CEN4088.01 Lab 5 Due 10/24/19

Brandon Thompson 5517

October 30, 2019

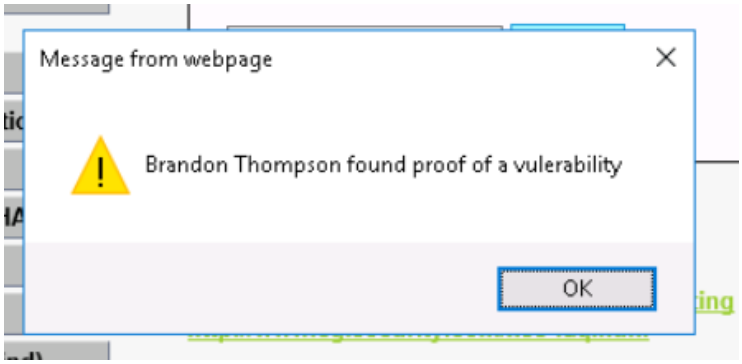

Figure 1: Part 1: Exposed XSS vulnerability. DVWA security set to low.

When the DVWA security is set to high the text box takes whatever input it is given and converts it to a string so that special characters do not conflict with the code of the text output.

SQL injection attack, input `a' ORDER BY 1;#` in the User ID field. Outputs a single first name and surname pair. When `a' ORDER BY 2;#` is passed to the input, outputs a single first name and surname pair. When `a' ORDER BY 3;#` is passed result is an error message: "Unknown column '3' in 'order caluse'." This shows that there are 2 columns in the database.

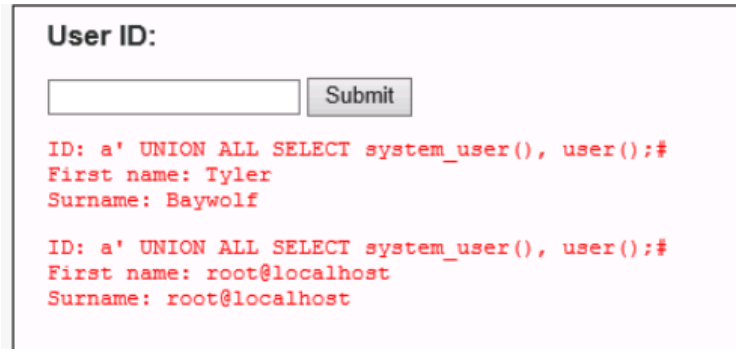

Figure 2: Part 1: User account information.

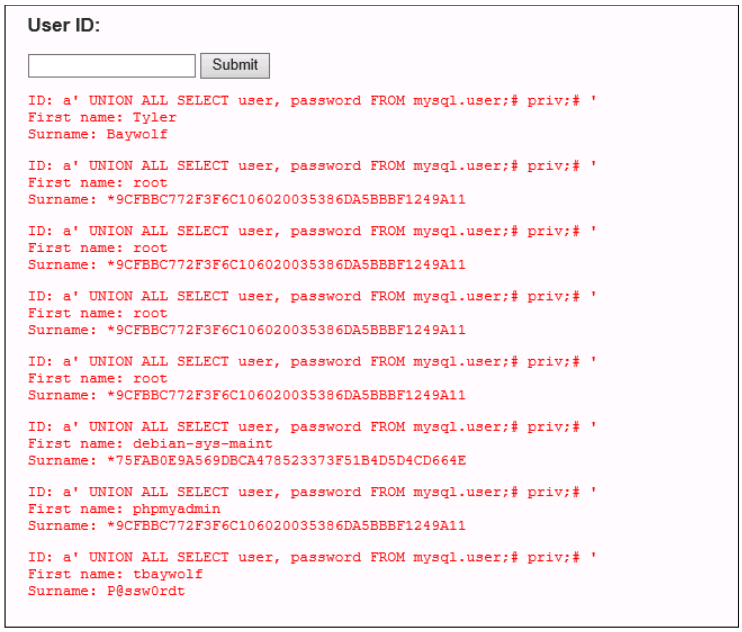

Figure 3: Part 1: Database hash information

Hashing generates a key related to the item being hashed. This key is shorter than the original value and thus makes it easier to find items based on their hashed key.

Figure 4: Contents of `brandon_thompson_S1.txt`

Sanitizing the inputs so that no special characters can be used will remove the vulnerability of the system by not allowing the user to input malicious code. If the system is compromised, not allowing file write/execute permissions will not allow users to create documents or execute scripts.

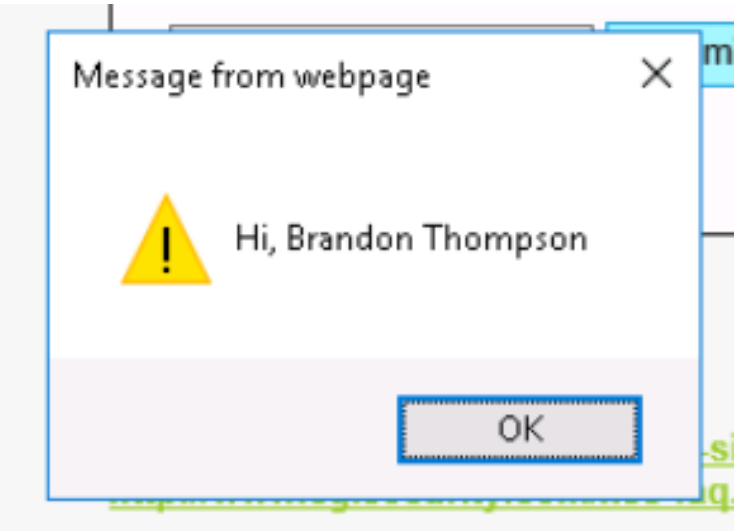

Figure 5: Part 2: Exposed XSS vulnerability. DVWA security set to low.

Question 2.2.9 answered in part 1.

Question 2.3.7 answered in part 1.

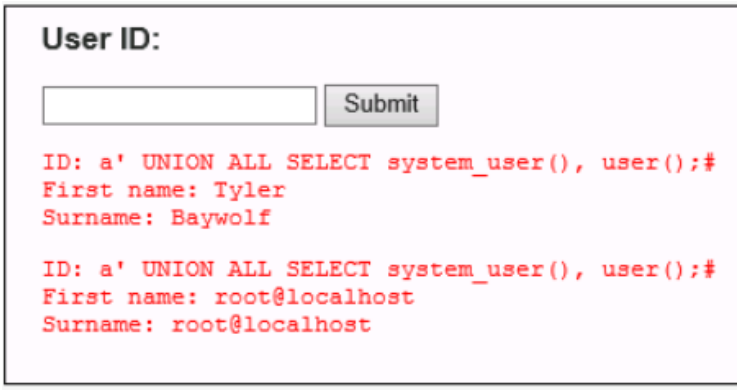

Figure 6: Part 2: User information from SQL injection.

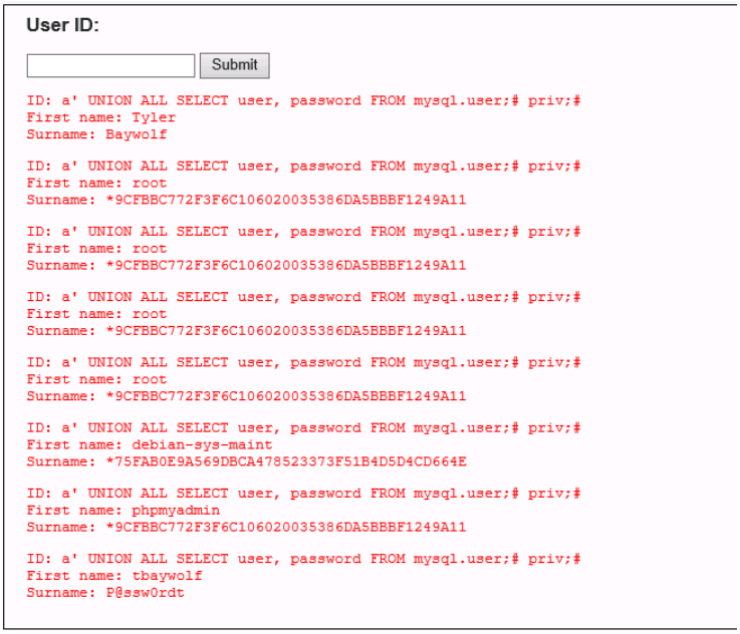

Figure 7: Part 2: Database hash information from SQL injection.

Question 2.3.19 answered in part 1.

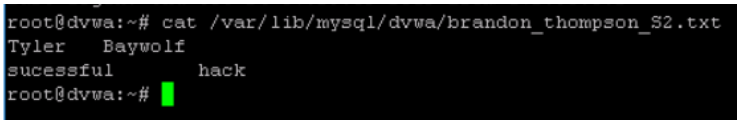

Figure 8: Contents of `brandon_thompson_S2.txt`

Question 2.4.5 answered in part 1.