Smartphone game vulnerabilities, cheats and countermeasures

By Seunghyun Seo

※ All the vulnerabilities were already reported to related company in 2013/6/16

Native Game

※ What's this background picture?


Let’s trace!

So many vulnerabilities !

Really?

Realie?

A mount of fishes !

Look delicious~

Dive deep into smartphone game world

MSIL?

ARM

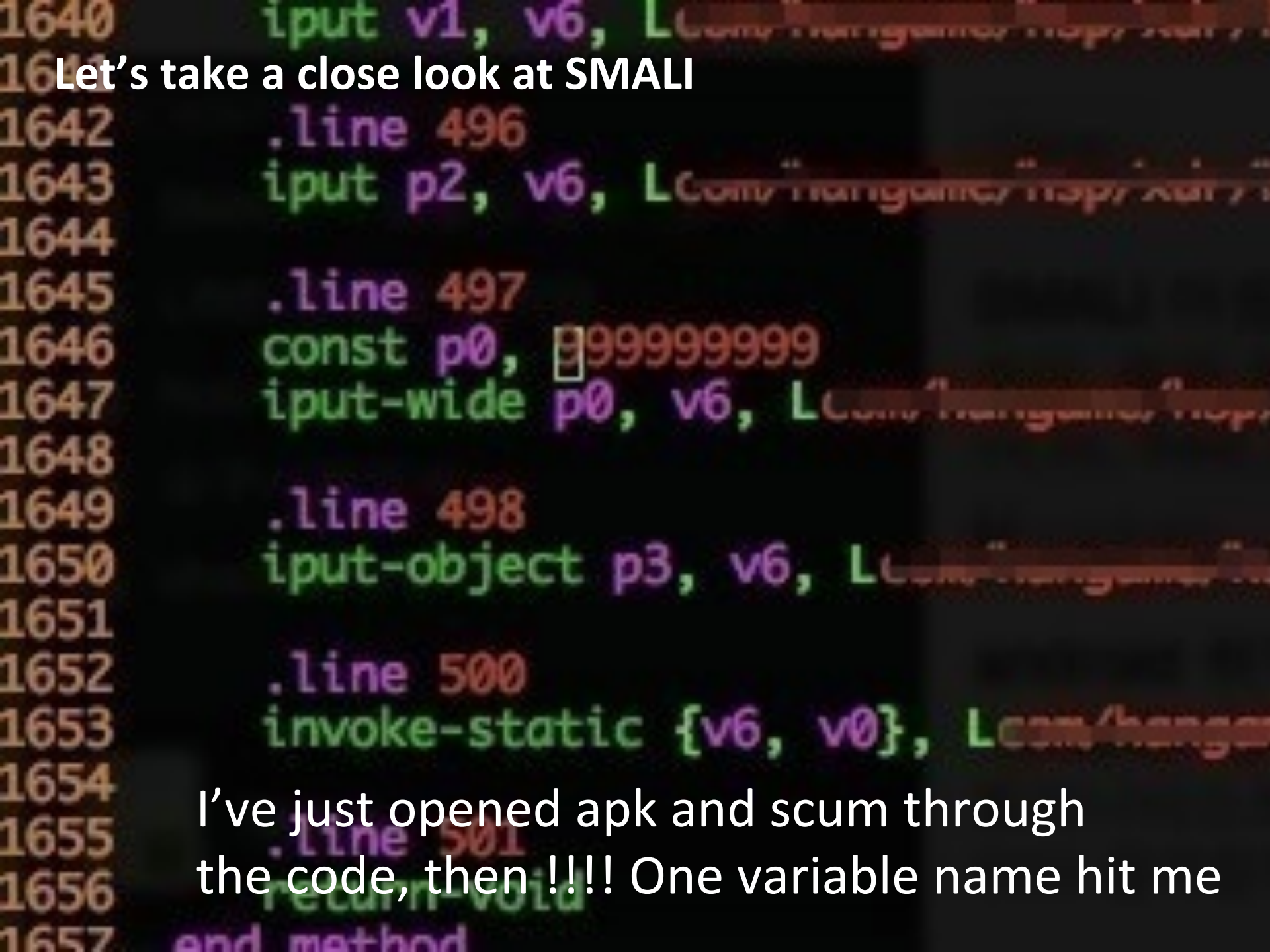
SMALI

ARM64


In 2013,
Japanese smartphone market
Enjoyed a sort of puzzle game
boom

I’d decided to play with one of the top 5 puzzle games.

Now, I will share the most vulnerable game among them


Let’s take a close look at SMALI
1640 iput v1, v6, L
1642 .line 496
1643 iput p2, v6, L
1644
1645 .line 497
1646 const p0, 99999999
1647 iput-wide p0, v6, L
1648
1649 .line 498
1650 iput-object p3, v6, L
1651
1652 .line 500
1653 invoke-static {v6, v0}, L
1654
1655 .line 501
1656 return-void
1657 .end method
I’ve just opened apk and scum through the code, then !!!! One variable name hit me


17
2919
16
97%
RANKING
5D LEFT
4
1
승현테스트
999,999,999
katakana
2
1,669,732
oo
3
979,999
4
917,173
DAILY MISSION
(0/1,600,000) points!
SHOP
READY
INVITE
WoW !
※ All the vulnerabilities were already reported t

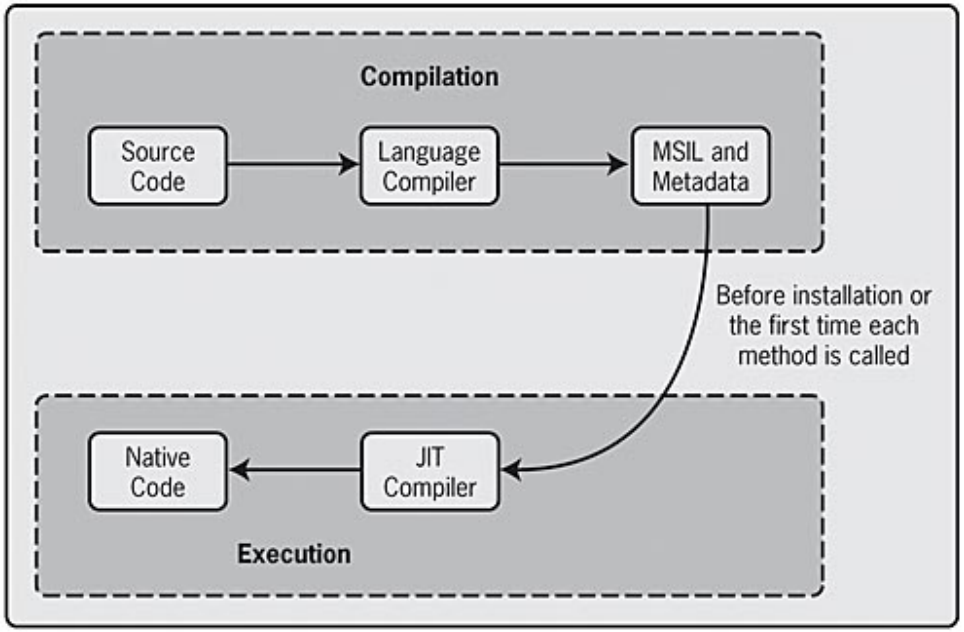
And MSIL :-)

Microsoft Intermediate Language

CIL's Microsoft version which is used in .NET

add, sub, div, mul,
br, jmp, call, ret,
ldloc.0, stloc.0, ldc.i4.0
ldstr, ldfld, ldobj,
shl, and, or, xor,
….

Looks very similar to x86 assembly language



```
/**
static void add()
{
    int value1 = 10;
    int value2 = 20;
    int value3 = value1 + value2;
}
*/

.method private hidebysig static void  'add'() cil managed
{
  // Code size       12 (0xc)
  .maxstack  2
  .locals init ([0] int32 value1,
           [1] int32 value2,
           [2] int32 value3) // three int32 local variables are declared

  IL_0000:  nop  // no operation ( no push or pop on the stack)

  IL_0001:  ldc.i4.s   10  //loads the int32 value(10) on the stack. Item on Stack=1

  IL_0003:  stloc.0 // pops off the item from the stack and stores in first local variable.
                    //Item on Stack=0

  IL_0004:  ldc.i4.s   20 //loads the int32 value(20) on the stack.Item on the stack =1

  IL_0006:  stloc.1 0 // pops off the item from the stack and stores in second local variable .
                      //Item on Stack=0

  IL_0007:  ldloc.0// Loads the value of first local variable on the stack. Item on Stack=1

  IL_0008:  ldloc.1// Loads the value of second local variable on the stack. Item on Stack=2

  IL_0009:  add //(Pops off first two numeric value from the stack and sends the result
                // back to the stack) //Item on stack=2-2+1=1
  IL_000a:  stloc.2 //(Pop off the item from the stack and store it in local variable [3].
                    //Item on the Stack=0

  IL_000b:  ret
} // end of method Program::'add'
```

It looks like this☺

```
ldc.i4   0xBB9
stsfld   int32 Global::_renderQueueEffect
ldc.i4   0xF3C
stsfld   int32 Global::_renderQueuePopup
ldc.i4.0
stsfld   int32 Global::
ldc.i4   0xDD
stsfld   int32 Global
ldc.i4   0x159
stsfld   int32 Global::
ldc.i4.s 0x76
stsfld   int32 Global::
ldc.i4.0
stsfld   bool Global::
ldc.i4   0x22111F
stsfld   int32 Global::mGameTime
ldc.i4   0x55183C
stsfld   int32 Global::
ldc.i4.3
stsfld   int32 Global::
ldc.i4   0x1BE
stsfld   int32 Global::
ldc.i4.0
```

```
  ldc.i4.s 0x76
  ldarg.0
  ldc.i4   0x577423
  xor
  add
  stsfld   int32 Global::mExp
  ret
}
.method public static hidebysig specialname int32 get__game
                                        // CODE XREF: SetTime
                                        // ResetStaticData+22
{
  .maxstack 8
  ldsfld   int32 Global::mGameTime
  ldc.i4   0x221123
  xor
  ret
}

.method public static hidebysig specialname int32 get__bonu
                                        // CODE XREF: SetTime
                                        // ResetStaticData+38
{
  .maxstack 8
  ldsfld   int32 Global::mBonusGameTime
  ldc.i4   0x551822
```

The most important feature
In puzzle game is the time limit
So, I just tried to look into more…

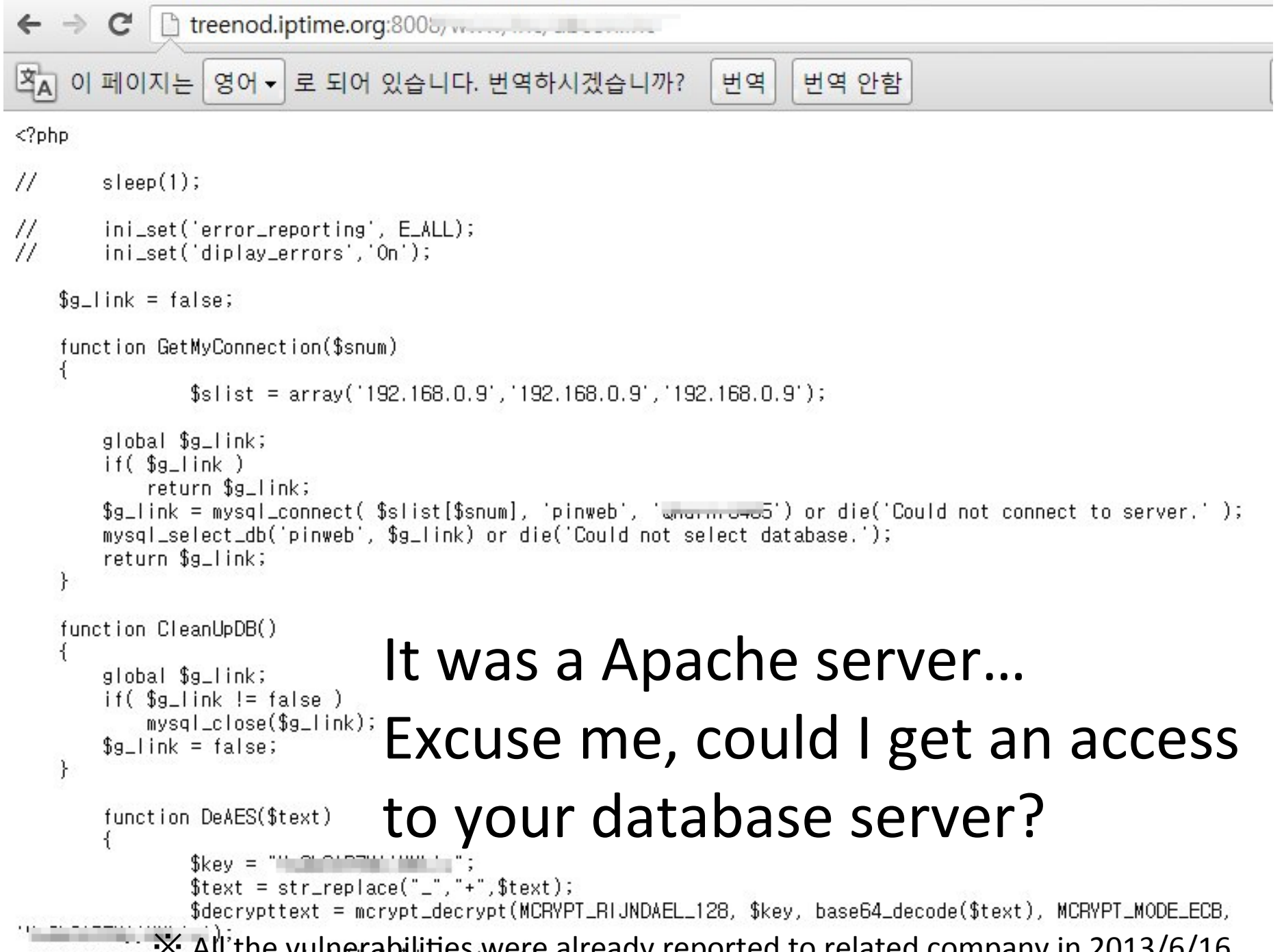
0x22111F ^ 0x221123 = ?

0x22111F ^ 0xffffffff= ?

if modified, this game will not end forever…

※ All the vulnerabilities were already reported to related company in 2013/6/16

```
loc_53F16:                              // CODE XREF: sub_53A50+4AF↑j
    ldsfld   class Global Global::instanse
    ldfld    bool Global::koreaTest
    brfalse  loc_53F2F
    ldstr    "http://treenod.iptime.org:8008/www/new/"
    stsfld   string Global::gameServerAddress

loc_53F2F:                              // CODE XREF: sub_53A50+4D0↑j
    ldc.i4.4
    stsfld   valuetype DataLoadState DataManager::_state
    ldarg.0
    ldsfld   string [mscorlib]System.String::Empty
    stfld    string <Start>c__Iterator25::<data>__5
    ldsfld   class CommandManager CommandManager::instanse
    ldstr    "gettime.php"
    ldarg.0
    ldfld    string <Start>c__Iterator25::<data>__5
    ldarg.0
    ldfld    class DataManager <Start>c__Iterator25::<>f__this
    ldftn    instance class [mscorlib]System.Collections.IEnumerator DataManager::CommandD
    newobj   instance void CommandDelegate::.ctor(object object, native int method)
    ldc.i4.0
    callvirt instance void CommandManager::AddCommend(string in_command, string in_data, c

loc_53F67:                              // CODE XREF: sub_53A50:loc_53F8F↓j
    ldarg.0
    ldfld    class DataManager <Start>c__Iterator25::<>f__this
    ldfld    bool DataManager::time_result
    brfalse  loc_53F7C
    br       loc_53F94
```



It was a Apache server…
Excuse me, could I get an access to your database server?

※ All the vulnerabilities were already reported to related company in 2013/6/16

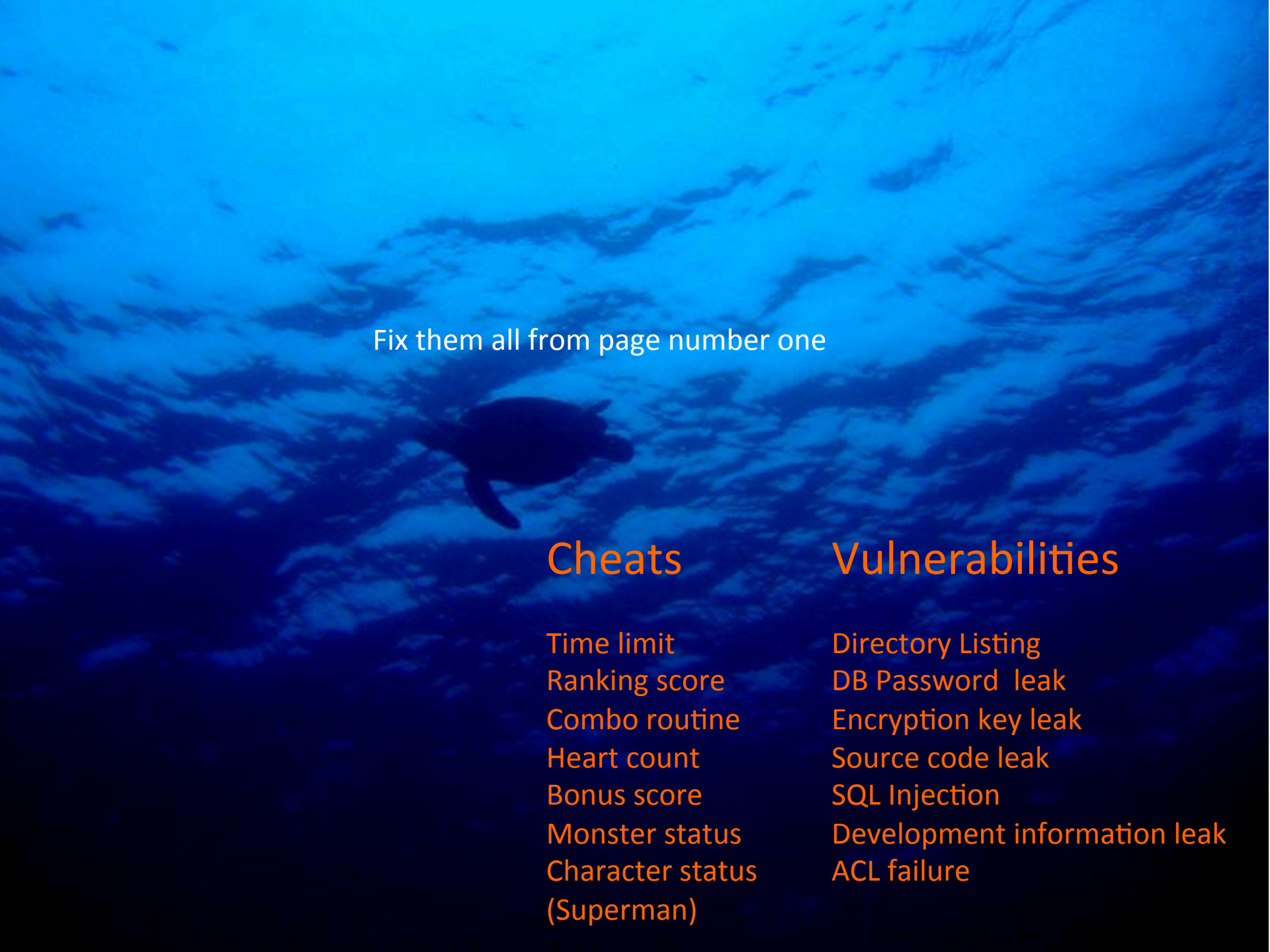

/www/old/pp_0326.zip
!!!

setresult.php
listinvite.php
addinvite.php
uplevel.php
getsendclover.php
sendrequestnoback.php
sendrequestback.php
join.php
my.php
addanib.php
addslot.php
buyclover.php
buycoin.php
buyjewel.php
countclover.php
getallclover.php
getclover.php
gettime.php
listanib.php
listclover.php
listcloverx.php

```
$qarr = DeAES($_POST["q"]);

if($qarr[0] == basename(__FILE__, '.php'))
{
        $clover = "";

// redis에서 해당 서버 가지고온다.
        $myserver = intval($qarr[1]);
        $sql = "delete from users where sno = '" . $qarr[2] . "

        $result = mysql_query($sql, GetMyConnection($myserver)
        if(!$result)
                oret(-1);

        $sql = "delete from users where sno = '" . $qarr[2] . "'

        $result = mysql_query($sql, GetMyConnection($myserver)
        if(!$result)
                oret(-1);

        $sql = "delete from clovers where sno = '" . $qarr[2] .

        $result = mysql_query($sql, GetMyConnection($myserver)
        if(!$result)
                oret(-1);
```

A bunch of
SQL injection vulnerabilities
☺


got tired of it….



Fix them all from page number one

Cheats

Time limit
Ranking score
Combo routine
Heart count
Bonus score
Monster status
Character status (Superman)

Vulnerabilities

Directory Listing
DB Password leak
Encryption key leak
Source code leak
SQL Injection
Development information leak
ACL failure

After that, I've also looked into the other games, but sad thing is that there were a bunch of vulnerabilities on them too.

So, for strengthening smart phone game apps

1. Security review by security expert on developing phase
2. pen-testers or security consultant before release phase
3. Security scan for game servers
4. Source code review or white box check for removing potential security risk

Please do your best !

Seeking for more secure and better smartphone game world

Thank you for listening