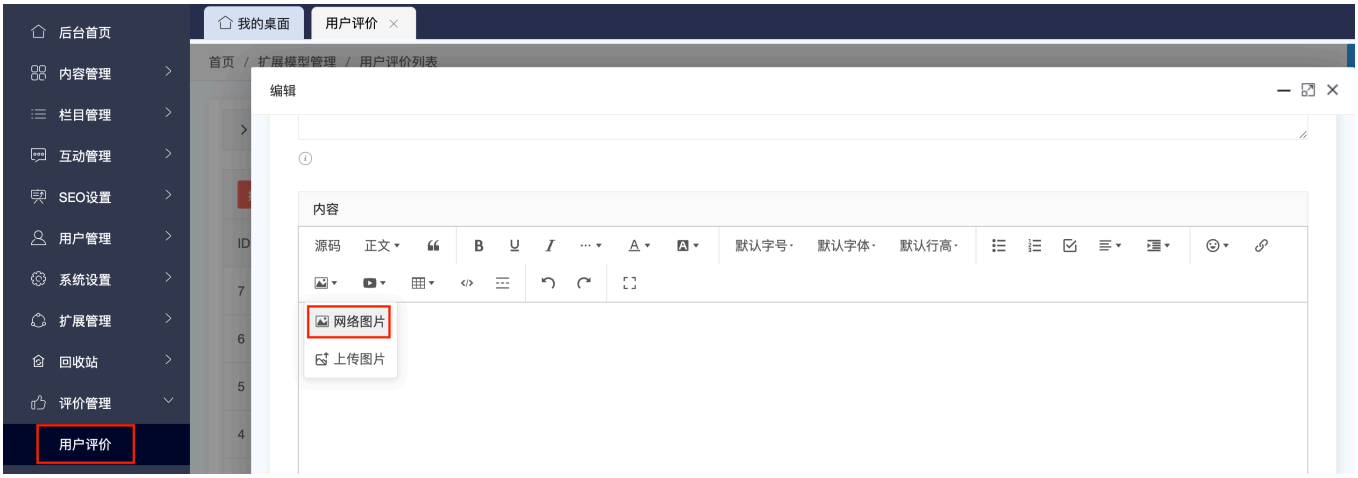
New issue

Jizhicms v2.5.4 is vulnerable to SSRF in User Evaluation, Message, and Comment modules. #104

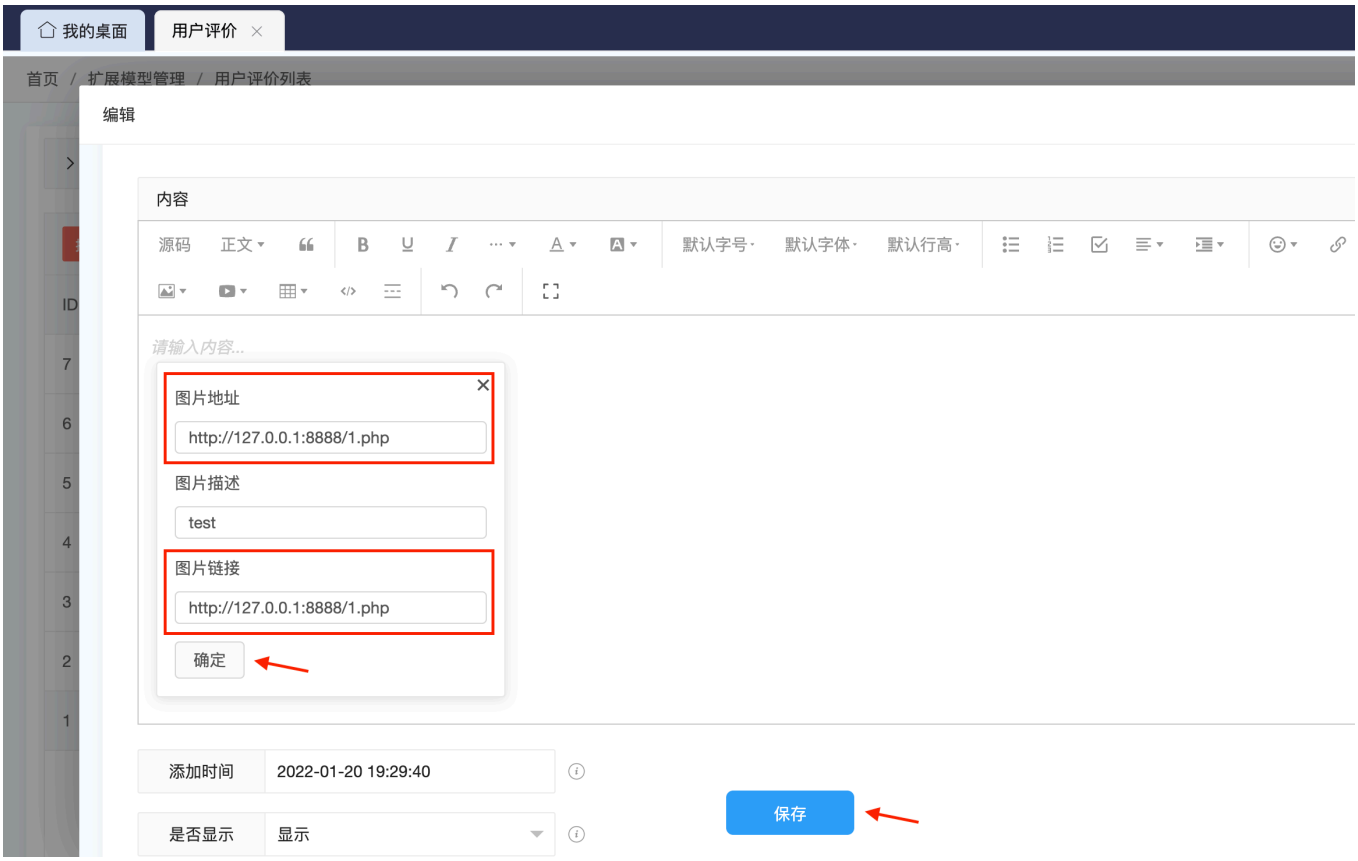
Closed

4iFei opened on Apr 22, 2025

The user evaluation module in Jizhicms backend can import network images：



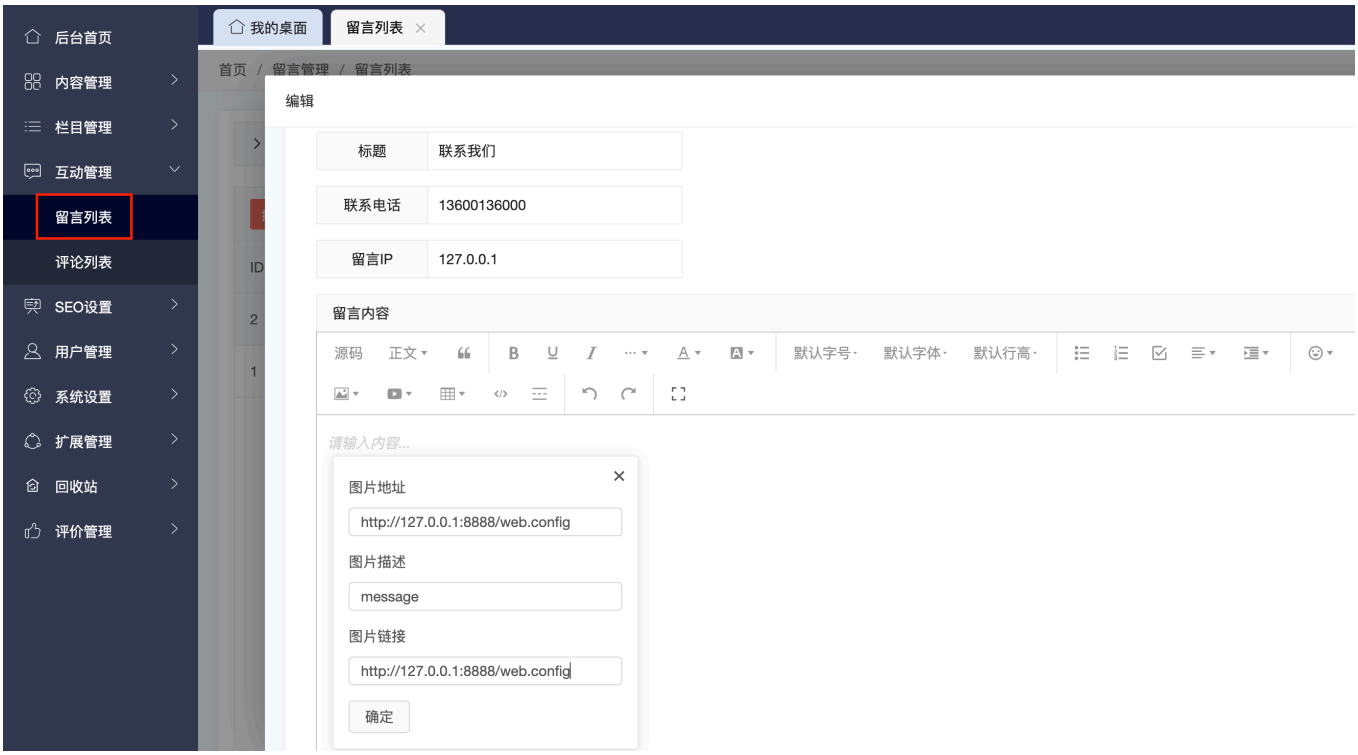
There are no restrictions imposed on URLs at the image address and image link, allowing us to input internal network addresses and leverage the server-side to dispatch probing requests into the internal network. Finally, save the content, and the SSRF vulnerability will be triggered.



Then we can see that the local web service has successfully received the request.

```
C:\phpstudy_pro\WWW>python -m http.server 8888
Serving HTTP on :: port 8888 (http://[::]:8888/) ...
::ffff:127.0.0.1 - - [22/Apr/2025 10:12:20] "GET /1.php HTTP/1.0" 200 -
::ffff:127.0.0.1 - - [22/Apr/2025 10:12:20] "GET /1.php HTTP/1.0" 200 -
```

The same issue also exists in the message and comment functions, which can import network images, so they also have SSRF vulnerabilities.




```
C:\phpstudy_pro\WWW>python -m http.server 8888
Serving HTTP on :: port 8888 (http://[::]:8888/) ...
::ffff:127.0.0.1 - - [22/Apr/2025 10:26:22] "GET /web.config HTTP/1.0" 200 -
::ffff:127.0.0.1 - - [22/Apr/2025 10:26:22] "GET /web.config HTTP/1.0" 200 -
```

Cherry-toto on Aug 20, 2025 Owner • • •

后台的漏洞暂时可能不会处理，如果你能进入后台，那已经获取了**超级权限**，所以这个无意义。

Cherry-toto closed this as completed on Aug 20, 2025

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants