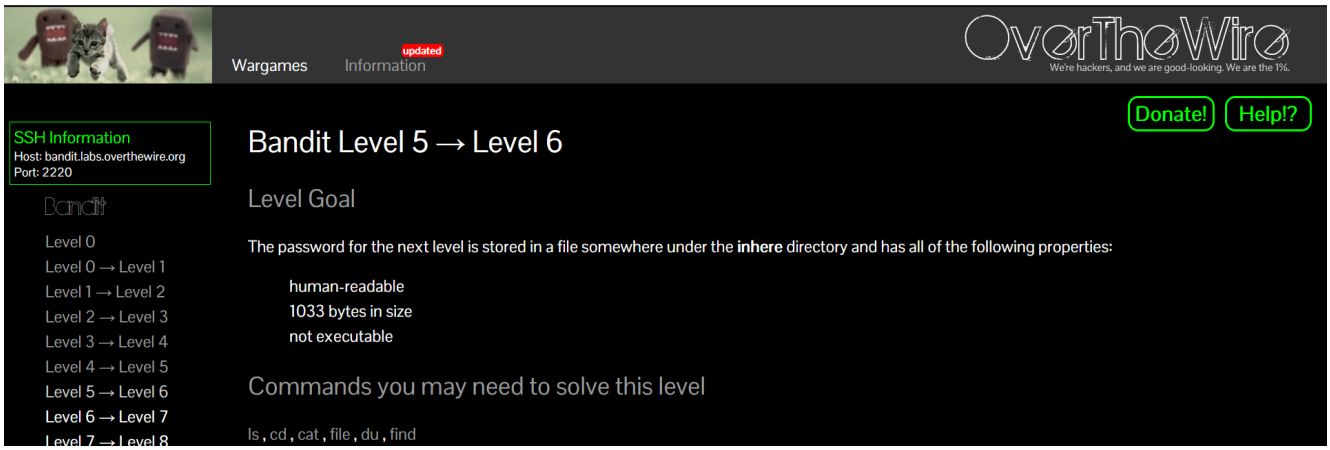
Bandit Level 5 —> Level 6

SSH Parameters	
Host:	bandit.labs.overthewire.org
Port:	2220

Website URLs	
Level 5 → Level 6	OverTheWire: Level Goal: Bandit Level 5 → Level 6
Level 6 → Level 7	OverTheWire: Level Goal: Bandit Level 6 → Level 7

Passwords		
Level	User Name	Password
Level 5 → Level 6	bandit5	lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
Level 6 → Level 7	bandit6	P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU




```
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$ #id and whoami command to verify log in to bandit5/level5
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$
bandit5@bandit:~$ id && whoami
uid=11005(bandit5) gid=11005(bandit5) groups=11005(bandit5)
bandit5
bandit5@bandit:~$
bandit5@bandit:~$
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$ #pwd to assess if we are in bandit5 home directory
bandit5@bandit:~$ #ls to determine if the inhere directory is within bandit5 home directory
bandit5@bandit:~$ #if inhere directory is present execute cd command to navigate there
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$
bandit5@bandit:~$ pwd
/home/bandit5
bandit5@bandit:~$
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$
```

```
bandit5@bandit:~/inhere$ ##########################################################################################################
#
bandit5@bandit:~/inhere$ #ls command to view contents of inhere directory
bandit5@bandit:~/inhere$ ##########################################################################################################
#
bandit5@bandit:~/inhere$
bandit5@bandit:~/inhere$ ls -la
total 88
drwxr-x--- 22 root bandit5 4096 Apr 23 18:04 .
drwxr-xr-x  3 root root    4096 Apr 23 18:04 ..
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere00
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere01
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere02
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere03
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere04
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere05
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere06
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere07
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere08
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere09
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere10
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere11
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere12
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere13
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere14
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere15
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere16
```

```
bandit5@bandit:~/inhere$ ##########################################################################################################
bandit5@bandit:~/inhere$ #There are 3 (three) methodologies with which to solve this level.  Note: If you used a different m
ethod to solve the level please comment
bandit5@bandit:~/inhere$ #
bandit5@bandit:~/inhere$ #First Method - Utilization of the du command and grep for 1033 (file size)
bandit5@bandit:~/inhere$ #Second Method - Use the ls -la command, grep for 1033 and then use the find command (utilizing fil
e size and file name) to locate the full path of the password file
bandit5@bandit:~/inhere$ #Third Method - Utilization of the find command by inputting the following parameters (A) File Size
 of 1033 (B) File is not executale (C) File is human readable
bandit5@bandit:~/inhere$ ##########################################################################################################
```

```
bandit5@bandit:~/inhere$ ##########################################################################################################
bandit5@bandit:~/inhere$ #METHOD 1 - UTILIZATION OF THE DU COMMAND
bandit5@bandit:~/inhere$ ##########################################################################################################
bandit5@bandit:~/inhere$
bandit5@bandit:~/inhere$ ##########################################################################################################
bandit5@bandit:~/inhere$ #The du command lists file size of directories
bandit5@bandit:~/inhere$ #Initizlization of the -a option/switch puts the command in recursive mode and provides sizes of fi
les
bandit5@bandit:~/inhere$ #Initialization of the -b option/switch outputs the size of files/directories in bytes
bandit5@bandit:~/inhere$ ##########################################################################################################
bandit5@bandit:~/inhere$
bandit5@bandit:~/inhere$ du -ab
9064    ./maybehere07/spaces file2
1033    ./maybehere07/.file2
3663    ./maybehere07/-file1
1022    ./maybehere07/spaces file3
1997    ./maybehere07/.file3
3362    ./maybehere07/-file3
4130    ./maybehere07/spaces file1
2488    ./maybehere07/-file2
3065    ./maybehere07/.file1
33920   ./maybehere07
3146    ./maybehere16/spaces file2
8472    ./maybehere16/.file2
4277    ./maybehere16/-file1
7509    ./maybehere16/spaces file3
```

```
bandit5@bandit:~$ du -ab | grep 1033
1033    ./inhere/maybehere07/.file2
bandit5@bandit:~$
bandit5@bandit:~$
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$ #The command above, du -ab | grep 1033, output the file/filepath to the Level 6 password.
bandit5@bandit:~$ #The next step will be to extract the filepath/file so we may cat itand retrieve the password
bandit5@bandit:~$ #We will utilize the cut command with options/switches -d " " [delineate on space], -f 2 [to grab the seco
nd file [filepath and directory]]
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$
```

```
bandit5@bandit:~$ #grep 1033 (for file(s) with a size of 1033 bytes) by using the input from du -ab
bandit5@bandit:~$ #command for the above is:
bandit5@bandit:~$ # du -ab | grep 1033
bandit5@bandit:~$
bandit5@bandit:~$ ls inhere/
maybehere00  maybehere03  maybehere06  maybehere09  maybehere12  maybehere15  maybehere18
maybehere01  maybehere04  maybehere07  maybehere10  maybehere13  maybehere16  maybehere19
maybehere02  maybehere05  maybehere08  maybehere11  maybehere14  maybehere17
bandit5@bandit:~$
bandit5@bandit:~$ du -ab | grep 1033
1033    ./inhere/maybehere07/.file2
```

```
bandit5@bandit:~$ du -ab | grep 1033
1033    ./inhere/maybehere07/.file2
bandit5@bandit:~$
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$ #We attempted to pipe the output of the du command to the cut command and parse the filepath and name via
the delineate [-d " "] option/switch on space and the option/switch to harvest the second field [-f 2].  This was not succes
sful as the string did not parse.
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$
bandit5@bandit:~$ du -ab | grep 1033 | cut -d " " -f 2
1033    ./inhere/maybehere07/.file2
bandit5@bandit:~$
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$ #We then copied the output of the du command, outputed it via echo, and successfully parsed the filepath/f
ile name on space [-d " "] and field [-f 2] as noted below.
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$
bandit5@bandit:~$ echo 1033     ./inhere/maybehere07/.file2 | cut -d " " -f 2
./inhere/maybehere07/.file2
bandit5@bandit:~$
```

```
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$ #To successfully parse the filepath/file name the echo command was utilized to output the contents of the
du command and its pipe to grep.  This output ws then parsed by the cut command with option/switch d to deleniate on space [
-d " "] and the f option/switch to extract the second field of the string [filepath and filename] [-f 2].
bandit5@bandit:~$
bandit5@bandit:~$ echo $(du -ab | grep 1033) | cut -d " " -f 2
./inhere/maybehere07/.file2
bandit5@bandit:~$
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$ #To extract the password the command above is encased in the cat command to read the file and output the L
evel 6 password
bandit5@bandit:~$
bandit5@bandit:~$ cat $(echo $(du -ab | grep 1033) | cut -d " " -f 2)
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

```
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$ #METHOD 2 - Utilization of the ls -alR command
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$
bandit5@bandit:~$ #The cd inhere command changes the current directory to inhere
bandit5@bandit:~$ #The ls -laR command is then executed (on the inhere directory) to output a listing of all folders/files (
recursively)
bandit5@bandit:~$
bandit5@bandit:~$ ##########################################################################################################
bandit5@bandit:~$
bandit5@bandit:~$ cd inhere && ls -alR
.:
total 88
drwxr-x--- 22 root bandit5 4096 Apr 23 18:04 .
drwxr-xr-x  3 root root    4096 Apr 23 18:04 ..
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere00
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere01
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere02
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere03
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere04
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere05
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere06
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere07
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere08
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere09
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere10
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere11
```

```
./maybehere00:
total 72
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 .
drwxr-x--- 22 root bandit5 4096 Apr 23 18:04 ..
-rwxr-x---  1 root bandit5 1039 Apr 23 18:04 -file1
-rwxr-x---  1 root bandit5  551 Apr 23 18:04 .file1
-rw-r-----  1 root bandit5 9388 Apr 23 18:04 -file2
-rw-r-----  1 root bandit5 7836 Apr 23 18:04 .file2
-rwxr-x---  1 root bandit5 7378 Apr 23 18:04 -file3
-rwxr-x---  1 root bandit5 4802 Apr 23 18:04 .file3
-rwxr-x---  1 root bandit5 6118 Apr 23 18:04 spaces file1
-rw-r-----  1 root bandit5 6850 Apr 23 18:04 spaces file2
-rwxr-x---  1 root bandit5 1915 Apr 23 18:04 spaces file3

./maybehere01:
total 80
drwxr-x---  2 root bandit5 4096 Apr 23 18:04 .
drwxr-x--- 22 root bandit5 4096 Apr 23 18:04 ..
-rwxr-x---  1 root bandit5 6028 Apr 23 18:04 -file1
-rwxr-x---  1 root bandit5 8944 Apr 23 18:04 .file1
-rw-r-----  1 root bandit5  288 Apr 23 18:04 -file2
-rw-r-----  1 root bandit5 3070 Apr 23 18:04 .file2
-rwxr-x---  1 root bandit5 9641 Apr 23 18:04 -file3
-rwxr-x---  1 root bandit5 3792 Apr 23 18:04 .file3
-rwxr-x---  1 root bandit5 4139 Apr 23 18:04 spaces file1
-rw-r-----  1 root bandit5 4543 Apr 23 18:04 spaces file2
```

```
bandit5@bandit:~/inhere$ ########################################################################################################
bandit5@bandit:~/inhere$ #Pipe output of command ls -laR to grep command.  Grep for 1033 (size of file)
bandit5@bandit:~/inhere$
bandit5@bandit:~/inhere$ ls -alR | grep 1033
-rw-r-----  1 root bandit5 1033 Apr 23 18:04 .file2
bandit5@bandit:~/inhere$
bandit5@bandit:~/inhere$ ########################################################################################################
bandit5@bandit:~/inhere$ #Pipe the output of the above command to cut and invoke options -d to delineate the string on space
 [-d " "] and field [-f 10]
bandit5@bandit:~/inhere$
bandit5@bandit:~/inhere$ ls -alR | grep 1033 | cut -d " " -f 10
.file2
bandit5@bandit:~/inhere$
bandit5@bandit:~/inhere$ ########################################################################################################
bandit5@bandit:~/inhere$ #To find the file containing the password we utilize the find command and invoke the name [-name .f
ile2] and size [-size 1033c]
bandit5@bandit:~/inhere$
bandit5@bandit:~/inhere$ find -name .file2 -size 1033c
./maybehere07/.file2
```

```
bandit5@bandit:~/inhere$ #cat the file output from the find command above to output password to Level 6
bandit5@bandit:~/inhere$
bandit5@bandit:~/inhere$ cat $(find -name .file2 -size 1033c)
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

```
bandit5@bandit:~$ ########################################################################################################
bandit5@bandit:~$ #METHOD 3
bandit5@bandit:~$ ########################################################################################################
bandit5@bandit:~$
bandit5@bandit:~$ #The most efficient way to solve the Level 5 challenge is via the find command and invoking the following pa
rameters:
bandit5@bandit:~$ #Parameter 1: size 1033c (identifies files that are 1033 bytes)
bandit5@bandit:~$ #Parameter 2: -type f (to narrow the search for files and not include directories)
bandit5@bandit:~$ #Parameter 3: ! -executable (excludes executable files
bandit5@bandit:~$ #Note: the period (.) after find signifies to search all directories/levels (recursive search)
bandit5@bandit:~$
bandit5@bandit:~$ #command: find . -size 1033c -type f ! -executable
bandit5@bandit:~$
bandit5@bandit:~$ find . -size 1033c -type f ! -executable
./inhere/maybehere07/.file2
bandit5@bandit:~$
bandit5@bandit:~$ #cat output of cut command to output Level 6 password
bandit5@bandit:~$
bandit5@bandit:~$ cat $(find . -size 1033c -type f ! -executable)
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

****

Level 6 —> Level 7 Password

****

P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU