DVWA(Damn Vulnerable Web Application)

The Damn Vulnerable Web Application (DVWA) is a deliberately vulnerable web application that is widely recommended for practicing web application security testing.

DVWA is an open-source application that can be installed on a local machine or a virtual machine, making it easily accessible for educational purposes.

The Damn Vulnerable Web Application (DVWA) is a highly recommended tool for practicing web application security testing due to its didactic value, comprehensive coverage of vulnerabilities, and practical approach to learning.

Some of the vulnerabilities that can be found in DVWA include SQL injection, cross-site scripting (XSS), command injection, remote file inclusion, and more.

By using DVWA, individuals can gain hands-on experience in identifying and exploiting vulnerabilities commonly found in web applications, thereby enhancing their skills in web application security testing.

Each vulnerability is carefully crafted to simulate real-world scenarios, ensuring that users are exposed to a diverse set of security issues commonly encountered in web applications.

This practical experience is invaluable in developing the skills necessary to identify and mitigate vulnerabilities in real web applications.

By exploiting these vulnerabilities, users can gain practical experience in understanding the underlying issues and potential risks associated with them.

For example, they can use manual testing techniques to identify vulnerabilities, such as inspecting the source code, analyzing network traffic, and manipulating input fields.

SOURCE

- https://eitca.org/cybersecurity/eitc-is-wapt-web-applications-penetration-testing/spidering/spidering-and-dvwa/examination-review-spidering-and-dvwa/what-is-the-damn-vulnerable-web-application-dvwa-and-why-is-it-recommended-for-practicing-web-application-security-testing/