ASSESSING WORDPRESS PLUGIN SECURITY: COMMON VULNERABILITIES, SECURITY-READINESS MEASUREMENT, AND A PROTOTYPE VULNERABILITY DETECTION TOOL

Student: Lubabatu Ibrahim Betso
C00304260@setu.ie

Supervisor: Mark Cummins

INTRODUCTION

Launched in 2003, WordPress has become a leading content management system (CMS) comprising 63% of the CMS maket and powering more than 42% of websites globally (Yadav, 2025). Its prevalence stems from its open-source nature, user-friendly interface and extensive plugin ecosystem with over 50,000 plugins. These plugins enable users to enhance their website functionality in areas such as SEC), e-commerce, and security without requiring high level coding skills (Balkhi, 2025). While these plugins come with advantages they also introduce security risks making them vulnerable to exploitation This study is aimed at evaluating the most common plugin vulnerabilities associated with WordPress using the CVSS and OWASP Top 10 vulnerabilites, their severity levels and lifecycle. The study also intends to explore current discussions amongst developers surrounding the improvement of plugin security and update practices.

LITERATURE REVIEW

Historically, WordPress plugin users were only cognizant of functionalities offered plugins giving very little regard for security As cybersecurity awareness became more widespread with time, the attention has significantly shifted to plugin risks particularly with events such as the mu-Plugin attack, traffic was redirected due to malicious PHP scripts injected into a hidden directory (Lakshmanan, 2025).
Mesa et al. (2018) identified Cross-site Scripting (XSS), SQL Injection, and CSRF as the most prevalent vulnerabilities associated with WordPress plugins The study however lacked insight into the primary causes and evolving patterns Walden et al. (2010) addressed this gap in prior research and highlighting the differences between core code and plugin code, indicating plugins with more than 50 lines of code containing more vulnerabilities than those with less.

EXPECTED FINDINGS

- XSS is the most common vulnerability in WordPress plugins.
- The developed vulnerability detection tool detects and alerts admins within the WordPress environment when a vulnerable plugin is activated. This reduces reliance on external sources like WPScan and National Vulnerability Database.
- The study introduces a quantitative metric to assess vulnerability severity relative to exposure time: SRM = (CVSS Score / Exposure Days) × 100

RESEARCH OBJECTIVES

1. The first objective of this study is to determine and evaluate the most common vulnerabilities associated with WordPress plugins at present, their impact and severity level according to the Common Vulnerability Scoring System (CVSS) and OWASP Top 10 Vulnerabilities.
2. The second objective of this study is aimed at evaluating the current lifespan of these plugin vulnerabilities to affirm whether there has been an increase or a decrease over the years and create a security readiness metric based on the CVE, CVSS and the vulnerability lifecycle.
3. The third objective is to develop and implement a tool that notifies WordPress Administrators when a plugin is identified as vulnerable during activation.

METHODOLOGY

- Empirical: Real-world data collection from vulnerability databases and plugin repositories.
- Quantitative: Statistical analysis of CVSS scores, vulnerability frequency, and exposure duration.
- Design Science Research (DSR). A Prototype vulnerability detection tool will be developed and deployed.

TOOLS

- XAMPP
- Apache
- VirtualBox
- Ubuntu
- WPScan
- WordPress
- Microsoft Excel
- Windows Powershell
- Linux Terminal
- Visual Studio
- Linux Text Editor