# Security Topic

ALTANGINJ TUMENGEREL

2018/05/01（3rd）

# PicoCTF 2017 Bash Loop



**Bash Loop**

We found a program that is hiding a flag but requires you to guess the number it is thinking of. Chances are Linux has an easy way to try all the numbers... Go to /problems/de905332a1594a49f78931c233b0eb2b and try it out!

▸ ❓ HINTS
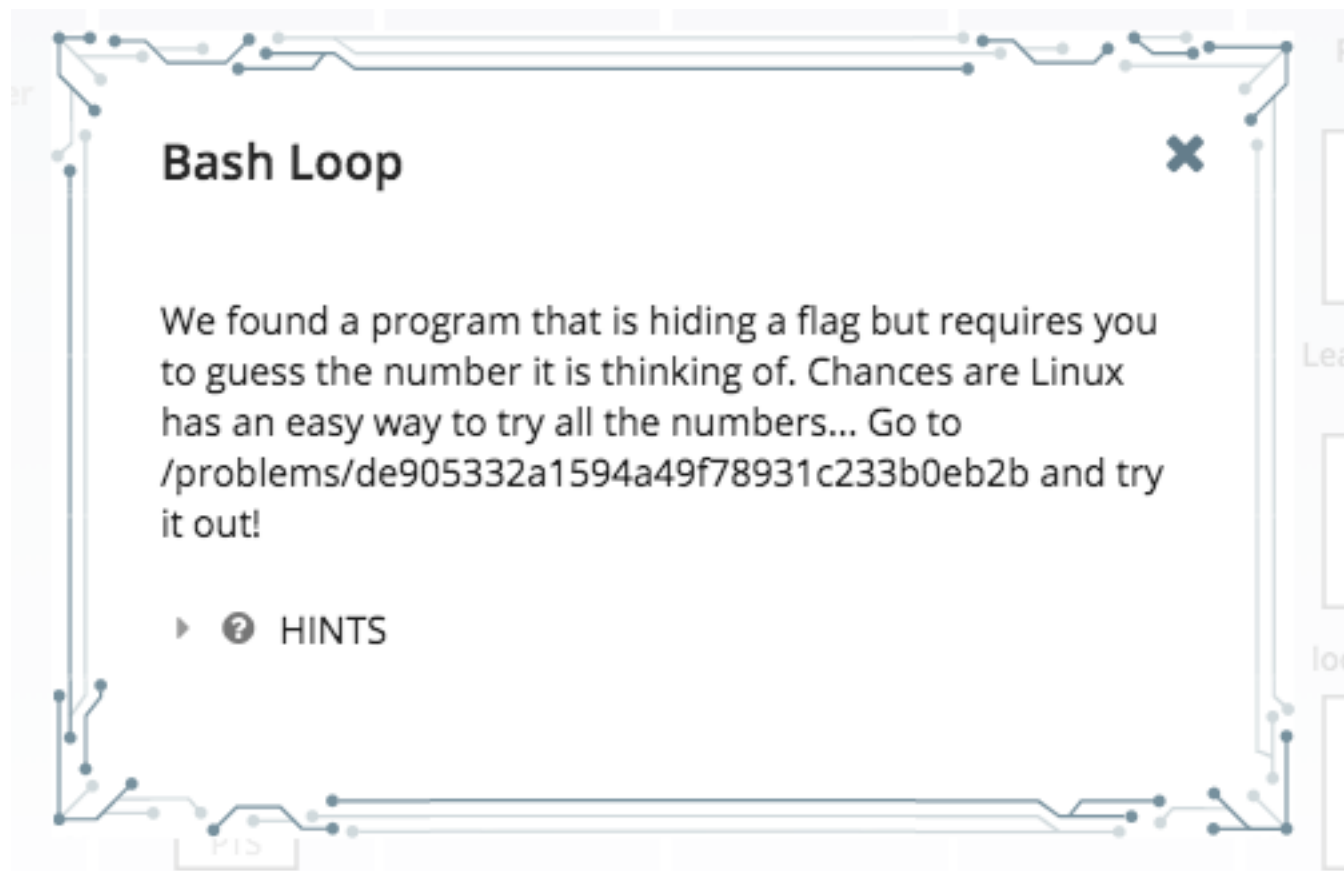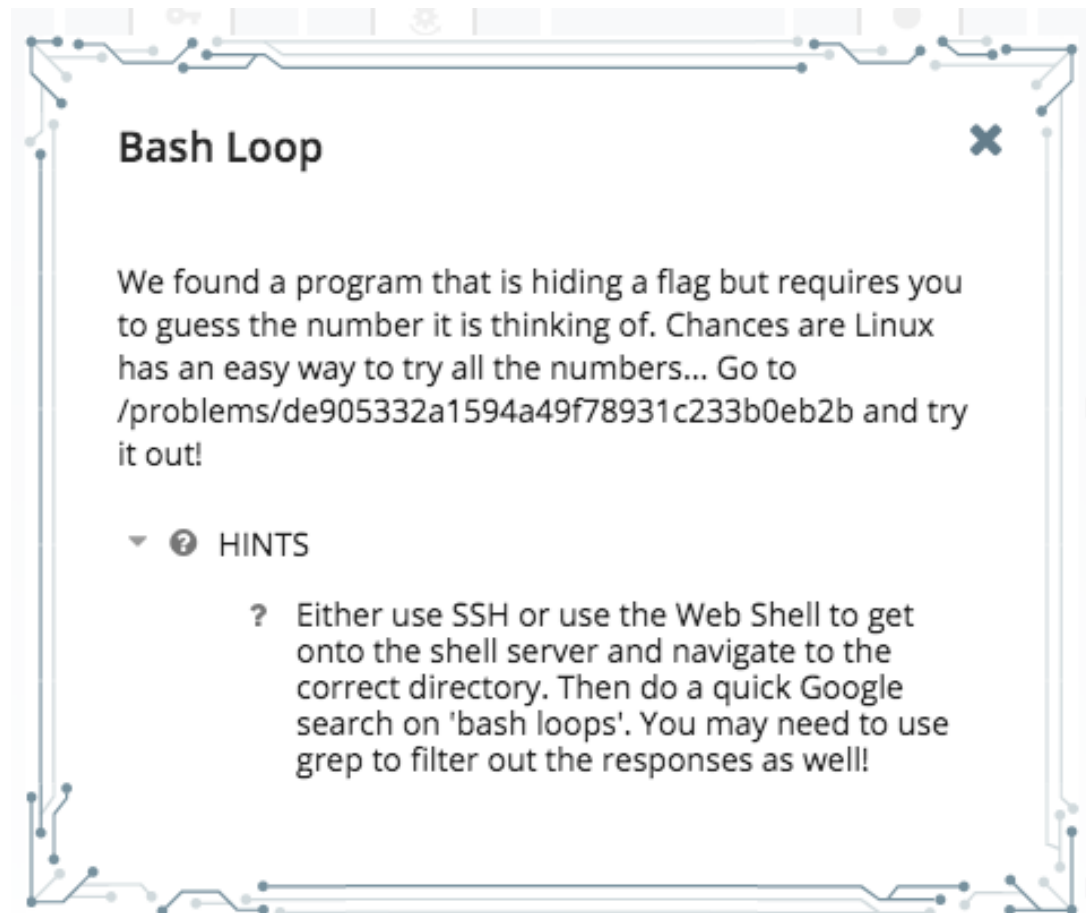
フラグを隠しているプログラムを見つけたが、どんな数字を考えているのが推測する必要がある。

# 問題文にあるところへ行って見たら



```
@shell-web:~$ cd /problems/de905332a1594a49f78931c233
b0eb2b
@shell-web:/problems/de905332a1594a49f78931c233b0eb2b
$ ls
bashloop   flag
```

# どんな数字を考えている？（０から４０９６の間)

# 問題文をよく見たら

## Bash Loop

We found a program that is hiding a flag but requires you to guess the number it is thinking of. Chances are Linux has an easy way to try all the numbers... Go to /problems/de905332a1594a49f78931c233b0eb2b and try it out!

▼ ❓ HINTS

　❓ Either use SSH or use the Web Shell to get onto the shell server and navigate to the correct directory. Then do a quick Google search on 'bash loops'. You may need to use grep to filter out the responses as well!

LINUXには全ての数字を試して見る簡単な方法がある。

- 全ての数字を確かめて見るんだ！！！

- BASHLOOPSを使う！！

# とりあえず、BASH LOOPSとgoogleで検索した。



Google

bash loops

All    Videos    Images    News    Shopping    More    Settings    Tools
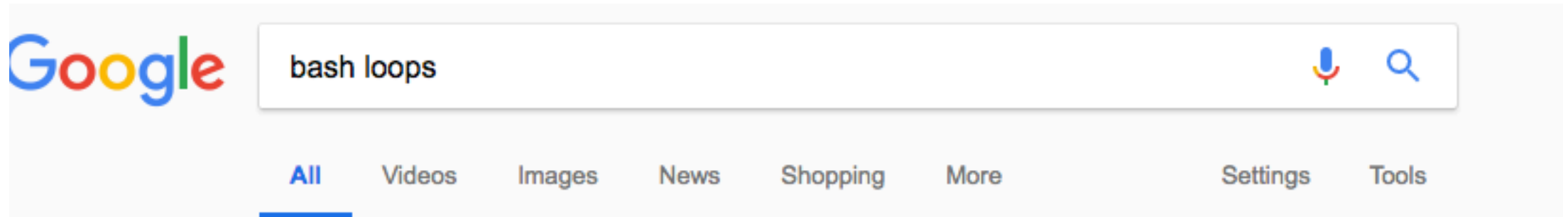
About 663,000 results (0.36 seconds)

**BASH Programming - Introduction HOW-TO: Loops for, while and until**
tldp.org/HOWTO/Bash-Prog-Intro-HOWTO-7.html ▼
**Loops** for, while and until. In this section you'll find for, while and until **loops**. The for **loop** is a little bit different from other programming languages. Basically, it let's you iterate over a series of 'words' within a string. The while executes a piece of code if the control expression is true, and only stops when it is false (or a explicit ...

ループを使用すると、一連のコマンドを実行して、特定の状況に達するまでループを再実行することができます。

Loops allow us to take a series of commands and keep re-running them until a particular situation is reached. They are useful for automating repetitive tasks.

https://ryanstutorials.net/bash-scripting-tutorial/bash-loops.php

# For文

## Ranges

We can also process a series of numbers

```
for_loop_series.sh
1.  #!/bin/bash
2.  # Basic range in for loop
3.
4.  for value in {1..5}
5.  do
6.      echo $value
7.  done
8.
9.  echo All done
```

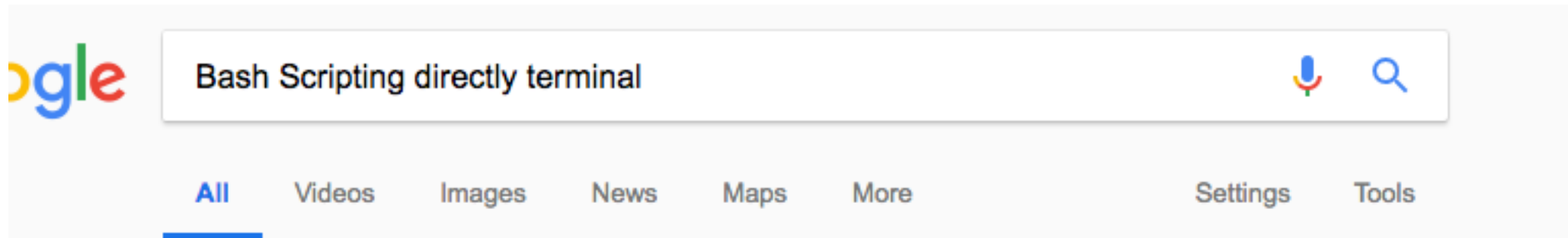# Nanoを使って、shell scriptを書こうと思ったら



```
GNU nano 2.2.6              File: for.sh                    Modified

for i in {1..4096}
        do ./bashloop $i
        echo $i
 done
```

書き込みが禁止らしい



```
                    [ Error writing for.sh: Permission denied ]
^G Get Hel^O WriteOu^R Read Fi^Y Prev Pa^K Cut Tex^C Cur Pos
^X Exit    ^J Justify^W Where I^V Next Pa^U UnCut T^T To Spell
```

# 直接ターミナル上でどうやってshell scriptを書くの

セミクロんを使えば実行できる。

```
        @shell-web:/problems/de905332a1594a49f78931c233b0eb2b
$ for i in {1..4096};
> do ./bashloop $i;
> echo $i;
> done;
```

# 結果は？

```
Nope. Pick another number between 0 and 4096
3162
Nope. Pick another number between 0 and 4096
3163
Nope. Pick another number between 0 and 4096
3164
Yay! That's the number! Here be the flag: c5d35a85c2c2ea7c69a84
f6756f57bb1

3165
Nope. Pick another number between 0 and 4096
3166
Nope. Pick another number between 0 and 4096
3167
Nope. Pick another number between 0 and 4096
3168
Nope. Pick another number between 0 and 4096
3169
```

# 参考文献

- BASH script directly in terminal: https://www.linuxquestions.org/questions/linux-software-2/bash-script-directly-in-terminal-4175534396/

- BASH LOOPS : https://ryanstutorials.net/bash-scripting-tutorial/bash-loops.php