

# Web Application Security

As more and more trust is placed in organisations and their IT infrastructure, it is increasingly important that personal data is protected. Starting with the 2018 update to the OWASP top 10, this course will teach you how to find and exploit common security vulnerabilities that can be used to attack both web servers and web users.

By taking a general approach to security, we will learn not only how specific vulnerabilities work (such as SQL Injection and Authentication Bypasses), but we will understand the wider classes of bugs. This will allow us to keep breaking and exploiting software even as the technology changes.

This course is for anyone that is interested in web application security – from would be penetration tester to software developers looking to understand how real attacks occur.

Note: This course **does** teach real hacking techniques that may be illegal if carried out on systems you do not have permission to test. Please only use these tools and techniques on your own systems and those provided in the course.

## Introduction to penetration testing



What is pen testing?  
Understanding HTTP  
OWASP Top 10 overview



## Bypassing Authentication

Brute Force Attacks  
Session Vulnerabilities  
Bypassing Client Controls  
Modifying Request Parameters

# Injection Attacks



SQL Injection  
Advanced SQL Injection  
OS Command Injection



## Attacking the Server

Attacking the server  
Abusing out of date components  
Abusing File Uploads  
Directory Traversal  
Cracking Passwords

# Client Attacks



Cross Site Scripting (XSS)  
Cross Site Request Forgery (CSRF)  
Click Jacking



## Web Applications

Java Application Vulnerabilities  
.NET Application Vulnerabilities  
Server Hardening  
Attacking Logic  
Cracking Passwords

0161-820-3056

[www.digitalinterruption.com](http://www.digitalinterruption.com)

[contact@digitalinterruption.com](mailto:contact@digitalinterruption.com)

