PENGUJIAN CELAH KEAMANAN PADA *WEBSITE CAPTIVE PORTAL* DENGAN MENERAPKAN *PENETRATION TESTING* (Studi Kasus: Teknik Informatika Universitas Pasundan)

TUGAS AKHIR

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

oleh :

Iqbaludin
NRP : 13.304.0147

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
JULI 2018

LEMBAR PENGESAHAN
LAPORAN TUGAS AKHIR

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal sidang sesuai berita acara sidang, tugas akhir dari :

Nama : Iqbaludin
Nrp : 13.304.0147

Dengan judul :

"PENGUJIAN CELAH KEAMANAN PADA *WEBSITE CAPTIVE PORTAL* DENGAN MENERAPKAN *PENETRATION TESTING*
(Studi Kasus: Teknik Informatika Universitas Pasundan)"

Bandung, 31 Juli 2018

Menyetujui,

Pembimbing Utama,	Pembimbing Pendamping,
(Doddy Ferdiansyah, S.T., M.T)	(Iwan Kurniawan, S.T., M.T)

ABSTRAK

Teknik Informatika Unpas sudah menerapkan *captive portal* untuk di lingkungan Fakultas Teknik Universitas Pasundan dalam mengamankan layanan internet. *Website captive portal* tersebut dapat diakses dimana saja dan oleh siapa saja tetapi jika ingin melakukan registrasi hanya bisa dilakukan jika pengguna merupakan mahasiswa Unpas. Hal tersebut tidak menutup kemungkinan adanya percobaan serangan atau gangguan baik dari internal maupun eksternal yang memungkinkan bahwa layanan *website* tersebut akan disalahgunakan oleh pihak yang tidak bertanggungjawab. Tentunya hal ini harus diperhatikan sebagai acuan untuk pengembang maupun pengelola dalam menjaga keamanan. Untuk menjaga keamanan pada *website captive portal*, pengembang atau pengelola harus mengetahui celah keamanan yang terdapat pada *website captive portal* terlebih dahulu sebelum diketahui oleh pihak yang tidak bertanggungjawab. Oleh karena itu, untuk mengetahui celah keamanan pada *website captive portal* diperlukan pengujian dengan menerapkan *penetration testing* pada *website captive portal* Teknik Informatika Unpas.

Penelitian ini dilakukan untuk mengetahui celah keamanan pada *website captive portal* dengan menerapkan *penetration testing*. Penelitian dilakukan dengan mengumpulkan informasi mengenai aplikasi web, melakukan analisis celah keamanan pada aplikasi web dan melakukan pengujian berdasarkan celah keamanan yang memiliki tingkat risiko sedang (*medium*) dan berdasarkan salah satu ancaman yang paling sering terjadi yang dimuat dalam OWASP Top 10 – 2017. Pengujian ini dilakukan untuk mengetahui apakah *website captive portal* Teknik Informatika Unpas rentan terhadap serangan yang diujikan tersebut.

Hasil akhir dari penelitian ini adalah sebuah hasil pengujian *website captive portal* yang dapat digunakan oleh pengembang maupun pengelola untuk memperbaiki keamanan pada *website captive portal* Teknik Informatika Unpas.

Kata kunci : *internet, aplikasi web, website captive portal, penetration testing, celah keamanan, OWASP Top 10 - 2017*

ABSTRACT

Informatics Engineering Unpas has applied captive portal to the environment of Pasundan University Faculty of Engineering in securing internet service. Website captive portal can be accessed anywhere and by anyone but if you want to register can only be done if the user is a student Unpas. It does not rule out any possible internal or external attack or intrusion attempts that would allow the website's services to be misused by irresponsible parties. Of course this should be considered as a reference for developers and managers in maintaining security. To maintain the security of the captive portal website, the developer or manager must know the security hole found on the captive portal website first before it is known by the irresponsible party. Therefore, to know the vulnerability of website captive portal required by applying penetration testing on website captive portal of Informatics Engineering Unpas.

This research was conducted to find out the vulnerability of website captive portal by applying penetration testing. The study was conducted by collecting information on web applications, analyzing security loopholes in web applications and performing security-based vulnerabilities that have medium to medium risk levels and based on one of the most frequent threats contained in OWASP Top 10 - 2017. This test conducted to find out whether the website captive portal of Informatics Engineering Unpas vulnerable to the attack that tested it.

The final result of this research is a result of testing website captive portal that can be used by developer and manager to improve security at website captive portal of Informatics Engineering Unpas.

Keywords: *internet, web application, website captive portal, penetration testing, security holes, OWASP Top 10 – 2017*

DAFTAR ISI

BAB 1
PENDAHULUAN

Pada bab ini berisi Latar Belakang Masalah, Identifikasi Masalah, Tujuan Tugas Akhir, Lingkup Tugas Akhir, Metodologi Tugas Akhir, serta Sistematika Penulisan Tugas Akhir.

1.1. Latar Belakang Masalah

Seiring dengan perkembangan teknologi, internet menjadi bagian dari kebutuhan dalam setiap aktivitas yang dilakukan oleh masyarakat secara umum, seperti komunikasi, mencari informasi, transaksi, berwirausaha dan banyak hal yang tidak bisa disebutkan satu persatu. Dalam penggunaan internet sudah banyak teknologi yang mendukung untuk bisa mengakses internet, contohnya seperti *wireless* yang saat ini sering di temukan di berbagai tempat. Dengan adanya *wireless* di berbagai tempat, tentunya memerlukan pengamanan yang kuat agar jaringan *wireless* tersebut tidak disalahgunakan. Salah satu pengamanan dalam infrastruktur jaringan *wireless* yaitu dengan menerapkan *captive portal*. Penerapan *captive portal* dilakukan untuk menahan agar tidak adanya trafik sehingga *user* harus melakukan registrasi terlebih dahulu untuk menggunakan jaringan *wireless* tersebut. *Captive portal* akan memaksa *user* yang belum terdaftar atau terautentikasi untuk masuk ke dalam *authentication web* dan akan langsung menampilkan halaman *login* (Efvy Zamidra Zam, 2014) [ZAM14].

Teknik Informatika Universitas Pasundan sudah menerapkan *captive portal* untuk di lingkungan Fakultas Teknik Universitas Pasundan dalam mengamankan layanan internet. *Website captive portal* tersebut dapat diakses dimana saja dan oleh siapa saja tetapi jika ingin melakukan registrasi hanya bisa dilakukan jika pengguna merupakan mahasiswa Unpas. Hal tersebut tidak menutup kemungkinan adanya percobaan serangan atau gangguan baik dari internal maupun eksternal yang memungkinkan bahwa layanan *website* tersebut akan disalahgunakan oleh pihak yang tidak bertanggungjawab. Salah satu contoh kasus yang terjadi adalah ada mahasiswa yang melapor pada pihak admin atau pengelola yang merasa dirinya belum melakukan registrasi tetapi kenyataannya menurut sistem mahasiswa tersebut sudah melakukan registrasi. Selain itu ada juga gangguan yang berasal dari aplikasi web *captive portal* seperti *error* atau *bug*, salah satu contohnya adalah ketika mahasiswa-mahasiswa baru melakukan pendaftaran, sinkronisasi data SITU ke aplikasi web *captive portal* berjalan lambat sehingga mahasiswa belum bisa menggunakan layanan internet sampai data SITU tersebut sudah tersinkronisasi dengan aplikasi web *captive portal*. Tentunya hal ini harus diperhatikan sebagai acuan untuk pengembang maupun pengelola dalam memperbaiki masalah yang terjadi sehingga dapat mencegah adanya gangguan atau *bug* yang terjadi pada aplikasi web *captive portal*. Maka dari itu pengembang atau pengelola harus mengetahui celah keamanan pada aplikasi web *captive portal* dalam mencegah terjadinya gangguan atau *bug* sebelum diketahui terlebih dahulu oleh pihak yang tidak bertanggungjawab.

Dari permasalahan tersebut penulis tertarik untuk melakukan penelitian tugas akhir untuk mengetahui celah keamanan pada aplikasi web *captive portal* dengan melakukan pengujian terhadap

aplikasi web yang disebut dengan *penetration testing. Penetration testing* adalah sebuah metode yang dilakukan pihak ketiga (*hacker*) yang bekerjasama dengan sebuah jaringan komputer perusahaan atau organisasi untuk menilai keamanan dari sistem tersebut (Whitaker, 2006) [NAB14]. *Penetration testing* ini dilakukan untuk mendeteksi adanya kelemahan-kelemahan pada aplikasi web. Pada penelitian ini penulis akan melakukan pengujian atau *penetration testing* terhadap *website captive portal* Teknik Informatika Universitas Pasundan dengan berdasarkan celah keamanan apabila ditemukannya celah keamanan pada *website captive portal* dan pengujian dengan berdasarkan OWASP Top 10 – 2017. Penerapan *penetration testing* pada *website captive portal* Teknik Universitas Pasundan bertujuan untuk menemukan celah keamanan yang terdapat pada *website captive portal* dengan melakukan pengujian atau *penetration testing*. Hasil pengujian ini dapat digunakan oleh pengembang atau pengelola dalam memperbaiki sisi keamanan dari aplikasi web *captive portal* sehingga meminimalkan gangguan dari pihak yang tidak bertanggungjawab.

1.2. Identifikasi Masalah

Berdasarkan latar belakang masalah yang telah diuraikan sebelumnya, maka masalah yang dapat diidentifikasi adalah sebagai berikut:

1. Apakah *website captive portal* Teknik Informatika Universitas Pasundan memiliki celah keamanan.
2. Bagaimana cara untuk menemukan celah keamanan pada *website captive portal* Teknik Informatika Universitas Pasundan.

1.3. Tujuan Tugas Akhir

Adapun tujuan dari penelitian tugas akhir ini adalah sebagai berikut:

1. Melakukan pengujian atau *penetration testing* pada *website captive portal* dengan berdasarkan celah keamanan yang diperoleh dan dengan berdasarkan OWASP Top 10 – 2017.
2. Menghasilkan informasi berupa hasil pengujian pada *website captive portal* yang berguna sebagai bahan acuan untuk pengelola atau pengembang dalam melakukan perbaikan keamanan.

1.4. Lingkup Tugas Akhir

Adapun penyelesaian penelitian tugas akhir ini dibatasi sebagai berikut:

1. *Captive portal* yang akan di uji adalah *captive portal* Teknik Informatika Universitas Pasundan.
2. Jenis pengujian yang dilakukan dalam melakukan *penetration testing* adalah jenis *black box testing*.
3. Pengujian dilakukan berdasarkan celah keamanan (*vulnerability*) yang memiliki tingkat risiko paling tinggi.
4. Pengujian dilakukan berdasarkan salah satu ancaman yang paling sering terjadi yang dimuat dalam OWASP Top 10 – 2017.
5. Tidak melakukan perbaikan program pada sisi keamanan terhadap *website captive portal*.

1.5. Metodologi Tugas Akhir

Berikut ini merupakan metodologi penelitian tugas akhir yang dapat dilihat pada Gambar 1.1 Metodologi Tugas Akhir, dibawah ini merupakan penjelasan dari metodologi penelitian 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. Analisis Celah Keamanan

   Pada tahap ini merupakan tahap dimana penguji melakukan analisis terhadap aplikasi web yang bertujuan untuk menemukan celah keamanan atau kerentanan pada aplikasi web yang akan diuji.

4. Pengujian

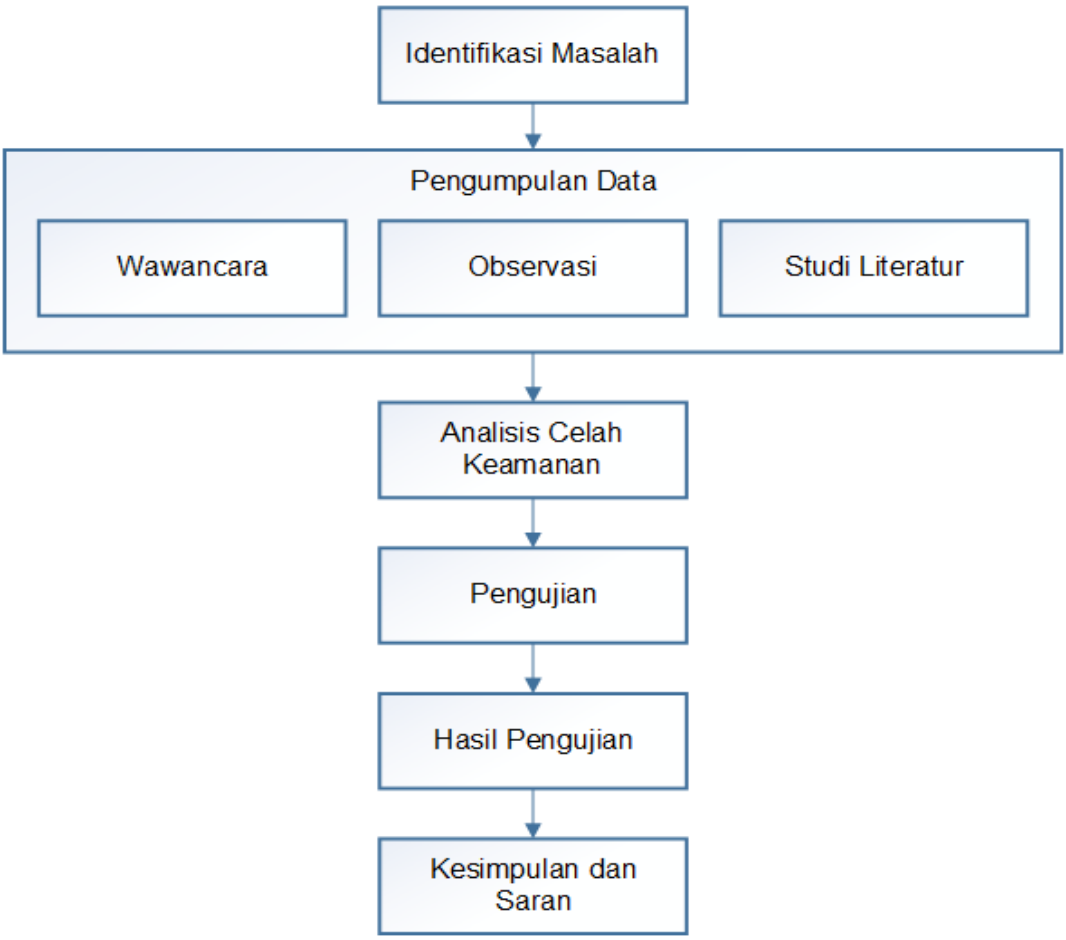
   Pada tahap ini merupakan tahap dimana penguji melakukan pengujian terhadap aplikasi web dengan celah keamanan atau kerentanan yang diperoleh yang memiliki tingkat risiko paling tinggi serta melakukan pengujian yang mengacu pada literatur yang sudah ada.

5. Hasil Pengujian

   Pada tahap ini merupakan tahap penjelasan mengenai pengujian yang telah dilakukan terhadap aplikasi web yang diperoleh dari tahap sebelumnya.

6. Kesimpulan dan Saran

   Pada tahap ini merupakan tahap dimana akan dijelaskan mengenai kesimpulan dari hasil pengujian yang telah dilakukan pada aplikasi web yang diuji serta saran bagi penelitian selanjutnya.



Gambar 1.1 Metodologi Tugas Akhir

1.6. Sistematika Penulisan Tugas Akhir

Untuk memberikan gambaran secara jelas, maka dirancang sebuah sistematika penulisan pada laporan tugas akhir, adapun sistematika penulisan laporan tugas akhir ini dibagi menjadi beberapa bab yaitu:

BAB 1 PENDAHULUAN

Bab ini berisikan penjelasan mengenai garis besar pada tugas akhir ini seperti latar belakang masalah, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi tugas akhir dan sistematika penulisan tugas akhir.

BAB 2 LANDASAN TEORI

Bab ini berisikan teori-teori yang berkaitan dan mendasari dalam penelitian serta penulisan tugas akhir ini.

BAB 3 SKEMA PENELITIAN

Bab ini menjelaskan mengenai tahapan-tahapan penelitian tugas akhir seperti rancangan penelitian, peta analisis dan langkah analisis, analisis masalah dan manfaat TA, analisis kegunaan konsep dan teori, serta tempat dan objek penelitian.

BAB 4 ANALISIS CELAH KEAMANAN PADA *WEBSITE CAPTIVE PORTAL*

Bab ini menjelaskan mengenai tahapan pengumpulan informasi mengenai *website captive portal* yang dilakukan dengan menggunakan *tools* dan melakukan identifikasi celah keamanan (*vulnerability*) yang dilakukan terhadap *website captive portal* dengan menggunakan *tools*.

BAB 5 PENGUJIAN (*PENETRATION TESTING*) PADA *WEBSITE CAPTIVE PORTAL*

Bab ini menjelaskan mengenai pengujian (*penetration testing*) yang dilakukan terhadap *website captive portal* berdasarkan celah keamanan (*vulnerability*) yang diperoleh dengan tingkat risiko paling tinggi dan dilakukan juga pengujian berdasarkan salah satu ancaman yang paling sering terjadi yang dimuat dalam OWASP Top 10 – 2017.

BAB 6 KESIMPULAN DAN SARAN

Bab ini menjelaskan mengenai kesimpulan yang diperoleh dari hasil penelitian tugas akhir, serta saran-saran untuk pengembangan selanjutnya agar dapat dilakukan perbaikan-perbaikan pada masa yang akan datang.

DAFTAR PUSTAKA

Daftar pustaka berisikan tentang sumber-sumber atau literatur yang digunakan pada landasan teori dalam penelitian tugas akhir ini.

LAMPIRAN

Lampiran berisikan tentang hal-hal yang menunjang dalam penelitian tugas akhir ini.

DAFTAR PUSTAKA

[ACU18] Acunetix, "*Audit your website security*", tersedia : 22 Maret 2018, https://www.acunetix.com/, Januari 2018.

[ADM14] Admin Bestariweb, "*Mengenal Apa itu DNS Record Domain*", tersedia : 10 Maret 2018, https://www.bestariwebhost.com/mengenal-dns-domain-record/, November 2014.

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

[AJI13] Ajidin, Didin, "*Pengertian Aplikasi Web*", tersedia : 20 Oktober 2016, http://strukturkode.blogspot.co.id/2013/04/pengertian-aplikasi-web.html, April 2013.

[COB16] Cobantoro, A. F., "*Penerapan OWASP versi 4 Untuk Uji Kerentanan Web Server* (*Studi Kasus Ejurnal Server Kampus X Madiun*)", Seminar Nasional Telekomunikasi dan Informatika, 2016.

[CRE14] Creative Commons Attribution-ShareAlike, "*Testing for authentication*", tersedia : 8 Juni 2018, https://www.owasp.org/index.php/Testing_for_authentication, Agustus 2014.

[CRE14] Creative Commons Attribution-ShareAlike, "*Testing for Authorization*", tersedia 8 Juni 2018, https://www.owasp.org/index.php/Testing_for_Authorization, Agustus 2014.

[CRE14] Creative Commons Attribution-ShareAlike, "*Testing for Session Management*", tersedia : 8 Juni 2018, https://www.owasp.org/index.php/Testing_for_Session_Management, Agustus 2014.

[CRE16] Creative Commons Attribution-ShareAlike, "*Testing for Clickjacking (OTG-CLIENT-009)*", tersedia : 10 Juni 2018, https://www.owasp.org/index.php/Testing_for_Clickjacking_(OTG-CLIENT-009), Mei 2016.

[CRE18] Creative Commons Attribution-ShareAlike, "*OWASP Zed Attack Proxy Project*", tersedia : 25 Maret 2018, https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project, Juni 2018.

[CRE18] Creative Commons Attribution-ShareAlike, "*Cross-Site Request Forgery (CSRF)*", tersedia : 10 Juni 2018, https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF), Maret 2018.

[DIR15] Dirgahayu, S.T., M.Sc., D. T., Prayudi, S.Si., M.Kom., Y., & Fajaryanto, A., "*Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server*", Jurnal Ilmiah NERO, 2015.

[ERW14] Erwin, Ernan, "*Makalah Vulnerability*", tersedia : 20 Oktober 2016, http://gankersmekti.blogspot. co.id/2014/03/makalah-vulnerability.html, Maret 2014.

[FAT11] Fathihadi, Ahmad, "*Acunetix – Web Vulnerability Scanner*", tersedia : 22 Maret 2018, http://fathihadi.net/acunetix-web-vulnerability-scanner/, Juni 2011.

[HAN09] Hantoro, G. D., "*WiFi (Wireless LAN) Jaringan Komputer Tanpa Kabel*", Bandung: Informatika, 2009.

[HER16] Heriyanto, Tedi, "*Panduan Refensi Nmap (Man Page, bahasa Indonesia)*", tersedia : 15 Maret 2018, https://nmap.org/man/id/index.html, Mei 2016.

[IND17] Indonesia Network Information Center (IDNIC), "*Panduan Whois*", tersedia : 12 Maret 2018, https://idnic.id/layanan/whois, Mei 2017.

[KEL95] Kelleher, Kevin, Casey G., Lois D., et al, "*Cause and Effect Diagram : Plain and Simple*", Joiner Associates Inc USA, 1995.

[MES16] Messier, R., "*Penetration Testing Basics*", USA: Apress, 2016.

[MUH15] Muhsin, M., & Fajaryanto, A., "*Penerapan Pengujian Keamanan Web Server Menggunakan Metode OWASP versi 4* (*Studi Kasus Web Server Ujian Online*)", Multitek Indonesia, 2015.

[NAB14] Nababan, I. M., "*Pendeteksi Celah Keamanan Pada Aplikasi Web Dengan Penetration Testing Menggunakan Data Validation Testing*", Skripsi Universitas Sumatera Utara, 2014.

[NAS16] Nashir, Muhammad, "*Celah (Lubang) Keamanan, Materi Kuliah Keamanan dan Administrasi Jaringan Komputer Politeknik Aceh Selatan* (*POLTAS*)", tersedia : 20 Oktober 2016, http://mrnashir.blogspot.co.id/2016/05/celah-lubang-keamanan-materi-kuliah.html, Mei 2016.

[NET17] Net Square, "*httprint*", tersedia : 18 Maret 2018, http://www.net-square.com/httprint.html, April 2017.

[NIR15] Nirmalasari, I., Irwansyah, & Agustini, E. P., "*Penetration Testing Pada Portal Website Kota Lubuklinggau*", Jurnal Informatika Universitas Bina Darma, 2015.

[POS18] Posciety, "*Pengertian, Jenis, Contoh & Syntax DNS Records*", tersedia : 12 Maret 2018, https://www.posciety.com/macam-macam-jenis-dns-records-syntax-lengkap/, Mei 2018.

[PUR14] Purnawan, A., "*Studi dan Implementasi Keamanan Website Menggunakan Open Web Application Security Project (OWASP) Studi Kasus : PLN Batam*", Jurnal Tugas Akhir Informatika Universitas Pasundan, 2014.

[STO17] Stock, A. V. D., Glas, B., Smithline, N., & Gigler, T., "*OWASP Top 10 – 2017 The Ten Most Critical Web Application Security Risks*", USA: The OWASP Foundation, 2017.

[TEK17] Teknik Informatika Universitas Pasundan, "*Program Studi*", tersedia : 27 Agustus 2017, https://if.unpas.ac.id/, Agustus 2017.

[ZAM11] Zam, E. Z., "*Buku Sakti Hacker*", Jakarta: Mediakita, 2011.

[ZAM14] Zam, E. Z., "*Cara Mudah Membuat Jaringan Wireless*", Jakarta: PT Elex Media Komputindo, 2014.