INTISARI

Situs website yang tidak memiliki keamanan yang memadai akan menjadi sasaran bagi para peretas cyber. Kerentanan keamanan website yang paling sering dijumpai adalah Injeksi SQL, Cross-Site Scripting (XSS), dan Cross-Site Request Forgery (CSRF) untuk mencuri data atau mengambil alih kontrol website. Peneliti ini bertujuan menganalis keamanan website menggunakan metode Penetration Testing Execution Standard (PTES) dengan tahapan yang digunakan Intelegence Gathering, Threat Modeling, Vulnerabillity Analysis, Exploitation, dan Reporting. Hasil penelitian menggunakan scaning tool OWASP ZAP menunjukkan adanya 7 kerentanan pada website, dengan tingkat risiko 4 medium risk dan 3 low risk. Pada tahapan exploitation disimpulkan bahwa website yang digunakan memiliki tingkat keamanan yang tinggi karena hanya ada satu pengujian yang berhasil. Hal ini terjadi karena website telah menerapkan penggunaan SSL, aktivasi fitur Content Security Policy (CSP), implementasi token anti Cross-Site Request Forgery (CSRF), dan konfigurasi header X-Frame-Options sebagai langkah keamanan. Meskipun website telah memiliki keamanan yang kuat pengembang harus melakukan cek keamanan teratur untuk memastikan website aman dari serangan ataupun kerentanan yang mungkin akan terjadi. Menggunakan alat scaning yang beragam adalah saran untuk peneliti lain untuk menemukan kerentanan dengan lebih akurat.

.

Kata kunci: Website, keamanan, PTES

ABSTRACT

Websites that do not have adequate security will be targeted by cyber hackers. The most common website security vulnerabilities are SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) to steal data or take control of the website. This researcher aims to analyze website security using the Penetration Testing Execution Standard (PTES) method with the stages used Intelligence Gathering, Threat Modeling, Vulnerabillity Analysis, Exploitation, and Reporting. The results of the research using the OWASP ZAP scaning tool showed 7 vulnerabilities on the website, with a risk level of 4 medium risk and 3 low risk. At the exploitation stage, it is concluded that the website used has a high level of security because there are no successful tests. This happens because the website has implemented the use of SSL, activation of the Content Security Policy (CSP) feature, implementation of anti Cross-Site Request Forgery (CSRF) tokens, and configuration of the X-Frame-Options header as a security measure. Even though the website has strong security in place developers should perform regular security checks to ensure the website is safe from any attacks or vulnerabilities that may occur. Using various scaning tools is a suggestion for other researchers to find vulnerabilities more accurately.

Keywords: Website's, security's, PTES