Secure Coding

Black Box Testing Tutorial
17th October 2014

Tutorial Plan

1. Quick recap on testing:
   - Black-box, Gray-box, White-box
   - Methodology: Recon, Mapping, Discovery, Exploitation
2. Explore Samurai WTF:
   - Checkout some tools to be used in project phase 2:
     - Zenmap, Nikto
     - Zed Attack Proxy (ZAP), Burp, w3af
     - Firebug, Web Developer Toolbar
     - DirBuster, etc.
3. Follow Web-Goat lessons on (credentials: guest-guest):
   - Access Control Flaws
   - Authentication Flaws
   - Cross-Site Scripting (XSS)
   - Injection Flaws
   - Session Management Flaws
4. If you are done, follow the lessons on DVWA and Samurai-dojo (installed on VM)

Resources

1. Samurai WTF Course v18 – Slides
   http://sourceforge.net/projects/samurai/files/SamuraiWTF%20Course/SamuraiWTF%20Course%20v18%20-%20Slides.pdf/download
2. OWASP ZAP Tutorial Videos
   https://www.youtube.com/playlist?list=PLEBitBW-Hlsv8cEIUntAO8st2UGhmrjUB
3. Burp Video Tutorials
   http://portswigger.net/burp/tutorials/
4. w3af User Guide
   http://w3af.sourceforge.net/documentation/user/w3afUsersGuide.pdf