9/14 @/


就只是個廢物
社長
童舒晧
全社最廢、最智障、最帥
資訊大三
專長：網頁安全 / 耍廢

介紹


喵
林飛飛
顧問
資訊系大四
專長：資訊安全 / 網站開發

介紹

-
-
- CTF

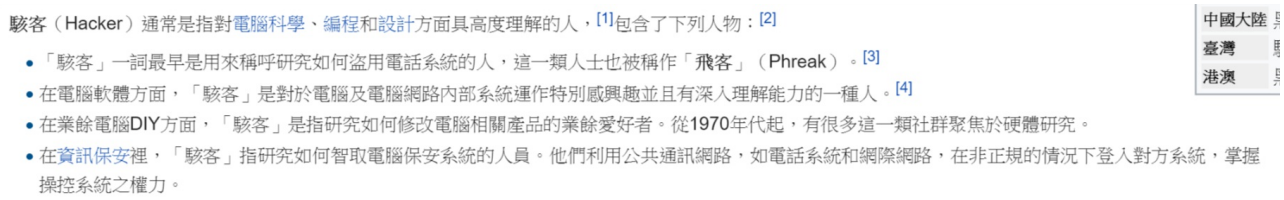
- Google Hacking
-
-

- demo
- ?
-
-
- CTF
- CTF
- google

---

whAt 1S HacK3R ?

[google (http://lmgtfy.com/?q=)](http://lmgtfy.com/?q=)



駭客（Hacker）通常是指對電腦科學、編程和設計方面具高度理解的人，[1]包含了下列人物：[2]

- 「駭客」一詞最早是用來稱呼研究如何盜用電話系統的人，這一類人士也被稱作「飛客」（Phreak）。[3]
- 在電腦軟體方面，「駭客」是對於電腦及電腦網路內部系統運作特別感興趣並且有深入理解能力的一種人。[4]
- 在業餘電腦DIY方面，「駭客」是指研究如何修改電腦相關產品的業餘愛好者。從1970年代起，有很多這一類社群聚焦於硬體研究。
- 在資訊保安裡，「駭客」指研究如何智取電腦保安系統的人員。他們利用公共通訊網路，如電話系統和網際網路，在非正規的情況下登入對方系統，掌握操控系統之權力。

中國大陸
臺灣
港澳

-
-
-

---

try

第 358 條
無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 359 條
無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 360 條
無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 361 條
對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
第 362 條
製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 363 條
第三百五十八條至第三百六十條之罪，須告訴乃論。

- '
- '
- google
-

- ,(https://gotyour.pw/)(gotyour.pw)
-
  - 

Ithome (https://www.ithome.com.tw/security) ←
(https://technews.tw/category/internet/%E8%B3%87%E8%A8%8A%E5%AE%89%E5%85%A8/)
(https://blog.trendmicro.com.tw/)
TDOH- (http://tdohacker.org/)

100

200

...ww

CTF

- Capture The Flag
-
- /
- Flag
- Flag
- Flag

CTF

- Reserve
- Pwn
- Web
- Crypto
- Forensic
- Misc
-

Reserve

-
-
-
- C
- APP
-
-

Reserve

- (binary)
-
-
-

```
int a = 1;
if (a == 87)
    getFlag();
else
    print("no flag");
```

Reserve

- (Static Analysis)
    - Global & Static data
- (Dynamic Analysis)
    - Registers()Memory()

PWN

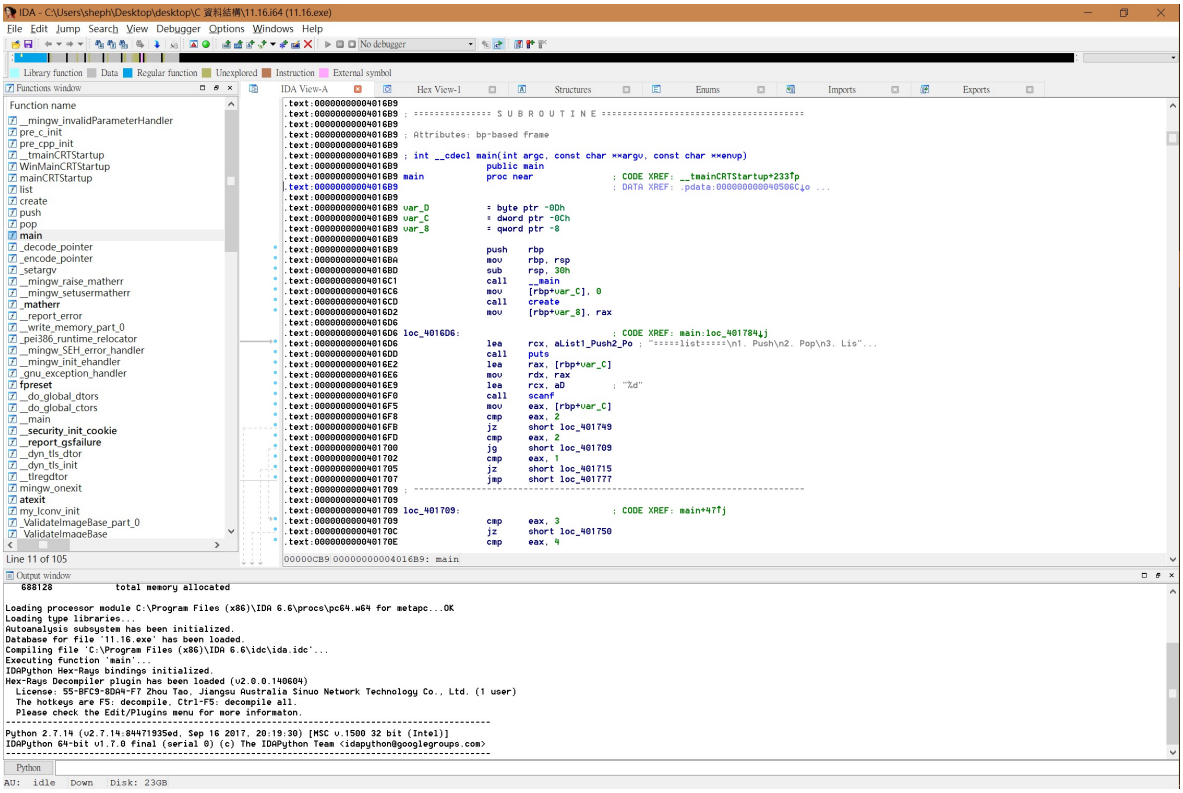
- (Reverse)(binary)
-
-

PWN

- (analysis)➔(bug)➔(exploit)
- bug
    - Buffer overflow,...etc
- exploit
    - (get shell)

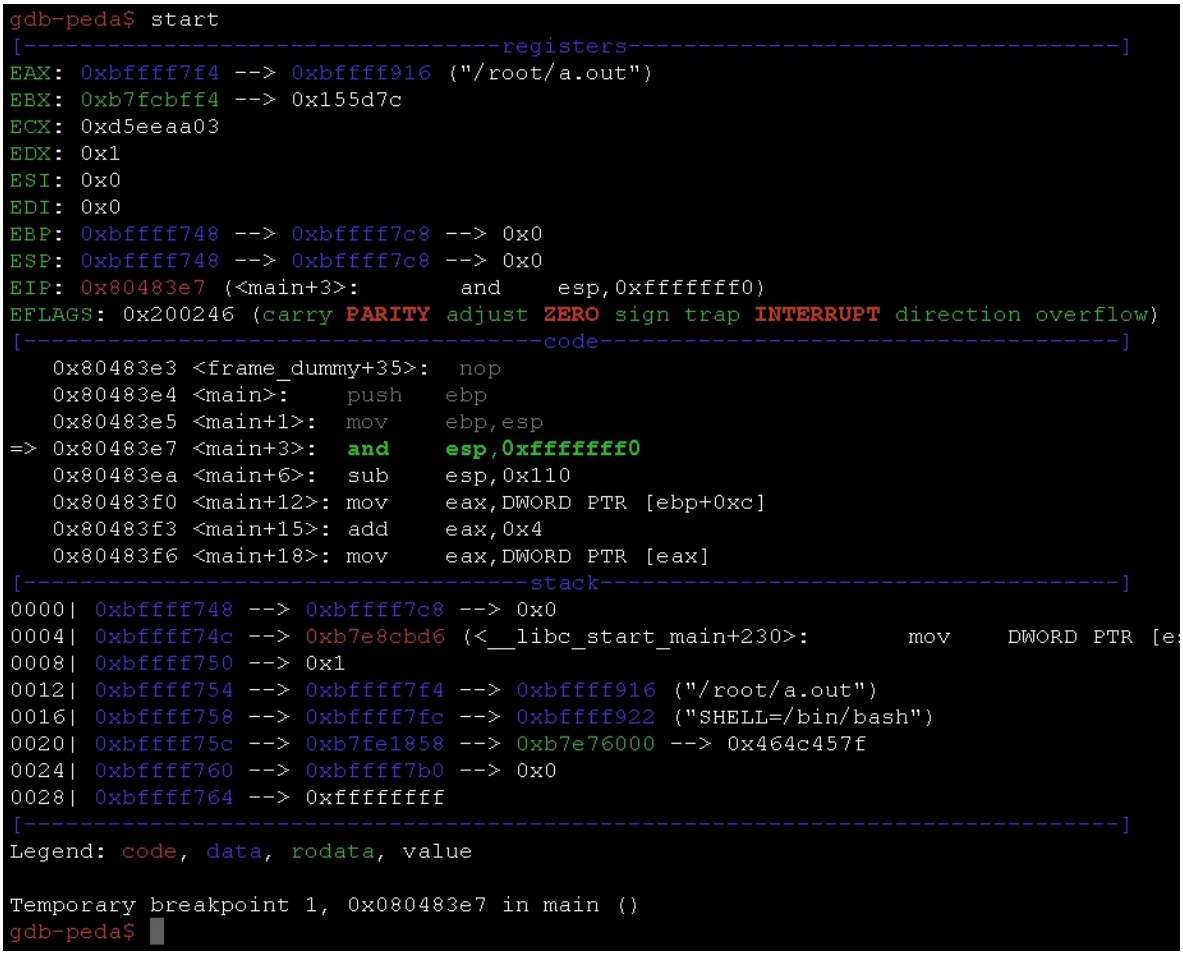
PWN

- IDA Pro
-

- 
IDA - C:\Users\sheph\Desktop\desktop\C 資料結構\11.16.i64 (11.16.exe)
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
__mingw_invalidParameterHandler
pre_c_init
pre_cpp_init
__tmainCRTStartup
WinMainCRTStartup
mainCRTStartup
list
create
push
pop
main
_decode_pointer
_encode_pointer
_setargv
__mingw_raise_matherr
__mingw_setusermatherr
_matherr
__report_error
__write_memory_part_0
_pei386_runtime_relocator
__mingw_SEH_error_handler
__mingw_init_ehandler
_gnu_exception_handler
fpreset
__do_global_dtors
__do_global_ctors
__main
__security_init_cookie
__report_gsfailure
__dyn_tls_dtor
__dyn_tls_init
__tlregdtor
mingw_onexit
atexit
my_lconv_init
_ValidateImageBase_part_0
_ValidateImageBase
Line 11 of 105
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
.text:00000000004016B9 ; =============== S U B R O U T I N E =======================================
.text:00000000004016B9 ; Attributes: bp-based frame
.text:00000000004016B9 ; int __cdecl main(int argc, const char **argv, const char **envp)
.text:00000000004016B9 main proc near ; CODE XREF: __tmainCRTStartup+233↑p
.text:00000000004016B9 ; DATA XREF: .pdata:0000000000405...
.text:00000000004016B9 var_D = byte ptr -0Dh
.text:00000000004016B9 var_C = dword ptr -0Ch
.text:00000000004016B9 var_8 = qword ptr -8
.text:00000000004016B9 push rbp
.text:00000000004016BA mov rbp, rsp
.text:00000000004016BD sub rsp, 30h
.text:00000000004016C1 call __main
.text:00000000004016C6 mov [rbp+var_C], 0
.text:00000000004016CD call create
.text:00000000004016D2 mov [rbp+var_8], rax
.text:00000000004016D6 loc_4016D6: ; CODE XREF: main:loc_401784↓j
.text:00000000004016D6 lea rcx, aList1_Push2_Po ; "=====list=====\n1. Push\n2. Pop\n3. Lis"...
.text:00000000004016DD call puts
.text:00000000004016E2 lea rax, [rbp+var_C]
.text:00000000004016E6 mov rdx, rax
.text:00000000004016E9 lea rcx, aD ; "%d"
.text:00000000004016F0 call scanf
.text:00000000004016F5 mov eax, [rbp+var_C]
.text:00000000004016F8 cmp eax, 2
.text:00000000004016FB jz short loc_401749
.text:00000000004016FD cmp eax, 2
.text:0000000000401700 jg short loc_401709
.text:0000000000401702 cmp eax, 1
.text:0000000000401705 jz short loc_401715
.text:0000000000401707 jmp short loc_401777
.text:0000000000401709 ; ---
.text:0000000000401709 loc_401709: ; CODE XREF: main+47↑j
.text:0000000000401709 cmp eax, 3
.text:000000000040170C jz short loc_401750
.text:000000000040170E cmp eax, 4
00000CB9 0000000004016B9: main
Output window
688128 total memory allocated
Loading processor module C:\Program Files (x86)\IDA 6.6\procs\pc64.w64 for metapc...OK
Loading type libraries...
Autoanalysis subsystem has been initialized.
Database for file '11.16.exe' has been loaded.
Compiling file 'C:\Program Files (x86)\IDA 6.6\idc\ida.idc'...
Executing function 'main'...
IDAPython Hex-Rays bindings initialized.
Hex-Rays Decompiler plugin has been loaded (v2.0.0.140604)
License: 55-BFC9-8DA4-F7 Zhou Tao, Jiangsu Australia Sinuo Network Technology Co., Ltd. (1 user)
The hotkeys are F5: decompile, Ctrl-F5: decompile all.
Please check the Edit/Plugins menu for more informaton.
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:19:30) [MSC v.1500 32 bit (Intel)]
IDAPython 64-bit v1.7.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
Python
AU: idle Down Disk: 23GB

PWN

- gdb
-



Web Security

-
-
-

Web Security

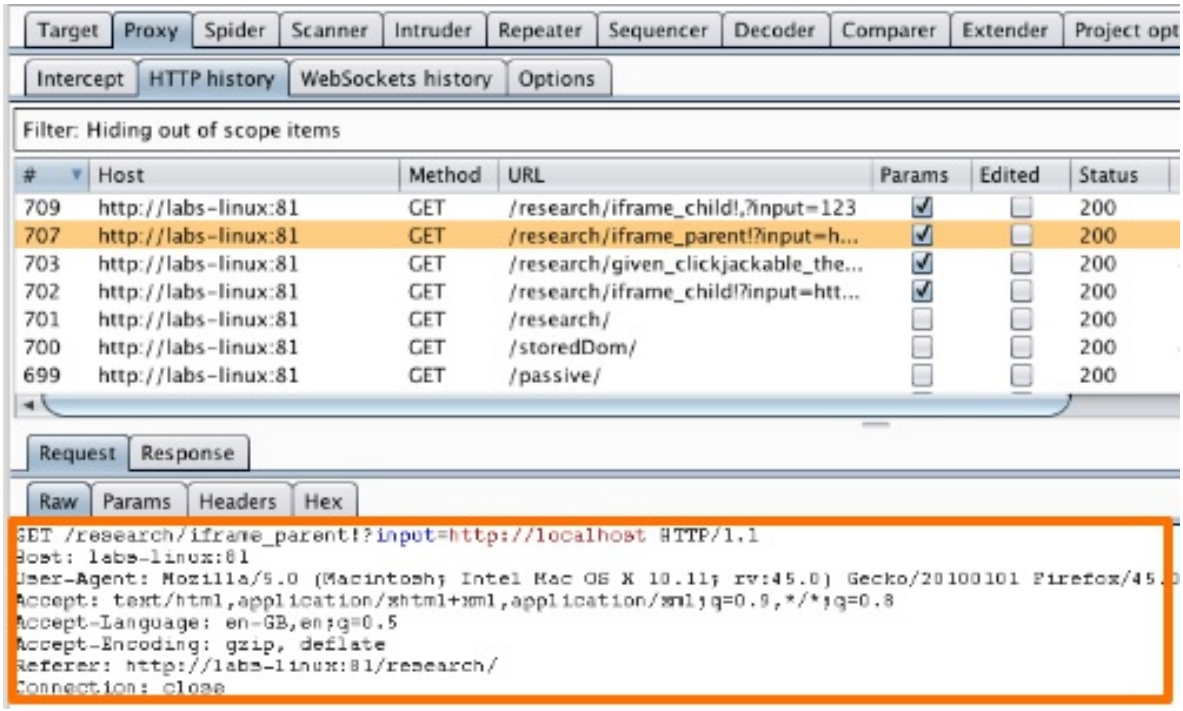
- →→
-
    - (framework)
    -

Web Security

-
    - (POSTGET)(login)
-
    - XSS, SQL Injection, File Inclusion, Command Injection, …etc
    - OWASP Top 10

Web Security

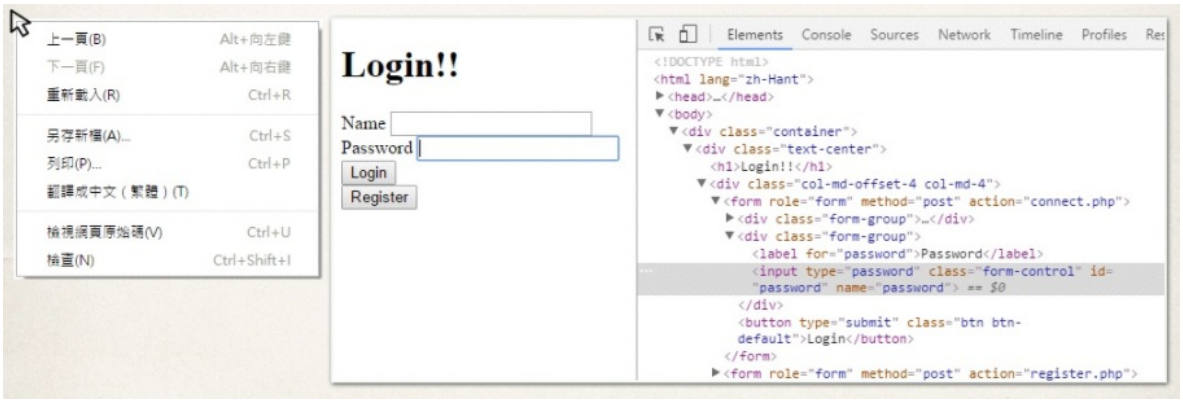
- Burp Suite



-

Web Security

- (F12)
- '



Crypto

-
-

Crypto

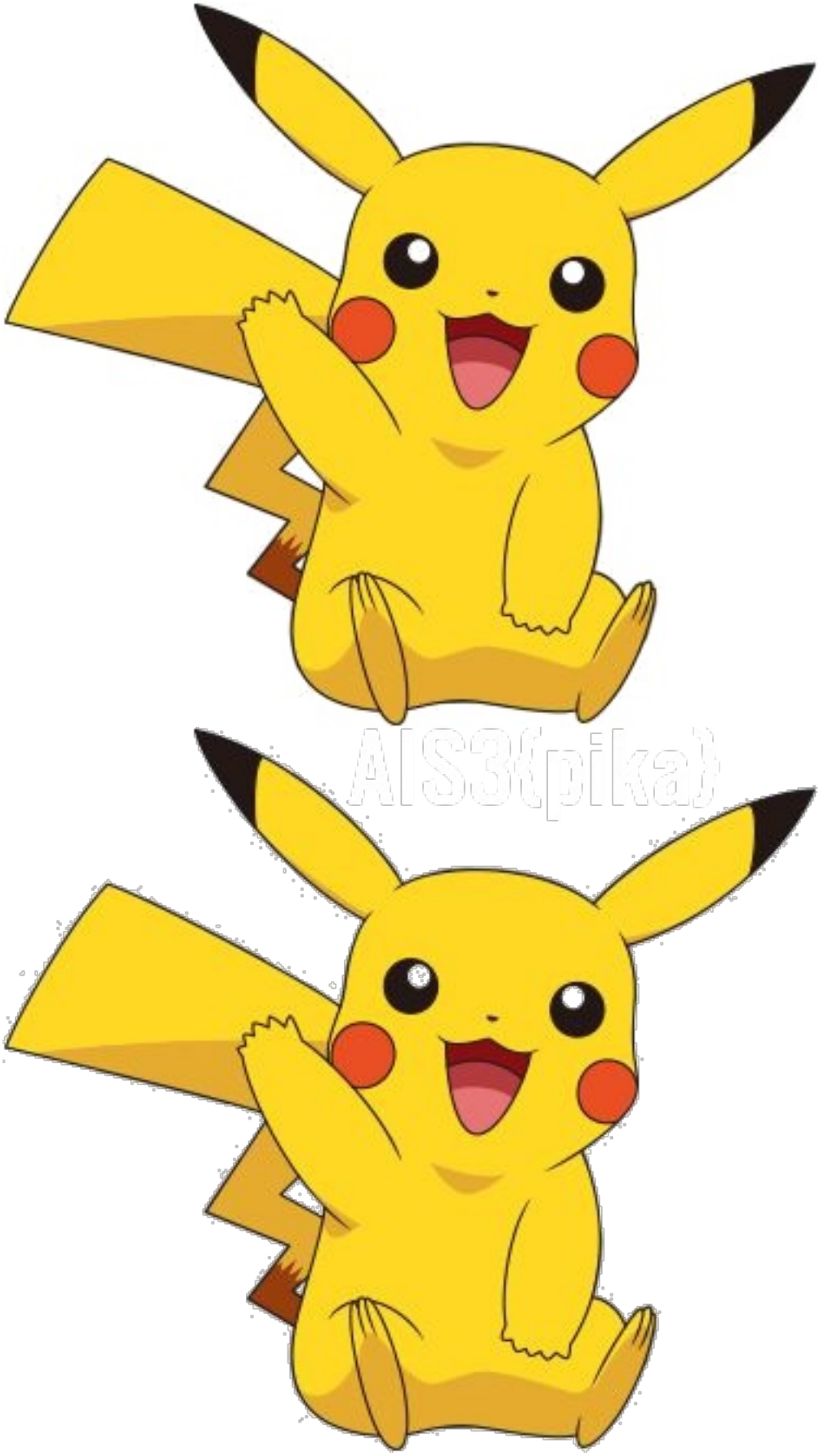
-

    - SHAMD5
-
    - AESDES()
    - RSA()
-
    -
    - OpenSSL
    - rsatool

Forensic

- (Steganography)
-

Forensic



Forensic

-
- Log
-
-
    -
    - Wireshark

Misc

- CryptoPwn
- Web Pwn
- Pwn + Web Crypto

CTF

- Jeopardy
- Attack & Defense
- King of Hill

Jeopardy

-
-
-
-

Attack & Defense

-
    -
    -
    - (exploit)
    - (patch)

Attack & Defense

-
-
- Flag
- Flag

    - Flag
    - Flag

Attack & Defense

- !
    -
        -

King of the Hill

- Flag
-
-
-

CTF

-
    - CSAW
        - NYU
    - ASIS
        -

CTF

-
    - PlaidCTF
        - PPP
    - SECCON
        -
    - Boston Key Party
        -
    - CodeGate
        -
    - RuCTFE
        -

CTF

-
    - XCTF
        -
    - DEFCON CTF
        -
        - CTF
        - Qualified CTF Final CTF
        - DEFCON
    - HITCON CTF
        -
        - DEFCON

CTF

-
    - WCTF
        -
        - WindowsLinux
    - CGC(Cyber Grand Challenage)
        - DARPA CTF
        -
        -
        -

CTF

- CTF TIME (https://ctftime.org/)
- GitHub - CTFs (https://github.com/ctfs)
- HITCON Knowledge Base (http://kb.hitcon.org/)
- pwnable(http://pwnable.kr/)
- Wargames(http://overthewire.org/wargames/)
    - practice security concepts in the form of fun-filled games
- W3Challs(https://w3challs.com/)

---

google hacking

http://lmgtfy.com/?q=google

- google
-
- ★★★★★
-
- ?!

- intext
    -

```
intext:
```

- intitle
    -

```
intitle:index of
```

    - server

```
intitle:"index of" (mp3)
```

- cache
    - google

```
cache:
```

- define
    -

```
define:hacker
```

- filetype
    -

```
filetype:pdf
doc,docx,ppt,xls...
```

    -
- info
    -

```
info:www.fcu.edu.tw
```

- related
    -

```
related:www.fcu.edu.tw
```

- inurl
    -

```
inurl:www.fcu.edu.tw
```

- site
    -

```
site:www.fcu.edu.tw
```

-

```
+ google
-
~
.
*
""
```

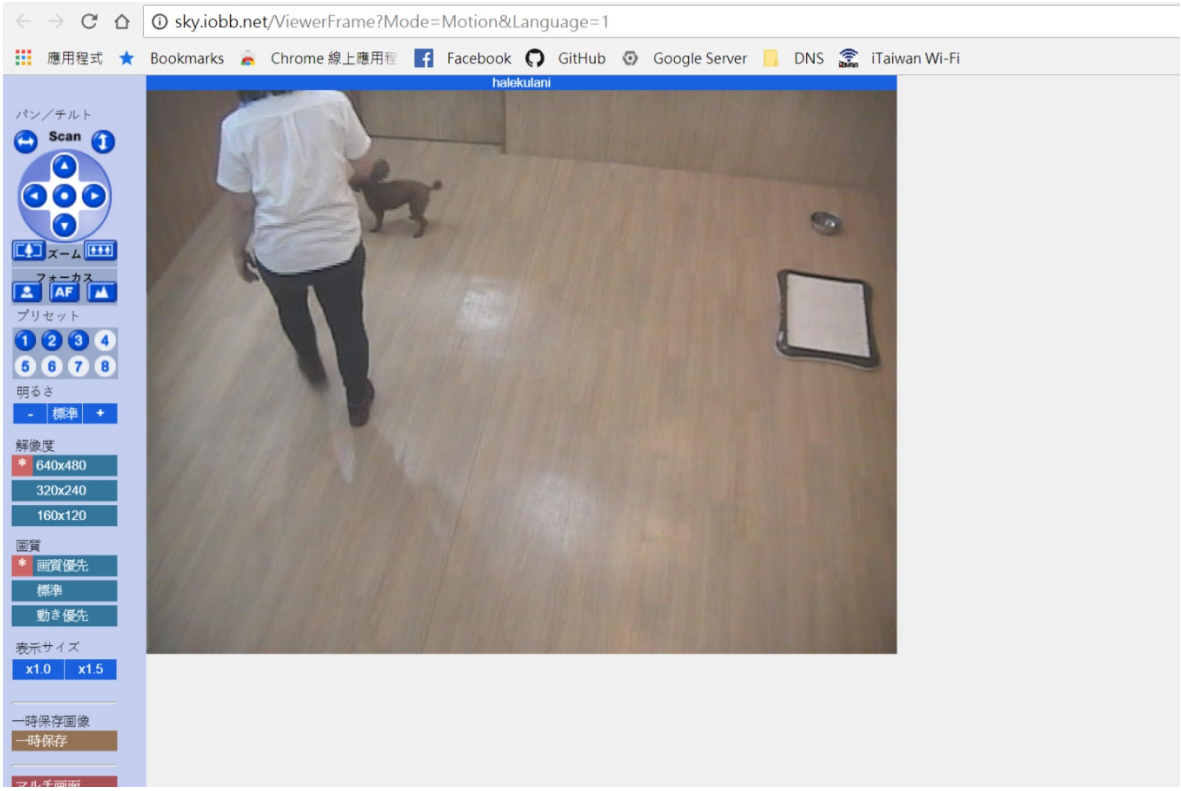
---

demo

-

```
inurl:"ViewerFrame?Mode="
```

- http://sky.iobb.net/ViewerFrame?Mode=Motion&Language=1



- web shell

```
ext:php intitle:sh3ll
```

-

(https://klionsec.github.io/2014/12/14/search-hacking/)

(X (https://www.insecam.org/en/bycountry/TW/)

---

shodan()

- https://www.shodan.io/explore
-
- minecraft server (https://www.shodan.io/search?query=net%3A140.134.0.0%2F16+port%3A25565)

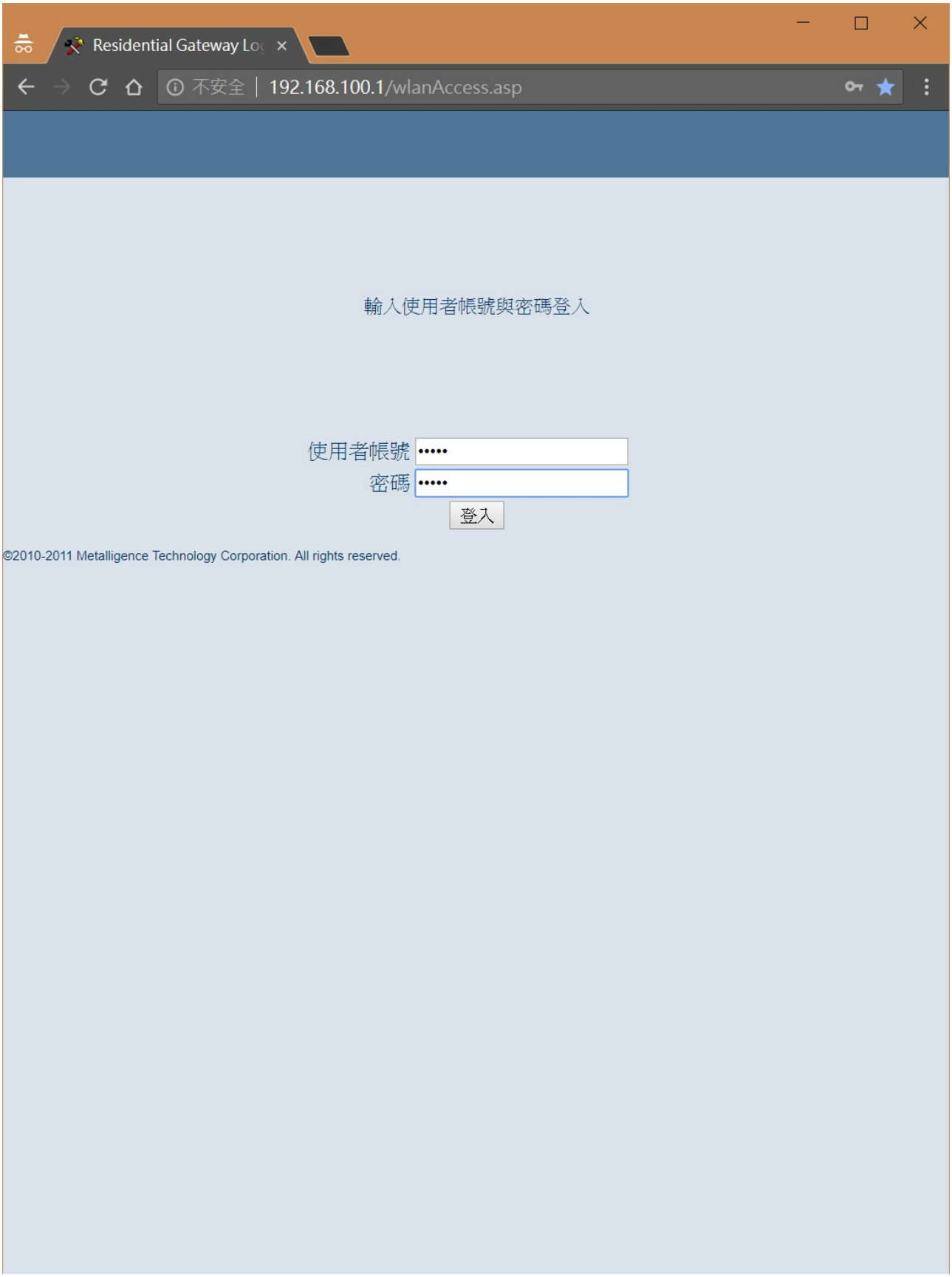
zoomeye()

- https://www.zoomeye.org/
-

Wifi

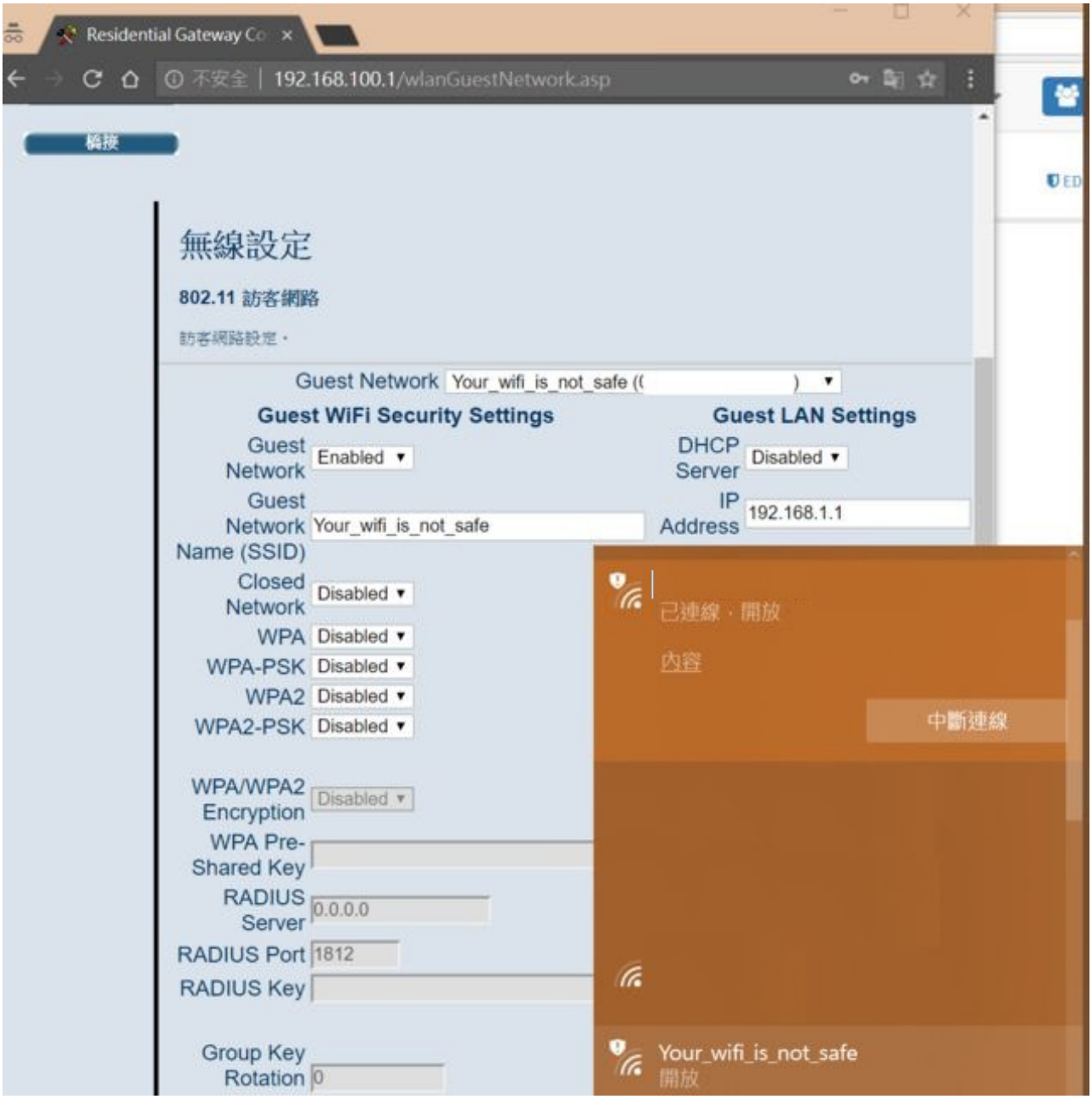

HTC Portable Hotspot CB92
已連線，安全
N_CFF77C
開放
其他人可能可以看到您透過此網路傳送的資訊
自動連線
連線


Residential Gateway Co
Speedtest by Ookla - Th
www.speedtest.net
Apps
Insights
Networl
刊登廣告還可獲得
抵免額高達1500元。
馬上刊登
Google
PING ms
16
DOWNLOAD Mbps
UPLOAD Mbps
0
1
5
10
20
30
50
75
100
40.69
Mbps
kbro
123.194.165.179
SEEDNET
We encourage you to read our updated Privacy Policy and Cookie Policy.


Residential Gateway Lo
不安全 | 192.168.100.1/wlanAccess.asp
輸入使用者帳號與密碼登入
使用者帳號
密碼
登入
©2010-2011 Metalligence Technology Corporation. All rights reserved.


Residential Gateway Co
不安全 | 192.168.100.1/RgSwInfo.asp
狀態
無線設定
基本設定
VPN設定
進階設定
登出
防火牆設定
家長管控
軟體
連接
安全性
橋接
診斷
事件紀錄
狀態
系統資訊
顯示目前系統資訊。
資訊
標準規範
硬體版本
軟體版本
Cable Modem MAC Address
Cable Modem序號
CM認證
Installed
狀態
已開機時間
0 days 05h:46m:17s
網路存取
Allowed
Cable Modem IP Address
©2010-2011 Metalligence Technology Corporation. All rights reserved.


Residential Gateway Co
不安全 | 192.168.100.1/wlanGuestNetwork.asp
無線設定
802.11 訪客網路
訪客網路設定：
Guest Network
_GUEST_0 (
Guest WiFi Security Settings
Guest Network
Disabled
Guest Network Name (SSID)
Your_wifi_is_not_safe
Closed Network
Disabled
WPA
Disabled
WPA-PSK
Disabled
WPA2
Disabled
WPA2-PSK
Disabled
WPA/WPA2 Encryption
Disabled
WPA Pre-Shared Key
RADIUS Server
0.0.0.0
RADIUS Port
1812
RADIUS Key
Group Key Rotation Interval
0
WPA/WPA2 Re-auth Interval
3600
WEP Encryption
Disabled
Shared Key Authentication
Optional
802.1x
Disabled
Guest LAN Settings
DHCP Server
Disabled
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Lease Pool Start
192.168.1.10
Lease Pool End
192.168.1.99
Lease Time
86400
確認
恢復訪客網路預設值



(Virtual Machine)

-
-

(Virtual Machine)

-
  -
  -
    -
    -
  -

-
-
  -

作業系統 / 比較項目	MS Windows	Linux	Mac OS	Unix
開發廠商	微軟公司	以unix為基礎發展出來	蘋果公司	由AT&T的貝爾實驗室開發
使用者介面	提供命令列介面以及圖形使用者介面	提供命令列介面以及圖形使用者介面	圖形使用者介面	提供命令列介面以及圖形使用者介面
系統原始碼	未開放	開放系統原始法讓使用者修改	未開放	未開放
硬體搭配	一般PC皆可使用	一般PC皆可使用	只能安裝在蘋果電腦上	一般PC皆可使用

- Ubuntu
  ,(https://hackmd.io/p/SkuIxUro-#/)

CTF (https://www.slideshare.net/HITCONGIRLS/hitcon-girls-ctf)

VM (http://www.digitimes.com.tw/tech/dt/n/shwnws.asp?cnlid=10&id=0000124512_q6m6fcij0cv9ds30t4krd)