OWASP TOP TEN SECURE DEVELOPMENT WORKSHOP

OVERVIEW

ABOUT THE OWASP TOP TEN

The OWASP Top Ten 2017 is a great place to start when learning about application security. OWASP is the Open Web Application Security Project and is a non-profit organisation that aims to educate individuals and businesses about web application security. They organise events, sponsor projects and run local chapter meetings to promote awareness of both offensive and defensive application security techniques.

Every three years (roughly) they publish something called the OWASP Top Ten which is a list of the ten most common web application security flaws seen in the real world and defence against these issues is intended as a good first step to secure software.

OUR TRAINING

Our OWASP Top Ten for Developers training is an **intensive half-day workshop** that aims to provide developers with an understanding of these weaknesses, how they manifest themselves, how hackers find them and what the impact can be and then, most importantly, we explain how to code defensively to prevent these weaknesses. We explain *what works* and *what doesn't* and some common issues we encounter during our penetrating testing engagements.

WORKSHOP OUTLINE

The workshop runs for half a day though it can be extended by incorporating more practical examples if desired. The course is delivered on site at your office though if you prefer an external training facility can be booked or you can come to our office in Northamptonshire. We can accommodate up to around ten attendees.

Our workshop walks attendees through the OWASP Top Ten 2017. Each issue is introduced, practical examples are given using our application security labs to show the potential impact, then defensive approaches are discussed.

Developers are not required to perform any hands-on activities themselves in this workshop and therefore do not need to bring anything other than an open mind and maybe a pen and paper.

The workshop covers the following issues:

- A1 – Injection
- A2 – Broken Authentication
- A3 – Sensitive Data Exposure
- A4 – XML External Entities (XXE)
- A5 – Broken Access Control
- A6 – Security Misconfiguration
- A7 – Cross-Site Scripting (XSS)
- A8 – Insecure Deserialization
- A9 – Using Components with Known Vulnerabilities
- A10 – Insufficient Logging & Monitoring

REQUIREMENTS

There are only three requirements we have for delivering the workshop at your office:

- Projector with VGA or HDMI connector
- Power
- Internet access for our trainer

4ARMED