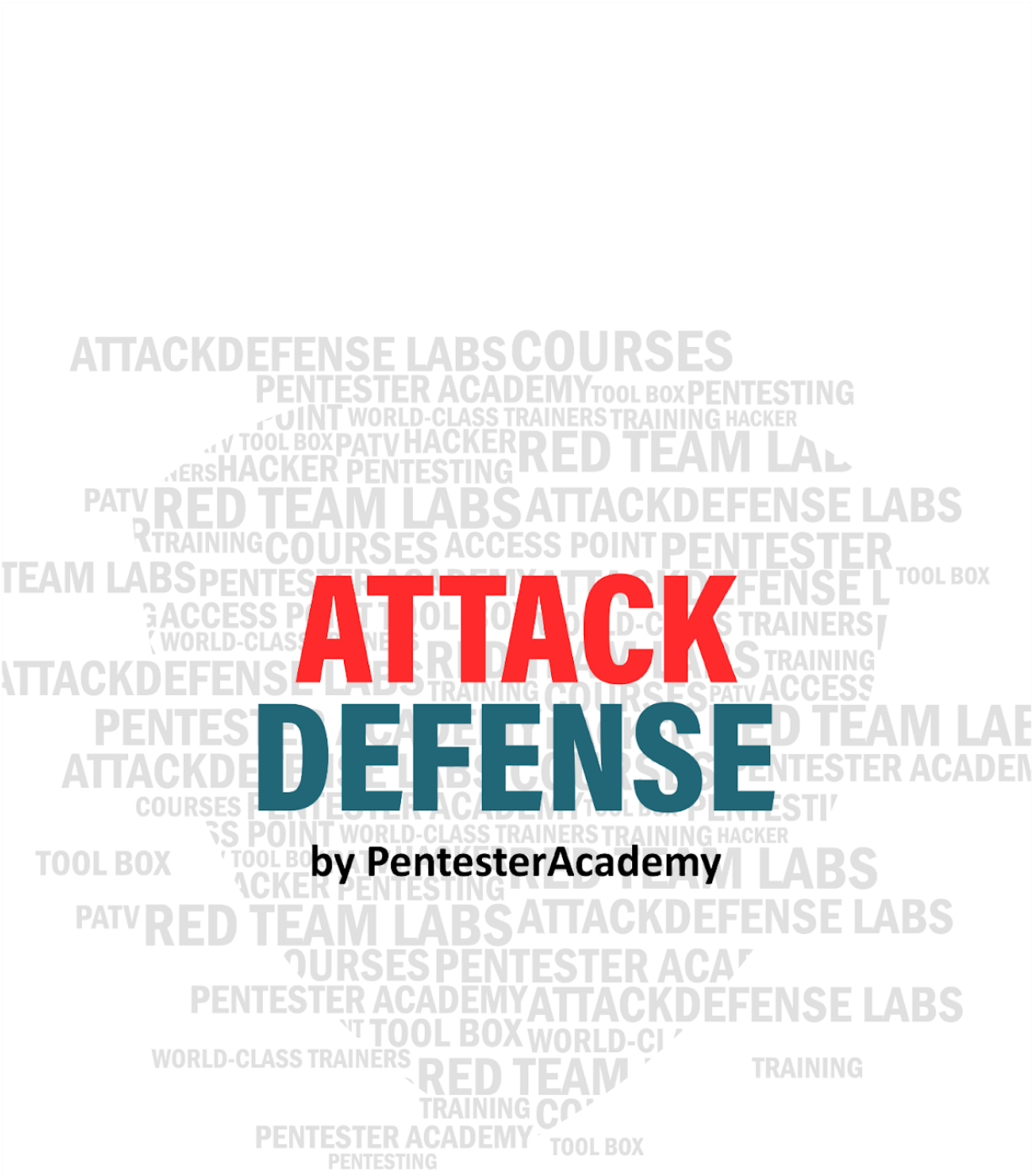
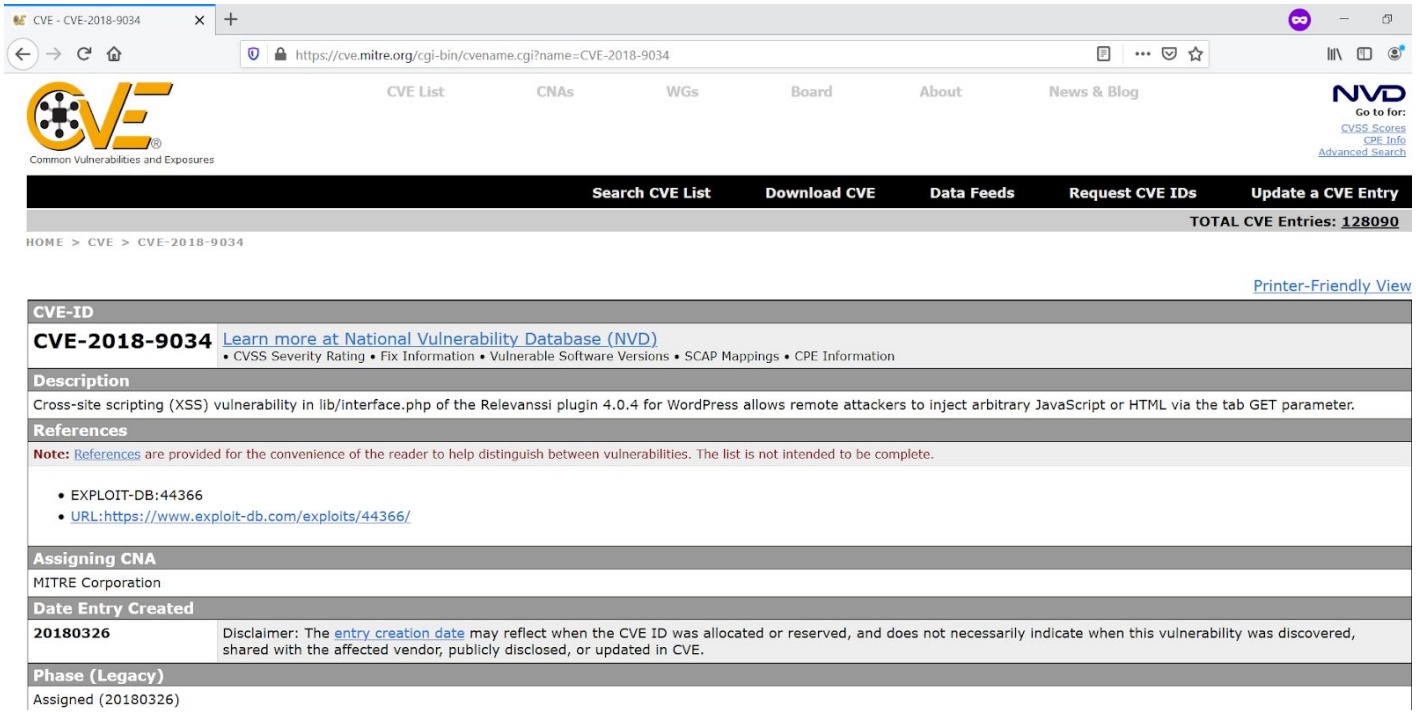

ATTACK
DEFENSE
by PentesterAcademy

Name	CVE-2018-9034
URL	https://www.attackdefense.com/challengedetails?cid=1023
Type	Webapp CVEs : 2018

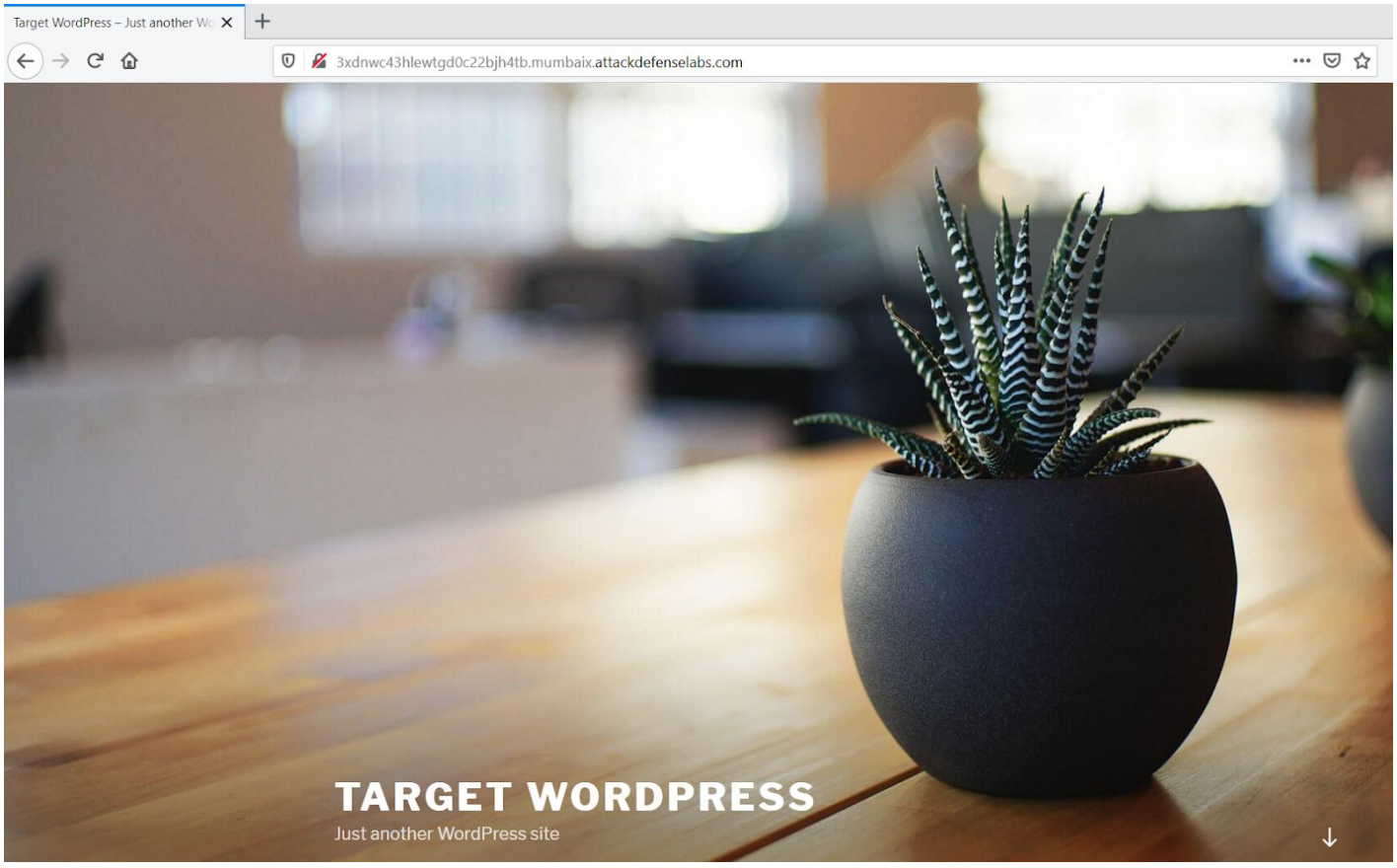
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

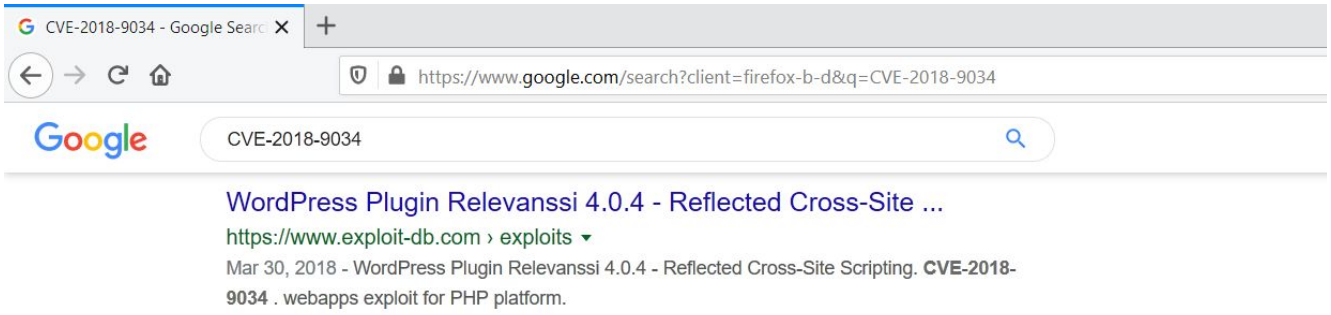
The web application is vulnerable to CVE-2018-9034



Step 1: Inspect the web application.

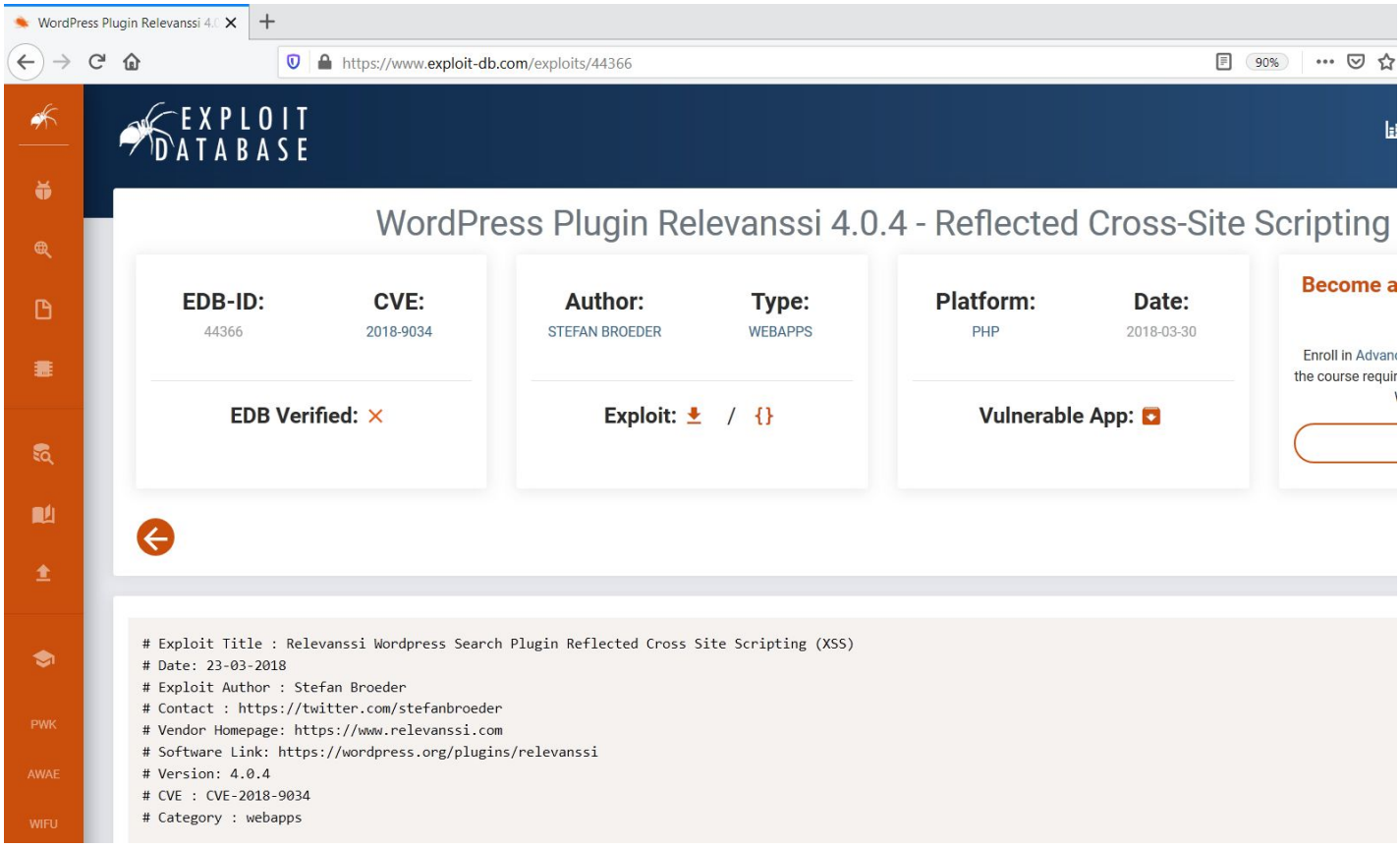


Step 2: Search on google “CVE-2018-9034”.



The exploit db link contains the steps to be followed to exploit the vulnerability.

Exploit DB Link: https://www.exploit-db.com/exploits/44366



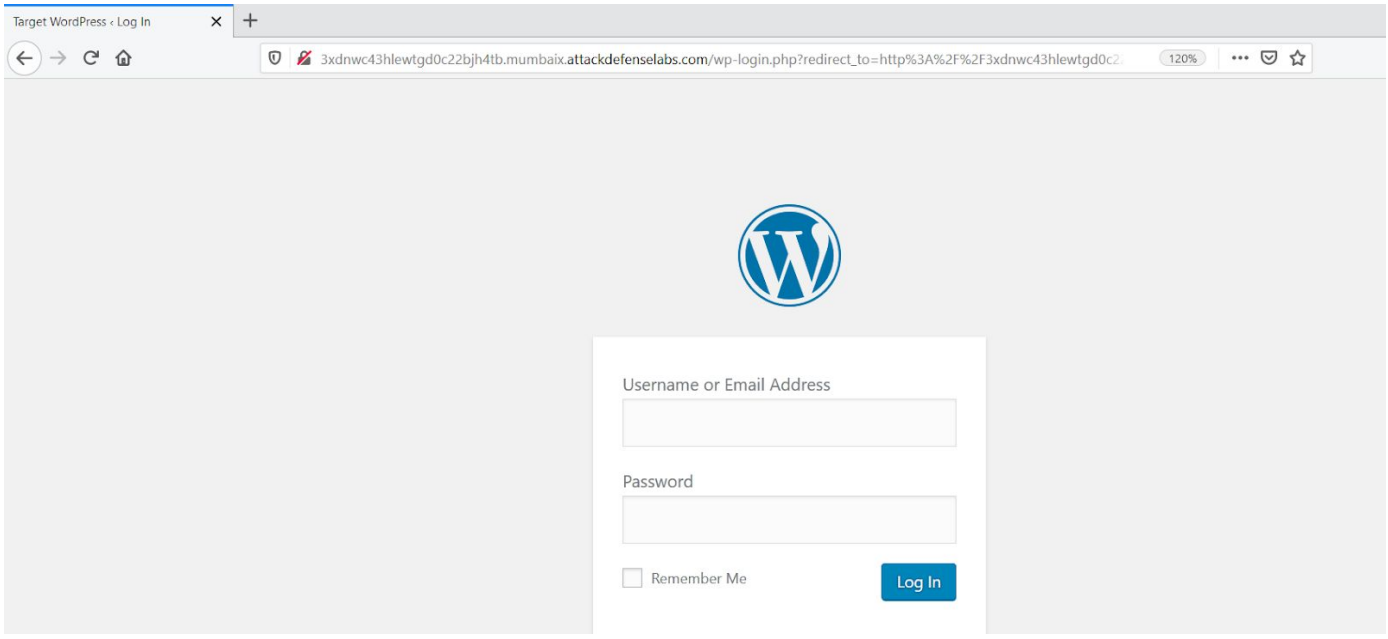
Step 3: The user has to authenticate in order to exploit the vulnerability. Credentials are provided in the challenge description.

Credentials:

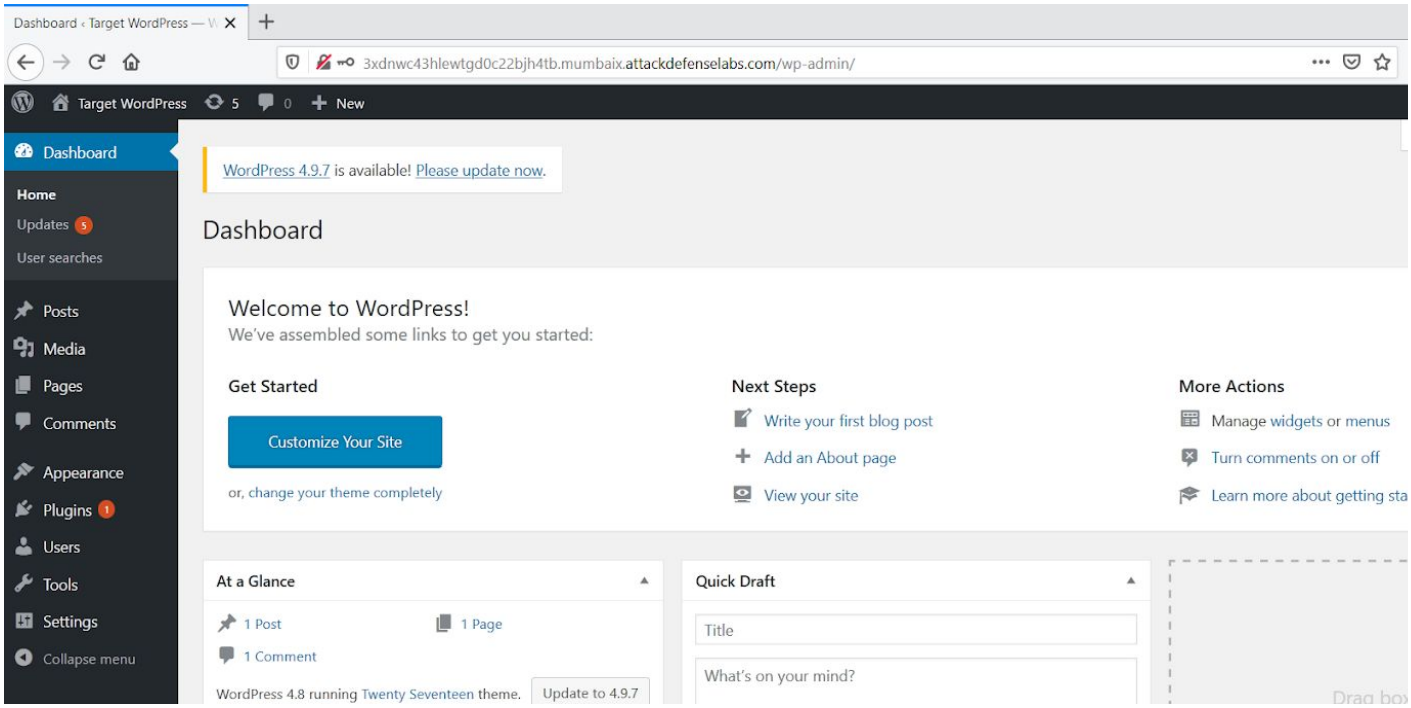
- **Username:** admin
- **Password:** password1

URL: http://3xdnwc43hlewtgd0c22bjh4tb.mumbaix.attackdefenselabs.com/wp-login.php

Admin Login:



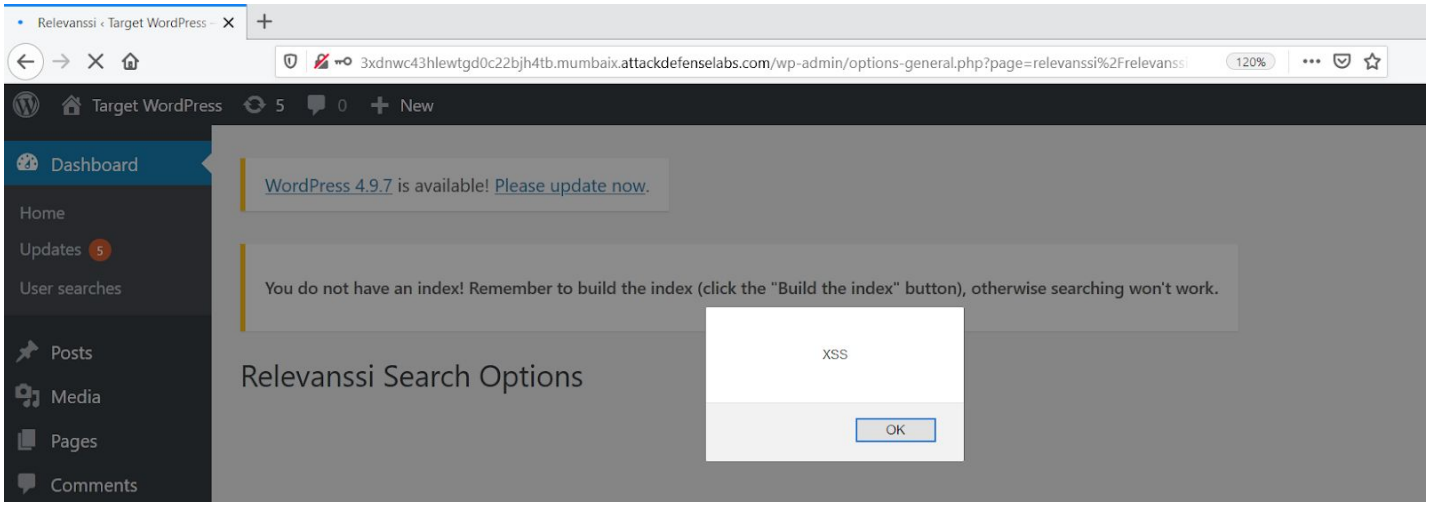
Admin Dashboard:



Step 4: Navigate to Vulnerable url and inject the payload in the URL.

Payload:
'><SCRIPT>var+x+%3D+String(%2FXSS%2F)%3Bx+%3D+x.substring(1%2C+x.length-1)%3Balert(x)<%2FSCRIPT><BR+

URL:
http://3xdnwc43hlewtgd0c22bjh4tb.mumbaix.attackdefenselabs.com/wp-admin/options-general.php?page=relevanssi%2Frelevanssi.php&tab=%27%3E%3CSCRIPT%3Evar+x+%3D+String%28%2FXSS%2F%29%3Bx+%3D+x.substring%281%2C+x.length-1%29%3Balert%28x%29%3C%2FSCRIPT%3E%3CBR+



The XSS attack was successful.

References:

1. Wordpress (http://wordpress.org/)
2. WordPress Plugin Relevanssi (https://wordpress.org/plugins/relevanssi)
3. CVE-2018-9034 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9034)
4. WordPress Plugin Relevanssi 4.0.4 - Reflected Cross-Site Scripting (https://www.exploit-db.com/exploits/44366)