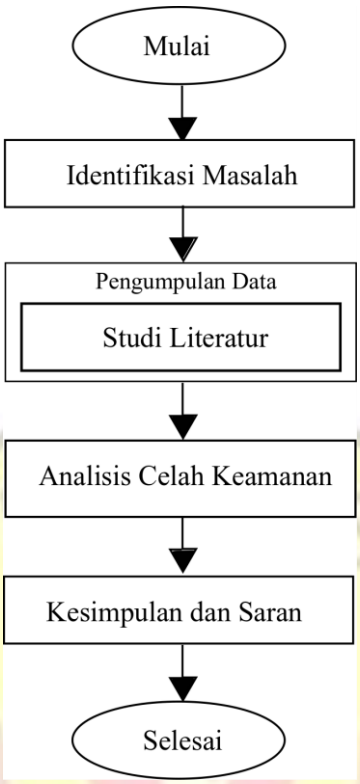
1.4 Lingkup Tugas Akhir

Penyelesaian Tugas Akhir dibatasi sebagai berikut :

1. Proses mencari celah keamanan dalam uji penetrasi hanya dilakukan dengan alamat akd.unpas.ac.id/unpas.
2. Jenis uji penetrasi yang dilakukan saat penelitian menggunakan *blackbox testing*.
3. Uji penetrasi hanya mencari celah keamanan dengan tingkat keparahan tinggi.
4. Tidak melakukan uji coba secara langsung terhadap web akademik.
5. Dokumentasi berupa penjelasan dalam analisis celah keamanan.
6. Pengaruh yang dilihat adalah dampak yang ditimbulkan dari temuan celah keamanan baik dari segi teknis maupun bisnis.

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 analisis celah keamanan Web Akademik Universitas Pasundan dapat dilihat pada gambar 1.1.



Gambar 1.1 Metodologi Tugas Akhir

1. Identifikasi Masalah

Pada tahap ini dilakukan identifikasi masalah dengan mencari permasalahan yang terjadi pada web akademik.

2. Pengumpulan Data

Pada tahap ini dilakukan pengumpulkan data untuk analisis celah keamanan web akademik dengan mengumpulkan referensi yang mendukung penyelesaian tugas akhir, yaitu:

a. Studi Literatur :

Mendapatkan ilmu atau materi yang berkaitan dengan tugas akhir melalui referensi seperti buku, jurnal, serta internet.

3. Analisis Celah Keamanan

Pada tahap ini dilakukan tahapan untuk menganalisis celah keamanan web akademik dengan metode *penetration testing*.

4. Kesimpulan dan Saran

Pada tahap ini dilakukan pembuatan kesimpulan dari hasil penelitian yang telah dilakukan pada web akademik , saran-saran untuk penelitian selanjutnya, dan rekomendasi perbaikan celah keamanan.

1.6 Sistematika Penulisan Tugas Akhir

Buku tugas akhir ditulis dengan mengikuti sistematika sebagai berikut :

Bab 1 : Pendahuluan

Bab ini berisi penjelasan mengenai usulan penelitian yang dilakukan selama penulis melaksanakan tugas akhir. Di bab ini terdapat latar belakang masalah, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi tugas akhir dan sistematika penulisan tugas akhir.

Bab 2 : Landasan Teori dan Penelitian Terdahulu

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 Celah Keamanan Web Akademik Universitas Pasundan

Bab ini berisi penjelasan mengenai tahapan dalam menganalisis web akademik yang akan dilakukan dengan menggunakan *tools* untuk mencari celah keamanan dengan melakukan identifikasi celah keamanan, serta mengkaji celah keamanan yang ada.

Bab 5 : Kesimpulan dan Saran

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

DAFTAR PUSTAKA

[ACU20] Acunetix, "Introduction to Acunetix", 2020, www.acunetix.com/support/docs/introduction/, 2020, diakses : 6 Juni 2020

[ACU20] Acunetix, "Web Application Vulnerability Report 2020", 2020, https://www.acunetix.com/acunetix-web-application-vulnerability-report, Maret 2020, diakses : 13 September 2020.

[ACU20] Acunetix."Acunetix as Automated Penetration Testing Software", 2020, https://www.acunetix.com/vulnerability-scanner/penetration-testing-software/, diakses : 22 September 2020.

[ALW20] Alwi. Erick Irawadi, Herdianti , Fitriyani Umar.," Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning", Informatics Journal, Volume 5, Nomor 2, 2020.

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

[ASS95] Assosiates, J., "Cause and Effect Diagram Plain and Simple", Oriel.Inc, USA, 1995.

[BAC11] Bacudio, Aileen. G, dkk.," An overview of Penetration Testing", International Journal of Network Security & Its Applications, 2011.

[BSS20] BSSN., " Rekap Serangan Siber (Januari – April 2020)" , 2020, https://bssn.go.id/rekap-serangan-siber-januari-april-2020/, 2020, diakses :14 September 2020.

[DEV16] Devi.D Rubidha, R.Venkatesan, Raghuraman.K.," A STUDY ON SQL INJECTION TECHNIQUES", International Journal of Pharmacy & Technology, Volume 8, Nomor 4, 2016.

[FUR08] Furnell, S, dkk.," Securing Information and Communications Systems Principles, Technologies, and Applications.", Artech House, London, 2008.

[FYO97] Fyodor., "*Introduction"*, 1997,https://nmap.org/. 2020, diakses : 31 Mei 2020.

[FYO97] Fyodor., "Nmap Network Scanning", 1997, https://nmap.org/book/man.html. 2020 , diakses : 14 September 2020

[MAY20] Mayasari. Rini, dkk,"Analisis Vulnerability pada Website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability", SYSTEMATICS, Volume 2, Nomor 1, 2020.

[NAS18] Nasution, M., “Keamanan Informasi:Pendahuluan”, *Technical Report*, 2018.

[PAR08] Paryati., “Keamanan Sistem Informasi”, Seminar Nasional Informatika 2008 (semnasIF 2008), 2008.

[PUT17] Putri, N, Idin Fasisaka, dan A.A.B. Surya Widya Nugraha., “Penanganan Cyber Attacks oleh Pemerintah Tiongkok Melalui Kebijakan Network Security Tahun 2000 – 2015”, Jurnal Hubungan Internasional, 2017.

[QAS18] Qasaimeh. Malik, Ala’A Shamlawi , Tariq Khairallah.,” BLACK BOX EVALUATION OF WEB APPLICATION SCANNERS: STANDARDS MAPPING APPROACH”, Journal of Theoretical and Applied Information Technology, Volume 96, Nomor 14, 2018.

[SAH19] Sahren, Ruri Ashari Dalimuthe, Muhammad Amin., “Penetration Testing untuk Deteksi Vulnerability Sistem Informasi Kampus”, Prosiding Seminar Nasional Riset Information Science (SENARIS), 2019.

[SYA18] Syarifudin, I., “Pentesting dan Analisis Keamanan Web Paud Dikmas”, 2018.

[TAM19] Tampubolon, K., ”Perbedaan Cyber Attack, Cyber Crime, dan Cyber Warfare”, Jurist-Diction, Jilid 2, Nomor 2, 2019.

[WAH19] Wahyudi., “ANALISA PENGUJIAN KERENTANAN TERHADAP WEB SERVER SIMAK (Studi Kasus : STMIK Kharisma Karawang)”, Jurnal Teknologi Informasi , Vol. 5, Nomor 1, 2019.

[WEI14] Weidman, G., “Penetration testing A Hands-On Introduction to Hacking”, no starch press, San Francisco, 2014.

[WHI06] Whitaker, A, Daniel. P. Newman., “Penetration Testing and Network Defense”, Cisco Press, Indianapolis, 2006.

[YUL17] Yulianingsih.,” Melindungi Aplikasi dari Serangan CrossSite Scripting (XSS) Dengan Metode Metacharacter”, TEKNOSI, Volume 03, Nomor 01, 2017.