

**PENETRATION TESTING TOWARDS DAMN VULNERABLE WEB
APPLICATION (DVWA)**

**METHOD ZERO ENTRY HACKING (ZEH) AND
OPEN WEB APPLICATION SECURITY PROJECT (OWASP)**

Leonardo Pandapotan

ABSTRACT

This study aims to test vulnerabilities to determine the security condition of the DVWA web application and describe the gaps found because information security systems are very important with advances in information technology and also to help the needs of the people who use them. The penetration testing (pentest) methodology used in this study is Zero Entry Hacking (ZEH) which has 4 (four) stages, namely Reconnaissance, Scanning, Exploitation, and Post Exploitation and Maintenance Access and takes solutions from the Open Web Application Security Project (OWASP). . The results obtained from the scanning process are in the form of warnings and vulnerabilities as well as knowing the condition of the security level of the DVWA web application system by exploiting cross-site scripting (XSS), command injection, file inclusion, file uploading, brute force attacks, and SQL injection along with solutions from Open the Web Application Security Project (OWASP).

Keyword : The security of information systems, DVWA, *penetration testing (pentest)*, *Zero Entry Hacking (ZEH)*, *Open Web Application Security Project (OWASP)*, *cross-site scripting*, *command injection*, *file inclusion*, *file upload*, *brute force attack*, dan *SQL injection*.

***PENETRATION TESTING TERHADAP DAMN VULNERABLE WEB
APPLICATION (DVWA)***

***MENGGUNAKAN METODE ZERO ENTRY HACKING (ZEH) DAN
OPEN WEB APPLICATION SECURITY PROJECT (OWASP)***

Leonardo Pandapotan

ABSTRAK

Penelitian ini bertujuan untuk pengujian kerentanan untuk mengetahui kondisi keamanan aplikasi web DVWA dan menjabarkan celah yang ditemukan karena keamanan sistem informasi sangat penting dengan diiringi kemajuan teknologi informasi dan juga untuk membantu kebutuhan orang-orang yang menggunakannya. Metodologi *penetration testing (pentest)* yang digunakan dalam penelitian ini adalah *Zero Entry Hacking (ZEH)* yang memiliki 4 (empat) tahapan yaitu *Reconnaissance, Scanning, Exploitation, dan Post Exploitation and Maintaining Access* serta mengambil solusi dari *Open Web Application Security Project (OWASP)*. Hasil yang didapatkan dari proses *scanning* berupa *warning* dan kerentanan serta mengetahui kondisi tingkat keamanan sistem aplikasi web DVWA dengan melakukan exploit *cross-site scripting (XSS), command injection, file inclusion, file upload, brute force attack, dan SQL injection* bersamaan dengan solusi dari *Open Web Application Security Project (OWASP)*.

Kata kunci : Keamanan sistem informasi, DVWA, *penetration testing (pentest), Zero Entry Hacking (ZEH), Open Web Application Security Project (OWASP), cross-site scripting, command injection, file inclusion, file upload, brute force attack, dan SQL injection.*