ABSTRACT

Analisis penetration testing web adalah tindakan menganalisa atau mencari suatu informasi yang berguna untuk pengelolaan suatu web yang fokus pada hal-hal yang berkaitan dengan suatu keamanan web. Tujuan penelitian ini adalah untuk mencari celah kerentanan keamanan pada web usahidsolo.ac.id dan memberikan solusi untuk memperbaiki celah kerentanan tersebut. Metode pengumpulan data dalam penelitian ini menggunakan metode observasi, wawancara dan studi literatur. Untuk mengetahui celah kerentanan keamanan pada usahidsolo.ac.id mengacu pada metode Open Web Application Security Project (OWASP) Top 10 Tahun 2017. Dengan didukung pencarian informasi dasar mengenai web usahidsolo.ac.id menggunakan tools whois dan google search engine. Sedangkan untuk pencarian informasi yang lebih spesifik tool yang digunakan adalah OWASPZap. Penelitian ini menghasilkan beberapa resiko keamanan yaitu directory browsing, Vulnerable JS Library, X-Frame-Option Header Not set, Absense Of Anti-CSRF Tokens dan Cross-Domain JavaScript Source File Inclusion. Untuk tingkatan resikonya menurut hasil penelitian yaitu tingkat medium dan tingkat low. Hasil penelitian celah keamanan ini nanti dapat membantu pengelola website untuk menyadari resiko keamanan yang mungkin terjadi sehingga dapat diambil tindakan pencegahan dan mengurangi resiko tersebut.

Kata Kunci : OWASP Top 10 2017, OWASPZap, analisis *penetration testing*

ABSTRACT

Web penetration testing analysis is the act of analyzing or searching for helpful information for managing a web focused on web security. The study aims to find security vulnerabilities on the usahidsolo.ac.id web and provide solutions to fix these vulnerabilities. The data collection method used the method of observation, interviews and literature study. To find out the security vulnerabilities in usahidsolo.ac.id, it refers to the Open Web Application Security Project (OWASP) Top 10 of 2017, and it is also supported by searching for basic information about the usahidsolo.ac.id web using whois tools and google search engines. Meanwhile, OWASPZap is used in searching for more specific information. This research resulted in several security risks, namely directory browsing, Vulnerable JS Library, X-Frame-Option Header Not set, Absense Of Anti-CSRF Tokens and Cross-Domain JavaScript Source File Inclusion. The study results show that the level of risk belongs to the medium level and low level. The results of this security vulnerability research can help website managers be aware of security risks that occurred so that preventive actions can be taken and reduce these risks.

Keywords: OWASP Top 10 2017, OWASPZap, Analysis Penetration Testing