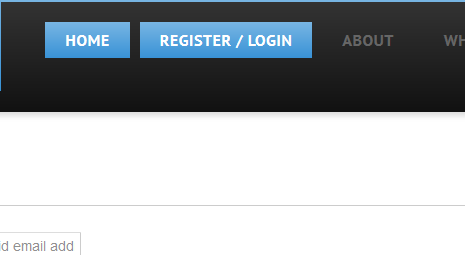
**Application Security CA 3**

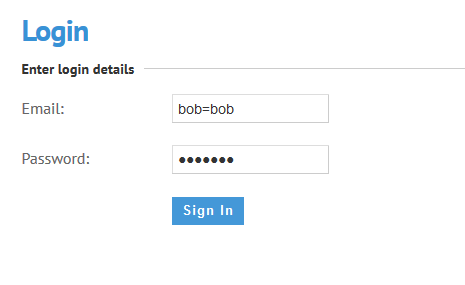
**SQL Injection**

1. Login without a username and password

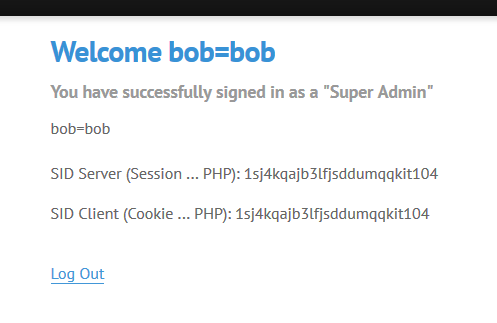
first click on register /login and scroll down to login



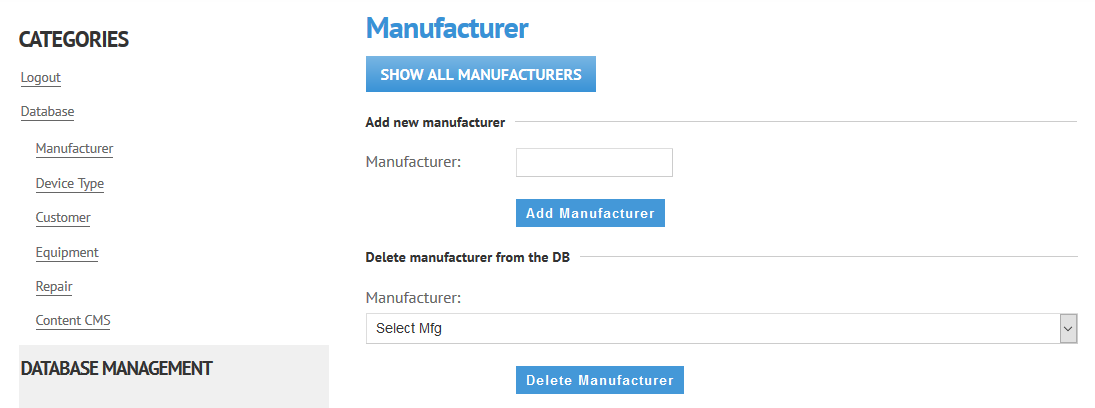
On login enter an SQL statement that will cause the value entered to be true, any value made equal to itself will be true indefinitely which tells the server that the below values are true even if they don’t actually exist.



Sign in was successful, I’m also logged in as the super admin.

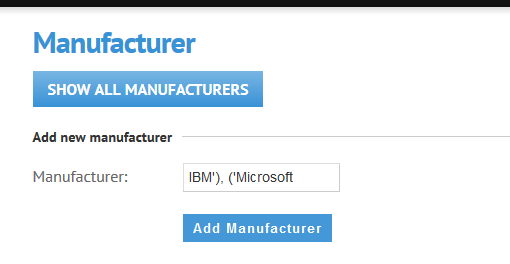


Click on the manufacturer tab to access the page for adding new manufacturers.

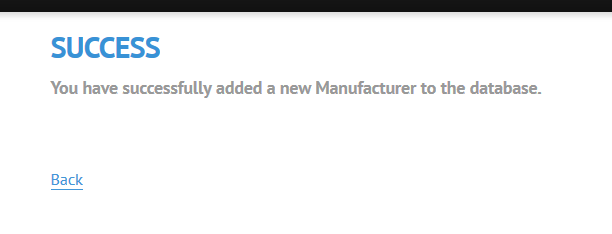


1. Adding Two manufacturers at the same time

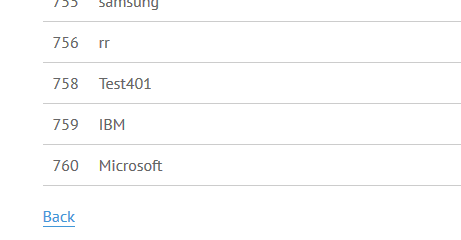
The SQL code written and inserted into the add manufacturer field adds two manufacturers at the same time. [IBM'), ('Microsoft]



Notification of success shows even on failure, important to double check the data has been entered.

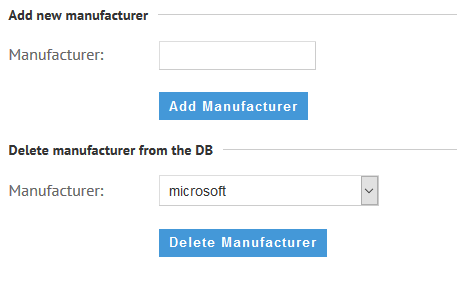


The new data entered is in the database.

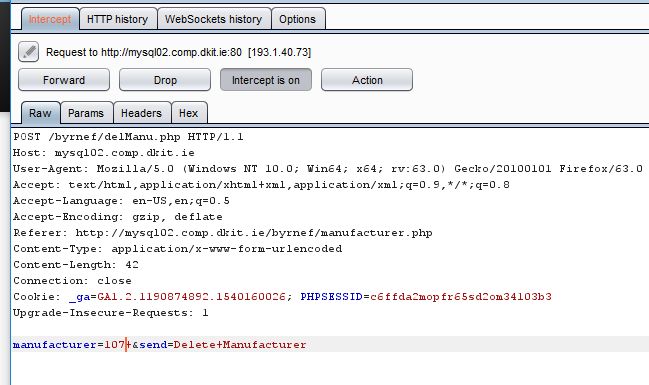


1. Delete two items at once

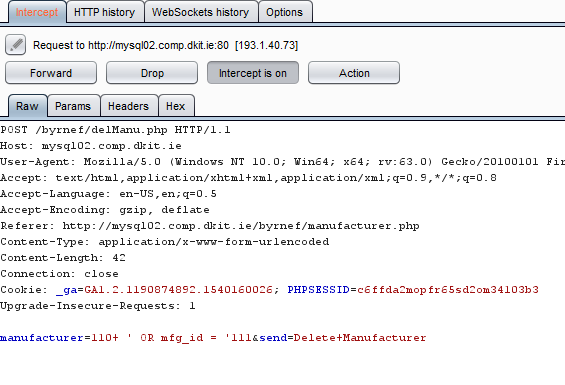
First a manufacturer was picked in Firefox to be deleted



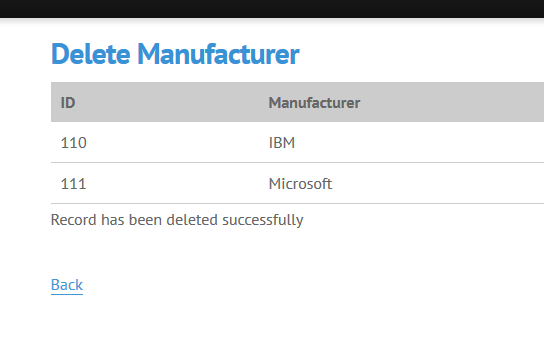
The query was intercepted in Burp which displays the selected manufacturers id number.



To delete a second manufacturer simultaneously, the OR operator was added, as well as the manufacturer id field name and another manufacturers id number. Forward id then clicked to force the action on the website.



With that action completed, two manufacturers have been deleted at the same time.



**Cross Site Scripting Flaws**

1. Include benign script display hello message

Add the script to the comment field to cause a “Hello” message to appear, this visually demonstrates what cross site scripting can do.



Once the script was entered into the comments section, it executed displaying a message with the “Hello” text written in the script.



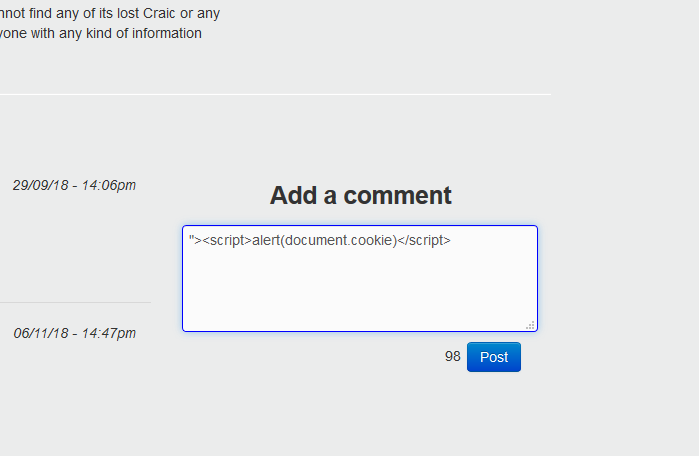
The Script does not display in the message thread on the website for other users to see, any who click on WTC news Still Craicless will get the hello message pop up on entry.



On immediate entry to the page a user is greeted with the message.



This script will display the cookie using the same method used to display the hello message.



The script has displayed the php session id cookie, which an attacker can use to access the site as that user. If the system thinks the attacker is the user based on this, an attacker may be able to obtain more sensitive information on the user.

