**The A-Team (#1) – SQL Injection Challenge**

**login1.php**

1. We started by adding ‘?debug=true’ to the URL to see the actual query executed.  
   Shape, rectangle

   Description automatically generated
2. We saw that the query contains “AND password = “ and except for user’s password. To bypass this, we closed the query after the username by adding apostrophe (‘) and then the number sign (#) for ignoring rest of the query (represents the beginning of a comment).
   * Instead of a number sign (#) we can use the double-dash (--), but required to be followed by a space (or a tab, newline, etc..).

Shape, rectangle

Description automatically generated

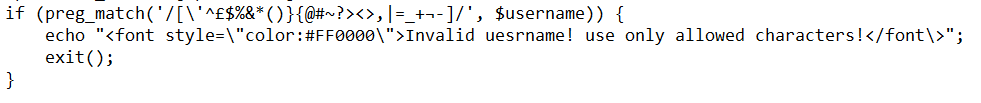
1. Inserting username can be avoided by adding a boolean condition to get True expression.

Shape, rectangle

Description automatically generated

**Fixed login1.php**

We have two suggestions to fix this page:

1. Using the ‘preg\_match’ function to monitor special characters in the input.  
   
2. Changed the query and using the ‘real\_escape\_string’ function on the input to escapes special characters.

Graphical user interface, text

Description automatically generated

**searchproducts.php**

1. We started by adding ‘?debug=true’ to the URL to see the actual query executed.  
   (and by sending an empty form we get the entire table).

Graphical user interface, text

Description automatically generated

1. After a few queries, we discovered that we can insert information into the table, and by trial and error with the select parameters, we saw that we have 5 columns in the table.  
   *' union select null, “Team1”, “Shir”, “Omer”, “Haim” #*

Graphical user interface, text, application

Description automatically generated

* 1. First, we used functions to insert useful information like the name of the database, version, user and more.  
     *' union select null, database(), user(), version(), null #*

Graphical user interface, text, application

Description automatically generated

* 1. Then, we wanted to find what are the columns and the tables in the database we found.  
     *' union select null, table\_name, column\_name, null, null from information\_schema.columns where table\_schema="sqlitraining" #*

Graphical user interface, text

Description automatically generated

* 1. Now, we want to see what inside the table “users”, this will give us all of the users and passwords (encoded by MD5 hash function).

*' union select null, id, fname, username, password from users #*

Text

Description automatically generated with low confidence

**Fixed searchproducts.php**

1. Changed the query and using the ‘real\_escape\_string’ function on the input to escapes special characters.  
   Text

   Description automatically generated

A picture containing text, person

Description automatically generated