INTISARI

SIPELITAMAS merupakan website yang dikelola oleh LPPM Universitas Amikom Purwokerto yang digunakan untuk memberikan pelayanan terkait dengan pengelolaan penelitian dan pengabdian kepada masyarakat. Berangkat dari hal tersebut, tentunya sistem ini tidak terlepas dari kemungkinan terjadinya serangan dan rentan terhadap pencurian data serta informasi. Oleh karena itu perlu adanya pengujian vulnerability website SIPELITAMAS dengan menggunakan metode Web Security Testing Guide (WSTG). Penelitian ini dilakukan dengan tujuan untuk mengidentifikasi celah keamanan pada website SIPELITAMAS dengan menggunakan metode Web Security Testing Guide v4.2. Penelitian ini hanya membahas mengenai metode WTSG. Pengujian yang dilakukan hanya menggunakan delapan teknik yaitu Information Gathering, Configuration And Deployment Management Testing, Authentication Testing, Authorization Testing, Session Management Testing, Input Validation Testing, Testing For Weak Cryptography dan Client-Side Testing. Hasil dari pengujian keseluruhan yang telah dilakukan pada website SIPELITAMAS ditemukan 14 celah keamanan yang dapat membahayakan keamanan website SIPELITAMAS dengan perincian pada pengujian menggunakan tools OWASP ZAP telah ditemukan 1 celah dengan tingkat risiko high, 2 celah dengan tingkat risiko medium, 3 celah dengan tingkat risiko low, pengujian menggunakan tools Bing diperoleh 5 celah kerentanan, pengujian menggunakan tools Terminator diperoleh 1 celah kerentanan, pada tools Chrom diperoleh 1 celah kerentanan dan pada tools Nmap diperoleh 1 celah kerentanan. Metode WSTG V4.2 layak dijadikan sebagai acuan dalam melakukan uji vulnerability pada website SIPELITAMAS. Hal ini dapat dilihat dari hasil pengujian dan analisa yang menunjukkan bahwa website SIPELITAMAS memiliki kelemahan yang dapat dieksploitasi setelah dilakukan pengujian celah keamanan berdasarkan panduan WSTG V4.2.

Kata kunci: WSTG V4.2, Website, Vulnerability

ABSTRACT

SIPELITAMAS is a website managed by LPPM Amikom University Purwokerto which is used to provide services related to research management and community service. Departing from this, of course this system is inseparable from the possibility of attacks and being vulnerable to data and information theft. Therefore it is necessary to test the vulnerability of the SIPELITAMAS website using the Web Security Testing Guide (WSTG) method. This research was conducted with the aim of identifying security holes on the SIPELITAMAS website using the Web Security Testing Guide v4.2 method. This study only discusses the WTSG method. The tests were carried out using only eight techniques, namely Information Gathering, Configuration And Deployment Management Testing, Authentication Testing, Authorization Testing, Session Management Testing, Input Validation Testing, Testing For Weak Cryptography and Client-Side Testing. The results of the overall testing that has been carried out on the SIPELITAMAS website found 14 security holes that could endanger the security of the SIPELITAMAS website with details on testing using OWASP ZAP tools found 1 gap with a high level of risk, 2 holes with a medium risk level, 3 holes with a low level of risk, testing using Bing tools obtained 5 vulnerabilities, testing using the Terminator tool obtained 1 vulnerability, Chrom tools obtained 1 vulnerability and Nmap tools obtained 1 vulnerability. The WSTG V4.2 method is appropriate as a reference in conducting vulnerability tests on the SIPELITAMAS website. This can be seen from the results of testing and analysis which show that the SIPELITAMAS website has weaknesses that can be exploited after testing for security holes based on WSTG V4.2 guidelines.

Keywords: WSTG V4.2, Website, Vulnerability