**Cross-Site Request Forgery Attack**

Using Damn Vulnerable Web App (DVWA) with Curl

|  |
| --- |
| Copyrights 2016-2017 Bowie State University.  The lab manual is developed for Cybersecuirty courses. Comments and suggestions can be sent to wxu@bowiestate.edu |

**Introduction**

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable.

Objectives:

1. Observe URL to change password
2. Capture and manipulate a CSRF URL to change the admin password.
3. Obtain the session cookie string using a reflective XSS attack.
4. Create a curl CSRF string to reset the admin password.

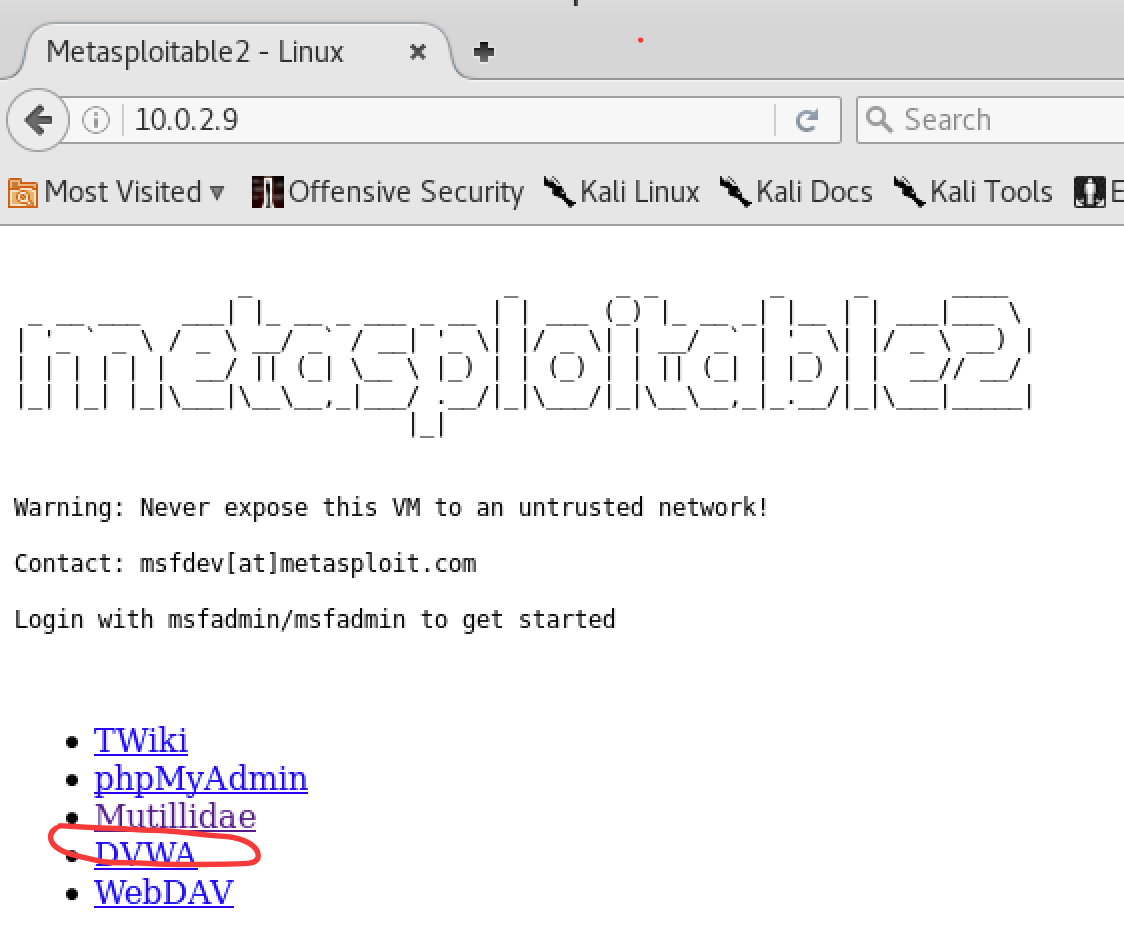
**Lab Environment**

Kali and Metasploitable 2 is required for the lab. The usernames and passwords for Kali are listed in the following:

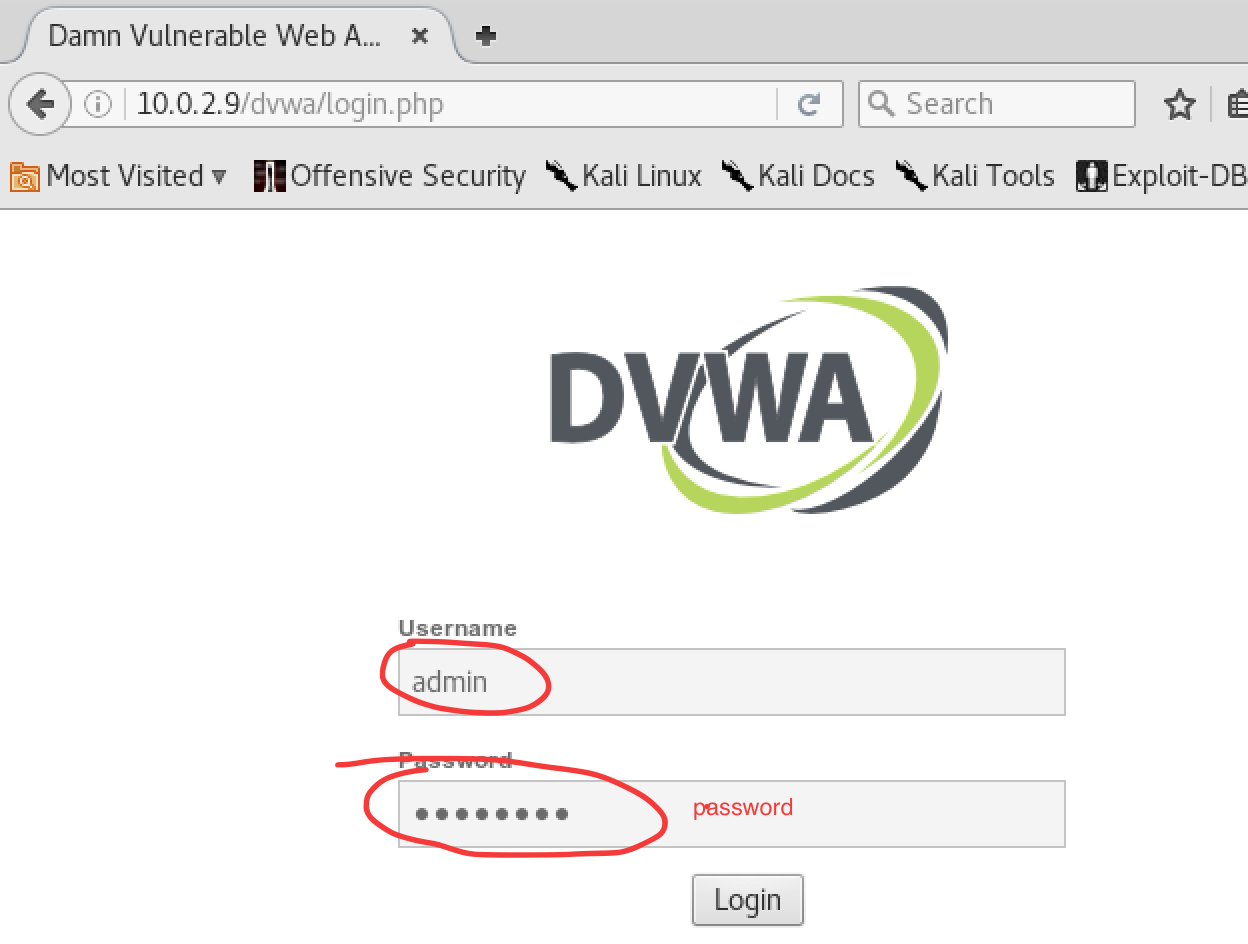
* + User ID: root, Password: *root*.
  + User ID: seed, Password: *toor*

**Task 1: Observe URL to change password**

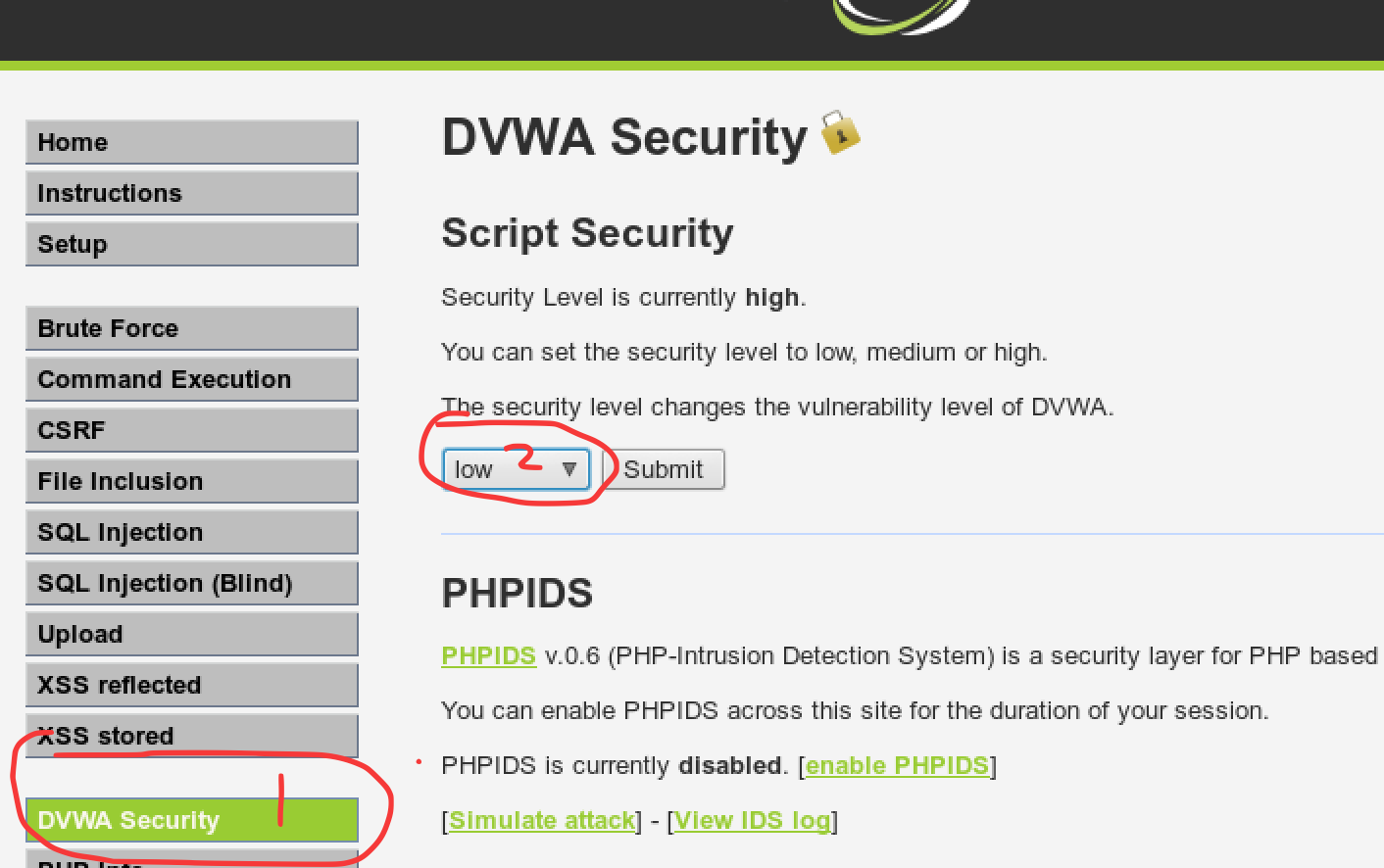
1. Start Metasploitable and open DVWA at Kali.



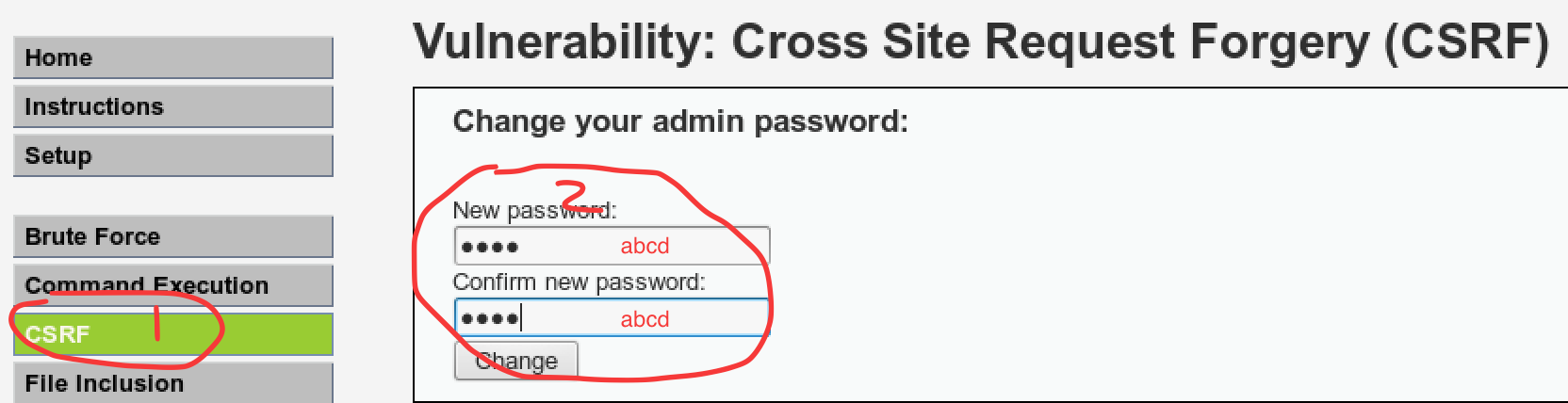
1. Log in to DVMA



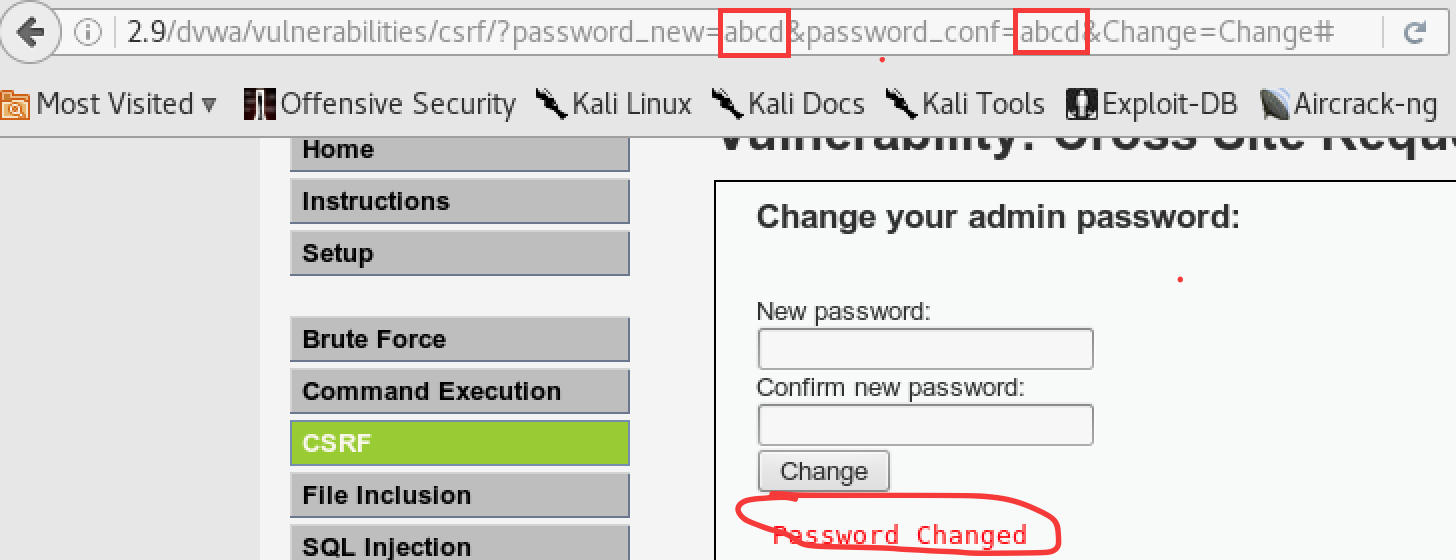
1. Setting security level



1. Reset password as a normal user

****

1. Observe the URL

****

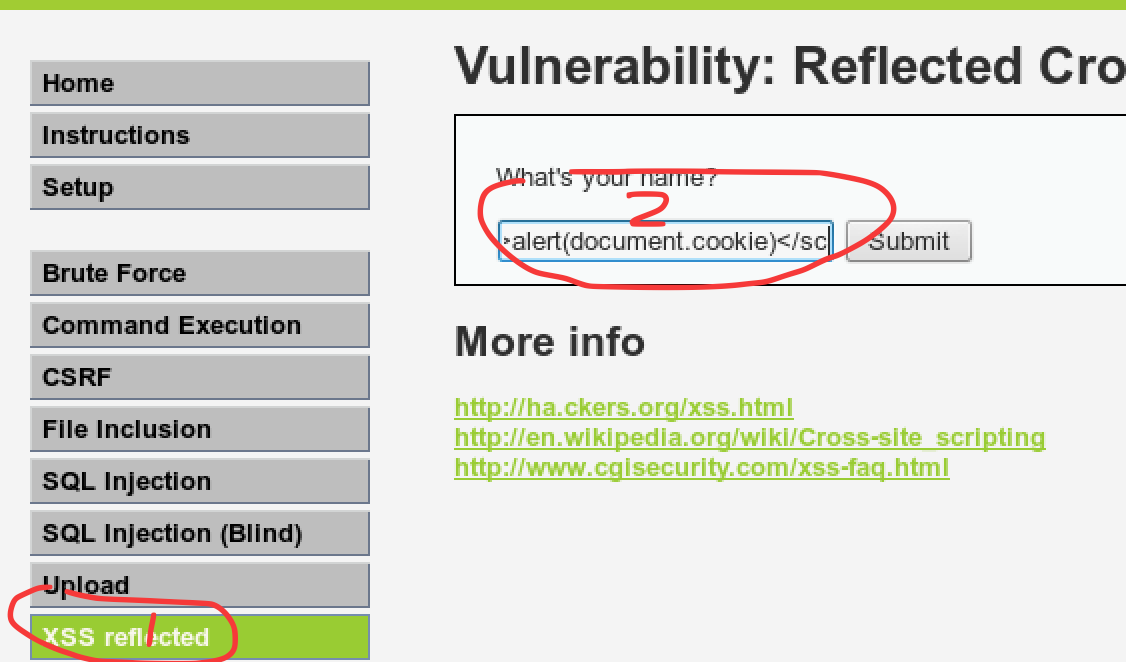
**Task 2: Capture and manipulate a CSRF URL to change the admin password**

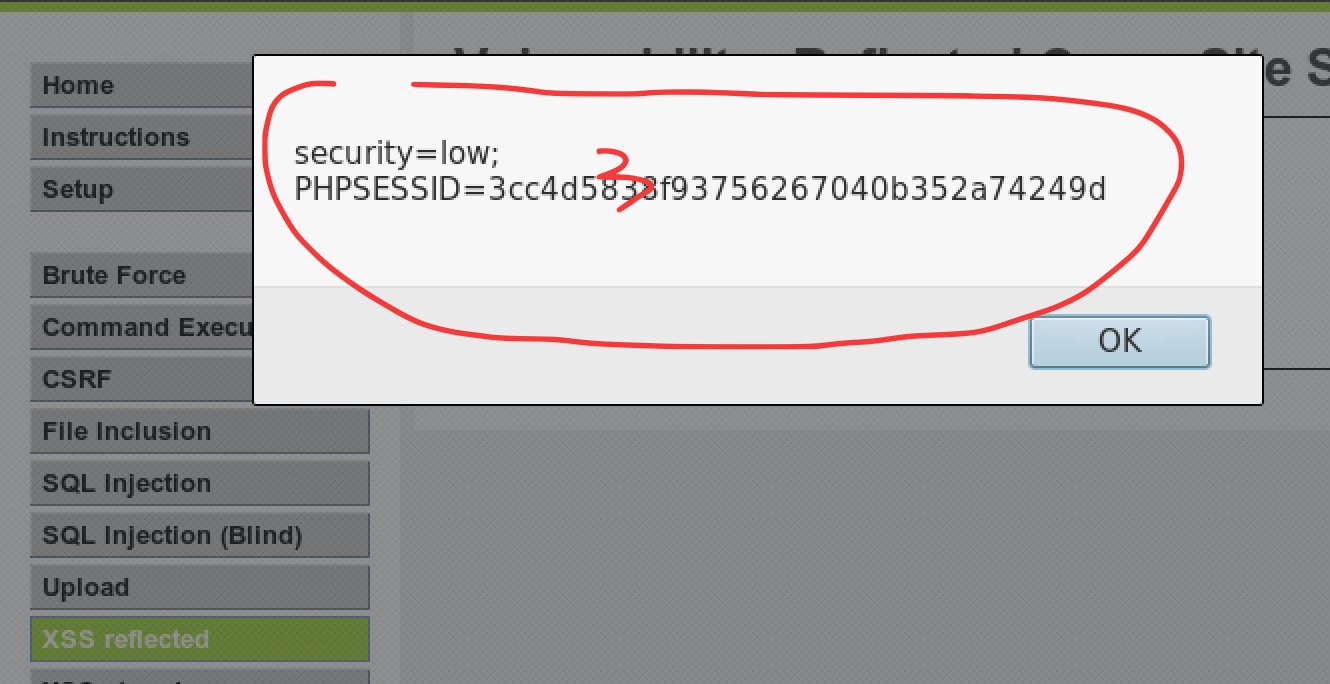
1. You can use the link to change any password if you reload the page.
   1. Why?
   2. Close the current browser, re-open it, and use the same URL to change it password. Are you able to change password successfully?

<http://10.0.2.9/dvwa/vulnerabilities/csrf/?password_new=abcd&password_conf=abcd&Change=Change#>

**Task 3: Obtain the session cookie string using a reflective XSS attack.**

1. Log in as admin with password “abcd”
2. Set DVWA Security Level as “low”
3. XSS attack to steal the session ID





**Task 4: Create a curl CSRF string to reset the admin password.**

1. Go to notepad
2. In notepad type the following
   1. curl --cookie "" --location ""
   2. Place the cookie string between the quotes after the --cookie tag.
   3. Place the html string between the quotes after the --location tag.
   4. Replace the password "abcd" password with any password you want, e.g.,"mypwd"

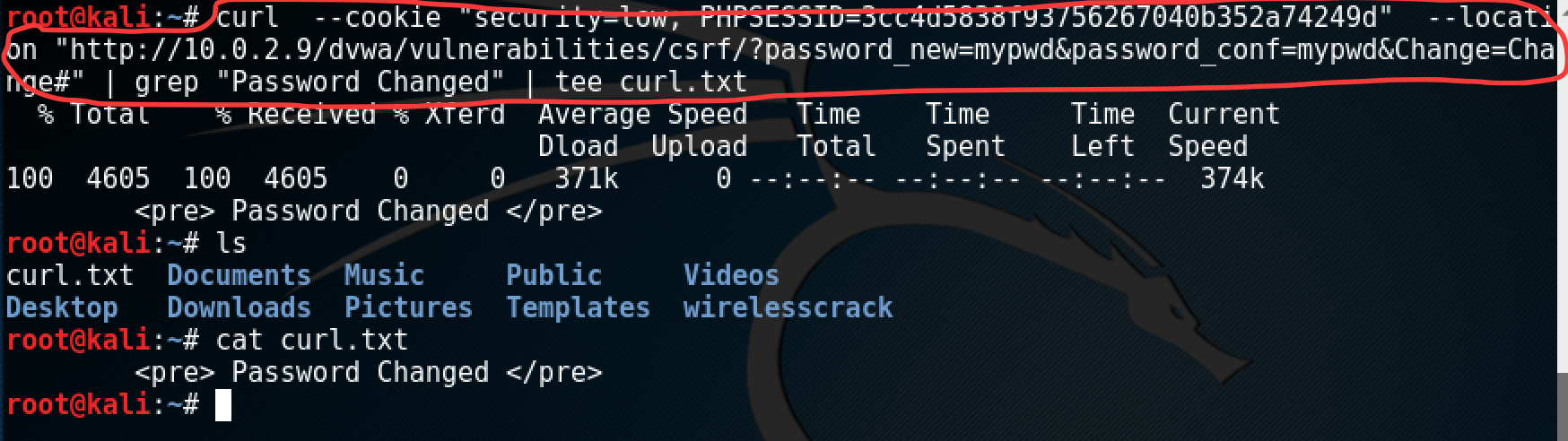
URL: http://10.0.2.9/dvwa/vulnerabilities/csrf/?password\_new=abcd&password\_conf=abcd&Change=Change#

Cookie: security=low; PHPSESSID=3cc4d5838f93756267040b352a74249d

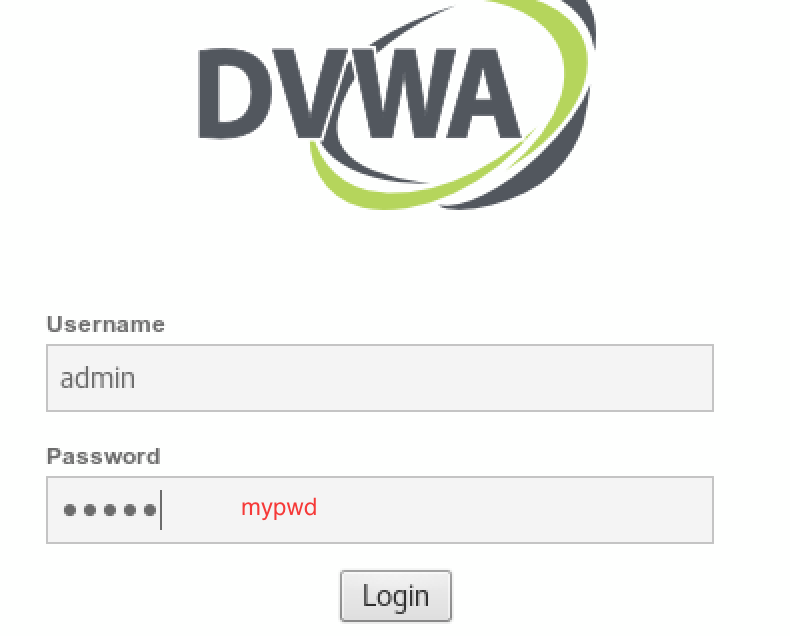
* 1. grep the key words and save in to a file, i.e., curl.txt

1. Open a terminal and execute the command

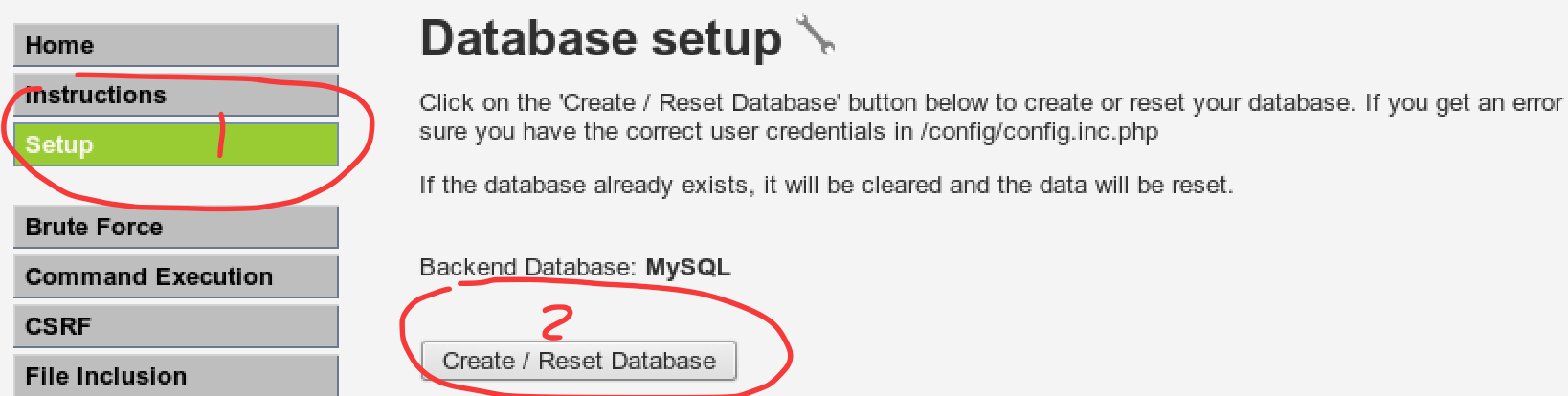
curl --cookie “security=low; PHPSESSID=3cc4d5838f93756267040b352a74249d“ --location <http://10.0.2.9/dvwa/vulnerabilities/csrf/?password_new=mypwd&password_conf=mypwd&Change=Change#> | grep “Password Changed” | tee curl.txt



1. Log in use the new password “mypwd”



1. Clear all the changes



**How Does It Work**

This part describes the theory of the project.

# Reference:

* http://www.computersecuritystudent.com/SECURITY\_TOOLS/DVWA/DVWAv107/lesson10/