Security Project
IN618 Security

May 31, 2016

Introduction

In this project you will work with a parter to do a thorough security audit of a web application. This project is worth 50% of your overall mark in the class, and it is due on **Friday, 10 June at 3:00**.

Scenario

A web development team is nearing completion of an initial version of new application and they need to have it carefully audited for security. A demo version has been deployed on an internal server for you to test and examine. At the completion of your audit, you will submit a detailed written report of your findings, identifying any security problems you find and making recommendations on how to improve the security of the application.

Process

You will carry out your audit in three phases:

Penetration testing

The application is running on a web server. Get the ip address from the lecturer and examine the application thoroughly. Using the web interface, attempt to perform various web-based attacks checking for vulnerabilities including SQL injection, cross-site scripting, and cross-site request forgery. Note carefully what tests you perform and include repeatable demonstrations of any successful exploits in your report.

Code review

Log onto the server (using our standard credentials), and examine the application source code. Besides checking the code for vulnerabilities mentioned above, ensure that any user data is handled with appropriate attention to security. If you performed any successful exploits, identify the vulnerable points in the source code and recommend corrective action to remove the vulnerabilities.

Server review

Finally , review the configuration of the application server, checking for exposed services, account security and general system issues. Identify any problems in your report along with recommended action to secure the server.

Exclusions

1. It is not your job to correct any problems or fix any bugs, just identify the problems you find and recommend steps to fix them.
2. Any issues with the application not related to security are outside the scope of this assignment. The application should work well enough for you to test, however, so tell the lecturer if it does not.
3. Each application includes a script to create the initial database. This is for development and testing and will not be included in released versions, so it's presence is not a security issue at this point.

Submission procedure

You are to submit a hard copy of your report to the lecturer in D205 on or before the due date and time. Your report document shall be written and presented to a high professional standard.