# Web Hacking 2 Days

2021 EDITION

**This is an entry-level web application security testing course and also a recommended pre-requisite course before enrolling for our "Advanced Web Hacking" course. This foundation course of "Web Hacking" familiarises the attendees with the basics of web application and web application security concerns. A number of tools and techniques, backed up by a systematic approach on the various phases of hacking will be discussed during this 2-day course. If you would like to step into a career of Ethical Hacking / Pen Testing with the right amount of knowledge, this is the right course for you.**

This course familiarises the attendees with a wealth of tools and techniques required to breach and compromise the security of web applications. The course starts by discussing the very basics of web application concepts, and gradually builds up to a level where attendees can not only use the tools and techniques to hack various components involved in a web application, but also walk away with a solid understanding of the concepts on which these tools are based. The course will also talk about industry standards such as OWASP Top 10 and PCI DSS which form a critical part of web application security. Numerous real life examples will be discussed during the course to help the attendees understand the true impact of these vulnerabilities.

## Who Should Attend

- **Security enthusiasts**
- **Anybody who wishes to make a career in this domain and gain some knowledge of networks and applications**
- **Web Developers**
- **System Administrators**
- **SOC Analysts**
- **Network Engineers**
- **Pen Testers who are wanting to level up their skills**

## Prerequisites

Delegates should bring their laptop with windows operating system installed (either natively or running in a VM). Further, Delegates must have administrative access to perform tasks such as installing software, disabling antivirus etc. Devices that don't have an Ethernet connection (e.g. MacBook Air, tablets etc.) will not be supported during the course.

## Course Outline

### UNDERSTANDING THE HTTP PROTOCOL
- HTTP Protocol Basics
- Introduction to proxy tools

### INFORMATION GATHERING
- Enumeration Techniques
- Understanding Web Attack surface

### ISSUES WITH SSL/TLS
- SSL/TLS misconfiguration

### USERNAME ENUMERATION & FAULTY PASSWORD RESET
- Attacking Authentication and Faulty Password mechanisms

### AUTHORIZATION BYPASS
- Logical Bypass techniques
- Session related issues

### CROSS SITE SCRIPTING (XSS)
- Various types of XSS
- Session Hijacking & other attacks

### CROSS SITE REQUEST FORGERY (CSRF)
- Understanding CSRF attack
- Various impacts of SSRF attack

### SQL INJECTION
- SQL Injection types
- Manual Exploitation

### XML EXTERNAL ENTITY (XXE) ATTACKS
- XXE Basics
- XXE exploitation

### DESERIALIZATION VULNERABILITIES
- Serialization Basics
- PHP Deserialization Attack

### INSECURE FILE UPLOADS
- Attacking File upload functionality

### COMPONENTS WITH KNOWN VULNERABILITIES
- Understanding risks known vulnerabilities
- Known vulnerabilities leading to critical exploits

### INSUFFICIENT LOGGING AND MONITORING
- Understanding importance of logging and monitoring
- Common pitfalls in logging and monitoring

### MISCELLANEOUS
- Understanding formula Injection attack
- Understanding Open Redirection attack

NotSoSecure part of claranet cyber security®

### For more information:

**UK:** +44 (0)1223 653 193
**US:** +1 (628)200-3053/3052
**Email:** contact@notsosecure.com
**Visit:** notsosecure.com