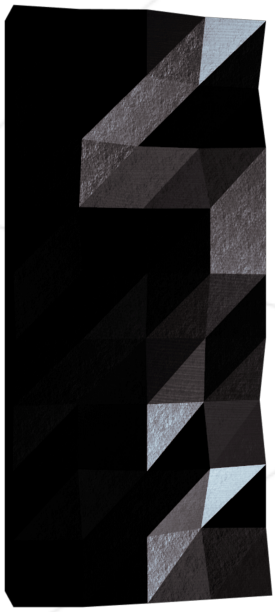

Bootcamp Ciberseguridad | 42 Madrid

Vaccine

Summary: SQL Injection

Version: 1

Contents

Chapter I

Introduction

We all know how important secure programming is. In this case you will try to find `filtering errors in the data input`. `SQL Injection` is the injection of SQL commands to alter the behaviour of a program and execute commands on the database. In this project you will create a tool that is able to detect SQL injections providing a URL.

Chapter II

Mandatory part

The tool should have a battery of tests to run against a given URL and, depending on the responses, be able to detect SQL injections. You can detect the type of database engine to make the tests more successful (2 minimum). The tests can be based on several types: union, error, boolean, time and even blind (2 minimum).

In case a website is confirmed to be vulnerable, the following can be obtained:

- The vulnerable parameters.
- The payload used.
- Database names.
- Table names.
- Column names.
- Complete database dump.

The tool must have some storage file for the data, if it does not exist it will be created on the first run.

Program name	`ftname`
Turn in files	`ftturnin`
External functs.	`ftfuncts`
Description	`ftdesc`

The program `vaccine` will allow you to perform SQL injection by providing a url as a parameter. You will manage the following programme options:

```
./vaccine [-oP] URL
```

- Option `-o` : Archive file, if not specified it will be stored in a default one.
- Option `-X` : Type of request, if not specified GET will be used.

You can use any programming language, you should not use libraries that automate SQL injection.

Chapter III

Bonus

The evaluation of the bonuses will be done `IF AND ONLY IF` the mandatory part is `PERFECT`. Otherwise, the bonuses will be totally `IGNORED`.

You can enhance your project with some or all of the following features:

- Wider range of database engines.
- Wider range of SQL injection methods.
- The tool allows you to edit various parameters of the request, e.g. the User-Agent.

Chapter IV

Peer review

This project will be corrected by your classmates. Deliver the files to the Git repository and make sure everything works as expected.