

**ANALISIS SISTEM KEAMANAN PADA SISTEM INFORMASI AKADEMIK
(SIKAD) UNIVERSITAS SATYA NEGARA INDONESIA MENGGUNAKAN
METODE PENETRASI TESTING**

SKRIPSI

Diajukan sebagai Salah Satu Syarat untuk Memperoleh Gelar

Sarjana Komputer

Program Studi Teknik Informatika



Oleh :

Nama : Maja Setiawan

NIM : 011401503125113

FAKULTAS TEKNIK

UNIVERSITAS SATYA NEGARA INDONESIA

JAKARTA

2019

**ANALYSIS SECURITY OF THE ACADEMIC INFORMATION SYSTEM
(SIAKAD) OF THE SATYA NEGARA INDONESIA UNIVERSITY USING
THE PENETRATION TESTING METHOD**

SKRIPSI

Proposed As One Of The Requirements To Obtain

Bachelor Degree In Computer Science

Major In Technical Information



**THE FACULTY OF ENGINEERING
SATYA NEGARA INDONESIA UNIVERSITY**

JAKARTA

2019

SURAT PERNYATAAN KARYA SENDIRI

Yang bertanda tangan dibawah ini :

Nama : Maja Setiawan
NIM : 011401503125113
Program Studi : Teknik Informatika

Menyatakan bahwa skripsi ini adalah murni hasil karya sendiri dan seluruh isi skripsi ini menjadi tanggung jawab saya sendiri. Apabila saya mengutip dari karya orang lain maka saya mencantumkan sumbernya sesuai dengan ketentuan yang berlaku. Saya bersedia dikenakan sanksi pembatalan skripsi ini apabila terbukti melakukan tindakan plagiat (penjiplakan).

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya untuk dapat digunakan sebagai mana mestinya.

Bekasi, 27 Agustus 2019



(Maja Setiawan)

011401503125113

LEMBAR PENGESAHAN SKRIPSI

NAMA : Maja Setiawan

NIM : 011401503125113

JURUSAN : Teknik Informatika

KONSENTRASI : Jaringan

JUDUL SKRIPSI : Analisis Sistem Keamanan Pada Sistem Informasi Akademik (SIKAD) Universitas Satya Negara Indonesia Menggunakan Metode Penetrasi Testing

TANGGAL SIDANG : 23 Agustus 2019

Bekasi, 27 Agustus 2019

Dosen Pembimbing II

Dosen Pembimbing I

(Fairy Panoman, S.Kom., MM)

(Abdul Kholiq, S.Kom., M.Kom)

Dekan Fakultas Teknik

Ketua Program Studi

(Ir. Nurhayati, M.Si.)

(Istiqomah Sumadikarta, ST., M.Kom)

LEMBAR PENGESAHAN PENGUJI

**ANALISIS SISTEM KEAMANAN PADA SISTEM INFORMASI
AKADEMIK (SIKAD) UNIVERSITAS SATYA NEGARA INDONESIA
MENGUNAKAN METODE PENETRASI TESTING**

OLEH :

Nama : Maja Setiawan

NIM : 011401503125113

Telah dipertahankan di depan penguji pada tanggal 23 Agustus 2019.

Dan dinyatakan telah memenuhi syarat untuk diterima.

Ketua penguji Rembimbing I

(Abdul Kholiq, S.Kom., M.Kom)

Anggota Penguji I

Anggota Penguji II

(Hernalom Sitorus ST., M.Kom)

(Istiqomah Sumadikarta, ST., M.Kom)

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena berkat rahmat dan karunia-Nya penulis mampu menyelesaikan penyusunan skripsi dengan judul **“Analisis Sistem Keamanan Pada Sistem Informasi Akademik (SIKAD) Universitas Satya Negara Indonesia Menggunakan Metode Penetrasi Testing”**.

Penulisan laporan skripsi ini tersusun atas dukungan berbagai pihak, untuk itu pada kesempatan ini penulis ingin menyampaikan terima kasih kepada:

1. Ibunda dan keluarga tercinta yang selalu memberikan motivasi, dukungan dan do'a.
2. Ibu Ir. Nurhayati, M.Si selaku Dekan Fakultas Teknik Universitas Satya Negara Indonesia.
3. Bapak Istiqomah Sumadikarta, ST., M.Kom selaku Ketua Program Studi Teknik Informatika Universitas Satya Negara Indonesia.
4. Bapak Hernalom Sitorus ST., M.Kom selaku Koordinator Kampus B.
5. Bapak Abdul Kholiq, S.Kom., M.Kom selaku Dosen Pembimbing Akademik sekaligus Dosen Pembimbing I dalam penyusunan skripsi.
6. Bapak Fairy Panomuan selaku Dosen Pembimbing II dalam penyusunan skripsi.
7. Ravika Welmina Mustikataru, S.E terkasih dan tersayang yang selalu support dan mendukung dalam penulisan skripsi ini.
8. Syahreza, S.Kom, Rama Fikli, Samara Ramadhan, Machfi dan Group Angkringan.

9. Sahabat Fakultas Teknik angkatan 2014-2018 di Universitas Satya Negara Indonesia.

10. Semua pihak yang tidak bisa penulis sebutkan satu-persatu yang telah membantu penulis, baik secara langsung maupun tidak langsung dalam menyelesaikan skripsi ini.

Penulis memohon maaf atas segala kekurangan yang terdapat di dalam penulisan skripsi ini. Semoga laporan skripsi ini bermanfaat untuk pengembangan ilmu pengetahuan dan untuk semua pihak yang bersangkutan.

Bekasi, 27 Agustus 2019

Penulis,


Maja Setiawan

ABSTRAK

Keamanan merupakan salah satu faktor penting yang harus diperhatikan dalam membangun sebuah *Website*. Kebutuhan keamanan sebuah *Website* ini timbul dari kebutuhan untuk melindungi data, baik dari kehilangan dan kerusakan maupun dari adanya pihak yang hendak menghalangi akses masuk kedalam sebuah sistem. *Website* Siakad USNI (Universitas Satya Negara Indonesia) dengan domain *siakad.usni.ac.id* merupakan *Website* yang digunakan sebagai media dan sarana publikasi informasi kampus. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap keamanan website, salah satunya adalah dengan melakukan SQL Injection. SQL injection adalah kerentanan yang terjadi ketika penyerang memiliki kemampuan untuk mempengaruhi Structured Query Language (SQL) query yang melewati suatu aplikasi ke database back-end. Dengan diadakannya penelitian ini, diharapkan dapat diperoleh kelemahan dari website UMK. Kelemahan tersebut akan dianalisa sehingga memperoleh solusi kedepan guna pengembangan website yang lebih aman.

Kata kunci: analisa, keamanan, website, SQL injection, DdoS

ABSTRACT

Security is one important factor that must be considered in building a Website. The security needs of this Website arise from the need to protect data, both from loss and damage and from parties who want to prevent access into a system. The Siakad USNI website (Universitas Satya Negara Indonesia) with the siakad.usni.ac.id domain is a Website that is used as a media and campus information publication tool. There are several ways that can be used to test the security of a website, one of which is to do SQL Injection. SQL injection is a vulnerability that occurs when an attacker has the ability to influence Structured Query Language (SQL) queries that pass an application to a back-end database. By holding this research, it is expected that weaknesses can be obtained from the UMK website. These weaknesses will be analyzed in order to obtain future solutions for the development of safer websites.

Keyword: analysis, security, website, SQL injection

DAFTAR ISI

HALAMAN JUDUL	
SURAT PERNYATAAN KARYA SENDIRI	i
LEMBAR PENGESAHAN SKRIPSI	ii
LEMBAR PENGESAHAN PENGUJI	iii
KATA PENGANTAR	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xiv
LAMPIRAN LAMPIRAN	xv
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	3
C. Batasan Masalah.....	3
D. Tujuan dan Manfaat Penelitian	3
D.1 Tujuan Penelitian.....	3
D.2 Manfaat Penelitian.....	4
E. Sistematika Penulisan.....	4
BAB II LANDASAN TEORI	6
A. Tinjauan Pustaka	6
A.1 Detty Metasari Fatah Yasin Irsyadi, S.T., M.T. Ir. Jatmiko, M.T. (2014).....	6

A.2 Pomeroy dan Tan (2011).....	6
A.3 Mia Zattu Maharani, Henry Rossi Andrian S.T., M.T, Setia Juli Irzal Ismail S.T., M.T (2017)	7
A.4 Richard Pangalila, Agustinus Noertjahyana, Justinus Andjarwirawan	7
B. Pengertian Website.....	8
C. Sistem Keamanan Website.....	8
C.1 SSL (<i>Secure Sockets Layer</i>)	9
C.1.a Manfaat Menggunakan SSL (<i>Secure Sockets Layer</i>)	9
C.2 <i>Firewall</i>	10
C.2.a Manfaat Menggunakan <i>Firewall</i>	11
D. Segi Keamanan Web	12
E. Ancaman Keamanan Web.....	14
E.1 Pengertian DOS dan DDoS.....	14
E.1.a Jenis Jenis DDoS Attack	17
a. <i>Ping of Death</i>	17
b. <i>Syn Flooding</i>	18
c. <i>Remote Controlled Attack</i>	18
d. <i>UDP Flood</i>	19
e. <i>Smurf Attack</i>	19
E.2 <i>SQL Injection</i>	20
E.2.a Type <i>SQL Injection</i>	21
E.3 <i>BlindSQL Injection</i>	22
E.4 <i>SSH Shell Injection</i>	23
E.5 <i>Brute Force Attack</i>	24

F. Penetrasi Testing	25
F.1 Tahapan Penetrasi Testing	25
F.1.a Planning	26
F.1.b Information Gathering	26
F.1.c Vulnerability Assessment	26
F.1.c.1 Acunetix Website application scanner	27
F.1.c.2 Nmap (Network Mapper)	27
F.1.d Eksploitasi.....	29
F.1.d.1 Browser	29
F.1.d.2 PuTTY.....	29
F.1.e Reporting.....	30
BAB III METODOLOGI PENELITIAN	31
A. Waktu dan Tempat Penelitian	31
A.1 Waktu Penelitian.....	31
A.2 Tempat Penelitian	31
B. Gambaran Umum Tempat Penelitian.....	31
B.1 Fakultas Teknik (FT).....	34
B.2 Fakultas Perikanan(FP)	34
B.3 Fakultas Ekonomi (FE)	34
B.4 Fakultas Ilmu Sosial dan Ilmu Politik(FISIP)	34
B.5 Fakultas Hukum	35
C. VISI dan MISI Kampus.....	35
C.1 Visi	35
C.2 Misi	35
D. Struktur Organisasi Kampus USNI B	36

E. Analisis Kebutuhan Sistem	36
E.1 Perangkat Keras (<i>Hardware</i>).....	36
E.2 Perangkat Lunak (<i>Software</i>).....	37
F. Metode Pengumpulan Data	37
G. Kerangka Berfikir.....	38
BAB IV ANALISIS DAN HASIL PEMBAHASAN.....	40
A. Analisis Keamanan <i>Website</i> siacad USNI saat ini.....	40
B. Implementasi Penetration Testing.....	42
B.1 Planning.....	42
B.2 Information Gatering	43
B.3 Vulnerability Assesment.....	43
B.3.a <i>Acunetix Vulnerability ApplicationScanner</i>	43
B.3.a.1 Portal Mahasiswa	43
B.3.a.2 Portal Operator.....	45
B.3.b Nmap (<i>Network Mapper</i>)	47
B.4 Exploitation	48
B.4.a Hasil Pengujian Sistem.....	50
a. Hasil Pengujian Dengan SQL Injection.....	50
b. Hasil Pengujian Dengan Blind SQL Injection.....	53
1. Blind SQL Injection	53
2. Mencari Versi MySql.....	55
c. Hasil Pengujian Dengan PuTTY SSH	57
d. Hasil Pengujian Dengan DDoS Attack.....	59
B.5 <i>Reporting</i>	60
C. Pelaksanaan Audit Keamanan Web	61

C.1 Port Scanning.....	61
C.1.a Open Port 22/SSH.....	61
C.2 Web Alert.....	62
C.2.a Blind SQL Injection.....	63
C.2.b HTML form without CSRF Protection	63
C.2.c Login Page Password-guessing Attack	64
D. Laporan Hasil Audit.....	66
BAB V KESIMPULAN DAN SARAN.....	68
A. Kesimpulan.....	68
B. Saran.....	68
DAFTAR PUSTAKA.....	70
LAMPIRAN LAMPIRAN.....	72

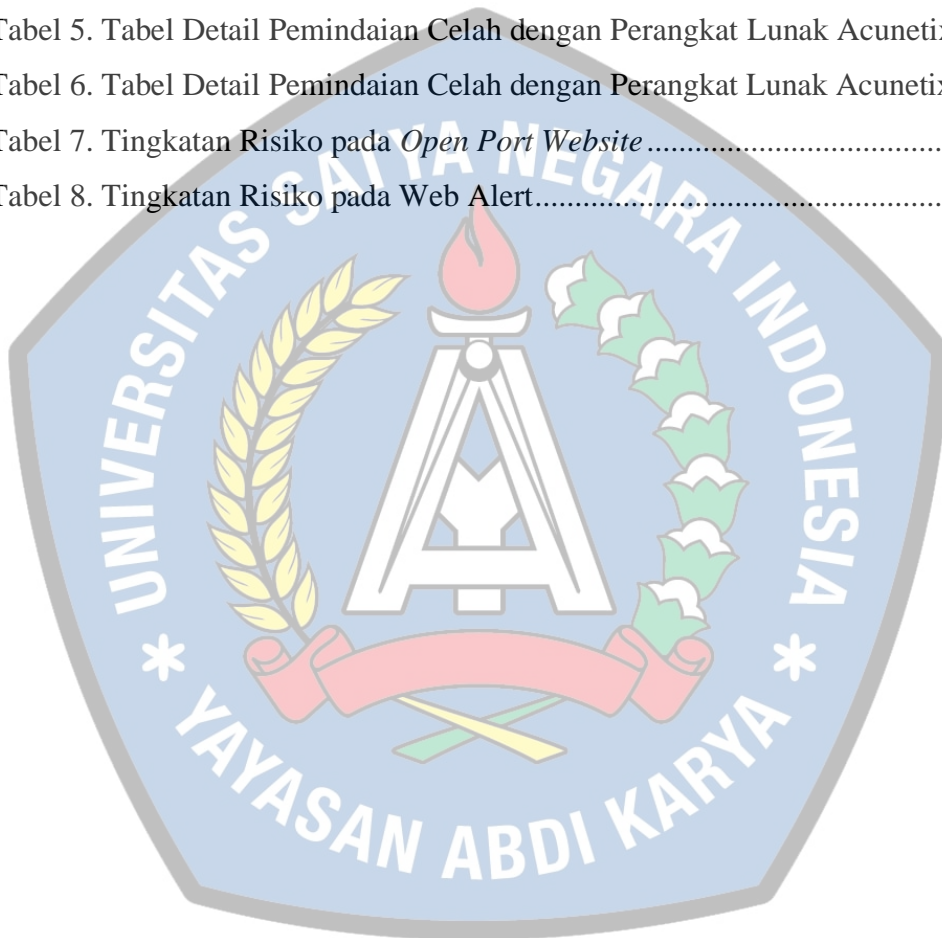


DAFTAR GAMBAR

Gambar 1. Ilustrasi Fiewall	11
Gambar 2. Skema Serangan DdoS	17
Gambar 3. Ilustrasi SQL Injection	20
Gambar 4. SSH Connection	24
Gambar 5. Alur Penetrasi Testing	25
Gambar 6. Struktur Organisasi Kampus B	36
Gambar 7. Skema Kerangka Berpikir	38
Gambar 8. Infrastruktur <i>Websites</i> akad USNI saat ini	40
Gambar 9. Grafik Jumlah Celah Portalmhs Berdasarkan Hasil Pemindaian Celah dengan Perangkat Lunak Acunetix	44
Gambar 10. Grafik Jumlah Celah Portalopr Berdasarkan Hasil Pemindaian Celah dengan Perangkat Lunak Acunetix	46
Gambar 11. Port SSH yang Open	47
Gambar 12. Detail Port SSH yang Open	47
Gambar 13. Tampilan Login Portal Mahasiswa	49
Gambar 14. Tampilan login Portal Operator	49
Gambar 15. Pengujian 1	50
Gambar 16. Pengujian 2	51
Gambar 17. Pengujian 3	51
Gambar 18. Hasil Pengujian SQL <i>Injection</i> (Bypass Halaman <i>Login</i>)	52
Gambar 19. Tampilan Normal KHS	54
Gambar 20. Tampilan setelah ditambah syntax	55
Gambar 21. Kondisi True	56
Gambar 22. Kondisi True	57
Gambar 23. Proses Konfigurasi PuTTY	58
Gambar 24. Percobaan memasukan <i>Password</i> sembarang	58
Gambar 25. Proses Ping ke IP Siakad	59

DAFTAR TABEL

Tabel 1. Penetrasi yang akan dianalisis.....	41
Tabel 2. Serangan yang akan dianalisis	41
Tabel 3. Rencana Analisa.....	42
Tabel 4. Karakteristik <i>Web</i> USNI	43
Tabel 5. Tabel Detail Pemindaian Celah dengan Perangkat Lunak Acunetix	44
Tabel 6. Tabel Detail Pemindaian Celah dengan Perangkat Lunak Acunetix	46
Tabel 7. Tingkatan Risiko pada <i>Open Port Website</i>	62
Tabel 8. Tingkatan Risiko pada Web Alert.....	64



LAMPIRAN LAMPIRAN

Lampiran 1. Web Alerts Portalmhs.....	72
Lampiran 2. Struktur Site Portalmhs.....	72
Lampiran 3. Web Alerts Portalopr	72
Lampiran 4. Struktur Site Portalopr	72
Lampiran 5. Struktur Site CKEditor 4.0.1	72
Lampiran 6. Pertanyaan Wawancara Penelitian.....	72
Lampiran 7. Form Bimbingan Skripsi	72
Lampiran 8. Lembar Persetujuan Sidang.....	72
Lampiran 9. Affected items Blind SQL Injection.....	72
Lampiran 10. Affected items HTML form without CSRF protection.....	72
Lampiran 11. Affected items Login Page Password.....	72

