Jurnal Integrasi
Vol. 9 No. 1, April 2017, 53-66
e-ISSN: 2548 - 9828

Article History
Received March, 2017
Accepted April, 2017

Penilaian Ancaman pada *Website* Transkrip Aktivitas Kemahasiswaan Politeknik Negeri Batam Menggunakan Metode DREAD

Anggariyona Saputra[1], Nelmiawati[2], 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: anggariyonasaputra@gmail.com, mia@polibatam.ac.id, maya.sitorus@polibatam.ac.id

Abstrak

Website merupakan media komunikasi yang memiliki peranan penting dalam penyebaran informasi terlebih dalam dunia pendidikan. Transkrip Aktivitas Kemahasiswaan (TAK) yaitu sebuah *website* yang ada di Politeknik Negeri Batam berisikan informasi tentang transkrip keaktifan mahasiswa selama menjadi mahasiswa. Beberapa informasi penting terkait transkrip aktivitas ada di *website* TAK sehingga rentan untuk di eksploitasi dan akan menimbulkan masalah yang besar. Oleh karena itu, perlu adanya analisis celah keamanan serta memberikan penilaian ancaman terhadap *website* tersebut. Pada penelitian ini, bertujuan untuk meminimalisir ancaman agar tidak mudah di eksploitasi. Metode yang digunakan yaitu DREAD. Metode ini dapat memberikan penilaian dan memberikan informasi yang berkualitas dengan menghasilkan peringkat risiko pada aplikasi *website*. Hasil penelitian ini memberikan informasi tingkat risiko suatu ancaman, meminimalisir risiko suatu ancaman, serta memberikan tindakan pencegahan dari suatu ancaman. Pada akhirnya, risiko yang paling tinggi terdapat pada pengujian otentikasi.

Kata kunci: DREAD, Penilaian Ancaman, Risiko Ancaman, TAK

Abstract

The website is a media communication which has a significant impact in information dissemination especially in the education. Transkrip Aktivitas Kemahasiswaan *(TAK) is a website that exists in* Politeknik Negeri Batam. *It contains information about student activity transcripts during becoming a student. Several of important informatian related to activity transcripts in the website might vulnerable to be exploited and will cause a big problem. Therefore, it is important to analyze the security and provide an assessment of the threat over the website. This study aimed to minimize the occurrence of threat whereby to make it difficult to exploit. The method used is DREAD, this method can provide an assessment and provide quality information. This information is intended to generate a risk rating of web applications. The results of the rating of the risks of using the method to provide information DREAD risk level of a threat, minimizing the risk of a threat, as well as provide preventive action towards the threat. At the end, the high risk that exist is in the authentication.*

Keywords: ***DREAD, Risk Rating, Threat Risk, TAK***

1 PENDAHULUAN

Website merupakan salah satu bentuk kemajuan zaman yang sangat berpengaruh dewasa ini. Penggunaan *website* di Politeknik Negeri Batam dimulai dari informasi kampus, informasi mengenai pembelajaran, informasi mengenai akademik mahasiswa, informasi mengenai penerimaan mahasiswa baru, informasi mengenai informasi beasiswa, informasi transkrip aktivitas kemahasiswaan dan informasi lainnya. *Website* tersebut dikunjungi oleh mahasiswa-mahasiswa Politeknik Negeri Batam karena berisikan

informasi yang sangat penting seperti data-data mahasiswa, transkrip nilai dan informasi penting lainnya.

Website Transkrip Aktivitas Kemahasiswaan (TAK) merupakan salah satu *website* yang sering dikunjungi oleh para mahasiswa tahun akhir (*http://www.tak.polibatam.ac.id)*. *Website* ini berisi informasi mengenai laporan aktivitas yang dilakukan oleh mahasiswa selama menjadi mahasiswa di Politeknik Negeri Batam disamping Proses Belajar dan Mengajar (PBM). *Website* ini juga berisi informasi mengenai kegitan-kegiatan Ormawa (Organisasi Mahasiswa). Sehingga, *website* ini menjadi tolak ukur keaktifan mahasiswa dan menjadi syarat wisuda mahasiswa. Nilai keaktifan mahasiswa dapat diketahui dengan meng-*upload file* (sertifikat/surat kerja/data penting lainnya) ke *website* tersebut. Nilai keaktifan mahasiswa tersebut penting untuk dijaga agar tidak terjadi sesuatu yang tidak diinginkan, terlebih mengenai sertifikat yang di *upload*, sertifikat tersebut bisa menjadi bahan untuk disalahgunakan oleh *attacker*, seperti mengambil manfaat dari sertifikat tersebut, mengubah, dan lain-lain. Sehingga *website* tersebut harus diperkuat tingkat keamanannya karena sangat rentan untuk dieksploitasi oleh oknum-oknum yang ingin merusak, merubah, mengganti, bahkan menghapus data penting tersebut. Ancaman-ancaman tersebut menjadi salah satu risiko yang harusnya ditangani dengan tepat.

Dari survei yang telah dilakukan oleh *Cenzic and Executive alliance* menjelaskan bahwa aplikasi web merupakan salah satu target yang paling sering diserang, terbukti serangan tersebut mencapai 71% dari laporan aplikasi *vulnerability* meliputi *web server*, aplikasi server, dan *web browser* [1]. Ada beberapa cara yang perlu dilakukan untuk meminimalisir ancaman dari serangan seperti dengan cara menganalisis celah keamanan dan manajemen risiko dari *website* TAK. Cara tersebut bertujuan untuk memperlihatkan celah-celah yang berpotensi terjadinya serangan.

Beberapa organisasi dan metode yang ikut berperan dalam menyelesaikan permasalahan dan penilaian risiko pada aplikasi *website*, seperti NIST (*National Institute of Standard & Technology*), FRAP (*The Facilitated Risk Assessment Process*), COBRA (*The Consultative Objective and Bi-functional Risk Analysis*), OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*), dan *Risk Watch* [2]. Akan tetapi, salah satu metode yang dianggap lebih luas cakupannya dengan menambahkan dimensi yang baru dalam menentukan dampak yang terjadi serta apakah ancaman tersebut benar berarti, metode tersebut adalah DREAD (*Damage Potential, Reproducibility, Exploitability, Affected User, Discoverability*). Metode DREAD merupakan metode yang digunakan untuk menghitung risiko yang dapat menghasilkan informasi peringkat risiko untuk sebuah ancaman yang terjadi [3].

Sehingga perlu adanya suatu analisis mengenai celah keamanan pada *website* TAK (*http://www.tak.polibatam.ac.id*) dan memberikan informasi mengenai manajemen risiko dengan menggunakan metode DREAD.

2 LANDASAN TEORI

Metode DREAD

Menurut OWASP (*Open Web Application Security Project*), metode DREAD (*Damage Potential, Reproducibility, Exploitability, Affected User, Discoverability*) merupakan sebuah teknik dan metode yang digunakan sebagai kerangka kerja yang dapat mengidentifikasi, menganalisa dan menganalisis celah keamanan pada sebuah *website* [4].

Gambar 1: Alur Kerja Metode DREAD (*Sumber: Threat modeling process* [3])

1. Identifikasi Ancaman

   Identifikasi ancaman merupakan tahap pertama dalam mencari informasi-informasi yang berhubungan dengan *website* yang menjadi target sebagai bahan penetrasi. Informasi tersebut meliputi identifikasi aset, *misuse case* diagram. Kemudian informasi mengenai hubungan aset dengan user beserta bentuk-bentuk ancamannya dapat ditentukan.

2. Dokumen Ancaman

   Dokumen ancaman adalah tahap kedua yang berisi tentang deskripsi ancaman, target ancaman, dan teknik ancaman. Tabel 1 berikut mendeskripsikan ancaman yang memungkinkan terjadi pada *website* tersebut.

Tabel 1: Deskripsi Ancaman

Deskripsi Ancaman	
Target Ancaman	
Rating Risiko	
Teknik Ancaman	
Tindakan Pencegahan	

3. Tingkat Ancaman

   Ini merupakan tahap terakhir mengenai *score calculated* dan *security report* dari sebuah ancaman.

   a. *DREAD Score Calculated*

      DREAD score calculated adalah hasil kalkulasi dari ancaman. Setiap komponen memiliki penilaian masing-masing. hasil yang akan didapatkan dari tiap komponen mulai dari angka 0-10, semakin besar

angkanya maka semakin besar tingkat ancamannya. Tabel 2 berikut contoh dalam menentukan DREAD *Score Calculated*.

Tabel 2: DREAD Score Calculated

Ancaman	D	R	E	A	D	Rating	Resiko

b. Security Report

Security report merupakan laporan akhir yang berisikan tentang deskripsi ancaman, target ancaman, *rating* ancaman, teknik ancaman, dan tindakan pencegahan terhadap ancaman / *threat* yang akan terjadi. Tabel 3 menunjukkan bentuk laporan *security* tersebut.

Tabel 3: *Security Report*

Threat *Description*	Ancaman 1	Ancaman 2	Ancaman 3	dst
Target Ancaman				
Risiko				
Teknik Ancaman				
Tindakan Pencegahan				

OWASP

OWASP merupakan organisasi *open source* yang dibangun untuk menemukan penyebab dari tidak amannya sebuah aplikasi *website* dan menemukan cara menanganinya [5].

Hal – hal yang bisa ditemukan di OWASP antara lain:

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

Keamanan Sistem Informasi

1. Hal yang menjadi masalah utama dari keamanan sistem informasi disimpulkan pada 2 hal yaitu:
   a. *Threats* (Ancaman)

      Ancaman/*threats* adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu ketidakseimbangan sistem informasi. Ancaman tersebut berasal dari 3 hal utama, yaitu ancaman alam (gempa, banjir, longsor, kebakaran), manusia (*malicious*, hacker, virus, dan lingkungan (polusi, efek bahan kimia, penurunan tegangan listrik).

   b. *Vulnerability* (Kelemahan)

      CIA atau yang biasa dikenal dengan *Confidentiality* (kerahasiaan), *Integrity* (intergritas) dan A*viability* (ketersediaan) merupakan salah satu parameter yang sering digunakan dalam menganalisis celah keamanan dan menjadi acuan dalam keamanan sebuah *website*. Parameter tersebut digunakan sebagai standar dan acuan dalam menilai baik atau buruknya sebuah keamanan pada suatu jaringan.

Ancaman Keamanan Sistem Informasi

Menurut OWASP, ada 10 kategori ancaman yang menjadi kelemahan pada aplikasi *website* meliputi *input validation, authentication, authorization, configuration management, sensitive data, session management, cryptography, parameter manipulation, exception management* dan *auditing and logging*.

Pengujian Keamanan pada *Website*

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

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.*

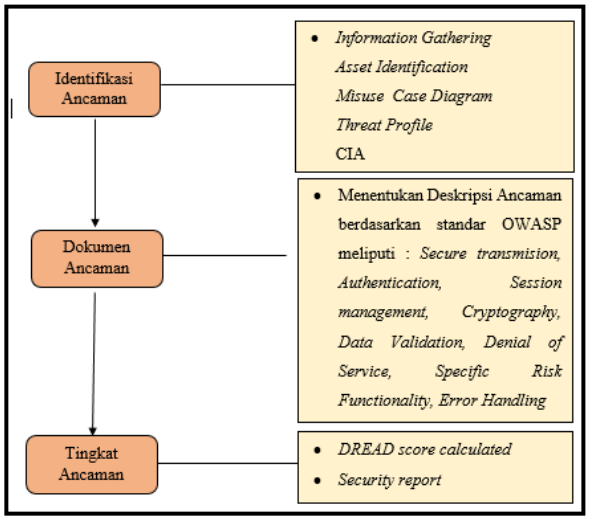
OWASP ZAP

OWASP ZAP (*Zed Attack Proxy)* merupakan sebuah aplikasi untuk melakukan *penetration testing* dalam menemukan *vulnerabilities*/celah keamanan pada suatu aplikasi *website.* ZAP menyediakan *scanner* secara automatis.

3 ANALISIS DAN PERANCANGAN

3.1. Proses Analisis

Proses penelitian yang dilakukan pada *website* TAK Politeknik Negeri Batam menggunakan metode DREAD dijelaskan pada Gambar 2 berikut:



Gambar 2: Proses Analisis TAK

1. Analisis Aset Informasi TAK

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

a. *User Name & Password*
b. Data diri (nama, *email*, no HP, prodi, tanggal masuk, jalur masuk, tahun lulus, tanggal lulus, nomor Ijazah, nomor Sertifikat, status)
c. Berkas TAK (Sertifikat, SK)
d. Informasi terbaru (pengumuman)
e. Informasi tabel transkrip

2. Analisis Jenis Ancaman

Jenis ancaman yang bisa terjadi pada aset *website* TAK dan pengaruhnya terhadap aspek keamanan CIA (*Confidentiality, Integrity dan Availability*) berdasarkan standar keamanan aplikasi *website* yang ditetapkan oleh Microsoft dan OWASP pada Tabel 4 sebagai berikut:

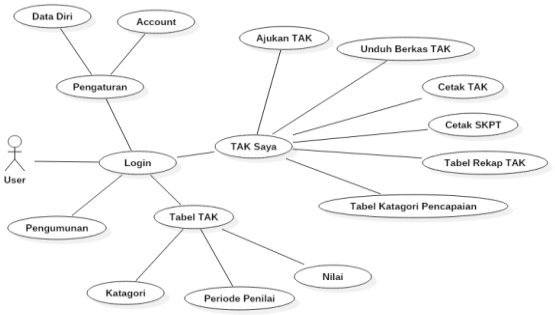
Tabel 4: Jenis Ancaman pada SIA

No	Aset	Kategori Ancaman	Jenis Ancaman	C	I	A
1	*User name dan password*	Authentication	*Cookie Replay*	V	V	
			Sniffing	V	V	
			Dictionary Attack	V	V	
			Menebak Akun	V	V	
			Pengguna			
2	Data Diri Mahasiswa	Validasi Masukan	*Session Hijacking*	V	V	V
			Session Replay	V	V	V
			Man-in-the-middle attacks	V	V	V
3	Dokumen Pribadi (Sertifikat, SK, Ijazah, dll)	Validasi Masukan	*Missing proper validation of file name*	V	V	
			Missing propert validation of file name	V	V	
4	Tabel Transkrip	Configuration Management	*Data tempering*		V	
			Elevation of privilage		V	
5	Informasi Pengumuman	*Authorization*	*Data tempering*		V	V
			Elevation of privilage		V	V

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

3. Analisis *Use Case* Diagram SIA

Berdasarkan pengamatan pengguna, didapat *Use Case* diagram mahasiswa yang menggunakan aplikasi *website* TAK. Berikut *Use Case* Diagram dari *website* tersebut.

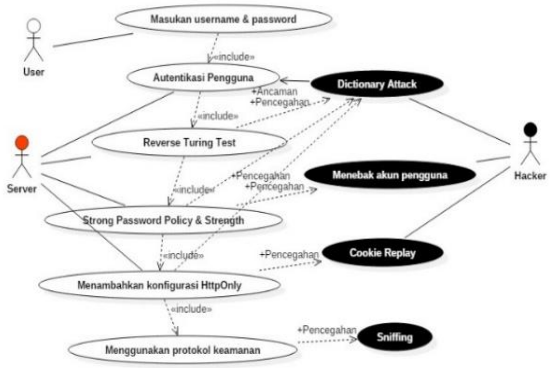


Gambar 3: *Use Case* Diagram TAK

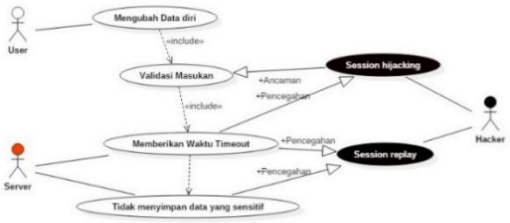
4. Analisis *Misuse Case* Diagram SIA

Terdapat beberapa skenario penyerangan yang akan terjadi pada *website* TAK.

a. Percobaan *login***Gambar 4: *Misuse Case Login***

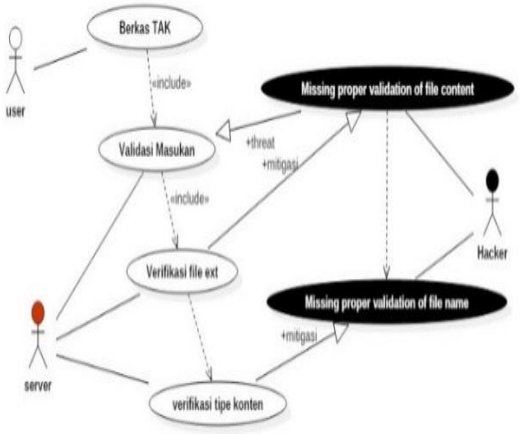


b. Percobaan *upload* sertifikat/ijazah/SK



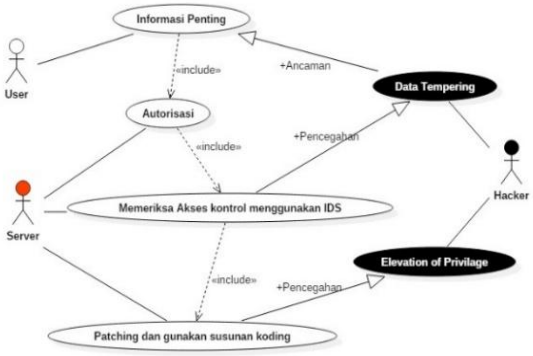
Gambar 5: *Misuse Case Upload Sertifikat/Ijazah/SK*

c. Percobaan mengubah data mahasiswa



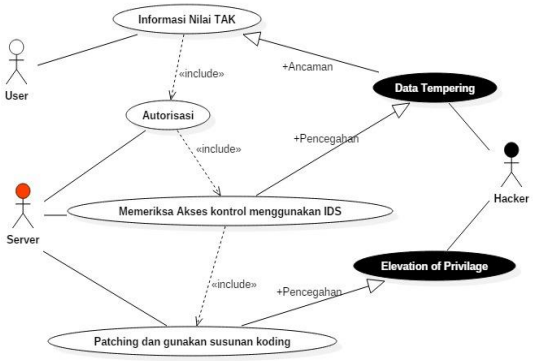
Gambar 6: *Misuse Case* data mahasiswa

d. Percobaan mengubah informasi penting



Gambar 7: *Misuse Case* Mengubah Informasi Penting

e. Mengubah nilai transkrip



Gambar 8: *Misuse Case* Mengubah Nilai Transkrip

3.2 Perancangan Pengujian Keamanan *Website*

3.2.1 Pencarian Informasi *Website* TAK

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

a. Mengunjungi *website* secara langsung dan kemudian melihat *source code* dari *website* tersebut.

b. Menggunakan bantuan alat pencarian informasi *builtwith*.

3.2.2 Identifikasi Kerentanan pada *Website*

Merujuk pada standar pengujian keamanan *website* OWASP, proses yang dilakukan pada pengujian keamanan *website* TAK disajikan pada Tabel 5 berikut.

Tabel 5: Pengujian Keamanan pada TAK

No	Proses Pengujian	Kegiatan Pengujian
1	*Secure Transmission*	• Memastikan protokol website yang digunakan pada website http://www.tak.polibatam.

No	Proses Pengujian	Kegiatan Pengujian
		ac.id. Protokol apa yang digunakan? • Memastika apakah *website* memberikan perlindungan kepada pengguna seperti *Digital Certificate Validity* apakah tersedia? • Memastikan *SSL Version*, apakah tersedia pada *website* tersebut?
2	*Authentication*	• Memeriksa kualitas dari suatu *password*? • Memeriksa apakah memiliki layanan remember me pada saat login gagal (hanya user saja yang sama namun password gagal)? • Memaastikan apakah captha tersedia pada saat *login*? • Memastikan apakah validasi memerlukan verifikasi untuk mengaktifkan sebuah akun?
3	*Session Management*	• Memastikan *website* memiliki batas waktu ketika sedang *login*? • Memastikan apakah *website* akan keluar dengan sendirinya ketika pengguna lupa untuk mengeluarkan akunnya? • Memastikan ketika pengguna sudah *logout*, apakah sesi id akan kedaluarsa pada sesi *client* dan tidak *valid* di sesi *server*?
4	*Cryptography*	• Memastikan apakah *file* yang penting sudah terenkripsi? • Memastikan algoritma yang digunakan dalam mengenkripsi suatu *file*?
5	*Data Validation*	• Apakah webite TAK termasuk web yang *vulnerability*? • Memastikan apakah

No	Proses Pengujian	Kegiatan Pengujian
		website bisa diserang dengan SQL *Injection*?
6	*Denial of Service*	• Memastikan apa yang terjadi bila pengguna gagal memasukkan *password* secara berulang ulang?
7	*Specific Risk of Functionality*	• Memastikan jenis file apa saja (ekstensi) yang bisa di upload? • Memastikan batasan limit size sebuah file saat upload? • Memastikan semua file upload memiliki anti virus scanning?
8	*Error Handling*	• Memastikan halaman apa yang muncul saat terjadi *error*? • Memastikan apa yang terjadi jika pengguna salah memasukkan url?

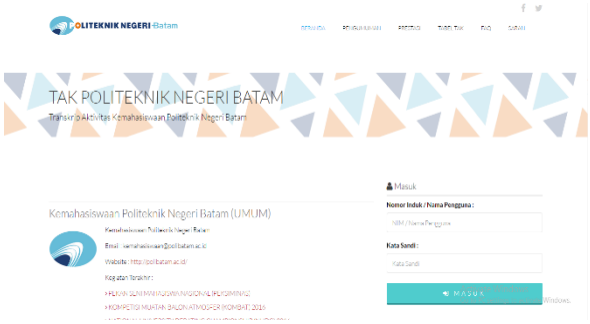
3.2.3 Menetukan Tingkat Ancaman

Pada tahap ini merupakan tahap akhir berisi tentang DREAD *score calculated* dan *security report* dari sebuah ancaman.

4 IMPLEMENTASI DAN HASIL

4.1 Implementasi Pencarian Informasi *Website* TAK

4.1.1 Hasil Pencarian pada *Website* TAK



Gambar 9. Website TAK

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

a. Protokol yang digunakan yaitu HTTP.
b. Meta charset (pengkodean teks) yang digunakan adalah utf-8.
c. *Javascript libraries* yang digunakan adalah

Datatables dan jQuery.

d. *Document Information* yang digunakan adalah HTML5 DocType, Meta Description, Conditional Comments, X-UA-Competible, Google Chrome IE Frame, Twitter Bootstrap, HTML5 Specific Tags, Iframe.

e. *Widgets* yang digunakan *Font Awasome.*

f. Untuk mengatur halaman *website* TAK digunakan CSS.

4.1.2 Hasil Pencarian dari Builtwith

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

a. *Web Server* yang digunakan adalah Apache versi 2.4.

b. *Frameworks* yang digunakan adalah Laravel.

c. *Java Script Libraries* yang digunakan adalah *jQuery* dan *Datatables*.

d. Sudah terintegrasi kedalam *mobile*, dengan menggunakan *Viewport Meta.*

e. *Widgets* yang digunakan *Font Awasome.*

f. *Document Information* yang digunakan adalah *HTML5 DocType, Meta Description, Conditional Comments, X-UA-Competible, Google Chrome IE Frame, Twitter Bootstrap, HTML5 Specific Tags, Iframe.*

g. *Encoding* yang digunakan UTF-8.

h. Sistem operasi server dari transkrip aktivitas mahasiswa adalah Ubuntu.

4.2 Hasil Pengujian Keamanan *Website* TAK

Hasil yang didapatkan dari hasil pengujian *website* TAK adalah sebagai berikut:

Tabel 6: Hasil Pengujian Keamanan TAK

No	Proses Pengujian	Kegiatan Pengujian	Jenis Ancaman
1	*Secure Transmission*	• Website TAK tidak memiliki sertifikat SSL • Source pada website TAK menggunakan protokol HTTP	• Attacker membatalkan sebuah operasi • Attacker melakukan eksploitsi aplikasi tanpa jejak • Attacker menutup hasil eksploitnya
2	*Authentication*	• Dari pengujian login dengan menggunakan NIM dan password yang sama didapatkan hasil yaitu 80% akun berhasil login • Website akan menampilkan pesan error, jika username atau password yang dimasukkan tidak valid. • Captcha tidak tersedia saat login • Kualitas password yang buruk • Apabila login gagal, tidak tersedia fungsi remember me/forget password • Akun pengguna dibuat secara default tidak ada konfirmasi email dalam pembuatan akun • Website bersifat multiple user	• Cookie Replay • Sniffing • Dictionary Attack • Menebak Akun Pengguna
3	*Session Management*	• Tidak memiliki batasan waktu saat login • Tidak tersedia auto logout (akun tidak akan keluar jika	• Session Hijacking • Session Replay

No	Proses Pengujian	Kegiatan Pengujian	Jenis Ancaman
		tidak di logout) • Sesi ID akan berubah setiap user login ke website TAK • Pengguna lain dapat menggunakan sesi ID dari pengguna utama dengan cara mengambil cookies dari pengguna utama tersebut • Apabila pengguna sudah logout, sesi ID akan kedaluarsa pada sesi client dan tidak valid di sesi server	
4	*Cryptography*	• Tidak tersedianya fungsi enkripsi saat login, sehingga user dan password dapat mudah diketahui oleh attacker	• Encryption Cracking • Sniffing
5	*Data Validation*	• Website TAK tidak memblokir pengguna yang telah salah memasukkan password berkali kali, dalam pengujian ± 15 kali	• SQL Injection • Buffer Overflow • Cross-Site Scripting
6	*Denial of Service*	• Website SIA tidak memblokir	• Denial of Service Attack

No	Proses Pengujian	Kegiatan Pengujian	Jenis Ancaman
		pengguna ketika pengguna salah memasukkan password sebanyak 10 kali	
7	*Specific Risk of Functionality*	• Hanya file yang berformat (ekstensi) jpg dan png saja yang bisa di upload • TAK telah menentukan ukuran maksimum untuk meng-upload file 1 MB, dan tidak memiliki ukuran minimum • File yang menjadi ancaman tidak bisa di-upload (exe, php, bat, vbs, dll)	• Data Tampering • XSS attack • Mengambil data penting (Sertifikat, Ijazah) • Attacker mengambil dokumen penting •
8	*Error Handling*	• Pada saat terjadinya error, akan memunculkan pesan error yang berisikan informasi mengenai web server dan sistem operasi yang digunakan yaitu Apache/2.4.16 Ubuntu • Apabila terjadi kesalahan dalam memasukan	• Serangan DOS • Penyerang mengeksploitasi dan menutupi jejak •

No	Proses Pengujian	Kegiatan Pengujian	Jenis Ancaman
		url, maka akan menampilkan gambar gifadalah web server yang digunakan oleh SIA adalah apache versi 2.2 dengan akses port 80	

4.3 Analisis Ancaman pada *Website* TAK

Berdasarkan hasil pengujian *website* TAK yang telah dilakukan sebelumnya, terdapat beberapa kriteria yang belum terpenuhi untuk dikatakan sebagai *website* yang aman menurut standar pengujian keamanan yang dikeluarkan OWASP. Jenis ancaman yang bisa terjadi dijelaskan pada Tabel 7 seperti berikut.

Tabel 7: Kategori dan Jenis Ancaman pada TAK

No	Kategori Ancaman	Jenis Ancaman
1	*Authentication*	• Cookie Replay • Sniffing • Dictionary Attack • Menebak Akun Pengguna
2	*Session Management*	• Session Hijacking • Session Replay
3	*Cryptography*	• Encryption Cracking • Unecryption Login Request
4	*Specific Risk Functionallity*	• Mengambil data penting (Sertifikat, SK)
5	*Error Hadling*	• Aplication Error

4.4 Analisis DRED

4.4.1 Penilaian DREAD

Penilaian ancaman pada *website* TAK dilakukan berdasarkan standar OWASP dapat dilakukan secara manual maupun menggunakan *tool*s, berikut hasil penilaian DREAD dari *website* TAK:

A. Penilaian DREAD secara Manual

Tabel 8: Penilaian DREAD *Website* TAK

Ancaman	D	R	E	A	D	T	Jlh	Rating
Dictionary Attack	5	10	7	0	9	31	6,2	Sedang
Menebak akun pengguna	5	10	10	0	10	35	7	Sedang
Unecryption Login Request	7	10	7	0	9	33	6,8	Sedang
SQL Injection	9	3	2	10	3	27	5,4	Sedang
Session Hijacking	5	5	7	0	9	26	5,2	Sedang
Session Replay	5	5	10	0	9	29	5,8	Sedang
Sniffing	5	5	7	0	9	26	5,2	Sedang
Mengambil Data penting (Sertifikat)	5	5	7	5	9	31	6,2	Sedang
Application Error	0	5	2	5	5	17	3,4	Rendah
Total	**46**	**58**	**59**	**20**	**72**	**255**	**5,66**	**Sedang**

B. Penilaian Menggunakan Tools OWASP ZAP

Tabel 9: Penilaian DREAD menggunakan tools

Ancaman	Rating
Frame-Options Header Not Set	Sedang
Cross-Domain JavaScript Source File Inclusion	Rendah
Cookie No HttpOnly Flag	Rendah
Password Autocomplite in Browser	Rendah
Web Browser XSS Protection Not Enabled	Rendah
X-Content Type Option Header Missing	Rendah
SQL Injection	Tinggi

C. Analisis Penilaian DREAD Manual dan Tools

Tabel 10: Perbandingan Penilaian DREAD Manual dan Tools

Ancaman	DREAD	
	Manual	*Tools*
Dictionary Attack	Sedang	-
Password Autocomplite in Browser (Menebak akun pengguna)	Sedang	Rendah
Unecryption Login Request	Sedang	-
Cookie No HttpOnly Flag (*Session Hijacking)*	Sedang	Rendah
Cookie No HttpOnly Flag (*Session Replay)*	Sedang	Rendah
Sniffing	Sedang	-
SQL Injection	Sedang	Tinggi
Mengambil Data penting (Sertifikat)	Sedang	-
Application Error	Rendah	-
X-Frame-Options Header Not Set	-	Sedang
Cross-Domain JavaScript Source File Inclusion	-	Rendah
Web Browser XSS Protection Not Enabled	-	Rendah
X-Content Type Option Header Missing	-	Rendah

Dari hasil analisis perbandingan nilai resiko diatas menjelaskan bahwa tidak semua penilaian yang dilakukan secara manual bisa didapati saat menggunakan *tool*s dan sebaliknya tidak semua yang dikerjakan di *tool*s ada pada manual, karena penggunaan *tools* hanya membaca *script* dari *website* tersebut, sedangkan manual tidak semua bisa dikerjakan secara menyeluruh tergantung dengan kemampuan dan hak akses dari seorang penilai ancaman.

4.4.2 Dokumen Ancaman

Berdasarkan hasil analisis penilaian ancaman yang telah dikerjakan sebelumnya, berikut hasil dari dokumen ancaman tersebut:

1. *Dictionary Attack*

Tabel 11: Dokumen Ancaman *Dictionary Attack*

Diskripsi Ancaman	*Dictionary Attack*
Target Ancaman	*Authentication* (Proses *Login*)
Penilaian Risiko	Tinggi
Teknik Ancaman	Menggunakan daftar kata yang ada di dalam kamus, dan kemudian daftar kata tersebut dimasukkan kedalam *tools dictionary attack*
Tindakan Pencegahan	Memperkuat *password strength*, mengganti default *username* dan *password*, membuat *strong password policy* , Menggunakan *Reverse Turing Test* (CAPTCHA)

2. Menebak Akun Pengguna

Tabel 12: Dokumen Ancaman Menebak Akun Pengguna

Diskripsi Ancaman	Menebak Akun Pengguna
Target Ancaman	*Authentication* (Proses *Login*)
Penilaian Risiko	Tinggi
Teknik Ancaman	Menebak akun pengguna secara manual dengan cara mengumpulkan *password* yang berkemungkinan digunakan *user* seperti di web TAK yaitu NIM
Tindakan Pencegahan	Hindari penggunaan akun secara *default* (NIM dan *Password*) , memperkuat *password strength*, membuat *strong password policy*, membuat konfirmasi email saat ingin membuat akun

3. *Unencryption Login Request*

Tabel 13: Dokumen Ancaman *Unencryption Login Request*

Diskripsi Ancaman	*Unencryption Login Request*
Target Ancaman	Akses Data
Penilaian Risiko	Tinggi
Teknik Ancaman	Mencuri informasi *login* pengguna seperti *username* dan *password* yang dikirim pengguna, namun informasi tersebut tidak terenkripsi ke *server*
Tindakan Pencegahan	Memberikan fungsi enkripsi pada setiap data yang sensitif seperti *password, user name*, dll

4. *SQL Injection*

Tabel 14: Dokumen Ancaman SQL Injection

Diskripsi Ancaman	*SQL Injection*
Target Ancaman	Akses Data
Penilaian Risiko	Sedang
Teknik Ancaman	Mempelajari struktur dari SQL query dan kemudian menggunakan pengetahuannya untuk menggagalkan query tersebut dengan cara meng inject suatu data agar dapat mengubah sintaks dari query tersebut.
Tindakan Pencegahan	menggunakan casting inputan (int atau string), memeriksa apaka teks menggunakan kata-kata yang berupa ancaman, menambahkan *script* khusus seperti pelarangan menggunakan simbol (petik, titik koma, sama dengan)

5. *Session Hijacking*

Tabel 15: Dokumen Ancaman *Session Hijacking*

Diskripsi Ancaman	*Session Hijacking*
Target Ancaman	*Session ID*
Penilaian Risiko	Sedang
Teknik Ancaman	Mengambil sesi ID pengguna lain agar bisa mendapatkan hak akses untuk masuk ke *resources*
Tindakan Pencegahan	Memberikan waktu *timeout* setiap sesi (misalnya 15 menit) dan mengantinya dengan sesi ID yang baru, hindari penyimpanan data data yang sensitif.

6. *Session Replay*

Tabel 16: Dokumen Ancaman *Session Replay*

Diskripsi Ancaman	*Session Replay*
Target Ancaman	*Session ID*
Penilaian Risiko	Tinggi
Teknik Ancaman	Mencuri pesan dari jaringan dan memutar kembali pesan tersebut untuk mencuri sesi dari pengguna
Tindakan Pencegahan	Memberikan waktu *timeout* setiap sesi (misalnya 15 menit) dan mengantinya dengan sesi ID yang baru, hindari penyimpanan data data yang sensitif.

7. *Sniffing*

Tabel 17: Dokumen Ancaman *Sniffing*

Diskripsi Ancaman	*Sniffing*
Target Ancaman	Akses Data
Penilaian Risiko	Sedang
Teknik Ancaman	*Attacker* masuk ke akun salah satu pengguna, kemudian mengambil data penting didalam website dengan cara men*download* nya
Tindakan Pencegahan	Memberikan watermark saat gambar sudah ter-*upload*

8. Mengambil Data Penting (Sertifikat, SK, dll)

Tabel 18: Dokumen Ancaman Mengambil Data Penting

Diskripsi Ancaman	Mengambil Data Penting
Target Ancaman	Akses Data
Penilaian Risiko	Sedang
Teknik Ancaman	Melakukan penyadapan dengan tujuan untuk

Diskripsi Ancaman	Mengambil Data Penting
	mengambil/mencuri data-data penting ataupun akun pribadi seseorang
Tindakan Pencegahan	Mengenkripsikan seluruh data yang sensitif seperti *user name* dan *password*, memasang SSL agar *website* dianggap lebih aman

9. *Application Error*

Tabel 19: Dokumen Ancaman *Application Error*

Diskripsi Ancaman	*Application Error*
Target Ancaman	Akses Data
Penilaian Risiko	Rendah
Teknik Ancaman	Memasukkan sembarang URL
Tindakan Pencegahan	Menutup informasi mengenai informasi *web server* dan sistem oprasi yang digunakan, karena informasi tersebut dapat membantu *hacker* untuk memulai suatu serangan.

4.4.3 Laporan Keamanan

5. Tabel 20 : Laporan Keamanan

Threat Duscription	***Dictionary Attack***	**Menebak akun penggguna**	***Unecryption Login Request***		***SQL Injection***	***Session Hijacking***	***Session Replay***	***Sniffing***	**Mengambil Data Penting**	***Application Error***
Target Ancaman	Authentication (Proses *Login*)	Authentication (Proses *Login*)	Akses Data		Akses Data	Session ID	Session ID	Akses Data	Akses Data	Akses Data
Risiko	Sedang	Sedang	Sedang		Sedang	Sedang	Sedang	Sedang	Sedang	Rendah
Teknik Ancaman	Menggunakan daftar kata yang ada di dalam kamus, dan kemudian daftar kata tersebut dimasukkan kedalam *tools* dictionary attack	Menebak akun penggguna secara manual dengan cara mengumpulkan *password* yang berkemungkinan digunakan *user* seperti di web TAK yaitu NIM	Mencuri informasi *login* penggguna yang dikirim penggguna, namun informasi tersebut tidak terenkripsi ke server		Mempelajari struktur dari SQL query kemudian menggagalkan query tersebut dengan cara meng inject suatu data agar dapat mengubah sintaks	mengambil sesi ID penggguna lain agar bisa mendapatkan hak akses untuk masuk ke resources	Mencuri pesan dari jaringan dan memutar kembali pesan tersebut untuk mencuri sesi dari penggguna	Melakukan penyadapan dengan tujuan untuk mengambil/mencuri data-data penting ataupun akun pribadi seseorang	*attacker* masuk ke akun salah satu pengguna, kemudian mengambil data penting didalam website dengan cara men*download* nya	Memasukkan sembarang URL agar terjadinya suatu error

Threat Duscription	***Dictionary Attack***	**Menebak akun penggunaa**	***Unecryption Login Request***		***SQL Injection***	***Session Hijacking***	***Session Replay***	***Sniffing***	**Mengambil Data Penting**	***Application Error***
					dari query					
Tindakan Pencegahan	Memperkuat *password* strength, mengganti default *user*name dan *password*, membuat strong *password* policy, , Menggunakan CAPTCHA	Hindari penggunaan akun secara default (NIM dan *Password*) , *password* strength, membuat strong *password* policy, membuat konfirmasi email saat ingin membuat akun	Memberikan fungsi enkripsi pada setiap data yang sensitif seperti *password*, *user* name, dll		menggunakan casting inputan (int atau string), menambahkan *script* khusus seperti pelarangan menggunakan simbol (petik, titik koma, sama dengan)	Memberikan waktu timeout setiap sesi (misalnya 15 menit) dan menganntinya dengan sesi ID yang baru, hindari penyimpanan data data yang sensitif	Memberikan waktu timeout setiap sesi (misalnya 15 menit) dan menganntinya dengan sesi ID yang baru, hindari penyimpanan data data yang sensitif.	Mengenkripsikan seluruh data yang sensitif seperti *user* name dan *password*, memasang SSL agar *website* dianggap lebih aman	Mengenkripsikan seluruh data yang sensitif seperti *user name* dan *password*, memasang SSL agar *website* dianggap lebih aman	Menutup informasi mengenai informasi web server dan sistem oprasi yang digunakan, karena informasi tersebut dapat membantu *hacker* untuk memulai suatu serangan.

5 PENUTUP

Kesimpulan yang diperoleh setelah dilakukan pengujian keamanan terhadap *website* TAK Politeknik Negeri Batam yaitu:

1. Terdapat 4 kategori ancaman dengan jenis ancaman yaitu *authentication*, kriptografi, dan *session management*. Dimana jenis ancaman *authentication* meliputi menebak akun pengguna, *dictionary attack, cookie replay attack,* dan *sniffing*, jenis ancaman kriptografi meliputi *unencryption login request*, jenis ancaman *session management* meliputi *session hijacking* dan *session replay*, jenis ancaman *specific risk funtionly* meliputi mengambil akun pengguna.
2. Berdasarkan analisis dari ancaman yang ditemukan, kategori ancaman *authentication* merupakan ancaman yang perlu menjadi prioritas utama untuk segera diperbaiki. Dengan terdapat 4 jenis ancaman yang bisa dieksploitasi yaitu menebak akun pengguna, *dictionary attack*, *cookie replay* dan *sniffing*, dari 4 jenis ancaman tersebut menebak akun pengguna yang merupakan ancaman terbesar pada penilaian ancaman *website* TAK.
3. Metode DREAD bertujuan untuk memberikan informasi mengenai nilai dari suatu ancaman dan juga sebagai panduan untuk mendapatkan nilai ancaman tersebut dengan membagi 3 metodologi yaitu identifikasi ancaman, dokumen ancaman, dan tingkat ancaman.
4. Hasil akhir dari pengujian ini yaitu berupa *security report* yang berisi tentang deskripsi ancaman, tingkat risiko ancaman, target ancaman, jenis serangan yang terjadi, serta pencegahannya.

Penelitian selanjutnya dapat melakukan analisis keamanan informasi dengan interasi yang berulang sehingga akan diperoleh hasil yang lebih lengkap. Dan

juga, dengan bantuan metode *threat modelling* yang lain seperti STRIDE (*spoofing, tampering, repudiation, information disclosure, denial of services, elevation of privilege*) dapat menghasilkan *security report* yang lebih spesifik dan dapat dimanfaatkan oleh UPT-SI Politeknik Negeri Batam dalam memperbaiki keamanan aplikasi *website* yang ada di Politeknik Negeri Batam.

6 Daftar Pustaka

[1] K. Mandeep, "Cenzic Application Security Trends Report -Q4," 2008. [Online].Available: http://www.Cenzic.com.

[2] S.Elky, An Introduction to Information System Risk Management, SANS Institute, 2006.

[3] J. Meier, A. Mackman, S. Vasireddy, M. Dunner, S. Escamilla and A. Murukan, “Improving Web Application Security: Threats and Countermeasures,” Microsoft Corporation, 2003.

[4] OWASP.2016. Threat Risk Modelling. Diakses pada tanggal 14 Oktober 2016. http://www.owasp.org/index.php/Threat_Risk_Modelling

[5] OWASP.2008. OWASP Testing Guide E-book: Edisi ke-3.