

SKRIPSI

**ANALISIS CELAH KEAMANAN DAN KERENTANAN PADA
SISTEM INFORMASI AKADEMIK (SIAKAD) UNIVERSITAS
ISLAM AHMAD DAHLAN (UIAD) MENGGUNAKAN
METODOLOGI OWASP**

PROGRAM MBKM



MACHFUD MUBARAK SAPANANG

NIM : 195410193

**PROGRAM STUDI INFORMATIKA
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA**

2023

SKRIPSI

**ANALISIS CELAH KEAMANAN DAN KERENTANAN PADA
SISTEM INFORMASI AKADEMIK (SIKAD) UNIVERSITAS
ISLAM AHMAD DAHLAN (UIAD) MENGGUNAKAN
METODOLOGI OWASP**

Diajukan sebagai salah satu syarat untuk menyelesaikan studi

**Program Sarjana
Program Studi Informatika
Fakultas Teknologi Informasi
Universitas Teknologi Digital Indonesia
Yogyakarta**

Disusun Oleh

Machfud Mubarak Sapanang

NIM : 195410193

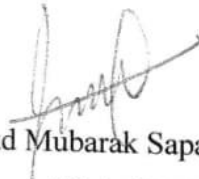
**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA**

2023

PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya menyatakan bahwa naskah skripsi ini belum pernah diajukan untuk memperoleh gelar Sarjana Komputer di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara sah diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 1 April 2023



Machfud Mubarak Sapanang

NIM: 195410193

HALAMAN PERSEMBAHAN

Puji syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan limpahan rahmat dan karunia-Nya. Dengan rasa syukur penuh nikmat serta rasa bangga yang luar biasanya penulis persembahkan karya tulis sederhana ini kepada:

1. Kedua orang tua penulis yang selalu memberikan kasih sayang, doa, serta dukungannya. Yang selalu senantiasa sabar dalam memberikan arahan dan semangat yang tiada hentinya sehingga penulis bisa sampai ke tahap ini.
2. Keluarga besar penulis yang selalu memberikan semangat, dukungan dan motivasi yang sangat berarti.
3. Bapak Ir. Muhammad Guntara, M.T. atas bimbingan dan arahan yang diberikan kepada penulis sehingga dapat menyelesaikan karya tulis ini.
4. Mentor yang terhormat, Mas Guruh Marindra Pratama yang selalu berkenan membantu penulis dalam mengerjakan penelitian ini.
5. Sahabat dan orang-orang terdekat penulis yang selalu memberikan support yang luar biasa sampai saat ini sehingga penulis dapat menyelesaikan karya tulis ini.

HALAMAN MOTTO

“Dari pengalaman kemenangan atau kegagalan,
kau akan belajar sesuatu yang berharga.”

-Shanks-

KATA PENGANTAR

Dengan memanjatkan puja dan puji syukur kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karunianya serta senantiasa memberikan Kesehatan dan kesempatan sehingga penulis dapat menyelesaikan penyusunan skripsi ini. Adapun judul skripsi yang penulis angkat adalah “ANALISIS CELAH KEAMANAN DAN KERENTANAN PADA SISTEM INFORMASI AKADEMIK (SIKAD) UNIVERSITAS ISLAM AHMAD DAHLAN (UIAD) MENGGUNAKAN METODOLOGI OWASP”, sebagai salah satu syarat untuk menyelesaikan Program Sarjana (S1) Program Studi Informatika Universitas Teknologi Digital Indonesia.

Adapun penelitian ini bertujuan untuk menggambarkan perjalanan penulis selama mengikuti program MBKM sehingga dengan kegiatan ini penulis mendapatkan begitu banyak pengalaman dan pengetahuan baru yang berbeda dengan sebelumnya. Penulis menyadari bahwa skripsi ini tidak mungkin terselesaikan tanpa adanya dukungan, bantuan, bimbingan, dan nasehat dari berbagai pihak selama penyusunan skripsi ini. Sehingga pada kesempatan ini penulis menyampaikan terima kasih setulus-tulusnya kepada :

1. Bapak Ir. Totok Suprawoto, M.M.,M.T. selaku Rektor Universitas Teknologi Digital Indonesia.
2. Bapak Ir. Muhammad Guntara, M.T. selaku Dosen Pembimbing skripsi atas segala bimbingan dan arahan yang diberikan kepada penulis.
3. Ibu Dini Fakta Sari, S.T., M.T. selaku Ketua Program Studi Informatika (S1) Universitas Teknologi Digital Indonesia.
4. Bapak Arif Suyanto Putro selaku Ketua Tim Kerja Tata Usaha dan Ketua Kelompok Kerja Talent Scouting Academy Badan Balitbang SDM Kementerian Komunikasi dan Informatika.
5. Bapak Guruh Marindra Pratama selaku mentor Program MBKM yang telah banyak memberikan bimbingan, motivasi, ilmu dan pengalaman selama

program ini berlangsung. Penulis juga banyak berterima kasih atas bantuan dan bimbingannya sehingga penulis dapat menyelesaikan penelitian ini.

6. Bapak Abdul Latif selaku Instruktur Cisco Networking Academy (NETACAD) yang telah memberikan banyak ilmu dan pembelajaran selama program ini.
7. Seluruh staff dan pegawai program TSA DTS dan Kampus Merdeka 2022 yang telah melaksanakan kegiatan ini dengan sangat baik.
8. Kedua orang tua penulis yang selalu memberikan kasih sayang, doa, serta dukungannya dalam setiap langkah, sehingga penulis dapat dengan semangat dalam menyelesaikan program magang.
9. Teman-teman program DTS yang sudah banyak membantu saya selama program ini.
10. Teman, keluarga, dan semua pihak yang telah membantu dan tidak dapat disebutkan satu persatu.

Penulis sangat bersyukur karena dapat menambah pengetahuan dan pengalaman selama mengerjakan penelitian ini. Penulis menyadari skripsi ini masih banyak memiliki kekurangan dan kesalahan, karena itu segala kritik dan saran yang membangun akan menyempurnakan penulisan skripsi ini serta bermanfaat bagi penulis dan pembaca

Yogyakarta, 15 Maret 2023

Penulis,

Machfud Mubarak Sapanang

DAFTAR ISI

HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
PERNYATAAN KEASLIAN SKRIPSI.....	v
HALAMAN PERSEMBAHAN.....	vi
HALAMAN MOTTO.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR GAMBAR.....	xii
DAFTAR TABEL.....	xiii
INTISARI.....	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Ruang Lingkup.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
1.6 Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA DAN DASAR TEORI.....	5
2.1 Tinjauan Pustaka.....	5
2.2 Dasar Teori.....	7
BAB III METODE PENELITIAN.....	19
3.1 Bahan/Data.....	19
3.2 Alat.....	19
3.3 Alur Penelitian.....	19
3.4 Vulnerability Testing.....	21
3.5 Identifikasi Celah Keamanan.....	21
3.6 Analisis Celah Keamanan.....	22
BAB IV IMPLEMENTASI DAN HASIL ANALISIS.....	25

4.1	Identifikasi dan Analisis Celah Keamanan	25
4.2	Hasil Analisis Celah Keamanan	45
BAB V PENUTUP.....		46
5.1	Kesimpulan.....	46
5.2	Saran.....	46
DAFTAR PUSTAKA		47
LAMPIRAN A		48
LAMPIRAN B		58

DAFTAR GAMBAR

Gambar 1. 2 Statistik Risiko Kerentanan Aplikasi Web Tahun 2022.....	2
Gambar 2. 1 Likelihood and Impact Levels	18
Gambar 2. 2 Overall Risk Severity	18
Gambar 3. 1 Alur Penelitian.....	20
Gambar 3. 2 Rincian Alur Penelitian	20
Gambar 3. 3 Rincian alur Penelitian	20
Gambar 3. 4 Rincian alur Penelitian	21
Gambar 4. 1 Vulnerability Testing.....	25
Gambar 4. 2 Vulnerability Testing 2.....	26
Gambar 4. 3 Hasil Scan Vulnerability Testing	26
Gambar 4. 4 Informasi Celah Keamanan	26
Gambar 4. 5 Hasil Generate Report	27
Gambar 4. 6 Contoh Data Informasi CWE dan OWASP	27
Gambar 4. 7 Common Weakness Enumeration	28
Gambar 4. 8 Diagram Hasil Analisis OWASP Risk Rating	42

DAFTAR TABEL

Tabel 2. 1 Skill Level	10
Tabel 2. 2 Motive	11
Tabel 2. 3 Opportunity	11
Tabel 2. 4 Size	11
Tabel 2. 5 Ease of Discover	12
Tabel 2. 6 Ease of Exploit	12
Tabel 2. 7 Awareness	13
Tabel 2. 8 Instrution Detection.....	13
Tabel 2. 9 Loss of Confidentiality.....	14
Tabel 2. 10 Loss of Integrity	14
Tabel 2. 11 Loss of Availability.....	15
Tabel 2. 12 Loss of Accountability	15
Tabel 2. 13 Financial Damage.....	16
Tabel 2. 14 Reputation Damage	16
Tabel 2. 15 Non-Compliance	17
Tabel 2. 16 Privacy Violation	17
Tabel 3. 1 Format Tabel Celah Keamanan.....	21
Tabel 3. 2 Contoh Tabel Penilaian Likelihood	22
Tabel 3. 3 Contoh Tabel Penilaian Impact	23
Tabel 3. 4 Format Tabel Penilaian Risk Rating	24
Tabel 3. 5 Format Tabel Penentuan Prioritas dan Solusi	24
Tabel 4. 1 Identifikasi Celah Keamanan	29
Tabel 4. 2 Analisis Overall Likelihood OWASP Risk Rating	30
Tabel 4. 3 Analisis Overall Impact OWASP Risk Rating.....	34
Tabel 4. 4 Hasil Analisis OWASP Risk Rating	38
Tabel 4. 5 Tabel Prioritas dan Solusi	39

INTISARI

Keamanan adalah salah satu faktor yang harus sangat diperhatikan ketika membuat sebuah website, perlu diketahui bahwa kelemahan suatu system bisa saja dimanfaatkan oleh beberapa pelaku kejahatan dunia maya dengan tujuan mencuri informasi penting sehingga dapat menyebabkan kerugian, baik secara materi maupun non materi. Seperti halnya pada Sistem Informasi Akademik (SIKAD) Universitas Islam Ahmad Dahlan (UIAD) yang tentunya tidak terlepas dari kemungkinan terjadinya masalah keamanan informasi. Terlebih pada sistem ini masih terdapat kerentanan yang bisa saja dimanfaatkan oleh orang-orang yang tidak bertanggung jawab.

Oleh karena itu penting untuk meningkatkan awareness terhadap keamanan informasi dimana salah satunya adalah melakukan Penilaian Kerentanan (Vulnerability Assesment). Sehingga Pada penelitian ini akan dilakukan identifikasi celah keamanan apa saja yang terdapat pada sistem dan melakukan analisis penilaian untuk menentukan tingkat keparahan dari risiko yang terlibat sehingga dapat dilakukan Tindakan pencegahan dari celah keamanan tersebut. Adapun metode yang digunakan dalam analisis ini adalah Metode OWASP Risk Rating.

Hasil dari analisis celah keamanan pada Sistem Informasi Akademik (SIKAD) adalah berupa daftar celah keamanan apa saja yang terdapat pada sistem, lalu dari hasil identifikasi tersebut kemudian akan dilakukan analisis atau penilaian tingkat keparahan dari celah keamanan yang ada berdasarkan dengan Metodologi OWASP Risk Rating. Dari hasil analisis tersebut akan dikasifikasikan celah keamanan berdasarkan tingkat keparahannya yaitu Critical, High, Medium, atau Low. Hasil dari penelitian ini juga akan diberikan solusi untuk mengatasi celah keamanan yang ada berdasarkan dengan rekomendasi yang ada pada Open Website Application Security Project (OWASP).

Kata Kunci: *Analisis Keamanan Siber, OWASP, Risk Rating, Penilaian Kerentanan*

ABSTRACT

Security is one of the factors that must be paid close attention to when creating a website, please note that the weaknesses of a system can be exploited by some cybercriminals with the aim of stealing important information so that it can cause losses, both material and non-material. As is the case with the University of Islam Ahamad Dahlan (UIAD) Academic Information System (SIKAD), which of course cannot be separated from the possibility of information security problems. Moreover, in this system there are still vulnerabilities that could be exploited by irresponsible people.

Therefore it is important to increase awareness of information security, one of which is to carry out a Vulnerability Assessment. So that this research will identify any security holes in the system and conduct an assessment analysis to determine the severity of the risks involved so that preventive measures can be taken from these security holes. The method used in this analysis is the OWASP Risk Rating Method.

The results of the analysis of security holes in the Academic Information System (SIKAD) are in the form of a list of any security holes that exist in the system, then from the identification results an analysis or assessment of the severity of the existing security holes will be carried out based on the OWASP Risk Rating Methodology. From the results of this analysis, security holes will be classified based on their level of severity, namely Critical, High, Medium, or Low. The results of this research will also provide solutions to overcome existing security holes based on the recommendations in the Open Website Application Security Project (OWASP).

Keywords: *Cyber Security Analyst, OWASP, Risk Rating, Vulnerability Assessment*