New issue

Jump to bottom

There are multiple reflective XSS vulnerabilities in the website #840

Closed kpa1on opened this issue on Mar 2 · 1 comment

Labels enhancement

kpa1on commented on Mar 2

Vulnerability name：Reflective XSS

Vulnerability level：Medium risk

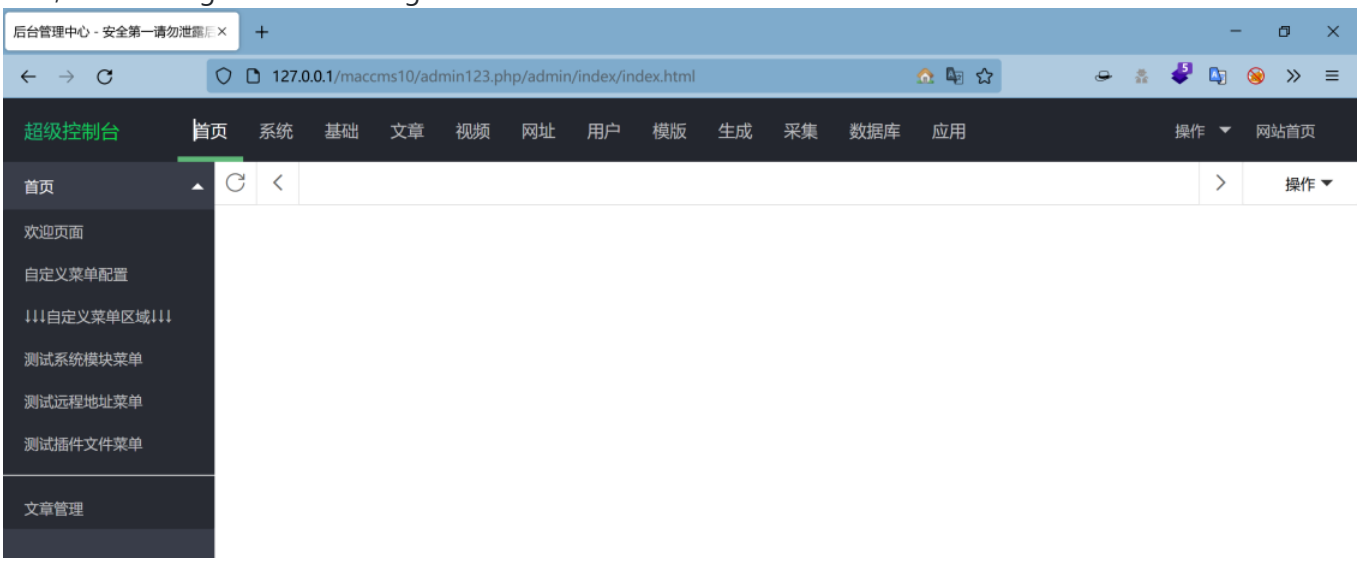
Affected version：v2021.1000.1081<=v2022.1000.3029

Vulnerability location：Many places，Here are some places I found
1、url：http://127.0.0.1/maccms10/admin.php/admin/art/data.html?select=&input=&type=&status=&level=&lock=&pic=&order=&wd= Affected parameters：select & input
2、url：http://127.0.0.1maccms10/admin.php/admin/website/data.html?select=&input=&type=&status=&level=&lock=&pic=&order=&wd= Affected parameters：select & input
3、url：http://127.0.0.1maccms10/admin.php/admin/plog/index.html?type=&wd= Affected parameters：wd
4、url：http://127.0.0.1maccms10/admin.php/admin/ulog/index.html?mid=&type=&wd= Affected parameters：wd
5、url：http://127.0.0.1maccms10/admin.php/admin/vod/data.html?repeat= Affected parameters：repeat

Verification process：

Get administrator cookies through reflective XSS：

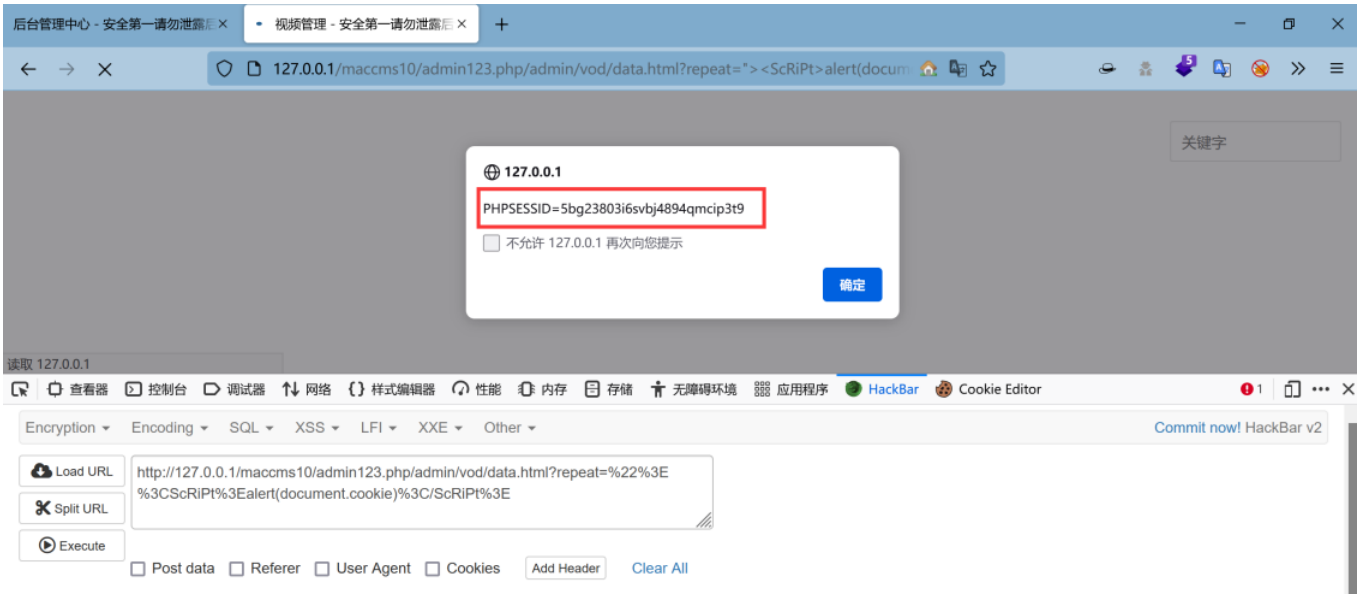
First, the user logs in to the background



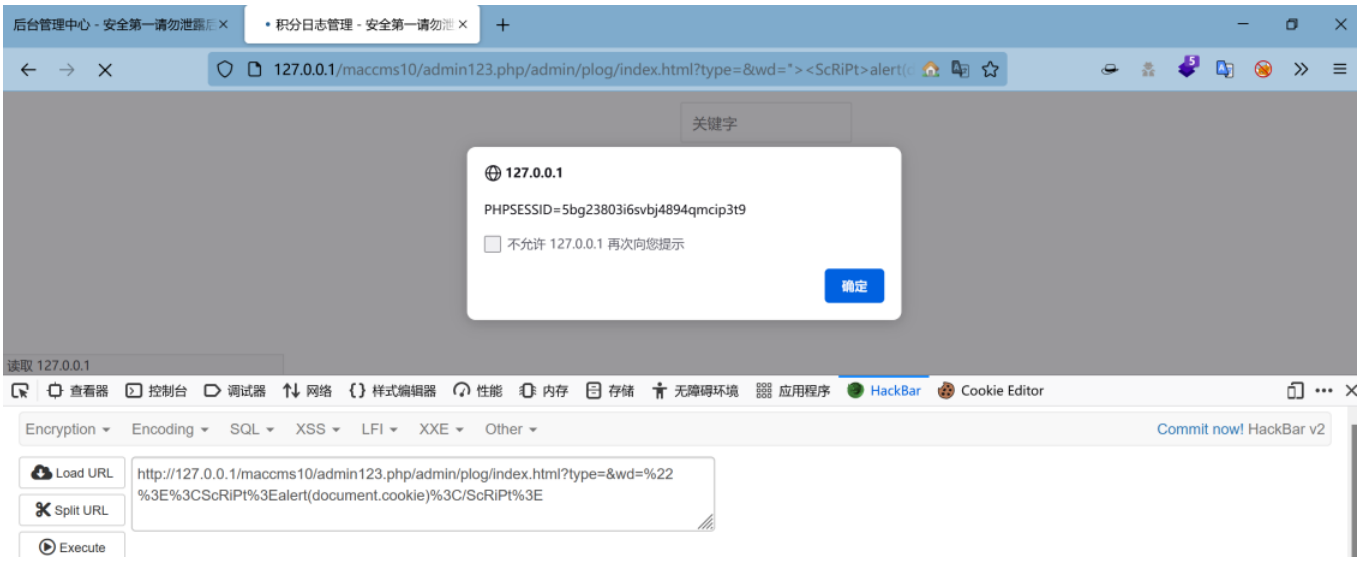
Then we make a payad that can get cookies by using the vulnerable URL， Send it to the victim or make it run by other means.

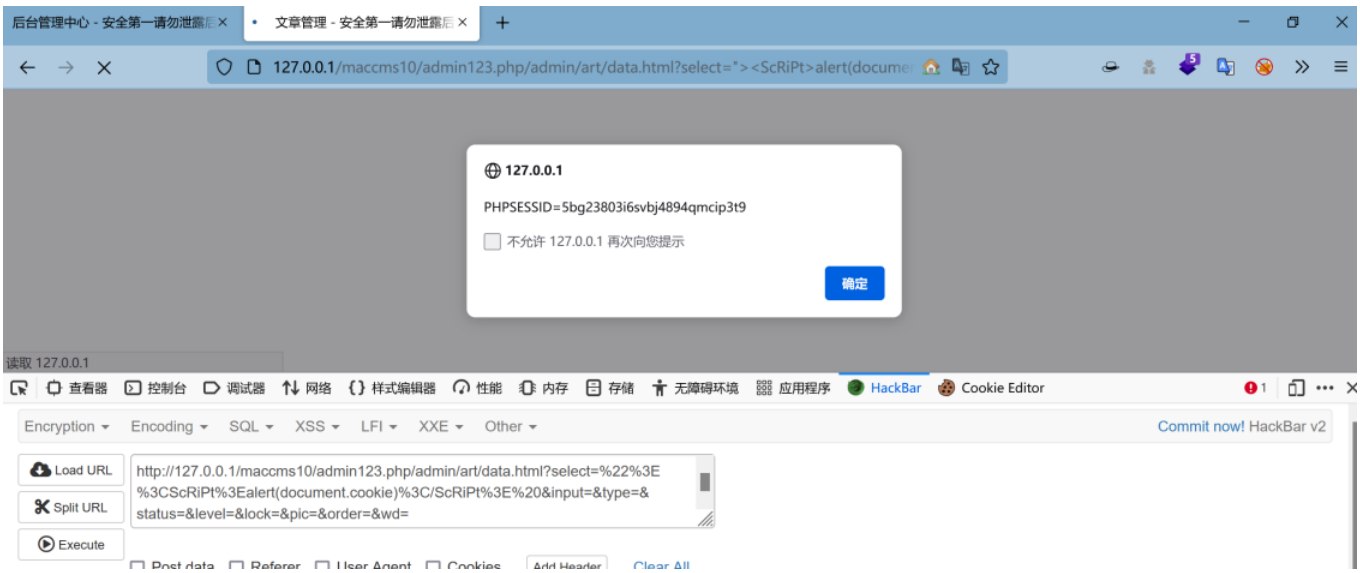
For example, here I choose this URL：[http://127.0.0.1/maccms10/admin123.php/admin/vod/data.html?repeat=%22%3E%3CScRiPt%3Ealert(document.cookie)%3C/ScRiPt%3E]

After the victim clicks, the cookie pops up successfully. Here, the XSS platform can also be used to accept the cookie.



Other URLs are the same：





Repair method：
【1】HTML escape the input data so that it is not recognized as an executable script
【2】Filter the data according to the tags and attributes of the whitelist to clear the executable script (such as script tag, oneror attribute of img tag, etc.)

magicblack added the **enhancement** label on Mar 4

magicblack commented on Mar 4 — Owner

thanks, will check and fix

magicblack closed this as completed in `026a289` on Mar 16

Assignees

Assignees

No one assigned

Labels

enhancement

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants