PCI DSS Secure Coding Workshop

Overview

PCI DSS Requirement 6.5

The Payment Card Industry Data Security Standard (PCI DSS) requires that organisations developing applications that handle card data secure their software against common vulnerabilities. As part of this, PCI DSS compliant organisations need to train their software developers in secure coding techniques.

Our Training

This is where we come in. 4ARMED's consultants have been helping organisations implement PCI DSS since 2006, we've also been writing code and hacking web applications all that time too so we put all that together into an **intensive half-day workshop** that we can deliver on site at your office, our office or another location of your choosing.

Our PCI DSS Secure Coding training aims to provide developers with an understanding of the issues highlighted in PCI DSS requirement 6.5, 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, typically 3 to 4 hours, though it can be extended by incorporating more practical examples if desired. The course can be delivered online via Google Meet or Zoom, on site at your preferred location internationally or in a hybrid manner with some delegates attending online and some in-person.

Our workshop walks attendees through the issues defined in PCI DSS v3.1 requirement 6.5. Each issue is introduced, practical examples are given using 4ARMED's custom built application security lab environment 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:

- 6.5.1 – Injection flaws
- 6.5.2 – Buffer overflows
- 6.5.3 – Insecure cryptographic storage
- 6.5.4 – Insecure communications
- 6.5.5 – Improper error handling
- 6.5.7 – Cross-site scripting (XSS)
- 6.5.8 – Improper access control
- 6.5.9 – Cross-Site Request Forgery
- 6.5.10 – Broken authentication and session management

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