# WEB APPLICATION PENETRATION TESTING TRAINING

The Web Application Penetration Testing training is a three-day entry-level course facilitated by a qualified and experienced instructor that is designed to teach students how to practically discover and exploit the security of web applications. Students are taught the real world tools and techniques that are used by modern hackers enabling them to discover and remediate the vulnerabilities in their own web applications.

The majority of the course consists of practical hands-on exercises in which the students are able to practice exploiting a wide range of web application vulnerabilities in a completely safe and isolated test environment. This test environment is purpose built to be vulnerable to a wide variety of security issues and students are given the opportunity to truly experiment with what is possible in order to cement their understanding.

The course begins with an introduction to the security industry and discussing the data breaches and technology trends that have shaped the information society that we live in. We explore the importance of data and how attackers are shifting tactics to compromise organisations for data theft. Students are taught about the motivations for attacks and that attacks are not always for financial gain, but can be motivated by ideologies that drive the disruption of a service or the sharing of a message, or for intellectual property theft that provides a competitive advantage. The training includes discussion regarding how different types of attacks are used based on these motivations and the nature of the attacker.

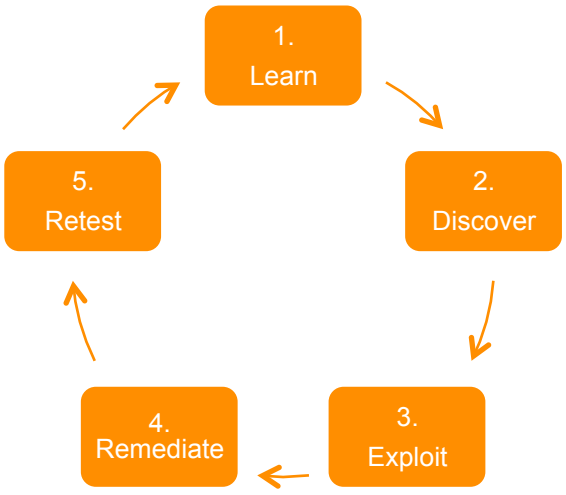


*Figure 1: Web application penetration testing course flow*

## REAL WORLD APPLICATION

Students will learn the background to common vulnerabilities and the instructor will share some war stories of how each vulnerability is actually exploited in the real world. The students are then guided through the discovery phase where, once a vulnerability has been discovered the students will exploit it with the same toolset that a real attacker may use. Time is provided for the students to experiment using the same techniques and tools used by attackers on a range of vulnerable training applications. The students will have the opportunity to discuss how the vulnerability could be prevented or remediated and typically share some personal insight into how their organisation has addressed the issue. The fix is then implemented and the students are able to retest and experience the effects of the fix.

At the end of the course a "capture the flag competition" is hosted where the students must use all of the techniques that they have learned to compromise a new web application. Upon completion of the course, students are presented with a certificate of completion.

## BENEFITS OF THE COURSE

Students will gain:

- An understanding of how web application security can be broken and bypassed.
- An understanding of how to fix the issues that cause modern web application vulnerabilities.
- An understanding of secure development practices.
- Windows and Linux security experience.
- Hands-on experience with a variety of security tools used by real hackers.

## COURSE OUTLINE (3 DAYS)

- State of the industry
- A brief history of web applications
- Authentication and authorisation
- Client side attacks
- Injection attacks
- Infrastructure level attacks
- Data security and encryption
- Practical security in the Systems Development Lifecycle (SDLC)
- Capture the flag competition