



UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA

**ANALISIS KEAMANAN SITUS PRESTASI MAHASISWA
UPNVJ MENGGUNAKAN METODE NIST SP 800-115
DENGAN KERENTANAN BERDASARKAN OWASP Top 10**

SKRIPSI

RAFAEL SALOMO SAHAT PIERO

1910511087

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2024

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut:

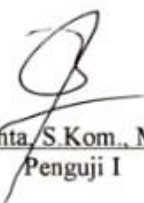
Nama : Rafael Salomo Sahat Piero

NIM. : 1910511087


Program Studi : S1 Informatika

Judul Skripsi/TA. : ANALISIS KEAMANAN SITUS PRESTASI MAHASISWA UPNVJ
MENGUNAKAN METODE NIST SP 800-115 DENGAN
KERENTANAN BERDASARKAN OWASP Top 10


Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian dari persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta.


Jayahta, S.Kom., M.Si.
Penguji I


Rio Wirawan, S.Kom., M.M.S.I.
Penguji II


Bayu Hananto, S.Kom., M.Kom.
Dosen Pembimbing




Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM
Dekan


Dr. Widya Cholil, S.Kom., M.I.T
Ketua Program Studi

Ditetapkan ini : Jakarta

Tanggal Ujian : Jumat, 12 Januari 2024

PERNYATAAN ORISINALITAS


Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun ditujuk telah saya nyatakan dengan benar.

Nama : Rafael Salomo Sahat Piero
NIM : 1910511087
Program Studi : S1 – Informatika

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 22 Januari 2024

Yang Menyatakan,

A handwritten signature in black ink is written over a yellow postage stamp. The stamp features the Garuda Pancasila emblem and the text '2000 METERAI TEMPEL' and 'B0AKX595910280'.

Rafael Salomo Sahat Piero

SURAT PERNYATAAN PERSUTUJUAN

Yang bertanda tangan di bawah ini, saya:

Nama : Rafael Salomo Sahat Piero
NIM : 1910511087
Program Studi : S1 – Informatika
Perguruan Tinggi : Universitas Pembangunan Nasional Veteran Jakarta
Jenis Karya Ilmiah : Skripsi/Tugas Akhir

Dengan ini menyetujui untuk memberikan izin kepada pihak **Universitas Pembangunan Nasional Veteran Jakarta. Hak Bebas Royalti Non-Eksklusif (*Non-exclusive Royalti-Free Right*)** atas karya ilmiah kami yang berjudul:

**ANALISIS KEAMANAN SITUS PRESTASI MAHASISWA UPNVJ
MENGUNAKAN METODE NIST SP 800-115 DENGAN KERENTANAN
BERDASARKAN OWASP Top 10**

Dengan **Hak Bebas Royalti Non-Eksklusif** ini, **Universitas Pembangunan Nasional “Veteran” Jakarta** berhak menyimpan, mengalih-media atau *format*-kan, mengelolanya dalam *database*, mendistribusikan-nya, dan menampilkan atau mempublikasikannya di *internet* atau media lain untuk kepentingan akademis tanpa perlu meminta izin selama tetap mencantumkan nama penulis/pencipta karya ilmiah tersebut.

Demikian pernyataan ini dibuat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 22 Januari 2024

Yang menyatakan,



Rafael Salomo Sahat Piero

ABSTRAK

Teknologi informasi menjadi bagian yang tidak dapat dipisahkan dari kehidupan manusia di masa ini. Salah satu bentuk teknologi informasi yang luas digunakan adalah website. Website mampu diakses dari semua perangkat yang memiliki internet dan web browser. Beberapa website menyediakan layanan yang mengharuskan pengguna menyimpan dan memasukkan data pribadi seperti alamat, nomor identitas, kredensial, dan nomor rekening dan ada juga data yang dihasilkan dari kegiatan pengguna selama mengakses website seperti riwayat transaksi. BSSN menemukan 714.170.967 anomali trafik atau serangan siber dimana 272.962.734 diantaranya terjadi pada bulan Januari 2022 dengan 30% serangan menargetkan lembaga akademik. *Hacker* atau penyerang terus menemukan cara baru dalam melakukan serangan pada aplikasi. Seiring dengan berkembangnya kemampuan *hacker* untuk menembus sistem keamanan web, sistem keamanan web harus diuji untuk mengetahui kemungkinan adanya celah keamanan yang terlewat oleh pihak developer. Untuk melaksanakan uji keamanan tersebut, penelitian ini melakukan penetration testing menggunakan metode NIST SP 800-115 dengan kerentanan berdasarkan Top 10 OWASP pada situs Prestasi Mahasiswa UPNVJ. Diharapkan dari penelitian, peneliti mampu mengetahui dan menjabarkan kerentanan yang ditemukan dalam website Daftar Ulang Calon Mahasiswa Baru UPNVJ beserta rekomendasi penanganannya dan tingkat kerentanannya.

Kata Kunci : Uji Penetrasi, NIST SP 800-115, OWASP Top 10, Keamanan Informasi

ABSTRACT

Information technology is an inseparable part of human life at this time. One form of information technology that is widely used is websites. The website can be accessed from all devices that have internet and web browsers. Some websites provide services that require users to store and enter personal data such as addresses, identity numbers, credentials, and account numbers and there is also data generated from user activities while accessing the website such as transaction history. BSSN found 714,170,967 traffic anomalies or cyberattacks of which 272,962,734 occurred in January 2022 with 30% of attacks targeting academic institutions. Hackers or attackers are constantly finding new ways of carrying out attacks on applications. As the ability of hackers to penetrate web security systems develops, web security systems must be tested to find out the possibility of security loopholes that are missed by the developer. To carry out the security test, this study conducted penetration testing using the NIST SP 800-115 method with vulnerabilities based on the Top 10 OWASP on the UPNVJ prospective new student re-registration site. It is hoped that from the research, researchers will be able to find out and describe the vulnerabilities found on the UPNVJ New Student Candidate Re-list website along with recommendations for handlers and vulnerability levels.

Keywords : *Penetration Testing, NIST SP 800-115, OWASP Top 10, Information Security*

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yesus Kristus, oleh karena berkat dan kasih karunia-Nya, penulis dapat menyelesaikan skripsi yang berjudul “Analisis Keamanan Situs Pendaftaran Ulang Mahasiswa Baru UPNVJ Menggunakan Metode NIST SP 800-115 Dengan Kerentanan Berdasarkan OWASP Top 10”.

Skripsi ini dibuat untuk memenuhi tugas akhir perkuliahan dan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Strata 1 di Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta. Skripsi ini juga dibuat sebagai salah satu wujud implementasi dari ilmu yang didapatkan penulis selama masa perkuliahan di Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, penulis berharap dapat belajar lebih banyak lagi dalam mengimplementasikan ilmu yang didapatkan. Penulis menyadari bahwa skripsi ini tentunya tidak lepas dari bimbingan, masukan, dan arahan dari berbagai pihak. Oleh karena itu, pada kesempatan ini saya ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Kedua orang tua, adik - adik, serta keluarga yang selalu memberi kasih sayang, dukungan material maupun moral dan mendoakan kesuksesan penulisan selama kuliah di Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta hingga mampu menyelesaikan skripsi ini.
2. Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
3. Ibu Dr. Widya Cholil, M.I.T. selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

4. Bapak Bayu Hananto, S.Kom. M.Kom., selaku dosen pembimbing skripsi yang telah membantu penulis dalam penelitian dan penyusunan tugas akhir ini.
5. Bapak Ing. Artambo Benjamin Pangaribuan, M.Eng. dan Bapak Hamonangan Kinantan Prabu, M.T. sebagai Dosen Pembimbing Akademik yang telah bersedia memberikan bimbingan akademik serta bantuan selama kuliah di Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta.
6. Seluruh Bapak/Ibu dosen Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta yang telah memberikan pengetahuan yang sangat bermanfaat selama perkuliahan.
7. Pejuang, The Underground Moles, Syalala, Bang Sam (Brew.inc) serta teman-teman lain yang selalu memberikan support dan dukungan penuh serta mendengarkan segala keluh kesah selama kuliah di Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta.
8. Serta seluruh pihak yang telah membantu dan tidak dapat penulis sebutkan satu persatu.

Tentunya dalam pembuatan skripsi ini, penulis menyadari banyaknya kekurangan pada laporan ini dan juga kendala yang dihadapi. Namun, penulis berharap penelitian ini dapat memberikan dampak dan manfaat bagi pembaca yang tertarik dengan topik penelitian ini.

DAFTAR ISI

LEMBAR PENGESAHAN	II
PERNYATAAN ORISINALITAS.....	II
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	III
ABSTRAK	IV
ABSTRACT	V
KATA PENGANTAR.....	VI
DAFTAR ISI.....	VIII
DAFTAR GAMBAR.....	X
DAFTAR TABEL.....	XIV
BAB I.....	1
1.1 LATAR BELAKANG	1
1.2 RUMUSAN MASALAH.....	3
1.3 TUJUAN PENELITIAN.....	3
1.4 MANFAAT PENELITIAN	4
1.5 RUANG LINGKUP	5
1.6 LUARAN YANG DIHARAPKAN	5
1.7 SISTEMATIKA PENULISAN.....	5
BAB II	7
2.1 KEAMANAN INFORMASI.....	7
2.2 <i>PENETRATION TESTING</i>	8
2.3 NIST SP 800-115	10
2.4 OWASP TOP 10	13
2.5 <i>TOOLS</i> YANG DIGUNAKAN	17
2.6 PENELITIAN TERDAHULU.....	19
BAB III.....	22
3.1 TAHAPAN PENELITIAN	22
3.2 ALAT BANTU PENELITIAN	26
3.3 JADWAL PENELITIAN	27
BAB IV	29
4.1 TOPOLOGI JARINGAN	29
4.1 OBSERVASI	30

4.2 PLANNING.....	34
4.3 DISCOVERY.....	38
4.4 ATTACK.....	40
4.5 REPORTING.....	72
BAB V.....	77
5.1 KESIMPULAN	77
5.2 SARAN.....	78
DAFTAR PUSTAKA	80
LAMPIRAN.....	84
RIWAYAT HIDUP	94

DAFTAR GAMBAR

GAMBAR 2.1 CIA TRIAD (KWEKU, 2009).....	7
GAMBAR 2.2 FASE <i>PENETRATION TESTING</i> PADA NIST SP 800-115 (SCARFONE, ET AL., 2008)	11
GAMBAR 2.3 TAHAPAN DALAM FASE ATTACK DENGAN KEMBALI KE FASE DISCOVERY (SCARFONE, ET AL., 2008)	12
GAMBAR 2.2 <i>OWASP TOP 10 2021</i> DIBANDINGKAN DENGAN 2017 (PRIETO, GONZALES, 2022).....	14
GAMBAR 3.1. TAHAPAN PENELITIAN	23
GAMBAR 3.2 TAHAPAN <i>ATTACK</i>	25
GAMBAR 4.1 TOPOLOGI JARINGAN PENYERANG	29
GAMBAR 4.2 TAMPILAN HALAMAN UTAMA SITUS PRESTASI MAHASISWA UPNVJ	30
GAMBAR 4.3 TAMPILAN SUBMENU AKTIFITAS MAHASISWA PRESMA UPNVJ.....	31
GAMBAR 4.4 TAMPILAN SALAH SATU DETAIL AKTIFITAS MAHASISWA PRESMA UPNVJ	31
GAMBAR 4.5 TAMPILAN MENU STATISTIK PRESMA UPNVJ.....	32
GAMBAR 4.6 TAMPILAN MENU PANDUAN PRESMA UPNVJ.....	32
GAMBAR 4.7 TAMPILAN MENU FAQ PRESMA UPNVJ	32
GAMBAR 4.8 TAMPILAN MENU FAQ PRESMA UPNVJ	33
GAMBAR 4.9 TAMPILAN DASHBOARD USER YANG TELAH LOGIN	33
GAMBAR 4.10 TAMPILAN MENU TAMBAH DATA AKTIVITAS MAHASISWA	34
GAMBAR 4.11 SURAT IZIN RISET DARI UPT TIK UPNVJ.....	35
GAMBAR 4.11 RECORD PADA SITUS WHO.IS.....	36
GAMBAR 4.12 RECORD YANG DITEMUKAN PADA SHODAN	37
<u>≡</u> GAMBAR 4.14 <i>SCANNING</i> DENGAN NMAP	38
GAMBAR 4.15 TAMPILAN DARI INFO.PHP	42
GAMBAR 4.16 KONFIGURASI YANG DITAMPILKAN PADA INFO.PHP	43
GAMBAR 4.17 INFORMASI SENSITIF YANG DITAMPILKAN PADA INFO.PHP.....	43
GAMBAR 4.18 MENU REPEATER PADA BURPSUITE.....	44

GAMBAR 4.19 TARGET HOST PADA TAB REPEATER	45
GAMBAR 4.20 REQUEST NORMAL DARI PROXY BURPSUITE	45
GAMBAR 4.21 REQUEST MENUJU KE ENDPOINT "/" MENGUNAKAN BURPSUITE.....	46
GAMBAR 4.22 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI.....	46
GAMBAR 4.23 REQUEST MENUJU KE ENDPOINT "/" MENGUNAKAN BURPSUITE.....	47
GAMBAR 4.24 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI.....	48
GAMBAR 4.25 REQUEST MENUJU KE ENDPOINT "/" MENGUNAKAN BURPSUITE.....	49
GAMBAR 4.26 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI.....	49
GAMBAR 4.27 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI (/KEGIATAN.HTML).....	51
GAMBAR 4.28 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI MENGGUNAKAN OWASP ZAP(/KEGIATAN/DETAIL/350F976A-94B7-4825-A00C- 175579668AC1_78520.HTML)	52
GAMBAR 4.29 REQUEST MENUJU SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI DENGAN PAYLOAD "?CMD=SLEEP(15)".....	53
GAMBAR 4.30 RESPONSE DARI PAYLOAD "?CMD=SLEEP(15)"	53
GAMBAR 4.31 REQUEST MENUJU SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI (/THEMES/ACE/JS/MYFUNCTIONS.JS?1688132921)	54
GAMBAR 4.32 RESPONSE DARI REQUEST DENGAN PAYLOAD /THEMES/ACE/JS/MYFUNCTIONS.JS?1688132921	55
GAMBAR 4.33 REQUEST MENUJU KE ENDPOINT "/" MENGUNAKAN BURPSUITE.....	56
GAMBAR 4.34 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI.....	56
GAMBAR 4.35 TAMPILAN HASIL DARI REQUEST MENUJU /KEGIATAN/DETAIL/.HTACCESS.....	57
GAMBAR 4.36 RESPONSE DARI REQUEST MENUJU /KEGIATAN/DETAIL/.HTACCESS.....	58

GAMBAR 4.24 TAMPILAN HASIL DARI REQUEST KE SITUS TARGET	58
GAMBAR 4.37 REQUEST MENUJU KE ENDPOINT “/” MENGUNAKAN BURPSUITE	59
GAMBAR 4.38 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	59
GAMBAR 4.39 REQUEST MENUJU KE ENDPOINT “/” MENGUNAKAN BURPSUITE	60
GAMBAR 4.40 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	61
GAMBAR 4.41 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	62
GAMBAR 4.42 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	63
GAMBAR 4.43 REQUEST MENUJU KE ENDPOINT “/” MENGUNAKAN BURPSUITE	64
GAMBAR 4.44 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	64
GAMBAR 4.45 REQUEST MENUJU KE ENDPOINT “/” MENGUNAKAN BURPSUITE	65
GAMBAR 4.46 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	66
GAMBAR 4.47 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	67
GAMBAR 4.48 CVE YANG DIMILIKI BOOTSTRAP VERSI 3.3.6	67
GAMBAR 4.49 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	68
GAMBAR 4.50 CVE YANG DIMILIKI HIGHCHARTS VERSI 6.0.7	68
GAMBAR 4.51 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	68
GAMBAR 4.52 CVE YANG DIMILIKI JQUERY-UI VERSI 1.11.4	69
GAMBAR 4.53 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	70
GAMBAR 4.54 RESPONSE DARI SALAH SATU ENDPOINT DENGAN KERENTANAN YANG TERDETEKSI	70

DAFTAR TABEL

TABEL 3.1 JADWAL PENELITIAN MEI 2022 S/D SEPTEMBER 2023 ...	28
TABEL 4.1 HASIL PEMINDAIAN DENGAN OWASP ZAP	39
TABEL 4.2 PENGELOMPOKAN KERENTANAN DENGAN OWASP TOP 10.....	40
TABEL 4.3 KERENTANAN YANG AKAN DIUJI PADA FASE ATTACK	41
TABEL 4.4 HASIL PENGUJIAN DARI FASE ATTACK.....	75