D2NA™

A spotlight on Web Application Penetration Testing

Version 1.0
November 2023
Written by Shaun Conway

Web application penetration testing, also known as web app penetration testing or web penetration testing, is a testing approach that aims to evaluate the security of a web application. Its main objective is to detect and fix vulnerabilities and weaknesses that could be exploited by malicious individuals.

Let's take a look at the different stages of a Web Application Penetration Test:

Scope Definition

- Clearly defining the scope of the penetration test, including the specific web applications, URLs, and functionalities that will be tested.
- Determining the rules of engagement, such as the testing methods to be used and any limitations on testing.

Information Gathering

- Collecting information about the target web application, including its architecture, technologies used, and potential entry points for attacks.
- Discussing with the client about their concerns and a history of the application.

Vulnerability Analysis

- Identifying and analysing vulnerabilities that could be exploited by attackers. These common vulnerabilities include SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), security misconfigurations, and more.

Testing

- Conducting manual testing to discover vulnerabilities that automated tools may not detect. This involves simulating real-world attack scenarios to identify unique or complex issues.
- Utilising automated tools to scan the web application for common vulnerabilities. These tools can help identify low-hanging fruit and save time compared to manual testing.

- Evaluating the strength of authentication mechanisms and identifying any weaknesses that could lead to unauthorised access.
- Assessing the effectiveness of the authorisation controls to ensure that users can only access the resources and functionalities they are authorised to use.

Session Management and Data Validation

- Testing the security of session management to prevent attacks like session hijacking and session fixation.
- Checking how the application validates and sanitizes user input to prevent vulnerabilities such as injection attacks.

Reporting

- Documenting and reporting the findings, including a detailed description of each vulnerability, its potential impact, and recommendations for remediation.

Remediation

- We can work with the development team to address and fix the identified vulnerabilities. This may mean the development team needs to implement code changes, configuration updates, or other security measures.

Re-Testing

- After remediation has been completed, conduct re-testing to ensure that the identified vulnerabilities have been successfully addressed and that new issues have not been introduced.

Web application penetration testing is a crucial part of the overall security posture of an organisation, helping to identify and fix potential security risks before they can be exploited by attackers. It's important to conduct regular penetration testing, especially when significant changes are made to the web application or its environment.

Contact us today on 0330 159 5969, via our website www.d2na.com or via email, sales@d2na.com.