Unit 13: Bouns

## **Step 3: Using Forms and a Cookie Jar**

1. Construct a curl request that enters two forms: "log={username}" and "pwd={password}" and goes to http://localhost:8080/wp-login.php. Enter Ryan's credentials where there are placeholders.

* [curl --form "log=Ryan" --form "pwd=123456" http://localhost:8080/w p-admin/login.php]
* Question: Did you see any obvious confirmation of a login? (Y/N) Yes

1. Construct the same curl request, but this time add the option and path to save your cookie: --cookie-jar ./ryancookies.txt. This option tells curl to save the cookies to the ryancookies.txt text file.

* [curl --cookie-jar ./ryancookies.txt --form "log=Ryan" --form "pwd=123456" http://localhost:8080/wp-admin/login.php]

1. Read the contents of the ryancookies.txt file.

* 4 separate cookies were set and are now stored in the file

Note that each one of these is a cookie that was granted to Ryan after logging in.

#### **Step 4: Log in Using Cookies**

1. Craft a new curl command that now uses the --cookie option, followed by the path to your cookies file. For the URL, use http://localhost:8080/wp-admin/index.php.
   * [curl --cookie ./ryancookies.txt http://localhost:8080/wp-admin/index.php]
   * **Question:** Is it obvious that we can access the Dashboard? (Y/N) Yes
2. Press the up arrow on your keyboard to run the same command, but this time, pipe | grep Dashboard to the end of your command to return all instances of the word Dashboard on the page.

* **Question:** Look through the output where Dashboard is highlighted. Does any of the wording on this page seem familiar? (Y/N) If so, you should be successfully logged in to your Editor's dashboard. Yes

#### 

#### 

#### 

#### **Step 5: Test the Users.php Page**

1. Finally, write a curl command using the same --cookie ryancookies.txt option, but attempt to access http://localhost:8080/wp-admin/users.php.  
   * [curl --cookie ./ryancookies.txt http://localhost:8080/wp-admin/users.php]
   * **Question:** What happens this time? error page pops up stating we do not have proper authorization.