Name: Caroline Wanjiku Macharia

Student ID: 669919

Lab4bInstructor: Professor Dennis Kaburu

Assignment: Lab 17.2.6 - Attacking mySQL Database

Title: Advanced Information System Security

Course: ISC6120

Due: Summer 2025

Part 1: Open Wireshark and load the PCAP file.

The Wireshark application can be opened using a variety of methods on a Linux workstation.

a. Start the CyberOps Workstation VM.

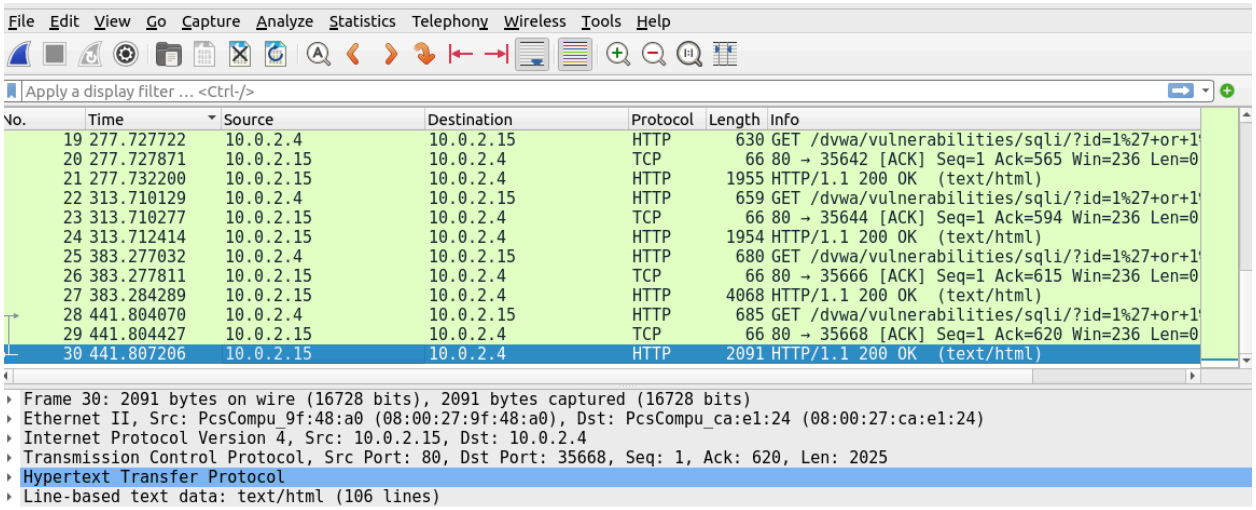
b. Click Applications > CyberOPS > Wireshark on the desktop and browse to the Wireshark application.

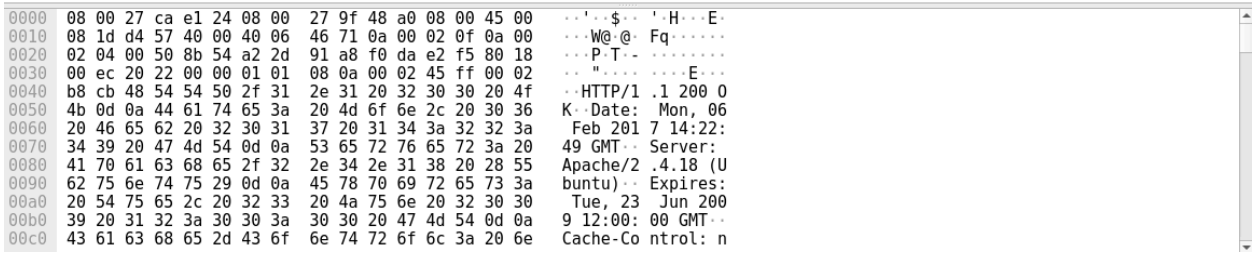
c. In the Wireshark application, click Open in the middle of the application under Files.

d. Browse through the /home/analyst/ directory and search for lab.support.files.

In the lab.support.files directory and open the SQL_Lab.pcap file.

e. The PCAP file opens within Wireshark and displays the captured network traffic. This capture file extends over an 8-minute (441 second) period, the duration of this SQL injection attack.



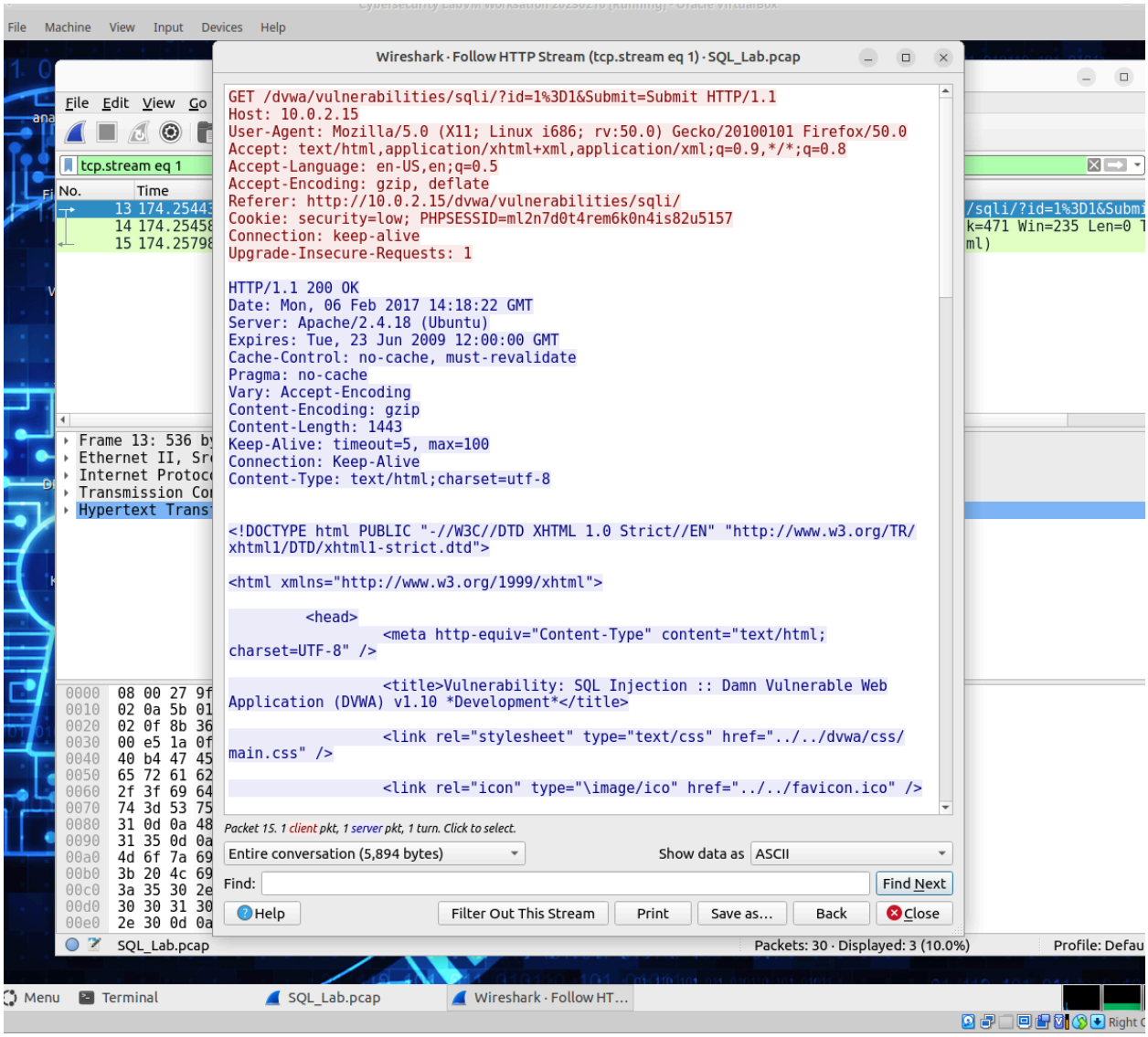


IP involved 10.0.2.15 & 10.0.2.4

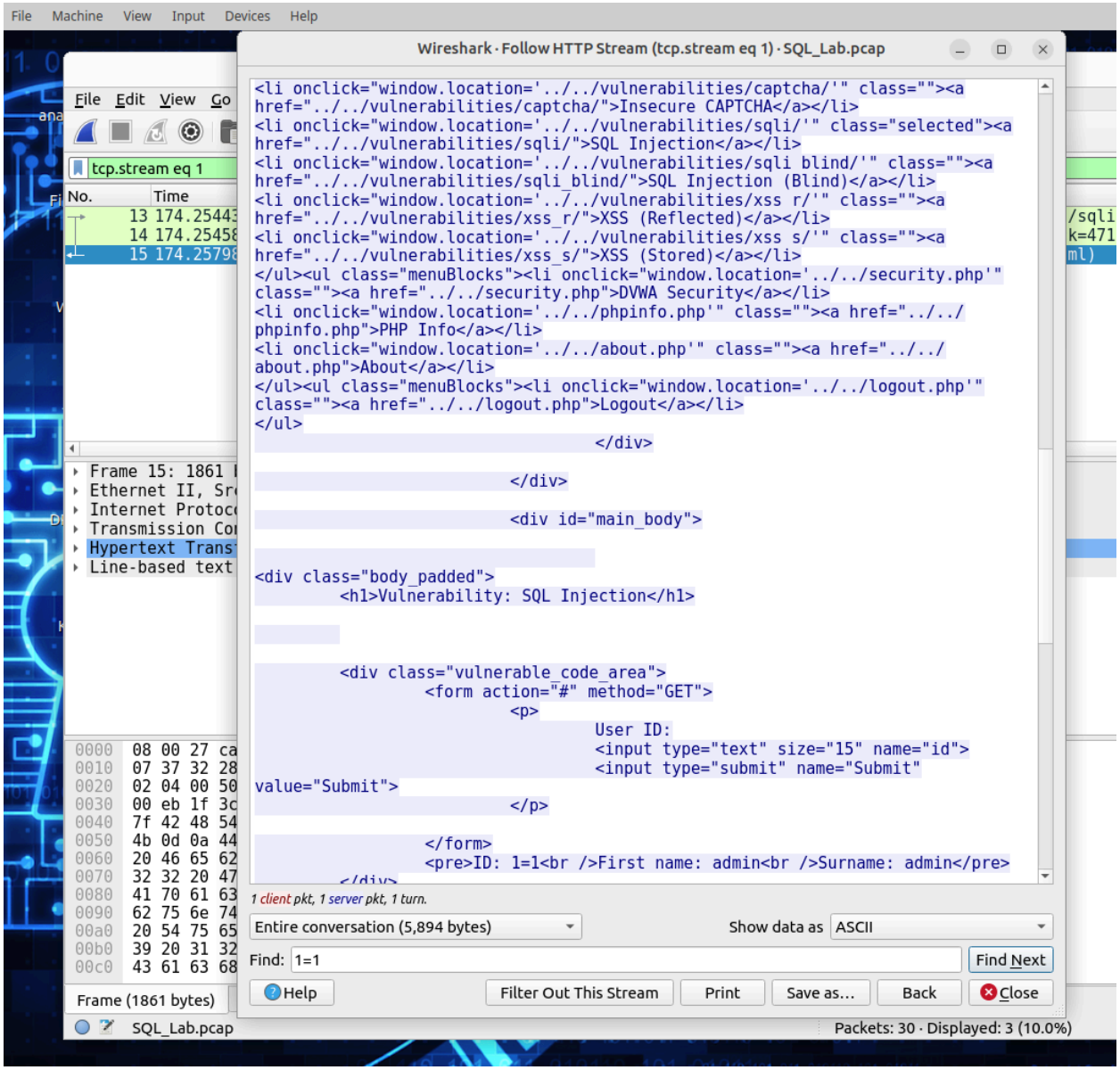
Part 2: View the SQL Injection Attack.

In this step, you will be viewing the beginning of an attack.

a. Within the Wireshark capture, right-click line 13 and select Follow > HTTP Stream. Line 13 was chosen because it is a GET HTTP request. This will be very helpful in following the data stream as the application layers sees it and leads up to the query testing for the SQL injection.



The attacker has entered a query (1=1) into a UserID search box on the target 10.0.2.15 to see if the application is vulnerable to SQL injection. Instead of the application responding with a login failure message, it responded with a record from a database. The attacker has verified they can input an SQL command and the database will respond. The search string 1=1 creates an SQL statement that will be always true. In the example, it does not matter what is entered into the field, it will always be true.



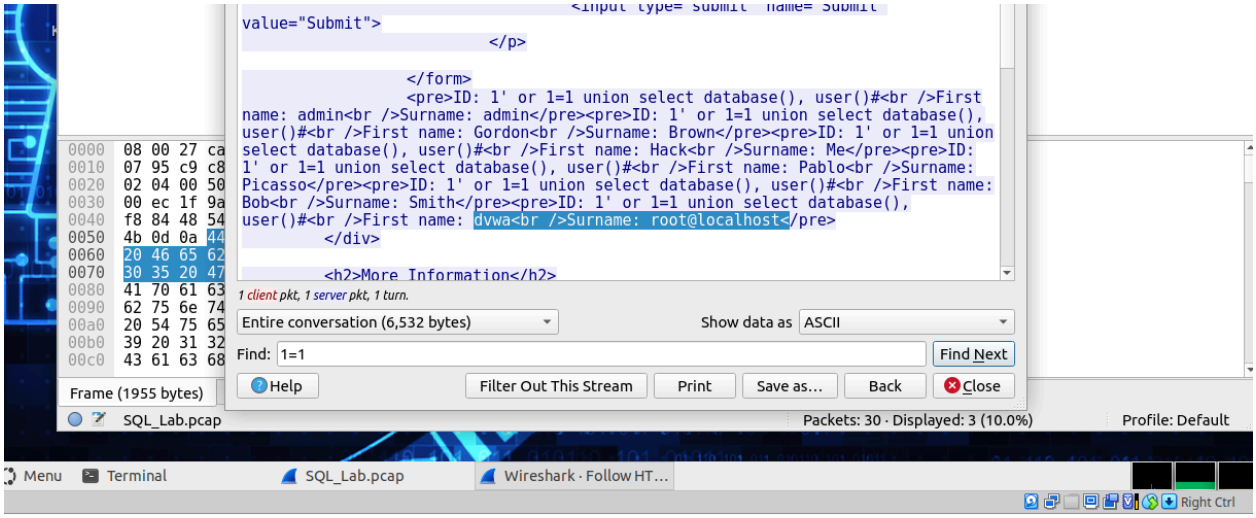
Part 3: The SQL Injection Attack continues...

In this step, you will be viewing the continuation of an attack.

a. Within the Wireshark capture, right-click line 19, and click Follow > HTTP Stream.

b. In the Find field, enter 1=1. Click Find Next.

c. The attacker has entered a query (1' or 1=1 union select database(), user()#) into a UserID search box on the target 10.0.2.15. Instead of the application responding with a login failure message, it responded with the following information:



The database name is dvwa and the database user is root@localhost. There are also multiple user accounts being displayed.

d. Close the Follow HTTP Stream window.

e. Click the Clear display filter to display the entire Wireshark conversation.

Part 4: The SQL Injection Attack provides system information.

The attacker continues and starts targeting more specific information.

a. Within the Wireshark capture, right-click line 22 and select Follow > HTTP Stream. In red, the source traffic is shown and is sending the GET request to host 10.0.2.15. In blue, the destination device is responding back to the source. Lab - Attacking a mySQL Database © 2018 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public Page 5 of 7 www.netacad.com

b. In the Find field, enter 1=1. Click Find Next.

c. The attacker has entered a query (1’ or 1=1 union select null, version ()#) into a UserID search box on the target 10.0.2.15 to locate the version identifier. Notice how the version identifier is at the end of the output right before the . closing HTML code.

What is the version? 5.7.12-0ubuntu1.1

d. Close the Follow HTTP Stream window.

e. Click Clear display filter to display the entire Wireshark conversation.

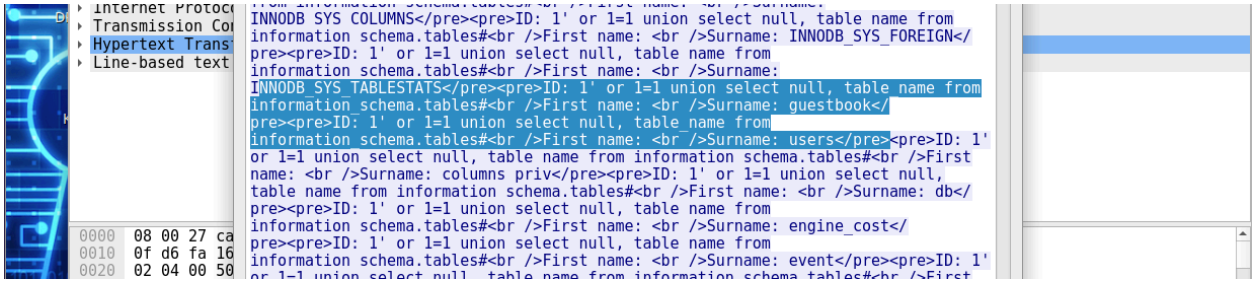
Part 5: The SQL Injection Attack and Table Information.

The attacker knows that there is a large number of SQL tables that are full of information. The attacker attempts to find them.

a. Within the Wireshark capture, right-click on line 25 and select Follow > HTTP Stream. The source is shown in red. It has sent a GET request to host 10.0.2.15. In blue, the destination device is responding back to the source.

b. In the Find field, enter users. Click Find Next.

c. The attacker has entered a query (1'or 1=1 union select null, table_name from information_schema.tables#) into a UserID search box on the target 10.0.2.15 to view all the tables in the database. This provides a huge output of many tables, as the attacker specified "null" without any further specifications.



What would the modified command of (1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users') do for the attacker?

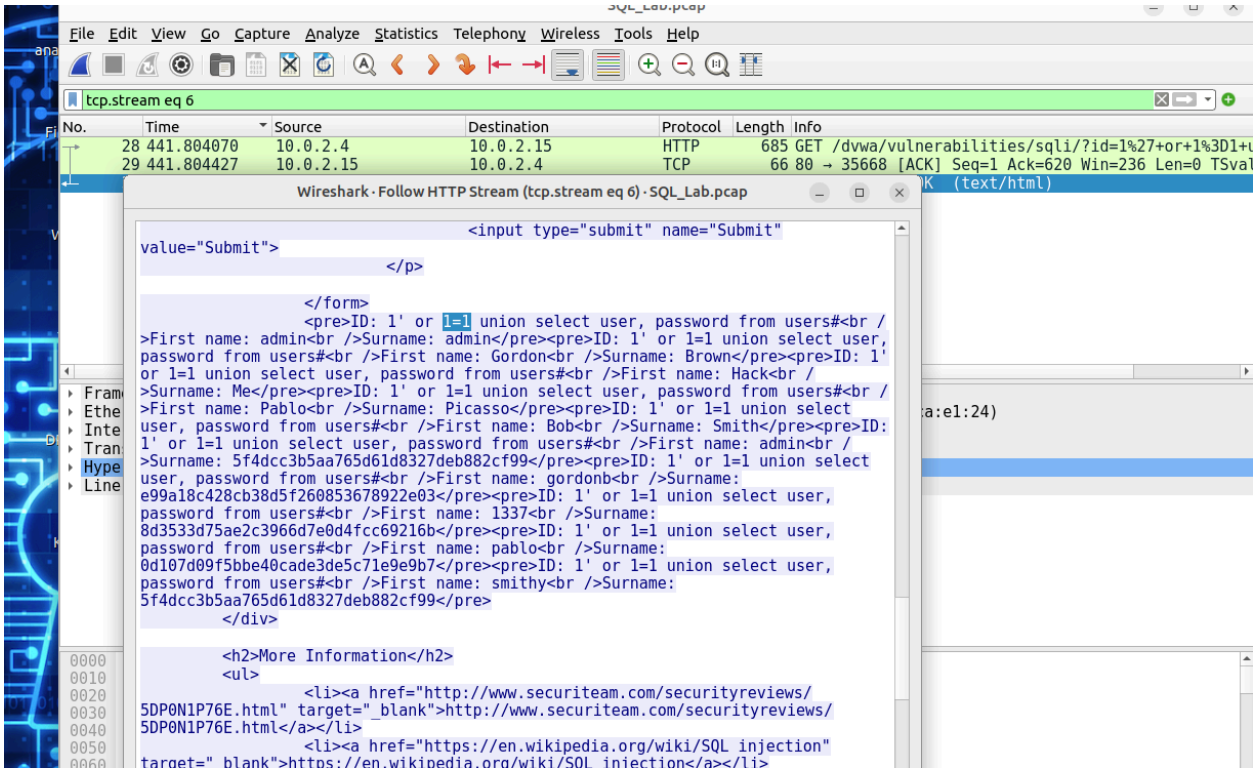
Type your answers here. **View all the tables in the database**

d. Close the Follow HTTP Stream window. e. Click Clear display filter to display the entire Wireshark conversation.

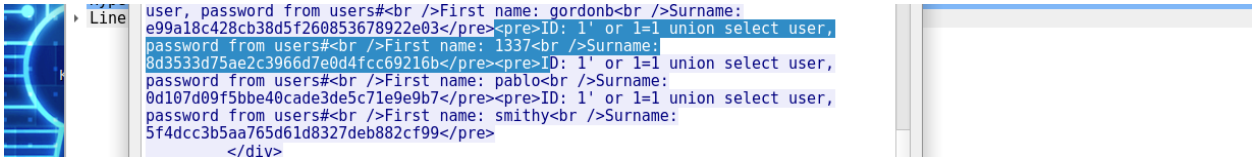
Part 6: The SQL Injection Attack Concludes.
The attack ends with the best prize of all; password hashes.

a. Within the Wireshark capture, right-click line 28 and select Follow > HTTP Stream. The source is shown in red. It has sent a GET request to host 10.0.2.15. In blue, the destination device is responding back to the source.

b. Click Find and type in 1=1. Search for this entry. When the text is located, click Cancel in the Find text search box.



Which user has the password hash of 8d3533d75ae2c3966d7e0d4fcc69216b?



User 1337

c. Using a website such as https://crackstation.net/, copy the password hash into the password hash cracker and get cracking.

Question: What is the plain-text password? `charley`

d. Close the Follow HTTP Stream window. Close any open windows.

Reflection Questions

1. What is the risk of having platforms use the SQL langauge?

Data theft, data corruption and complete hostile takeover

- **Data Theft:** Bypassing authentication to view and steal all data, including user credentials, personal information, and company secrets.
- **Data Corruption:** Modifying or deleting critical data, destroying the integrity of the application.
- **Complete Hostile Takeover:** Gaining administrative control over the database server, which can be used to pivot and attack the entire network.

2. Browse the internet and perform a search on “prevent SQL injection attacks”. What are 2 methods or steps that can be taken to prevent SQL injection attacks?

1. Use Prepared Statements (Parameterized Queries)

This is the most effective method. It separates the SQL command from the user data, so the database treats the input strictly as data and never as executable code. The attack is neutralized at its source.

2. Enforce Strict Input Validation

Define rules for what is acceptable input (e.g., must be a number, specific length, no special characters). Reject any input that does not conform to these rules before it is ever used in a query.