secarma®
CYBERSECURITY EXPERTS

SECURITY TRAINING OVERVIEW

Hacking & Defending Web Apps

The Secarma training team regularly run hands-on security training courses across the UK and remotely. With labs to allow you to get practical experience breaking security systems before teaching you how to build systems in a more resilient way.

WHO IS IT FOR?

Our web application hacking course is designed to teach web application developers the tools and techniques we use when targeting web applications during real world penetration tests.

It's also a useful course for those looking to break into Penetration Testing who want a first step on the journey.

HOW CAN WE HELP?

Software developers often focus on building an application and making it functional. They're often tied to strict deadlines and therefore, ensuring everything is secure is sometimes not the first priority.

Additionally, many security flaws can be subtle or difficult to spot if you're not well versed in common vulnerability types and testing methods.

By using the "hackers" point-of-view throughout the training course we allow those interested in developing a security testing capability to get started on that journey.

HANDS ON - Labs

Our training course includes the following hands-on labs to ensure you gain practical understanding as well as getting to grips with our testing methodology:

- **Injection**
  Leveraging injection vulnerabilities to extract confidential data, in order to compromise databases and web servers directly.
- **Cross-site Scripting**
  Leveraging XSS attacks to perform virtual defacement, extract confidential information, and perform privilege escalation.
- **Abusing File**
  Upload Bypassing file restrictions to upload malicious files to gain command execution on vulnerable web servers and to pivot into DMZ and internal networks.
- **Broken Authentication**
  We cover a range of authentication and access control issues, from simple bruteforce attacks, to bypassing multi-factor authentication, and missing functional level access controls.

FEATURES

- Guidance on the Penetration Testing methodology.
- Covers the OWASP Top 10 and other key security issues.
- Detail remediation guidance for every vulnerability type covered.
- Multiple challenges for each lab, for beginner to intermediate skill levels.

secarma®
CYBERSECURITY EXPERTS

SECURITY TRAINING OVERVIEW

Hacking & Defending Web Apps

This course steps you through the common phases of a Web Application Penetration Test and allows you to gain an understanding of how hackers hack.

COURSE OVERVIEW

Our training teaches candidates about web application security vulnerabilities by stepping them through the process of a Penetration Test.

We'll map an application and approach the work like a real work threat actor before hunting for vulnerabilities. Once vulnerabilities are discovered we walk through exploitation to demonstrate the real-world risk of issues.

At the end of each section we'll review the discovered vulnerability and offer guidance on remediation.

At the end of the day we'll review all of the findings and give guidance on how systems and applications could be hardened to make exploitation action more difficult and attack detection easier.

Mapping and Intelligence Gathering

Before the engagement begins, we will map the attack surface to discover alive hosts, services, and versions. As well as mapping application functionality.

Vulnerability Discovery

We'll demonstrate methods of finding and confirming vulnerabilities to minimise false positives being highlighted.

Proof of Concept and Confirmation

Where vulnerabilities are discovered a proof of concept exploit will be created to demonstrate the potential business risk. This ensures that false positives are removed by manually confirming and demonstrating all discovered vulnerabilities.

Exploitation

Exploitation involves discovering weaknesses within exposed applications and leveraging those weaknesses to demonstrate as much business risk as possible.

OTHER COURSES

HACKING & DEFENDING WEB APPS

From injection vulnerabilities to abusing file handling functions, we look at how to hack web applications and how to make them more secure.

HACKING & DEFENDING NETWORKS

We run your team through breaking into internal corporate networks and teach them about attack mitigations and defence in depth.

SECURITY AWARENESS

We teach your staff how we compromise organisations and how they can stay safer online, at work and at home.

BESPOKE TRAINING

Looking for something specific? Need something not covered on this page? Talk to us about our bespoke training course development.

WHY SECARMA?

Secarma are a cybersecurity consultancy that specialises in security testing. We're not a training company trying to talk about security testing; we're penetration testers teaching your team what we do every single day.

We aim to combine instructor-led training with hands-on labs, to help your team build stronger software and to help you reduce your organisational risk.

☎ 0161 513 0960 secarma.com enquiries@secarma.com