Jurnal Integrasi
Vol. 9 No. 1, April 2017, 35-47
e-ISSN: 2548 - 9828

Article History
Received March, 2017
Accepted April, 2017

Manajemen Risiko Ancaman pada Aplikasi *Website* Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE

Fernando Reza Destrianto[1], Nelmiawati[2] dan Maya Armys Roma Sitorus[3]

[1,2,3] Politeknik Negeri Batam

Program Studi Teknik Multimedia dan Jaringan

Jalan Ahmad Yani, Batam Center, Batam 29461, Indonesia

E-mail: fernandoreza18@gmail.com, mia@polibatam.ac.id, maya.sitorus@polibatam.ac.id

Abstrak

Aplikasi *website* merupakan layanan informasi yang sering digunakan oleh pengguna Internet saat ini. Salah satu aplikasi *website* yang digunakan di Politeknik Negeri Batam saat ini yaitu Sistem Informasi Akademik (SIA). SIA digunakan untuk menyimpan berbagai macam informasi berupa catatan, nilai dan biodata diri mahasiswa dan dosen. Informasi ini sangat penting digunakan dalam berbagai aktivitas akademik. Sehingga kebutuhan terhadap identifikasi risiko dan manajemen risiko dari ancaman pada SIA perlu dilakukan untuk mengamankan informasi sensitif tersebut. Penelitian ini bertujuan untuk melakukan pengujian keamanan dan manajemen risiko ancaman yang terjadi pada SIA dengan menggunakan metode OCTAVE. Berdasarkan Open Web Application Security Project (OWASP), OCTAVE merupakan sebuah metode dalam manajemen risiko secara sistematik dengan melakukan pengidentifikasian risiko. Metode ini bertujuan untuk menyediakan tahapan dalam mengelola risiko terhadap ancaman yang telah ditemukan. Hasil yang diperoleh menemukan bahwa terdapat 4 kategori ancaman terhadap SIA berupa otentikasi, enkripsi, manajemen sesi dan manajemen konfigurasi. Oleh karena itu, kategori tersebut dapat digunakan oleh UPT-SI Politeknik Negeri Batam sebagai bentuk tindakan pencegahan terhadap kelemahan yang terdapat pada SIA.

Kata kunci: Manajemen Risiko, Ancaman, Metode OCTAVE, *Website,* Sistem Informasi Akademik

Abstract

Website application is an information services used by the Internet users today. One of the application used in Politeknik Negeri Batam is Academic Information System (SIA)*. It is used to keep several informations such as a record, grade and biographical data of students and lecturers. These information is very important used in the academic activities. So that, the needs of risk identification and risk management of threats on* SIA *are necessarily to be done to secure the sensitive information. This research is aim to to test the safety and risk management threats that occur at* SIA *by using* OCTAVE*. Based on the Open Web Application Security Project* (OWASP)*, OCTAVE is a method in managing risk systematically through an identifying the risk. The intention of this method is to provide a stage in managing the risk towards threats that have been found. The results obtained that there are 4 categories of threats found in SIA, such as authentication, encryption, session management and configuration management. Therefore, the categories can be used by* UPT-SI Politeknik Negeri Batam *as a preventive against vulnerability found in* SIA*.*

Keywords: Threat Risk Management,* OCTAVE *Method, Website Application, Academic Information System

1. PENDAHULUAN

Sistem informasi saat ini memiliki peranan penting terhadap perusahaan atau institusi. Hal ini penting agar dapat menghasilkan kemudahan saat menyebarkan informasi mengenai perusahaan, organisasi atau institusi tersebut. *Website* merupakan salah satu layanan informasi yang banyak diakses oleh pengguna Internet di dunia [1]. Sebagai salah satu layanan informasi maka *website* perlu dibangun agar mampu menangani permintaan pengguna dengan baik. Penanganan *website* yang baik penting adanya agar dapat menutup celah kemanan sehingga *website* dapat diakses tanpa adanya gangguan. Gangguan baik berupa internal ataupun eksternal dari sebuah perusahaan atau institusi.

Dengan adanya celah keamanan pada *website* membuat seorang *hacker* (peretas) mampu merubah atau mengambil informasi yang tidak seharusnya bisa dibaca oleh orang yang tidak memiliki hak akses. Seperti kasus yang terjadi pada 8 Februari 2015 lalu, dimana seorang mahasiswa Politeknik Negeri Batam masuk kedalam *website* Sistem Informasi Akademik (SIA) [2]. Kasus lainnya pada April 2015, salah satu sistem keamanan yang ada di White House telah di bobol seorang *hacker* dan tujuan utama *hacker* tersebut adalah untuk mengambil informasi rahasia yang dimiliki oleh Amerika Serikat [3].

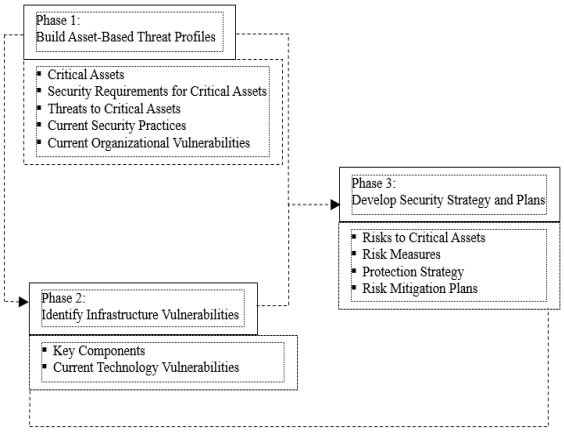
Berdasarkan kasus pembobolan yang dilakukan salah satu mahasiswa Politeknik Negeri Batam, ini membuktikan bahwa *website* SIA masih memiliki celah keamanan sehingga celah keamanan ini menjadi kelemahan pada *website* yang ada di Politeknik Negeri Batam. Dengan adanya kelemahan ini memungkinkan mahasiswa dapat memanfaatkan kelemahan sistem ini untuk melakukan aksi-aksi lainnya. Oleh karena itu, perlu adanya analisis risiko ancaman yang terjadi pada aplikasi *website* SIA. Menurut OWASP (*Open Web Application Security Project*), salah satu metode yang dapat digunakan untuk melakukan manajemen risiko terhadap ancaman pada aset aplikasi sebuah *website* adalah OCTAVE [4].

Berdasarkan hal tersebut, maka dalam penelitian ini dilakukan identifikasi ancaman, analisis ancaman dan manajemen risiko terhadap ancaman yang terjadi pada aplikasi *website* SIA Politeknik Negeri Batam.

2. LANDASAN TEORI

Metode OCTAVE

Metode Octave (*Operationally Critical Threat, Asset and Vulnerability Evaluation*) merupakan sebuah teknik dan metode yang digunakan sebagai kerangka kerja yang dapat mengidentifikasi, menganalisa dan mengawasi pengelolaan risiko keamanan informasi berdasarkan pengidentifikasian risiko [5].



Gambar 1: Alur Kerja Metode Octave

(*Sumber: Octave Criteria Version 2.0, Software Engineering Institute, Carnegie Mellon University*)

1. Fase 1

   Fase ini merupakan tahap dalam mengidentifikasi aset yang dianggap kritis dan berpotensi memiliki ancaman. Dimulai dengan mengklasifikasikan aset yang penting bagi organisasi. Proses yang dikerjakan pada fase ini adalah identifikasi aset kritis, identifikasi ancaman aset kritis, identifikasi keamanan yang sedang digunakan dan identifikasi kelemahan aset kritis.

2. Fase 2

   Fase ini merupakan tahap mengidentifikasi kelemahan pada teknologi yang digunakan. Proses yang dikerjakan pada fase ini adalah identifikasi komponen utama dan kelemahan teknologi yang ada saat ini.

3. Fase 3

   Fase ketiga ini merupakan tahap akhir dari metode OCTAVE. Proses yang dikerjakan adalah identifikasi risiko pada aset yang ditemukan, membuat strategi perlindungan dan rencana mitigasi risiko.

OWASP

Open Web Application Security Project (OWASP) merupakan proyek *open source* yang dibangun untuk menemukan penyebab dari tidak amannya sebuah *software* atau aplikasi *website* dan menemukan cara menanganinya [6].

Hal – hal yang bisa ditemukan di OWASP antara lain:

a. *Tool* dan standar keamanan aplikasi.
b. Buku yang membahas mengenai uji keamanan aplikasi *website*, pengembangan kode keamanan dan *review* kode keamanan.
c. Kendali keamanan.
d. Riset terbaru dan lainnya.

Keamanan Sistem Informasi

1. Komponen Keamanan Sistem Informasi

   Komponen keamanan informasi secara umum terdiri atas 6 komponen yaitu:

   a. *Physical Security* merupakan keamanan informasi yang befokus pada aset fisik.
   b. *Personal Security* merupakan keamanan informasi yang berkaitan dengan keamanan personil.
   c. *Operation Security* merupakan keamanan yang berkaitan dengan kegiatan operasional.
   d. *Communication Security* merupakan keamanan yang berkaitan dengan jalur komunikasi dan teknologi komunikasi.
   e. *Network Security* merupakan keamanan yang berkaitan terhadap jaringan dan data.
   f. *Information Security* merupakan keamanan yang berkaitan terhadap informasi.

2. Aspek Keamanan Sistem Informasi

   Keamanan informasi memiliki lima aspek utama yaitu *privacy, identification, authentication, authorization,* dan *accountability* [7]. *Privacy* memberikan jaminan kerahasiaan data dari pemilik informasi. *Identification* merupakan langkah awal untuk memperoleh hak akses kedalam sistem yang diamankan. *Authentication* merupakan proses yang dilakukan sistem dengan membuktikan bahwa pengguna merupakan orang yang benar. *Authorization* merupakan jaminan yang diberikan sistem bahwa pengguna mendapatkan hak untuk mengakses. *Accountability* merupakan proses yang dilakukan sistem dengan memberikan log data semua aktifitas yang telah dilakukan.

   Dari kelima elemen tersebut aspek informasi dapat diklasifikasikan kedalam tiga aspek utama yaitu *Confidentiality, Integrity* dan *Availability* [8]. *Confidentiality* merupakan aspek yang menjamin kerahasiaan data atau informasi, dengan menjamin informasi hanya bisa digunakan oleh pengguna yang berhak. *Integrity* merupakan aspek yang menjamin bahwa data tidak bisa diganti oleh pengguna yang tidak berhak sehingga keutuhan data tetap terjaga. *Availability* merupakan aspek yang menjamin data bisa digunakan setiap saat.

Ancaman Keamanan Sistem Informasi

Ancaman merupakan setiap peristiwa yang akan memberikan dampak terhadap sistem sehingga membuat hilangnya aspek *confidentiality, integrity* dan *availability* [9]. Menurut S. Janner, ada sepuluh kategori ancaman pada aplikasi *website* yang menjadi kelemahan pada aplikasi *website.* Hal ini berupa: *input validation, authentication, authorization, configuration management, sensitive data, session management, cryptography, parameter manipulation, exception management* dan *auditing and logging* [10].

Pengujian Keamanan pada *Website*

Berdasarkan standar yang dikeluarkan oleh OWASP terdapat sebelas langkah yang dapat dilakukan untuk menilai dan menguji keamanan pada sebuah *website* [11]:

1. *Information gathering.*
2. *Configuration management.*
3. *Secure transmission.*
4. *Authentication.*
5. *Session management.*
6. *Authorization.*
7. *Cryptography.*
8. *Data validation.*
9. *Denial of service.*
10. *Specific risky functionality.*
11. *Error handling.*

MITM

Man-in-the-Middle (MITM) *Attacks* merupakan sebuah metode serangan yang dilakukan oleh penyerang dengan menjadi perantara antara komunikasi komputer pengguna dan komputer tujuan [12]. Konsep serangan yang dilakukan oleh MITM adalah dengan meyakinkan dua *host* bahwa tidak ada komputer lain berada diantara mereka, dimana ada host lain yang berada ditengahnya [13]. Contoh penerapan MITM dalam jaringan adalah terdapat koneksi TCP antara *klien* dan *server*. Dengan menerapkan konsep MITM, penyerang membagi koneksi TCP asli menjadi dua koneksi baru. Koneksi pertama antara klien dan penyerang, sedangkan koneksi kedua antara penyerang dan *server.* Setelah koneksi dicegat, penyerang bertindak sebagai *proxy* dimana penyerang dapat membaca, memasukkan dan memodifikasi data dalam komunikasi yang disadap. Metode MITM tidak hanya menjadi sebuah metode penyerangan, namun dapat digunakan sebagai penilaian kerentanan aplikasi *website* pada tahap pengembangan.

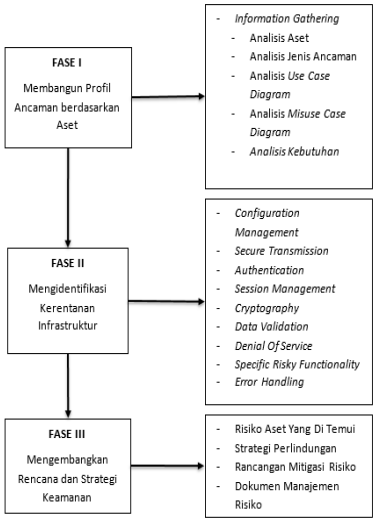
Sniffing

Sniffing atau pengendusan data merupakan metode serangan dengan mengendus data atau menyadap data pada lalu lintas sebuah jaringan komputer. Proses *sniffing* dibagi menjadi dua yaitu *sniffing* pasif dan *sniffing* aktif. *Sniffing* pasif merupakan kegiatan penyadapan data tanpa mengubah data maupun paket data yang ada di jaringan. Sementara, s*niffing* aktif merupakan kegiatan atau tindakan yang dilakukan penyerang dengan mengubah paket data yang berada di jaringan [12].

3. ANALISIS DAN PERANCANGAN

3.1 Proses Analisis

Proses penelitian yang dilakukan pada *website* SIA Politeknik Negeri Batam menggunakan metode OCTAVE disajikan pada Gambar 2.



Gambar 2: Proses Analisis SIA

1. Analisis Aset Informasi SIA

Aset yang ditemukan berdasarkan pengamatan pengguna pada aplikasi *website* SIA adalah sebagai berikut:

a. *Username* dan *password*.
b. Dokumen pribadi (foto pengguna, foto KTP, foto akta, foto ijazah SMA sederajat).
c. Data pribadi mahasiswa (biodata diri).
d. Kuesioner.
e. Krs.
f. Data nilai mahasiswa.
g. Informasi terbaru.

Analisis Jenis Ancaman

Jenis ancaman yang bisa terjadi pada aset aplikasi *website* dan pengaruhnya terhadap aspek keamanan CIA (*Confidentiality, Integrity* dan *Availability*) dari aplikasi *website* SIA berdasarkan standar keamanan aplikasi *website* yang ditetapkan oleh [11] dan [14] disajikan pada Tabel 1.

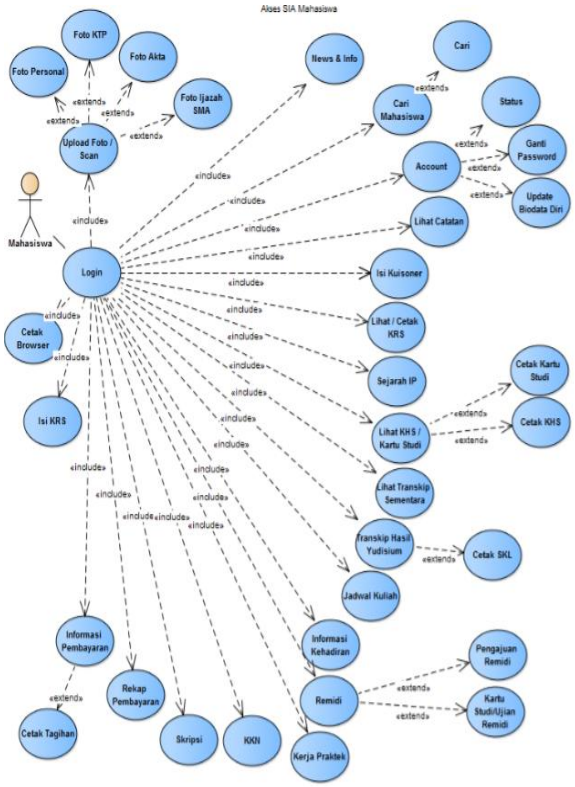
Tabel 1: Jenis Ancaman pada SIA

No	Aset	Kategori Ancaman	Jenis Ancaman	C	I	A
1	*Username* dan *password*	Otentikasi	*Cookie Replay*	V	V	
			Sniffing	V	V	
			Dictionary Attack	V	V	
2	Dokumen pribadi mahasiswa	Validasi Masukan	*Missing proper validation of file name*	V	V	
			Missing proper validation of file content and size	V	V	
3	Data pribadi mahasiswa	Validasi Masukan	*SSI Injection*	V	V	V
			SQL Injection	V	V	V
4	Krs	Manajemen Konfigurasi	*Clickjacking vulnerability*		V	V
5	Kuisoner	Manajemen Konfigurasi	*Clickjacking vulnerability*	V	V	V
6	Data Nilai Mahasiswa	Otorisasi	*Data Tampering*		V	
			Elevation of privilege		V	
7	Informasi terbaru	Otorisasi	*Data Tampering*		V	V
			Elevation of privilege		V	V

Keterangan : C = *Confidentiality*, I = *Integrity* dan A = *Availability*.

2. Analisis *Use Case* Diagram SIA

Berdasarkan pengamatan pengguna, didapatkan *use case* diagram mahasiswa yang menggunakan aplikasi *website* SIA. *Use case* tersebut disajikan pada Gambar 3.

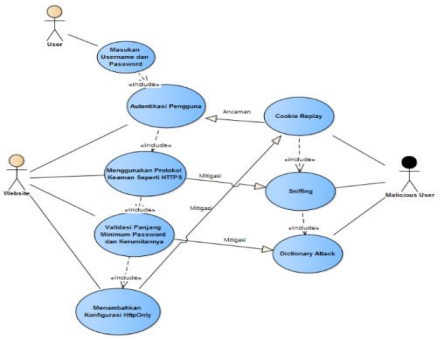


Gambar 3: *Use Case* Diagram SIA

3. Analisis *Misuse Case* Diagram SIA

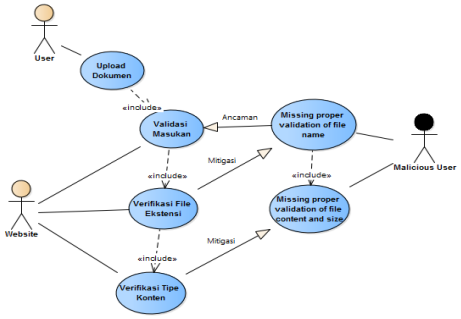
Terdapat beberapa skenario penyerangan yang akan terjadi pada SIA [15].

a. Percobaan *login*



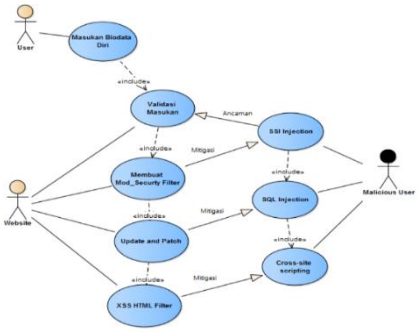
Gambar 4: *Misuse Case Login*

b. Percobaan *upload* dokumen



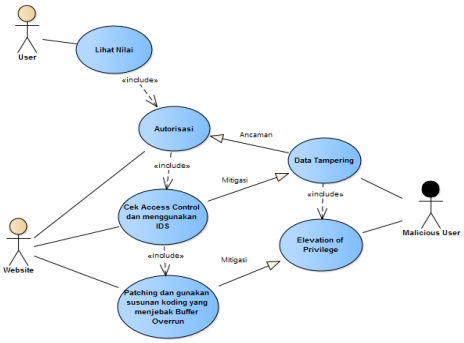
Gambar 5: *Misuse Case Upload*

c. Percobaan isi biodata diri dan ganti *password*



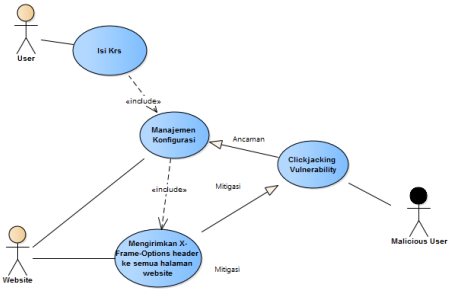
Gambar 6: *Misuse Case* Isi Biodata dan Ganti *Password*

d. Percobaan mengganti nilai mahasiswa dan informasi



Gambar 7: *Misuse Case* Mengganti Nilai Mahasiswa dan Informasi

e. Percobaan mengisi krs dan kuesioner



Gambar 8: Misuse Case Mengisi Krs dan Kuisoner

3.2 Perancangan Pengujian Keamanan *Website*

3.2.1 Pencarian Informasi *Website* SIA

Pencarian informasi pada aplikasi *website* SIA dilakukan melalui dua cara yaitu:

a. Mengunjungi aplikasi *website* secara langsung dan melihat *source code website* untuk mengetahui informasi mengenai *website* tersebut.

b. Menggunakan bantuan alat pencarian informasi builtwith.

3.2.2 Identifikasi Kerentanan pada *Website*

Merujuk pada standar pengujian keamanan *website* [11], proses yang dilakukan pada pengujian keamanan *website* SIA disajikan pada Tabel 2.

Tabel 2: Pengujian Keamanan pada SIA

No	Proses Pengujian	Kegiatan Pengujian
1	*Secure Transmission*	• Memastikan halaman *login* hingga halaman *logout* dilindungi oleh protokol HTTPS • Memastikan setiap aset yang dilindungi oleh protokol HTTPS tidak dapat diakses melalui HTTP • Memastikan sertifikat yang ada pada *website* valid
2	*Authentication*	• Memastikan *website* yang menggunakan *login* sepenuhnya dilindungi oleh protokol HTTPS • Memastikan pesan *error* yang ditampilkan sama apabila salah memasukkan *username* atau *password* • Memastikan apakah *website* perlu melakukan verifikasi e-mail untuk mengaktifkan akun • Memastikan *website* menggunakan verifikasi

No	Proses Pengujian	Kegiatan Pengujian
		captcha untuk menghindari serangan *brute force attack* • Memastikan apakah *website* memiliki mekanisme *forgot password* • Memastikan akun tidak menggunakan *username* dan *password default*
3	*Session Management*	• Memastikan sesi id baru akan dibuat setiap pengguna *login* • Memastikan batas kadaluarsa sesi tidak lebih dari 15 menit • Memastikan *website* tidak bisa digunakan lebih dari satu pengguna
4	*Cryptography*	• Melakukan pengecekan data yang harus dienkripsi • Menguji algoritma yang digunakan apakah memiliki kelemahan
5	*Data Validation*	• Melakukan percobaan SQL Injeksi, SSI Injeksi dan XSS Injeksi.
6	*Denial of Service*	• Melakukan pengujian apakah akun dari sebuah *website* akan terkunci apabila salah memasukkan *password* sebanyak 10 kali.
7	*Specific Risk of Functionality*	• Memastikan pengecekan fungsi batas maksimum ukuran file yang bisa di *upload* berjalan dengan baik • Memastikan jenis file yang terdaftar yang bisa di *upload* sehingga file lain tidak bisa di *upload* • Memastikan *website* mampu membaca ukuran dari file
8	*Configuration Management*	• Melakukan pengujian keamanan HTTP Headers
9	*Error Handling*	• Melakukan pengujian dengan memasukkan alamat yang tidak ada pada *website* untuk melihat informasi yang diberikan

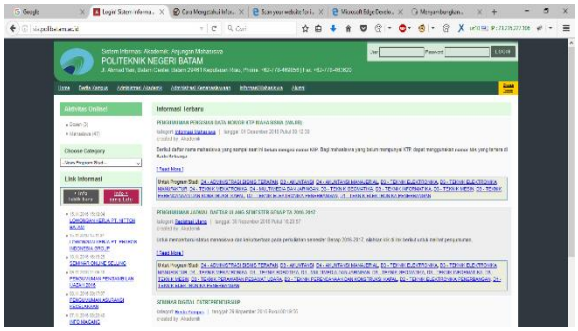
3.2.3 Rencana dan Strategi Keamanan

Proses yang dikerjakan pada fase ini adalah mengidentifikasi risiko yang ditemukan, memberikan strategi perlindungan, membuat rencana mitigasi risiko dan membuat dokumen manajemen risiko.

4. IMPLEMENTASI DAN HASIL

4.1 Implementasi Pencarian Informasi *Website* SIA

4.1.1 Hasil Pencarian pada *Website* SIA.



Gambar 8. Antarmuka *Website* SIA

Informasi yang didapatkan dengan melihat *source code* dari *website* SIA adalah sebagai berikut:

a. *Source code* yang ada pada aplikasi *website* SIA hanya dilindungi oleh protokol HTTP.
b. Versi dari SIA adalah siakad v2.0.
c. Meta Charset (pengkodean teks) yang digunakan adalah utf-8.
d. *Javascript libraries* yang digunakan adalah firebug-lite dan jquery-1.7.1.
e. Pengaturan halaman menggunakan CSS.
f. Tidak ada sertifikat SSL pada *website* SIA.

4.1.2 Hasil Pencarian dari Builtwith

Informasi yang didapatkan dari builtwith mengenai *website* SIA adalah sebagai berikut:

a. *Web Server* yang digunakan adalah Apache versi 2.2.
b. *Frameworks* yang digunakan adalah PHP.
c. *JavaScript Libraries* yang digunakan adalah Firebug Lite dan jQuery 1.7.1.
d. Informasi Dokumen yang digunakan adalah X-UA-Compatible, Meta Robot, Cascading Style Sheets, Javascript, Conditional Comments.
e. *Encoding* yang digunakan adalah UTF-8.
f. Sistem operasi *server* dari SIA adalah Ubuntu.

4.2 Hasil Pengujian Keamanan *Website* SIA

Hasil yang didapatkan dari hasil pengujian *website* SIA disajikan pada Tabel 3.

Tabel 3: Hasil Pengujian Keamanan SIA

No	Proses Pengujian	Kegiatan Pengujian	Jenis Ancaman
1	*Secure Transmission*	• *Website* SIA tidak memiliki sertifikat SSL *Source* pada SIA seluruhnya menggunakan protokol HTTP	• Penyerang membatalkan sebuah operasi. • Penyerang mengeksploitasi SIA tanpa bisa dilacak • Penyerang menutupi hasil eksploitasi
2	*Authentication*	• Halaman *login* hingga *logout* tidak dilindungi oleh protokol HTTPS • *Website* SIA akan menampilkan pesan *error* jika *username* atau *password* yang dimasukan salah • Tidak ada mekanisme verifikasi email dan mekanisme *forgot password* pada SIA • Ada verifikasi captcha sebelum masuk ke sistem • *Multiple User* masih bisa dilakukan pada *website* SIA • *Login* menggunakan *username* dan *password default* tidak berhasil dilakukan	• *Cookie Replay* • *Sniffing* • *Dictionary Attack*
3	*Session Management*	• Sesi baru akan dibuat setiap *user login* ke *website* SIA • Pengguna lain bisa menggunakan sesi hasil tangkapan sesi pengguna resmi dengan melakukan pengendusan jaringan • Sesi akan berakhir jika 15 menit tidak digunakan oleh pengguna	• *Session Hijacking* • *Session Replay* • *Man in the middle attacks*
4	*Cryptography*	• *Username* dan *password* dari pengguna masih bisa dicuri dengan melakukan pengendusan jaringan • Enkripsi yang digunakan untuk melindungi *username* dan *password*	• *Encryption Cracking*

No	Proses Pengujian	Kegiatan Pengujian	Jenis Ancaman
		masih tidak aman	
5	*Data Validation*	• Serangan SQL Injeksi, SSI Injeksi dan XSS Injeksi tidak berhasil dilakukan.	• *SQL Injection* • *SSI Injection* • *XSS Injection*
6	*Denial of Service*	• Website SIA tidak memblokir pengguna ketika pengguna salah memasukkan *password* sebanyak 10 kali	• *Denial of Service Attack*
7	*Specific Risk of Functionality*	• SIA telah menentukan batas maksimum ukuran file yang bisa di *upload*. • Jenis file yang bisa di *upload* pada *website* hanya file gambar berformat .JPG • SIA telah menentukan beberapa ukuran maksimum dan minimum gambar yang bisa di *upload*	• *Data Tampering* • *XSS attack*
8	*Configuration Management*	• Tidak adanya x-frame-options header pada *website* SIA	• *Clickjacking Vulnerability*
9	*Error Handling*	• *Website* SIA menghasilkan pesan *error* 404 dengan informasi yang diberikan adalah *web server* yang digunakan oleh SIA adalah apache versi 2.2 dengan akses *port* 80	• Serangan DOS • Penyerang mengeksploitasi dan menutupi jejak

4.3 Analisis Ancaman pada *Website* SIA

Berdasarkan hasil pengujian *website* SIA yang telah dilakukan, *website* SIA memiliki beberapa kriteria yang belum terpenuhi untuk dikatakan sebagai *website* yang aman menurut standar pengujian keamanan [11] dan [14]. Jenis ancaman yang bisa terjadi berdasarkan hasil pengujian pada *website* SIA disajikan pada Tabel 4.

Tabel 4: Kategori dan Jenis Ancaman pada SIA

No	Kategori Ancaman	Jenis Ancaman
1	*Authentication*	• *Cookie Replay* • *Sniffing* • *Dictionary Attack*
2	*Session Management*	• *Session Hijacking* • *Session Replay* • *Man in the middle attacks*
3	*Cryptography*	• *Encryption Cracking*
4	*Configuration Management*	• *Clickjacking Vulnerability*
5	*Auditing and Loging*	• *DOS Attack* • *Attacker exploits and cover his tracks*

Kategori ancaman *cryptography* merupakan ancaman yang perlu atau menjadi prioritas utama untuk segera diperbaiki. Dengan mudahnya dekripsi yang dilakukan,

membuat penyerang mampu memecahkan segala variasi *password* yang dimiliki oleh akun SIA mahasiswa di Politeknik Negeri Batam. Kategori ancaman lainnya adalah *authentication* dan *session management,* dengan melakukan *MITM attack*, penyerang mampu mendapatkan *username, password* serta *cookie* dari SIA. Metode penyerangan ini membuat penyerang bisa menggunakan akun seorang mahasiswa tanpa perlu melalui mekanisme *login*. Kategori ancaman *configuration management* merupakan kategori ancaman lainnya yang perlu menjadi perhatian utama karena penyerang mampu mengelabui pengguna yang sedang *login* dengan menyisipkan perintah tersembunyi pada *form* atau *image* pada *website* SIA. Kategori ancaman *error handling* perlu ditindak lanjuti karena sangat memungkinkan pengguna yang tidak berhak menggunkan akun resmi dari seorang mahasiswa untuk mendapatkan akses penuh ke akun resmi tersebut seperti merubah nilai mahasiswa.

4.4 Rencana dan Strategi Keamanan SIA

4.4.1 Risiko Aset yang Ditemukan

Berdasarkan fase 1 dan 2 yang telah dilakukan, metode OCTAVE secara keseluruhan menghasilkan data mengenai risiko terhadap aset *website* SIA Politeknik Negeri Batam beserta pengaruhnya pada 3 elemen aspek keamanan yaitu *Confidentiality* (Kerahasiaan), *Integrity* (Integritas) dan *Availability* (Ketersediaan) yang disajikan pada Tabel 5.

Tabel 5: Risiko Aset yang Ditemukan

No	Aset	Kategori Ancaman	Jenis Ancaman	C	I	A
1	Biodata Diri, Krs, Kuisoner dan Dokumen Pribadi.	*Authentication*	• *Cookie Replay* • *Sniffing* • *Dictionary Attack*	V	V	V
2	Biodata Diri, Krs, Kuisoner dan Dokumen Pribadi	*Session Management*	• *Session Hijacking* • *Session Replay* • *Man in the middle attacks*	V	V	V
3	*Username* dan *Password*, Biodata Diri, Krs, Kuisoner dan Dokumen Pribadi.	*Cryptography*	• *Encryption Cracking*	V	V	V
4	*Username* dan *Password*, Biodata Diri, Krs, Kuisoner dan Dokumen Pribadi.	*Configuration Management*	• *Clickjacking* *Vulnerability*	V	V	

4.4.2 Strategi Perlindungan terhadap Risiko

Strategi perlindungan yang dapat dilakukan berdasarkan jenis ancaman yang ditemukan pada *website* SIA secara keseluruhan adalah sebagai berikut:

1. ***Sniffing***

   Melakukan enkripsi data terhadap *website* SIA dengan menggunakan protokol jaringan HTTPS, IPSec, VPN dan protokol keamanan lainnya. Jika ingin menjadikan *website* SIA menjadi lebih aman, maka Politeknik Negeri Batam harus memiliki sertifikat SSL yang nantinya akan menjamin

keamanan data pada *website* SIA.

2. *Man in the Middle Attacks*

Man in the middle attacks dapat dilakukan dengan beberapa teknik:

a. Menggunakan sertifikat SSL

b. Menggunakan *Virtual Private Network* (VPN)

c. Menggunakan *Secure Shell Tunneling* (SSH)

3. *Cookie Replay*

Dengan menambahkan konfigurasi *flag httpOnly* saat *cookie* dibuat, berikut konfigurasi yang dapat dilakukan:

- Konfigurasi *flag httpOnly* pada Java

```
Cookie cookie = getMyCookie("myCookieName");
cookie.setHttpOnly(true);
```

- Konfigurasi *flag httpOnly* pada PHP di file php.ini

```
session.cookie_httponly = True
```

4. *Encryption Cracking*

a. Menggunakan alogritma lainnya seperti algoritma hash, misalnya MD5 dan SHA-1. Berikut *source code* enkripsi pada MD5 dan SHA-1:

- Source code enkripsi MD5

```
<?php echo md5("TugasAkhir"); ?>
```

- Source code enkripsi SHA-1

```
<?php echo sha1("TugasAkhir"); ?>
```

b. Menggunakan *plugin* jQuery jcryption, dimana algoritma yang digunakan pada *plugin* ini adalah AES (*Advanced Encryption Standard*) dan RSA. Contoh enkripsi menggunakan *plugin* jQuery jcryption adalah sebagai berikut:

```
var encryptedString = $.jCryption.encrypt($("#text").val(), password);
```

5. *Session Hijacking* dan *Session Replay*

a. Dengan memberikan konfigurasi *flag httponly* saat *cookie* dibuat, berikut konfigurasi yang bisa dilakukan:

- Konfigurasi *flag httpOnly* pada Java

```
Cookie cookie = getMyCookie("myCookieName");
cookie.setHttpOnly(true);
```

- Konfigurasi *flag httpOnly* pada PHP di file php.ini

```
session.cookie_httponly = True
```

b. Database dari *website* SIA harus menolak *multiple login* (login lebih dari 1 akun) pada sebuah akun. dengan membuat penyaringan *login* untuk mengidentifikasi sebuah akun yang sedang aktif dapat menghindarkan dari *multiple login*. Berikut contoh konfigurasi database untuk melakukan penyaringan *login* pada *database*:

```
UsersBase userdto = appService.getUserByUsername(username);
if (userdto != null) {
if ((userdto.getUser_loggedin())) {
if (request.getSession().getId().equals(userdto.getSessionId())) {
        authRequest.eraseCredentials();
request.getSession().setAttribute("error", "You are already logged in ");
        }
       }}
```

6. Clickjacking Vulnerability

Untuk konfigurasi yang bisa dilakukan pada *website* SIA adalah dengan melakukan konfigurasi *website* pada *httpd.conf* yang merupakan file konfigurasi apache dengan mengirimkan *X-Frame-Options header* ke semua halaman *website*, konfigurasinya adalah sebagai berikut:

```
Header always append X-Frame-Options SAMEORIGIN
```

Konfigurasi lainnya yang bisa dilakukan adalah dengan membuat kode javascript untuk mencegah *website* ditampilkan di dalam sebuah *frame.* Contoh kode *script* tersebut adalah sebagai berikut:

```
<style> html{display : none ; } </style>
<script>
  if( self == top ) {
    document.documentElement.style.display = 'block' ;
```

```
  } else {
    top.location = self.location ;
  }
</script>
```

4.4.3 Rancangan Mitigasi Risiko

Terkait masalah kategori ancaman dan jenis ancaman yang telah ditemukan terhadap aset dari *website* SIA Politeknik Negeri Batam, menghasilkan rencana mitigasi risiko yang meliputi kategori ancaman dan jenis ancaman [14]. Hal ini disajikan pada Tabel 6.

Tabel 6: Rancangan Mitigasi Risiko

No	Kategori Ancaman	Mitigasi Risiko
1	*Authentication*	• Menggunakan kebijakan kata sandi yang kuat • Mengunci akun apabila *username* yang sama salah memasukkan *password* sebanyak beberapa kali percobaan. Contohnya : salah memasukkan *password* sebanyak 5 kali. • Enkripsi saluran komunikasi untuk mengamankan token otentikasi. • Menggunakan mekanisme otentikasi yang tidak mengirimkan *password* melalui jaringan seperti protokol Kerberos atau Windows otentikasi. • Memastikan *password* akan dienkripsi (jika harus mengirimkan *password* melalui jaringan) atau menggunakan saluran komunikasi terenkripsi, misalnya dengan SSL. • Menggunakan *timeout cookie* dengan selang interval waktu yang relatif lebih singkat. Pada *website cookie* SIA memiliki batas waktu selama 15 menit. Dengan pengurangan waktu menjadi 5 – 10 menit setelah tidak digunakan akan mengurangi dampak dari *cookie replay*.
2	*Session Management*	• Jangan mengembangkan algoritma kustom sendiri apabila tidak dilakukan pengujian terhadap kekuatan algoritma enkripsi tersebut. • Menggunakan layanan atau algoritma kriptografi yang sudah terbukti kuat. Sebagai Contoh : menggunakan metode RNGCryptoServiceProvider untuk menghasilkan angka acak ketika proses enkripsi dan dekripsi • Tetap mancari informasi kemungkinan pengungkapan algoritma atau teknik yang bisa digunakan untuk memecahkan algoritma enkripsi yang sedang digunakan. • Hindari melakukan manajemen kata sandi. • Secara berkala melakukan perubahan kata sandi.
3	*Cryptography*	• Menggunakan sertifikat SSL untuk membuat saluran komunikasi yang aman dan hanya melalui otentikasi *cookie* melalui koneksi HTTPS • Melaksanakan fungsi *logout* secara paksa apabila sesi lain telah dimulai • Menekan periode kadaluarsa sebuah sesi jika tidak menggunakan SSL. Meskipun ini tidak akan mencegah pembajakan sesi, namun akan mengurangi batas waktu yang tersedia bagi attacker (Penyerang). • Membuat sebuah fungsi pilihan "*do not remember me*" yang memungkinkan tidak ada data sesi yang tersimpan di klien.

No	Kategori Ancaman	Mitigasi Risiko
		• Melakukan otentikasi ulang saat menjalankan fungsi penting. Contohnya : penyerang ingin mengubah data pribadi seorang mahasiswa maka perlu adanya otentikasi ulang dengan membuat penyerang harus memasukkan kata sandi ulang. • Menggunakan kriptografi agar mengenkripsi data *username* dan *password* yang dikirimkan ke server. Sehingga penyerang masih bisa membaca namun tidak berhasil memecahkan *username* dan *password* yang melewati jaringan.
4	*Configuration Management*	• Menggunakan otentikasi dan otorisasi yang kuat, misalnya dengan menggunakan sertifikat. • Mempertimbangkan untuk menggunakan VPN atau SSL karena sifat sensitif dari data akan dikirimkan. • Melakukan peninjauan ulang terkait masalah konfigurasi yang ada pada *website* Sistem Informasi Akademik.
5	*Auditing and Loging*	• Menyembunyikan versi *Web Server* yang digunakan oleh website SIA pada file konfigurasi httpd.conf . • *Back up* file log secara teratur dan analisis untuk melihat tanda – tanda adanya aktifitas yang mencurigakan. • Amankan file log dengan menggunakan pembatasan ACL. • Pindahkan file log jauh dari lokasi default.

.4.4 Dokumen Manajemen Risiko

Dokumen manajemen risiko disajikan pada Tabel 7.

Tabel 7: Dokumen Manajemen Risiko

Kerentanan	Jenis Ancaman	Pengaruh Ancaman	Penanggulangan
Penggunaan algoritma enkripsi yang masih lemah	*Encryption Cracking* (Pemecahan Enkripsi)	Penyerang dapat dengan mudah mengetahui hasil enkripsi *username* dan *password*	Menggunakan algoritma enkripsi yang lebih aman. Seperti mengkombinasikan algoritma enkripsi dan *encode.*
Pembuatan *cookie* pada *browser* tanpa menggunakan *flag httponly*	*Man in the middle attack* dan *sniffing* jaringan untuk mencuri *cookie*	*Cookie* yang didapatkan bisa digunakan untuk melakukan *cookie replay*	Menambahkan *flag httponly* saat pembuatan *cookie*
Website bisa diakses dalam *frame*	*Clickjacking vulnerability*	Membuat sebuah *frame* transparan dengan memasukkan sebuah perintah	Melakukan konfigurasi “Header always append X-Frame-Options SAMEORIGIN”pada *apache*
Tidak adanya sertifikat SSL	Pengungkapan informasi sensitif	Informasi sensitif atau informasi penting yang dikirm mampu dibaca pihak ketiga	Penggunaan sertifikat SSL

5. PENUTUP

Kesimpulan yang diperoleh setelah dilakukan pengujian terhadap aplikasi *website* SIA Politeknik Negeri Batam adalah sebagai berikut:

1. Metode OCTAVE yang digunakan mampu memberikan panduan manajemen risiko ancaman yang sistematik dengan membagi aktifitas identifikasi risiko ancaman kedalam 3 fase yaitu fase identifikasi risiko, fase pengujian dan fase manajemen risiko ancaman.
2. Kegiatan pengujian menemukan 4 kategori ancaman beserta jenis ancamannya pada setiap kategori yaitu, kategori *authentication* dengan jenis ancaman *sniffing* dan *cookie replay*, kategori *cryptography* dengan jenis ancaman *encryption cracking*, kategori *session management* dengan jenis ancaman *session hijacking, session replay* dan *man-in-the-middle attacks*. Serta kategori ancaman *configuration management* dengan jenis ancaman *clickjacking vulnerability*.
3. Berdasarkan analisis ancaman yang ditemukan, kategori ancaman *cryptography* merupakan ancaman yang perlu menjadi prioritas utama untuk segera diperbaiki. Hal ini dikarenakan SIA masih menggunakan algoritma enkripsi sederhana sehingga dapat dengan mudah dimasuki. Kategori ancaman lainnya yang perlu diperbaiki yaitu *authentication, session management* dan *configuration management*.
4. Manajemen risiko dari ancaman yang ditemukan menghasilkan dokumen manajemen risiko sebagai solusi penanggulangan terhadap kerentanan yang ditemukan.

Pada penelitian selanjutnya, untuk menilai prioritas dari suatu ancaman dapat diperoleh dengan tambahan metode *Damage Reproducibility Exploitability Affected Users Discoverability* (DREAD). Dengan bantuan metode ini dapat mengukur dan menentukan ancaman mana yang akan diprioritaskan lebih dahulu untuk dikerjakan. Hal ini dapat diukur dengan nilai 0-10, dimana nilai berarti tidak terjadi masalah, dan 10 berarti masalah ini perlu diselesaikan terlebih dahulu. Nilai 0-10 ini akan diberikan pada masing-masing poin ancaman seperti: *potential damage, reproducibility, exploitability, affected users,* dan *discoverability*.

Daftar Pustaka

[1] Direktorat Keamanan Informasi, Direktorat Jendral Aplikasi Informatika, Kementerian Komunikasi dan Informatika Republik Indonesia, Panduan Keamanan Web Server, e-book, edisi 1, 2011.

[2] P. David, *Vulnerabilities Assessment* pada Aplikasi Web www.polibatam.ac.id Menggunakan Metode Black Box Testing, *Tugas Akhir*, Jurusan Informatika, Politeknik Negeri Batam, Batam, 2016.

[3] CNN, How the U.S. Thinks Russians hacked the White House, *http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/,* diakses pada tanggal 25 September 2016. Pukul 19.15 WIB, 2015.

[4] Software Engineering Institute, *Introduction to the* OCTAVE *Approach*, e-book, edisi 1, Pittsburgh, 2003.

[5] Software Engineering Institute, OCTAVE *Criteria , Verison 2.0*, e-book, edisi 1, Pittsburgh, 2001.

[6] OWASP, *The Ten Most Critical Web Application Security Risk*, e-book, edisi 2, 2013.

[7] M. E. Whitman dan H. J. Mattord. *Principles of Information Security*. e-book, edisi 3, 2009.

[8] ISO 27001, *Infomation technology-Security techniques Information Security Management System-Requirements*, International Standard Organization, e-book, edisi 1, 2013.

[9] R. L. Krutz dan D. R. Vines, *The CISSP Prep Guide – Mastering the Ten Domains of Computer Security*. Penerbit CA: Wiley Computer Publishing John Wiley & Sons, Inc, edisi 1, United States of America, 2006.

[10] S. Janner, *Rekayasa Web,* edisi 1, Penerbit C.V Andi Offset, Yogyakarta, 2010.

[11] OWASP, Web Application Security Testing Cheat Sheet, *https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet*, diakses pada tanggal 05 Oktober 2016. Pukul 16.25, 2016.

[12] S'to, *Seni Teknik Hacking 2*, edisi 2, Penerbit Jasakom, Jakarta, 2007.

[13] Sans Institute. 2006. *Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks.* Paper. United States of America.

[14] Microsoft. 2016. *Cheat Sheet: Web Application Security Frame*. Diakses pada tanggal 05 Oktober 2016.https://msdn.microsoft.com/en-us/library/ms978518.aspx#tmwacheatsheet_webappsecurityframe.

[15] OWASP, OWASP *Testing Guide*, e-book, edisi 3, 2008.