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

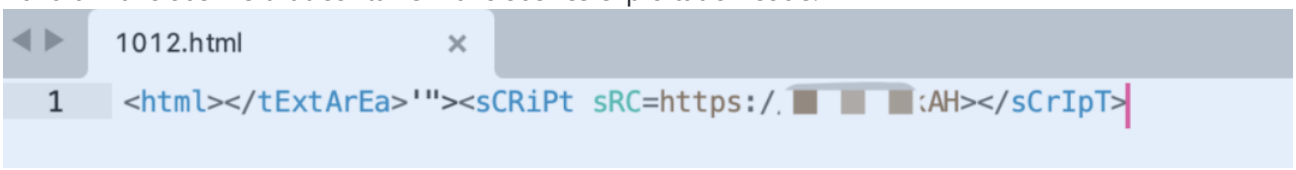
After logging in to the sra-admin background, you can add an html page containing xss attack code in "Personal Center" - "Profile Picture Upload" during the upload process, which can cause remote attackers to steal the user's personal information, or even phishing.

References

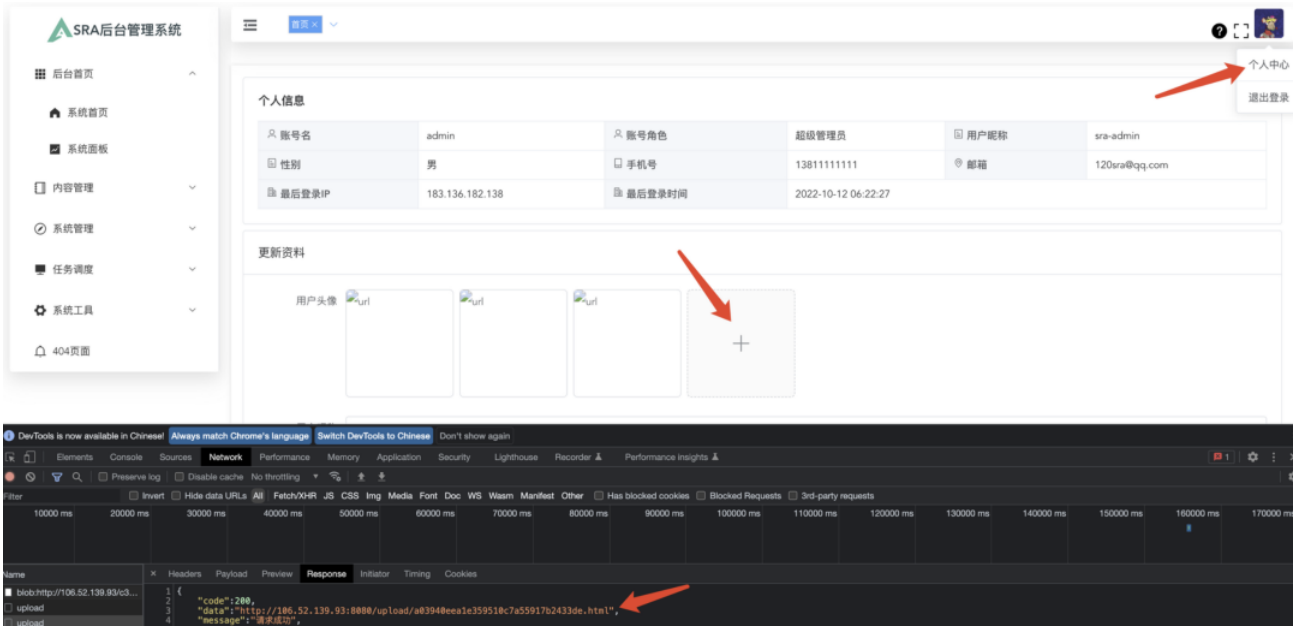
None

For more information

Build a malicious file that contains malicious xss exploitation code.



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.

Severity

High

CVE ID

CVE-2022-39201

CVE-2022-39301

Weaknesses

CWE-80 CWE-434

Credits

LuckyT0mat0