

Dylan Ramdhan

CS 357, Prof. Goldberg

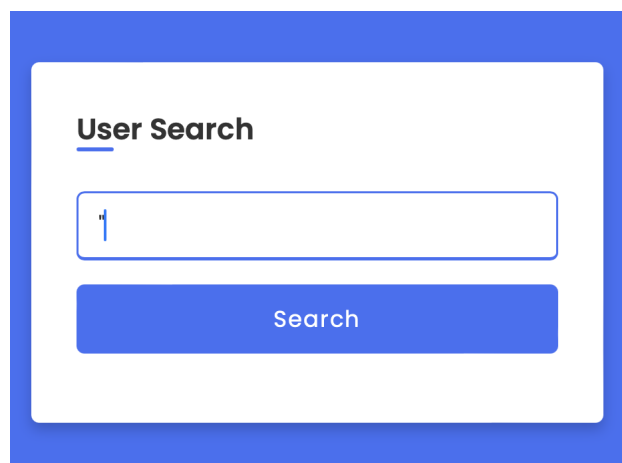
Login Authentications Challenges: Challenge 3

Nov 3, 2023

### Login Authentication Challenges Report: Challenge #3

#### Step #1: Checking for Security Weaknesses

In this challenge we do multiple steps with MD5. We first append '/search' to the site's link, which brings up the search page (1). After I typed " into the search and got the result of **Internet Server Error** (2) which indicates that the developer had written the SQL code in single quotations and not double quotations.



*1. User Search*

#### **Internal Server Error**

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

*2. Internet Server Error*

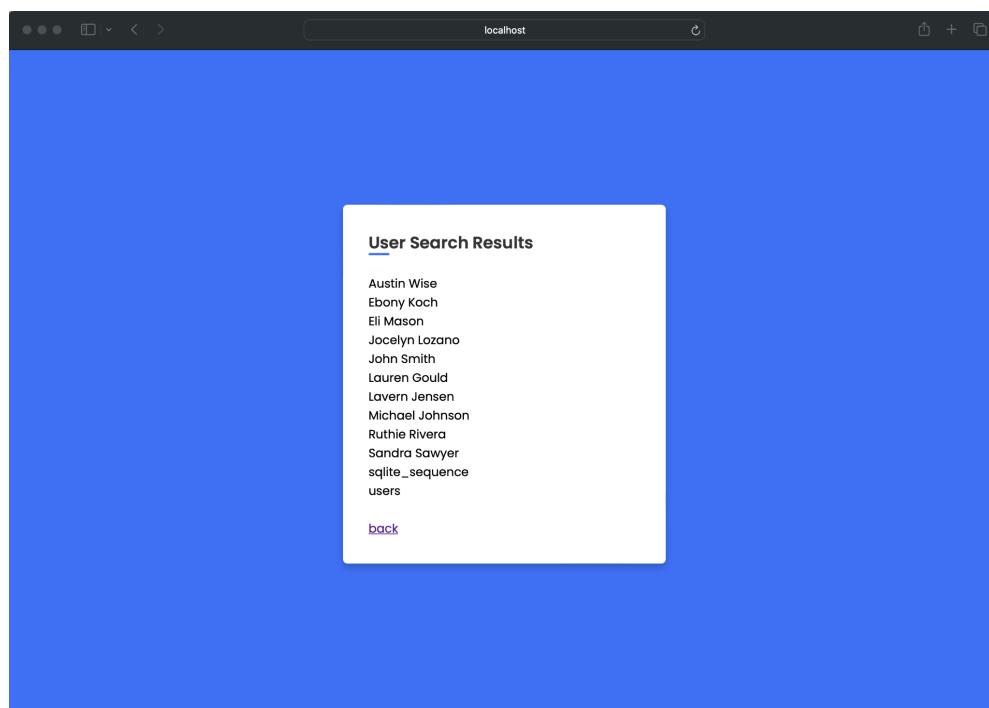
## Step #2: Attacking Website with SQLite

After noticing this mistake, it can be shown that we could proceed in the hack. After typing the SQL code:

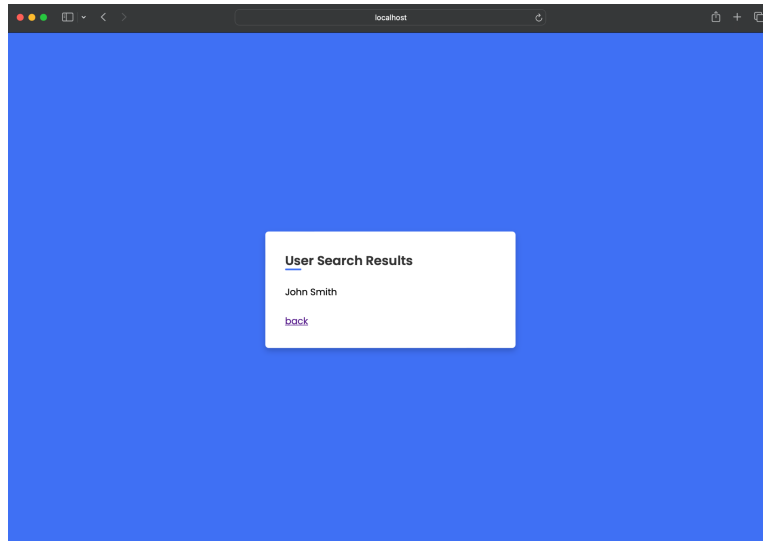
*" UNION SELECT name FROM sqlite\_master WHERE type="table"; --*

We would then receive the names of all the users of the site (1). After we continue the attack by really finding the main admin of the website which can be found by using the SQL code (2):

*"" or username="admin"; --*



### *1. Users of Website*

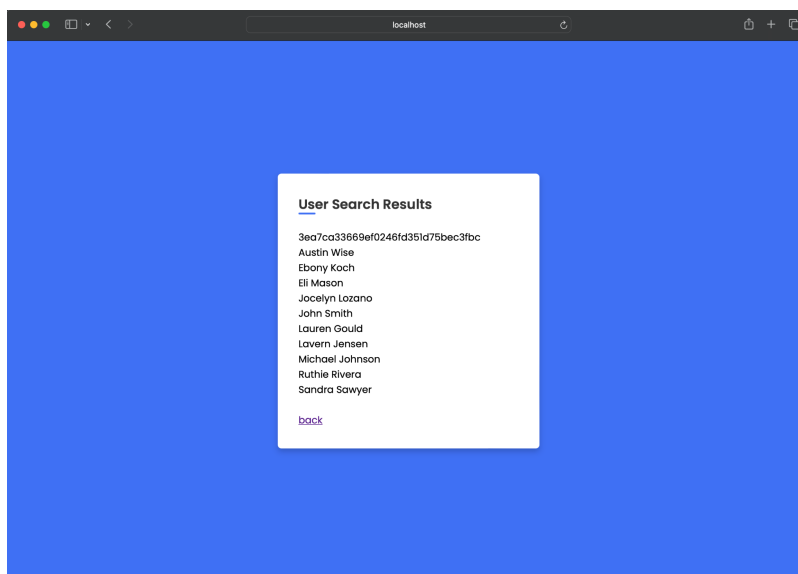


## 2. Main Admin of Website

### Step #3: Retrieving Admin Password from Reversing MD5 Hashes

After finding out the main admin of the website, John Smith, we can now focus on finding the admin's password through the use of SQL code in the User Search. Which would result in looking like this (1):

*" UNION SELECT password FROM users WHERE username="admin" --*



## 1. Entering SQL for Admin's Password

*2. Link for Reversing the MD5 Link:*

<https://md5.gromweb.com/?md5=3ea7ca33669ef0246fd351d75bec3fbc>

Thus revealing the admin's password in MD5 is: **3ea7ca33669ef0246fd351d75bec3fbc**. Once acquiring the MD5 code, we can reverse the MD5 code of the password and reveal the password. Thus the password is: **SecurePasscode2015!** After retrieving the password, we can test it by having username "admin", and password "SecurePasscode2015!", revealing that this password works.