Sistemas de Software Seguros
Segurança de Software
2024/2025
Class Project: Experiments with WebGoat (class 3)

1. Setup the System

Like in the previous classes, we will WebGoat in this lab. Whenever there are questions on how to setup the tools, please look at the last project description. Execute the following steps to initiate the class:

a) Start the image of the course in a virtual machine (VirtualBox player)

b) Initiate the WebGoat by opening a Terminal, changing the current directory to `~/apps/WebGoat` and running: `java -jar webgoat*` . Then, you have to run the web browser (Firefox) and open WebGoat by selecting the URL:

```
http://localhost:8080/WebGoat
```

c) To enter, either register a new user or utilize the account with the username "`guestss`" and the password "`guestss`". Select the "Sign in" button to initiate the lessons.

2. LAB: SQL Injection

Let's start by recalling a few of SQL commands by running the following lessons over a table called "employees", which contains the information about several people working at a company.

Try to solve the lesson Injection >> SQL Injection (intro) >> step 2

The objective of this lesson is to retrieve the information about Bob Franco. Which SQL query should you use to get this information from the table? (HINT: if you have questions regarding SQL, maybe you can look at the site http://www.sqlcourse.com/ ; the SELECT command might be a good place to start)

Try to solve the lesson Injection >> SQL Injection (intro) >> step 3

The objective of this lesson is to change the department of Tobi Barnett to 'Sales'. Which SQL query allows you to change this information from the table? (HINT: maybe you can try UPDATE)

Try to solve the lesson Injection >> SQL Injection (intro) >> step 4

The objective of this lesson is to modify the table scheme by adding the column "phone" (varchar(20)). Which SQL query allows you to modify the table? (HINT: maybe you can try ALTER TABLE)

Try to solve the lesson Injection >> SQL Injection (intro) >> step 5

The objective of this lesson is to grant the user "unauthorized_user" rights to the table “grant_rights”. How can we achieve that? (HINT: maybe you can use a GRANT command)

Now things get a bit more interesting as we will be able to experiment with SQL injection attacks. Nevertheless, we will start slowly by experimenting first with the inputs and see how they affect the SQL query. Do not forget that your keyboard has several characters to delimitate strings (“ , ‘ , ´ , `) ; **Make sure you pick the right one** for your database!

Try to solve the lesson Injection Flaws >> SQL Injection (intro) >> step 6

This lesson allows you to see how different inputs can modify the resulting SQL query. Experiment with several input until you are comfortable at making this sort of modifications.

Try to solve the lesson Injection Flaws >> SQL Injection (intro) >> step 9

It is time to perform a String SQL Injection. You have a SELECT query and you can modify one of the predicate fields by providing an input. How can you retrieve the information about all users?

Try to solve the lesson Injection Flaws >> SQL Injection (intro) >> step 10

Now let’s do a Numeric SQL Injection. There are two fields where you can input data and one of them is vulnerable. How can you perform the injection? Maybe you can start with the first field, and if it doesn’t work, you experiment with the second one.

Try to solve the lesson Injection >> SQL Injection (intro) >> step 11

In the lesson, the attacker uses SQL injection to retrieve sensitive data from the database. In particular, you are user John Smith, and you want to take a look at the data of all your colleagues to check their current salaries. The web page has two input fields. How can you exploit a String SQL Injection to get all data?

Try to solve the lesson Injection >> SQL Injection (intro) >> step 12

Now let's take advantage of query chaining to break the integrity of the database. In particular, you want to increase your salary to make you the employee that earns most at the company. What sort of injection should you perform to achieve this goal?

Try to solve the lesson Injection >> SQL Injection (intro) >> step 13

Great! Now you earn a lot but there is the risk that your previous actions are seen by one of the administrators. How can you cover your tracks? Maybe you can delete the log! What would you inject?

Delivery of the Report

The output of the class project is a report answering all the questions and including the justifications for the responses. Each group should deliver the report either by submitting it in the course moodle page, or if there is some difficulty with this method, by emailing it to the professor of the TP class. The file type should be a pdf.

Deadline: 25 November 2024 (there will be no extensions)

==========
The next exercise is optional!
==========

Try to solve the lesson Injection >> SQL Injection (advanced) >> step 3

This exercise has two sub-objectives, first to obtain information from the `user_system_data` table, and second, to retrieve the password of user Dave. How can you achieve this? (HINT: Maybe you could use a UNION, or alternatively by concatenating a SELECT.)