Adam Romayor

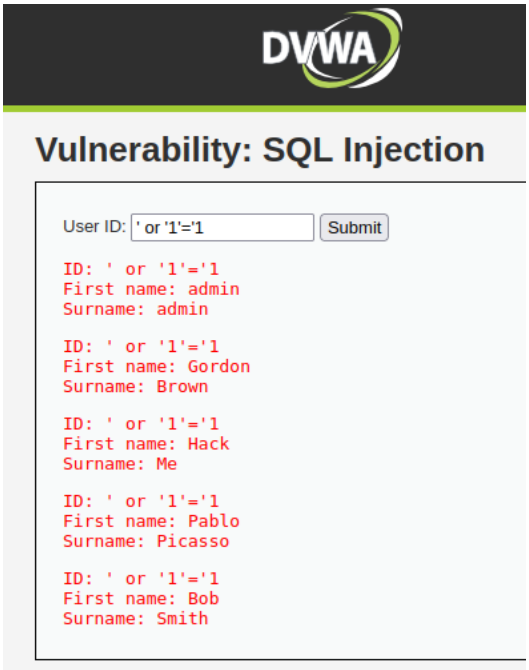
Assignment 3

Describe the SQLi attack you used. How did you cause the user table to be dumped? What was the input string you used?

I included a command that always returns true, so all the user tables will be printed.

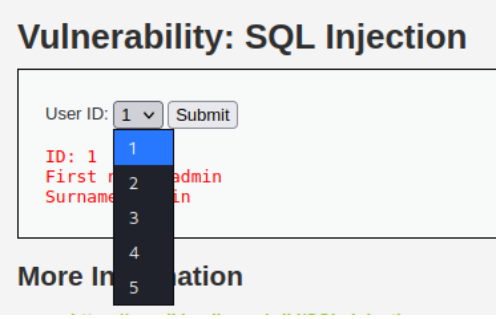
The exact string I used is: **' or '1'='1**

The first single quote closes the expected input string, and the second command **or ‘1’=‘1** will always return true. This does not include a single closing quote, because the program adds it when executing the query.



If you switch the security level in DVWA to "Medium", does the SQLi attack still work?

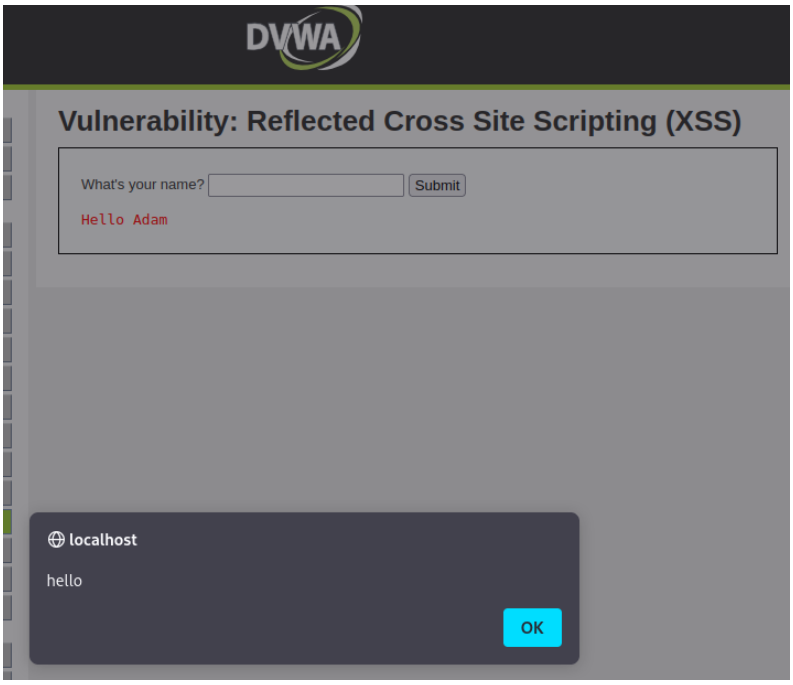
The exploit does not work when the security level is medium. In this mode, the user cannot type any input string, they can only select the user id. However, since the program lists all user IDs, an attacker can simply click through all IDs and obtain the same information.



Describe the reflected XSS attack you used. How did it work?

In the input I typed the following string: **Adam<script>alert("hello");</script>**

The program prints my name, but it also executes the code in the script tags, so an alert pops up on the browser. This exploit allows an attacker to inject and run any JavaScript.



If you switch the security level in DVWA to “Medium”, does the XSS attack still work?

This exploit does not work when the security level is set to “Medium.” It looks like the script tags are stripped and the text within the script tags is treated as simple text instead of JavaScript.