CS3511 - P3 - SQL INJECTION

Overview

In this practical we are looking at SQL injection. The aim is to explore injection flaws and to get a feeling for how hackers use these. Again, the aim of this practical is not to teach you how to become a hacker, instead it is the aim to understand what hackers do so that you can implement appropriate defence methods. Use the tools and environments provided for this practical; do not attempt injection attacks on existing web services!

In this practical we use *WebGoat* which has been used as well in the previous practical. In addition, a web browser is required and for the very last exercise you might use python. You also need a basic understanding of SQL.

WebGoat

From the WebGoat's description page: WebGoat is a deliberately insecure application that allows interested developers just like you to test vulnerabilities commonly found in Java-based applications that use common and popular open source components. Now, while we in no way condone causing intentional harm to any animal, goat or otherwise, we think learning everything you can about security vulnerabilities is essential to understanding just what happens when even a small bit of unintended code gets into your applications. What better way to do that than with your very own scapegoat? Feel free to do what you will with him. Hack, poke, prod and if it makes you feel better, scare him until your heart's content. Go ahead, and hack the goat. We promise he likes it. Thanks for your interest! The WebGoat Team.

For this practical WebGoat is installed on the server X.X.X.X on port 8080. Using a web browser you can navigate to *http://X.X.X.X:8080/WebGoat/* to interact with the service. As a first step you have to create an account by providing a username and password. After logging in you will be provided with a bunch of hacking exercises. In this practical we will look at a subset of these exercises as explained later.

PART1: Introduction

This part is only required if you have not done this in the practical 2 weeks ago.

Use a web browser to navigate to WebGoat: *http://X.X.X.X:8080/WebGoat/*. Create an account on the system by providing a username and password.

Navigate to the *Introduction* section and read about WebGoat.

PART2: SQL Injection I

Navigate to the *Injection* section and in there to the subsection *SQL Injection (intro)*.

Complete the 13 lesson steps....

PART3: SQL Injection II

Navigate to the *Injection* section and in there to the subsection *SQL Injection (advanced)*.

Complete the 6 lesson steps....

CS3511 Continuous Assessment - PART 3

Please submit an answer to the following question with your CS3511 Continuous Assessment. Your answer should not be longer than half a page (You can use figures or code pieces to illustrate your answer).

Question P3 [2 MARKS]: Prepared Statements

Explain how the use of Prepared Statements prevents SQL injection attacks. Please give a commented code example, describing the difference between data base access with and without the use of Prepared Statements (any programming language may be used for illustration).