



ANALISA KERENTANAN SIS.TRISAKTI.AC.ID MENGUNAKAN TEKNIK VULNERABILITY SCAN

Is Mardianto, Agung Sedyono & Ahmad Hafzan

Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Trisakti

Jalan Kiai Tapa No. 1 Jakarta Barat 11440

E-mail: is.mardianto@gmail.com

ABSTRACT

Security means freedom from the fear of losing the object, his or her secret known to others. According to the terminology of US DoD 2011, Information Security (InfoSec) is safeguards for information and information systems, from someone's access or unauthorized information modification that occurs on storage media or data transmission. The purpose of this study is to determine the "definition", system architecture, Misuse Cases Diagram, Categorizing and Detailing and recommendations for improvements the sis.trisakti.ac.id system. sis.trisakti.ac.id is one of the Trisakti University web site that provides academic information system services for the Trisakti University academic community. To test the system security level and the data on the website sis.trisakti.ac.id vulnerability scan method is required and the result will be recommended for improvement of the existing systems. From the test results using a vulnerability scan, there is a vulnerability gap in the form of SQL injection vulnerabilities on the sis.trisakti.ac.id system.

Keyword: *Vulnerability Scanning, Penetration Testing, SQL Injection*

ABSTRAK

Keamanan dapat diartikan bebas dari rasa takut akan kehilangan benda miliknya, ataupun rahasianya diketahui orang lain. Menurut terminologi dari DoD US 2011, Keamanan Informasi (InfoSec) adalah upaya perlindungan informasi dan sistem informasi terhadap akses atau modifikasi informasi yang tidak sah yang dapat terjadi pada media penyimpanan atau transmisi data. Tujuan penelitian ini digunakan untuk menentukan "definisi", system architecture, Misuse Cases Diagram, Categorizing and Detailing dan rekomendasi perbaikan untuk sistem sis.trisakti.ac.id. sis.trisakti.ac.id merupakan salah satu situs web Trisakti yang menyediakan layanan sistem informasi akademik bagi sivitas akademika Universitas Trisakti. Untuk menguji tingkat keamanan sistem dan data pada website sis.trisakti.ac.id diperlukan metode vulnerability scan yang hasilnya berupa rekomendasi perbaikan sistem yang telah ada. Dari hasil pengujian menggunakan vulnerability scan didapatkan informasi tentang celah kerentanan sistem dalam bentuk kerentanan injeksi SQL pada sistem sis.trisakti.ac.id.

Kata kunci: *Pemindai Kerentanan, Pengujian Penetrasi, Injeksi SQL*



1. PENDAHULUAN

Keamanan Informasi (InfoSec) adalah upaya perlindungan informasi dan sistem informasi, terhadap akses atau modifikasi informasi yang tidak sah yang dapat terjadi pada media penyimpanan atau transmisi data. Selama 20 tahun keamanan informasi dibentuk oleh 3 pilar konsep utama yaitu *Confidentiality*, *Integrity* dan *Availability* (CIA) *Triad* [1]. Menurut model keamanan informasi terbaru Parkerian Hexad [2], keamanan Informasi meliputi 6 hal yaitu *Confidentiality*, *Possession or Control*, *Integrity*, *Authenticity*, *Availability* dan *Utility*. *Confidentiality* adalah proses melindungi informasi dari "*unauthorised disclosure*". *Integrity* adalah proses melindungi informasi dari "*unauthorised modification*" dan menjamin sebuah informasi lengkap dan akurat. *Availability* adalah proses menjamin informasi tersedia ketika dibutuhkan. *Possession/Control* berkaitan dengan kekhawatiran akan hilangnya kendali atau kepemilikan informasi, tetapi tidak melibatkan pelanggaran atas elemen *confidentiality*. *Authenticity*, merujuk pada kebenaran klaim atas keaslian (sumber) informasi. *Utility* berkaitan pada segi manfaat.

Untuk memenuhi kebutuhan akan keamanan sistem informasi akademik yang dijalankan Universitas Trisakti dibutuhkan pengujian sistem menggunakan teknik *Penetration Testing* dan *Vulnerabilities Scanning*, untuk mengetahui kerentanan dan ancaman yang dapat dieksploitasi oleh pihak luar

2. KAJIAN PUSTAKA

2.1. Penetration Testing

Penetration Testing (PenTest) adalah metode serangan pada sebuah sistem komputer dengan maksud menemukan kelemahan keamanan yang berpotensi untuk mendapatkan akses ke dalam sistem, baik secara fungsional maupun data [3]. Tahapan PenTest diantaranya melibatkan pengidentifikasian target sistem dan tujuan selanjutnya mereview informasi dan usaha yang ada untuk mencapai tujuan. Pengujian sistem dapat dilakukan secara *white box* (dimana semua latar belakang dan informasi sistem disediakan) atau *black box* (dimana hanya diberikan informasi dasar atau bahkan tanpa informasi sama sekali). Sebuah *penetration test* dapat membantu

menentukan apakah sistem rentan untuk diserang atau tidak, lewat kemampuan sistem bertahan terhadap berbagai jenis serangan.

Manfaat dari *Penetration Tests* diantaranya:

1. Menentukan layak tidaknya sehimpunan vektor serangan tertentu.
2. Mengidentifikasi kerentanan berisiko tinggi yang dihasilkan dari kombinasi kerentanan berisiko rendah yang dieksploitasi dalam urutan tertentu.
3. Mengidentifikasi kerentanan yang mungkin sulit atau mustahil untuk dideteksi dengan aplikasi perangkat lunak pemindai kerentanan.
4. Menilai besarnya potensi dampak terhadap bisnis dan operasional perusahaan dari serangan yang sukses.
5. Menguji kemampuan pertahanan jaringan dalam mendeteksi dan menanggapi serangan.
6. Memberikan bukti untuk mendukung investasi peningkatan personil keamanan dan teknologi.

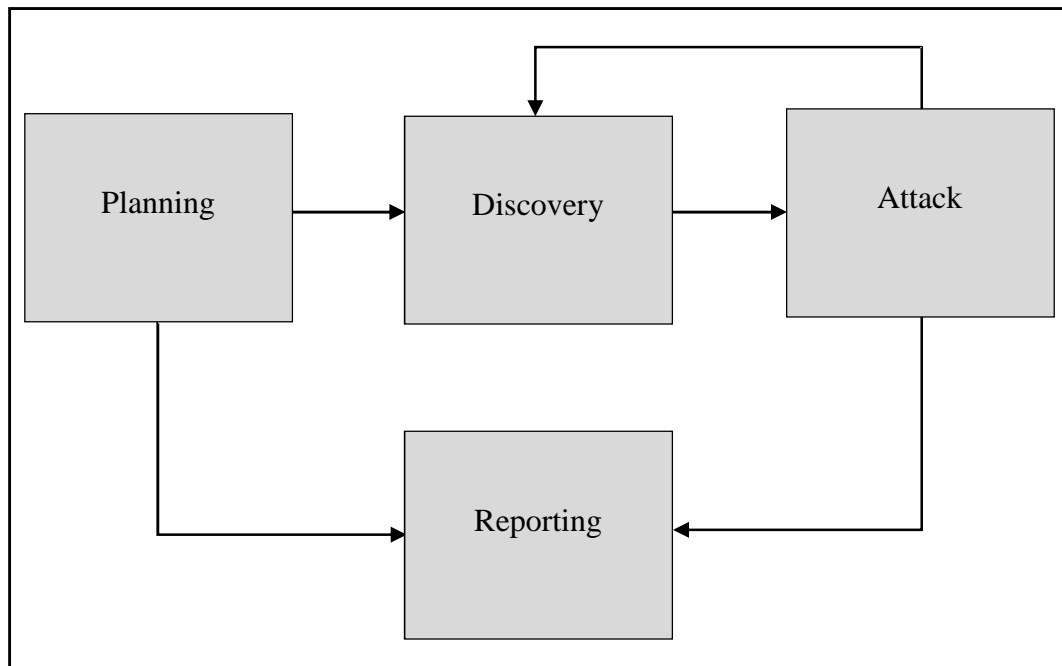
2.2. Vulnerability Assessment

Vulnerability Assessment adalah proses mengidentifikasi, mengkuantifikasi dan memprioritaskan (peringkat) kerentanan dalam sebuah sistem. *Vulnerability Assessment* memiliki banyak kesamaan dengan *risk assessment*, dimana penilaian dilakukan dengan mengikuti langkah-langkah berikut [4]:

1. Mengkatalog aset-aset dan kemampuan (sumber daya) dalam sebuah sistem.
2. Memberi nilai dihitung (atau setidaknya dalam urutan peringkat) dan pentingnya sumberdaya tersebut.
3. Mengidentifikasi kerentanan dan potensi ancaman terhadap setiap sumber daya.
4. Memindahkan atau mengurangi kerentanan yang paling besar terhadap sumber daya yang paling berharga.

3. METODOLOGI PENELITIAN

Dalam konteks teknologi informasi *vulnerability assessment* dilakukan dengan menggunakan teknik *Vulnerability Scanner*.



Gambar 1. Metodologi *Penetration Testing*

Gambar 1 menjelaskan proses *Penetration Testing* dimulai dari perencanaan, yang kemudian dilanjutkan ke proses penemuan dengan melakukan teknik serangan hingga keluaran yang diperoleh berupa laporan atas kerentanan sistem yang diuji.

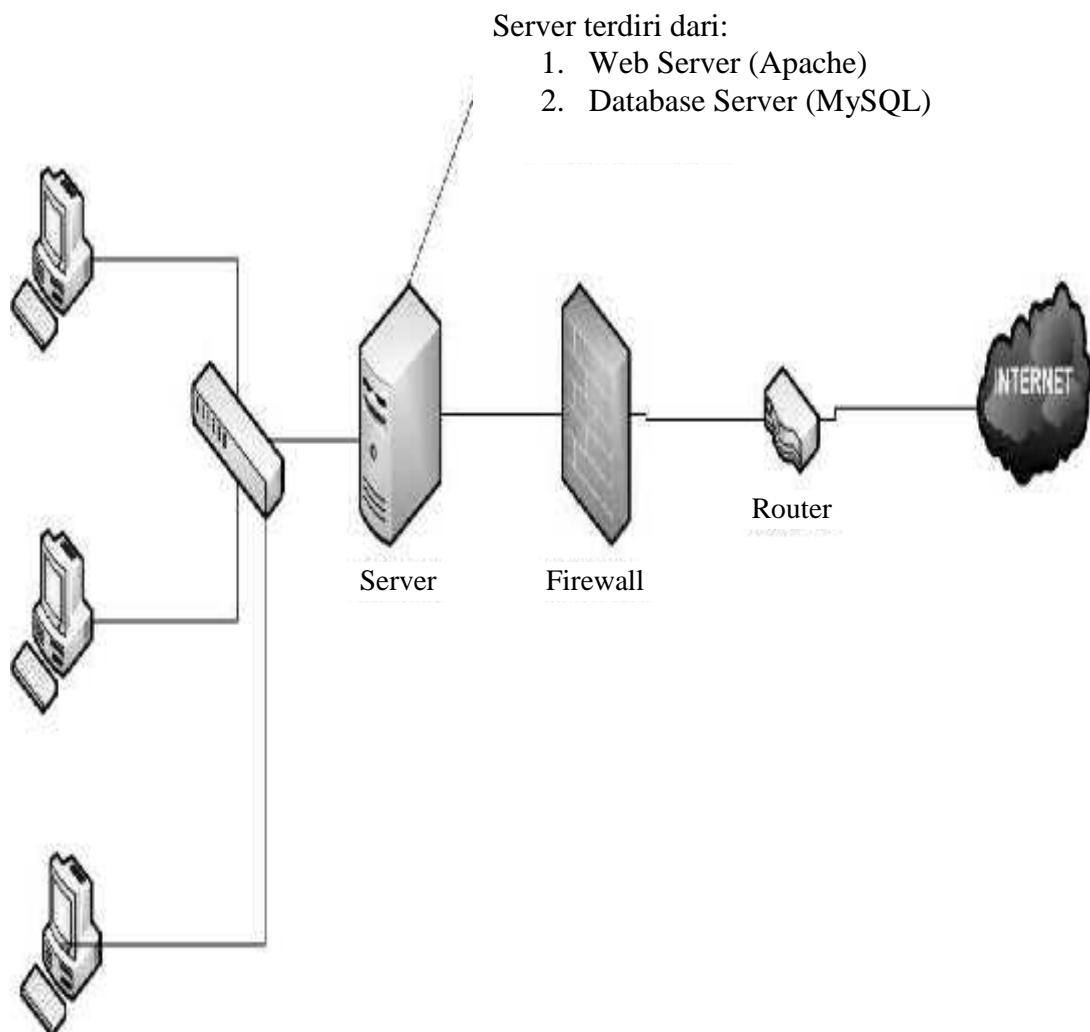
3.1. Definisi

Pada tahapan ini, dideskripsikan definisi atau istilah yang di gunakan dalam penulisan berdasarkan analisis keamanan sis.trisakti.ac.id.

1. sis.trisakti.ac.id merupakan portal *website* sistem informasi akademik Universitas Trisakti.
2. *Server* merupakan terminal akhir yang mengkoordinasikan semua aktivitas yang terjadi dalam infrastruktur jaringan yang bertugas untuk menangani penyimpanan, pengolahan, pendistribusian data secara terpusat serta sebagai pusat aplikasi bersama (*shared*) dan pintu gerbang menuju *gateway* (*internet*).
3. *Client* merupakan komputer yang terhubung ke *server*.

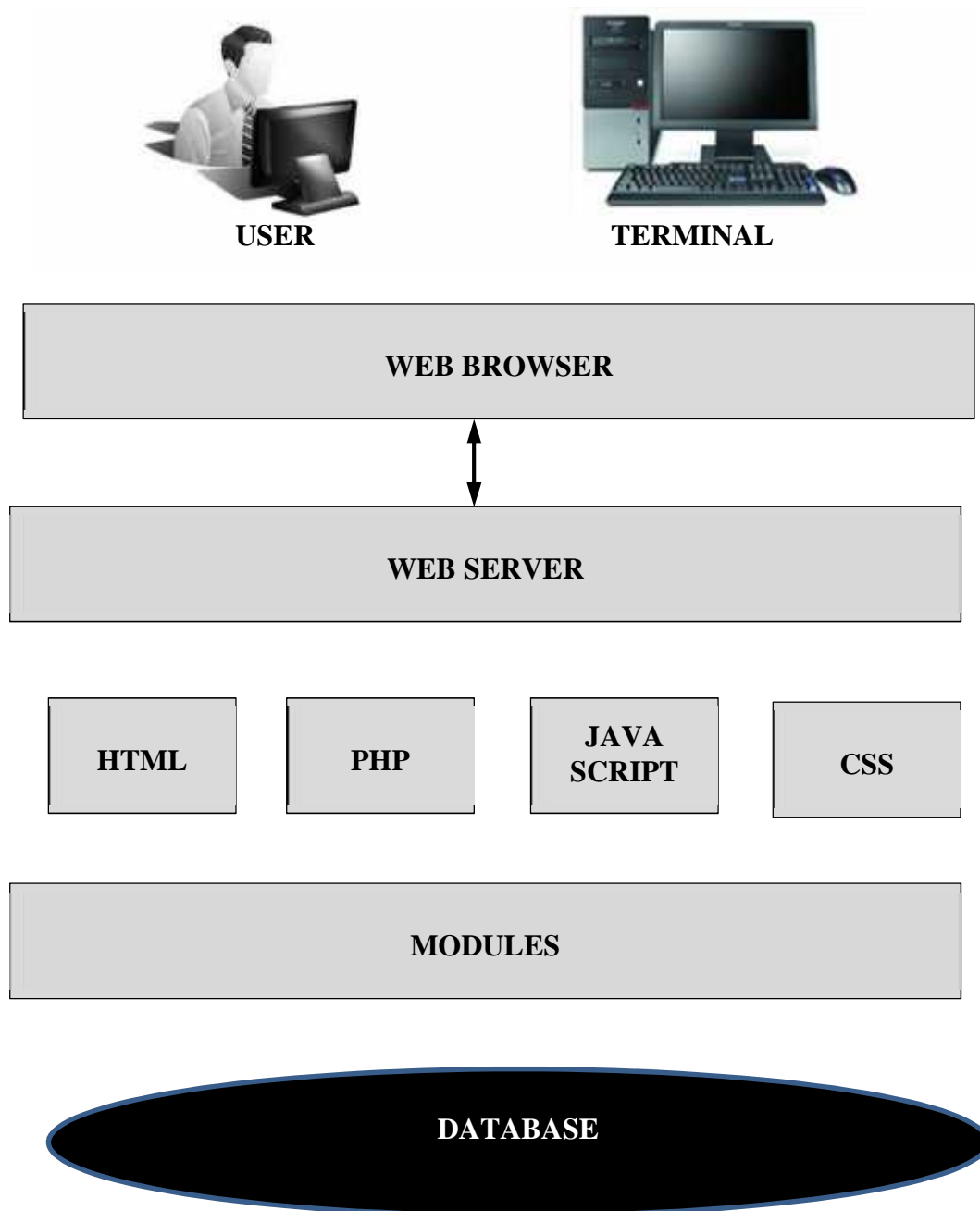
3.2. Arsitektur Sistem

Topologi jaringan umumnya terdiri atas *server*, *firewall*, *router* dan koneksi ke jaringan internet seperti yang terlihat pada Gambar 2. Server terdiri dari Web Server (Apache) dan Database Server (MySQL).



Gambar 2. Topologi jaringan

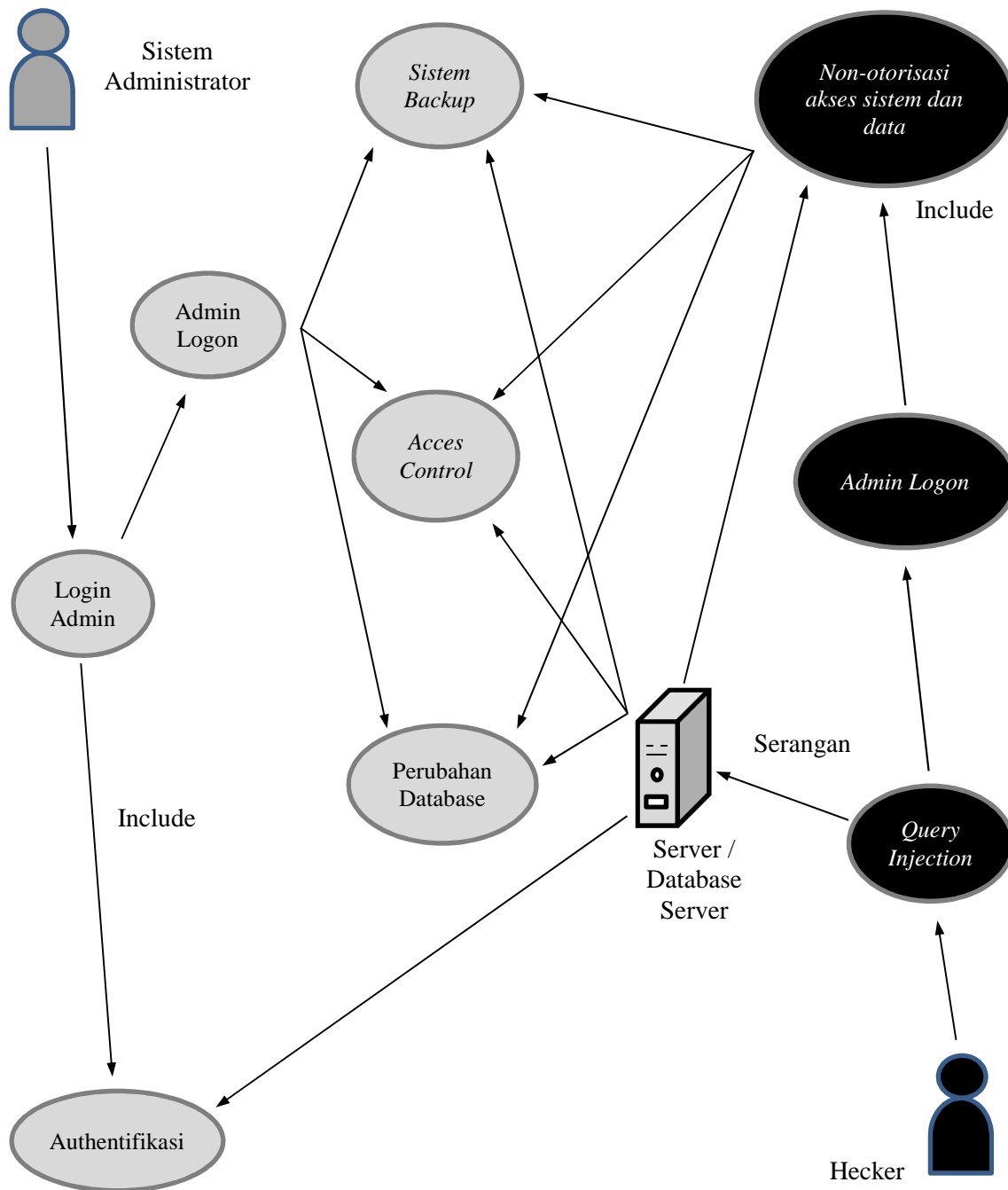
Arsitektur sistem informasi merupakan koneksi antara bagian *database* dengan modul-modul sistem informasi yang diakses hasil koneksi dari *web browser (client)* dengan *web server (server)*, seperti yang terlihat pada Gambar 3 pada halaman berikut.



Gambar 3. Arsitektur sistem *apache webserver*

3.3. Diagram *Misuse Cases*

Diagram *Misuse Case* pada Gambar 4 adalah diagram yang menggambarkan tindakan yang tidak sah yang dilakukan aktor *Hacker* untuk memperoleh akses kedalam sistem.



Gambar 4. Diagram misuse case

Misuse case 1, 2 dan 3 yang terdapat pada Tabel 1, 2 dan 3 memberikan sebagian skenario kemungkinan yang dapat terjadi ketika penyerang mencoba masuk kedalam sistem secara tidak sah.

Tabel 1. *Misuse case query injection*

Kode Use Case	MUC_01
Nama Use Case	<i>Usecase Query Injection</i>
Aktor	<i>Hacker</i>
Pra Kondisi	Mencari kelemahan dari sistem dengan melakukan percobaan <i>query injection</i> .
Post Kondisi	Masuk ke dalam sistem sebagai admin .
Tujuan	Mendapatkan akun sistem.
Skenario	<i>Hacker</i> melakukan pengecekan bagian dari web yang dapat di lakukan <i>query injection</i> . Setelah mengetahui halaman yang dapat dilakukan <i>query injection</i> untuk mendapatkan akun sebagai admin.

Tabel 2. *Misuse case admin logon*

Kode Use Case	MUC_02
Nama Use Case	<i>Usecase Admin Logon</i>
Aktor	<i>Hacker</i>
Pra Kondisi	Melakukan <i>query injection</i> ke sistem
Post Kondisi	Otorisasi dan administrasi data sebagai admin
Tujuan	Melakukan pencurian data dari <i>database</i> . Melakukan perubahan terhadap <i>access control</i> pada sistem.
Skenario	<i>Hacker</i> masuk ke sistem sebagai admin, lalu melakukan otorisasi data sebagai admin.

Tabel 3. *Misuse case authorisasi system*

Kode Use Case	MUC_03
Nama Use Case	<i>Usecase Authorisasi system</i>
Aktor	<i>Hacker</i>
Pra Kondisi	Masuk ke sistem sebagai admin
Post Kondisi	Melakukan serangkaian aktivitas meliputi pencurian <i>database</i> dan pengrusakan sistem
Tujuan	Melakukan pencurian data dari <i>database</i> . Melakukan perubahan terhadap <i>access control</i> pada sistem.
Skenario	<i>Hacker</i> masuk ke dalam sistem sebagai admin, lalu <i>hacker</i> dapat melakukan pencurian data dan perubahan data

4. HASIL DAN PEMBAHASAN

4.1. Vulnerability Information

Setelah dilakukan percobaan menggunakan *tools webcruiser* ditemukan beberapa celah keamanan diantaranya adalah *vulnerability POST SQL INJECTION BooleanBased String*.

Tabel 4. Hasil pengujian dengan *webcruiser*

N0.	1
<i>ReferURL</i>	<i>http://www.sis.trisakti.ac.id/</i>
<i>ActionURL</i>	<i>http://www.sis.trisakti.ac.id/index/login^username=1388696&Login=Login&IdUniversity=1&password=99999999</i>
<i>Parameter</i>	<i>Password</i>
<i>Vulnerability</i>	<i>POST SQL INJECTION Boolean Based Integer</i>
N0.	2
<i>ReferURL</i>	<i>http://www.sis.trisakti.ac.id/index/?lang=</i>
<i>ActionURL</i>	<i>http://www.sis.trisakti.ac.id/index/?lang=</i>
<i>Parameter</i>	<i>Lang</i>
<i>Vulnerability</i>	<i>COOKIE SQL INJECTION Boolean Based String</i>
N0.	3
<i>ReferURL</i>	<i>http://www.sis.trisakti.ac.id/forgotpassword</i>
<i>ActionURL</i>	<i>http://www.sis.trisakti.ac.id/forgotpassword/index^retrievepassword=retrievepassword&email=99999999</i>
<i>Parameter</i>	<i>Email</i>
<i>Vulnerability</i>	<i>POST SQL INJECTION Boolean Based String</i>
N0.	4
<i>ReferURL</i>	<i>http://www.sis.trisakti.ac.id/forgotpassword</i>
<i>ActionURL</i>	<i>http://www.sis.trisakti.ac.id/forgotpassword/index^retrievepassword=retrievepassword&email=3721105</i>
<i>Parameter</i>	<i>Email</i>
<i>Vulnerability</i>	<i>POST SQL INJECTION Boolean Based String</i>

4.2. Categorizing and Detailing

Pada tahapan ini difokuskan membuat kategori dan rincian dari arsitektur sistem dan kebutuhan untuk kebijakan yang akan diterapkan. Tujuannya untuk dapat mengetahui cara pengamanan sistem dan sebagai acuan untuk diterapkan. Pada Tabel 5 diperlihatkan analisis pada tahapan *categorizing and detailing*.

Tabel 5. *Categorizing dan Detailing*

Goal(s)	Confidentiality, Integrity, Availability
<i>Requirement(s)</i>	<i>AC: Access Control, EN : Encryption, PV : Privacy, AU : Autherization</i>
<i>Category</i>	<i>Unauthorize Attack (UA), Access Control (AC), Privacy (PV)</i>
<i>Misuse Case</i>	<i>MUC_01, MUC_02, MUC_03</i>
<i>Implementation Choice</i>	Menerapkan enkripsi <i>password</i> dan kode <i>captcha</i> pada <i>form login</i> . Menerapkan DMZ untuk mencegah terjadinya <i>hacker</i> melakukan percobaan untuk masuk ke sistem. Menerapkan batasan percobaan pada saat <i>login</i> . Menerapkan keamanan jalur komunikasi data yaitu dengan menggunakan <i>https</i> dan <i>SSL</i> .



4.3. Rekomendasi

Dari hasil *vulnerability scanning* pada sistem yang diuji, dapat diberikan rekomendasi sebagai berikut :

- a. Mengaktifkan anti *injection* pada *website*.
- b. Migrasi menggunakan cms seperti Joomla.
- c. Jika tidak ingin migrasi ke cms, gunakan pemrograman berbasis *framework* seperti *code igniter*, *symphony* dan *laravel*.
- d. Menerapkan algoritma enkripsi data seperti RSA, SHA dan AES.

5. KESIMPULAN

Hasil *vulnerability scan* yang dilakukan dapat membantu memperbaiki keamanan sistem sis.trisakti.ac.id sehingga dapat meningkatkan performa sistem informasi akademik *online* melalui penerapan rekomendasi perubahan sistem yang harus dilakukan, terutama perbaikan dibagian penerapan "*anti SQL injection*".

Informasi data-data *vulnerability scan* dapat memudahkan *programmer* untuk memperbaiki sistem yang ada, untuk menghindari kebocoran informasi yang bersifat rahasia, lewat mekanisme penerapan metode enkripsi data simetrik AES, enkripsi data asimetrik RSA dan enkripsi *hash* SHA. Disarankan untuk menambahkan tools *vulnerability scanning* lainnya agar bisa membandingkan hasil yang didapat dari masing-masing *tools* dan untuk lebih banyak mengeksplorasi lebih jauh terutama kerentanan dibagian *unauthorized logon*

UCAPAN TERIMA KASIH

Terimakasih kepada Fakultas Teknologi Industri Universitas Trisakti yang mendanai penelitian ini dalam bentuk Hibah Penelitian Internal Universitas Trisakti 2014, dengan judul penelitian "Implementasi Teknik *Penetration Testing* Pada Sistem Informasi Akademik Universitas Trisakti".

DAFTAR PUSTAKA

- [1] Simon Holloway. *Security? What security?*. [Online]. Tersedia di <http://www.bloorresearch.com/analysis/security-what-security-p1-p1/> [20 Agustus 2010].
- [2] Donn B. Parker. *Fighting Computer Crime*. New York, NY: John Wiley & Sons. 1998.
- [3] Kevin M. Henry. *Penetration Testing: Protecting Networks and Systems*. ITGP. 2012.
- [4] Foresec. *FCCH Course Book*. 2014.
- [5] Department of Defense US. *Dictionary of Military and Associated Term*. Joint Publication 1- 02. 2011.

Filename: 25.27 (hal 90-100) Analisa Kerentanan Is mardianto_1158326
Directory: C:\Users\FTI-USAKTI\AppData\Local\Temp
Template: C:\Users\FTI-USAKTI\AppData\Roaming\Microsoft\Templates\Normal.dotm
Title:
Subject:
Author: KOMP-10
Keywords:
Comments:
Creation Date: 27/01/2016 8:18:00
Change Number: 2
Last Saved On: 27/01/2016 8:18:00
Last Saved By: 062 FTI-USAKTI
Total Editing Time: 1 Minute
Last Printed On: 01/02/2016 13:06:00
As of Last Complete Printing
Number of Pages: 11
Number of Words: 1.808 (approx.)
Number of Characters: 12.623 (approx.)