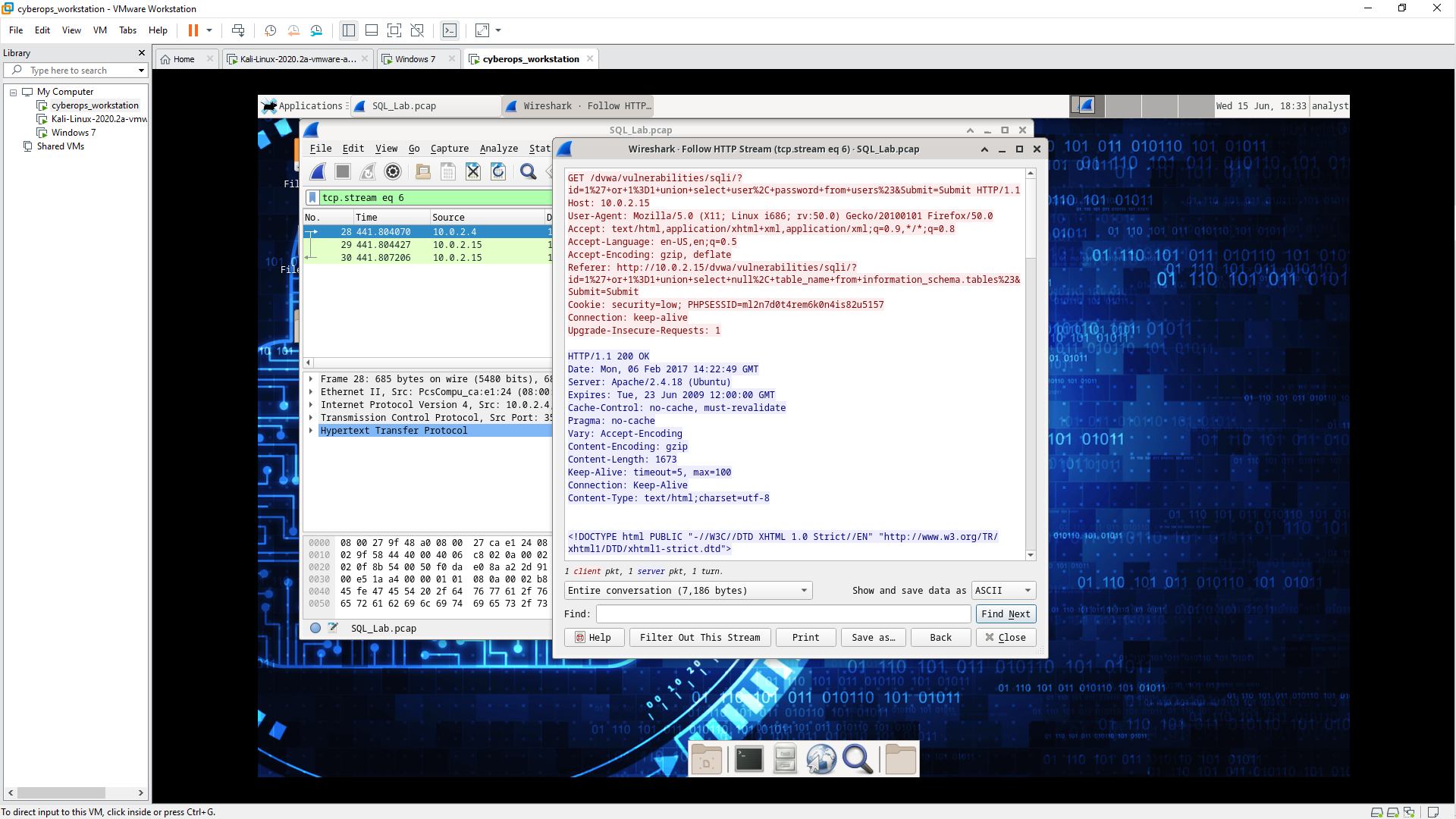
**Lab - Attacking a mySQL Database**

Part 6: The SQL Injection Attack Concludes.

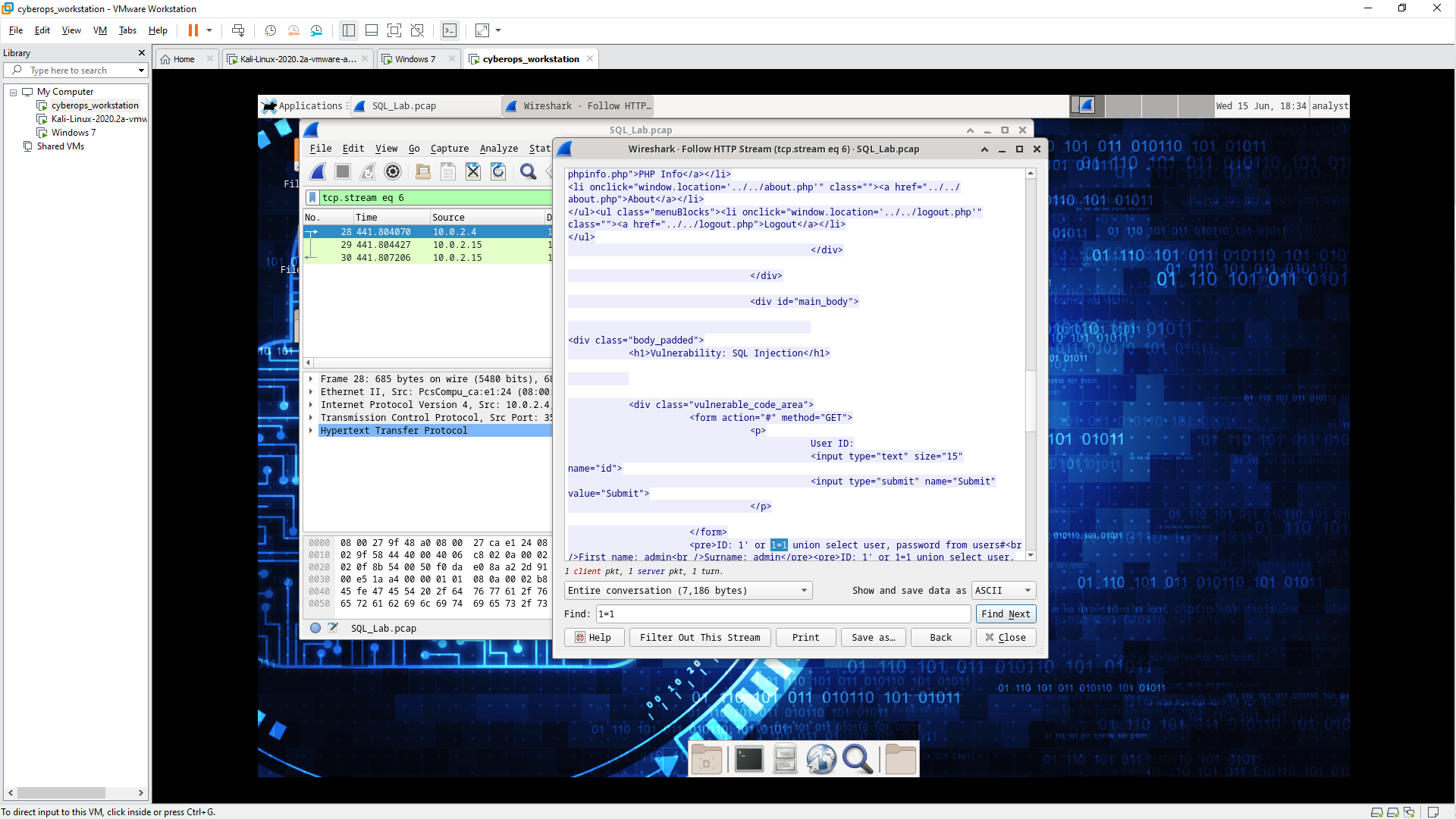
The attack ends with the best prize of all; password hashes.

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. The attacker has entered a query (1’or 1=1 union select user, password from users#) into a UserID search box on the target 10.0.2.15 to pull usernames and password hashes!

Which user has the password hash of 8d3533d75ae2c3966d7e0d4fcc69216b?



1337

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

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?

Web sites are commonly database driven and use the SQL language. The severity of a SQL injection attack is up to the attacker.

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?

- Input validation and parametrized queries including prepared statements

- Raise Virtual Or Physical Firewalls