

Practical Report: Cross-Site Scripting (XSS) in OWASP Mutillidae II - Password Generator



**by
Rajan Nisargan**

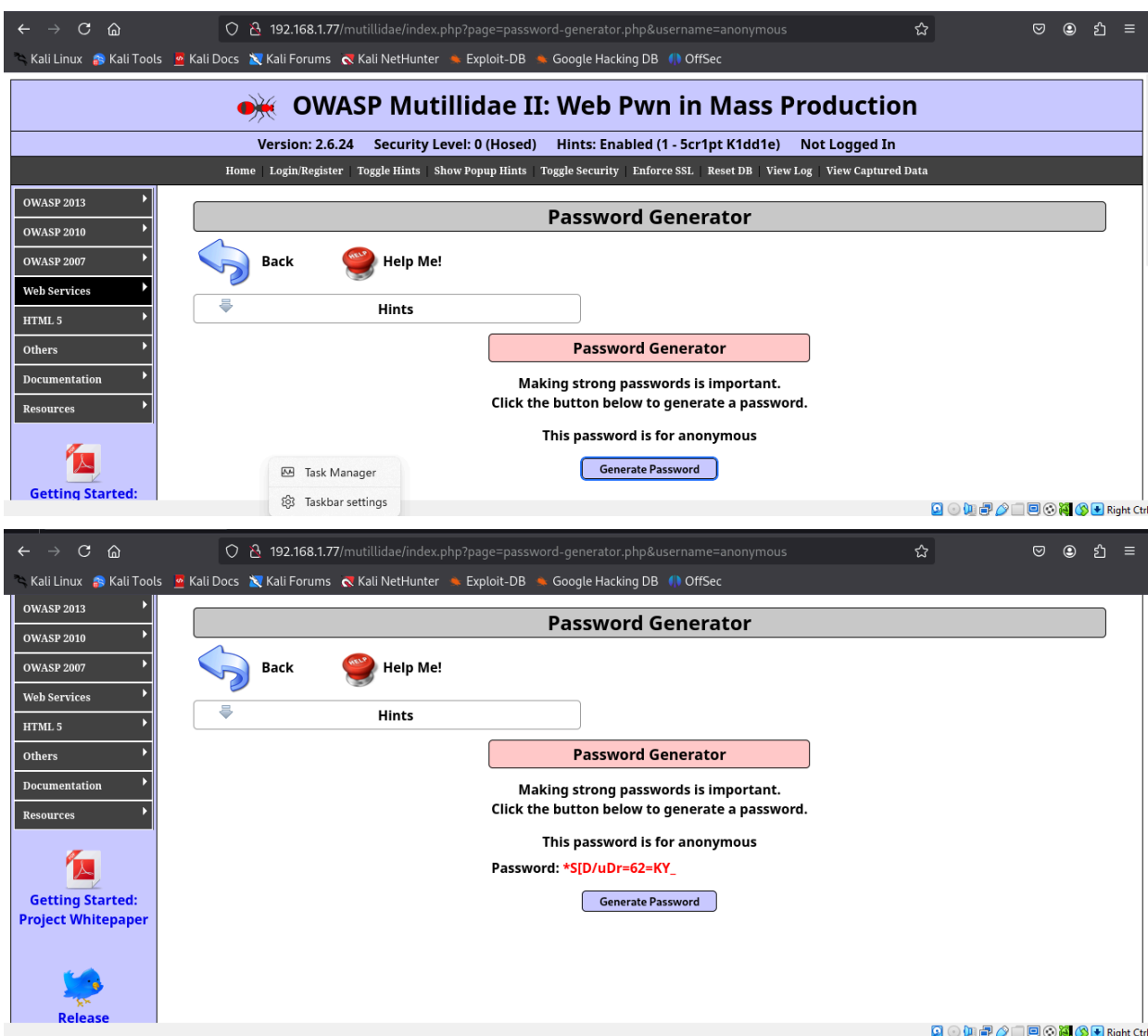
Introduction:

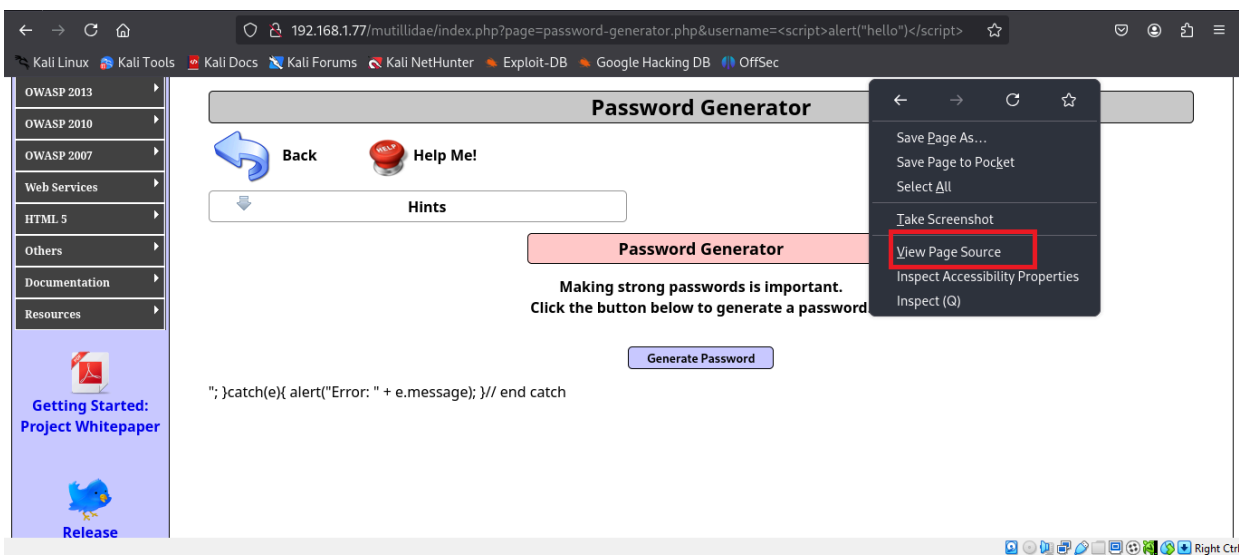
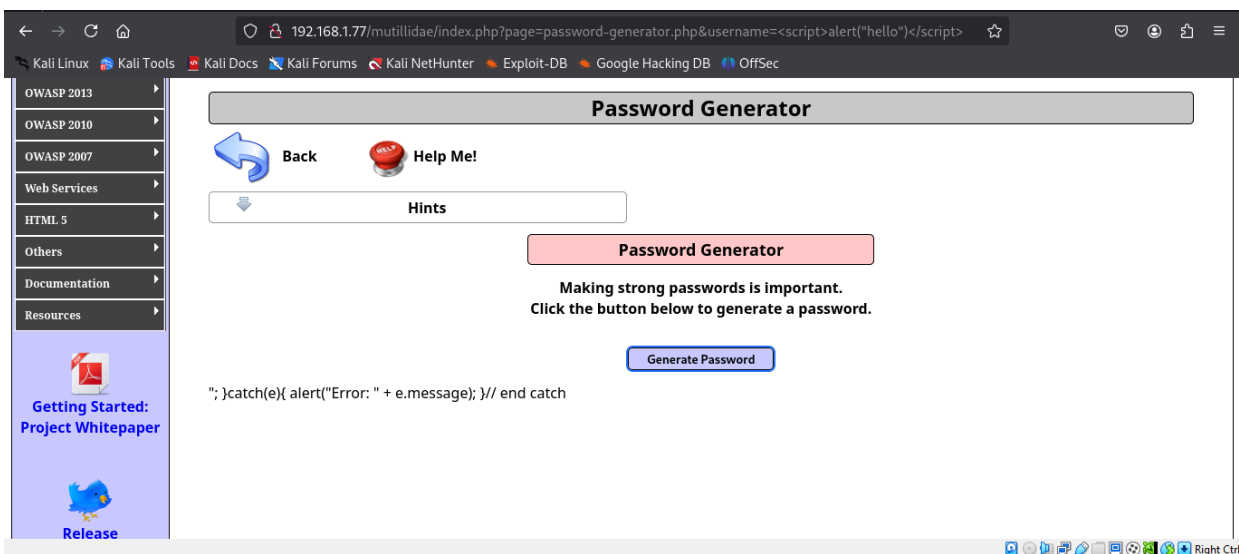
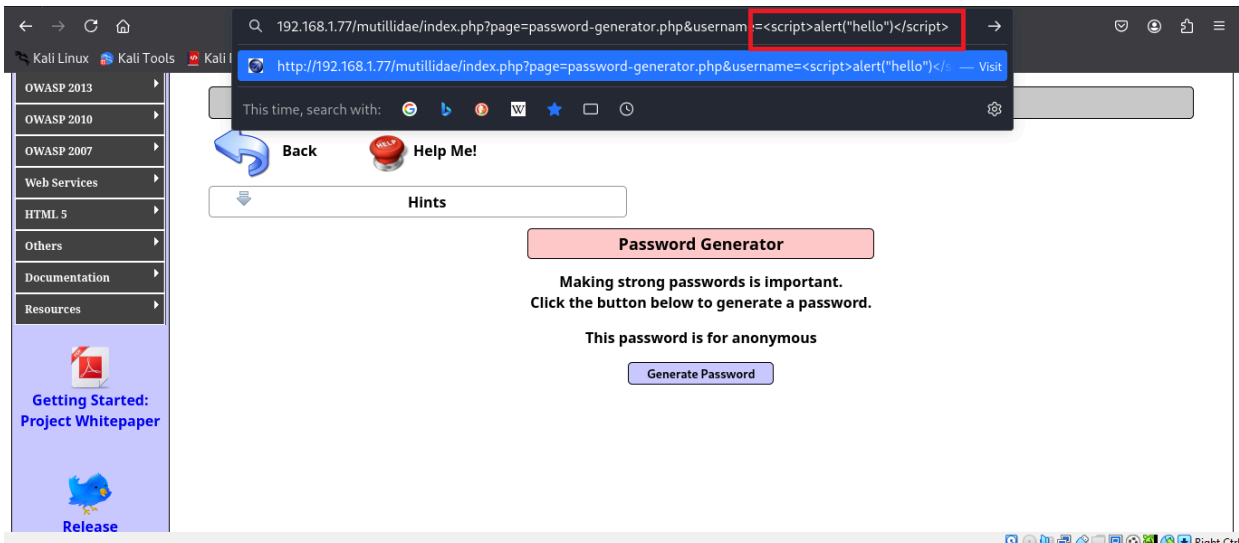
OWASP Mutillidae II is a deliberately vulnerable web application designed to help security professionals and students practice various web vulnerabilities. In this report, we explore Cross-Site Scripting (XSS) vulnerabilities in the Password Generator feature of Mutillidae II.

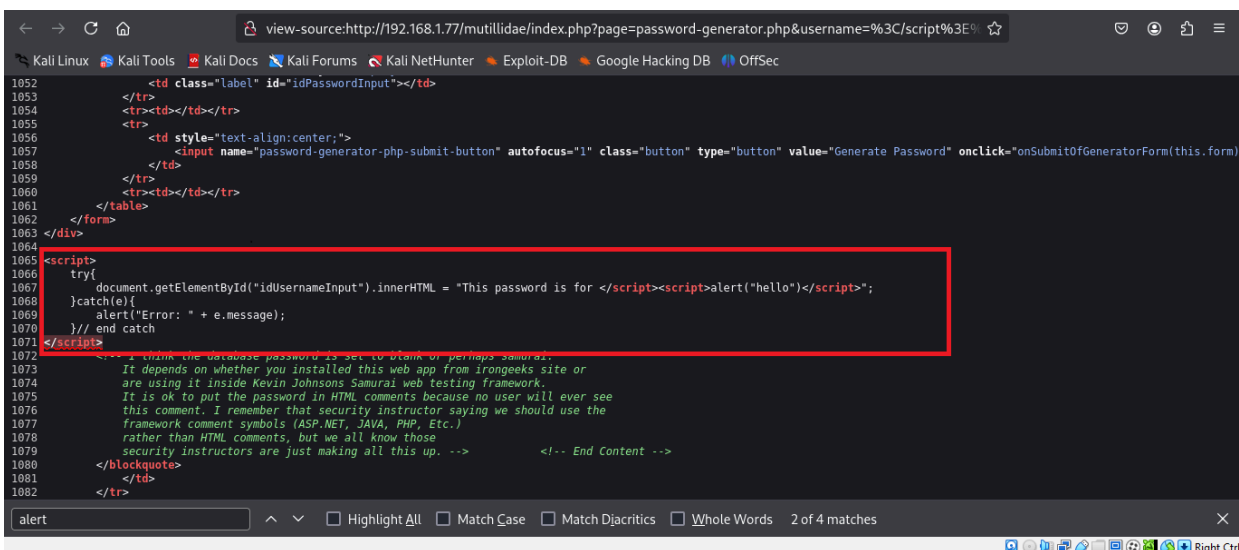
Objective:

To identify and exploit XSS vulnerabilities in the Password Generator module of OWASP Mutillidae II, demonstrating how attackers can inject malicious scripts.

Steps to Identify XSS Vulnerability:







Mitigation Measures:

- Implement proper input validation and sanitization.
- Use output encoding to prevent script execution.
- Enable Content Security Policy (CSP) to restrict script execution.
- Use security libraries such as OWASP's AntiSamy to filter malicious input.

Conclusion:

This practical experiment demonstrated how an XSS vulnerability in the Password Generator feature of OWASP Mutillidae II can be exploited. Proper security measures must be taken to prevent such attacks and ensure application security.

