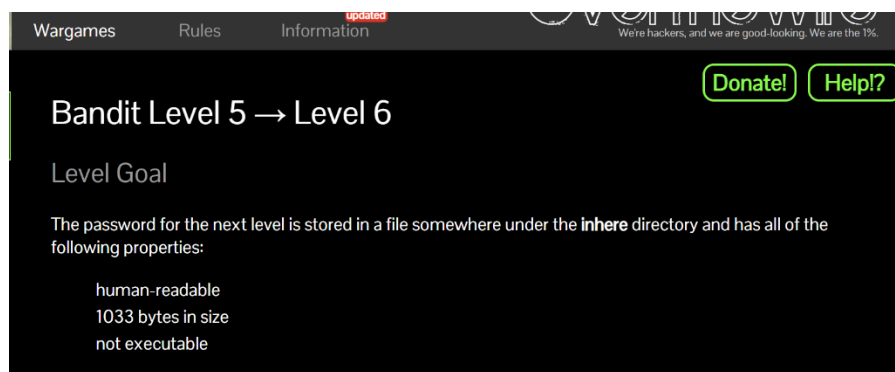


2회차 - 20. 케로로

Bandit 레벨 5 ~ 8 라이트업

정보보호학부 2024111262 조현서

Lv. 5 → 6



다음 레벨의 비밀번호는 `inhere` 디렉토리 어딘가에 저장되어 있으며, 사람이 읽을 수 있고, 크기가 1033바이트이고, 실행할 수 없는 파일이라고 한다.

```
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere02 maybehere04 maybehere06 maybehere08 maybehere10 maybehere12 maybehere14 maybehere16 maybehere18
maybehere01 maybehere03 maybehere05 maybehere07 maybehere09 maybehere11 maybehere13 maybehere15 maybehere17 maybehere19
bandit5@bandit:~/inhere$ find . -size 1033c
./maybehere07/.file2
```

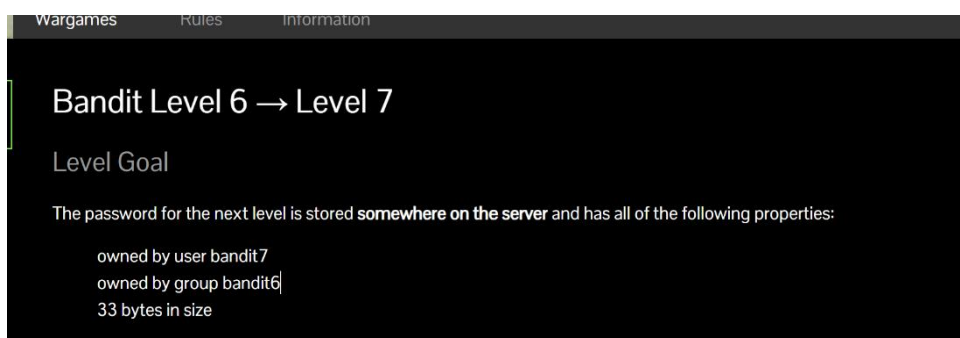
일단 “cd”를 통해, `inhere`로 이동한 후, “ls” 명령어를 입력하니, 많은 디렉토리가 나열되었다. 이 디렉토리를 하나하나 뒤져볼 수는 없기에, 명령어 “`find . -size 1033c`”를 통해, 파일 크기가 1033바이트인 파일을 출력하게끔 하였다. 해당 크기인 파일이 `maybehere07` 디렉토리에 있는 `file2` 라는 파일이라는 것을 알 수 있었다.

```
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

해당 파일을 "cat" 명령어를 통해 출력하니, 출력된 비밀번호는 "HWasnPhtq9AVKe0dmk45nxy20cvUa6EG" 이다.

Lv.5 → 6 해결

Lv. 6 → 7



다음 레벨의 비밀번호는 서버 어딘가에 저장되어 있고, 사용자는 bandit7이고, 그룹은 bandit6이고, 크기는 33바이트인 파일에 저장되어 있는 것으로 유추된다.

```
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/root': Permission denied
find: '/snap': Permission denied
find: '/tmp': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/3633790/task/3633790/fd/6': No such file or directory
find: '/proc/3633790/task/3633790/fdinfo/6': No such file or directory
find: '/proc/3633790/fd/5': No such file or directory
find: '/proc/3633790/fdinfo/5': No such file or directory
find: '/home/bandit31-git': Permission denied
find: '/home/ubuntu': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/drifter8/chroot': Permission denied
find: '/home/drifter6/data': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/polkit-1/rules.d': Permission denied
find: '/etc/multipath': Permission denied
find: '/etc/stunnel': Permission denied
find: '/etc/xinetd.d': Permission denied
find: '/etc/credstore.encrypted': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/credstore': Permission denied
find: '/dev/shm': Permission denied
find: '/dev/mqueue': Permission denied
find: '/var/log/amazon': Permission denied
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/log/private': Permission denied
find: '/var/tmp': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
```

서버 어딘가에 있다고 하였으니, 최상위 경로인 "/" 에서 find 명령어를 활용해 찾아보 고자 했다. "find / -size 33c -user bandit7 -group bandit6" 명령어를 입력해, 해당 속성을 만족하는 파일을 찾고자 하였다. 그 결과 수 많은 파일들이 출력되었다.

```

find: /var/lib/dpkg/info: Permission denied
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6 2> /dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOIFVAaj
bandit6@bandit:~$

```

이들을 보니, 대부분이 Permission Denied 된 것들이 많다. 그래서 "2> /dev/null" 을 추가적으로 입력하여, 에러난 결과를 모두 걸러지게끔 하였다. 그러더니, bandit7.password 라는 파일 하나를 발견하였다. 이를 cat 명령어로 출력하니, 비밀번호는 "morbNTDkSW6jIlUc0ymOdMaLnOIFVAaj"이다.

Lv.6 → 7 해결

Lv. 7 → 8

Bandit Level 7 → Level 8

Level Goal

The password for the next level is stored in the file **data.txt** next to the word **millionth**

Commands you may need to solve this level

man, grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

다음 레벨의 비밀번호는 data.txt 파일에 저장되어 있으며, 단어 "millionth" 옆에 있다고 한다.

```

bandit7@bandit:~$ cat data.txt

```

```

mallard's      MTKvAaiubyq3Ie88Ulua0HY7ZgFZ4zed
barometric     sV8kzJtlqpjJn6boaaa4gtFGB6GuwhvJ
tracers 2ZITFahgp9og6GNRSOXLt46QiT3PuNvP
outflanks      YqKPcc2DzEHNqjN2I5DxyM2p06zbev bq
triumphing     gUzNHyBcDAYvRnG2a8m8Rt5q8bw776Pa
aspect's       xdoF0oK7LWNkM6eeIBwYQazCC35Zm0VM
distribute     jvQId40mRNK9w5bNSKXWG0cPn0tRlFDq
humiliation    bNtphrnEeCKgPKkAeio0uGzVKuj9Bz8h
crowds  lcLZWfW9Y1H9ijvCM1Hx2R6zvJqHgsMt
refurnishes    hFF11AaZoViObnrtdAA0TcRg9fWV3h6U
Hindi's gEPWTgmaR0cPV9Q5B69JrkqxeUDIePRj
perfumeries    RFR7ZFHI0WfyBBcQDe1G7rpHo4iGKkmV
recomence      uqAu36x9lViN0sJpqjePhp5Ty2XocPKB
complaint      Ch3MnrWSfvaR6lrPT4ZN4FbXIVbRTuUw
telekinesis's  u00d6SmlsJvqbbpD2wX1urojDvGKnvna
sutured S3S5Bz1ZIALg9pWuvAez3eif9TpZ3g4T
mechanic       bmiYfQiKgQxohljoFhLGFAPGrKSfKem4
unluckiest     OXKwX7Zdo8lB82TexwVwt22GAhULh65A
obsession      SLiXncgs0tGAZnpJePzLN10Jo3DELTHB
footman's      zet6GehCCq4kLxSJZS36Y6ES5ngq0n65
Filippo's      FB8VvtGT14D4hcaZr2uIKYMuY4qvEQx

```

Cat 명령어로 data.txt 파일을 불러오면, 엄청 많은 내용들이 쏟아진다. 해당 파일 내용을 출력할 때, 필터링이 필요할 거 같아서, "grep" 이라는 명령어를 활용하려고 한다.

```
bandit7@bandit:~$ cat data.txt | grep millionth
millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

비밀번호가 millionth라는 단어 옆에 있다고 하였으니, "cat data.txt | grep millionth" 명령어를 입력해보았다. 다음 단계의 비밀번호는 "**dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc**"이다.

Lv.7 → 8 해결

Lv. 8 → 9

Bandit Level 7 → Level 8

Level Goal

The password for the next level is stored in the file **data.txt** next to the word **millionth**

Commands you may need to solve this level

man, grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

다음 레벨의 비밀번호는 data.txt 파일에 저장되어 있으며, 단 한 번만 등장하는 텍스트 줄에 있다고 한다.

```
bandit8@bandit:~$ cat data.txt

7qHmEo1FEbzthgyNpKc38YofXjYKZv18
RpRE5maDwMQTa8oJt7vVNqff7ElrjLTq
zokSjnkcdJ1hdGEBE4feukfCtFmv82ZZ
omBfCRI91Zm06GI0RLngq05AMwe8Ndqo
35l6mr3f6TvLJyDwU6aUgJX07cLhr6t9
iGmmKP7APsDfPxrZjCL7eDpGEWR3ot3q
4P8FsHcdr7d5WKnpTAaXY5Ss1KICd2gL
5hYz0028e1Q2TrtPVz5GZbpMzZNjebhh
IkJadTScIdBQY9a4KVjBEHyXKubCxSLx
HloFLs5IpuFLuVJugBxKEipr5Qa0bJmk
qEi18Iw0qI0fe3fGMr6tTPpL6SbPMjk3
s8SnoFuk0jR1CTdQ7pctd67nakJWN2Vc
omBfCRI91Zm06GI0RLngq05AMwe8Ndqo
WVQJq1JYFGgtR69JgWxUAKPb0RaKc90J
```

Cat 명령어로 data.txt 파일을 출력해보니, 알 수 없는 수 많은 문자열들이 출력되었다. 이 중에서 단 한 번만 등장하는 텍스트 줄에 비밀번호가 있다고 하니, data.txt의 중복을 제거하는 작업이 필요해 보인다. 중복을 제거하기 위해서, "uniq"를 사용하려고 한다. 이는 파일 내용이 중복되면 제거한다고 한다. 이 uniq의 옵션인 "-c"를 활용하여, 몇 번 중복되었는지도 출력해 주게끔 하려고 한다. 단, 이 uniq는 이어진 중복만 제거하기 때문에 추가적인 명령이 더 필요해 보인다. 그리고, "sort" 명령어를 활용하여, 파일을 오름차순으로 정렬해주려고 한다.

```
bandit8@bandit:~$ cat data.txt | sort | uniq -c
10 0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
10 0eJPctF8gK96ykGBBaKydHJgxSpTLJtz
10 0kJ7XHD4gVtNsZIpqyP1V45sfz90BLFo
10 0lPovKhpHzebxji0gdjtGcd5GWiZnNBj
10 0REUHKk0yMq0OweI6NK9ZqIpE5dVlWWM
10 1jfUH1m4XCjr7eWaeLeGdaNSxFXRTx0L
10 1VKPEkd0bCtIRwMFVQfY7InuLwOFyDsn
10 2u8fvAzvnaFlvQG3iPt4Wc1TFhPcGxhH
10 35L6mr3f6TVLJyDwU6aUgJX07cLhr6t9
10 3FIgaJBlaQA1TMVGo1gxRDSiACNyvvJ
10 3nNA2le0gfURQKNHVIhGkMNLqLw4yyLN
1 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
10 4P8F5HcdR7d5WKnPTAaXY55sLKICd2gL
10 5EmwMKZHwF6Lwq5jHuaDlffJBhbcX0b
10 5hYz0028e1Q2TrtPVz5GZbpMzZNjebhh
10 5I2jWpqjtVp576xXI2TLh1UCyXJtGQ78
10 6Boy6esAjn1xCyn8uI6KZ7VD7zysDM8i
10 7cP8ssLElERHXq0Jc9T84bxsmJBjNXk2
10 7qHnEo1FEbzthgyNpKc38YofXjYKZv18
10 8FCtUQlFXsJnNeyiDY5KfE3vRy6sZFEEJ
10 8pePxslMzXqA2mi87wFjxd44qDRdrPiW
10 9jfKbkGp40LjMu1iH9cce4bUo9y8nd0j
10 9PqZLdu143n5djN9mL1MCanrmHERUv7k
10 9Tar2wcD3Urge6s2yp18CAE8zX1poUwV
10 A4MlxXbxP5t0RE87qkmAdwWPJ03Aw6r0
10 aFStfHbnQdPWqyRHEzhqe91Wch408xHJ
10 aMKlTMrptUxxTypChocCTrqYRkR2gT8h
10 AOz67fZdaabu2Q0yatGKX1dXNUIuyU0D
10 BIA2jxKMFnitEvp0WmsM0oDAwj4WSUa
10 BmwX4bYhJXyImwt4AVHr7wFyLYCn4IIIs
10 BooZo7QXA1Tft7d6zbVkgJlGoJzuBTXS
```

"cat data.txt | sort | uniq -c"을 입력하니, 다른 문자열들은 다 10번 중복되는데, 유일하게 한 번만 출력된 문자열을 확인할 수 있었다. 다음 단계 비밀번호는 "4CKMh1JI91bUIZZPXDqGanal4xvAg0JM"이다

Lv.8 → 9 해결

2주차 Bandit 워게임 문제 풀이

2024111205 강미주

Lv. 5 -> Lv. 6

Bandit Level 5 → Level 6

Level Goal

The password for the next level is stored in a file somewhere under the `inhere` directory and has all of the following properties:

- human-readable
- 1033 bytes in size
- not executable

Commands you may need to solve this level

`ls` , `cd` , `cat` , `file` , `du` , `find`

```
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere04  maybehere08  maybehere12  maybehere16
maybehere01  maybehere05  maybehere09  maybehere13  maybehere17
maybehere02  maybehere06  maybehere10  maybehere14  maybehere18
maybehere03  maybehere07  maybehere11  maybehere15  maybehere19
bandit5@bandit:~/inhere$ cd
bandit5@bandit:~$ vi inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ find ./ -size 1033c
./maybehere07/.file2
```

```
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

inhere로 이동해서

문제에서 나온 글을 통해 얻은 힌트 사이즈가 1033이므로 사용해서 명령어를 입력함

```
find ./ -size 1033c
```

그럼 inhere디렉토리에 있는 파일중에 사이즈가 1033인 파일을 출력해줌

결과로 .file2에 있다는걸 알 수 있음

+추가적으로 파일명 앞에 .이 붙어있으면 숨겨진파일임

비밀번호 획득 완.

Lv.6 -> Lv.7

Bandit Level 6 → Level 7

Level Goal

The password for the next level is stored somewhere on the server and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

Commands you may need to solve this level

ls, cd, cat, file, du, find, grep

Bandit7의 유저파일이면서 bandit 그룹의 파일이며 크기는 33인 파일에 비밀번호가 있다고 나와있음

```
bandit6@bandit:~$ find ./ -size 33c
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/root': Permission denied
find: '/snap': Permission denied
find: '/tmp': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/1329710/task/1329710/fd/6': No such file or directory
find: '/proc/1329710/task/1329710/fdinfo/6': No such file or directory
find: '/proc/1329710/fd/5': No such file or directory
find: '/proc/1329710/fdinfo/5': No such file or directory
find: '/home/bandit31-git': Permission denied
find: '/home/ubuntu': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/drifter8/chroot': Permission denied
find: '/home/drifter6/data': Permission denied
```

솔직히 날로 먹고싶어서 사이즈만 입력해서 명령어를 입력하니 ㅎ당연하게도 찾을 수 없었음.

그래서 조건들을 다 입력한 명령어를 입력함

그러니 permission denied된 것들이 같이 엄청나게 많이 출력되어 정답 파일을 찾기 힘들어서 접근 불가능한 파일들을 제외 할 수있는 명령어를 구글링 해보니

뒤에 2>/dev/null을 입력하면 됨

null=오바이트인 파일 2는 표준에러

즉 표준에러를 다진 리다이렉션(<)를 이용해서 화면에 출력 X하고 /dev/null파일에 저장한다라는 뜻~

그래서 화면상에서 출력안됨

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
```

출력된 파일을 cat으로 확인해서 비밀번호 찾을 수 있었음.

Lv. 7 -> Lv.8

Bandit Level 7 → Level 8

Level Goal

The password for the next level is stored in the file data.txt next to the word millionth

Commands you may need to solve this level

man, grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

millionth단어 옆에 비밀번호가 있다고함.

```
bandit7@bandit:~$ ls
data.txt
```



```

abjure ZlW4oog9188Qd8df3HW2reNri2aMxo26
renal 80cKdVMuGVVmIC6IZH39bx3rpDSkCbWv
sans IzDQf2WJGG7nPuqHbVIQKCbEPQwZIA3s
meting mFY3wNpY9FvSVGZ1mgi5N8U83US5Ywzu
Franck cErFvuq2QsmlqvRoE9JIb3eP95XTD94b
reader's uc94SAup0ckmTILYobI8t6LK4FXiopA0
tundra's AMPxMOHtyyQyOSQ0eG819far1kJXkDAB
terminus PTCL1CY5EAoUu9vhU8Q3Rhvm55qvlLjH
subtotal 7a709N9ZIIYSETwdEGBR2mFSKMfKrxBTX
wrongfulness mMDI21VOMyZxkV2R7b61ERqPIyBVslsV
whitens 0ryQZCxD3dXX60E9xMeDIgjeY0B2ivxj
treading vmeULGaYMd69JwbAdEJtL2UiXZfgQOJN
reimpose XJubELpBFTp0wx0qybxfByHoKm1tE5C
battalions hf3EPFD5eVFRedNnHLciwlH60iClh4rW
Soho's uW70GRbkWX3CkzZjrU5KmIOdnd3paxTG
Mondays TEzFxcQ7IC1VdsvqGs5fX4kwR22GwVNf
unsuccessfully 1aVW4qvBdy39Wkkl5vyAZZV89qVkNSuW
Odessa cMnmUf3hUk3zKizQQ9MygtjE0KBauwwN
jacket sS3sDdscHJbJfSN1d36VJLppXoYE3mW5
seeping hhrdfoZgoMQmINOrmmZlL5t8sVhDGDWZ
renounces H5pjlsprVRLLDbiSKtxAIG6NSBCkmzq2
impoverishment hwijIqvXQqbMMdW7Va80qMEZmcXXZL8i

```

역시 cat으로 하니 엄청나게 많이 나와서 찾기 거의 불가능함
grep 명령어를 사용해야겠음

grep millionth data.txt
를 입력하면

찾고자하는 문자열이 포함된 행을 출력해줌

```

bandit7@bandit:~$ grep millionth data.txt
millionth dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

```

비밀번호 찾음

Lv. 8 -> Lv. 9

Bandit Level 8 → Level 9

Level Goal

The password for the next level is stored in the file data.txt and is the only line of text that occurs only once

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

Helpful Reading Material

Piping and Redirection

비밀번호는 한번만 입력된 유일한 문자열임.

바로 생각나는 건 `uniq -c`임

1번 카운팅된게 정답일 듯 하다..

```
bandit8@bandit:~$ cat data.txt | sort | uniq -c
10 0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
10 0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
10 0kJ7XHD4gVtNSZIpqyP1V45sfz90BLFo
10 0lP0vKhphZebxji0gdjtGCd5GWiZnNBj
10 0REUhKk0yMqQ0wei6NK9ZqIpE5dVlWWM
10 1jfUH1m4XCjr7eWAeLeGdaNSxFXRtX0l
10 1VKPEkd0bCtIRwMFVQfY7Inulw0FyDsn
10 2u8fvAzvnaFlvQG3iPt4Wc1TFhPcGxhH
10 35l6mr3f6TvlJyDwU6aUgJX07cLhr6t9
10 3FIgajXBiaQAiTMVGo1gxRDSiACNyvvJ
10 3mNA2le0gfURQKNHVIhGkMNLqLwjyyLN
1 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
10 4P8FsHcdr7d5WKnPtAaXY5SslKICd2gL
10 5EmwMKZHwF6Lwq5jHUaDlfFJBcHbcX0b
10 5hYz0028e1Q2TrtPVz5GZbpMzZNjebhh
10 5I2jWpqjtVp576xXI2TLh1UCyXJtGQ78
10 6Boy6esAjnIxCYn8uI6KZ7VD7zysDM8i
10 7eP8eclF1FPUXc07e0T84hxcw3B4MYk2
```

생각했던 명령어를 치니 카운팅이 1번된 문자열을 찾음

정답~~

4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

2주차 Bandit 워게임 문제 풀이

김효주

1. [Bandit] Level 5 -> 6

Bandit Level 5 → Level 6

Level Goal

The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

- human-readable
- 1033 bytes in size
- not executable

Commands you may need to solve this level

ls, cd, cat, file, du, find

이번 문제는 inhere 디렉토리 안에 있는 파일에서 비밀번호를 찾아야 하는 문제이다.

먼저, -type과 -exec 옵션을 사용하고 grep 명령어를 활용해 사람이 읽을 수 있는 파일을 찾을 수 있다. find . -type f는 현재 디렉토리 및 그 하위 디렉토리에서 모든 파일을 검색한다. -exec file {} \;는 찾은 파일마다 file 명령어를 실행하는데, {}는 파일 이름으로 대체되고 \;는 -exec 명령어의 끝을 의미한다. 또한 grep 명령어를 사용하여 텍스트 형식이 아닌 파일들을 제외할 수 있다.

```
bandit5@bandit:~/inhere$ find . -type f -exec file {} \;
./maybeh ere07/-file3: data
./maybeh ere07/spaces file2: ASCII text, with very long lines (9063)
.....

bandit5@bandit:~/inhere$ find . -type f -exec file {} \; | grep -i text
./maybeh ere07/spaces file2: ASCII text, with very long lines (9063)
./maybeh ere07/-file2: ASCII text, with very long lines (2487)
```

다음으로, -size 옵션을 사용하면 정확히 1033바이트 크기의 파일을 찾을 수 있다. -size 옵션은 파일이 지정된 용량을 초과하거나 미만이거나 정확한 크기를 사용하는지를 나타내며, 여기서 c는 바이트 단위를 나타낸다.

```
bandit5@bandit:~/inhere$ find . -type f -size 1033c -exec file {} \; | grep -i text
./maybehere07/.file2: ASCII text, with very long lines (1000)
```

마지막으로, -perm 옵션을 사용하여 소유자, 그룹 또는 다른 사용자에게 실행 권한이 설정된 파일을 검색할 수 있다. 하지만 ! -perm은 소유자, 그룹 또는 다른 사용자에게 실행 권한이 없는 파일을 찾는다. 옵션 앞에 !가 붙으면 조건이 반대가 된다. 따라서 find ! -perm /111은 소유자, 그룹, 다른 사용자 모두에게 실행 권한이 없는 파일을 찾아낸다.

```
bandit5@bandit:~/inhere$ find . -type f ! -perm /111 -size 1033c -exec file {} \;
./maybehere07/.file2: ASCII text, with very long lines (1000)
```

```
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

결국, 비밀번호는 'HWasnPhtq9AVKe0dmk45nxy20cvUa6EG'임을 알 수 있었다.

2. [Bandit] Level 6 -> 7

Bandit Level 6 → Level 7

Level Goal

The password for the next level is stored **somewhere on the server** and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

Commands you may need to solve this level

ls, cd, cat, file, du, find, grep

가장 먼저 find 명령어의 사용 가능한 옵션을 확인하기 위해 man find 명령어를 사용할 수 있다.

```
bandit6@bandit:~$ find / -user "bandit7"
find: '/sys/kernel/tracing': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/bpf': Permission denied
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/cgroup.procs
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/cgroup.threads
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/app.slice
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/app.slice/cgroup.events
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/app.slice/memory.events
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/app.slice/io.pressure
.....
```

여러 파일을 검색할 때, Permission denied 메시지를 접할 수 있었다. 이는 해당 파일을 읽을 권한이 없다는 것을 의미한다. find 명령어 끝에 2>/dev/null을 추가하면, 셸이 오류 메시지를 /dev/null로 리디렉션하게 되어 화면에 표시되지 않도록 할 수 있다.

```
bandit6@bandit:~$ find / -user "bandit7" 2>/dev/null
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/cgroup.procs
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/cgroup.threads
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/app.slice
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/app.slice/cgroup.events
/sys/fs/cgroup/user.slice/user-11007.slice/user@11007.service/app.slice/memory.events
```

다음 조건은 파일이 bandit6 그룹에 속해야 한다는 것이다. 이러한 파일을 찾을 수 있었다.

```
bandit6@bandit:~$ find / -user "bandit7" -group "bandit6" 2>/dev/null
/var/lib/dpkg/info/bandit7.password
```

마지막으로, 모든 조건을 충족하기 위해 파일 크기를 확인해야 한다.

```
bandit6@bandit:~$ find / -user "bandit7" -group "bandit6" -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
```

이제 비밀번호를 찾을 수 있었다.

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
```

다음 문제로 접속할 수 있는 비밀번호는 'morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj'이다.

3. [Bandit] Level 7 -> 8

Bandit Level 7 → Level 8

Level Goal

The password for the next level is stored in the file **data.txt** next to the word **millionth**

Commands you may need to solve this level

man, grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

이번 문제는 'millionth'라는 단어가 있는 파일 안에 비밀번호가 있는데, 다음과 같이 내용이 너무 길어서 한 줄씩 검색하기 어렵다.

```
bandit7@bandit:~$ ls  
data.txt  
bandit7@bandit:~$ cat data.txt  
Togo's    zMSk3jmZQL60Hd0BnkBcantGvGbTuyDR  
loader    6kP31IsFVItYVYIuLUXVorvHQpct2F6A  
horseradish's  LAD77UITMQFCxqRiAA06KNSCRUaqdQJ4  
Savoyard   uKtULf3kVyUGKd1KBE006JVvXtkrapBe  
Keller's   BG48vRqDH3HjHDDk5ZEivyz7Q5Ex4qCU  
.....
```

따라서 grep 명령어를 사용해 패턴을 매칭하면 빠르게 해당 내용을 찾아 비밀번호를 얻을 수 있다.

```
bandit7@bandit:~$ cat data.txt | grep millionth  
millionth    dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
```

4. [Bandit] Level 8 -> 9

Bandit Level 8 → Level 9

Level Goal

The password for the next level is stored in the file `data.txt` and is the only line of text that occurs only once

Commands you may need to solve this level

`grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd`

Helpful Reading Material

Piping and Redirection

이번 문제는 특정 단어가 한 번만 등장하는 파일을 찾아야 하는데, 내용이 너무 길어서 수동으로 검색하기 어렵다. 이번에는 `grep` 명령어를 사용할 수 없는 상황이다. 왜냐하면 매칭할 특정 패턴을 모르기 때문이다. 하지만 그 단어는 한 번만 나오기 때문에 이를 이용해야 한다.

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ cat data.txt
riAxnw3RnsFuQiOD8BlZbR6TlERU9866
pJyx6KXXkALfk2n5VSyWS4fqKvnyuN8G
tAw9D85F6PkUdTdlCwmRWYlQNPbkcVox
WwKtMcgokvQfZKjkt2yfJDtMMclL3cMn
fYJtDkXtfgl2A0r3i0lMNRmmCePl568B
.....
```

이때 `uniq` 명령어가 유용하다. `-c` 옵션을 사용하면 각 줄이 몇 번 등장했는지 확인할 수 있다. 하지만 `uniq`는 인접한 동일한 줄만 필터링하기 때문에, 먼저 파일을 정렬해야 효과적으로 사용할 수 있다.


```
bandit8@bandit:~$ uniq -c data.txt
1 riAxnw3RnsFuQiOD8BlZbR6TlERU9866
1 pJyx6KXXkALfk2n5VSyWS4fqKvnyuN8G
1 tAw9D85F6PkUdTdlCwmRWYlQNPbkVox
1 WwKtMcgokvQfZKjkt2yfJDtMMclL3cMn
1 fYJtDkXtfgl2A0r3iOlMNRmmCePl568B
.....
```

uniq 명령어는 두 가지 방법으로 활용할 수 있다. 첫번째는 -c 옵션을 사용해 각 줄이 몇 번 나타나는지 확인하는 것이다. 두번째는 -u 옵션을 사용해 고유한 줄만 출력하는 방법이다. 이를 통해 비밀번호를 찾을 수 있었다.

```
bandit8@bandit:~$ sort data.txt | uniq -c
10 0KCctkqCfY7BIOwqolXsHDaboXVTkZ49
10 1SKCEfQ151hW0x9JkeIAmOQdXiC813h1
10 3hHLoFjM7m3sdyiKJF5QsMqvEIfFh5b1
10 3hW8tLnDV8acjhTQi44CKXEzHsJb3sqz
10 3nUXvAjKo7yu6fYykYu7nGGKDMuNMWZf
10 42qjuz5hdLlItNwdJYsDRpkbbvoEYiWK
1 4CKMh1JI91bUIZZPXDqGana14xvAg0JM
10 5g2sV40okwqDv29Pfo6C7twjKcOk4wQV
10 5YlL2xxyEUqV6tF0P6NoHt8LOY2EGEcO
10 6lMDNhQjl0oCOZ5F8ULK2g0uT0rCdnoQ
.....
```

```
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGana14xvAg0JM
```

20. 케로로 - 2주차

Bandit Lv.6-9 Write-Up

전지해

Lv.5 → Lv.6

Bandit Level 5 → Level 6

[Donate!](#) [Help?](#)

Level Goal

The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

human-readable
1033 bytes in size
not executable

Commands you may need to solve this level

ls, cd, cat, file, du, find

문제를 읽어보니 비밀번호는 inhere 디렉토리 안의 어떤 파일에 있으며, 파일 조건은 사람이 읽을 수 있으며, 1033 byte이고 실행할 수 없는 파일이라고 한다. 우선 cd 명령어로 inhere 디렉토리로 이동했다. 그리고 찾고 있는 파일의 조건들이 많다 보니 find 명령어를 이용해서 찾아보았다. 그리고 cat 명령어를 이용해 파일을 열어보았다.

\$ find [경로] [옵션]

- ./ : 현재 디렉토리
- -type f : 파일
- -size 1033c : c(=byte)
- ! - executable : !(=not)

\$ find ./ -type f -size 1033c ! -executable

```
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ find ./ -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

비밀번호를 찾았다!

Lv.6 → Lv.7

Donatel Help?

Bandit Level 6 → Level 7

Level Goal

The password for the next level is stored **somewhere on the server** and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

Commands you may need to solve this level

ls, cd, cat, file, du, find, grep

문제를 읽어보니 다음 레벨의 비밀번호는 user가 bandit7이고 group은 bandit6, 33 byte인 서버 어딘가에 저장되어 있다고 한다. 우선 find 명령어를 사용해서 해당 조건에 맞는 파일을 찾아보자.

\$ find [경로] [옵션]

- / : 모든 경로
- -user bandit7
- -group bandit6
- -size 33c

\$ find / -user bandit7 -group bandit6 -size 33c

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/root': Permission denied
find: '/snap': Permission denied
find: '/tmp': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/3482740/task/3482740/fd/6': No such file or directory
find: '/proc/3482740/task/3482740/fdinfo/6': No such file or directory
find: '/proc/3482740/fd/5': No such file or directory
find: '/proc/3482740/fdinfo/5': No such file or directory
find: '/home/bandit31-git': Permission denied
```

여러 파일들이 뜨는데 permission denied 오류가 대부분이다. 찾아보니 이 오류는 <권한 오류>로 사용자가 특정 디렉토리나 파일에 접근할 권한이 없음을 의미한다고 한다. 이때 오류가 뜨는 항목들이 안 뜨게 하기 위해서는 아래와 같은 명령을 추가하면 된다고 한다.

2>/dev/null

- 2: 표준 오류의 id, 프로그램이 오류 메시지를 출력할 때 사용하는 스트림이다.
 - 0: 표준 입력 id
 - 1: 표준 출력 id
- > : redirection으로, 경로를 바꿔준다는 것을 의미한다.
- /dev/null: 특수파일로, 블랙홀이라고 생각하면 된다. 모든 버려진다.

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jI1Uc0ymOdMaLn0lFVAaj
```

비밀번호를 찾았다!

Lv.7 → Lv.8

[Donate!](#) [Help?](#)

Bandit Level 7 → Level 8

Level Goal

The password for the next level is stored in the file `data.txt` next to the word `millionth`

Commands you may need to solve this level

`man, grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd`

문제를 읽어보니 다음 레벨의 비밀번호는 `data.txt` 파일안에 `million` 단어 옆에 있다고 한다. 텍스트 파일을 읽고 편집하는 `vim` 명령어를 이용하여 파일을 열어보자. 그리고 ?[찾고 싶은 단어]를 입력하면 비밀번호를 찾을 수 있을 것 같다.

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ vim data.txt
Lilian s9lUxPFDRQzV9xzPQYOvPWNGf6NI37zo
quark's l9sURQRRace2eUz7VljAL7YIuybi8elz
conspirator 7SNeFn5yY0xgGhGZBRUjn548IGcy6I8P
millionth dfwvzFQi4mU0wfNbF0e9RoWskMLg7eEc
bistros 0uUWlqktnXxl1SbHceHzB2L6LgZEBhER
wifeliest I90cYhcx09Prp2ddfj5ngvnbdx157F6D
legionnaire diL66wsns24U8uOZ4Rmaqbd48aRnSVmX
Grenoble's 1MB4kpeF706AgORHdmsqEjFpNkTU6Bm7
reneging rx6BWAUyx7X4BzuoEOEvdqNp3phCL9PU
gluttony X0D0WWRj314aZq8tcqRbjLYHYDz6FJib
Beatriz d77kG0t13qo1b1WIi3bA7WabTiT6s5jG
igloo's P947lICfJcOvSEVxa3apAXYNbuwP4ohd
reminiscence's vWu2sfQuj166vZ9zM3mS4DYL5dgLITNF
babbler uW091DRRGxey4vwsWfwqEIAACVEk6BpK
sublimed 1xPHzqvU9G4zNQZ60fWELxBhqtFLE6ux
joist's p92B8hJbRPWzDne0jYROC6Qk2FsDjohS
itinerary LSF13MuLyfEPMPfbfBJhdgLF10z1R2RN
popularization's qWuys0Xxk08QX6bku1KkjuAlGj004Qno
traversing 4YamkhsNbhx5q25HKMaePl9UJ009geEB
educator NpAea3ukXSukR1W8FGoGDw401PsSs12I
chalice's 9A4M0uJnpMbaTa2ISmdtZZG13b33HkUa
interpretation's qpePY1dudBMrWrs5CvQpEXDK0oMzIHZQ
?millionth
```

비밀번호를 찾았다!

Lv.8 → Lv.9

Bandit Level 8 → Level 9

Level Goal

The password for the next level is stored in the file `data.txt` and is the only line of text that occurs only once

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

Helpful Reading Material

Piping and Redirection

문제를 읽어보니 다음 단계 비밀번호는 data.txt 파일에 있고 한번만 나타나는 유일한 라인이라고 한다. 정확히 무슨말인지 이해가 되지는 않지만 일단 data.txt 파일을 열어보자,

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ cat data.txt
aMKlTMrptUxxTypCHocCTrqYRkR2gT8h
PRerp5EfTvXJHKuCZDXfAfRyCQSDpJMi
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
6Boy6esAjinIXcYn8uI6KZ7VD7zysDM8i
tgHSfEXcbYceJwXfsWDO4VXXbqtTVcqS
KZJOZECxhLxDhXDbGzdNy8m0uplzpP11
w6x5XtaoRWDqMCsYxgZIWuOKVdiGByAu
0kJ7XHD4gvtNSZIpqyP1V45sfz90BLFo
Wr4hWlUhGCKJpGDceio8C1pLvT7DZm3X
Su9w1lri9UACf53cL1evAMKXVgI0nfqe
6Boy6esAjinIXcYn8uI6KZ7VD7zysDM8i
CgUjZiluCoMEvzNAge1Nbv3g9tpLQQj2
ysKmfYcysVfnViisRBcXzgjJXMDgnKKv
1VKPEkd0bCtIRwMFVQfY7InulwOfYDsn
```

뜻을 알 수 없는 문자들이 끝없이 나온다. 뭔가 문자열에 규칙이 있을 수 있겠다는 생각에 반복되는 문자들을 묶기 위해 파일의 텍스트 내용을 정렬하는 sort 명령어를 사용해 보았다.

[illegible]

이어서 중복되는 문장들을 지우기 위해 `uniq` 명령어에 한번 발생하는 줄을 찾는 `-u` 옵션을 추가해 보았다.

```
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXQqGanaI4xvAg0JM
```

비밀번호를 찾았다!!