

In today's Informatic world, many operations such as shopping, communication, research, banking and even citizenship procedures can be carried out through web applications. The widespread usage of web applications and the handling of sensitive data have made such applications the number one target for cyber attackers. The increase in attacks against Web applications has also increased the importance of web application security. The most important factor in ensuring web application security is Web application penetration tests. The most important aid for experts who want to perform effective and successful penetration testing is the web application security labs in which they can do various attack experiments. In this study; we developed a web application security lab called EWASL that contains major web vulnerabilities and allows penetration testing experiments to be conducted on those vulnerabilities. Developed EWASL differs from the laboratories in the literature due to the fact that vulnerabilities are listed both under the headings and hidden within the pages. Another feature that distinguishes EWASL from other laboratories is that it contributes to develop secure software development by means of showing the malicious codes that cause vulnerabilities and the reliable codes that should be written in place of them.