Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 14
DATABASE HACKING

DRAFT

HACKING IS LEARNING
www.hackerhighschool.org

ISECOM

WARNING

The Hacker Highschool Project is a learning tool and as with any learning tool there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there is not enough research on possible effects of emanations from particular technologies. Students using these lessons should be supervised yet encouraged to learn, try, and do. However ISECOM cannot accept responsibility for how any information herein is abused.

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool Project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license, including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the HHS web page at http://www.hackerhighschool.org/licensing.html.

The Hacker Highschool Project Project is an open community effort and if you find value in this project, we ask that you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

Contributors

Marta Barceló, ISECOM

Pete Herzog, ISECOM

Bob Monroe, ISECOM

ISECOM

Introduction

Databases, as their name implies, store data for our use. They are the backbone of any organization. Databases run in the background of almost every application businesses use today. Most websites could not function without an RDBMS.

What is an RDBMS?

A relational database management system (RDBMS) is the system most database solutions use today. MySQL, PostgreSQL, SQLite, Microsoft SQL Server, and many other solutions use the relational database model. In this model, data is stored in database objects called tables, and the tables are made of columns and rows of data. A collection of rows and columns is a table, a collection of tables and their relationships with each other is a database.

MySQL

MySQL is an RDBMS that is open source and freely available. It is stable and very widely used. Companies like Google, Facebook, and most websites run on MySQL.

Microsoft SQL Server

SQL Server is a Microsoft product widely used in business applications due to its tight integration with Microsoft and other products.

SQL

Every databasing solution has the letters "SQL" in their name. SQL is an acronym that stands for Structured Query Language. It is a programming language that is specifically designed to retrieve, sort, and otherwise manipulate data efficiently in an RDBMS. Relational database solutions use queries, or a collection of SQL statements, to function. SQL can pose a vulnerability in any application that uses it, called SQL injection. We will discuss SQL injection later. SQL is a very extensive language, and there are many things you can do with it. We will only visit two basic statements, SELECT and INSERT INTO. Here is the syntax of a basic SELECT statement:

SELECT column_name1, column_name2,... FROM table_name;

Here is a simple SELECT query:

SELECT * FROM my_table;

This statement selects all columns in my_table. If you wanted to select certain columns, you would specify which columns separated by commas. Next is the INSERT INTO statement:

INSERT INTO my_table (column1, column2,...) VALUES (value1, value2,...);

This statement inserts a new row of data into your database, containing the values you specified.

SQL Injection

SQL injection is a technique used by crackers to hack databasing solutions. This is accomplished using "escape" characters and inserting rougue code into the application,

which can do anything, only limited by the crackers creativity. SQL injections can dump the database to the attackers computer, modify administrative accounts of the web application, modify data to suit the crackers needs, and they can even just destroy all the data. Here is how it works.

Let's say that an application takes an input from a user and uses it in the variable $input in this SQL query:

$mysql_query = "SELECT username, password FROM user_table WHERE username = "'.$input.'"";

When the user types in the user name to search for, say user123, the $input value is inserted into the SQL statement, and it becomes the finished statement, ready to be executed:

SELECT username, password FROM user_table WHERE username = user123

An attacker would enter something like this into the user name field:

' OR '1'='1

Lets replace $input with the above injection and check out how that looks when it is inserted into the SQL statement:

$mysql_query = "SELECT username, password FROM user_table WHERE username = "" OR '1'='1";

And the executed SQL statement would look like this:

SELECT username, password FROM user_table WHERE username = '' OR '1'='1'

This is the most basic SQL injection attack. Since the OR clause 1=1 always evaluates to true, the access would be given to the attacker, even though they have no real credentials.

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM