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