



**UJI PENETRASI SERVER UNIVERSITAS PQR
MENGUNAKAN METODE *NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY* (NIST SP 800-115)**

SKRIPSI

SYIFA SABRINA ANELIA

1710511076

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2021



**UJI PENETRASI SERVER UNIVERSITAS PQR
MENGUNAKAN METODE *NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY* (NIST SP 800-115)**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar
Sarjana Komputer**

SYIFA SABRINA ANELIA

1710511076

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2021

PERNYATAAN ORISINALITAS

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

Nama : Syifa Sabrina Anelia

NIM : 1710511076

Tanggal : 29 Juni 2021

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

Jakarta, 29 Juni 2021

Yang Menyatakan,



(Syifa Sabrina Anelia)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta saya yang bertanda tangan di bawah ini :

Nama : Syifa Sabrina Anelia

NIM : 1710511076

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non Eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :

UJI PENETRASI SERVER UNIVERSITAS PQR MENGUNAKAN METODE *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* (NIST SP 800-115)

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 29 Juni 2021

Yang Menyatakan,



(Syifa Sabrina Anelia)

LEMBAR PENGESAHAN

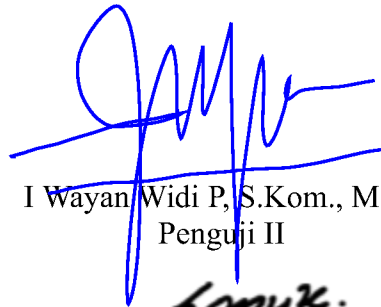
Skripsi diajukan oleh:

Nama : Syifa Sabrina Anelia
NIM : 1710511076
Program Studi : Informatika
Judul Skripsi : Uji Penetrasi Server Universitas PQR Menggunakan Metode *National Institute of Standards and Technology* (NIST SP 800-115)

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



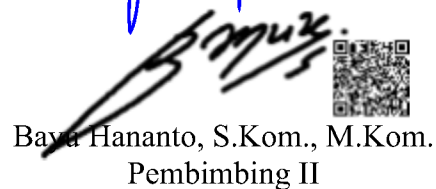

Henki Bayu Seta, S.Kom., MTI.
Penguji I



I Wayan Widi P, S.Kom., MTI.
Penguji II


REVISI_2021

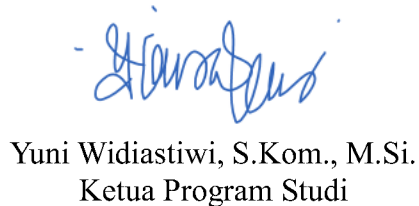
Jayanta, S.Kom., M.Si.
Pembimbing I

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



Dr. Ermatita, M. Kom.
Dekan



Yuni Widiastiwi, S.Kom., M.Si.
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Ujian : 12 Juli 2021



Uji Penetrasi Server Universitas PQR Menggunakan Metode *National Institute of Standards and Technology (NIST SP 800-115)*

Syifa Sabrina Anelia

1710511076

Abstrak

Ancaman keamanan berupa serangan siber telah terjadi di beberapa universitas, sekolah, dan bahkan rumah sakit. Data penting yang terletak pada server sebuah organisasi bisa saja diretas dan diakses oleh orang yang tidak berhak. Salah satu cara untuk menghindari terjadinya peretasan adalah dengan menutup celah-celah keamanan yang mungkin dimiliki sistem. Sebelum menutup celah keamanan, tentu kita harus mengetahui celah keamanan yang ada dengan melakukan pengujian seperti yang dilakukan oleh peretas, namun dengan prosedur yang telah disetujui. Pada penelitian ini dilakukan pengujian penetrasi yang bertujuan untuk menguji kerentanan serta menemukan celah keamanan yang ada pada server Universitas PQR yang menyimpan data pribadi mahasiswa. Uji penetrasi yang dilakukan pada penelitian ini menggunakan metode *National Institute of Standards and Technology (NIST SP 800-115)* yang terdiri dari 4 fase pengujian, yaitu fase *planning*, fase *discovery*, fase *attack*, dan fase *reporting*. Hasil yang didapatkan pada penelitian ini yaitu ditemukannya 13 kerentanan yang dapat dieksploitasi dengan rincian 2 kerentanan termasuk kategori *critical* yaitu *Default Credentials* dan *PHP Unsupported Version Detection*, 3 kerentanan termasuk kategori *high* yaitu *SSL Version 2 and 3 Protocol Detection*, *PHP < 7.3.24 Multiple Vulnerabilities*, *SSL Medium Strength Cipher Suites Supported (SWEET32)*, 8 kerentanan termasuk kategori *medium* yaitu *SSL Certificate Cannot Be Trusted*, *SSL Self-Signed Certificate*, *TLS Version 1.0 Protocol Detection*, *PHPinfo() Information Disclosure*, *Unencrypted Password Form*, *HTTP TRACE / TRACK Methods Allowed*, *SSL Certificate Expiry*, *SSL RC4 Cipher Suites Supported (Bar Mitzvah)*, dan 1 kerentanan adalah *false positive* yaitu *PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability*.

Kata kunci: Uji Penetrasi, NIST SP 800-115, Keamanan Data

Penetration Testing of PQR University's Server Using the National Institute of Standards and Technology (NIST SP 800-115) Method

Syifa Sabrina Anelia

1710511076

Abstract

Security threats in the form of cyber attacks have occurred in several universities, schools, and even hospitals. Important data located on an organization's servers can be hacked and accessed by unauthorized persons. One way to avoid hacking is to close any security holes that the system might have. Before closing the security gap, of course, we must know the existing security holes by doing tests like hackers do, but with an approved procedure. In this study, penetration testing was carried out to test vulnerabilities and find weaknesses that exist on the PQR University's server that stores student personal data. The penetration test conducted in this study uses the National Institute of Standards and Technology (NIST SP 800-115) method which consists of 4 testing phases, namely the planning phase, discovery phase, attack phase, and reporting phase. The results obtained in this study are the discovery of 13 vulnerabilities that can be exploited with details of 2 vulnerabilities including critical categories, namely Default Credentials and PHP Unsupported Version Detection, 3 vulnerabilities including high categories, namely SSL Version 2 and 3 Protocol Detection, PHP < 7.3.24 Multiple Vulnerabilities, SSL Medium Strength Cipher Suites Supported (SWEET32), 8 vulnerabilities including medium categories namely SSL Certificate Cannot Be Trusted, SSL Self-Signed Certificate, TLS Version 1.0 Protocol Detection, PHPinfo() Information Disclosure, Unencrypted Password Form, HTTP TRACE / TRACK Methods Allowed, SSL Certificate Expiry, SSL RC4 Cipher Suites Supported (Bar Mitzvah), and 1 vulnerability is a false positive that is PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

Keywords : Penetration Testing, NIST SP 800-115, Data Security

KATA PENGANTAR

Puji dan syukur Penulis panjatkan ke hadirat Allah SWT atas segala nikmat dan karunia-Nya, sehingga Skripsi ini berhasil diselesaikan. Penulis ingin mengucapkan terima kasih kepada:

1. Orangtua dan keluarga penulis yang selalu mendoakan, serta memberikan dorongan dan nasihat yang terbaik agar dapat menyelesaikan Skripsi ini.
2. Bapak Jayanta, S.Kom., M.SI. selaku dosen pembimbing I Skripsi yang membantu memberikan saran yang bermanfaat.
3. Bapak Bayu Hananto, S.Kom., M.Kom selaku dosen pembimbing II Skripsi yang membantu memberikan saran yang bermanfaat.
4. Rekha, Taufik, Alvita, Yum, Yohanne, dan Bang Rico yang selalu setia memberikan *support* dan membantu menyelesaikan Skripsi ini.
5. Ibu, Bapak Dosen Informatika UPN Veteran Jakarta atas segala pembelajaran dan ilmu-ilmu yang bermanfaat semasa perkuliahan.
6. Teman-teman Informatika 2017 yang selalu mendukung dan membantu semasa perkuliahan.

Akhir kata, semoga skripsi ini dapat bermanfaat bagi para pembacanya.

Jakarta, 29 Juni 2021

Penulis

DAFTAR ISI

UJI PENETRASI SERVER UNIVERSITAS PQR MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST SP 800-115)	1
PERNYATAAN ORISINALITAS	2
PERNYATAAN PERSETUJUAN PUBLIKASI	3
LEMBAR PENGESAHAN	4
Abstrak	5
Abstract	6
KATA PENGANTAR	7
DAFTAR ISI	8
DAFTAR TABEL	11
DAFTAR GAMBAR	12
DAFTAR SIMBOL	13
BAB I	
PENDAHULUAN	14
1.1 Latar Belakang Masalah	14
1.2 Perumusan Masalah	15
1.3 Ruang Lingkup Penelitian	15
1.4 Tujuan dan Manfaat Penelitian	16
1.5 Luaran yang diharapkan	17
1.6 Sistematika Penulisan	17
BAB II	
LANDASAN TEORI	19
2.1 Keamanan Informasi	19
2.2 Uji Penetrasi	20
2.2.1 Black Box Testing	20
2.2.2 White Box Testing	21
2.2.3 Gray Box Testing	21
2.3 NIST SP 800-115	21
2.4 Keamanan Server	24
2.5 NMAP	25
2.6 Metasploit Framework	25

2.7 Nessus	27
2.9 SSLScan	27
2.10 Wireshark	28
2.11 Studi Literatur	28
BAB III	
METODOLOGI PENELITIAN	31
3.1 Tahapan Penelitian	31
3.2 Metode Penelitian	32
3.2.1 Identifikasi Masalah	32
3.2.2 Perumusan Masalah	32
3.2.3 Studi Literatur	32
3.2.4 Fase Planning	32
3.2.5 Fase Discovery	33
3.2.6 Fase Attack	33
3.2.7 Fase Reporting	33
3.3 Alat Bantu Penelitian	34
3.4 Jadwal Penelitian	34
BAB IV	
HASIL DAN PEMBAHASAN	36
4.1 Fase Planning	36
4.2 Fase Discovery	37
4.3 Fase Attack	41
4.3.1 PHP Remote Code Execution Vulnerability	42
4.3.2 PHP Unsupported Version Detection	43
4.3.3 PHP < 7.3.24 Multiple Vulnerability	44
4.3.4 HTTP TRACE / TRACK Methods Allowed	45
4.3.5 SSL Version 2 and 3 Protocol Detection	46
4.3.6 SSL Medium Strength Cipher Suites Supported (SWEET32)	47
4.3.7 TLS Version 1.0 Protocol Detection	47
4.3.8 SSL Certificate	48
4.3.9 SSL RC4 Cipher Suites Supported (Bar Mitzvah)	49
4.3.10 SSH Brute Force	50
4.3.11 Unencrypted Password Form	51
4.3.12 PHPinfo() Information Disclosure	52
4.3.13 Default Credential	54
4.3.14 PostgreSQL Login Brute Force	56
4.4 Fase Reporting	57
BAB V	
KESIMPULAN DAN SARAN	62

5.1 Kesimpulan	62
5.2 Saran	63
DAFTAR PUSTAKA	65
RIWAYAT HIDUP	67
LAMPIRAN	68





DAFTAR TABEL

Tabel 3.1 Jadwal Penelitian	35
Tabel 4.1 Hasil Pemindaian <i>Port</i> dengan NMAP	37
Tabel 4.2 Hasil Analisis Kerentanan Menggunakan Nessus	38
Tabel 4.3 Hasil Analisis Kerentanan Menggunakan Nikto	40
Tabel 4.4 Hasil Pemindaian Kerentanan Pada Port 80	42
Tabel 4.5 Hasil Pemindaian Kerentanan Pada Port 443	46
Tabel 4.6 Tabel Hasil Uji Kerentanan	58

DAFTAR GAMBAR

Gambar 2.1 Aspek dalam Keamanan Informasi (CIA Triad)	19
Gambar 2.2 Fase <i>Penetration Testing</i> Pada Metode NIST	22
Gambar 2.3 Fase <i>Attack</i> dengan umpan balik ke fase <i>Discovery</i>	23
Gambar 3.1 <i>Flowchart</i> Tahapan Penelitian	31
Gambar 4.1 Hasil Pemindaian <i>dig</i>	37
Gambar 4.2 Exploit pada Kerentanan PHP <i>Remote Code Execution</i>	43
Gambar 4.3 Versi PHP yang Digunakan Sistem Target Saat Ini	43
Gambar 4.4 Versi PHP yang Didukung Saat Ini	44
Gambar 4.5 Cabang PHP yang Tidak Didukung	44
Gambar 4.6 Metode yang didukung HTTP TRACE	45
Gambar 4.7 Eksploitasi HTTP TRACE	45
Gambar 4.8 Pemindaian SSL	46
Gambar 4.9 Pemindaian <i>ssl-enum-ciphers</i>	47
Gambar 4.10 Pemindaian TLS	48
Gambar 4.11 Validasi Kerentanan Sertifikat SSL	49
Gambar 4.12 Pemindaian <i>ssl-enum-ciphers</i>	50
Gambar 4.13 SSH <i>Brute Force</i>	51
Gambar 4.14 <i>Network Sniffing</i> pada Wireshark	52
Gambar 4.15 Hasil pemindaian <i>files_dir</i> dengan Metasploit	53
Gambar 4.16 Informasi yang ada pada <i>/info.php</i>	54
Gambar 4.17 Percobaan <i>Login</i> pada Halaman Awal Server	55
Gambar 4.18 Data Pribadi Pegawai dalam Sistem Target	55
Gambar 4.19 <i>PostgreSQL Login Brute Force</i>	56
Gambar 4.20 <i>PostgreSQL Brute Force</i> dengan <i>Hydra</i>	56

DAFTAR SIMBOL

Simbol	Nama Simbol	Keterangan
	Simbol Proses	Menggambarkan Proses
	Simbol Dokumen	Dokumen yang dibutuhkan dalam proses sistem
	Simbol arah data atau arus data	Sebagai petunjuk arah data dan arus data pada proses
	Simbol Terminator	Simbol untuk permulaan atau akhir dari suatu kegiatan