

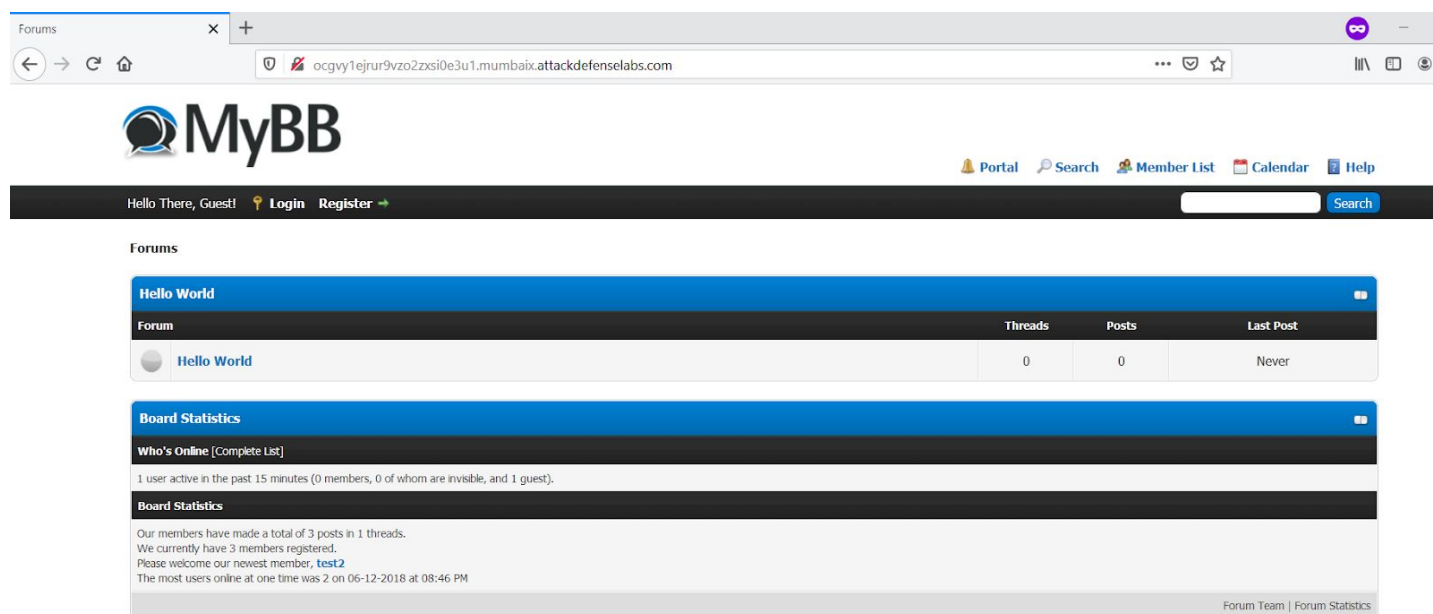
[illegible]

Name	MyBB Downloads Plugin
URL	https://www.attackdefense.com/challengedetails?cid=9
Type	Real World Webapps : Stored XSS

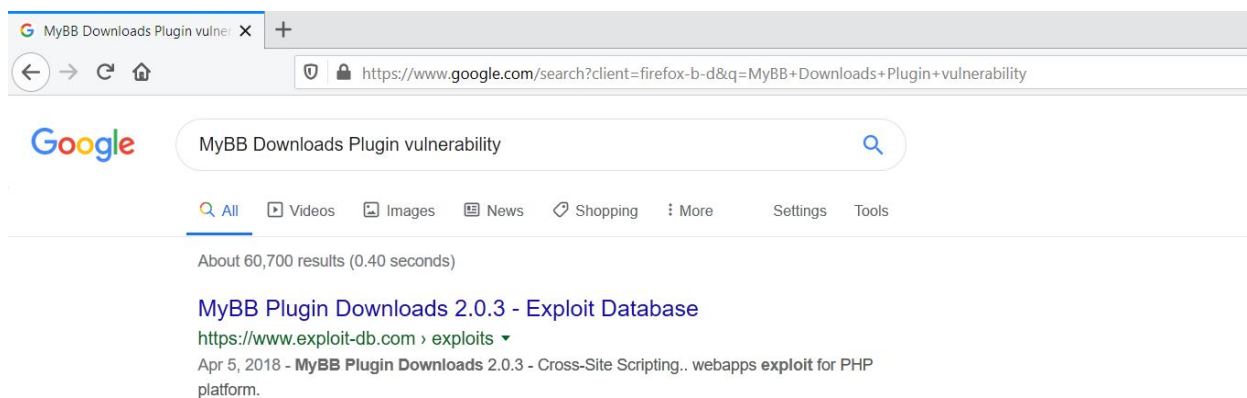
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

Step 1: Inspect the web application.

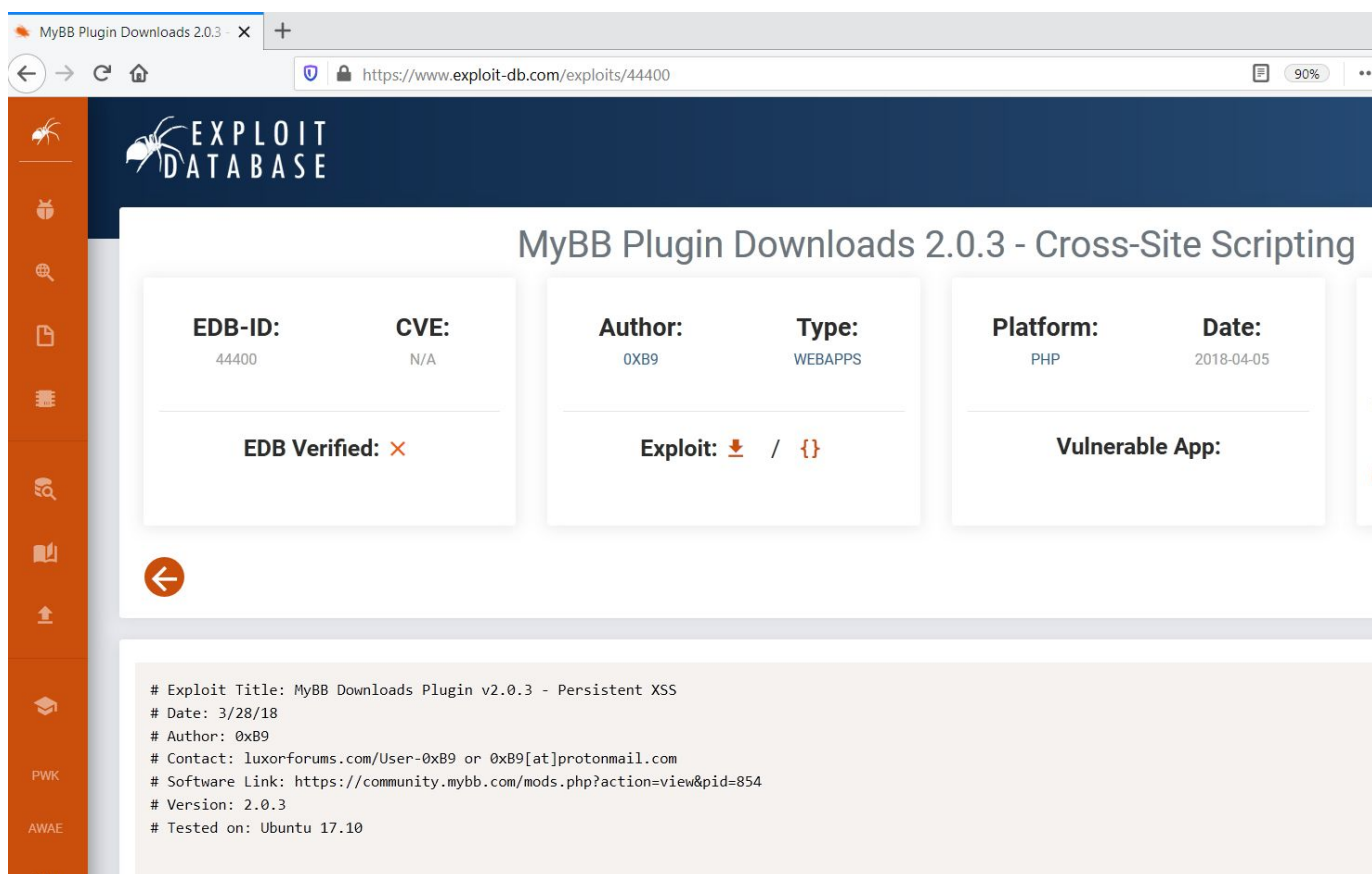


Step 2: Search on google “MyBB Downloads Plugin vulnerability” and look for publicly available exploits.



The exploit db link contains the payload required to exploit the vulnerability.

Exploit DB Link: <https://www.exploit-db.com/exploits/44400>



Step 3: The user has to authenticate in order to exploit the vulnerability. The login credentials are provided in the challenge description.


URL:

<http://ocgvv1ejrur9vzo2zksi0e3u1.mumbaix.attackdefenselabs.com/member.php?action=login>

Credentials:

- **Username:** test2
- **Password:** password

Login Page



The screenshot shows a web browser window with the title "Forums - Login". The address bar displays the URL: ocgvv1ejrur9vzo2zksi0e3u1.mumbaix.attackdefenselabs.com/member.php?action=login. The page features the MyBB logo at the top left. A navigation bar includes the text "Hello There, Guest!" followed by "Login" and "Register" links. Below this, a breadcrumb trail shows "Forums" and "Login". The main content area is titled "Login" and contains two input fields: "Username:" and "Password:". The password field includes a "(Lost your password?)" link. A "Remember me" checkbox is located at the bottom right of the login form.

Admin Dashboard

Forums

ocgvy1ejrur9vzo2zxi0e3u1.mumbaix.attackdefenselabs.com/index.php

MyBB

Portal Search Member List Calendar

Welcome back, test2. You last visited: 07-06-2018, 12:55 PM [Log Out](#)

User CP Open Buddy List View New Posts View Today's Posts Private Messages

Forums

Hello World

Forum	Threads	Posts	Last
Hello World	0	0	Ne

Board Statistics

Who's Online [Complete List]

1 user active in the past 15 minutes (1 member, 0 of whom are invisible, and 0 guests).
test2

Board Statistics

Our members have made a total of 3 posts in 1 threads.
We currently have 3 members registered.

Step 4: Navigate to the downloads page.

URL: <http://ocgvy1ejrur9vzo2zxi0e3u1.mumbaix.attackdefenselabs.com/downloads.php>

Downloads

ocgvy1ejrur9vzo2zxi0e3u1.mumbaix.attackdefenselabs.com/downloads.php

MyBB


Portal Search Member List Calendar Help

Welcome back, test2. You last visited: 07-06-2018, 12:55 PM [Log Out](#)

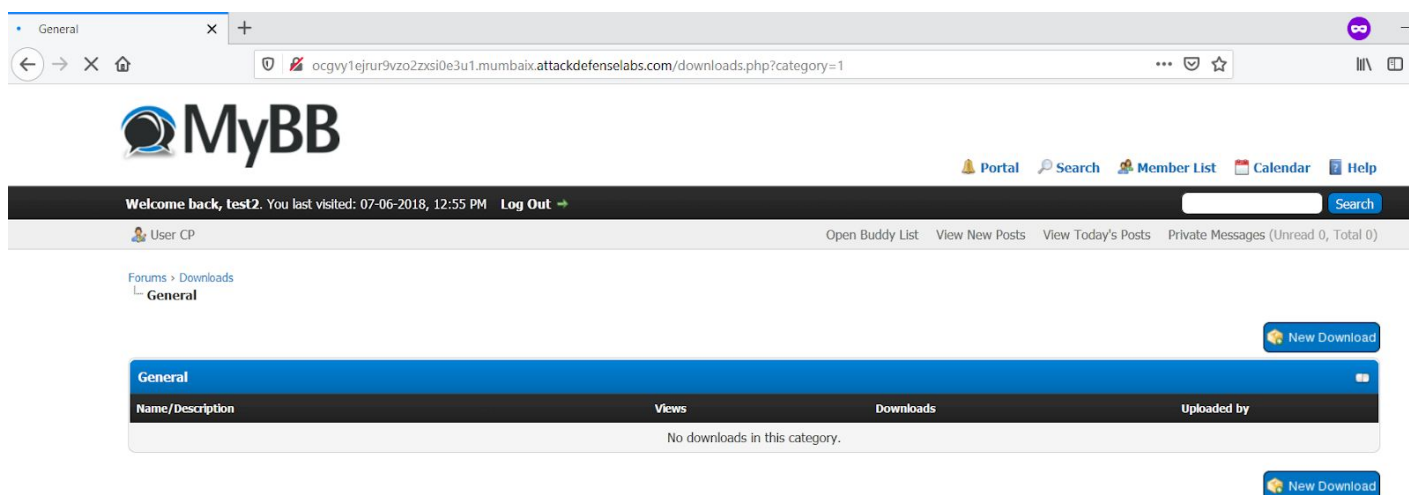
User CP Open Buddy List View New Posts View Today's Posts Private Messages (Unread 0, Total 0)

Downloads

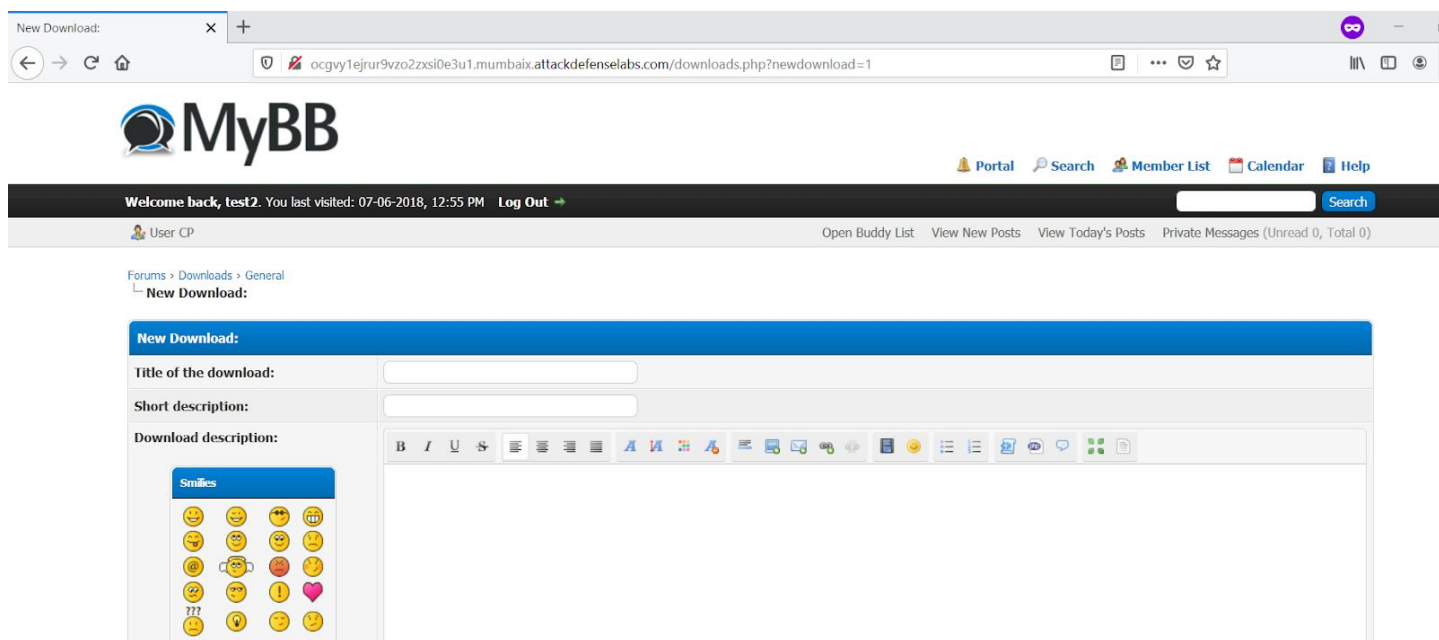
Categories:

Description	Posts	Last Post
 <p>General General downloads</p>	0	Never

Step 5: Click on the General button.



Step 6: Click on New Download button.



Step 7: Inject the payload in the title field and enter any data in Short description, Download description, Title page field.

Payload: <BODY ONLOAD=alert('XSS')>

New Download: x +

ocgv1ejrur9vzo2zxi0e3u1.mumbaix.attackdefenselabs.com/downloads.php?newdownload=1

New Download:

Title of the download: <BODY ONLOAD=alert("XSS")>

Short description: this is a test data

Download description:

Smilies

this is a test data

Title Page:
Enter the URL of the picture on the title page. this is test data

Links
Enter the file number of links. 1

Images:
Enter the number of images will have. ☐ Want to enter images
Number of images to upload: 4 (Maximun 10)

Publish download

Click on Publish Download button.

Add links x +

ocgv1ejrur9vzo2zxi0e3u1.mumbaix.attackdefenselabs.com/downloads.php?newlinks=1&urls=1&boximg=0&images=4

MyBB

Welcome back, test2. You last visited: 07-06-2018, 12:55 PM Log Out →

User CP Open Buddy List View New Posts View Today's P

Forums > Downloads > General > Add links

Add links

link 1:

Name: Links:

XSS

OK



The XSS payload triggered successfully.

References:

1. MyBB (<https://mybb.com/>)
2. MyBB Plugin Downloads
(<https://community.mybb.com/mods.php?action=view&pid=854>)
3. MyBB Plugin Downloads 2.0.3 - Cross-Site Scripting
(<https://www.exploit-db.com/exploits/44400>)