**CMSC 491/791 Active Cyber Defense HW 7**

**Name:**

**Due: Nov 6th, 2019 at 7:00pm**

Summary:

In this assignment you are given a vulnerable website called Bates Motel. You will use concepts such as SQL injection and command injection to complete this assignment. You will need to complete each question before moving on to the next.

1. Use the “Register” page to register an account on Bates Motel. What is the registration code? How did you find this information? (10 pts)

1. The lookup.php script runs the following MySQL query when a username is queried:

SELECT \* FROM users WHERE username='$user'

It prints the following fields from the SQL query results:

echo "Username: " . $row['username'] . "<br />Real Name: " . $row['name'] . "<br />About me: " . $row['about'];

Perform SQL injection on the Username input field of the “Lookup a User” page to list all of the users registered in the Bates Motel. What is the name of the user with administrator status? What was your SQL injection? (15 pts)
2. The login.php script runs the following MySQL query when a user enters a username and password:

SELECT \* FROM users WHERE username='$user' AND password='$pass'

Perform SQL injection on the Username input field of the “Login” page to log in as the administrator. What is the secret note on the “Admin panel” page? What was your SQL injection? (20 pts)
3. Exploit a vulnerability in the Admin panel’s network connectivity tool to retrieve the flag stored in a .txt file on the webserver. What is the flag? What input did you provide to the network connectivity tool? (15 pts)
4. Perform SQL injection on the Username input field of the “Lookup a User” page to find the encrypted password of the administrator. What is that user’s encrypted password? What was your SQL injection? (20 pts)
5. Which .php file on the webserver contains the encrypt\_password() function? In a few sentences, describe what this function does. (10 pts)
6. What is the administrator’s plaintext password? (10 pts)