Challenge #3 SQL Injection

[ 1. SETUP ]

Setting up Virtualbox:

For this particular challenge we’re going to be using a virtual machine that contains a local web application. We’re going to run it and use it to practice SQL injection! Before we do that we need to download and install VirtualBox: <https://www.virtualbox.org/wiki/Downloads>.

Importing the VM:

The important step is to download the virtual machine at this link: [Download](https://www.dropbox.com/s/u9odw1myr3owqxh/OSS_Ubuntu16.04.3.zip?dl=0). Afterwards you want to start up VirtualBox and select **File -> Import Appliance -> Select the VM you’ve just downloaded**. The import setup should be pretty straightforward and you should be able to double click on the **OSS\_Ubuntu16.04.3** your VirtualBox manager to start it up.

Starting up the web application:

The password for the login is: **secure123**. Once you’ve logged in, open up the terminal or press (CTRL + ALT + T). Type these commands in the terminal:

* cd OSS\_SQL
* npm start

Afterwards you should see something like [this](https://i.imgur.com/kGcXWoY.png) pop up in your terminal, the web server is now running! To access the actual web page open up the browser and type **localhost:3000** in the address bar. You should now be able see all three of the sub [challenges](https://i.imgur.com/eBhJ65A.png).

Note: If the server crashes somehow just open up the terminal and run the commands again.

[ 2. WHAT IS SQL INJECTION? ]

Summary:

SQL injection is an attack that occurs when an attacker tries to execute malicious [SQL statements](https://www.w3schools.com/sql/sql_syntax.asp) on a web application. This will result in allowing the attacker login to a website without having to provide a correct username and password. The attacker could also add themselves into the system or even modify different parts of the database.

More info: <https://www.acunetix.com/websitesecurity/sql-injection/>

Try out these hands on resources (Good for beginners!):

* <https://www.codebashing.com/sql_demo>
* <http://sqlzoo.net/hack/>

Important!

SQL INJECTION IS ILLEGAL IF YOU DO IT WITHOUT PERMISSION!

[ 3. NOVICE CHALLENGES ]

Sub Challenge #1:

Can you figure out how to login without knowing the username and password?

* What SQL statement did you use to bypass the login portal?
* Screenshot the result!
* Hint #1: What are the error messages telling you? (If there are any.)

Sub Challenge #2:

It seems like there’s a database that holds information about sick patients. This form requires that we enter a patient ID in order to get the information about that patient, but we don’t really need that do we? (If you want to see what a result would look like, use 2 as the patient ID.)

* Can you obtain a list of ALL patient info in the database?
* What SQL statement did you use to get it?
* What kind of issues does patient Josh Christ have? What about Tyler McConnell?
* Screenshot the result!
* Hint #1: What are the error messages telling you? (If there are any.)

Sub Challenge #3:

Hmmm… Looks like you weren’t added to the V.I.P. list, too bad.

* Get yourself on that list!
* What SQL statement did you use to add yourself?
* Screenshot the result!
* Hint #1: What type of information is shown on the V.I.P. list?
* Hint #2: The table name is **vip** and it has the attributes **fname** and **lname**.
* Hint #3: What are the error messages telling you? (If there are any.)
* Hint #4: [This](https://www.w3schools.com/sql/sql_insert.asp) might give it away.

[ 4. VETERAN CHALLENGES ]

Sub Challenge #4:

* In sub challenge #1 can you figure out one or two usernames that are in the database?(excluding admin)
  + Hint #1: The usernames are common first names with no numbers.
  + Hint #2: You can verify your guess by trying to log into the login portal with the username.
  + Hint #3: [Hmmm…](http://sqlzoo.net/hack/20user.htm)
* Same thing in sub challenge #1 but find the table name instead.

Sub Challenge #5:

* Given [this](https://i.imgur.com/dmuq59N.png) code snippet explain how you would defend against something like SQL injection?