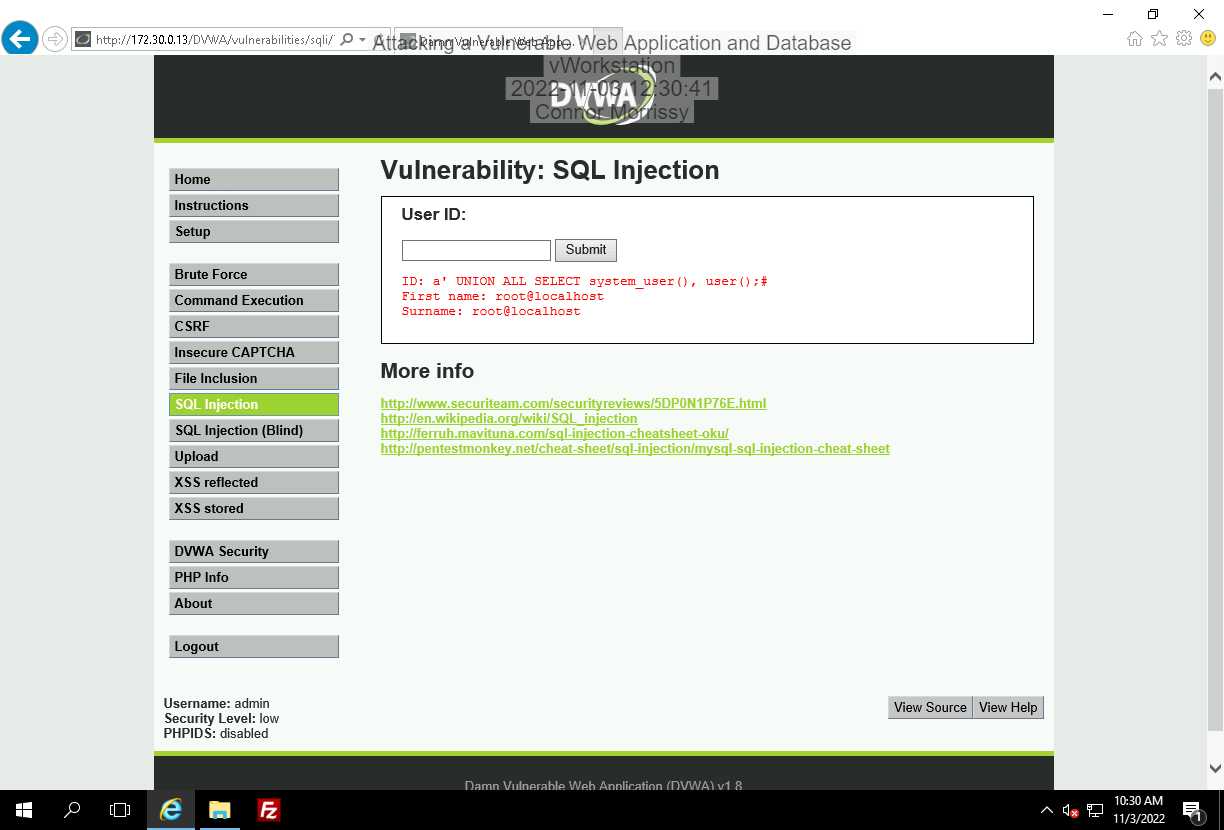
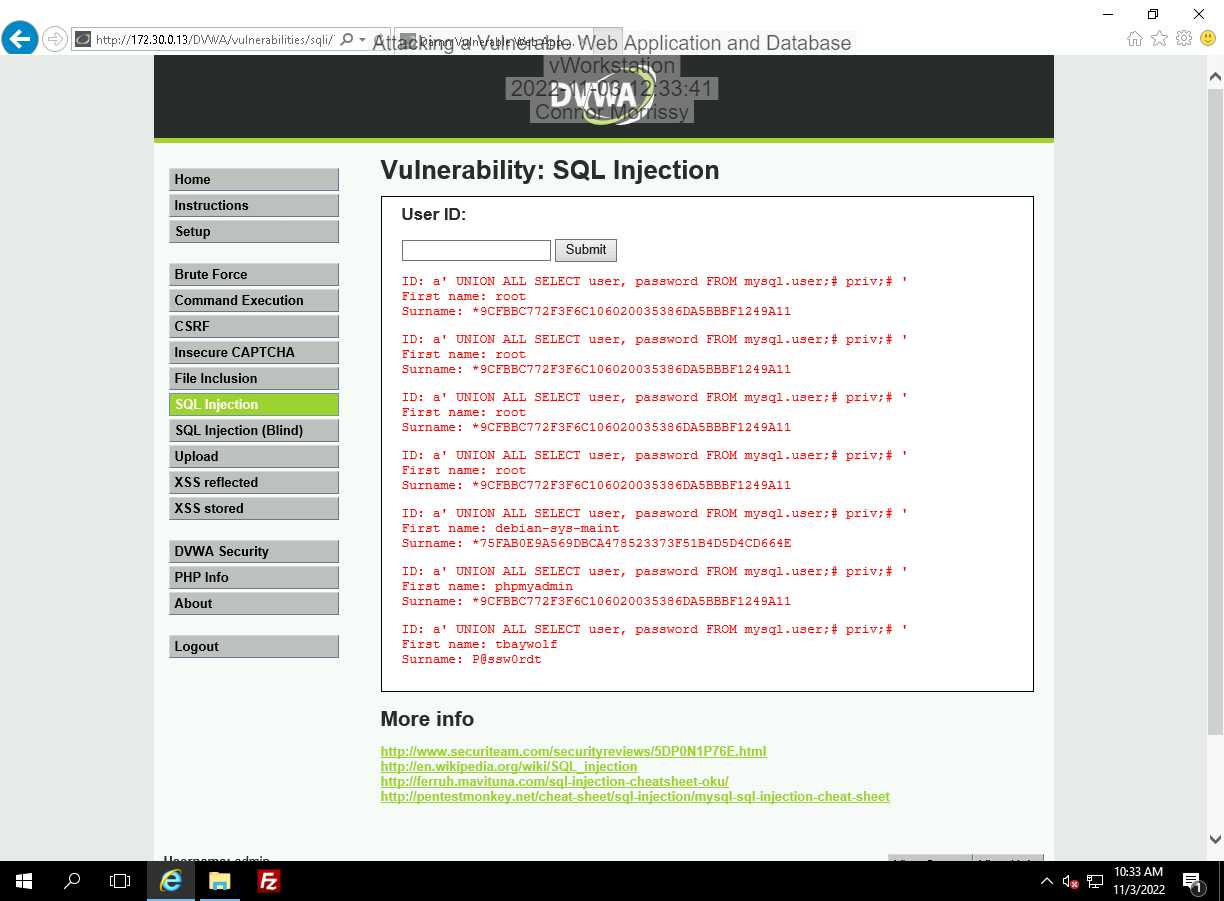


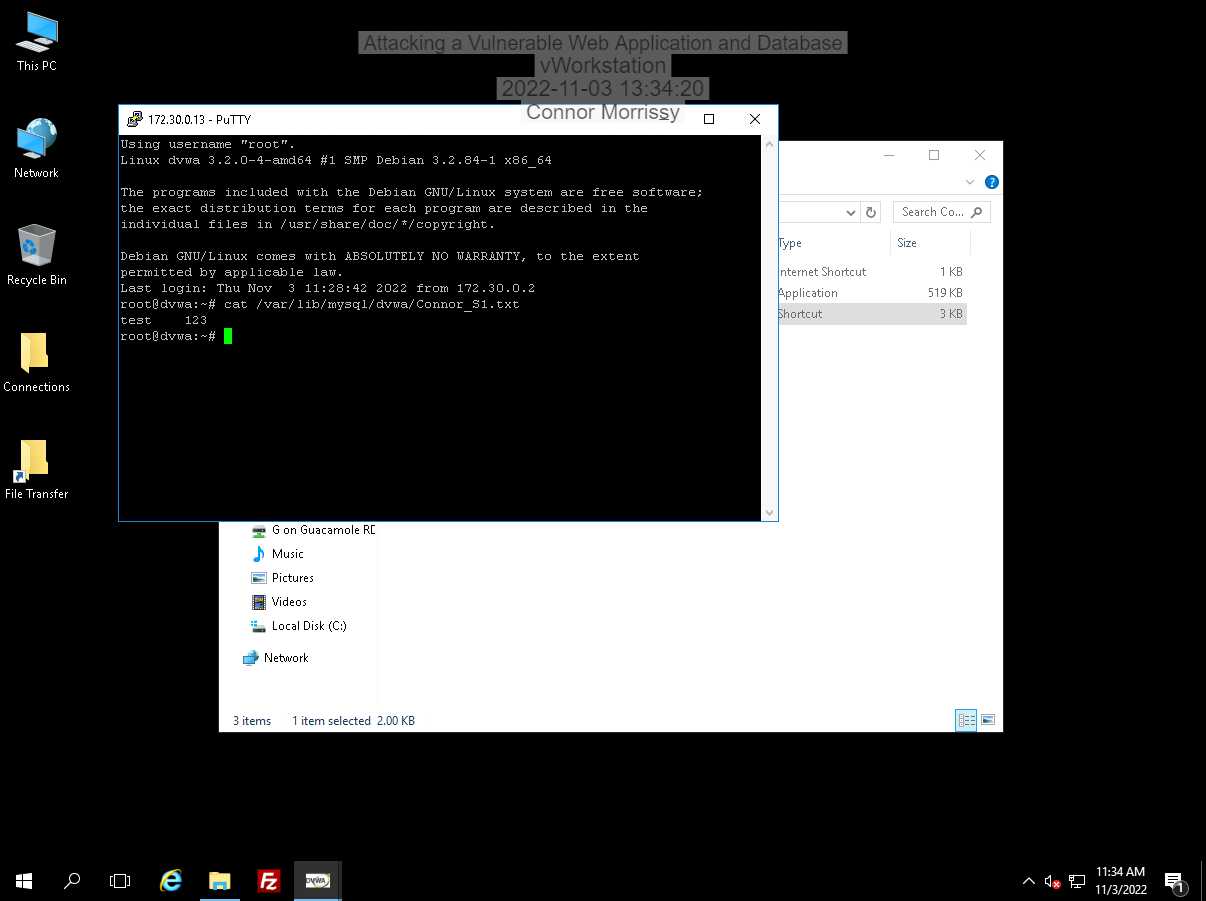
After changing the security to high, the form will no longer run scripts. Instead, it outputs the script as if it is normal text.

The results from steps 7-9 in Section 1 Part 1 told me how many columns there are in the SQL database. After entering “a’ ORDER BY 3;#”, it returned an error, telling me there are not 3 columns, only 2.



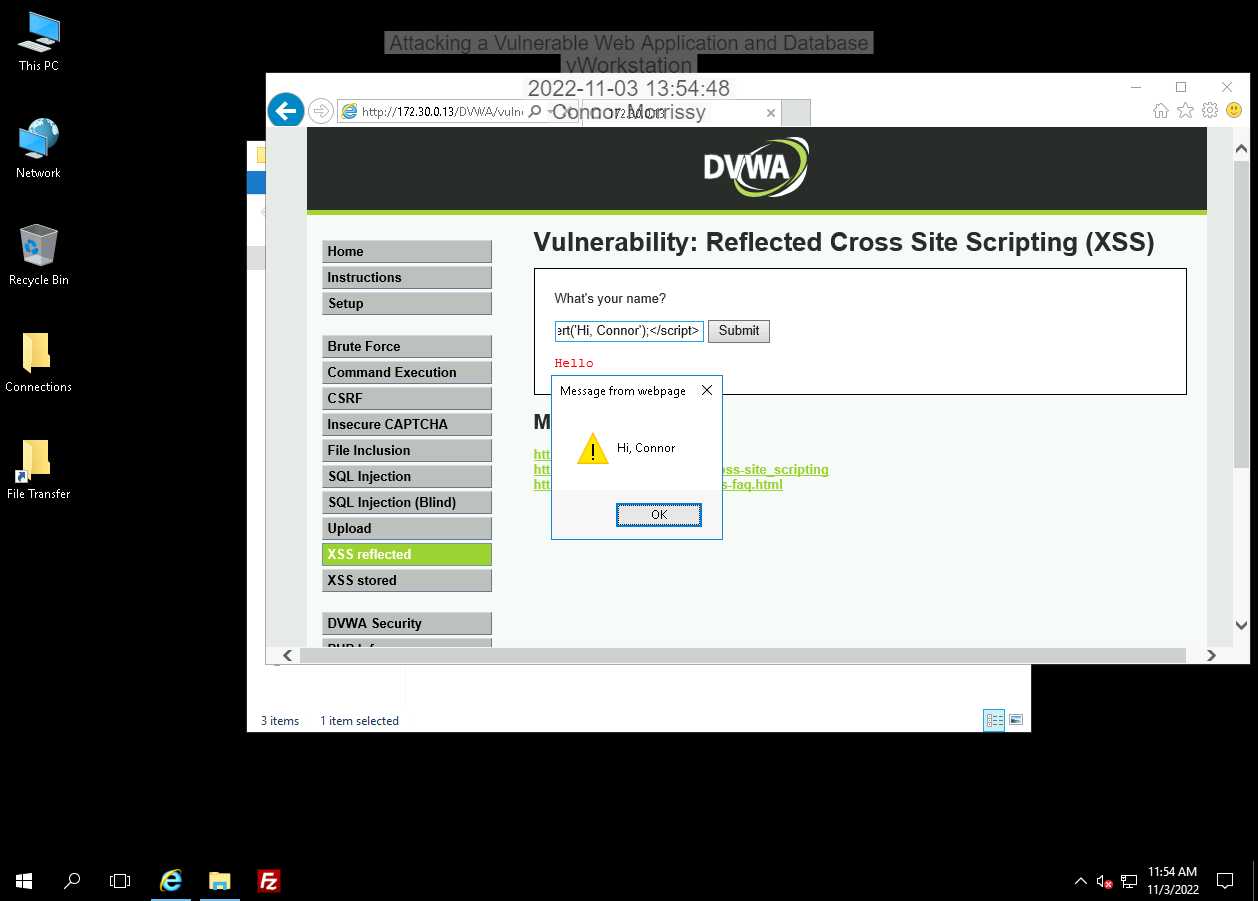


Hashing can be used for encryption to store a password as a hash instead of plaintext. Hashing is also commonly used in databases for indexing and retrieval purposes. The hash key can be used to find a value.



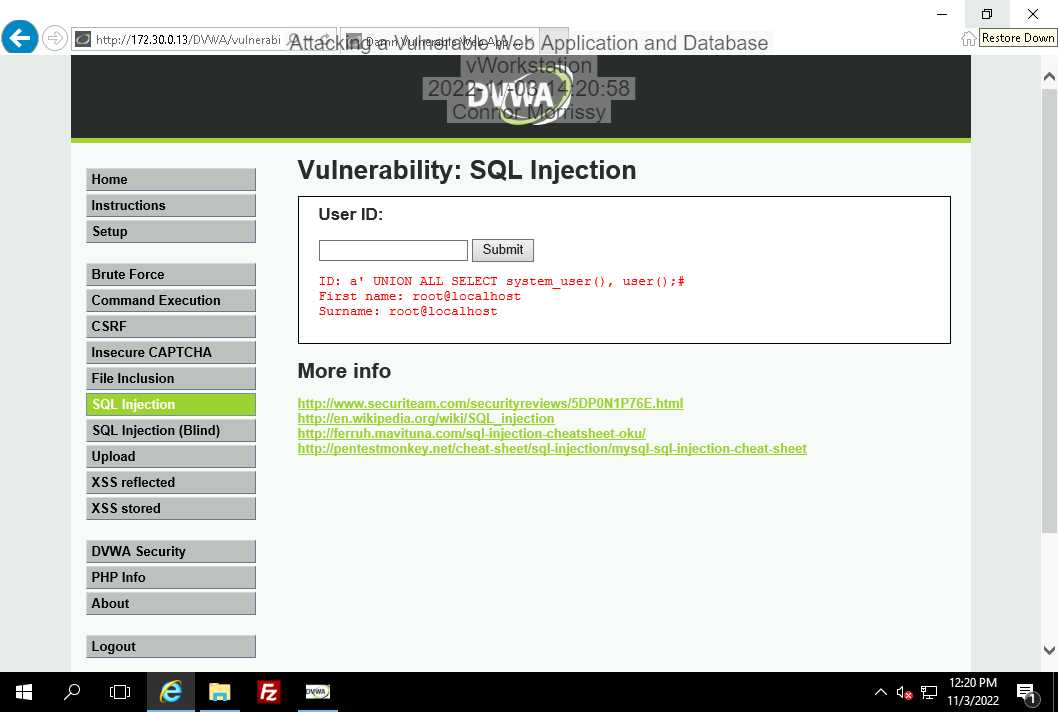
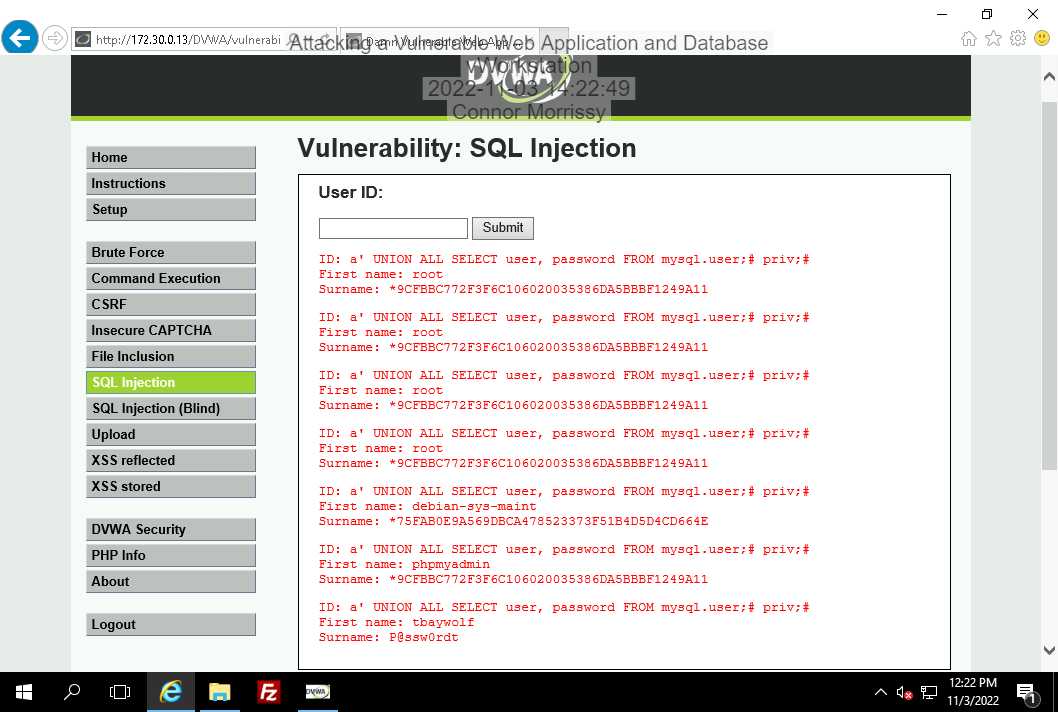
In order to protect from SQL injections like this, countermeasures should be put in place in website’s code to stop them. For example, preventing forms from allowing script characters such as ‘<’ and ‘>’ as input, or being able to handle apostrophes as input would protect from SQL code injection.

**Section 2**

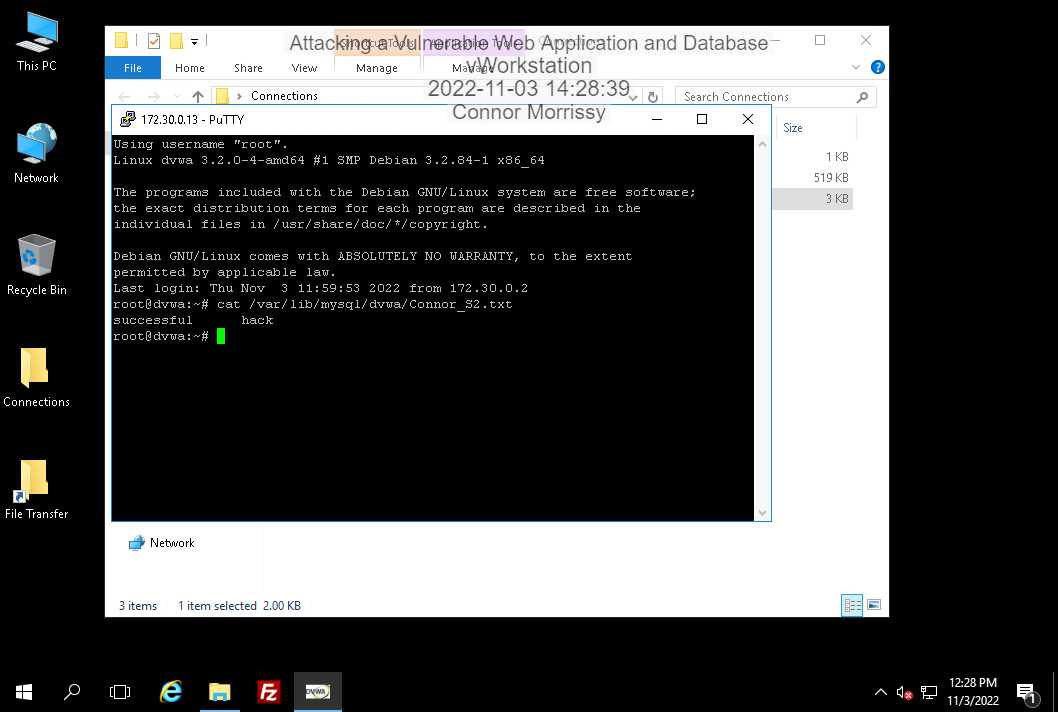


Again, after changing the security to high, the form will no longer run scripts. Instead, it outputs the script as if it is normal text.

In steps 4-6, I determined there are two columns. When I checked for a third column, I received an error message, meaning there isn’t a third column.



Hashing can be used for encryption to store a password as a hash instead of plaintext. Hashing is also commonly used in databases for indexing and retrieval purposes. The hash key can be used to find a value.



In order to protect from SQL injections like this, countermeasures should be put in place in website’s code to stop them. For example, preventing forms from allowing script characters such as ‘<’ and ‘>’ as input, or being able to handle apostrophes as input would protect from SQL code injection.

**Section 3**

**Part 1:**

A UNION-based SQL injection attack is an attack against a vulnerable web application where the attacker can extract information from other tables in the database by using the UNION keyword, which allows additional queries to be made in the command. This is useful for getting valuable information stored in any table on the vulnerable database.

**Part 2:**

1. It processed the input as plaintext.
2. The command worked and the group file was displayed.
3. The script worked and the alert was shown.

**Part 3:**

First attempt: a’ OR surname IS NULL;# -- This gave an error. This is not the name of the column.  
Second attempt: a’ OR lastname IS NULL;# -- This also gave an error and is not the name of the column.  
Third attempt: a’ OR last\_name IS NULL;# -- This gave no errors or output, indicating that this IS the name of the column.