



If the port is shut down, it will take more than two thousand Milliseconds, if the port is not enabled, the request takes almost twice as long.

程序正在执行中...

程序正在初始化...

[hunter] 未抓取到任何内容, 请确保连接[http://127.0.0.1:8007/testSSRF2333333]是否正在运行

[hunter] bye~~



Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成, 签署流程更高效
- 📄 内置可自定义的协议模板
- 👤 让开源贡献也能有据可依

I know

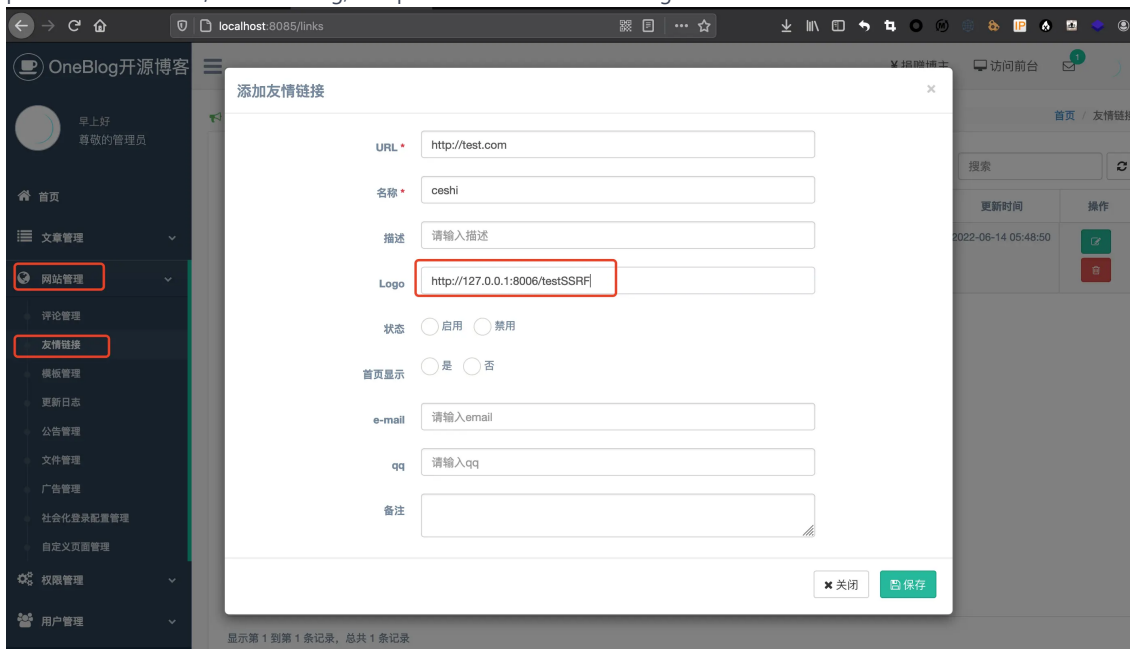
View Details

The request record for the HTTP server is as follows:

```
127.0.0.1 - - [14/Jun/2022 04:51:52] "GET /testSSRF2333333 HTTP/1.1" 404 -
127.0.0.1 - - [14/Jun/2022 04:53:17] code 404, message File not found
127.0.0.1 - - [14/Jun/2022 04:53:17] "GET /testSSRF2333333 HTTP/1.1" 404 -
127.0.0.1 - - [14/Jun/2022 04:53:18] code 404, message File not found
127.0.0.1 - - [14/Jun/2022 04:53:18] "GET /testSSRF2333333 HTTP/1.1" 404 -
```

The second SSRF vulnerability

After logging in, click website Management-> Link module, add a link, and enter the URL of the test at the Logo parameter. Click Save, When saving, a request will be made to the target URL



Then refreshing the link will also request the target URL.

Then check the access record of the HTTP service

```
$ python -m SimpleHTTPServer 8006
Serving HTTP on 0.0.0.0 port 8006 ...
127.0.0.1 - - [14/Jun/2022 08:17:37] code 404, message File not found
127.0.0.1 - - [14/Jun/2022 08:17:37] "GET /testSSRF HTTP/1.1" 404 -
```



[Sign in to comm](#)



©OSCHINA. All rights reserved

[Git Resources](#)

[Learning Git](#)

[CopyCat](#)

[Downloads](#)

[Gitee Reward](#)

[Gitee Stars](#)

[Featured Projects](#)

[Blog](#)

[Nonprofit](#)

[Gitee Go](#)

[OpenAPI](#)

[Help Center](#)

[Self-services](#)

[Updates](#)



Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👉 让开源贡献也能有据可依

[I know](#)

[View Details](#)

777320883

git@oschina.cn

Gitee

+86 400-606-0201



Mini Program

