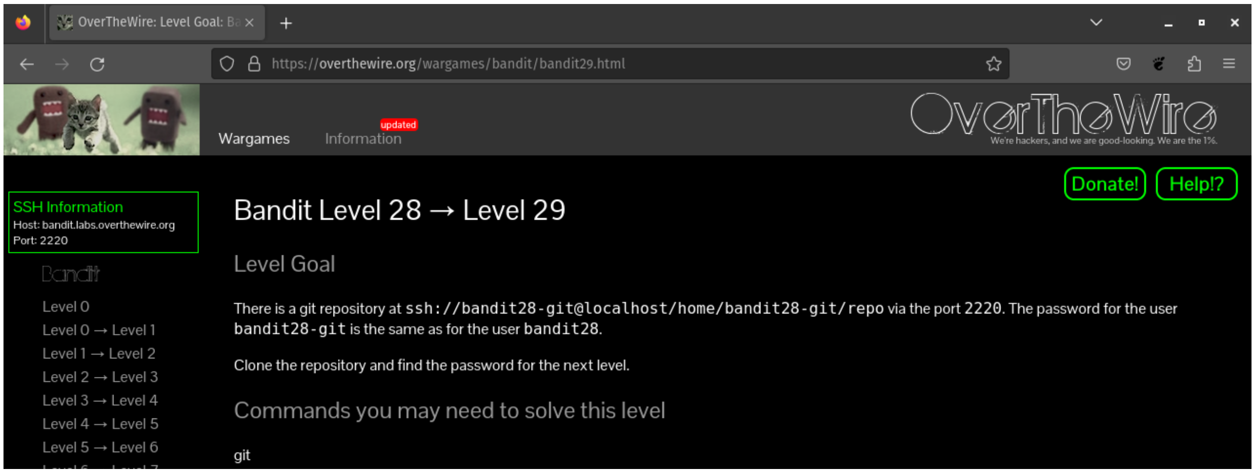
Bandit Level 28 —> Level 29

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

Website URLs	
Level 28—>29	[OverTheWire: Level Goal: Bandit Level 28 → Level 29]()
Level 29—>30	[OverTheWire: Level Goal: Bandit Level 29 → Level 30]()

Passwords		
Level	**User Name**	**Password**
Bandit 28—->29	bandit28	AVanL161y9rsbcJIsFHuw35rjaOM19nR
Bandit 29—->30	bandit29	tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S



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

Bandit Level 28 → Level 29

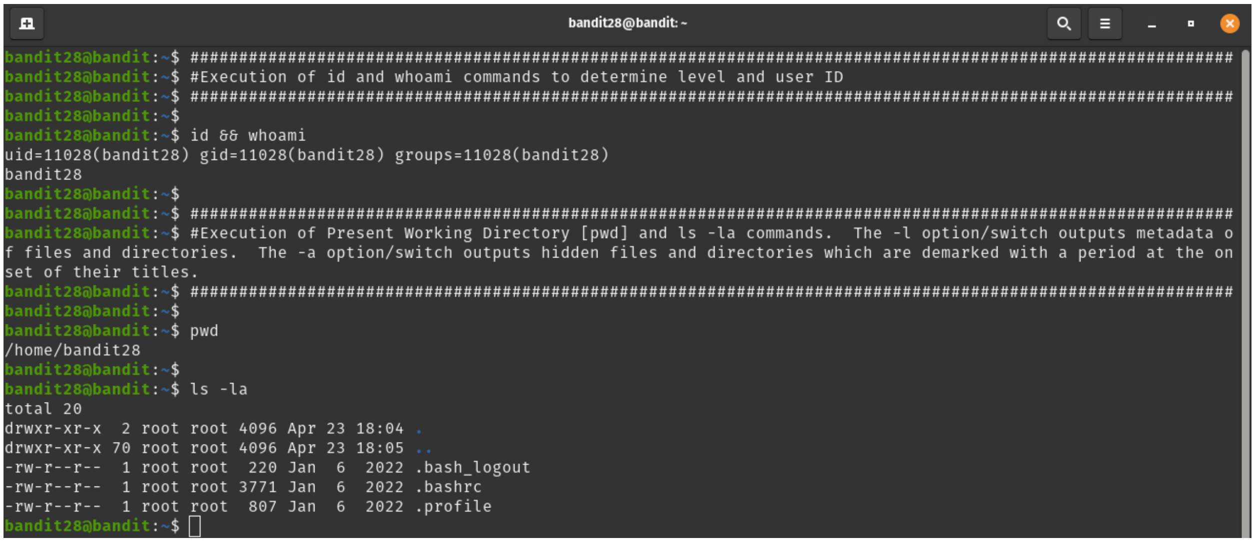
Level Goal

There is a git repository at `ssh://bandit28-git@localhost/home/bandit28-git/repo` via the port `2220`. The password for the user `bandit28-git` is the same as for the user `bandit28`.

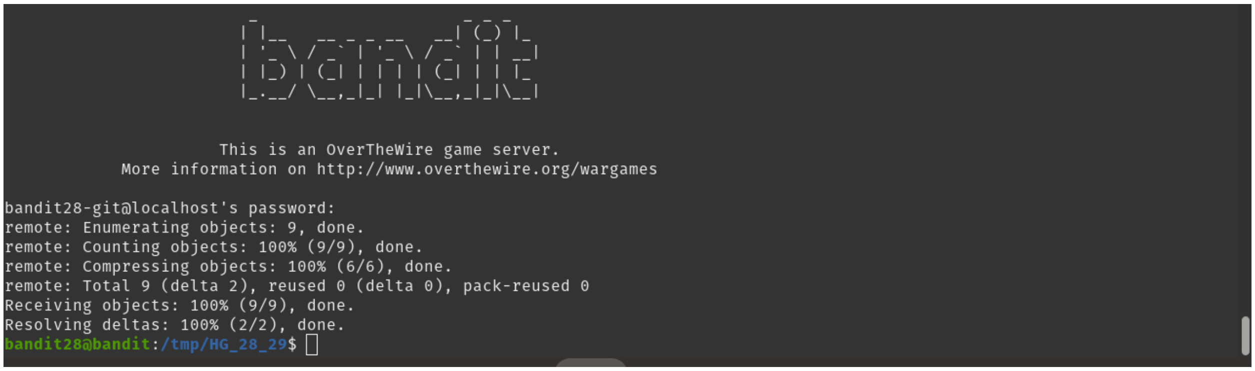
Clone the repository and find the password for the next level.

Commands you may need to solve this level

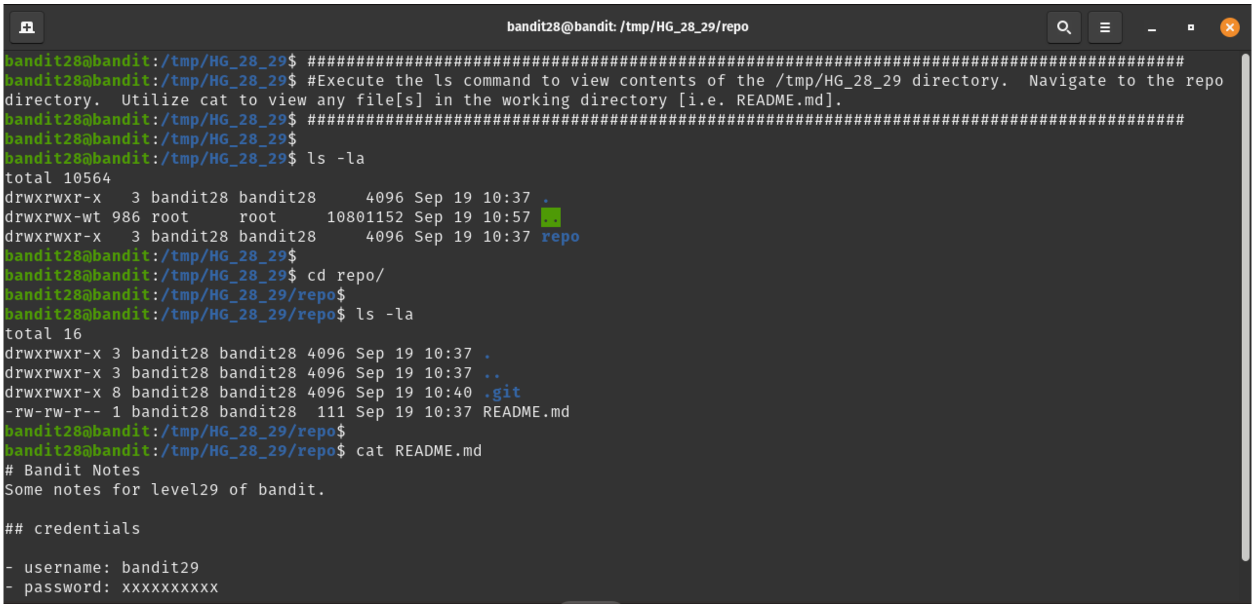
git



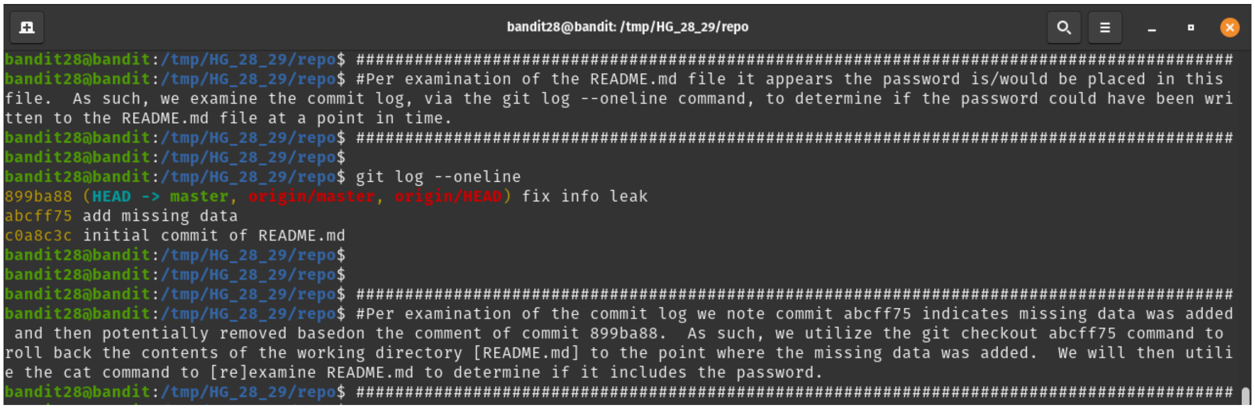
```
bandit28@bandit:~$ ###########################################################################################################
bandit28@bandit:~$ #Execution of id and whoami commands to determine level and user ID
bandit28@bandit:~$ ###########################################################################################################
bandit28@bandit:~$
bandit28@bandit:~$ id && whoami
uid=11028(bandit28) gid=11028(bandit28) groups=11028(bandit28)
bandit28
bandit28@bandit:~$
bandit28@bandit:~$ ###########################################################################################################
bandit28@bandit:~$ #Execution of Present Working Directory [pwd] and ls -la commands.  The -l option/switch outputs metadata o
f files and directories.  The -a option/switch outputs hidden files and directories which are demarked with a period at the on
set of their titles.
bandit28@bandit:~$ ###########################################################################################################
bandit28@bandit:~$
bandit28@bandit:~$ pwd
/home/bandit28
bandit28@bandit:~$
bandit28@bandit:~$ ls -la
total 20
drwxr-xr-x  2 root root 4096 Apr 23 18:04 .
drwxr-xr-x 70 root root 4096 Apr 23 18:05 ..
-rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root root  807 Jan  6  2022 .profile
bandit28@bandit:~$ 
```



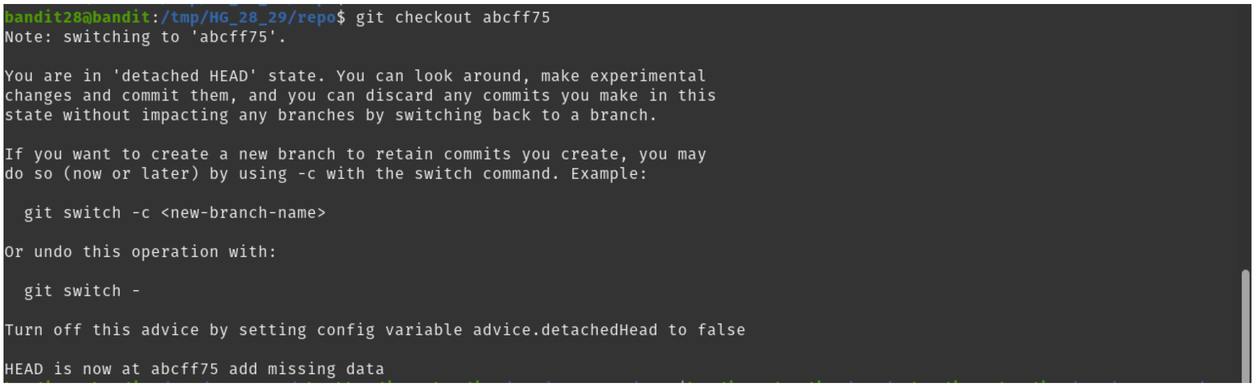
```
                         _                     _ _ _   
                        | |__   __ _ _ __   __| (_) |_ 
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_ 
                        |_.__/ \__,_|_| |_|\__,_|_|\__|
                                                       

                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit28-git@localhost's password:
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 9 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (9/9), done.
Resolving deltas: 100% (2/2), done.
bandit28@bandit:/tmp/HG_28_29$ 
```



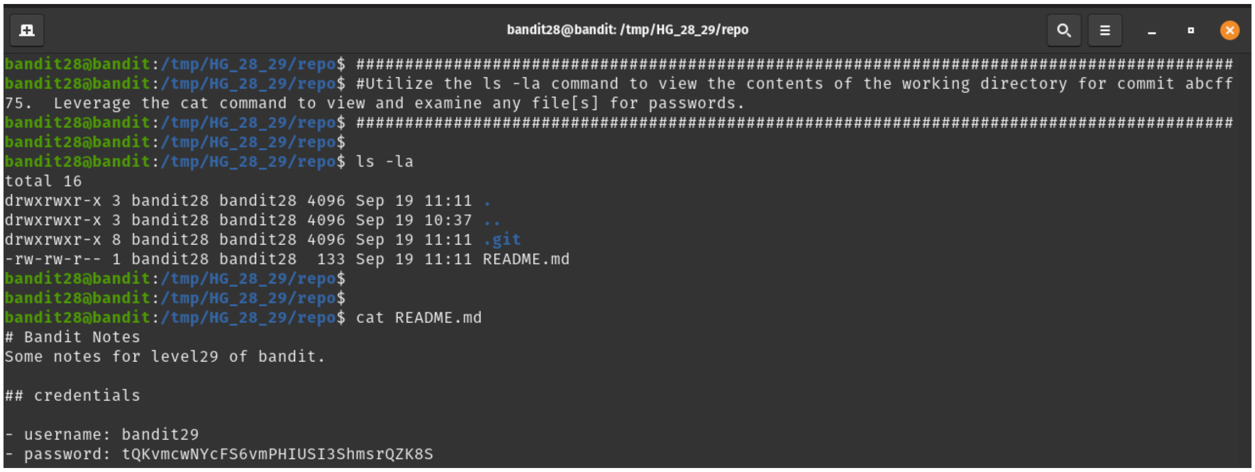
```
bandit28@bandit:/tmp/HG_28_29$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29$ #Execute the ls command to view contents of the /tmp/HG_28_29 directory.  Navigate to the repo
directory.  Utilize cat to view any file[s] in the working directory [i.e. README.md].
bandit28@bandit:/tmp/HG_28_29$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29$
bandit28@bandit:/tmp/HG_28_29$ ls -la
total 10564
drwxrwxr-x   3 bandit28 bandit28     4096 Sep 19 10:37 .
drwxrwx-wt 986 root     root     10801152 Sep 19 10:57 ..
drwxrwxr-x   3 bandit28 bandit28     4096 Sep 19 10:37 repo
bandit28@bandit:/tmp/HG_28_29$
bandit28@bandit:/tmp/HG_28_29$ cd repo/
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$ ls -la
total 16
drwxrwxr-x 3 bandit28 bandit28 4096 Sep 19 10:37 .
drwxrwxr-x 3 bandit28 bandit28 4096 Sep 19 10:37 ..
drwxrwxr-x 8 bandit28 bandit28 4096 Sep 19 10:40 .git
-rw-rw-r-- 1 bandit28 bandit28  111 Sep 19 10:37 README.md
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxx
```



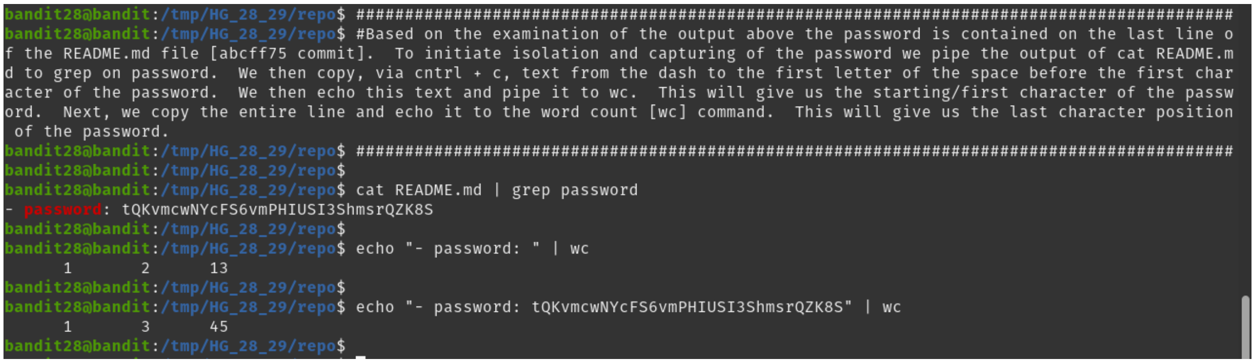
```
bandit28@bandit:/tmp/HG_28_29/repo$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29/repo$ #Per examination of the README.md file it appears the password is/would be placed in this
file.  As such, we examine the commit log, via the git log --oneline command, to determine if the password could have been wri
tten to the README.md file at a point in time.
bandit28@bandit:/tmp/HG_28_29/repo$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$ git log --oneline
899ba88 (HEAD -> master, origin/master, origin/HEAD) fix info leak
abcff75 add missing data
c0a8c3c initial commit of README.md
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29/repo$ #Per examination of the commit log we note commit abcff75 indicates missing data was added
 and then potentially removed basedon the comment of commit 899ba88.  As such, we utilize the git checkout abcff75 command to
roll back the contents of the working directory [README.md] to the point where the missing data was added.  We will then utili
e the cat command to [re]examine README.md to determine if it includes the password.
bandit28@bandit:/tmp/HG_28_29/repo$ ##########################################################################################
```



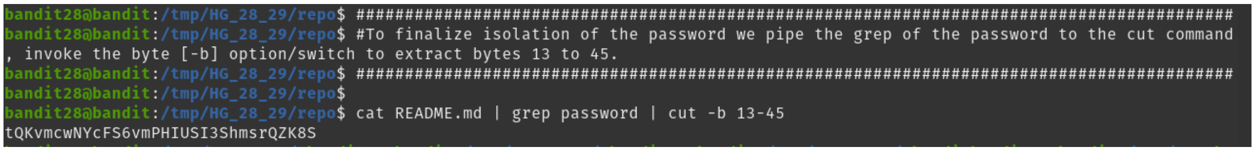
```
bandit28@bandit:/tmp/HG_28_29/repo$ git checkout abcff75
Note: switching to 'abcff75'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at abcff75 add missing data
```



```
bandit28@bandit:/tmp/HG_28_29/repo$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29/repo$ #Utilize the ls -la command to view the contents of the working directory for commit abcff
75.  Leverage the cat command to view and examine any file[s] for passwords.
bandit28@bandit:/tmp/HG_28_29/repo$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$ ls -la
total 16
drwxrwxr-x 3 bandit28 bandit28 4096 Sep 19 11:11 .
drwxrwxr-x 3 bandit28 bandit28 4096 Sep 19 10:37 ..
drwxrwxr-x 8 bandit28 bandit28 4096 Sep 19 11:11 .git
-rw-rw-r-- 1 bandit28 bandit28  133 Sep 19 11:11 README.md
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
```



```
bandit28@bandit:/tmp/HG_28_29/repo$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29/repo$ #Based on the examination of the output above the password is contained on the last line o
f the README.md file [abcff75 commit].  To initiate isolation and capturing of the password we pipe the output of cat README.m
d to grep on password.  We then copy, via cntrl + c, text from the dash to the first letter of the space before the first char
acter of the password.  We then echo this text and pipe it to wc.  This will give us the starting/first character of the passw
ord.  Next, we copy the entire line and echo it to the word count [wc] command.  This will give us the last character position
 of the password.
bandit28@bandit:/tmp/HG_28_29/repo$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$ cat README.md | grep password
- password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$ echo "- password: " | wc
      1       2      13
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$ echo "- password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S" | wc
      1       3      45
bandit28@bandit:/tmp/HG_28_29/repo$ _
```



```
bandit28@bandit:/tmp/HG_28_29/repo$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29/repo$ #To finalize isolation of the password we pipe the grep of the password to the cut command
, invoke the byte [-b] option/switch to extract bytes 13 to 45.
bandit28@bandit:/tmp/HG_28_29/repo$ ##########################################################################################
bandit28@bandit:/tmp/HG_28_29/repo$
bandit28@bandit:/tmp/HG_28_29/repo$ cat README.md | grep password | cut -b 13-45
tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
```

****

Level 29 —> Level 30 Password

****

tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S