Pen Testing Methods, Prep and Reporting Cheat Sheet

by binca via cheatography.com/44948/cs/13446/

Black Box

Little or no information provided to tester other than the name of the target, an IP range or applicable URLs.

The target is a "black box".

This type of testing requires close coordination between testers and target system personnel to ensure that the testing stays within scope.

This type of testing is not typically done in web application testing.

White Box Penetration Testing

Testers are provided with information in advance including target URLs, application functionality summary, application map and test accounts.

Target system personnel are available to answer questions.

This type of testing is an integral part of the development process and as a result it is often performed by an internal team.

Grey Box Testing

Testers are provided with some information at the beginning of testing including URLs and user accounts.

Information gathering is a critical part of this type of testing.

Communication between the tester and target system personnel is critical.

This is the most common type of testing performed today.

Manual Testing

Manual testing using scripts and tools

The tester processes each page of the target application using tools and script to help manipulate and formulate requests as well as gather and analyze data.

It is time consuming but allows for the discovery of logic and business flaws that tools cannot find.

Thoroughness is dependent on the tester's time, attention and skill set.

Automated Testing

Automated tools are used to scan a target for vulnerabilities.

Many automated scanners are available including **HP WebInspect, Trustwave App Scanner, IBM AppScan, ZAP, Burp Suite.**

Rapidly scans site but can still take a long time.

Tester has less control and it is more prone to false positives.

Lacks the ability to provide business implications to discovered flaws.

Hybrid Web App Penetration Testing

Combines manual and automated techniques.

Scanner provide a starting point with manual verification and exploitation as follow-up.

As new components of an application are discovered the process returns to automated scanning, repeating the cycle.

Scripting is done as needed.

This is the most frequently used technique for testing.

Preparation

It is the first step, and is continuous.

Practicing and developing skills is paramount.

Managing a Web App Pen Test

Begins BEFORE the hands-on testing, involves the testing team and the target system personnel.

Developers can be brought in to help improve security awareness.

Any vendors or infrastructure providers should be included.

Establishing the Test Scope

The scope is defined by the purpose of the test. What are the concerns associated witht he target application.

The type of of test should be agreed upon black, crystal or grey box testing.

The scope of the test will define which applications and/or servers are involved and which should be avoided.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

Information Required for Testing

Applications included in the scope

Multiple user IDs and passwords, each pair having different access.

Technology restrictions such as client types, ports and servers to avoid

Emergency contact information.

Rules of Engagement

Identifying tester traffic and data
Target system personnel should be know source identifiers such as IP addresses, email addresses, and other identifiers.

Agreeing upon a testing time frame
This includes testing windows and time for analysis, reporting and follow-up. The deliverables should be scheduled prior to testing.

Establishing communications plans
There should be various contacts both technical and management, as well as methods including email, phone, and possibly IM. Sensitive information regarding vulnerabilities should be discussed over secured channels with PGP/GnuPG for email or OTR/encrypted IM.

Reporting

Probably the most important part of the penetration test, since it is the most lasting portion.

Format:
1. Executive Summary
2. Introduction
3. Methodology
4. Findings
5. Conclusions

All information gathered during testing becomes part of reporting, important notes, permissions, memos and other items may be included in the appendices.

Executive Summary

Contains a high-level overview of our test and findings

The audience is higher-level personnel.

Maximum 1.5 pages, best kept to a single page.

Contains the findings, including the root cause, and recommendations, which should be reasonable and accomplishable. Including recommended time frames including short-term versus long-term changes.

Introduction

Outlines the parts of the test including the scope, objective and the team.

This section should be 1-2 pages in length.

Methodology

A step-by-step explanation of testing including tools used.

It should be clear enough that a competent tester could reproduce and verify the test.

This section is often 3-10 pages in length.

Findings

This is the meat of the report including each finding categorized by risk as pertaining to the application.

In some cases findings will be divided by application.

Recommendations are part of the findings. If there are multiple, each should be provided with an explanation of the most beneficial.

Conclusions

This is the final part of the report and is similar to the executive summary.

The audience is the technicians, unlike the executive summary which is geared to higher-level.

Any appendices are added after the conclusion including
✔permission memos
✔lists of users harvested
✔records retrieved from the database
✔detailed tool output

Presentation

An optional part of penetration tests but an excellent way to work with developers.

Audience should be chosen by target personnel, possibly hold multiple sessions to focus the presentation on different kinds of staff such as developers, administrators, management and testing staff.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com