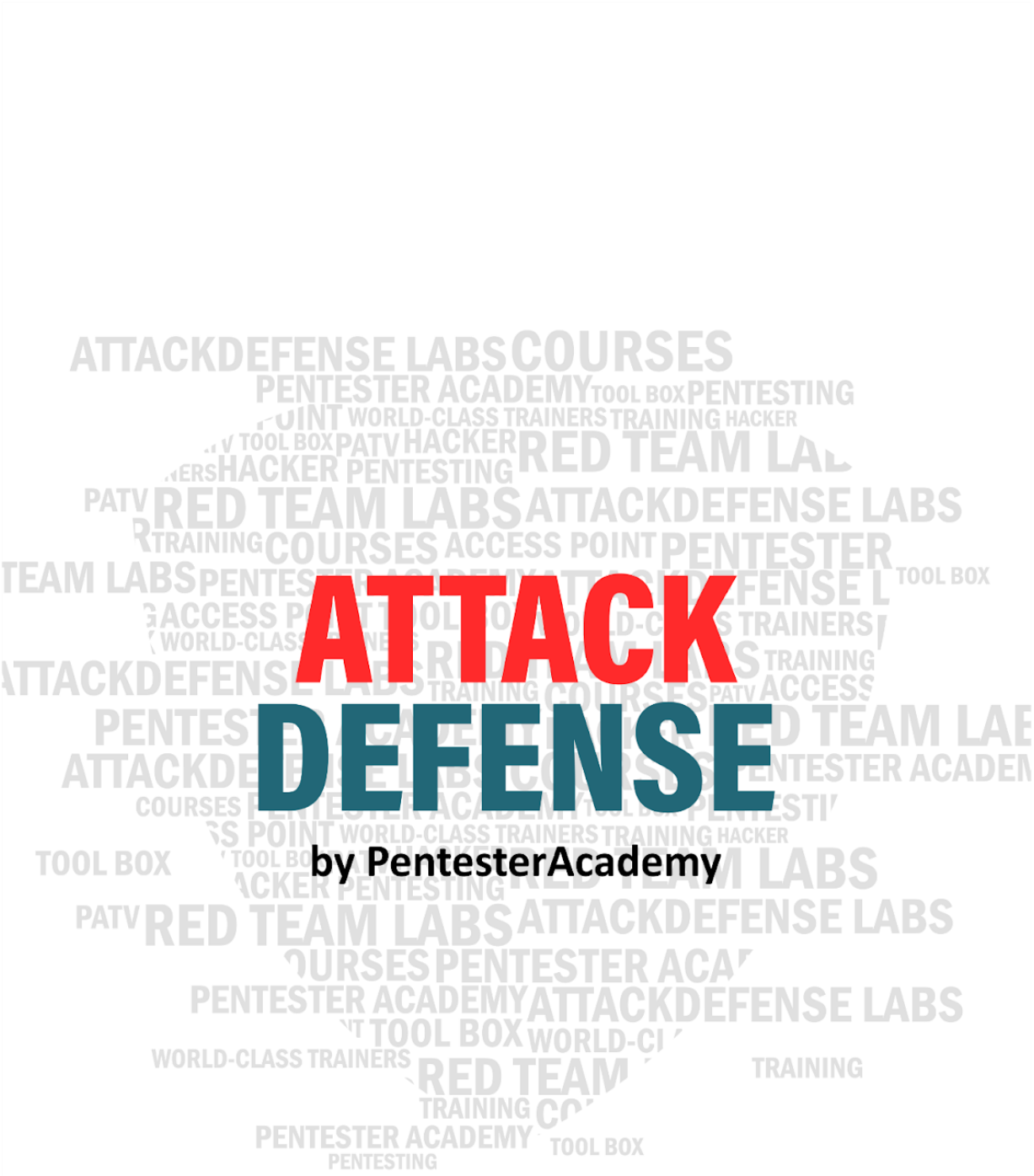
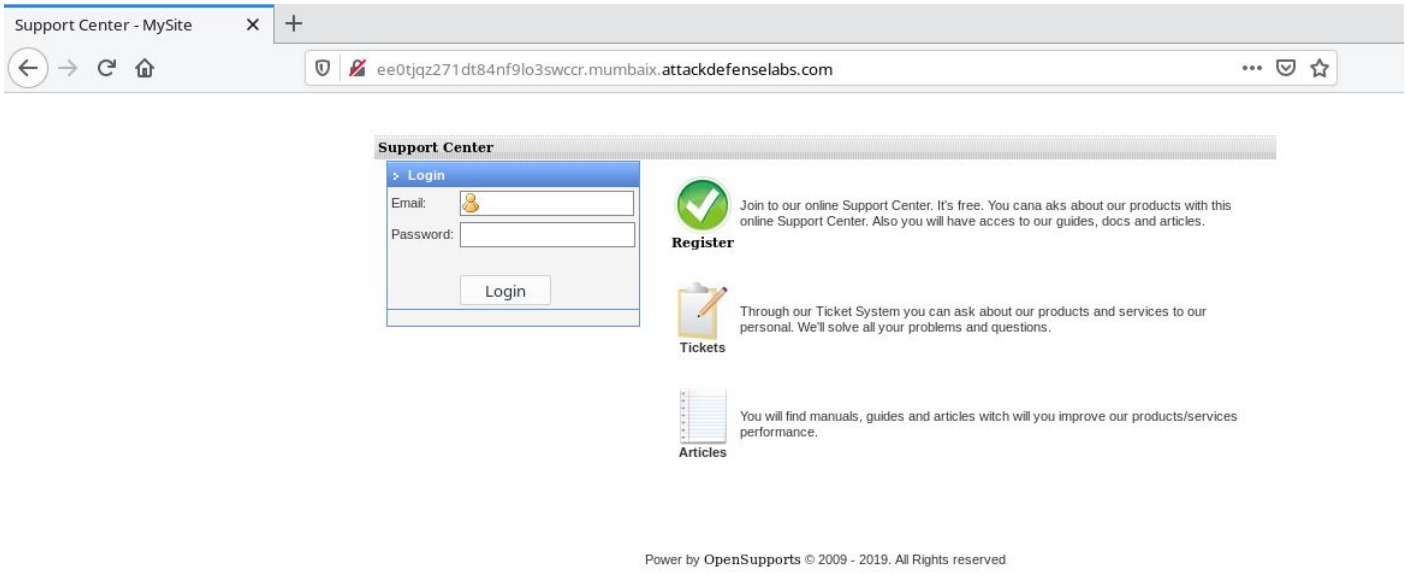

ATTACK
DEFENSE
by PentesterAcademy

Name	OpenSupports
URL	https://attackdefense.com/challengedetails?cid=437
Type	Real World Webapps : Broken Authentication

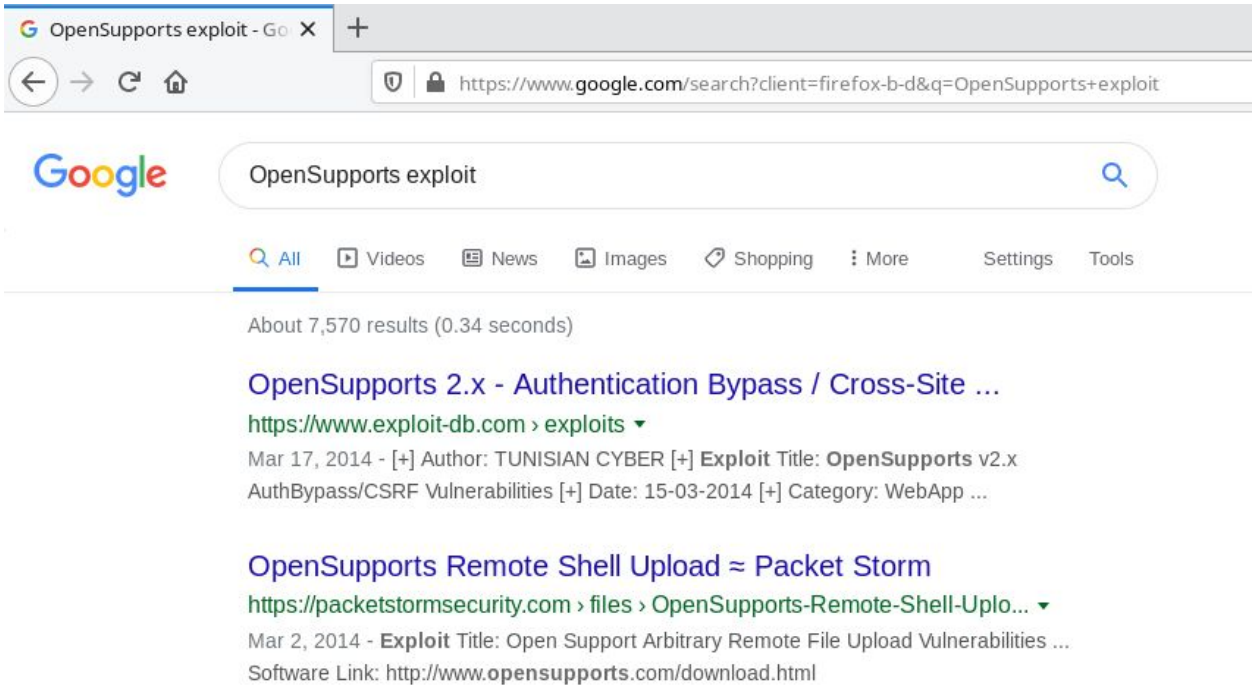
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

Step 1: Inspect the web application.

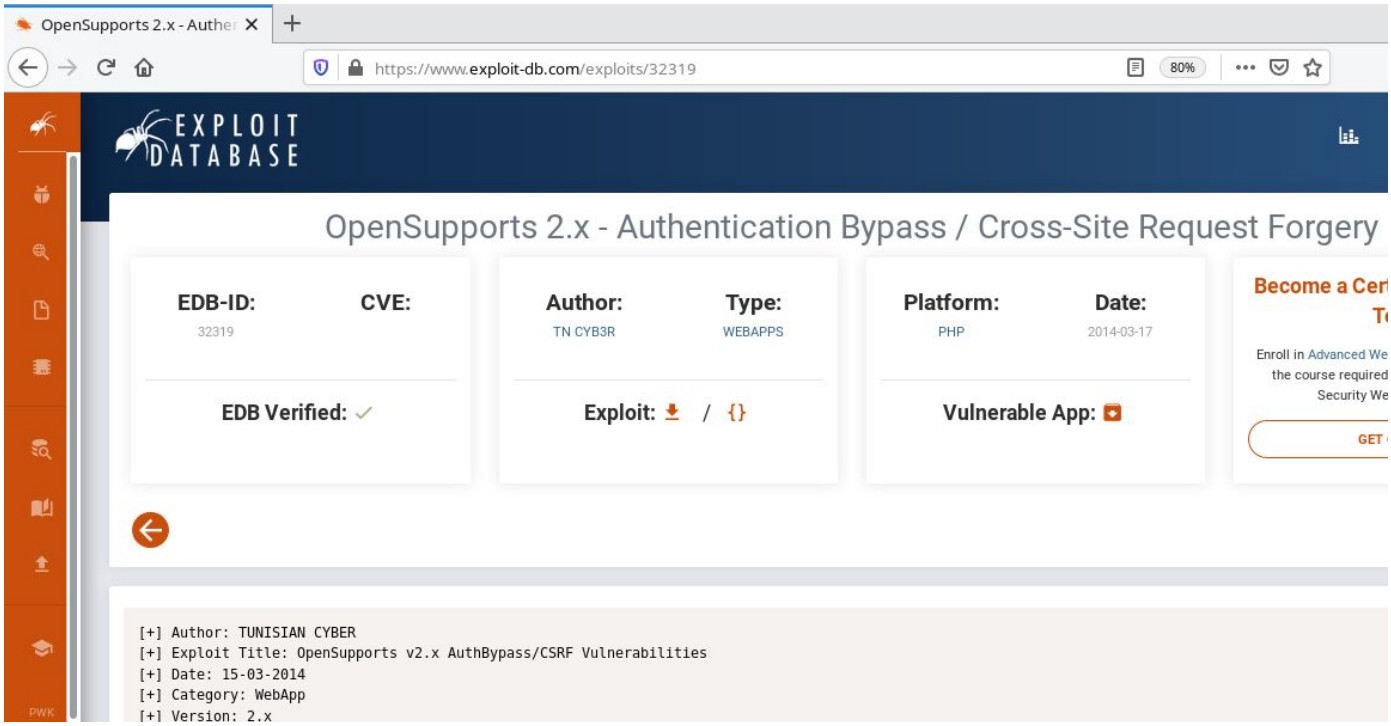


Step 2: Search on google “OpenSupports exploit” and look for publicly available exploits.



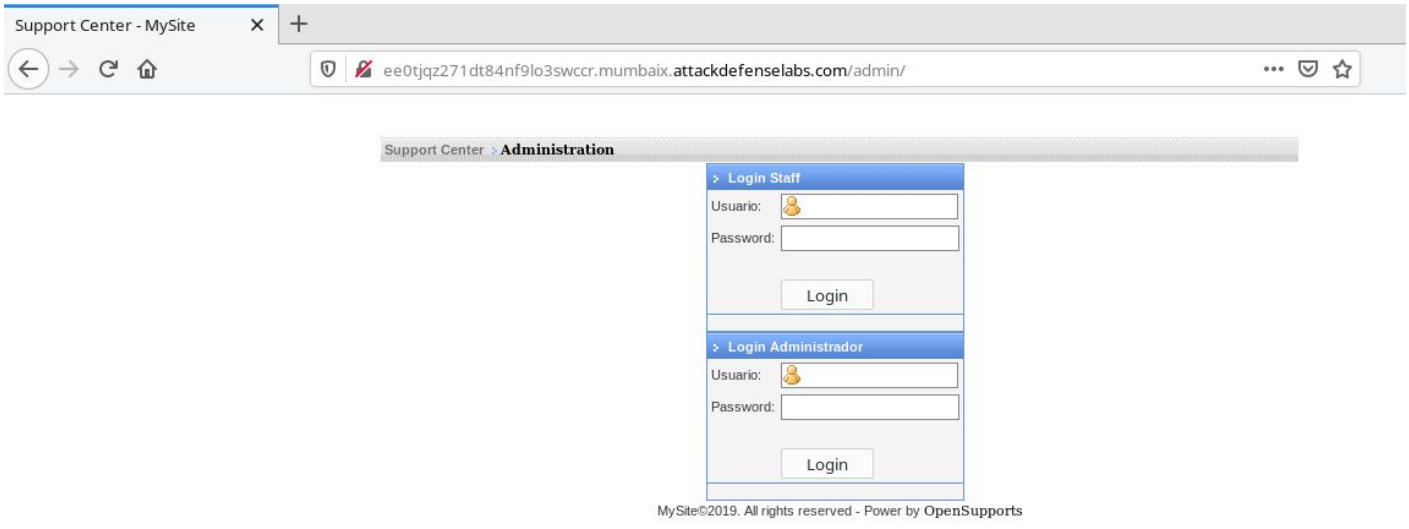
The exploit db link contains an HTML script which can be used to exploit the vulnerability.

Exploit DB Link: https://www.exploit-db.com/exploits/32319



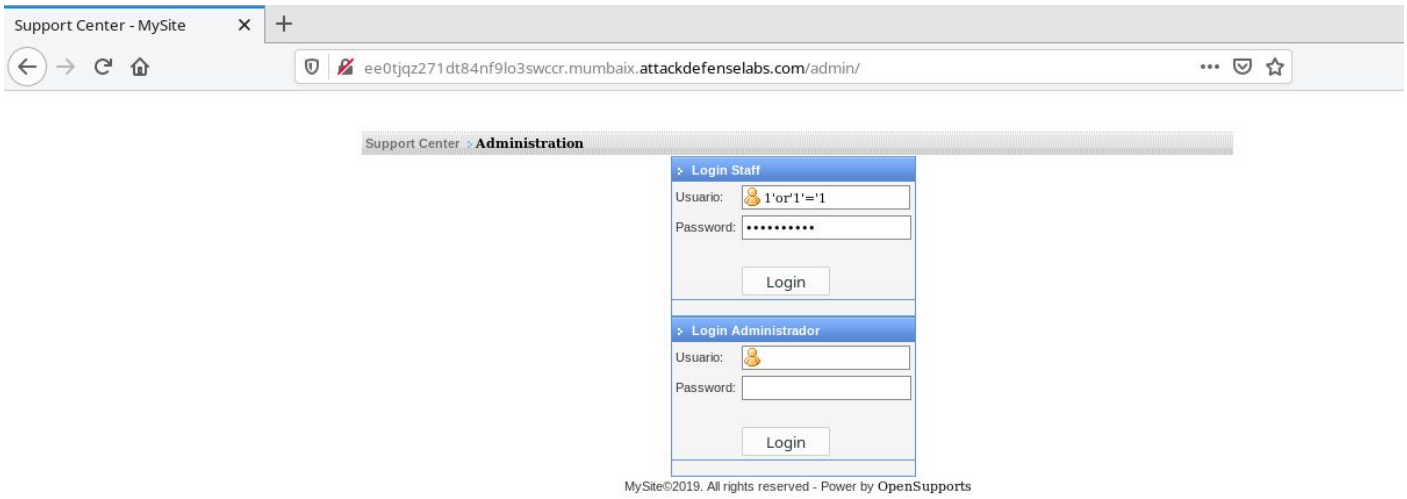
Step 3: Navigate to the login page located at /admin/

URL: http://ee0tjqz271dt84nf9lo3swccr.mumbaix.attackdefenselabs.com/admin/

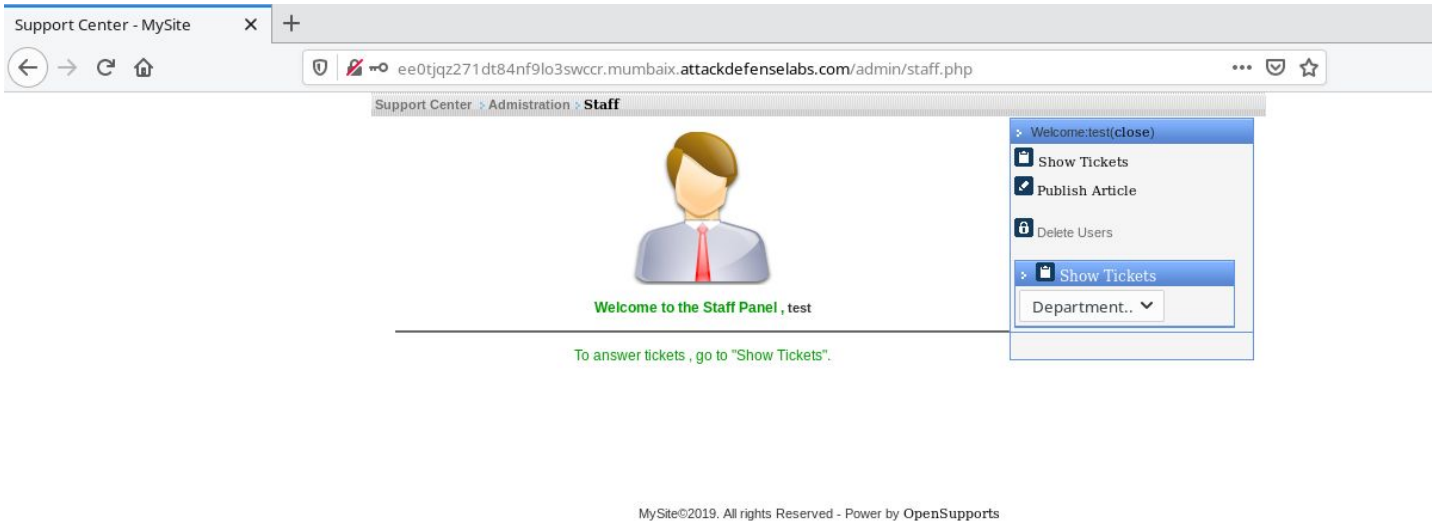


Step 4: In the Login Staff login portal, inject the SQLI payload in username and password field.

Payload: 1'or'1'='1



Step 5: Click on the Login button.



Authentication was bypassed successfully.

References:

1. Open Support (https://www.opensupports.com/)
2. OpenSupports 2.x - Authentication Bypass / Cross-Site Request Forgery (https://www.exploit-db.com/exploits/32319)