ATTACKDEFENSE LABS COURSES

PENTESTER ACADEMYTOOL BOX PENTESTING

JUNT WORLD-CLASS TRAINERS TRAINING HACKER

PATY RED TEAM LABS ATTACKDEFENSE LABS

TRAINING COURSES ACCESS POINT PENTESTER

TEAM LABS PENTESTY TO THE OLD OF DOLD-CLASS TRAINERS I WORLD-CLASS TRAINING COURSES PAY THE OLD OF DOLD-CLASS TRAINING THAN THE STAINING TO TEAM LAB

ATTACKDEFENSE LABS TRAINING COURSES PENTESTER ACADEM

COURSES TO LABS TRAINING COURSES PENTESTER ACADEM

COURSES TO LABS TRAINING COURSES PENTESTER ACADEM

COURSES TO LABS TRAINING THAN THE STIP

S POINT WORLD-CLASS TRAINERS TRAINING HACKER

TOOL BOX

TOOL BOX

TOOL BOX TOOL BOX WORLD-CI

WORLD-CLASS TRAINERS TRAINING HACKER

TOOL BOX TOOL BOX WORLD-CI

WORLD-CLASS TRAINERS TRAINING TRAINING

TRAINING CO

PENTESTER ACADEMY ATTACKDEFENSE LABS

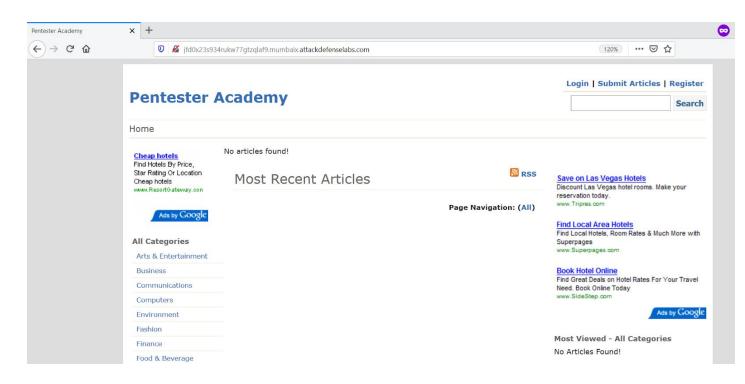
TRAINING

Name	ArticleSetup
URL	https://www.attackdefense.com/challengedetails?cid=492
Туре	Real World Webapps : Reflected XSS

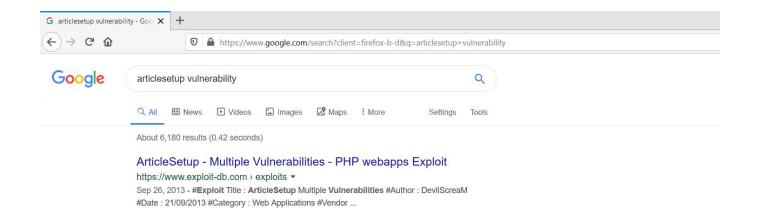
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

Step 1: Inspect the web application.

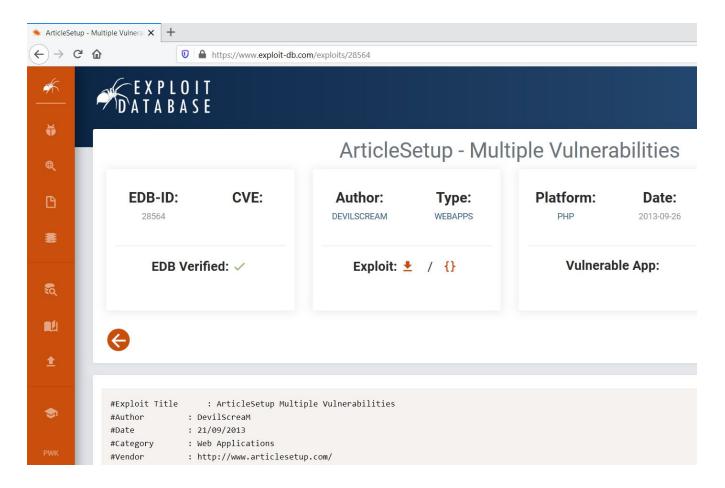


Step 2: Search on google "articlesetup vulnerability" and look for publicly available exploits.



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

Exploit DB Link: https://www.exploit-db.com/exploits/28564



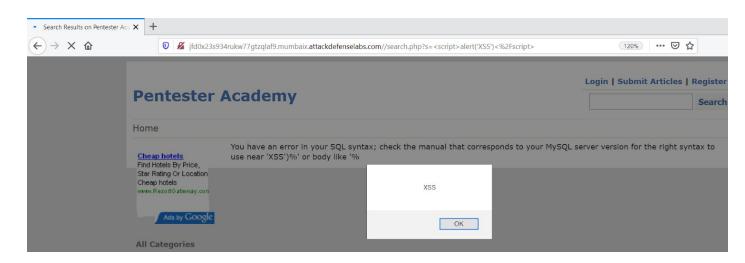


Step 3: Inject the payload in search field to exploit the vulnerability.

Payload: <script>alert('XSS')</script>



Click on Search



The XSS payload triggered successfully.

References:

- 1. ArticleSetup (http://www.articlesetup.com/)
- ArticleSetup Multiple Vulnerabilities (https://www.exploit-db.com/exploits/28564)