

ABSTRACT

Information systems play an important role in various fields and aspects of life in the world of business, economy and politics. This is because information systems make it easier for people to get information. However, there are still many parties who take advantage of this information technology development irresponsibly. The problem that often occurs in this era is hacking. Hacking is an activity of breaking into computer programs belonging to other people/parties. Hackers are people who like to hack computers, have the expertise to create and read certain programs, and are obsessed with observing their security. SMK XYZ provides information via the website, both information regarding school introductions to information regarding registration of new students. A weak website security system can become a target for irresponsible parties. Irresponsible parties can steal important data on the PPDB SMK XYZ website, such as username and password data, and personal data of prospective students. Based on the existing conditions, the authors conducted research to be able to find out and analyze the level of security used on the PPDB SMK XYZ website. In this study, the authors tested the PPDB website owned by SMK XYZ using the Penetration Testing (Pentest) method with the Open Web Application Security Project (OWASP) approach. The test results will become suggestions, recommendations, and website vulnerability solutions that can be used by PPDB SMK XYZ web managers so that the security level is even better.

Keywords: *(OWASP Framework, Information System Security, Penetration Testing, PPDB website)*