Jerry Olds

1001533643

CSE-4380-001

4/19/2020

Pre-CTF

1) Basic Mission 1
    a) The password is plainly written in the HTML source code.
    b) View page source by pressing ctrl+U. The password is displayed in the comments.

2) Basic Mission 2
    a) The password file was not uploaded, so when the script checks to see if the password is correct, it looks for the password file and does not find it, making the password **NULL**.
    b) Exploit the vulnerability by pressing the submit button, the password is **NULL.**

3) Basic Mission 3
    a) The name of the password file is visible if you right click the password field and then left click inspect
    b) Exploit the vulnerability by pasting password.php at the end of the URL and then entering the password **92309ca0** in to the password field

4) Basic Mission 4
    a) If you right click inspect on the "Send password to Sam" button, you can edit the email address the password is sent to
    b) Exploit the vulnerability by first right clicking "Send password to Sam" button. Edit the email address to your email, then hit the "Send password to Sam" button. Check your email to find the password that is sent then enter the password **b0865ef6** in to the password field.

5) Basic Mission 5
    SOLUTION IS THE SAME AS PREVIOUS MISSION ^^^^

6) Basic Mission 6
    a) We know the encrypted password and we have the encryption technique that encrypted the password. By encrypting a couple of test strings, we can maybe figure out the algorithm used to encrypt the passwords.
    b) After encrypting a few test strings, I figured out that the encryption technique that is used is string[i] = string[i] + i. It increases the ascii value of the character in the string by its position in the string. Now knowing the encryption technique, the decrypted password is **5588353b**

7) Basic Mission 7
    a) The webpage provides a field that will execute UNIX commands, so if you execute the “ls” command you will be able to see other files in the directory
    b) Enter ;ls in to the field and click view. Paste the k1kh31b1n55h.php file at the end of the URL to find the password **a00851c9**. Enter that password in to the password field and click submit.

8) Basic Mission 8
    a) This mission works similar to the previous mission, except instead of just entering the “ls” command and the webpage executing it, you use a SSI injection to execute the “ls” command
    b) First enter some text in to the “Enter your name” field. After being redirected to a new page you will be in a child directory of the desired parent directory. Go back to the original webpage and enter <!--#exec cmd=”ls ..”--> in the “Enter your name” field. Copy the au12ha39vc.php file and paste it to the end of the URL. Copy the password **f9a6282d** and paste it into the password field and click submit.

9) Realistic Mission 2
    a) The webpage has a hidden link which can be found by pressing ctrl+A. The hidden link takes you to the admin sign in page.
    b) Press ctrl+A to find the hidden link. Click the hidden link to be redirected to the admin admin log in page. Use an SQL injection attack ‘OR 1 ‘1’=’1 in the username and password fields to gain access.

10) Realistic Mission 8 part 1
    a) User Info
    b) Vulnerable to SQL injection attacks
    c) Used SQL injection attack ‘OR 1 ‘1’=’1 to display all usernames and passwords

11) Realistic Mission 8 part 2
    a) login2.php (page after successful login)
    b) Vulnerable to changing cookie information to other user’s username and password
    c) Using Firebug under the cookies tab, change your username and password to GaryWilliamHunter and -- $$$$$ -- respectively. Then enter dropCash in the account to send the money to, then enter 10000000 in the amount of money field. Click the “Move Money To A Different Account” button.

12) Realistic Mission 8 part 3
    a) login2.php (page after successful login)
    b) Files that are actually cleared can be changed by editing HTML code
    c) Right click “Clear Files in Personal Folder” button. Change the value of “<username>SQLFiles” to logFiles. Change your username and password to GaryWilliamHunter and -- $$$$$ -- respectively using Firebug. Click the “Clear Files In Personal Folder” button.