Exploring Security

What is Exploring Security?

Information security affects everyone in the world. Whether it's our user credentials, personal data, financial data, intellectual property, or our devices and other hardware; it all needs to be kept safe and secure. Software development organisations have a unique place in the creation of products. We design, develop, test and deploy, often very rapidly and frequently. But this is often at the cost of security.

Each day we hear about new security breaches, hacks and data thefts across the world. So, what are we doing wrong? If we seek to understand the key security issues that affect organisations today we can be more prepared. If we examine the behaviour, intentions and skills of those who seek to do applications and organisations harm, we develop our skills and approaches to meet the challenge that malicious hackers offer.

Exploring Security is a new course designed and taught by Daniel Billing. Its aim is to help attendees to become more aware of the application and infrastructure security issues that affect your organisation, products, and customers.

Why should you attend this course?

All organisations that build and support software products ought to have a security strategy. This should include all aspects of production from business analysis, design, development through to testing and support. If you seek to add value to your teams from a security perspective, then this course will help you to start doing that.

Course Outline

Day 1

To develop an effective security strategy for your organisation, it is important to be able to understand the core principles of application security so that we can develop models of the applications we are building, identifying potential risks and vulnerabilities.

By the end of day one you will be able to:

- Understand what security means for us, in our lives and work as well as the potential risks through a lack of security.
- Understand the first principles of application security - confidentiality, integrity and availability.
- Build threat models are the basis of a security strategy; such as STRIDE.
- Identify approaches to mitigating the identified risks, allowing us to build a test strategy.

Day 2

In order to identify the actual risks and vulnerabilities in a system, we have to utilize the skills and techniques of security professionals and malicious hackers alike.

By the end of day two you will be able to:

- Model the behaviours of humans using software, understand their motivations and needs, through exploring the techniques of social engineering.
- Examine, develop and explore a range of personas as models for testing the security of an application.
- Develop reconnaissance skills which is one of the key tools of both hackers and security professionals.
- identify vulnerabilities in the system under test.
- Be able to update our models and approaches to identify more vulnerabilities.
- Become practiced with a range of security testing tools, such as scanners, fuzzers and proxies.

Day 3

Hackers and security professionals work in teams. We need to be able to do the same.

By the end of day three you will be able to:

- Work together to identify as many vulnerabilities as possible.
- Communicate the value of your security testing strategies and approaches
- Identify the needs, interests and desired outcomes of your stakeholders with regard to security
- Clearly communicate the security issues you identify.
- Begin to build and apply a strategy in your context.

Workshop Format

Whilst we are covering a lot of security theory, this will be a practical course. We will be using a range of technical tools, environments and techniques. Please be prepared for a technical and human challenge throughout, with a lot of real world and simulated examples of security issues.

You will need

Please bring a laptop, OS X, Linux or Windows with all the prerequisites installed that will be sent to you.

Biography

Daniel Billing is an experienced software tester, consultant and trainer. He has a deep passion for testing, and especially security. He is an active member of the software testing community, participating in a number of conferences and other events, as an attendee, speaker, trainee and volunteer.

With 18 years experience, Daniel has worked with a wide range of organisations, including start ups, financial institutions, health and scientific, public and the defence sector. He currently runs the consultancy The Test Doctor, which aims to develop test strategies and skills of his clients, particularly in the sphere of security.