ABSTRAK

Judul : Penerapan Metode NIST 800-115 Framework Untuk Mendeteksi Keamanan Informasi Pada Aplikasi *Repositori Digital* Berdasarkan OWASP Top 10 Model 2021 (Studi Kasus: Perpustakaan Universitas Esa Unggul)

Nama : Willy Apriza

Program Studi : Teknik Informatika

Universitas Esa Unggul merupakan salah satu perguruan tinggi swasta terkemuka di Indonesia. Salah satu layanan yang disediakan adalah Repositori Digital. Sebelumnya, aplikasi repositori digital tersebut pernah mengalami serangan spam. Maka dari itu, perlu dilakukan tinjauan aspek keamanan yang ada pada aplikasi tersebut. Pada penelitian ini, akan dilakukan penerapan metode NIST 800-115 untuk mendeteksi keamanan informasi yang terdapat pada aplikasi *Repositori Digital* Universitas Esa Unggul berdasarkan OWASP Top 10 2021. Hasil dari penelitian ditemukan bahwa aplikasi web memiliki 3 kerentanan dengan *severity high* yaitu Cross-Site Scripting (XSS), *Session Hijacking*, *Cross-Site Request Forgery* (CSRF); 5 kerentanan dengan *severity medium* yaitu *Absence of Anti-CSRF Tokens*, *Content Security Policy* (CSP) *Header Not Set*, *Directory Browsing*, *Missing Anti-clickjacking Header*, *Permits Brute Force Attack*; dan 10 kerentanan dengan *severity low* yaitu *Cookie Without SameSite Attribute, Private IP Disclosure, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Cookie No HttpOnly Flag, Cookie Without Secure Flag, Strict-Transport-Security Disabled, Strict-Transport-Security Header Not Set, X-Content-Type-Options Header Missing, Outdated PHP version 5.3.10, Cross-Domain JavaScript Source File Inclusion*. Untuk mengatasi kerentanan tersebut, diberikan beberapa rekomendasi seperti perlunya validasi dan sanitasi input, pengaturan keamanan pada server, dan pengaturan header keamanan pada aplikasi web sebagai upaya peningkatan aspek keamanan aplikasi repositori digital Universitas Esa Unggul.

Kata kunci : NIST 800-115, *Penetration Testing*, OWASP Top 10 2021

ABSTRACT

Title : Implementation of NIST 800-115 Framework Method to Detect Information Security in Digital Repository Application Based on OWASP Top 10 Model 2021 (Case Study: Esa Unggul University Library)

Name : Willy Apriza

Study Program : Informatics Enggineering

Esa Unggul University is one of the leading private universities in Indonesia. One of the services provided is the library. One of the library's asset is digital repository. Previously, the digital repository application had experienced spam attacks. Therefore, it is necessary to conduct a security review of the applications. In this research, the application of the NIST 800-115 method will be carried out to detect information security contained in the Esa Unggul University Digital Repository application based on the OWASP Top 10 2021. The research found that the web application has 3 vulnerabilities with high severity, namely Cross-Site Scripting (XSS), Session Hijacking, and Cross-Site Request Forgery (CSRF); 5 vulnerabilities with medium severity, namely Absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header Not Set, Directory Browsing, Missing Anti-clickjacking Header, and Permits Brute Force Attack; and 10 vulnerabilities with low severity, namely Cookie Without SameSite Attribute, Private IP Disclosure, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Cookie No HttpOnly Flag, Cookie Without Secure Flag, Strict-Transport-Security Disabled, Strict-Transport-Security Header Not Set, X-Content-Type-Options Header Missing, Outdated PHP version 5.3.10, and Cross-Domain JavaScript Source File Inclusion. To address these vulnerabilities, several recommendations are provided, such as the need for input validation and sanitization, security configuration on the server, and setting security headers on the web application, as part of the efforts to enhance the security aspects of the digital repository application at Esa Unggul University.

Keywords : NIST 800-115, *Penetration Testing*, OWASP Top 10 2021