Michael Young (myoung10)

Ethical Hacking

**Briefly describe in a few sentences for each method, the top 3 changes that would help the security of the login page.**1. **Prepared Queries** – This guarantees that the username and password are treated as their respective types (text) rather than string concatenation in creating the query. The query is separated from the injected data. Similar to a sprintf(“%s”, data) command. This is likely the most desirable prevention.

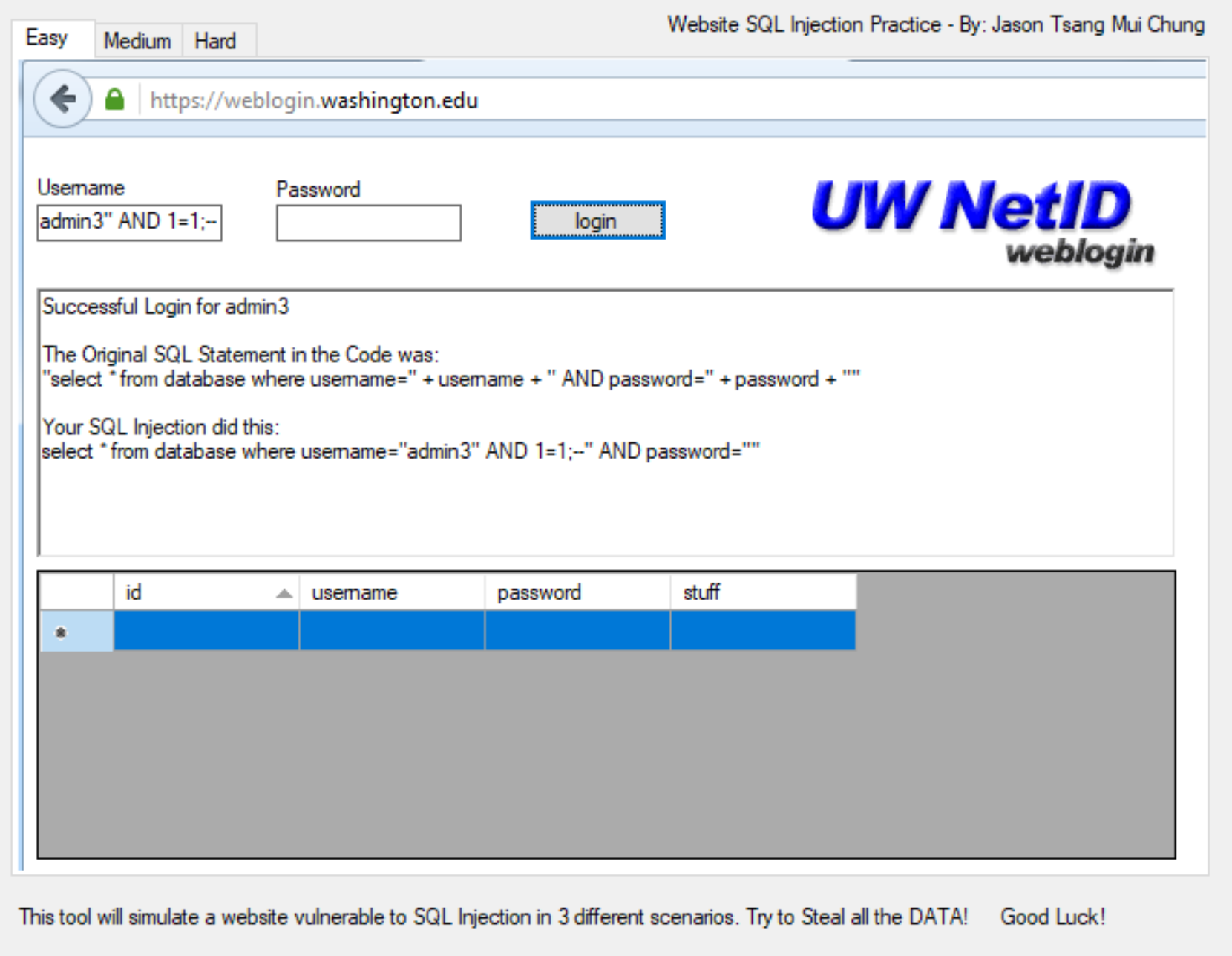
2. **Parsing/sanitizing input** – Making sure special/interpretable characters by MySQL are used. I.E. in certain languages they have functions like: sqlite\_escape\_string() to pass the input into prior to injecting it into the query.

3. **Whitelisting certain characters** – For example, doing RegEx on the username and password and only allowing alphanumeric characters prior to building the query with the potentially malicious input.

4. **Not passing user data into queries** – *In case 2 and 3 are too similar*, another way (potentially inefficient) is to make the query select ALL users, and then have a programmatic loop iterate over all the users (array) until it finds the correct user and the password matches. That way the user’s malicious input wouldn’t be part of the SQL query but instead a part of a programmatic expression.

# Easy

**User Access**

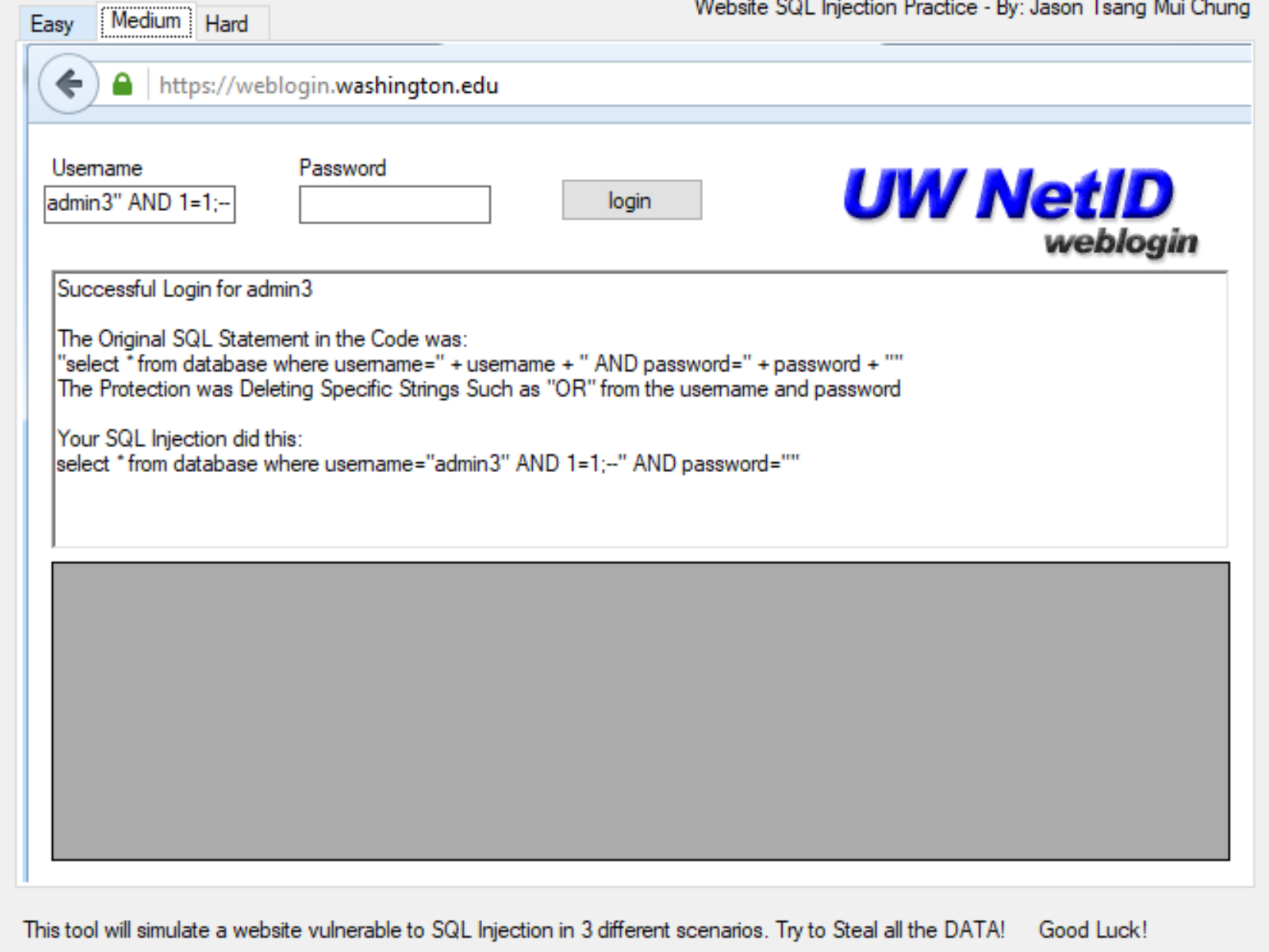


**Data Dump**

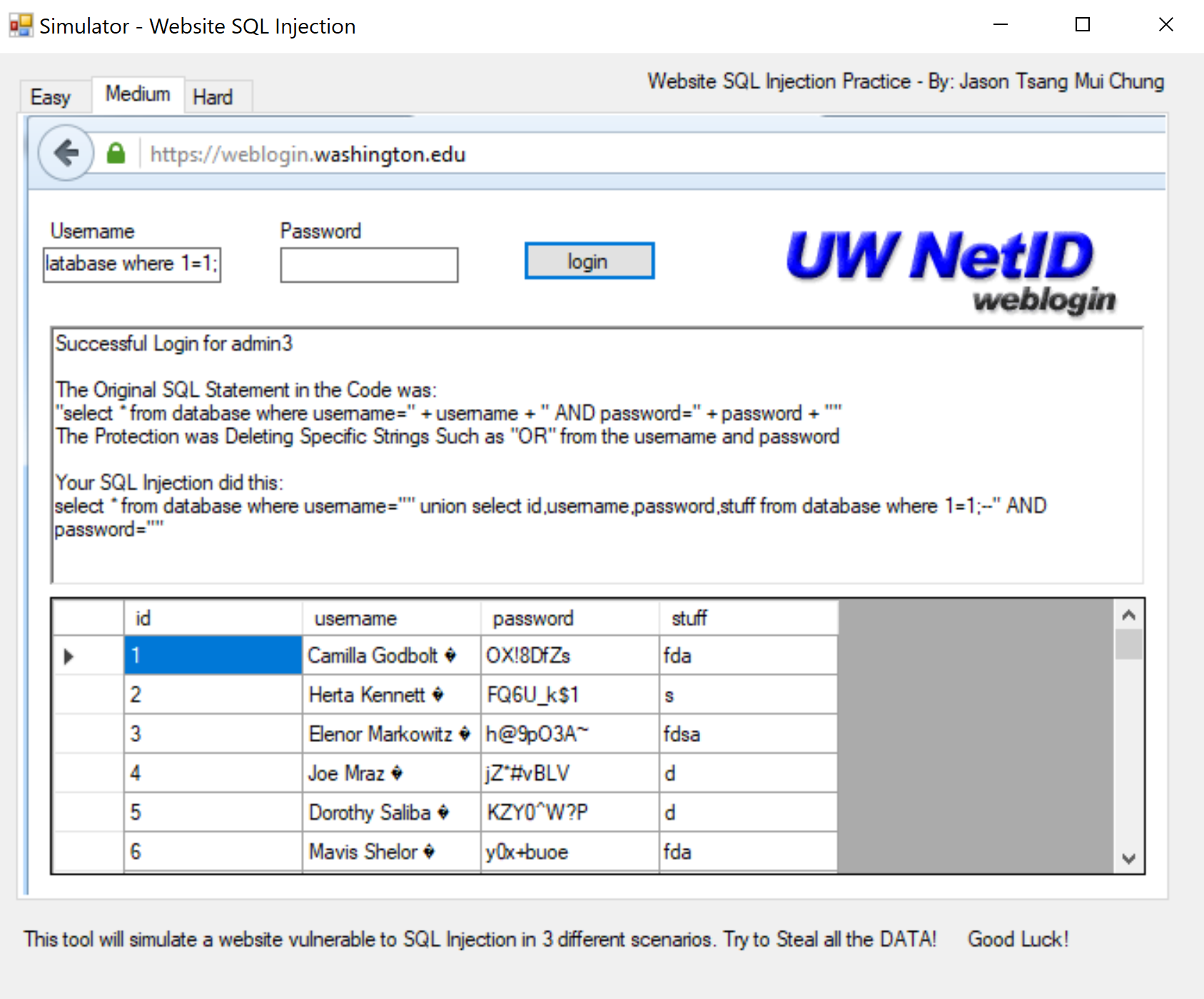
Could not retrieve the data.

# Medium

**User Access**

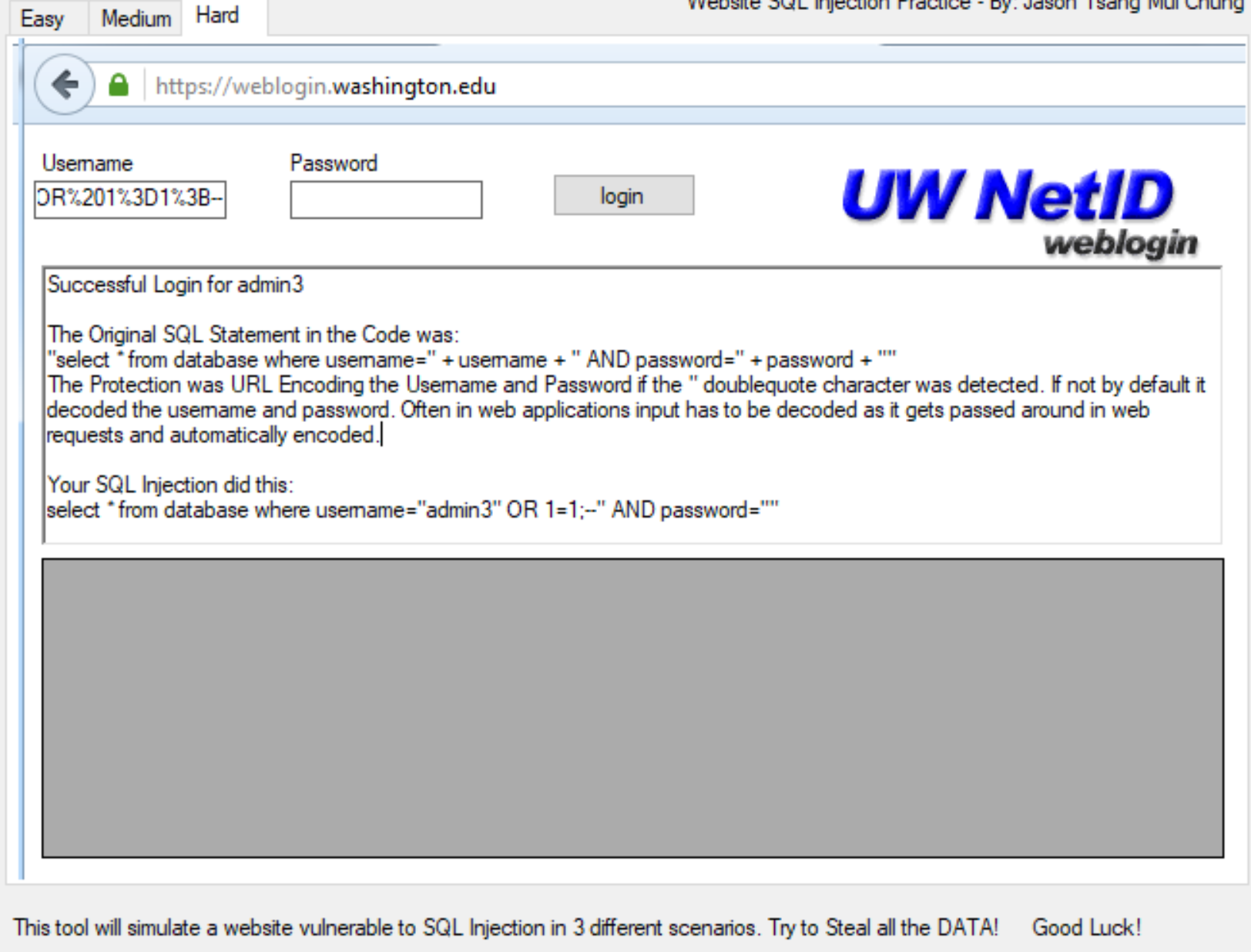


**Data Dump**



# Hard

**User Access**



**Data Dump**

Could not retrieve.