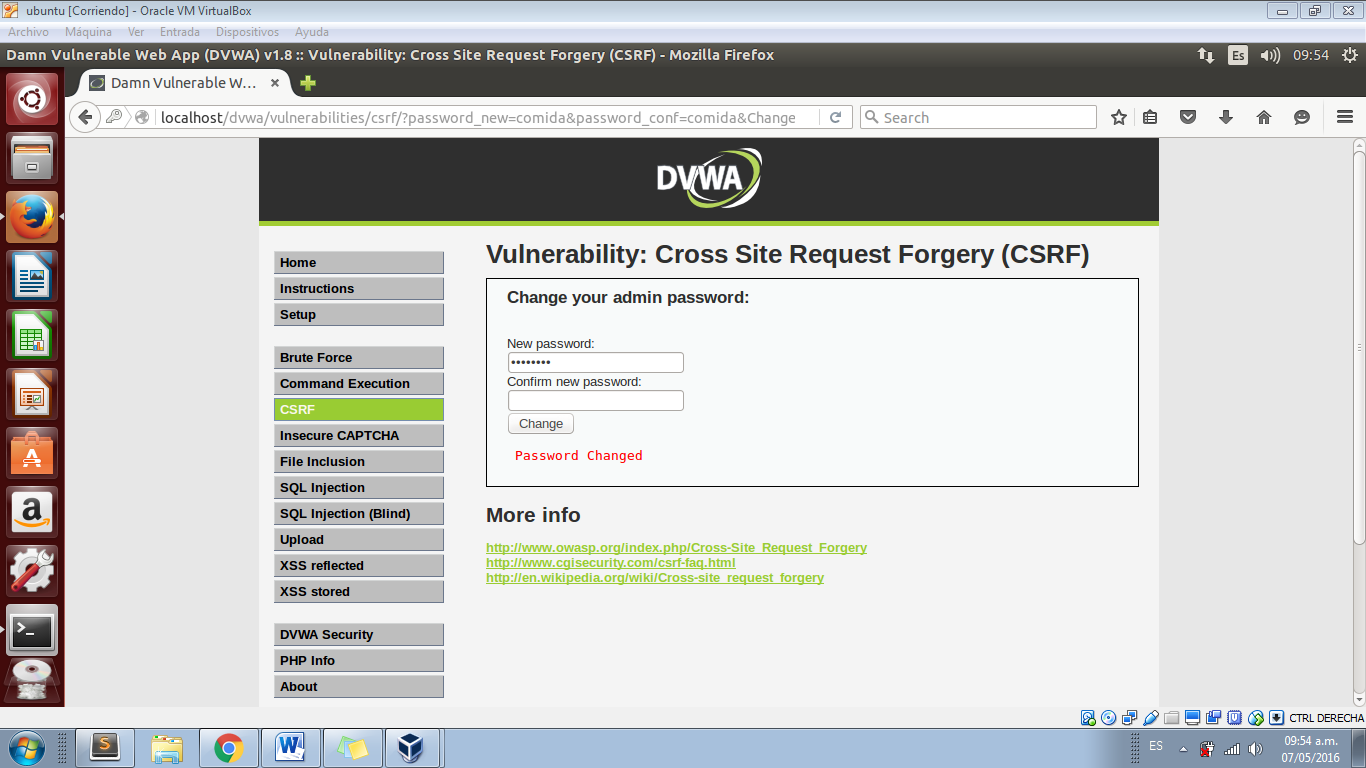
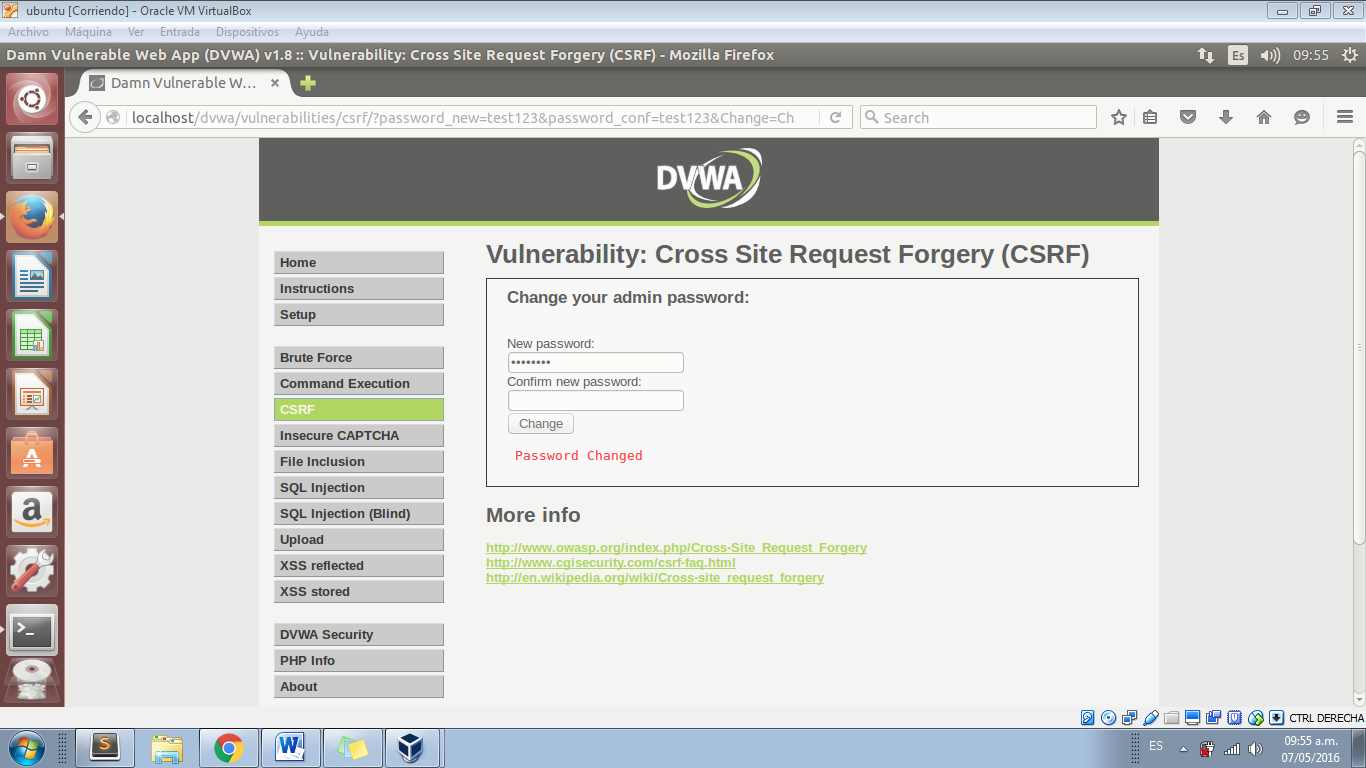
**Laboratorio 8**

Al empezar con el CSRF, cabe destacar un error en cuanto al cambio de contraseña, el sitio web nunca pide una contraseña antigua. Es decir desde el principio no existe una validación nuevamente (además de la validación del inicio) que si el usuario necesita escribir la contraseña antigua para cambiarla por la nueva.

El primer paso consiste en cambiar la contraseña, al parecer esta pasa por el método “get”. Como se puede ver en esta imagen



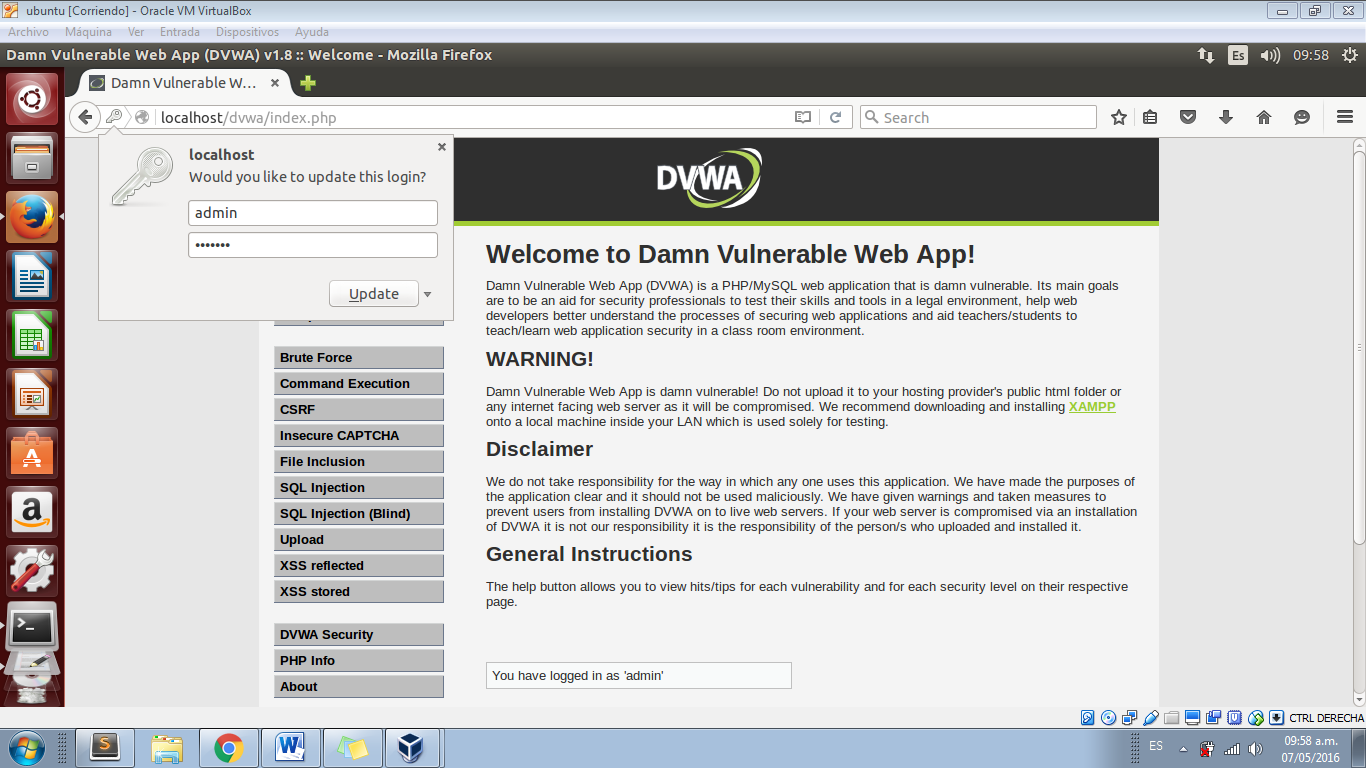
La contraseña password\_new = comida y password\_conf=comida, nos otorgan ambos campos con su respectivo valor. Desde el navegador cambiaremos los campos de password. En vez de colocar “comida” lo cambiaremos por “test123”



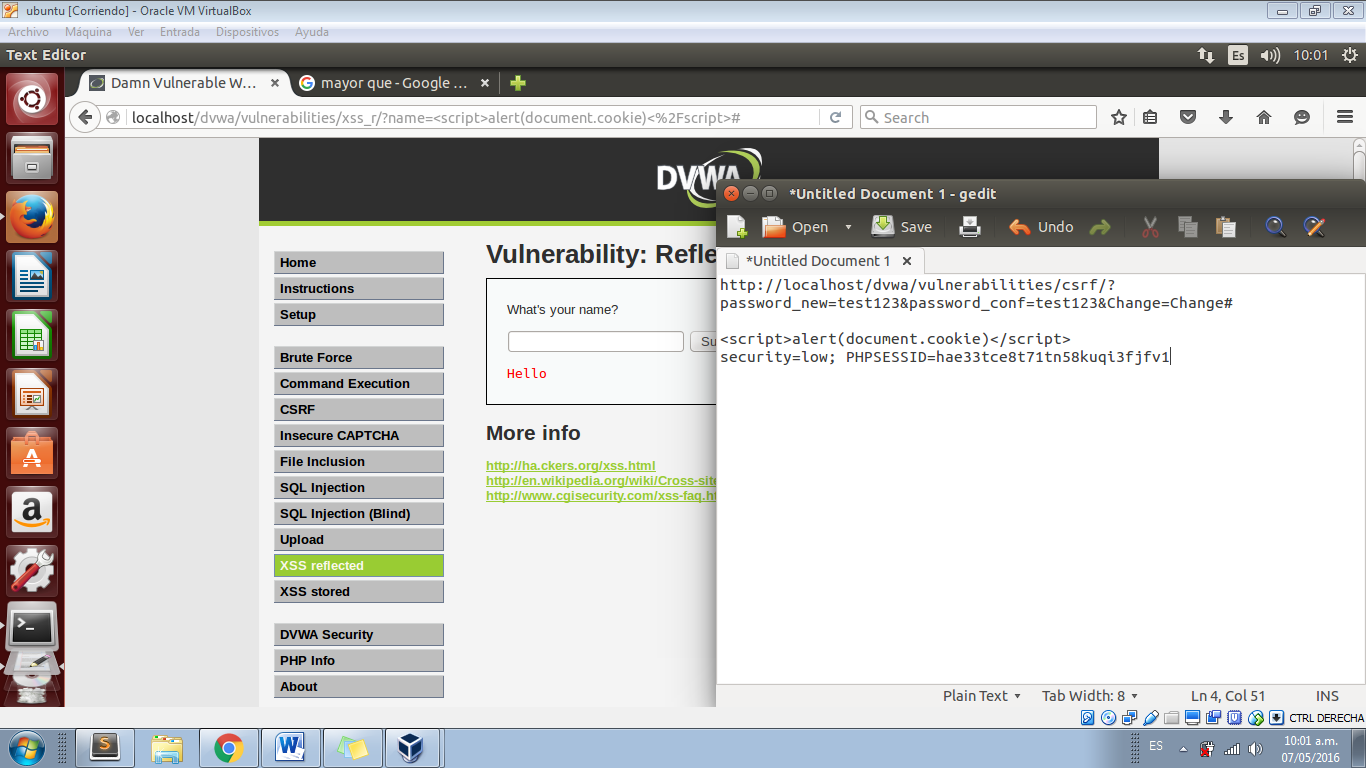
Hemos cambiado la contraseña de “comida” a “test123”, para comprobar esto, nos logeamos nuevamente con la última contraseña.



Y finalmente volvemos a acceder al sistema:

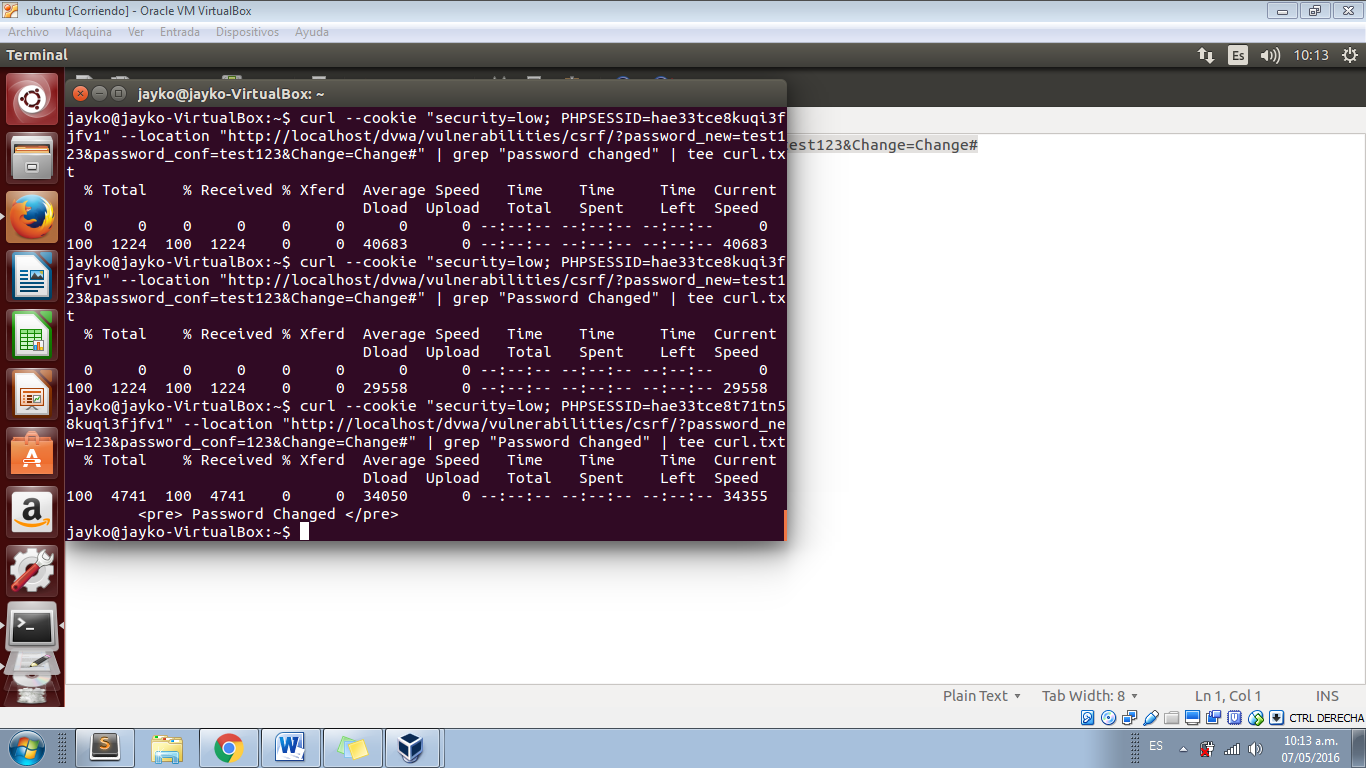


Ahora accedemos al XSS reflected y sacamos el phpsessid con el document.cookie



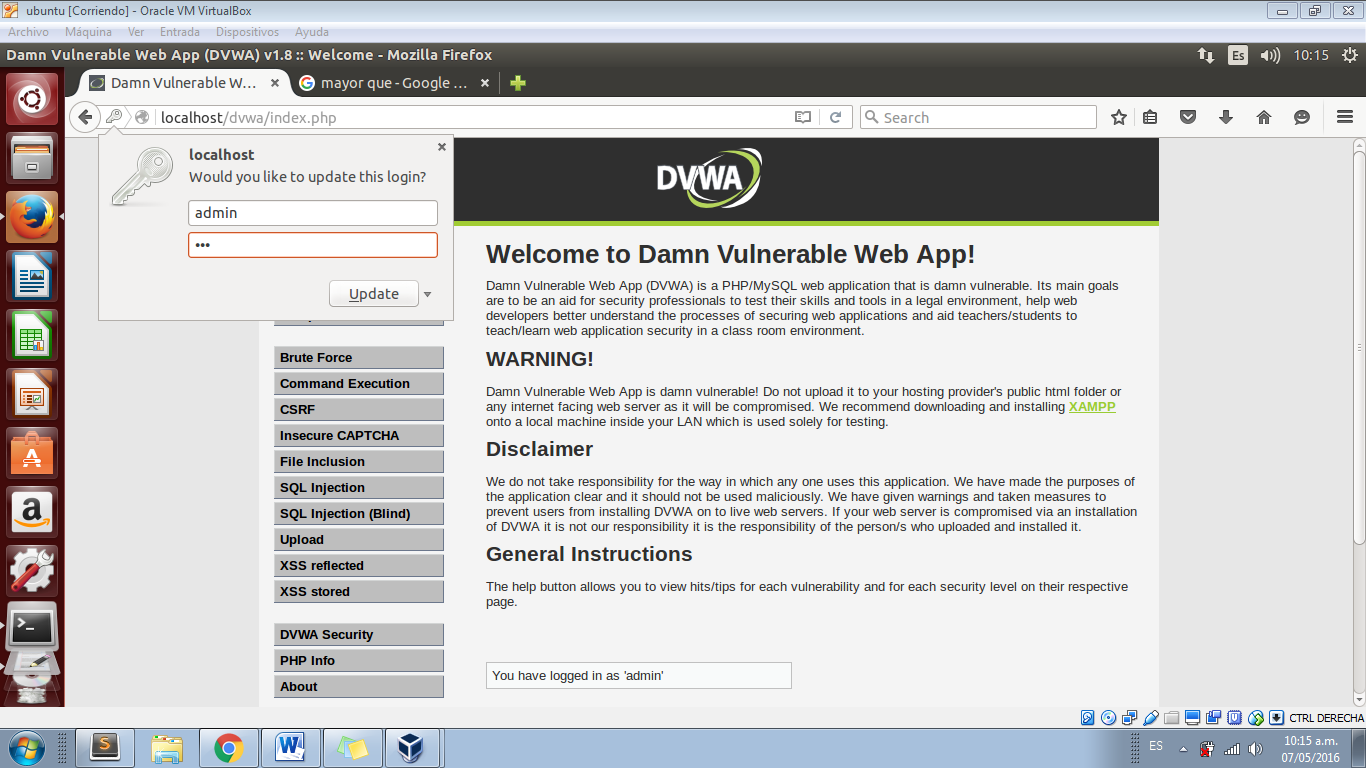
Accedemos ahora al curl y copiamos el siguiente código.

Cabe destacar que el siguiente código tiene la contraseña como “test123”, entonces lo modificamos para que cambie la contraseña por “123”



En el resultado vemos que la contraseña ha sido cambiada. Hacemos un logout y revisamos la contraseña





Y hemos accedido.

Datos y usuario:

