

COURSE PROFILE:

# AppSec for Developers



2 Day **Specialist** training

## Your course

The future of secure software is in your hands. Join this extremely informative 2-day course to bring your application security skills up to the industry standard and widen your career prospects. Get significant hands-on experience with our popular virtual labs and learn from industry experts, practicing penetration testers with a legacy of training at Black Hat. You'll learn how to find and fix vulnerabilities in code, enhance the security culture within your dev team, apply DevSecOps thinking day to day, and more...

## Who it's for

- **Software developers (beginner to advanced)**
- **Development team leads**

This course is suitable for software developers and development teams who want to build and maintain secure software. The syllabus considers different application development strategies, from preserving legacy applications to developing new products.

## Top 3 takeaways

- **Practical application security skills and knowledge to use daily**
- **Techniques and tools to help you code securely by second nature**
- **DevSecOps awareness to help you transform your dev practices from the ground up**

## What you'll learn

This course uses a Defense by Offense methodology based on real world offensive research (not theory). That means everything we teach has been tried and tested on live environments and in our labs, so you can put it into practice as soon as the training is over. By the end of the course, you'll know:

- **Everything you need to know about application security vulnerabilities, including why they occur, how they impact your applications, and what risk they pose to the wider organization**
- **The principles of application security and Secure by Design thinking**
- **How to develop secure applications, from writing secure code to building and governing secure processes**
- **How to find and fix vulnerabilities in existing application code**
- **How to build and maintain a culture of security across the team using secure practices and tools**

## What you'll be doing

You'll be learning hands on:

- **Hacking insecure code to see what vulnerabilities look like in your applications**
- **Fixing these vulnerabilities so you can secure your own applications**
- **Discussing the functionality requirements of secure application development so you can design security into everything**
- **Applying real world case studies to your development thinking**
- **Competing in a timed, fast-paced Capture the Flag (CTF) game to test your new skills**

## Why it's relevant

Have you ever developed an application without testing the code for vulnerabilities or shipped software with known security flaws? Software has become a frontline target for cybercriminals who want to disable, disrupt, and destroy systems and harm individuals. And some of the most newsworthy hacks in recent years – including credit reporting agency Equifax, telecommunications giants T-Mobile and Optus, and even the Shanghai Police – have been the result of vulnerabilities in application code. From customer data being stolen, to entire organizations going offline, secure code matters.

There are other reasons to develop your ability too. As security becomes more embedded in the way we work, employers are increasingly looking for development specialists who can demonstrate technical application security skills all the way up to CTO level. Secure coding proficiency directly correlates with your growth and career progression and can lead you into new areas.

This course is packed full of exercises and topics relevant to the current threat landscape and the latest industry-standard development systems and processes. Our syllabuses are also revised regularly to reflect the latest in-the-wild hacks and whatever proof of concepts we've been developing through our own research. Because they remain so up to date with the threat landscape and security industry standard, **many delegates return every 1-2 years** to update their skills and get a refresh.

## What's in the syllabus

Note: our syllabuses are subject to change based on new vulnerabilities found and exploits released.

### APPLICATION SECURITY BASICS

- Why do you need application security?
- Understanding the OWASP Top 10

### UNDERSTANDING THE HTTP PROTOCOL

- What is the HTTP/HTTPS protocol?
- Understanding requests and responses – attack surface
- Configure Burp Suite to intercept HTTP/HTTPS traffic

### SECURITY MISCONFIGURATIONS

- Common misconfigurations in web applications
- Sensitive information exposure and how to avoid it
- Using software with known vulnerabilities

### INSUFFICIENT LOGGING AND MONITORING

- Types of logging
- Introduction to Filebeat with the Elastic Stack (Elasticsearch, Logstash, and Kibana) (F-ELK)

### AUTHENTICATION FLAWS

- Understanding anti-automation techniques
- NoSQL security

### AUTHORISATION BYPASS TECHNIQUES

- Securing JWT and OAuth
- Local file inclusion
- Mass assignment vulnerabilities

### CROSS-SITE SCRIPTING (XSS)

- Types of XSS
- Mitigating XSS

### SERVER-SIDE REQUEST FORGERY (SSRF)

- Understanding SSRF
- Mitigating SSRF

### SQL INJECTION

- Error and blind SQL injections
- Mitigating SQL injection
- ORM framework: HQL injection

## **XAML EXTERNAL ENTITY (XXE) ATTACKS**

- Default XML processors: XXE
- Mitigating XXEel

## **UNRESTRICTED FILE UPLOADS**

- Common pitfalls of file upload
- Mitigating file upload vulnerabilities

## **DESERIALIZATION VULNERABILITIES**

- What is serialization?
- Identifying deserialization functions and deserialized data
- Mitigation strategies for deserialization

## **CLIENT-SIDE SECURITY CONCERNS**

- Understanding same-origin policy
- Client-side security headers and their server configurations

## **SOURCE CODE REVIEW**

- How to validate source code security
- Walkthrough: How threat actors chain vulnerabilities to achieve greater impact
- Capture the Flag: a timed competition challenging you to spot flaws in different samples of source code

## **DEVSECOPS**

- DevSecOps: what is it, how do you build it, and what tools can you use?

## What you'll get

- **Certificate of completion**
- **24 hours' lab access after the course (with the opportunity to extend)**
- **8 Continuing Professional Education (CPE) credits awarded per day of training fulfilled**
- **Learning pack: question & answer sheets, setup documents, and command cheat sheets**

## Course highlights

What delegates love:

- **Offensive angle: you'll learn from practicing penetration testers and red teamers with up to date, working knowledge of the latest and most common software hacks**
- **Multiple mitigations: for every vulnerability covered, you'll explore 3 to 4 remediations, helping you develop a versatile, relevant approach**
- **Focus on awareness and process as well as code: you'll learn the principles behind the practical approach**
- **Browser based: the course is fast to set up, requiring a single installation of Burp Suite**
- **Individual access: you'll have your own infrastructure to play with, enabling you to try out secure coding and mitigation techniques independently, at your own pace**
- **Real-world learning: in an industry where most of the leading cybersecurity training courses are based on theory, our scenario-led, research-based approach ensures you learn how real threat actors think and act.**

## Outcomes for budget holders

This course is designed to help organizations upskill their development team in response to evolving cyber risk, helping senior decision makers:

- **Manage the likelihood and impact of security incidents originating from insecure code and development practices**
- **Lower the cost of retrofitting security into existing applications and workflows and totally eradicate this need going forward**
- **Lower costs by managing code reviews and remediation internally**
- **Develop the organization's competitive advantage for security-conscious customers**
- **Nurture and retain highly skilled, security conscious employees**
- **Demonstrate commitment to security through training and change management**



WHY NOTSOSECURE?

# We hack. We teach.


**NotSoSecure is Claranet's dedicated training division and part of its global penetration testing practice. We're one of the largest training partners at Black Hat and a respected provider of web, mobile, and network penetration testing.**

All our trainers are experienced, practicing, accredited penetration testers with their own field of excellence. This translates into our course syllabuses, where each module is designed around real-world engagements and in-the-wild research. No other provider of cybersecurity training is modelled in this way. The delegates we train leave our courses armed with knowledge and skills based on current and authentic attacker tactics and tradecraft, not theory alone.

It's our mission to help organizations raise the bar when it comes to their cybersecurity, and to inspire and empower the next generation of IT and security professionals to remain relevant in the way they think and hack. We achieve this by delivering practical content, giving delegates the hands-on experience needed to understand the context behind each offensive and defensive technique. They go on to use this with confidence in their own work, be that within an organisation or their personal research.



**WE HACK.  
WE TEACH.**

 claranet cyber security®

