Assignment 4

Xueli Yang

008737742

1. Describe the attack you used. How did it work?

I choose CSRF attack for this homework. For the first question, I set security level at low in DVWA. I create a HTML page, show in the Figure 1,2. The page does not contain password opinion (I hidden the opinion). I could not type in the new password and confirm password.

Text

Description automatically generated

Figure 1

Graphical user interface, application, Word

Description automatically generated

Figure 2

I clicked on change password, it shows “Password Changed” even the password is “NULL”, it still shows the password changed so the security is low.

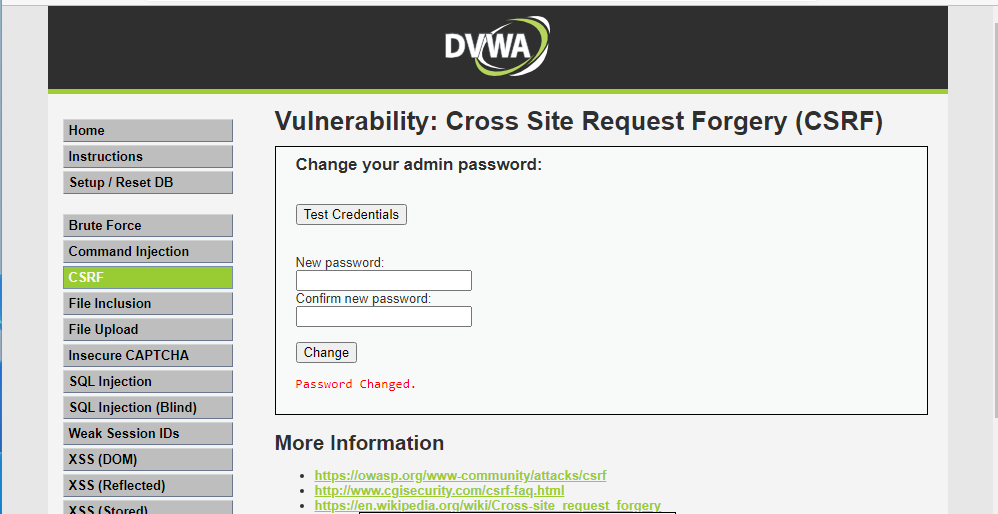


Figure 3

1. Does your attack work in “Medium” security level?

When I change the security to “Medium” and the attack does not work as below. The “Medium.php” has been added “$\_SERVER[ ‘SERVER\_NAME’]) !== false).

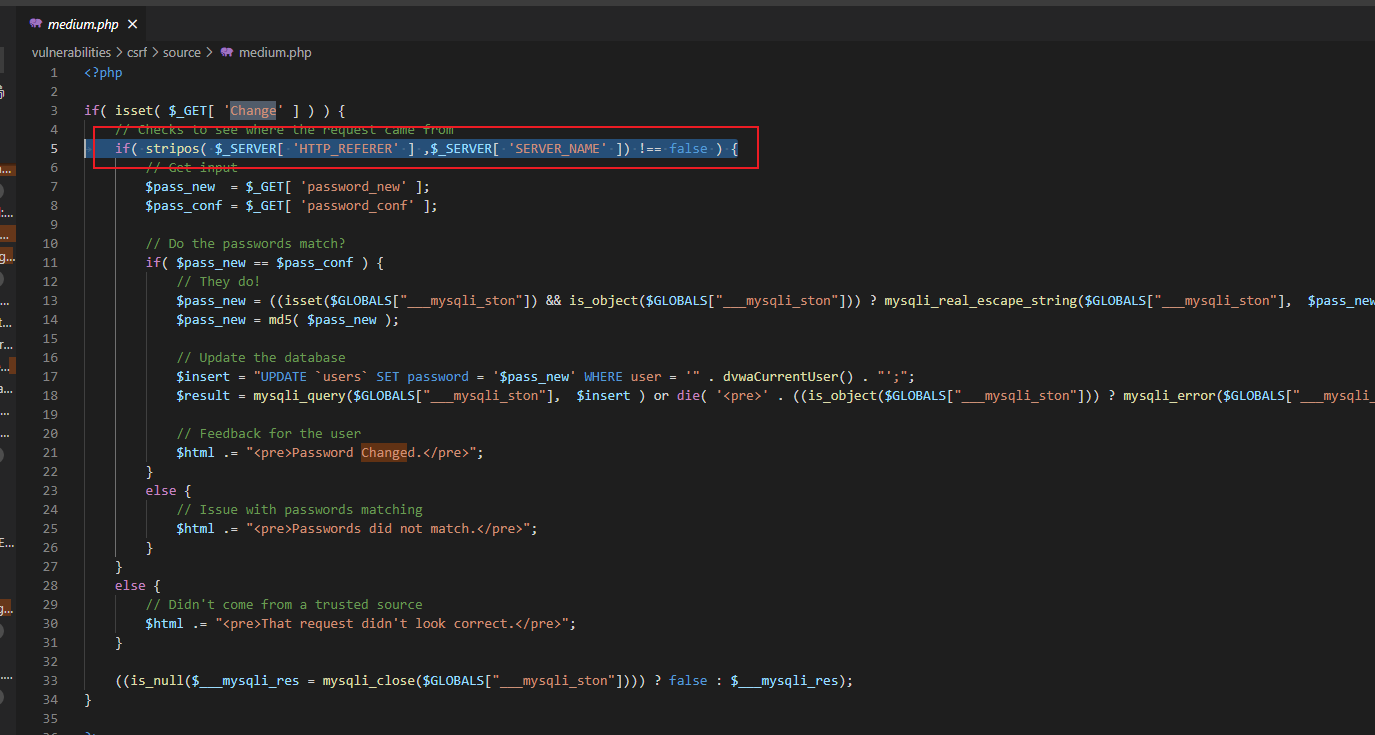


Figure 4

Figure 5 will show the attack has failed.

Graphical user interface, text, application, email

Description automatically generated

Figure 5

1. Set the security mode to “Low” and examine the code that is vulnerable, and then set the security mode to “High” and reexamine the same code. What changed? How do the changes prevent the attack from succeeding?

At higher security levels, when an attacker attempts to obtain an old password, it is evident in the code that the Session\_token set when the password was changed is verified in preference.

In the checkToken code, I can see the relevant validation for the token, and the page will be redirected if the if condition is met

Text

Description automatically generated

Figure 6

In the checkToken code, I could see the relevant validation for the token, and the page will be redirected if the “If condition” has been met.

Text

Description automatically generated

Figure 7