Intisari

Uji Keamanan Sistem Informasi UGM Dalam Menghadapi Serangan Siber

Oleh

Daffa Nafis Sing Bagus
19/440787/PA/19107

Dalam beberapa tahun terakhir ini, serangan dan kejahatan siber semakin meningkat, terutama pada organisasi. Dari berbagai perusahaan dan organisasi, sektor edukasi merupakan salah satu yang paling sering mengalami serangan siber. Serangan siber terhadap institusi edukasi mengalami peningkatan sebanyak 70%, dari 129 serangan pada tahun 2022 menjadi 265 serangan pada tahun 2023. Tentunya serangan tersebut bersifat merugikan baik bagi institusi maupun individu. UGM sendiri memiliki sistem informasi yang digunakan oleh *civitas academica*, sehingga memiliki berbagai data dan informasi sensitif. Oleh karena itu, akan dilakukan uji keamanan terhadap sistem informasi UGM berdasarkan OWASP Top 10 untuk mengetahui kerentanan yang dimiliki sistem dan cara mengeksploitasi kerentanan tersebut.

Uji keamanan dilakukan secara *black-box*, yang berarti diketahui beberapa arsitektur dan cara kerja sistem informasi sesuai dengan ruang lingkup yang ditentukan. Uji keamanan menggunakan metodologi uji penetrasi NIST yang memiliki 4 tahap. Tahap pertama (*planning*) menentukan ruang lingkup pengujian, tahap kedua (*discovery*) menggunakan *tools* seperti nmap, wireshark, zap, dan burp suite untuk mencari dan mengidentifikas kerentanan, tahap ketiga (*attacking*) menggunakan *tools* untuk melakukan penyerangan dan memastikan kerentanan tersebut bukan *false positive*, dan tahap terakhir (*reporting*) melaporkan kerentanan yanbg ditemukan, memberi nilai keparahan, dan rekomendasi aksi yang dapat dilakukan.

Setelah dilakukan uji keamanan, ditemukan ditemukan 12 kerentanan. Dari 12 kerentanan tersebut, 1 termasuk tingkat High, yang berupa *Server-Side Request Forgery*, 4 termasuk tingkat Medium, yang berupa *Content Security Policy (CSP) Header Not Set, Cross Site Scripting (Reflected), Vulnerable Bootstrap version*, dan *Vulnerable jQuery version*, dan 7 termasuk tingkat Low, yang berupa *Cookie No HttpOnly Flag, Cookie Without Secure Flag, Cookie without SameSite Attribute, Big Redirect Detected (Potential Sensitive Information Leak), Cross-Domain JavaScript Source File Inclusion, Server Leaks Version Information via "Server" HTTP Response Header Field, dan Strict-Transport-Security Header Not Set*.

Kata Kunci: Uji penetrasi, Keamanan siber, Sistem Informasi UGM, *Vulnerability Assessment*, OWASP Top 10, Black-Box testing

Abstract

Security Analysis of UGM Information System in Facing Cyber Attacks

By

Daffa Nafis Sing Bagus
19/440787/PA/19107

In recent years, cyberattacks and crimes have been on the rise, especially in organizations. Of the various companies and organizations, the education sector is one of the most frequently affected by cyberattacks. Cyberattacks against educational institutions have increased by 70%, from 129 attacks in 2022 to 265 attacks in 2023. Of course, these attacks are detrimental to both institutions and individuals. UGM itself has an information system that is used by the academic community, so it has a variety of sensitive data and information. Therefore, a security test will be conducted on the UGM information system based on the OWASP Top 10 to find out the vulnerabilities that the system has and how to exploit these vulnerabilities.

Security tests are conducted in a black-box manner, which means that some of the architecture and workings of the information system are known according to the specified scope. The security test uses the NIST penetration test methodology which has 4 stages. The first stage (planning) determines the scope of testing, the second stage (discovery) uses tools such as nmap, wireshark, zap, and burp suite to search for and identify vulnerabilities, the third stage (attacking) uses tools to perform attacks and ensure that the vulnerability is not a false positive, and the last stage (reporting) reports the vulnerabilities found, gives a severity value, and recommends actions that can be taken.

After conducting security tests, 12 vulnerabilities were found. Of the 12 vulnerabilities, 1 belongs to the High level, which is Server-Side Request Forgery, 4 belongs to the Medium level, which is Content Security Policy (CSP) Header Not Set, Cross Site Scripting (Reflected), Vulnerable Bootstrap version, and Vulnerable jQuery version, and 7 belongs to the Low level, which are Cookie No HttpOnly Flag, Cookie Without Secure Flag, Cookie without SameSite Attribute, Big Redirect Detected (Potential Sensitive Information Leak), Cross-Domain JavaScript Source File Inclusion, Server Leaks Version Information via "Server" HTTP Response Header Field, and Strict-Transport-Security Header Not Set.

Keywords: Penetration Test, Cyber Security, UGM Information System, *Vulnerability Assessment*, OWASP Top 10, Black Box testing