Penetration Test of a Web Application

March 13, 2009

1 Overview

In this exercise, students will perform a penetration test of the BadStore web application. Students will work in teams to complete the analysis and write a report identifying the vulnerabilities discovered and describing their relative risks. Students will use web application penetration testing tools from the OWASP Live CD to perform the assessment.

2 Resources Required

To complete this assignment, students will need a copy of the BadStore Live CD to analyze and a copy of the OWASP Live CD to provide tools for the analysis. The BadStore CD contains the web application that will be the subject of the penetration test. The OWASP Live CD contains a wide variety of web application security tools, including proxies (Burp Suite, Paros Proxy, and WebScarab), vulnerability scanners, and brute force and fuzz testing tools. The CD also contains a copy of the Firefox web browser with a wide variety of security add-ons, including EditCookie, FoxyProxy, LiveHeaders, and TamperData.

Both live CDs are available for free download. These CDs are used by booting a computer with the CD; no software needs to be installed on the computer's hard disk. The CDs can also be used by creating a virtual machine and booting the virtual machine with an ISO image of the CD. The advantage of using virtual machines is that both CDs may be used on a single computer by using one virtual machine for each CD. Virtual machine software, such as VMWare or Virtual Box, may be freely downloaded.

Students may use other free web application security tools if they want to. However, this exercise is a black box penetration test, so white box techniques such as static analysis of the application's source code may not be applied.

3 Rules of Engagement

This exercise is a black box penetration test. That means you cannot use your direct access to the BadStore VM to access the application's source code. However, you can attempt to access any URLs that are available and you can even use command injection attacks or file uploads to run commands on the VM to gain access to the source code that way. If you have any questions about whether a technique is black box or not, contact your instructor for confirmation on whether the technique is acceptable.

This requirement is not meant to make the exercise more difficult. It's meant to make the assignment more realistic and to help you understand the different types of vulnerabilities that can be found in a black box assessment versus a white box assessment like a code review assignment. Evaluating will be done based on how well you completed a black box assessment, not on how well you completed a white box assessment. In other words, it's about how you found the vulnerabilities, not simply how many you found.

4 High Level View

Study the BadStore application as a whole, exploring the entire site and following all accessible links. Search for hidden and default content, as well as content that is directly linked. Explore the site both as an anonymous user and as an authenticated user by logging in as the user specified in the BadStore manual. Test for hidden debug or administrative flags that may provide access to more content.

Once the site has been surveyed, identify the core functions that the application was designed to provide, along with the assets involved. Identify the primary security mechanisms that it uses to protect those assets and determine how they function. Identify the technologies used, including the operating system, web server software, and both client and server side technologies used to produce the web application.

Based on this survey of the site and your more detailed investigations, your penetration testing report should address all of the following questions.

1. What technologies are used in producing the site, including OS, server type and version, and client and server side technologies? List the known vulnerabilities by CVE number that exist in these technologies that underlie the application.

2. What entry points could someone use to enter the application? Write entry points as relative URLs. Except for the `action` parameter of `badstore.cgi`, ignore URL parameters. In other words, consider two URLs with different parameters the same entry point except for the `action` parameter. Prioritize the entry points by ease of access by an attacker. Use a three point qualitative (high, medium, low) score for ease of access.

3. What assets does this application have? What are the threats to those assets? Prioritize the assets by value.

4. What security controls does the application use? Describe each control, noting the URL where it was accessed.

5 Individual Assignment: Learn a Tool

Each person in the group must select one non-proxy testing tool from the OWASP Live CD or from other free sources that we did not discuss in class and that no one else in the group is using. Learn how this tool works and apply it to the penetration test. Write up a one page description of the tool, including its effectiveness as part of the penetration test and giving a step by step description of how to use the tool.

6 Auditing Vulnerabilities

For each vulnerability in the BadStore web application that was discovered during testing, write a description including:

1. The URL(s) where the vulnerability was found.
2. The type of vulnerability discovered (SQL injection, XSS, etc.)
3. The risk (ease of access multiplied by value of assets impacted) presented by the vulnerability.
4. Detailed instructions on how to replicate the vulnerability.
5. A one paragraph analysis explaining the impact of the vulnerability and its ease of exploitation.

List the vulnerabilities in order of risk from highest to lowest in your report.

Provide coverage analysis in your report, listing all entry points with the tests performed and a description of the percentage of vulnerable entry points. Provide a table or graph that shows the vulnerable entry points with the number of vulnerabilities discovered for each.

7 Submission

The final assignment submission will be a report describing your analysis of BadStore, including all of the components discussed above. Include tool output as appendices in separate files. Encapsulate all of the documents in a single ZIP file for submission.