yadong.zhang / OneBlog

Watch 532 Star 4.5K

Gitee Pages
JavaDoc
sonarqube Quality Analysis
Jenkins for Gitee
Baidu Efficiency Cloud
Tencent CloudBase
Tencent Cloud Serverless
OPENSCA 悬镜安全

Don't show this again

Issues / 详情

OneBlog v2.3.4 background SSRF vulnerability

○ Backlog #I5CB2A qumh Opened this issue 2022-06-15 00:3

vulnerability Abstract

There are two SSRF vulnerabilities in OneBlog v2.3.4, one in adding frienc
function, which can be exploited by attackers to initiate probes on intran

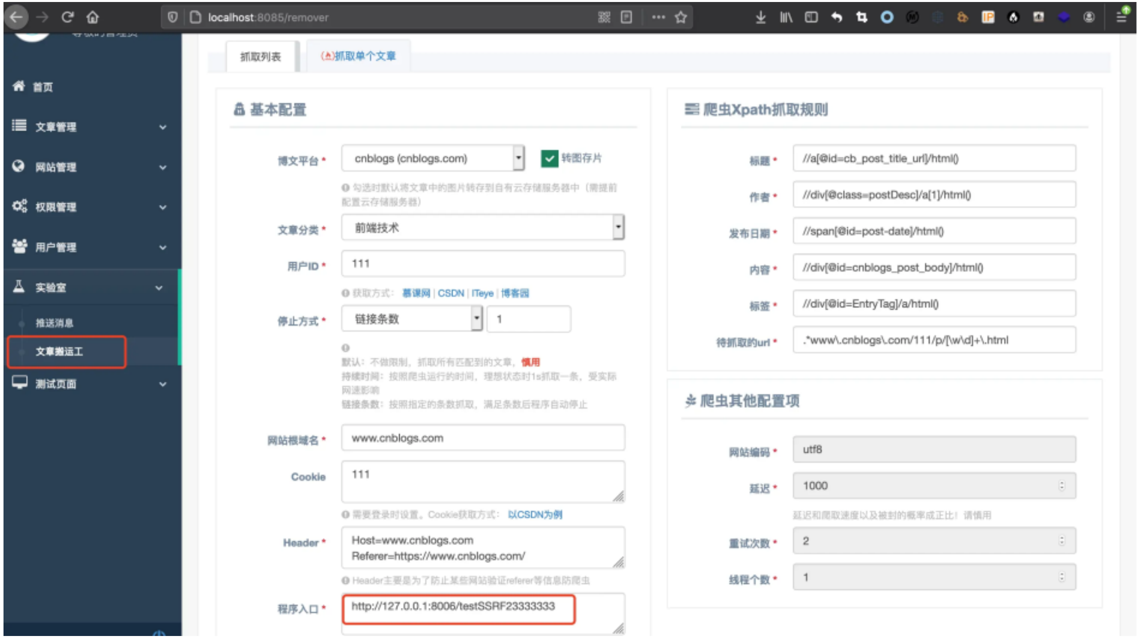
Scope of influence

OneBlog v2.3.4

vulnerability Reappearance

The first SSRF vulnerability:

To log in to the system using the account password root/123456, click Lab-> Article Porter Module



基本配置

博文平台 * cnblogs (cnblogs.com) ☑ 转图存片
勾选时默认将文章中的图片转存到自有云存储服务器中（需提前配置云存储服务器）
文章分类 * 前端技术
用户ID * 111
获取方式： 慕课网 | CSDN | ITeye | 博客园
停止方式 * 链接条数 1
默认：不做限制，抓取所有匹配到的文章，慎用
持续时间：按照爬虫运行的时间，理想状态时1s抓取一条，受实际网速影响
链接条数：按照指定的条数抓取，满足条数后程序自动停止
网站根域名 * www.cnblogs.com
Cookie 111
需要登录时设置。Cookie获取方式： 以CSDN为例
Header * Host=www.cnblogs.com
Referer=https://www.cnblogs.com/
Header主要是为了防止某些网站验证referer等信息防爬虫
程序入口 * http://127.0.0.1:8006/testSSRF23333333

爬虫Xpath抓取规则

标题 * //a[@id=cb_post_title_url]/html()
作者 * //div[@class=postDesc]/a[1]/html()
发布日期 * //span[@id=post-date]/html()
内容 * //div[@id=cnblogs_post_body]/html()
标签 * //div[@id=EntryTag]/a/html()
待抓取的url * .*www\.cnblogs\.com/111/p/[\w\d]+\.html

爬虫其他配置项

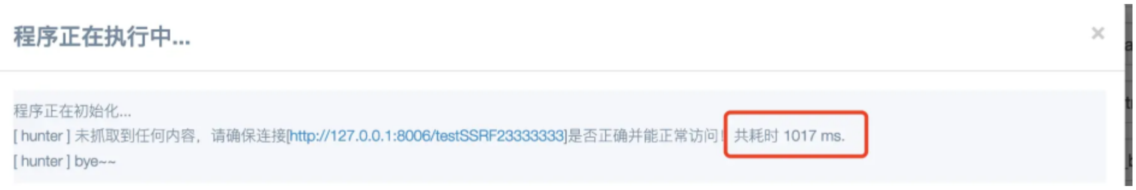
网站编码 * utf8
延迟 * 1000
延迟和爬取速度以及被封的概率成正比！ 请慎用
重试次数 * 2
线程个数 * 1

Vulnerability parameter：entryUrls

We can use python to set up a HTTP service as the target server，Judge whether the service is enabled according to the response result of the server accessing the target URL

This vulnerability can realize the function of intranet port detection, access different ports, open echoes will be different

If the port is open, it will take more than a thousand Millisecond



```
程序正在初始化...
[ hunter ] 未抓取到任何内容，请确保连接[http://127.0.0.1:8006/testSSRF23333333]是否正确并能正常访问！共耗时 1017 ms.
[ hunter ] bye~~
```

Status

Backlog

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull reque
issue.

Branches

No related branch

Planed to start - Planed t

Unscheduled - Unschedule

Top level

Not Top

Priority

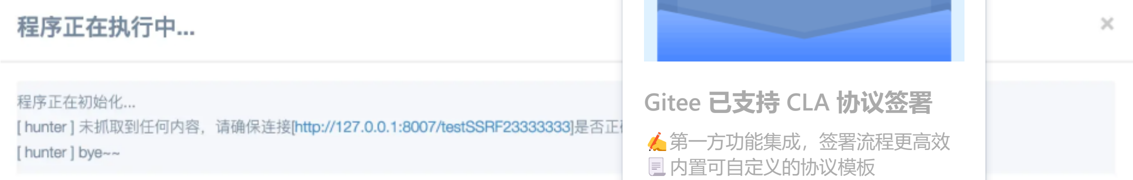
Not specified

参与者 (2)

S Q

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

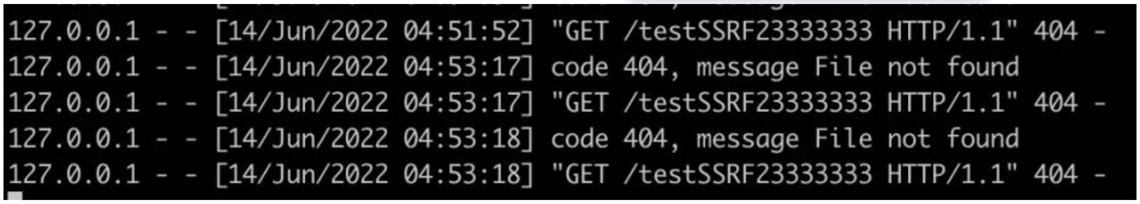
If the port is shut down, it will take more than two thousand Millise
s not enabled, the request takes almost twice as long.



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/testSSRF23333333]是否正
[ hunter ] bye~~
```

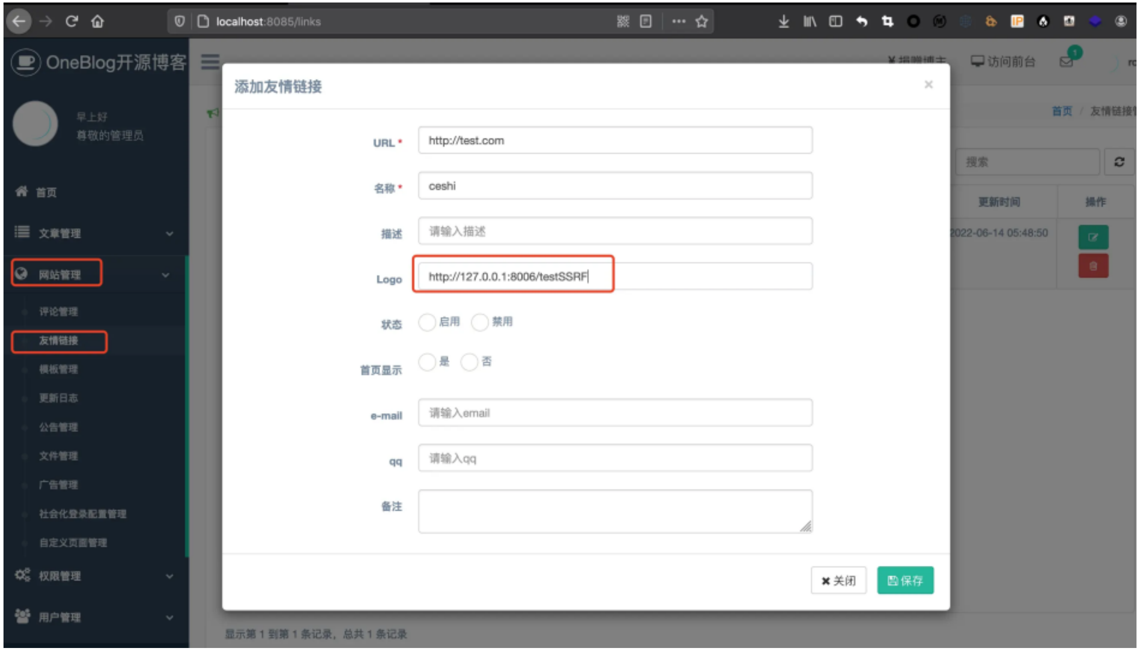
The request record for the HTTP server is as follows:



```
127.0.0.1 - - [14/Jun/2022 04:51:52] "GET /testSSRF23333333 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 /testSSRF23333333 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 /testSSRF23333333 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



localhost:8085/links
OneBlog开源博客
早上好
尊敬的管理员
首页
文章管理
网站管理
评论管理
友情链接
模板管理
更新日志
公告管理
文件管理
广告管理
社会化登录配置管理
自定义页面管理
权限管理
用户管理
访问前台
首页 / 友情链接
搜索
更新时间
操作
2022-06-14 05:48:50
显示第 1 到第 1 条记录，总共 1 条记录

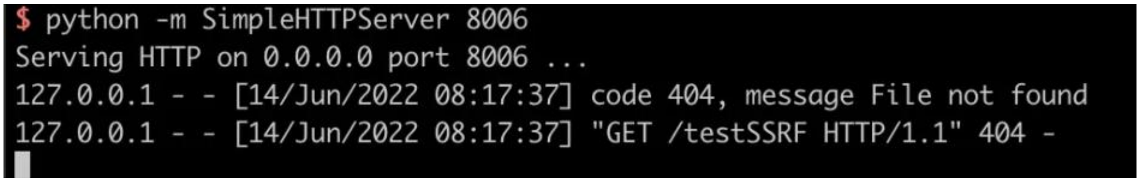
添加友情链接

URL * http://test.com
名称 * ceshi
描述 请输入描述
Logo http://127.0.0.1:8006/testSSRF
状态 ○ 启用 ○ 禁用
首页显示 ○ 是 ○ 否
e-mail 请输入email
qq 请输入qq
备注

✖ 关闭 保存

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 -
```

qumh created **任务** 5 months ago Expand operation logs

SSJT 4 months ago

Sign in to comm

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