ABSTRACT

Security vulnerability detection in web applications is commonly performed through penetration testing, an attack simulation process to identify and address security weaknesses. However, manual penetration testing requires in-depth technical expertise and is time-consuming. This research aims to develop a Python-based engine, CA-Scanner, for the automated detection of website security vulnerabilities, focusing on one of the most common vulnerabilities, Path Traversal. CA-Scanner has been successfully implemented as a Python-based application capable of automatically identifying Path Traversal vulnerabilities on target URLs. The detection results are presented in an informative web interface, displaying the vulnerable URL, the attack payload used, and recommended solutions such as stricter input validation and directory access restrictions. This application is expected to contribute to enhancing website information security against cyber threats.

Keywords: ***Automatic Vulnerability Detection***, ***Path Traversal***, ***Website Security***, **Python**