

ABSTRACT

Along with technological developments, information is very ease to obtain and disseminate and has become an important asset for companies. System security is one part of technological development. Information systems must ensure confidentiality, availability and integrity of all information resources. XYZ Hospital Surabaya is one of the health agencies that uses a website-based information system for health information media. However, based on the results of interviews with the IT coordinator at the XYZ hospital stated that the instansixyz.com website had been hacked by changing the appearance of the website. This proves that the instansixyz.com website is vulnerable to attacks, and the antrianinstansixyz.com website, which contains sensitive patient data such as KTP, NIK, Address, etc., is also feared to suffer similar attacks like instansixyz.com, so it is necessary to carry out security testing to minimize vulnerability gaps. which can be exploited by irresponsible parties. The aim of this research is to conduct a vulnerability analysis on the XYZ Hospital website to find out what vulnerabilities are on the website and provide recommendations to the hospital. The method used in this research is penetration testing with the OWASP framework approach. The research results found how many vulnerabilities there were using different tools. As many as 21 different vulnerabilities were found on both websites. From the vulnerabilities found, researchers made recommendations for improvements for website developers to increase security for both websites.

Keywords: Penetration Testing, OWASP, System Security