Pentesting Plan

The SQA team will choose either White Box Pentesting, Black Box Pentesting, or Grey Box Pentesting for a certain web application to be tested, and will decide what pentesting tool will the SQA team use. If the tool for pentesting is decided, then the SQA team can either train the team's internal test resources or hire expert consultants to do the penetration task for the team. To make pentesting possible, the SQA team and the developer/s of a certain web application to be tested by the SQA team must agree to the terms and conditions in the pentesting contract regarding the security tests to be performed by the SQA team. The SQA team will find the security holes in the web application to be tested. These are the plans of the SQA team:

- Check the login form.
- Make sure the admin panel will not be public. Only certain people like system admins, business owners, and network engineers can only access it.
- Check the ports for vulnerability.
- Check the source codes for vulnerability.
- Run a simulation within the work place in order to check human vulnerabilities.
- If the vulnerabilities are found:
    1. Use the vulnerable part/s to see what to fix.
    2. Since the SQA team is not the developer of the web application to be tested, notify the appropriate IT personnels.

Pentesting It is an attack on a computer system that looks for security weakness, potentially gaining access to the computer's features and data.
Pentesting Tool It is a tool used for testing the security of a web application.
White Box Pentesting It is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality.
Black Box Pentesting One of the most common approaches in assessing the security level of an application is to simulate an attacker's perspective with no prior knowledge of the system.
Grey Box Pentesting It is in between black box and white box pentesting.

Pentesting, https://en.wikipedia.org/wiki/Penetration$_{t}estPentestingTool, https://www.techoped$

White Box Pentesting, https://en.wikipedia.org/wiki/White-box$_{t}estingBlackBoxPentesting, http$

Grey Box Pentesting, https://blog.secureideas.com/2012/12/grey-box-penetration-testing.html

Penetration Testing Execution Standard, http://www.pentest-standard.org/index.php/Main$_{P}age$

0.1 Penetration Testing Execution Standard

The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

The following are the main sections defined by the standard as the basis for penetration testing execution:

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting