Assignment 7

Security Testing – SQL Injection

Simple and blind SQL injection + Mitigation techniques

Due Date: Mar. 12, 2020

You have about two weeks for completing this activity. When you finish your individual part, you can demo your work during the lab sessions.

The second security assignment will be released next week and will be due on March 19.

Yasaman Amannejad, 2020

TABLE OF CONTENTS

1 INTRODUCTION

In this assignment, you will learn SQL injection and practice testing applications against possible SQL injection attacks.

This assignment needs to be done a **combination of individual and group work**.

Students can use Kali Linux and Web Goat installation in B215 to complete this assignment or they can set up their own environment. Metasploitable, will be used in the group activity, and students can install it in their cloud machines.

Students must complete all SQL injection tasks in WebGoat (normal, blind and mitigation) individually, and then complete three tasks (steps 5-7) in Section 3. Finally, you need to write about the definition and importance of ethical hacking (step 8).

Submission - Students must demo their WebGoat activities during the lab session. The group work (steps 5-8) must be submitted in BlackBoard before the assignment due date.

2 TOOLS & SYSTEM UNDER TEST

2.1 KALI LINUX

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security Ltd. You can access the documentation for Kali Linux at https://www.kali.org/docs/ . Kali linux is installed for you in lab B215. Kali Linux has security tools grouped in different categories. Blind SQL injection usually takes longer time, and you may need to use a tool for completing your tasks. SQLMap or Metasploit (it is different from metasplitable!) can help you with this process. Open SQLMap commandline in Kali Linux and type sqlmap --help to see the options that you can use in this tool. Follow the steps in the class to use this tool.

2.2 WEBGOAT 8.0

WebGoat is a deliberately insecure web application maintained to learn Web application security lessons. It includes step-by-step activities that you can complete and get immediate feedback! Your task in this assignment is to complete the SQL injection tasks in WebGoat. WebGoat is installed for you in the lab. You can complete and save all your tasks there.

`

2.3 METASPLOITABLE 2.0

Metasploitable contains a set of vulnerable Web applications that can be used as software under test for Web application security testing. We will use DVWA (Damn Vulnerable Web Application). Metasploitable is **NOT** installed on the lab machines, please follow the provided installation guideline and install it on your cloud machines.

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help

web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface. You will complete your tasks with Security level = low.

3 INSTRUCTION

❖ **Open WebGoat, and complete these tasks:**

1. All students must complete the WebGoat tasks, **individually**. Please feel free to get together as a team and discuss possible solutions with your team members, but when you find a solution, each member must complete their tasks individually, in their WebGoat system. This will allow everyone to have a basic understanding of SQL Injection.

   Tasks 1-5 are a review of your DB knowledge, and tasks 6-13 are designed for practicing simple SQL injection. Some steps are designed just as a reading material and prepare you for the next steps. Do not miss the reading parts! There are hints for some of the tasks. Do not check them as your first option, but if you need help, feel free to use the hints provided in WebGoat to complete your tasks!

   The completed tasks will appear in Green in your WebGoat. Each student must demo/show their completed tasks in WebGoat during the lab sessions. Your instructor may ask you questions about the solutions you have used.

   After completing each task in WebGoat, to make sure that you have a copy of your answers, you can document them in a word file (so that you do not lose them accidentally or because of any weird reason!). No excuse is accepted for loosing your answers! ☺

2. Follow the same team discussions and individual implementations for SQL injection (advanced) tasks. Feel free to use SQLMap or Metasploitable for blind injections, if needed.

3. Follow the same team discussions and individual implementations for SQL mitigation tasks.

❖ **Install Metasploitable 2.0 and complete the following tasks:**

4. Please refer to the installation guide to install Metasplitable on your cloud machine. Note that Metasploitable is a very vulnerable application. Do not keep your cloud VM up and running for a long time. It can get attacked and black-hat hackers can exploit your VM! The default username and password for DVWA are **admin**, **password**. Set up the database and set the security level to Low.

   Complete the following tasks and **document your solutions in a Word document and submit it in Blackboard**. Feel free to use SQLMap or Metasploitable for blind injections, if needed.

You can use the SQL injection tabs (normal or blind) to complete the following tasks:

5. Write an input in the User Id field to find out the first name and last name of all users in the database!

6. Assuming that password of users are stored in the "password" column of the "users" table and in password column, extract the hashcode of all passwords in the system. Explain the process and results and provide your input string and screen shots of steps in your report file.

7. Attack the system using the SQL injection tabs (manually, or using the automated tools) and extract as much as information you can from the database of the DVWA application. Document the steps that you have tried (your inputs and screenshots) and include the information that you have extracted.

   This is an open-ended task and grading will be mainly done based on the completeness of the steps that are followed. Make sure to document your steps in a clear and readable way.

8. In your report, answer the following questions:
   a. What is **ethical hacking**?
   b. Why is it important to follow ethical hacking process in security testing.

4 SUBMISSION

4.1 DELIVERABLES

- **Individual tasks with WebGoat -** Each student must demo their WebGoat tasks on their WebGoat account. You can demo during the lab sessions.

- **Group activity** – You should submit your group report in BlackBoard.

4.2 MARKING SCHEME

	Item	Grade
Individual work	Web Goat, SQL injection (Introductory tasks)	15%
	Web Goat, SQL injection (advanced)	20%
	Web Goat, SQL injection (Mitigation)	20%
Group work	DVWA – extracting the list of users	5%
	DVWA – extracting the password hashes	10%
	DVWA – extracting any information you can! - Comprehensive testing process and try of different SQL injection attacks (manually/automated) - Final outputs	 20% 5%
	Ethical hacking – definition and importance	5%