Vulnerable Web Applications:

Websites and web applications that are vulnerable by design and offer a safe hacking space are rich ground for learning. By using them, new hackers can get comfortable with finding the vulnerabilities, security researchers and bug bounty hunters can expand their knowledge and find new vulnerabilities, and professional hackers, developers and pen testers can keep their own skills sharp and current.

bWAPP:

bWAPP stands for Buggy Web Application. It is a free and open source deliberately insecure web application. bWAPP prepares one to conduct successful penetration testing and ethical hacking projects. The bWAPP application is an intentionally vulnerable web application. It was developed for educational purposes. The bWAPP application has a number of vulnerabilities, some of them easier to exploit than others.

Deliberately insecure web application, includes all major known web vulnerabilities. It helps security engineers, developers and students to discover and to prevent issues. Prepares one for successful penetration testing and ethical hacking projects. bWAPP helps to improve your security testing skills. it has over 100 web vulnerabilities. Covering all major known web bugs. Including all risks from the Top 10 project

Open source PHP application

Backend MYSQL database

Linux/windows apache/IIS

WAMP or XAMPP

DVWA:

Damn Vulnerable Web Application, often known as DVWA, is developed in PHP and MySQL. It is intentionally left vulnerable so security professionals and ethical hackers can test their skills without legally compromising anyone's system. To run, DVWA requires the installation of a web server, PHP, and MySQL. The main advantage of DVWA is that we can set the security levels to practice testing on each vulnerability. Each level of security needs a unique set of talent. The Damn Vulnerable Web Application is a good place for a beginner to start.

OWASP Broken Web Application:

A collection of purposefully vulnerable applications to safely practice penetration testing. A selection of tools for testing web applications. It makes easy for application developers, penetration testers, and security engineer, management to flex their offensive muscle in the safety of a virtual machine on their own laptop. The OWASP Broken Web Applications Project comes bundled in a Virtual Machine (VM) that contains a large collection of deliberately broken web applications.

Metasploitable 2:

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques. The default login and password is msfadmin/msfadmin. Metasploitable machine enables users to set up a penetration testing environment to learn and practice hacking.