Mobile App Security Training

Mobile App Security

- Why is app security so important?
- What are the risks to *your* app users?

SDL in depth

- Analysing security and privacy risk
- Attack surface analysis
- Threat Modeling
- Identifying the right tools
- Enforcing banned functions
- Static analysis
- Dynamic / Fuzz Testing
- Response Plan
- Final Security Review

Hands-on with the OWASP Mobile Top 10 Security Risks

Keeping up to date with the latest OWASP To 10 vulnerabilities:

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

Beyond OWASP

- Authorisation and Authentication options
- Mobile Data and asset encryption

- Enforcing user-level app security policies
- Minimising network exposure
- Secure auditing and logging solutions
- OS checks (rooted / jailbroken devices)

Summary

- Applying what you've learnt in the real world.
- Understanding the business impact of insecure software.