Introduction to Website Database Vulnerabilities

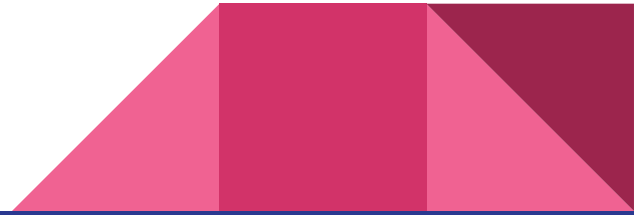
Mr. Lee and Mrs. Weiss

Introduction to Website Database Vulnerabilities

Database Vulnerabilities = Hackable!

How do you define “to hack a database”?

To hack a database is to “trick” the databases to do things that the programmers did not intend to allow to be done.



Introduction to Website Database Vulnerabilities

DISCLAIMER:

Remember that you are testing a vulnerability in a permitted, contained environment. Attempting any of these techniques on another website that is not wholly owned by you is considered a **cyber crime** and most likely falls under **federal jurisdiction**.

In other words: ***DON'T TRY THIS AT HOME!***

Introduction to Website Database Vulnerabilities

Types of Vulnerabilities

Error based: If the application displays database errors to the user, an attacker may learn key information.

Union based: append the data that the attacker wants to a table that is already displayed in the page.

Blind(brute force): E.g. you could send the statement "if the first name of the username is an *a*, wait 10 seconds. If the application takes 10 seconds to perform the query, the username starts with an *a*. Obviously brute force is time intensive, so this approach should be considered a last resort.

Introduction to Website Database Vulnerabilities

YOUR TASK:

Test Error Based Vulnerability

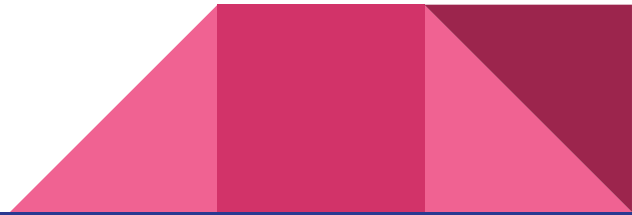
Log onto the following website: http://34.197.52.233/DVWA-master/index.php
This is a sample web application.

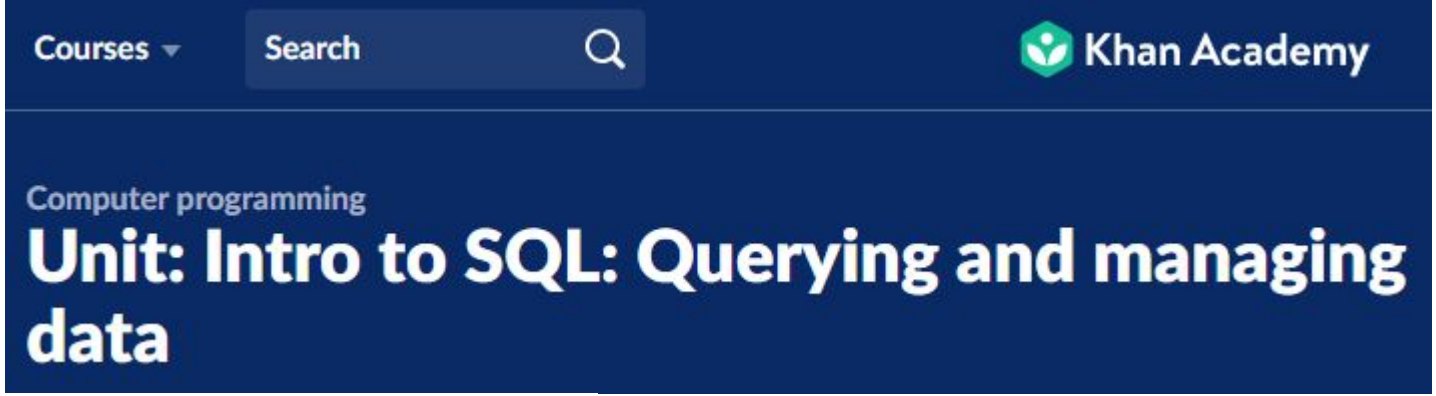
Fill in the table with your answers first, and then supporting screenshots when applicable. Read carefully!

Follow-up:

Presentation of some commands, and the results, visually.

We focused on the general syntax of SQL by using the “SELECT” command, since that is the command students saw on the worksheet. For example, show how variable type and upper/lowercase do not make a difference.





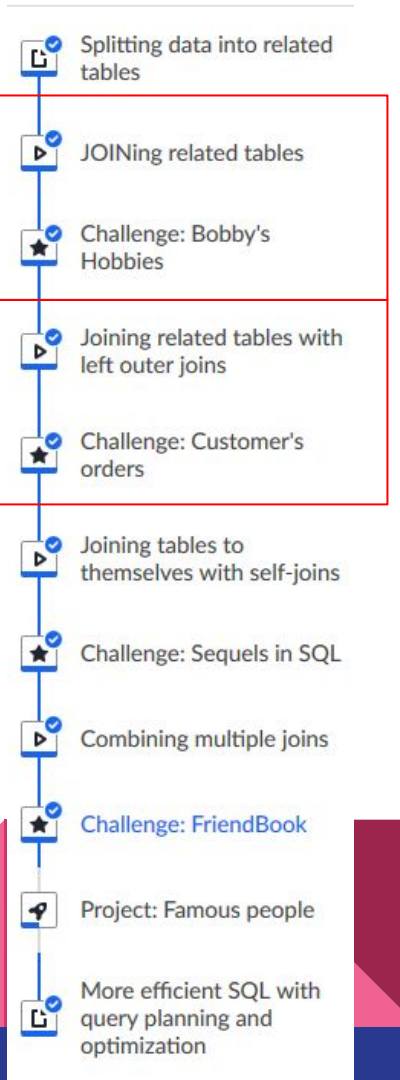
Khan offers 4 sub-units on SQL.

You don't have to cover them all.

Topics/days

Each lesson is a video followed by an assignment.

We recommend assigning up to 2 “challenges” a day.



SQL Server not needed for small tasks