Analisis Keamanan Pendaftaran Akun Wi-Fi Pada Website Captive Portal

Muhamad Ridwan Fauzan[1)], Rita Rijayanti[2)]
Universitas Pasundan
Jln. Dr. Setiabudhi no. 193, Bandung, 40153
e-mail: ridwan.fauzan@mail.unpas.ac.id, rita.rijayanti@unpas.ac.id

Abstrak

Kesadaran dan kewaspadaan mengenai keamanan informasi terhadap aplikasi harus diterapkan oleh perusahaan atau organisasi, terutama terhadap informasi yang bersifat rahasia. Akan tetapi dalam pendaftaran akun wi-fi di website hotspot unpas terdapat suatu celah, baik itu dari integrasi data maupun bug pada program sehingga dibutuhkan keamanan informasi. Keamanan informasi perlu diterapkan untuk menjaga kerahasiaan data, agar data tidak dapat diubah oleh orang yang tidak berwenang dan data dapat diakses bila dibutuhkan. Penelitan ini menggunakan OWASP sebagai acuan untuk mengembangkan tingkat keamanan sebuah aplikasi dengan tahapan mempelajari literatur, analisis kebutuhan dan analisis kode program serta alur data. Hasil dari penelitian ini berupa rekomendasi peningkatan keamanan pendaftaran akun wi-fi pada *website captive portal.*

Kata kunci: *keamanan informasi, OWASP, C.I.A, Website Hotspot, analisis keamanan*

1. Pendahuluan

Pendaftaran akun *wi-fi* adalah salah satu fitur dari sebuah *website captive portal* yang menggunakan konsep SDN atau dikenal dengan *Software Defined Networking* yang merupakan sebuah pola pikir dimana sebuah pusat perangkat lunak, yang disebut *controller*, menentukan keseluruhan tingkah laku jaringan [1]. *Captive Portal* telah menjadi sebuah penelitian untuk menyaring pengguna internet dimana *captive portal* merupakan sebuah *router* atau *gateway* untuk tidak memperbolehkan *traffic* untuk lewat sampai pengguna mempunyai konfirmasi otentikasi dirinya sendiri [2].

Pada studi kasus yang diambil di Laboratorium Teknik Informatika Universitas Pasundan, teknologi *captive portal* sudah bertahun-tahun digunakan untuk membatasi penggunaan internet terhadap pengguna karena institusi ini hanya mengizinkan masyarakat pasundan yang dapat menggunakan layanan internet. *Captive portal* yang digunakan di Laboratorium Teknik Informatika Universitas Pasundan menggunakan *wi-fi* sebagai media akses internet untuk efisiensi, dikarenakan jumlah pengguna yang sangat banyak sehingga penggunaan kabel LAN (*Local Area Network*) tidak dipilih sebagai media akses internet pada jaringan terbuka dan hanya digunakan dibagian internal.

Akan tetapi, dengan teknologi baru yang diterapkan pada *captive portal* yang menggunakan konsep SDN pada pendaftaran akun *wi-fi* menjadi sebuah ancaman baru untuk membobol sistem seperti duplikasi akun yang menyebabkan pengguna dapat menggunakan lebih dari satu akun *wi-fi* ataupun terdapat kesalahan dalam sebuah program (*bug*) yang dibuat menyebabkan penyaringan *bandwidth* yang diharuskan ke Teknik Teknik Informatika dapat digunakan oleh jurusan lain.

Berdasarkan paparan diatas, disimpulkan untuk memberikan peningkatan keamanan dari sistem pendaftaran akun *wi-fi* pada *website captive portal* sehingga menghasilkan rekomendasi peningkatan keamanan pendaftaran akun *wi-fi* pada *website captive portal* untuk diterapkan pada modul keamanan pendaftaran akun *wi-fi*.

2. Metode Penelitian

Metode Penelitian memberikan penjelasan tentang langkah-langkah, data, lokasi penelitian, metode evaluasi yang digunakan serta penjelasan terstruktur tentang algoritma atau metode dari penelitian yang dibahas.

2.1 Metodologi Penelitian

Pada bagian ini menjelaskan tahapan-tahapan pengerjaan terkait penelitian analisis keamanan pendaftaran akun *wi-fi* pada *website captive portal*. Pada tahap pertama, yang dilakukan adalah membaca beberapa studi literatur untuk mengumpulkan seluruh informasi dan mempelajari materi serta sumber-

sumber data yang terkait dengan keamanan pendaftaran akun *wi-fi* pada *website captive portal*. Pada tahap kedua, melakukan analisis kebutuhan pendaftaran akun *wi-fi* yang dibutuhkan untuk meningkatkan keamanan pada pendaftaran akun *wi-fi*. Tahap terakhir, melakukan analisa kode program dan alur pengiriman data berdasarkan standar keamanan aplikasi web yaitu OWASP.

2.2 Landasan Teori

Pada bagian ini berisi definisi-definisi, teori-teori serta konsep dasar yang diperlukan untuk menganalisa situasi yang diteliti.

2.2.1 Keamanan Informasi

Keamanan informasi adalah sebuah praktek untuk melindungi informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi, inspeksi, rekaman atau kehancuran [3]. Keamanan informasi terdapat 3 prinsip dasar, yaitu : *Confidentiality, Integrity* dan *Availability*. *Confidentiality* atau kerahasiaan adalah sebuah property, dimana informasi yang tidak tersedia atau diungkapkan kepada individu yang tidak sah, entitas atau proses [3]. *Integrity* atau integritas berarti menjaga dan menjamin akurasi dan kelengkapan data melalui seluruh siklus hidup. Yang berarti bahwa data tidak dapat dimodifikasi secara tidak sah atau tidak terdeteksi [3]. *Avaibility* atau ketersediaan dibutuhkan untuk setiap sistem informasi agar melayani tujuan, informasi harus tersedia saat dibutuhkan. Yang mana sistem komputasi yang digunakan untuk menyimpan dan memproses informasi, kontrol keamanan yang digunakan untuk melindunginya dan saluran komunikasi yang digunakan untuk mengaksesnya harus berfungsi dengan benar [3].

2.2.2 Wi-Fi

Wi-Fi merupakan sebuah nama yang diberikan oleh *Wi-Fi Alliance* terhadap standar rangkaian IEEE 802.11. Pada dasarnya *Wi-Fi* adalah sebuah transmisi sinyal radio dan 802.11 didefinisikan sebagai standar untuk *Wireless Local Area Networks* (WLANs) [4].

2.2.3 MikroTik RouterOS

MikroTik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi *router network* yang handal, mencakup berbagai fitur yang dibuat untuk IP *Network* dan jaringan *wireless*, cocok digunakan oleh ISP dan provider *hotspot* [5].

2.2.4 Website

Website atau *web* merupakan serangkaian halaman-halaman, tiap halaman *web* mempunyai alamat unik tersendiri yang mana ketika masuk ke sebuah *web browser* akan dipindahkan ke halaman yang dituju secara langsung. Kebanyakan alamat *web* dimulai dengan kata www (*World Wide Web*) [6]. Sekelompok halaman terkait tersebut dinamakan *website* dan semua alamat dari seluruh halaman dalam *website* tersebut akan dimulai dengan nama alamat yang sama [6].

2.2.5 PHP HyperText Preprocessor

PHP adalah *open source* yang secara luas digunakan, umumnya dirancang untuk penggunaan dalam pengembangan *website*. PHP dibuktikan sangat berguna dan terkenal, sehingga bertambah besar dan menjadi bahasa yang penuh dengan fitur sampai sekarang ini, dengan mendapatkan nama *PHP HyperText Preprocessor* dan berjalan dalam mengembangkan kemampuannya dalam memproses halaman *web* sebelum ditampilkan [7].

2.2.5 Captive Portal

Captive Portal merupakan suatu teknik yang membuat pengguna pada suatu jaringan harus melalui satu halaman *web* khusus, (umumnya untuk otentikasi) sebelum dapat mengakses internet. *Captive Portal* memanfaatkan *web browser* sebagai sarana atau perangkat otentikasi yang aman dan terkendali [8]. *Captive Portal* pada umumnya digunakan sebagai halaman *login* yang kemungkinan membutuhkan otentikasi, pembayaran, persetujuan penggunaan atau tanda pengenal yang telah sah dan disetujui oleh kedua belah pihak yaitu pengguna dan *host*.

2.2.6 CodeIgniter

CodeIgniter adalah sebuah *framework* PHP. *Framework* itu sendiri adalah suatu kerangka kerja yang berupa sekumpulan *folder* yang memuat berkas-berkas php yang menyediakan *class libraries, helpers* dan lain-lain. *Framework* menyediakan konfigurasi dan teknik *coding* tertentu. CodeIgniter atau CI

menerapkan pola MVC fleksibel, karena model dapat tidak digunakan. Konsep MVC adalah konsep pemisahan antara *logic* dengan tampilan dan *database* [9].

2.2.7 Software Defined Networking

Software Defined Networking atau dikenal SDN adalah sebuah pendekatan baru dalam jaringan yang memberikan operator jaringan dan pemilik dalam mengontrol lebih dalam infrastruktur, mendukung optimasi, kustomisasi dan virtualisasi yang memungkinkan pembuatan tipe baru dari layanan jaringan. Seperti layanan jaringan baru mempunyai kemampuan untuk membuat model bisnis baru, produk dan layanan, yang mana mengurangi modal dan biaya operasional [10].

2.2.8 OWASP

OWASP (*The Open Web Application Security Project*) merupakan sebuah organisasi non-profit di dunia yang memfokuskan pada pengembangan keamanan pada aplikasi. Dalam misinya untuk membuat keamanan aplikasi lebih terlihat, sehingga perseorangan atau organisasi dapa membuat keputusan yang tepat.

2.2.9 Application Security Verification

Standar OWASP yang digunakan pada penelitian adalah *Application Security Verification Standard* 3.0, yang lebih memfokuskan pada bagian autentikasi. Autentikasi adalah sebuah tindakan membangun atau konfirmasi, sesuatu (atau seseorang) sebagai otentik, yaitu bahwa klaim yang dilakukan oleh sesuatu yang benar [11].

2.3 Identifikasi Kebutuhan

Identifikasi kebutuhan digunakan untuk mengidentifikasi kebutuhan apa saja yang dibutuhkan bagi sistem. Identifikasi kebutuhan didapatkan dari hasil wawancara dengan bagian *IT Support* di laboratorium teknik informatika berupa permasalahan-permasalahan yang didapatkan dari hasil implementasi sistem pendaftaran akun *wi-fi*.

2.4 Analisis Kode Program dan Alur Data Pendafaran Akun Wi-Fi

Analisis kode program dibutuhkan untuk mengidentifikasi kode program yang menjadi sebuah *bug* dari program. Alur data dibutuhkan untuk memahami alur pengiriman data dari aplikasi ke perangkat MikroTik sehingga dapat diidentifikasi masalah yang terjadi pada sistem pendaftaran akun *wi-fi*.

3. Hasil dan Pembahasan

Pada bagian ini berisi hasil dari bahasan-bahasan penelitian yang didapatkan dari identifikasi kebutuhan dan analisis kode program dan alur data pendaftaran akun *wi-fi*.

3.1 Hasil Identifikasi Kebutuhan

Dari hasil identifikasi kebutuhan yang didapatkan dari wawancara dengan bagian *IT Support* di laboratorium teknik informatika didapatkan permasalahan seperti masyarakat pasundan yang mendaftar masuk akun *wi-fi* terdapat kesalahan pada program yang menyebabkan penggunaan *bandwidth* yang tidak sesuai grup dari penggunaan *bandwidth* yang telah ditentukan. Kemudian terdapat masyarakat pasundan yang tidak dapat melakukan pendaftaran akun *wi-fi* dikarenakan tidak terdapat integrasi dengan data masyarakat pasundan.

3.2 Hasil Analisis Kode Program dan Alur Data Pendaftaran Akun Wi-Fi

Sistem pendaftaran akun *wi-fi* pada *website captive portal* merupakan solusi alternatif dalam mendaftarkan akun-akun *wi-fi* dengan mudah oleh pengguna yang nantinya data tersebut akan dikirimkan kedalam sistem *router* MikroTik tanpa bantuan operator jaringan. Sistem pendaftaran akun *wi-fi* dibangun dengan basis *web* sehingga dapat digunakan dimana saja dan dalam pembangunan aplikasi pendaftaran akun *wi-fi* menggunakan sebuah *framework website* berbahasa pemrograman PHP yaitu CodeIgniter.

Dalam mengembangkan aplikasi pendaftaran akun *wi-fi*, pengembang aplikasi membutuhkan pemahaman tentang SDN atau dikenal *Software Defined Networks* untuk mengetahui alur pengiriman data dari aplikasi ke sistem perangkat MikroTik. Dikarenakan sebelum mengirim data, sistem aplikasi diharuskan terkoneksi terlebih dahulu ke sistem MikroTik dan setelah terhubung maka aplikasi dapat memanipulasi data yang terdapat pada sistem MikroTik.

3.3 Rekomendasi Keamanan Pendaftaran Akun Wi-Fi Pada Website Captive Portal

Rekomendasi keamanan pendaftaran akun *wi-fi* pada *website captive portal* dapat digunakan untuk meningkatkan keamanan pendaftaran akun *wi-fi* sehingga dapat sesuai dengan standar keamanan internasional OWASP. Rekomendasi keamanan pendaftaran akun *wi-fi* digambarkan dengan bentuk tabel yang didapatkan dari hasil identifikasi kebutuhan dan hasil analisis kode program dan alur data pendaftaran akun *wi-fi*. Tabel *Authentication Verification Requirements* didapatkan dari standar keamanan internasional yang telah didefinisikan oleh OWASP pada bagian *Application Security Verification* yang memfokuskan pada otentikasi, sehingga setelah diidentifikasi maka didapatkan beberapa rekomendasi dari poin-poin yang telah didefinisikan. Untuk membaca tabel rekomendasi keamanan pendaftaran akun *wi-fi* dijelaskan deskripsi dan dengan tiga tingkatan yaitu :

Pada tingkat 1, komponen dari aplikasi telah diidentifikasi dan mempunyai alasan untuk digunakan pada aplikasi.

Pada tingkat 2, komponen telah didefisinisikan dan kode telah ditanam pada komponen aplikasi.

Pada tingkat 3, komponen dan rancangan aplikasi telah dipasang pada lingkungan teknik informatika unpas, telah digunakan dan efektif.

Tabel 1. *Authentication Verification Requirements*

#	Deskripsi	1	2	3
2.1	Verifikasi halaman dan sumber daya membutuhkan autentikasi kecuali yang spesifik dikhususkan untuk public	v	v	v
2.2	Verifikasi semua kolom kata sandi tidak menampilkan kata sandi pengguna ketika dimasukan.	v	v	v
2.4	Verifikasi semua kontrol autentikasi dilakukan di bagian server.	v	v	v
2.6	Verifikasi semua pengamanan pengelolaan autentikasi yang gagal untuk memastikan penyerang tidak dapat masuk.	v	v	
2.7	Verifikasi inputan kata sandi diperbolehkan, atau didorong, menggunakan *passphrases*, dan tidak mencegah *passphrases* yang panjang/ kata sandi yang sangat kompleks dimasukan.	v		
2.8	Verifikasi seluruh fungsi autentikasi identitas akun (seperti halaman ubah profil, lupa kata sandi, menon-aktifan / token hilang, helpdesk atau IVR) berkemungkinan mendapatkan akses kedalam akun yang setidaknya tahan terhadap serangan sebagai mekanisme autentikasi utama.	v	v	
2.9	Verifikasi fungsi perubahan kata sandi termasuk kata sandi lama, kata sandi baru, dan konfirmasi kata sandi.	v		
2.12	Verifikasi seluruh keputusan autentikasi yang mencurigakan dibuatkan pencatatan. Termasuk permintaan dengan metadata yang relevan yang dibutuhkan untuk investigasi keamanan.	v		
2.13	Verifikasi bahwa kata sandi akun menggunakan kekuatan enkripsi yang mencukupi untuk bertahan dari serangan brute force.	v		
2.16	Verifikasi surat pengenal dikirim menggunakan link enkripsi yang cocok dan seluruh halaman atau fungsi yang membutuhkan surat pengenal pengguna menggunakan link enkripsi.	v		
2.17	Verifikasi bahwa fungsi lupa kata sandi dan dan fitur lain untuk pengembalian data tidak memperlihatkan kata sandi baru dan kata sandi baru tersebut tidak secara langsung terlihat dalam teks yang jelas kepada pengguna.	v	v	
2.18	Verifikasi pencacahan informasi tidak dapat digunakan lewat login, reset kata sandi, atau fungsi lupa kata sandi	v		
2.19	Verifikasi bahwa tidak ada kata sandi default yang digunakan pada framework aplikasi atau komponen lain yang digunakan (seperti “admin/password”)	v		
2.20	Verifikasi bahwa pencegahan pengiriman telah dilakukan untuk mencegah penyerangan autentikasi otomatis biasa seperti serangan bruteforce atau peniadaan layanan.	v		
2.21	Verifikasi bahwa seluruh autentikasi surat pengenal untuk mengakses layanan eksternal pada aplikasi telah terenkripsi dan disimpan dalam lokasi yang dilindungi.	v		
2.22	Verifikasi bahwa lupa kata sandi dan fitur yang sama menggunakan token, push mobile, atau mekanisme offline recovery.			

4. Simpulan

Kesimpulan dari penelitian ini adalah terdapat dua belas poin arsitektur dan rancangan yang belum ditempatkan pada aplikasi dan sembilan poin yang belum ditanam kode dan didefinisikan pada arsitektur. Sehingga hasil analisis ini dapat digunakan pada pengembangan selanjutnya agar aplikasi setidaknya lebih aman dari sebelumnya. Hasil dari analisis ini juga sebenarnya dapat digunakan tidak hanya pada lingkup kampus saja akan tetapi dapat juga diterapkan pada akses poin - akses poin yang bertebaran di daerah bandung untuk meningkatkan layanan pemerintahan kota bandung dalam hal layanan akses internet.

Ucapan Terimakasih

Ucapan terimakasih disampaikan kepada jurusan Teknik Informatika dan Fakultas Teknik Universitas Pasundan Bandung baik dalam bentuk fasilitas dan peralatan yang telah banyak membantu bagi keberhasilan dan kelancaran kegiatan penelitian.

Daftar Pustaka

[1] Hyoujoon Kim, Nick Feamster. *Improving Network Management with Software Defined Networking*. 2013.
[2] Choi, J., dkk. *Secure MAC-Layer Protocol for Captive Portals in Wireless Hotspots*. *IEEE ICC*. 2011;
[3] Whitman, Michael E, Herbert J.Mattord. *Principle of Information Security*. Vol: 4. *Course Technology*. 2012
[4] RABBIT. *An Introduction to Wi-Fi.* Digi International Inc. 2008
[5] Prasetyo, Helmi, Herika H, Sri Puji U. Modul Workshop Mikrotik Dasar : Pengenalan Mikrotik dan Perintah – perintah Dasar. Universitas Yarsi. 2014
[6] Ireland Failte. *Introduction to the Web.* 2013
[7] Valade Janet. PHP 5 *For Dummies*. Willey Publishing. 2004
[8] Astri Elisabeth D.S. Analisis Autentikasi pada Captive Portal. Universitas Kristen Satya Wacana. 2013
[9] Sofwan Akhmad. Belajar PHP dengan *Framework Code Igniter.* Komunitas e-Learning IlmuKomputer.com. 2017
[10] Nadeau, T.D, Gray K. SDN – *Software Defined Networks*. Beijing.O'Reilly Media Inc. 2013.
[11] OWASP. *Application Security Verification Standard 3.0,* 2015