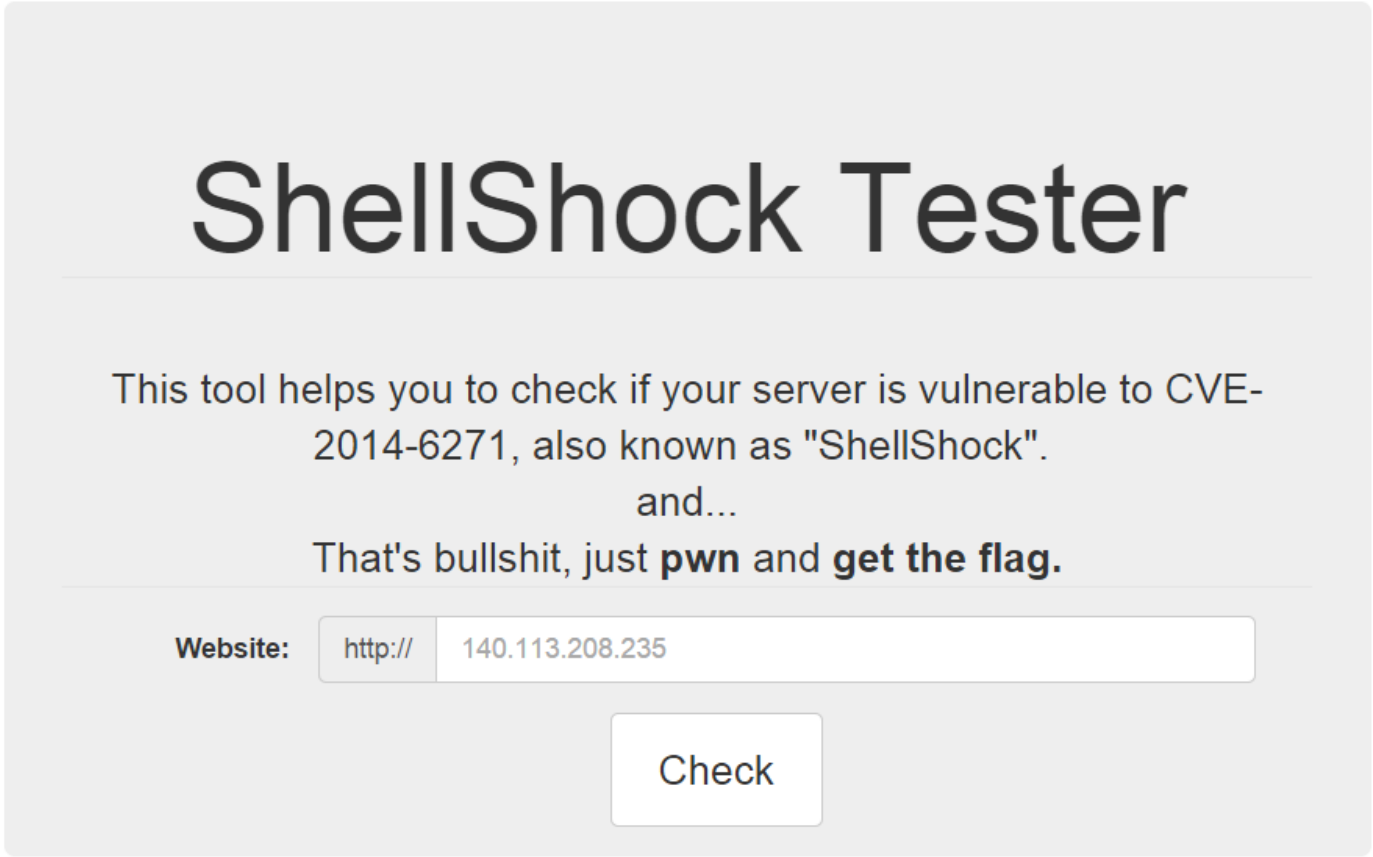
Homework 0x04 hint

ddaa

道歉啟事

- 由於前陣子忙著打 CTF，完全忘記 hw4 要放 hint 這回事...
- 因此 hw4 的 deadline 順延一星期

ShellShock



The response will be collected into database.

Course WebSite: http://secprog.cs.nctu.edu.tw Made by atdog.

ShellShock

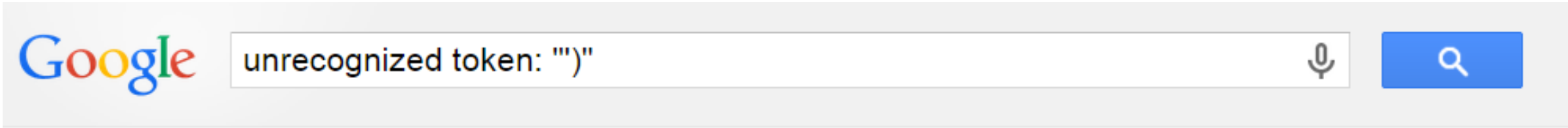
Error: IP (140.113.208.235) is not vulnerable.

Error (7): Failed to connect to 127.0.0.1 port 80: Connection refused

Error (28): Connection timed out after 2001 milliseconds

DATABASE Msg: Insert OK @2014-12-22 15:36:24

Response: ShellShockTester_atdog



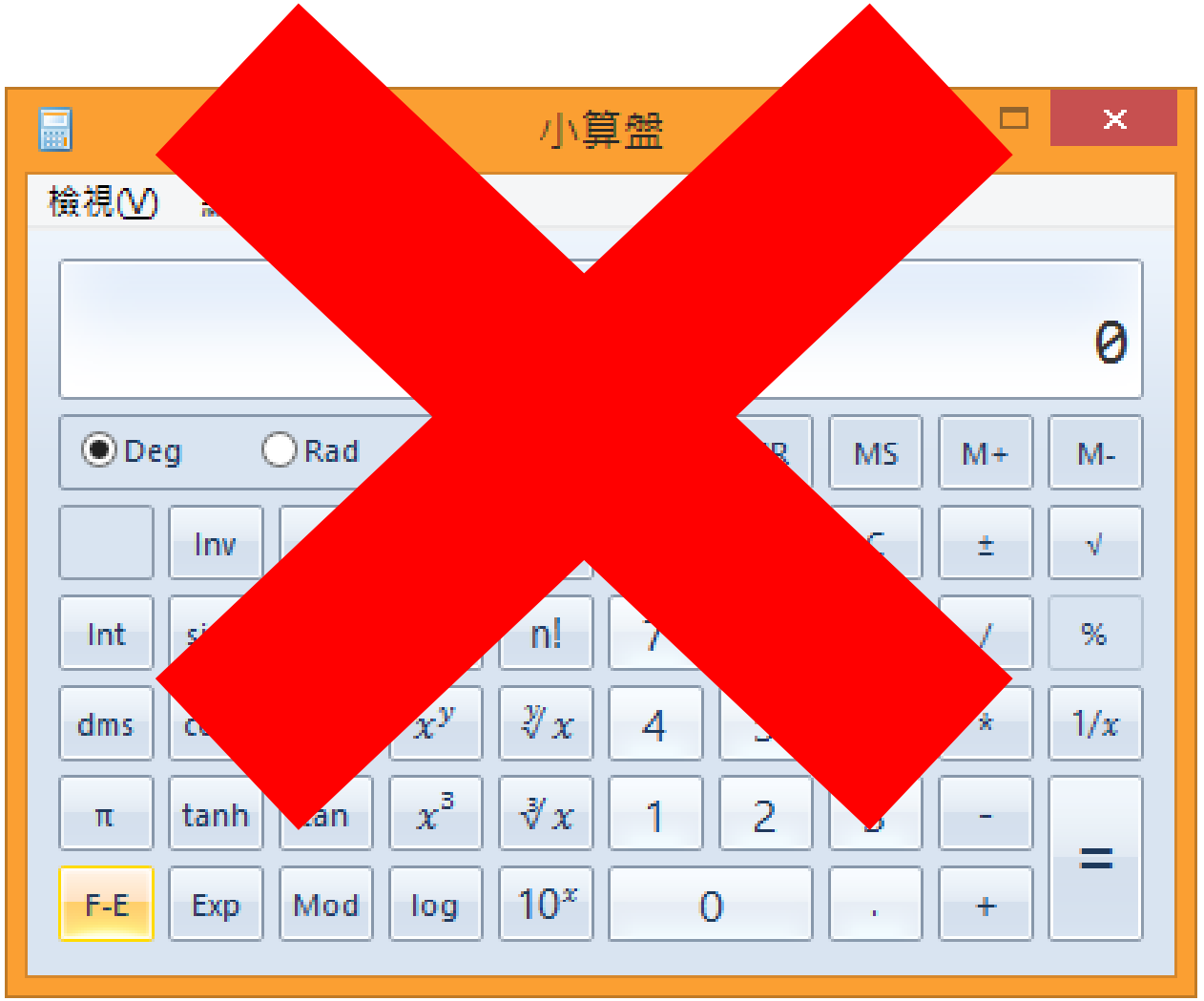
約有 335,000 項結果 (搜尋時間：0.20 秒)

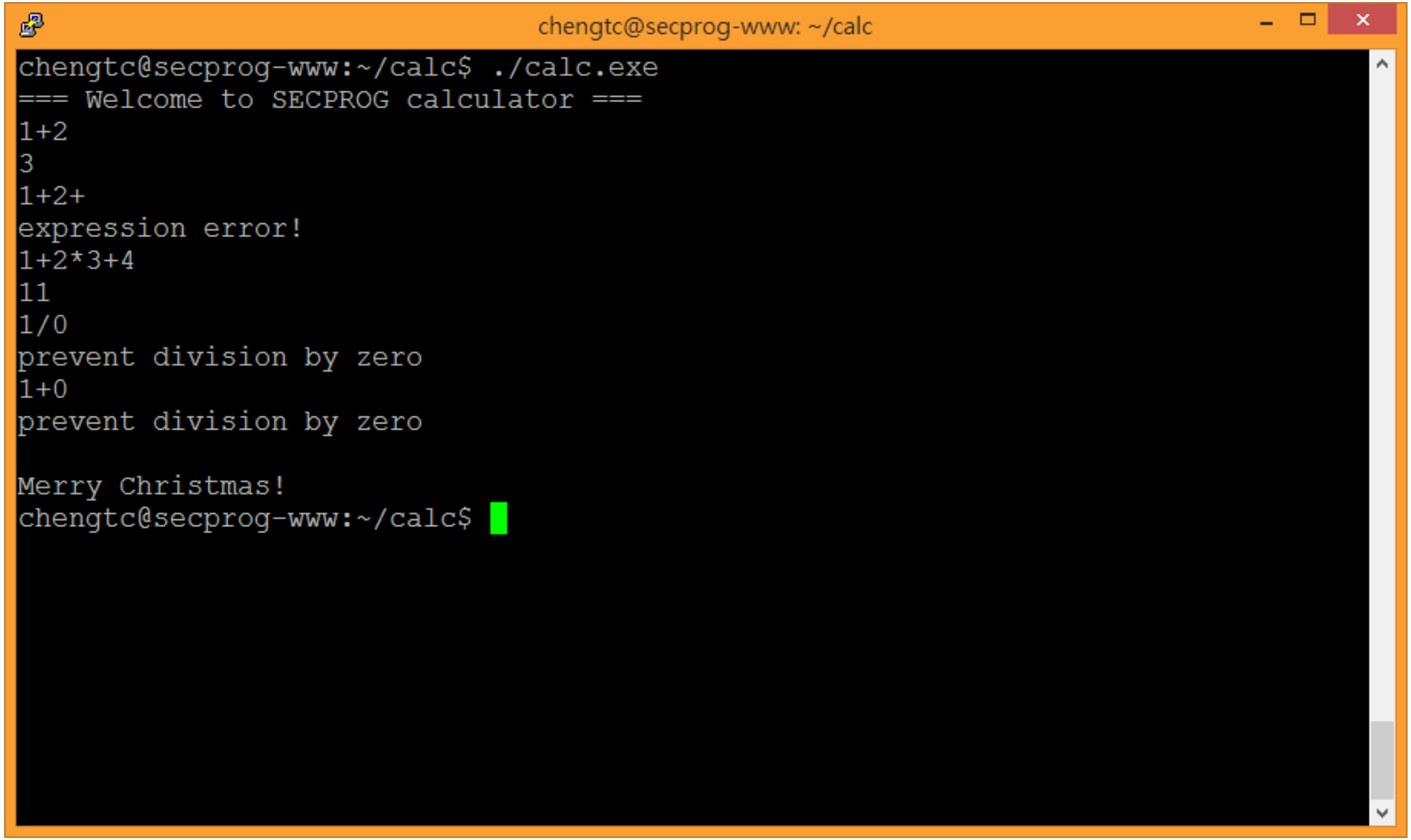
提示： 只顯示繁體中文搜尋結果。您可以在使用偏好中指定搜尋語言

SQLiteException: unrecognized token - Stack Overflow
stackoverflow.com/.../sqliteexception-**unrecognized-token** ▾ 翻譯這個網頁
2014年6月18日 - Table names cannot begin with a number, unless you use escaping symbols. Try String sqlTables = "[1_BASICA_1500]"; ...

- Union based?
- Boolean based?
- Error based?
- Time based?
- Out-of-band?

calc.exe


小算盤
檢視(V)
0
Deg
Rad
MS
M+
M-
Inv
±
√
Int
n!
%
dms
x^y
$\sqrt[y]{x}$
4
1/x
π
tanh
x^3
$\sqrt[3]{x}$
1
2
-
=
F-E
Exp
Mod
log
10^x
0
.
+


chengtc@secprog-www: ~/calc
chengtc@secprog-www:~/calc$ ./calc.exe
=== Welcome to SECPROG calculator ===
1+2
3
1+2+
expression error!
1+2*3+4
11
1/0
prevent division by zero
1+0
prevent division by zero
Merry Christmas!
chengtc@secprog-www:~/calc$

```
chengtc@secprog-www:~/calc$ objdump -R calc.exe

calc.exe:     file format elf32-i386

objdump: calc.exe: not a dynamic object
objdump: calc.exe: Invalid operation
```

gcc –static

return to libc => gg

But easier to find gadgets.

Structure

```
1  int calc()
2  {
3    int v1; // [sp+18h] [bp-5A0h]@4
4    int v2[100]; // [sp+1Ch] [bp-59Ch]@5
5    char s; // [sp+1ACh] [bp-40Ch]@2
6    int v4; // [sp+5ACh] [bp-Ch]@1
7
8    v4 = *MK_FP(__GS__, 20);
9    while ( 1 )
10   {
11     bzero(&s, 0x400u);
12     if ( !get_expr(&s, 1024) )
13       break;
14     init_pool(&v1);
15     if ( parse_expr((int)&s, (int)&v1) )
16     {
17       printf((const char *)&unk_80BF804, v2[v1 - 1]);
18       fflush(stdout);
19     }
20   }
```

```
19  for ( i = 0; ; ++i )
20  {
21    if ( (unsigned int)(*(_BYTE *)(i + a1) - 48) > 9 )
22    {
```

Without checking the bound.

```
if ( a2 == 43 )
{
  *(_DWORD *)(a1 + 4 * (*(_DWORD *)a1 - 2) + 4) += *(_DWORD *)(a1 + 4 * (*(_DWORD *)a1 - 1) + 4);
}
else if ( a2 > 43 )
```

Can we overwrite last value?

```
v10 = atoi(s1);
if ( v10 > 0 )
{
  v4 = (*(_DWORD *)a2)++;
  *(_DWORD *)(a2 + 4 * v4 + 4) = v10;
}
```

Try to pass filter!

Homework 成績計算

- 大家作業繳交狀況欠佳，因此取消作業五，希望大家都可以把前四個作業做出來
- 作業佔總成績 40%，因此每個作業佔總成績 5 分
- 準時繳交可以拿到 5 分，前三名解出額外加成 1、0.5、0.25 分
  - 以送 flag 的時間為基準
  - 需繳交 write up，沒交 write up 視同未完成作業
- 遲交以每個星期為區間扣 0.2 分，扣到 3.8 分不再向下扣，因此學期末之間繳交都可以拿到 3.8 分
- Homework 3-3 eliza (bonus) 算一次作業成績