# Introduction to Computer Security
# Homework 1

0316213 Yu-wen Pwu

1. Select a web site. Use "Wget" or "Teleport Pro" to mirror the site. Look for comments within comment tags. Give screen dumps and explain what you found. Use "DirBuster" with a proxy feature through "privoxy" to enumerate hidden files and directories. Screen dump and explain the hidden files and directories you found.

```
~ wget http://speed.cis.nctu.edu.tw/
--2016-03-19 18:56:55--  http://speed.cis.nctu.edu.tw/
正在查找主機 speed.cis.nctu.edu.tw (speed.cis.nctu.edu.tw)... 140.113.207.2
正在連接 speed.cis.nctu.edu.tw (speed.cis.nctu.edu.tw)|140.113.207.2|:80... 連上了。
已送出 HTTP 要求，正在等候回應... 200 OK
長度: 22569 (22K) [text/html]
Saving to: ‘index.html’

index.html                                          100%[=========================

2016-03-19 18:56:55 (4.53 MB/s) - ‘index.html’ saved [22569/22569]
```

```
308                         <div style="color:#ff0000; font-weight:bold;">  Guidelines</div>
309                         <ol>
310                         <li><a href="labpolicy.htm">Lab Policies</a><font color=ff6600 face=arial si
311                         <li><a href="/avoid/avoid.htm">21 Patterns to Avoid</a>
312                         <li><a href="/review.html">Guidelines for Paper Review</a>
313                         <li><a href="/schedule.htm">Thesis Guidelines</a>
314                         <!--<li><a href="/thesispro.html">Protocol for Finishing Up Your Thesis</a>-
315                         <!--<li><a href="plan_for_master.ppt">Tips on Planning Master Study(ppt)</a>
316                         <li><a href="http://www.cs.columbia.edu/~hgs/etc/writing-style.html">Hints o
317                         <li><a href="/outline.html">Guidelines for Paper Outline</a>
318                         <li><a href="/writing.htm">Guidelines for Paper Writing</a>
319                         <li><a href="knoy_note.htm">English Technical Writing</a>-->
320                         <li><a href="./html/Programming_Certification.html">Programming Certificatio
321                         <!--    <li><a href="SOP.htm">Lab SOPs</a>-->
322                         </ol>
```

```
420                         <tr>
421                                 <!--<td><a href="http://speed.cis.nctu.edu.tw/~cnlu">Chun-Nan Lu</a></td><td>(呂俊男
422                                 <!--<td><a href="./resume/chia-yu/Chia-Yu.htm">Jia-Yu Gu</a></td><td>(古佳育)</td>--
423                                 <!--td><a href="http://speed.cs.nctu.edu.tw/resume/iwei/iwei.html">I-Wei Chen</a></
424                                 <!--td><a href="http://sites.google.com/site/stanleychangnctu/home/resume_lab">Shun-
425                                 <!--td><a href=#>Hung-Cheng Chang</a></td><td>(張宏鉦)</td-->
426                                 <td><a href="">Chien-Ting Wang</a></td><td>(汪建廷)</td>
427                                 <td><a href="">Minh-Tuan Thai</a></td><td>(蔡明俊)</td>
428                     <!--td><a href="">Robert Yang</a></td><td>(楊錫昌)</td-->
429                 <td><a href="">Yao-Chun Wang</a></td><td>(王耀駿)</td>
```

There are removed links and lists of graduated students.

```
~ service privoxy status
● privoxy.service - Privacy enhancing HTTP Proxy
   Loaded: loaded (/lib/systemd/system/privoxy.service; enabled; vendor prese
   Active: active (running) since 六 2016-03-19 19:38:19 CST; 11min ago
 Main PID: 10511 (privoxy)
   CGroup: /system.slice/privoxy.service
           └─10511 /usr/sbin/privoxy --pidfile /var/run/privoxy.pid --user pr

3月 19 19:38:18 yuwen41200 systemd[1]: Starting Privacy enhancing HTTP Proxy
3月 19 19:38:19 yuwen41200 systemd[1]: Started Privacy enhancing HTTP Proxy.
```

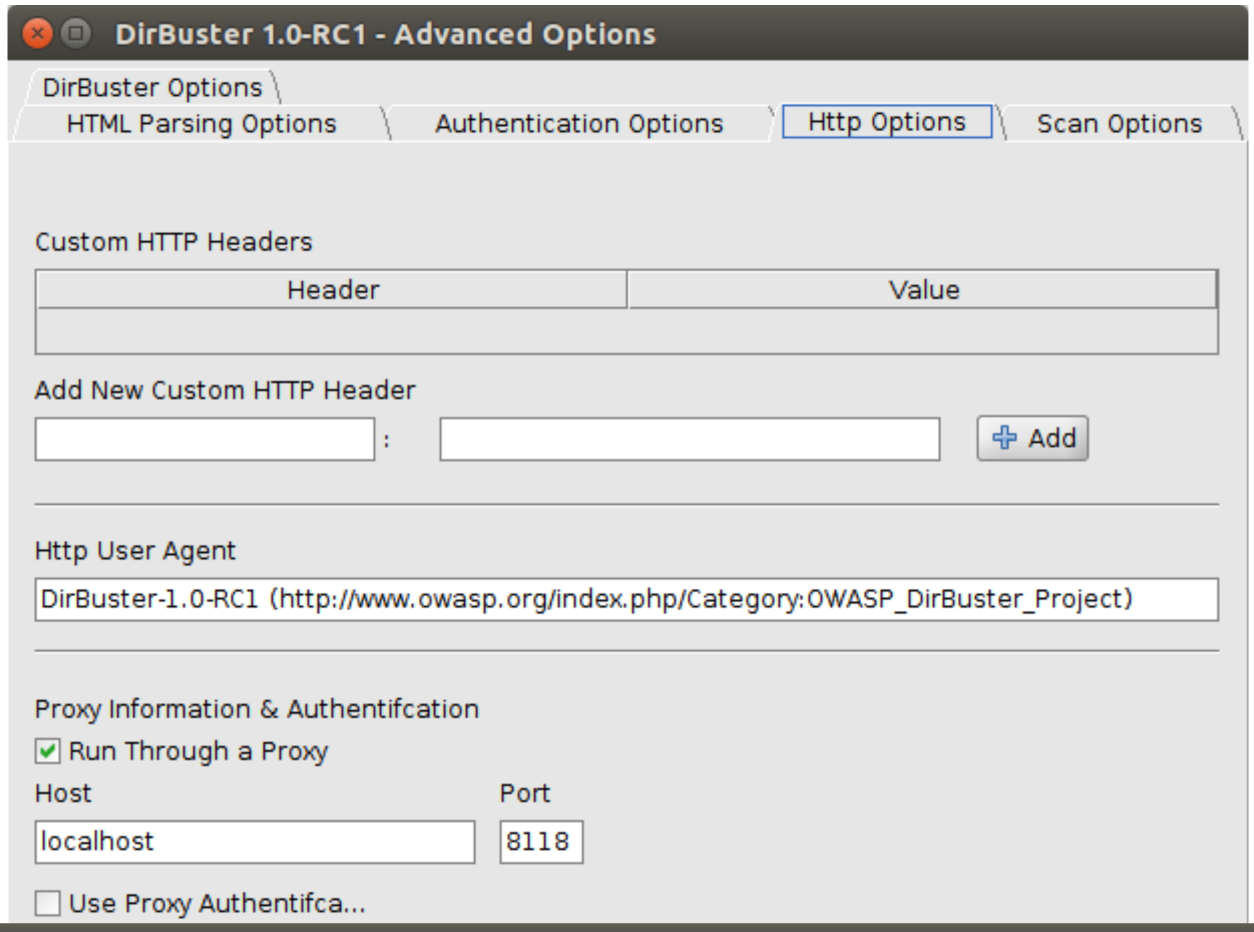


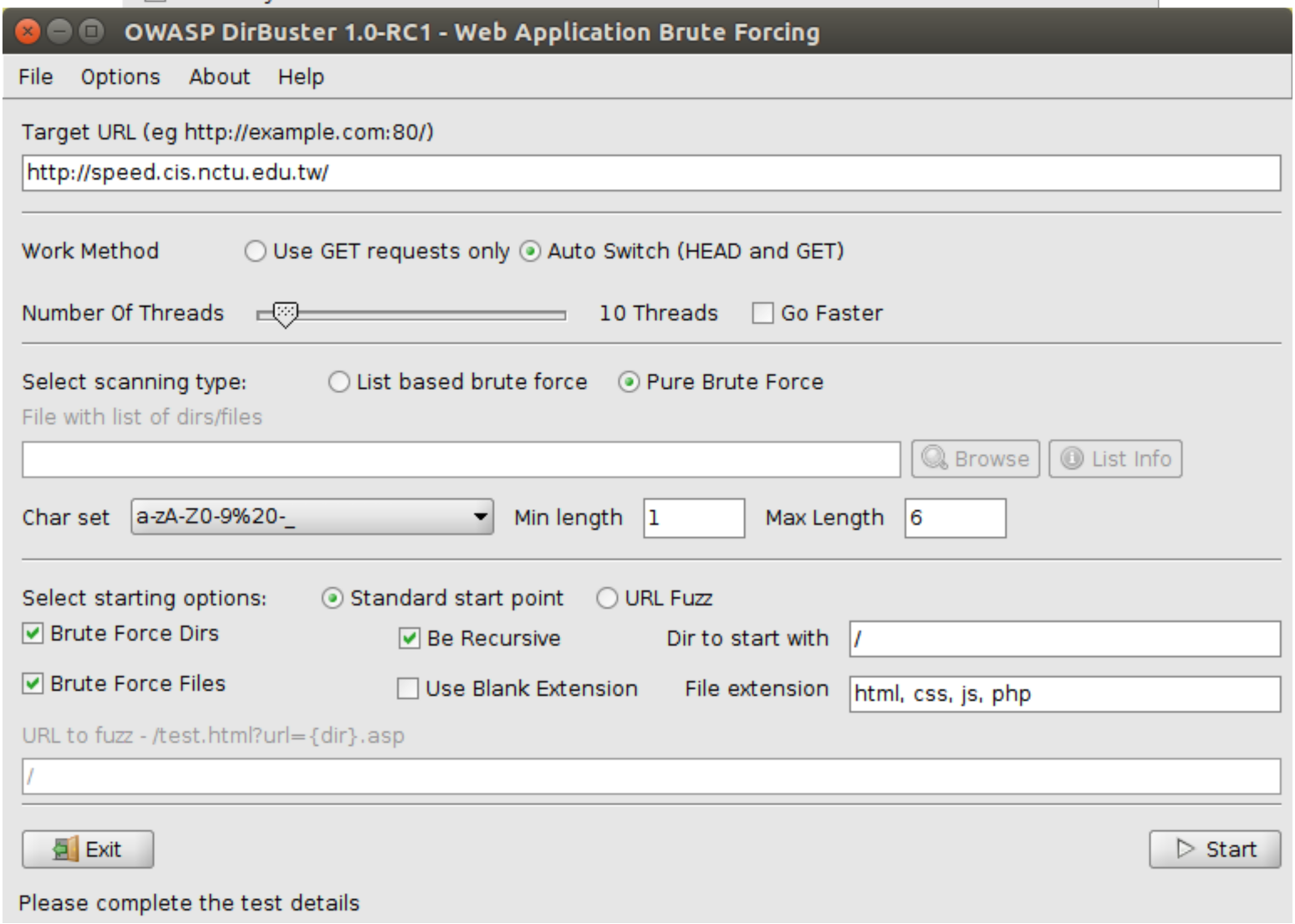


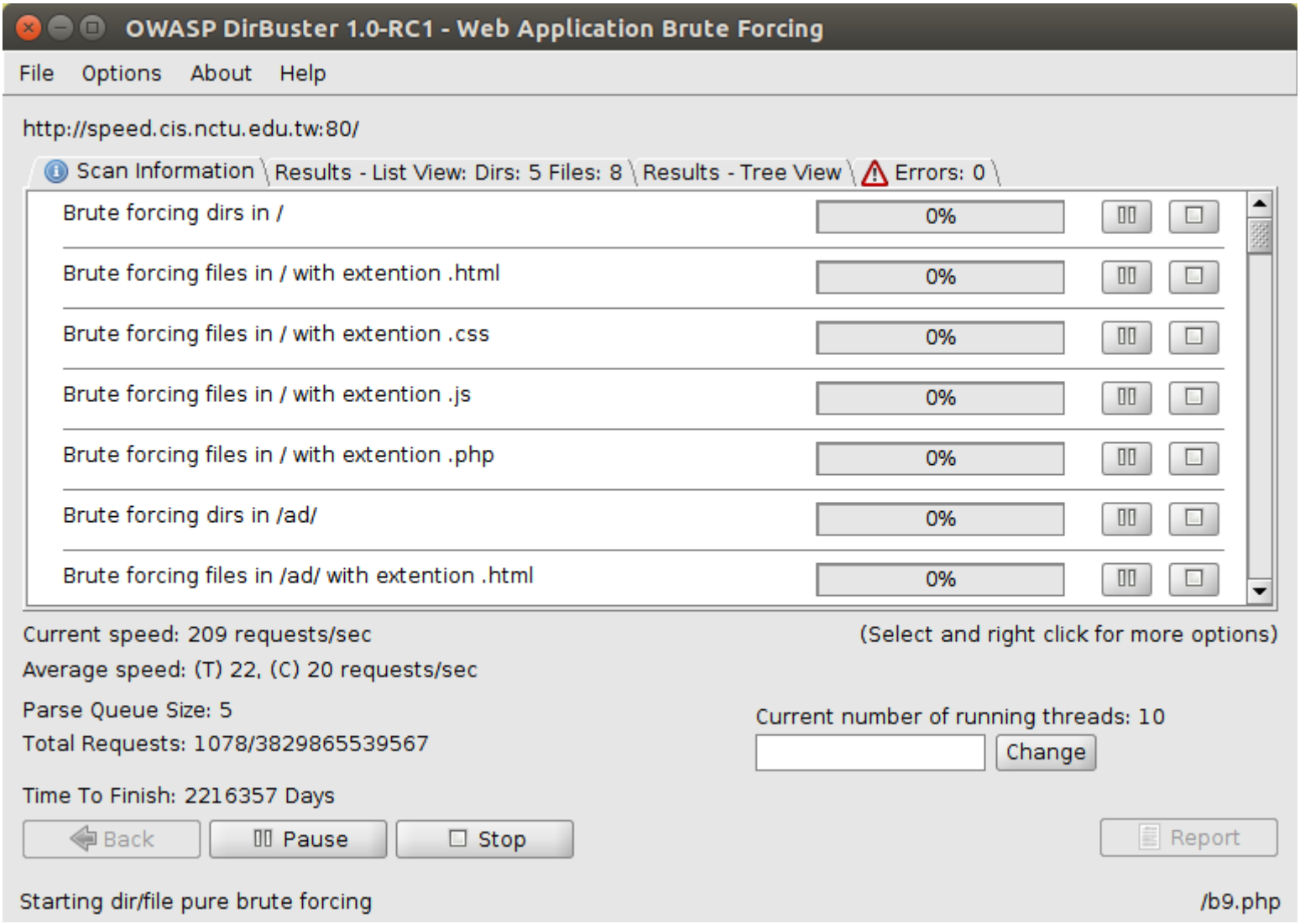
**This is Privoxy 3.0.23 on localhost (127.0.0.1), port 8118, enabled**

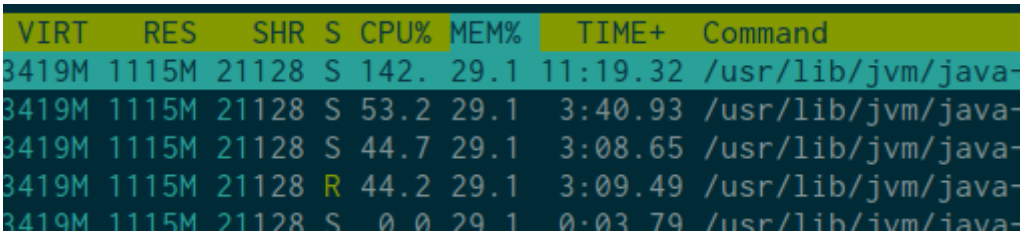
**Privoxy Menu:**

- View & change the current configuration
- View the source code version numbers
- View the request headers
- Look up which actions apply to a URL and why
- Documentation

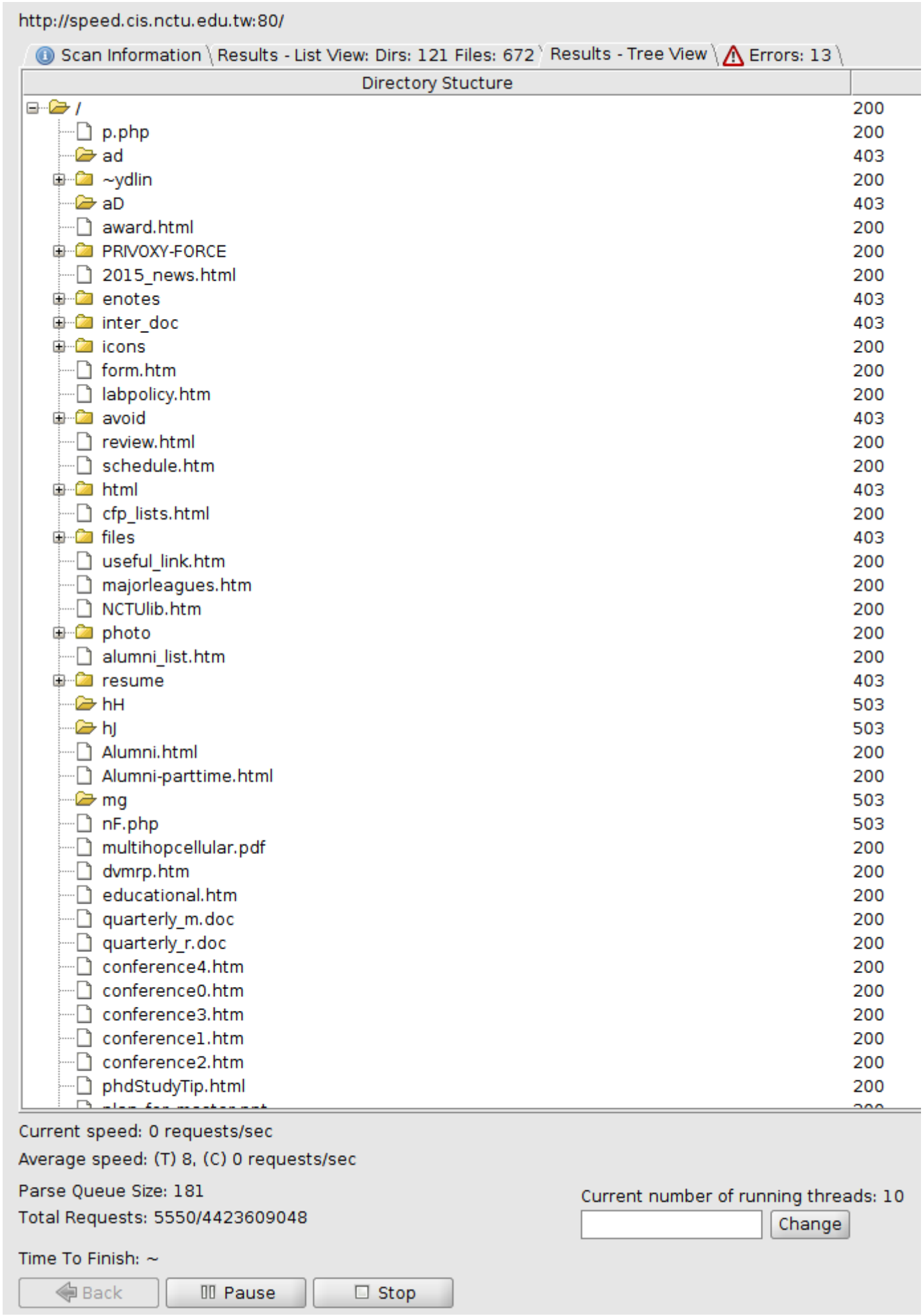

DirBuster 1.0-RC1 - Advanced Options
DirBuster Options
HTML Parsing Options
Authentication Options
Http Options
Scan Options
Custom HTTP Headers
Header
Value
Add New Custom HTTP Header
:
Add
Http User Agent
DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)
Proxy Information & Authentifcation
Run Through a Proxy
Host
Port
localhost
8118
Use Proxy Authentifca...


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Target URL (eg http://example.com:80/)
http://speed.cis.nctu.edu.tw/
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
10 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
6
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
html, css, js, php
URL to fuzz - /test.html?url={dir}.asp
/
Exit
Start
Please complete the test details



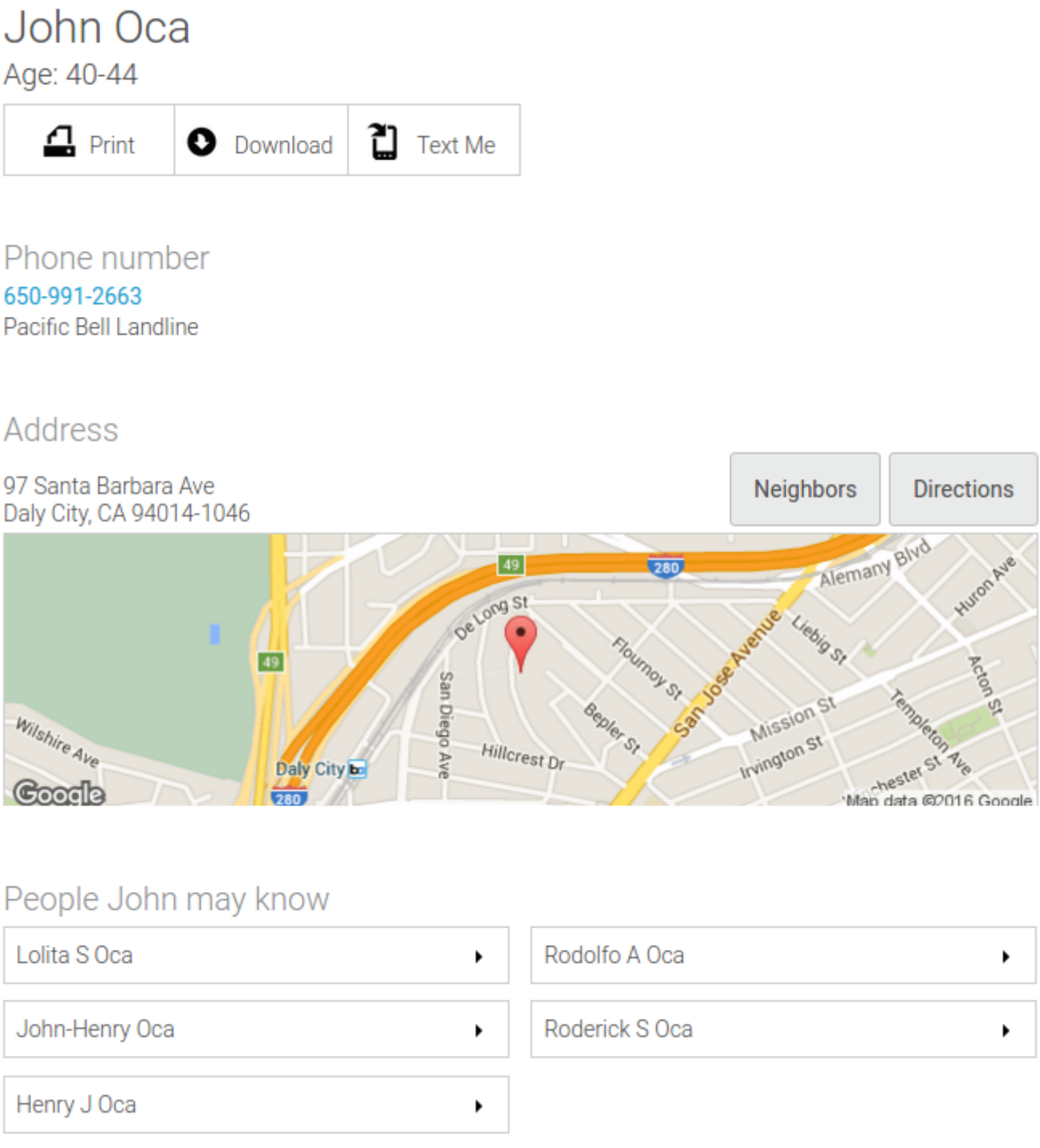

DirBuster used up all the resources on my computer every time. Then it crashed. After trying to reduce the range for scanning, this is what I finally found. I can see a list of some available files and directories, just like logged into the FTP server of the site.


http://speed.cis.nctu.edu.tw:80/
Scan Information
Results - List View: Dirs: 121 Files: 672
Results - Tree View
Errors: 13
Directory Stucture
/ 200
p.php 200
ad 403
~ydlin 200
aD 403
award.html 200
PRIVOXY-FORCE 200
2015_news.html 200
enotes 403
inter_doc 403
icons 200
form.htm 200
labpolicy.htm 200
avoid 403
review.html 200
schedule.htm 200
html 403
cfp_lists.html 200
files 403
useful_link.htm 200
majorleagues.htm 200
NCTUlib.htm 200
photo 200
alumni_list.htm 200
resume 403
hH 503
hJ 503
Alumni.html 200
Alumni-parttime.html 200
mg 503
nF.php 503
multihopcellular.pdf 200
dvmrp.htm 200
educational.htm 200
quarterly_m.doc 200
quarterly_r.doc 200
conference4.htm 200
conference0.htm 200
conference3.htm 200
conference1.htm 200
conference2.htm 200
phdStudyTip.html 200
Current speed: 0 requests/sec
Average speed: (T) 8, (C) 0 requests/sec
Parse Queue Size: 181
Total Requests: 5550/4423609048
Current number of running threads: 10
Change
Time To Finish: ~
Back
Pause
Stop

2. Lookup "How I met your girlfriend" in the BlackHat 2010 demo to explain, in 0.5 page, how this was done.

- The entropy for PHP sessions (before 5.3.2) is 160 bits. However, we can easily know one's IP address, epoch, and even lcg_value(), so the total entropy can be reduced to 20 bits (from microsecond).
- By using cross-protocol scripting (XPS), we can run a protocol (e.g. IRC) within another protocol (e.g. HTTP). This can be done by using JavaScript to submit hidden forms. We may even use NAT pinning to cheat routers, helping us attack the client.
- If the port is blocked by the browser, we can intentionally overflow the port number (add 65536 for TCP/UDP ports). This will work for those browsers which only check if these two integers are equal.
- After successfully luring the victim to visit our website, we can guess his or her router type and get the MAC address of the router. This can also be done by using JavaScript and AJAX to try some addresses like 192.168.1.1.
- Use the location services from Google to get the geolocation data of the MAC address, then use Google Maps to know its real address. This is called XXXSS by Samy Kamkar.

3. Select a person. Use on-line sites for phone book, social network, information, job, photo management, business directory, jigsaw.com, etc. to summarize, with screen dumps and explanations, what information you can get. If your target is not in US nor native English speaker, you might need to use on-line sites different from the textbook.




We can get people's age, phone number, and real address from 411.com. We can get even more information, like photos, locations, families, and social backgrounds, from spokeo.com. In fact, there are a lot of such sites that collect and distribute personal information without your permission.

John H Oca

Phone and Email (1)

Location History (1)

Photos & Social Profiles

Family Members (10)

Court Records

Historical Records

Personal Details (2) ›

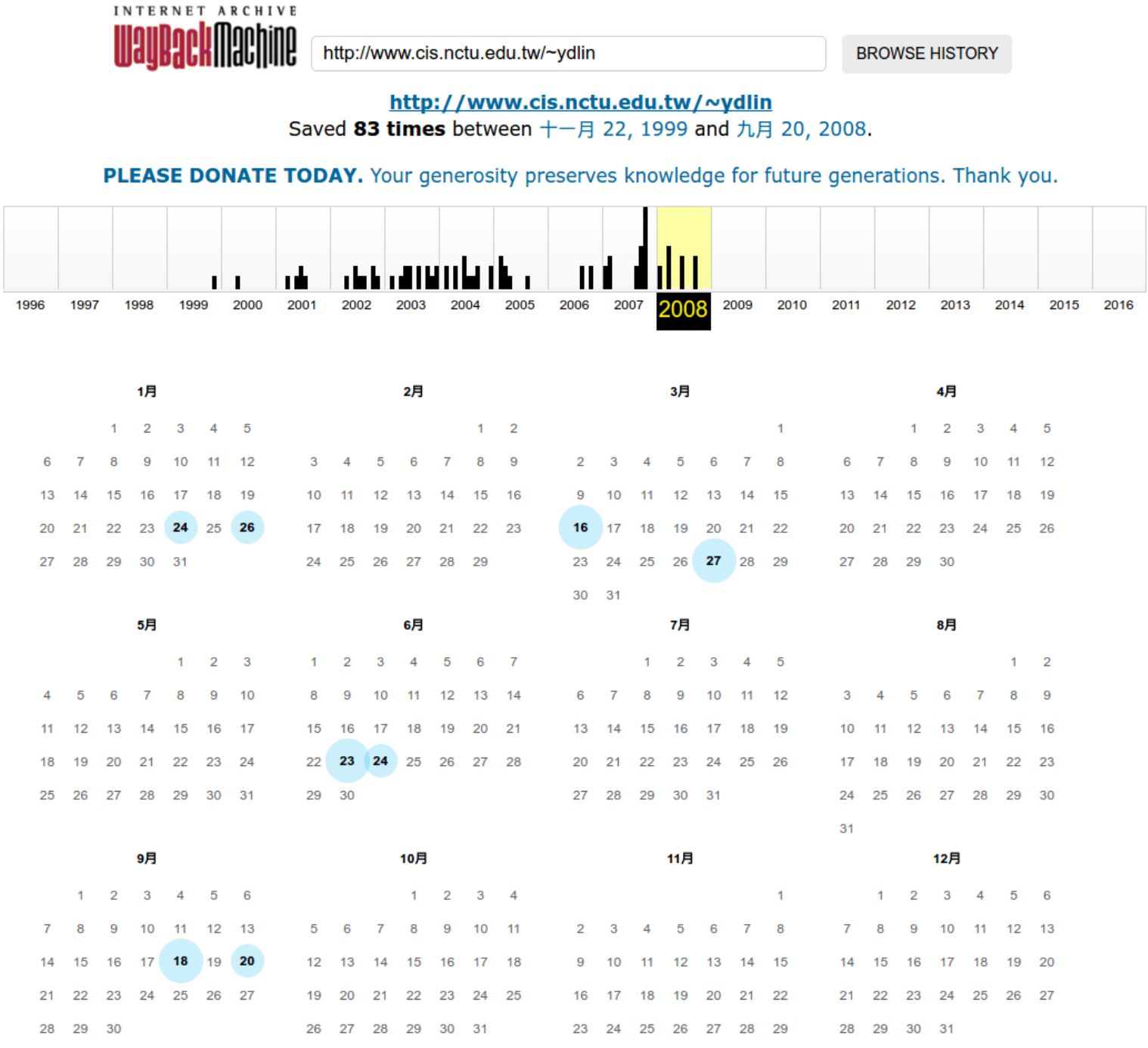
4. Google "XYZ resume firewall" and "XYZ resume intrusion detection" where "XYZ" is the name of your target company. Screen dump "useful" results and explain what you got.

I googled "Sony resume firewall," and found the person "Subramanyam I" once in charge of the firewall in Applied Materials Inc., India and Information Systems & Solutions Asia Pacific.

| | |
|---|---|
| **Responsibility** | To setup India GDC for applied materials. establish data and voice communication links and partner connectivity. |
| **Client:** | **Applied Materials Inc., India** |
| **Duration** | 6 Months |
| **Description:** | The work involved configuring Cisco layer 3 switches, Cisco routers, establishing ISDN connections. Administration of Checkpoint NG firewall. This includes co-ordination between vendors and clients of Wipro. |
| **Position:** | Project Manager |
| **Contribution:** | • Configuring cisco swithes for LAN connectivity and making VLANs.<br>• Configuring Cisco routers for Leased circuit connectivity.<br>• Creating policies, installing and administration of Checkpoint NG firewall.<br>• Configuring Cisco routers for ISDN connectivity.<br>• Co-ordinating with the main office of AMAT in Santaclara.<br>• Provide help to partners as and when required to configure the routers.<br>• Implementation and testing of each indiviual activity.<br>• Management and co-ordination with vendors such as telecom service providers and equipment vendors.<br>• Documentation according to customer's requirements. |
| **Team size:** | 4 |
| **Environment:** | Cisco IOS 11.x ,12.x, TCP /IP ,Checkpoint NG firewall. |

| | |
|---|---|
| **Responsibility** | To manage the Wide Area network operations. Activities include administration and planning of Wide area networks, Safeword remote access servers, DNS and Sendmail systems for Sony, Singapore as regional hub for Asia Pacific region. Cisco router administration. |
| **Client:** | **Information Systems & Solutions Asia Pacific (a division of Sony Electronics, Singapore.)** |
| **Duration:** | 3 Years |
| **Description:** | The work involved in administration of Cisco 7500 series routers setting up and configuring DNS, sendmail and administration of Sun solaris unix systems, Netscape Proxy, Guantlet firewall, Safeword remote access software administration and cacheflow system administration. |
| **Position:** | Consultant. |
| **Contribution:** | • Understanding the WAN setup of Sony which is connected across Asia pacific region.<br>• Administration of Cisco routers and reviewing configurations on critical implementations and changes. |

5. Lookup archive.org and Google cached results, and select a target web site. Compare the differences between an archived and cached copy with its current on-line web site. Give screen dump and explain the differences.




Google cache has the latest version, but Wayback Machine (archive.org/web) has 83 old versions of this site. The following is the version in 2001/05/18.

Dr. Ying-Dar Lin (林盈達)

*Internal Links:*



*External Links:*

- Highspeed Network Lab
- Offered Courses
- Other Publications (in Chinese)


Contact Information
Postal Address: Prof. Ying-Dar Lin
Dept. of Comp. & Info. Sci.
National Chiao-Tung University.
Hsinchu, Taiwan.
Tel: +886-3-5731899
Fax: +886-3-5721490
Email: ydlin@cis.nctu.edu.tw


## Background

Ying-Dar Lin was born in Hsi-Lo, Taiwan in 1965. He received the Bachelor's degree in Computer Science and Information Engineering from National Taiwan University in 1988, and the and 1993, respectively.

At UCLA Computer Science Department, he worked as a Research Assistant from 1989 to 1993 and worked as a Teaching Assistant from 1991 to 1992. In the summers of 1987 and 1991 He joined the faculty of the Department of Computer and Information Science at National Chiao Tung University in August 1993 and is Professor since 1999.

His research interests include design, analysis, and implementation of network protocols and algorithms, wire-speed switching and routing, quality of services, and intranet servers. He has Computer Network Experiments. Dr. Lin is a member of ACM and IEEE. He can be reached at ydlin@cis.nctu.edu.tw and http://www.cis.nctu.edu.tw/~ydlin.

## Research Activities

Devices over the Internet can be categorized into three types: access, core, and server. In the Highspeed Networks Lab at National Chiao Tung University, we conduct research in designin devices.

Specifically, we focus on broadband cable (DOCSIS and IEEE 802.14) and wireless (GPRS and IEEE 802.11) in access networks, QoS routers (DiffServ) in core networks, and intranet se interests are in the algorithmic design and implementation of slot allocation and scheduling in access networks, fast packet classification, scheduling, routing, forwarding, and bandwidth b plug-n-play, appliance-style, and scalability. We deliver papers, patents, reports, technical transfers, and prototypes. Our research projects are funded by government agencies including Na Zyxel, Mentor Data, Far Eastone, Axtronics, etc.

## Research Areas

- Network Protocols and Algorithms: Design, Analysis, Implementation
- Internet QoS Switch Routers
- Access Networks: Broadband Cable and Wireless
- Intranet Servers: Appliances and Services

## Research Projects

speed.cis.nctu.edu.tw/~ydlin/

應用程式 eCampus Moodle GitHub Wikipedia Facebook Messenger Dcard LinkedIn Moedict iCIBA BS2

Dr. Ying-Dar Lin (林盈達)

[News] Research Associate, ONF (Open Networking Foundation), since June 2014

[News] IEEE ComSoc Distinguished Lecturer for 2014 ~ 2017

[News] New Book – Collegiate Programming Exam: CPE Handbook

[News] IEEE Fellow (Class of 2013)

[News] New Book - Computer Networks: An Open Source Approach ***Ship It!***

[News] Well-Cited Classical Paper with Over 600 Citations and Standardized into IEEE 802.11s, IEEE 802.15.5, WiMAX IEEE 802.16j,

[News] 中文網頁

[News] 給碩博士班新生(Also for perspective international students)

**Internal Links:**

- Background
- Services
- Research
- Research Projects
- Patents

**External Links:**

- Highspeed Network Lab
- Network Benchmarking Lab (NBL)10th Anniversary
- Embedded Benchmarking Lab (EBL)
- ACM ICPC Taiwan Council
- Offered Courses
- Other Publications (in Chinese)

**Contact Information:**

Postal Address: Prof. Ying-Dar Lin
Dept. of Computer S
National Chiao Tung
Hsinchu, Taiwan.
Tel: +886-3-5731899
Fax: +886-3-5721490
Email: ydlin@cs.nctu.ec

## Background

**Concise Biography**

YING-DAR LIN is a Distinguished Professor of Computer Science at National Chiao Tung University (NCTU) in Taiwan. He received his Ph.D. in Computer Science from UCLA in 1993. He serv Cisco Systems in San Jose during 2007–2008. Since 2002, he has been the founder and director of Network Benchmarking Lab (NBL, www.nbl.org.tw), which reviews network products with rea (ONF). He also cofounded L7 Networks Inc. in 2002, which was later acquired by D-Link Corp. His research interests include design, analysis, implementation, and benchmarking of network protoc communications, embedded hardware/software co-design, and recently software defined networking. His work on "multi-hop cellular" was the first along this line, and has been cited over 600 time LTE-Advanced. He is an IEEE Fellow (class of 2013), an IEEE Distinguished Lecturer (2014&2015), and a research associate of ONF. He is currently on the Editorial Boards of *IEEE Transact Network Testing Series, IEEE Wireless Communications, IEEE Communications Surveys and Tutorials, IEEE Communications Letters, Computer Communications, Computer Networks, Journal of N* He has guest edited several Special Issues in IEEE journals and magazines, and co-chaired symposia at IEEE Globecom'13 and IEEE ICC'15. He published a textbook, *Computer Networks: A* (McGraw-Hill, 2011). It is the first text that interleaves open source implementation examples with protocol design descriptions to bridge the gap between design and implementation.

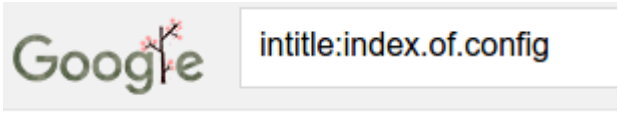
**Full Biography**

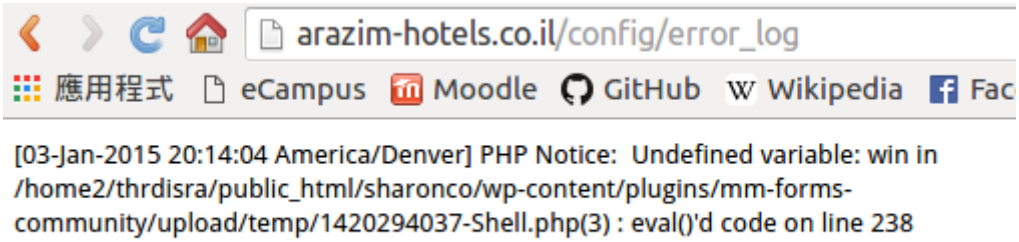
Ying-Dar Lin was born in Hsi-Lo, Taiwan, in 1965. He received the Bachelor's degree in Computer Science and Information Engineering from National Taiwan University in 1988, and the M.S. (UCLA) in 1990 and 1993, respectively. At UCLA Computer Science Department, he worked as a Research Assistant from 1989 to 1993 and a Teaching Assistant from 1991 to 1992. In the

This is the current version. As you can see, there are lots of differences. This exercise tells us that, if we accidentally upload sensitive data to the Internet, even if we remove them later, these data may still remain on the Internet.

6. Find Google Hacking Database at hackersforcharity.org/ghdb/. Summarize what it has and select 3 strings to search. Screen dump and explain what you got.

We can simply use Google to retrieve sensitive data because someone upload it or because of the bug in that web application. GHDB collects all these searching keywords.

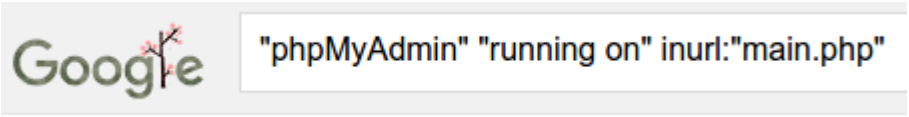



Error log; some WordPress plugins have trouble executing an eval() function.


Noooooooo!!! I'm banned by Google!!! Google think I am a hacker...


User “intro” failed to log in the MySQL server webhosting.cs.nctu.edu.tw.




cardinstudio.com/phpMyAdmin-2.2.7-pl1/

應用程式 eCampus Moodle GitHub Wikipedia Facebook Messenger Dcard

**Home**

cardinstudio (1)

asd

# Database *cardinstudio* - table *asd* running on *localhost*

[ **Browse** ] [ **Select** ] [ **Insert** ] [ **Empty** ] [ **Drop** ]

| | Field | Type | Attributes | Null | Default | Extra | Action | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | asdad | varchar(24) | | No | | | Change | Drop | Primary | Index | Unique | Fulltext |

*With selected:* Change

Indexes : [Documentation]

| Keyname | Type | Cardinality | Action | | Field |
|---|---|---|---|---|---|
| asdad | INDEX | None | Drop | Edit | asdad |
| asdad_2 | FULLTEXT | None | Drop | Edit | asdad |
| asdad_3 | FULLTEXT | None | Drop | Edit | asdad |
| asdad_4 | INDEX | None | Drop | Edit | asdad |
| asdad_5 | FULLTEXT | None | Drop | Edit | asdad |
| asdad_6 | FULLTEXT | None | Drop | Edit | asdad |
| asdad_7 | FULLTEXT | None | Drop | Edit | asdad |
| asdad_8 | INDEX | None | Drop | Edit | asdad |
| asdad_9 | INDEX | None | Drop | Edit | asdad |
| asdad_10 | INDEX | None | Drop | Edit | asdad |
| asdad_11 | FULLTEXT | None | Drop | Edit | asdad |

Space usage :

| Type | Usage | |
|---|---|---|
| Data | 0 | Bytes |
| Index | 2,048 | Bytes |
| Total | 2,048 | Bytes |

Row Statistic :

| Statements | Value |
|---|---|
| Format | dynamic |
| Rows | 0 |

Create an index on 1 columns Go

- Print view
- Run SQL query/queries on database cardinstudio [Documentation] :

```
SELECT * FROM `asd` WHERE 1
```

☑ Show this query here again

*Or* Location of the textfile :

選擇檔案 未選擇任何檔案

Go

- Add new field : 1 At End of Table Go
- Alter table order by : asdad Go (singly)
- Insert data from a textfile into table
- View dump (schema) of table

◉ Structure only
○ Structure and data
○ Data only

☐ Add 'drop table'
☐ Complete inserts

Wooooooow!!! I find your phpMyAdmin!!!
And you have already logged in for me!!! It's so kind of you <3

7. Select a web site. Start from whois.iana.org to find its registry, registrar, and registrant. Also select an IP address. Start from arin.net to find who owns the IP address. Show your screen dump and explain.

fgisc.org Submit

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.pir.org

domain:       ORG

organisation: Public Interest Registry (PIR)
address:      1775 Wiehle Avenue
address:      Suite 102A
address:      Reston Virginia 20190
address:      United States

contact:      administrative
name:         Michelle Coon
organisation: Public Interest Registry (PIR)
address:      1775 Wiehle Avenue
address:      Suite 200
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 889 5762
fax-no:       +1 703 889 5779
e-mail:       mcoon@pir.org

contact:      technical
name:         Senior Director, DNS Infrastructure Group
organisation: Afilias
address:      Building 3, Suite 105
address:      300 Welsh Road
address:      Horsham, Pennsylvania 19044
address:      United States
phone:        +1 215.706.5700
fax-no:       +1 215.706.5701
e-mail:       tld-tech-poc@afilias.info

nserver:      A0.ORG.AFILIAS-NST.INFO 199.19.56.1 2001:500:e:0:0:0:0:1
nserver:      A2.ORG.AFILIAS-NST.INFO 199.249.112.1 2001:500:40:0:0:0:0:1
nserver:      B0.ORG.AFILIAS-NST.ORG 199.19.54.1 2001:500:c:0:0:0:0:1
nserver:      B2.ORG.AFILIAS-NST.ORG 199.249.120.1 2001:500:48:0:0:0:0:1
nserver:      C0.ORG.AFILIAS-NST.INFO 199.19.53.1 2001:500:b:0:0:0:0:1
nserver:      D0.ORG.AFILIAS-NST.ORG 199.19.57.1 2001:500:f:0:0:0:0:1
ds-rdata:     9795 7 2 3922b31b6f3a4ea92b19eb7b52120f031fd8e05ff0b03bafcf9f891bfe7ff8e5
ds-rdata:     9795 7 1 364dfab3daf254cab477b5675b10766ddaa24982

whois:        whois.pir.org

status:       ACTIVE
remarks:      Registration information: http://www.pir.org

created:      1985-01-01
changed:      2015-09-30
source:       IANA
```

Domain ID: D155627217-LROR
WHOIS Server:
Referral URL: http://www.enom.com
Updated Date: 2016-03-01T07:21:17Z
Creation Date: 2009-03-16T14:25:00Z
Registry Expiry Date: 2019-03-16T14:25:00Z
Sponsoring Registrar: eNom, Inc.
Sponsoring Registrar IANA ID: 48
Domain Status: ok https://www.icann.org/epp#ok
Registrant ID: d17668574243b666
Registrant Name: Nan Chen  Chen
Registrant Organization:
Registrant Street: 3F., No.27, Lane 13, Yongkang St.,
Registrant City: Da-an District
Registrant State/Province: TAIPEI CITY
Registrant Postal Code: 10650
Registrant Country: TW
Registrant Phone: +886.922430667
Registrant Phone Ext:
Registrant Fax: +886.922430667
Registrant Fax Ext:
Registrant Email: aikosenoo@gmail.com
Admin ID: d17668574243b666
Admin Name: Nan Chen  Chen
Admin Organization:
Admin Street: 3F., No.27, Lane 13, Yongkang St.,
Admin City: Da-an District
Admin State/Province: TAIPEI CITY
Admin Postal Code: 10650
Admin Country: TW
Admin Phone: +886.922430667
Admin Phone Ext:
Admin Fax: +886.922430667
Admin Fax Ext:
Admin Email: aikosenoo@gmail.com
Tech ID: d17668574243b666
Tech Name: Nan Chen  Chen
Tech Organization:
Tech Street: 3F., No.27, Lane 13, Yongkang St.,
Tech City: Da-an District
Tech State/Province: TAIPEI CITY
Tech Postal Code: 10650
Tech Country: TW
Tech Phone: +886.922430667
Tech Phone Ext:
Tech Fax: +886.922430667
Tech Fax Ext:
Tech Email: aikosenoo@gmail.com
Name Server: DNS1.NAME-SERVICES.COM
Name Server: DNS2.NAME-SERVICES.COM
Name Server: DNS3.NAME-SERVICES.COM
Name Server: DNS4.NAME-SERVICES.COM
Name Server: DNS5.NAME-SERVICES.COM
DNSSEC: unsigned
>>> Last update of WHOIS database: 2016-03-20T07:50:51Z <<<

"For more information on Whois status codes, please visit
https://icann.org/epp"

Access to Public Interest Registry WHOIS information is provided to assist persons in determining the contents of a
domain name registration record in the Public Interest Registry registry database. The data in this record is provided by Public Interest Registry for informational purposes only, and Public Interest Registry does not guarantee its accuracy. This service is intended only for query-based access. You agree that you will use this data
only for lawful purposes and that, under no circumstances
will you use this data to(a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile
of mass unsolicited, commercial advertising or solicitations
to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic
processes that send queries or data to the systems of Registry Operator, a Registrar, or Afilias except as reasonably necessary to register domain names or modify
existing registrations. All rights reserved. Public Interest Registry reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this
policy.

Registry: Public Interest Registry (PIR)
Registrar: eNom, Inc.
Registrant: Nan-chen Chen

In fact, fgisc.org is bought by Nan-chen Chen, former president of Taipei First Girls' High School Information Study Club (FGISC).

You searched for: **210.71.78.27**

| Network | |
|---|---|
| Net Range | 210.0.0.0 - 210.255.255.255 |
| CIDR | 210.0.0.0/8 |
| Name | APNIC-CIDR-BLK2 |
| Handle | NET-210-0-0-0-1 |
| Parent | |
| Net Type | Allocated to APNIC |
| Origin AS | |
| Organization | Asia Pacific Network Information Centre (APNIC) |
| Registration Date | 1996-07-01 |
| Last Updated | 2010-08-02 |
| Comments | This IP address range is not registered in the ARIN database.<br>For details, refer to the APNIC Whois Database via<br>WHOIS.APNIC.NET or https://wq.apnic.net/apnic-bin/whois.pl<br>** IMPORTANT NOTE: APNIC is the Regional Internet Registry<br>for the Asia Pacific region. APNIC does not operate networks<br>using this IP address range and is not able to investigate<br>spam or abuse reports relating to these addresses. For more<br>help, refer to https://www.apnic.net/apnic-info/whois_search2/abuse-and-spamming |
| RESTful Link | https://whois.arin.net/rest/net/NET-210-0-0-0-1 |
| See Also | Related organization's POC records. |
| See Also | Resource links. |
| See Also | Related delegations. |

```
% APNIC found the following authoritative answer from: whois.apnic.net
```

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html
```

```
% Information related to '210.70.0.0 - 210.71.127.255'
```

```
inetnum:        210.70.0.0 - 210.71.127.255
netname:        TANET
descr:          Taiwan Academic Network
country:        TW
admin-c:        TA61-AP
tech-c:         TA61-AP
mnt-by:         MAINT-TW-TWNIC
changed:        snw@www.edu.tw 19980908
status:         ALLOCATED PORTABLE
source:         APNIC
```

```
person:         TANET ADMIN
nic-hdl:        TA61-AP
e-mail:         tanetadm@moe.edu.tw
address:        12F, No 106, Sec. 2, Heping E. Rd., Taipei
address:        Taipei, 106, R.O.C
phone:          +886-2-2737-7044
fax-no:         +886-2-2737-7043
country:        TW
changed:        hostmaster@twnic.net.tw 20090212
mnt-by:         MAINT-TW-TWNIC
source:         APNIC
```

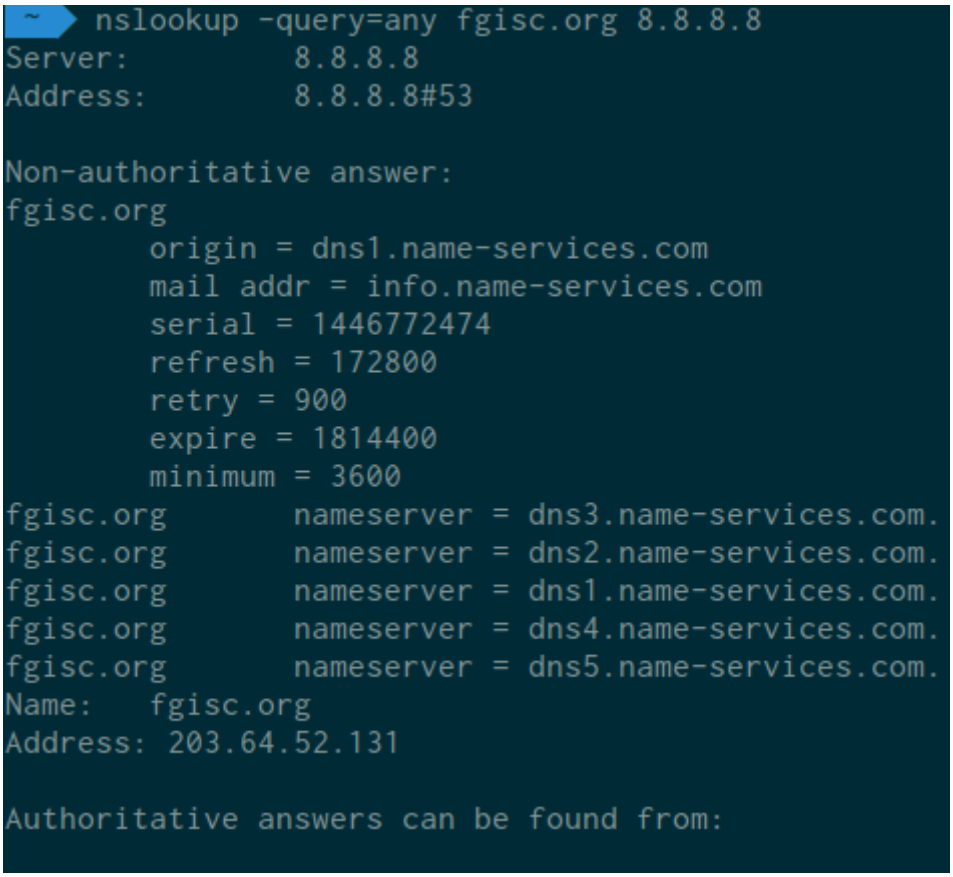
Report invalid contact

```
% This query was served by the APNIC Whois Service version 1.69.1-APNICv1r7-SNAPSHOT (WHOIS4)
```

**Search for** 210.71.78.27

The owner of 210.71.78.27 is Taiwan Academic Network (TANet).
In fact, this is an IP address in Taipei Municipal Chienkuo High School.

8. Select a domain name. Use nslookup to dump its DNS records. Show your screen dump and explain.




By adding the –query=any option, I can see all the available records (its DNS servers). But I can use "dig" to see more (DNS record types, etc.).

```
~ dig fgisc.org

; <<>> DiG 9.9.5-11ubuntu1.3-Ubuntu <<>> fgisc.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37652
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fgisc.org.                     IN      A

;; ANSWER SECTION:
fgisc.org.              1488    IN      A       203.64.52.131

;; AUTHORITY SECTION:
fgisc.org.              3288    IN      NS      dns2.name-services.com.
fgisc.org.              3288    IN      NS      dns5.name-services.com.
fgisc.org.              3288    IN      NS      dns1.name-services.com.
fgisc.org.              3288    IN      NS      dns3.name-services.com.
fgisc.org.              3288    IN      NS      dns4.name-services.com.

;; ADDITIONAL SECTION:
dns1.name-services.com. 260     IN      A       98.124.192.1

;; Query time: 2 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sun Mar 20 17:38:45 CST 2016
;; MSG SIZE  rcvd: 182
```

9. Select a domain name. Use traceroute or similar tools to find the access path to that domain. Show your screen dump and explain.

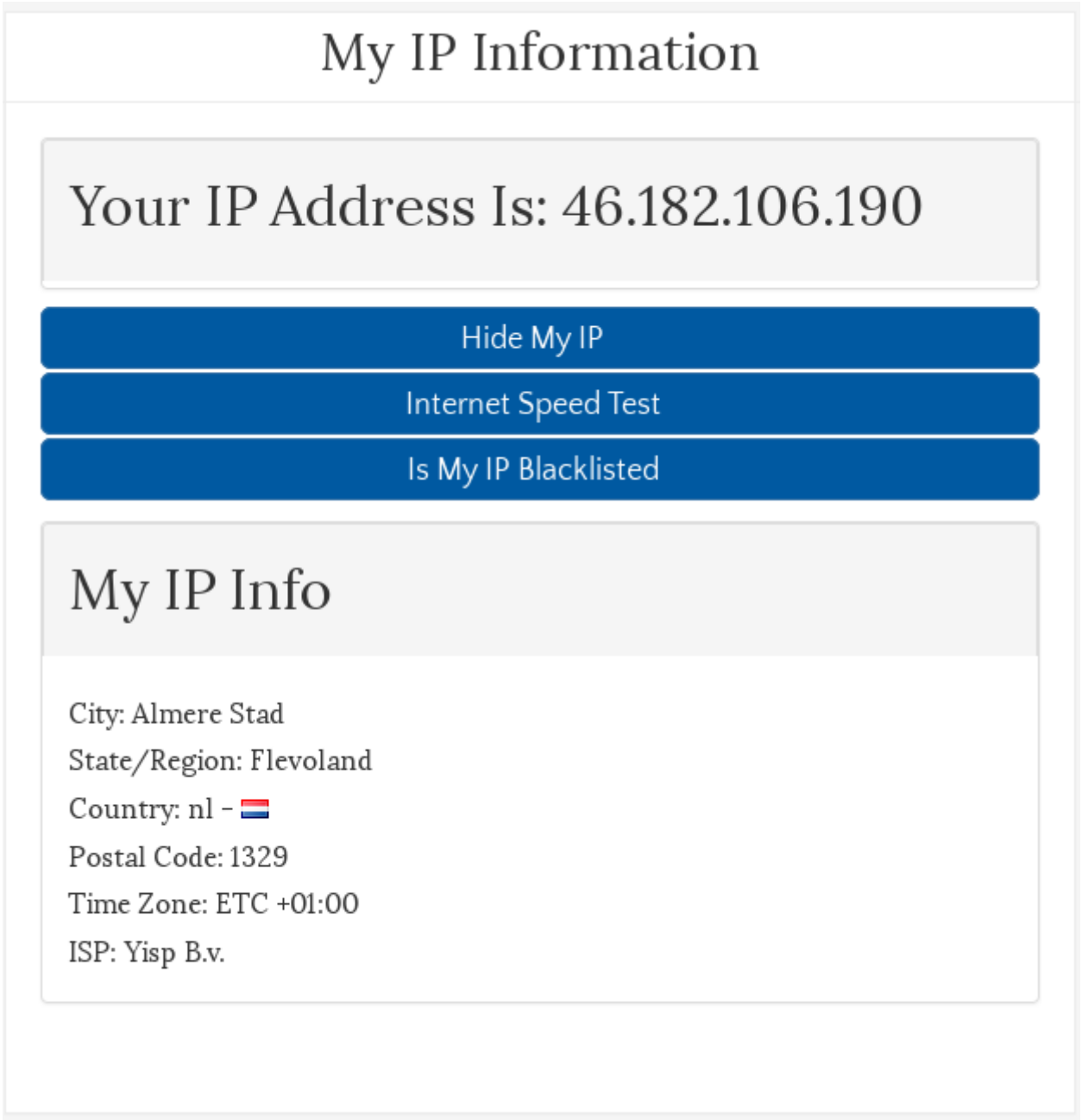
```
~ traceroute ck.tp.edu.tw
traceroute to ck.tp.edu.tw (210.71.78.1), 30 hops max, 60 byte packets
 1  Gateway-140-113-121-0.Dorm13.NCTU.edu.tw (140.113.121.254)  2.880 ms  3.073 ms  3.070 ms
 2  172.16.83.2 (172.16.83.2)  0.948 ms  0.924 ms  0.883 ms
 3  140.113.0.170 (140.113.0.170)  13.678 ms  13.670 ms  13.634 ms
 4  140.113.0.74 (140.113.0.74)  0.869 ms  0.845 ms  0.842 ms
 5  bb-NTU.Nctu.edu.tw (140.113.255.112)  3.748 ms  8.670 ms  3.718 ms
 6  bc-TP-CHT21.TANet.edu.tw (192.83.175.165)  3.478 ms  4.123 ms  3.827 ms
 7  * * *
 8  libra.ck.tp.edu.tw (210.71.78.1)  5.060 ms  4.522 ms  4.522 ms
```

From NCTU, through TANet, to Taipei Municipal Chienkuo High School.

10. Follow the case study right before chapter 1. Select one target and run through all tools (Tor, Vidalia, Privoxy, tor−resolve, proxychains, Nmap, socat, nc). Screen dump the process and explain what you got in your screen.

```
~/Downloads/tor-browser_en-US  sudo service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; enabled; vendor preset: enabled)
   Active: active (exited) since 日 2016-03-20 19:21:43 CST; 32s ago
  Process: 16135 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 16135 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/tor.service

3月 20 19:21:43 yuwen41200 systemd[1]: Stopped Anonymizing overlay network for TCP (multi-instance-master
3月 20 19:21:43 yuwen41200 systemd[1]: Stopping Anonymizing overlay network for TCP (multi-instance-maste
3月 20 19:21:43 yuwen41200 systemd[1]: Starting Anonymizing overlay network for TCP (multi-instance-maste
3月 20 19:21:43 yuwen41200 systemd[1]: Started Anonymizing overlay network for TCP (multi-instance-master
```




# 恭喜!此瀏覽器已設定成使用 Tor。

您的 IP 位址顯示為: 166.70.207.2

請參閱Tor 網站有關安全使用 Tor 的進一步資訊。您現在是以匿名方式瀏覽網際網路。
此出口中繼的更多相關資訊，請參閱: Atlas.

捐款來贊助 Tor

Tor Q&A 網站 | 志願者 | 執行 Relay | 保持匿名

Tor Project 是一個美國 501(c)(3) 非營利組織，致力於線上匿名與隱私的研究、開發和教育。 了解更多資訊 »

JavaScript 已停用。

After setting up tor, my real identity is concealed. The tor browser also shows that I am connected to the targeted website through a lot of relays. However, Google suspect that I am a hacker again, due to all these unusual behavior.

```
~ tor-resolve -v fgisc.org
Mar 20 19:24:15.943 [debug] main(): defaulting to localhost
Mar 20 19:24:15.943 [debug] main(): defaulting to port 9050
203.64.52.131
```

This is what I got from tor-resolve. It's much like nslookup, but runs via tor.

```
~ nmap -V

Nmap version 7.10 ( https://nmap.org )
Platform: x86_64-redhat-linux-gnu
Compiled with: liblua-5.2.4 openssl-1.0.2g nmap-libpcre-7.6 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

I installed the latest version of nmap.

---

```
$ nmap -v -A codesensor.tw

Starting Nmap 7.10 ( https://nmap.org ) at 2016-03-20 19:59 CST
NSE: Loaded 138 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:59
Completed NSE at 19:59, 0.00s elapsed
Initiating NSE at 19:59
Completed NSE at 19:59, 0.00s elapsed
Initiating Ping Scan at 19:59
Scanning codesensor.tw (140.113.203.221) [2 ports]
Completed Ping Scan at 19:59, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:59
Completed Parallel DNS resolution of 1 host. at 19:59, 0.00s elapsed
Initiating Connect Scan at 19:59
Scanning codesensor.tw (140.113.203.221) [1000 ports]
Discovered open port 22/tcp on 140.113.203.221
Discovered open port 80/tcp on 140.113.203.221
Discovered open port 443/tcp on 140.113.203.221
Completed Connect Scan at 20:00, 46.41s elapsed (1000 total ports)
Initiating Service scan at 20:00
Scanning 3 services on codesensor.tw (140.113.203.221)
Completed Service scan at 20:00, 12.06s elapsed (3 services on 1 host)
```

```
NSE: Script scanning 140.113.203.221.
Initiating NSE at 20:00
Completed NSE at 20:00, 0.99s elapsed
Initiating NSE at 20:00
Completed NSE at 20:00, 0.00s elapsed
Nmap scan report for codesensor.tw (140.113.203.221)
Host is up (0.99s latency).
rDNS record for 140.113.203.221: codesensor.cs.nctu.edu.tw
Not shown: 996 filtered ports
PORT    STATE  SERVICE  VERSION
22/tcp  open   ssh      OpenSSH 6.6.1 (protocol 2.0)
| ssh-hostkey:
|   2048 7e:bb:a4:52:f3:fa:4a:f8:a3:60:68:67:85:d6:b3:c0 (RSA)
|_  256 d6:90:93:47:ab:7d:02:6a:ac:09:12:b7:f6:06:b1:01 (ECDSA)
80/tcp  open   http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips
PHP/5.4.16)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
|_http-title: Did not follow redirect to https://codesensor.tw/
113/tcp closed ident
443/tcp open   ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips
PHP/5.4.16)
| http-methods:
|   Supported Methods: POST OPTIONS GET HEAD TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
|_http-title: SENSE Lab - Code Sensor
| ssl-cert: Subject: commonName=www.codesensor.tw/countryName=TW
| Issuer: commonName=AlphaSSL CA - SHA256 - G2/organizationName=GlobalSign
nv-sa/countryName=BE
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2015-12-23T08:23:15
| Not valid after:  2017-01-22T08:23:15
| MD5:   a316 4d89 be96 efde 37e3 db59 ba9d e148
|_SHA-1: 1610 c855 a760 d012 5cb3 abb8 878c 772a 1fa3 c6f8
|_ssl-date: 2016-03-20T12:00:50+00:00; 0s from scanner time.

NSE: Script Post-scanning.
Initiating NSE at 20:00
Completed NSE at 20:00, 0.00s elapsed
Initiating NSE at 20:00
Completed NSE at 20:00, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.35 seconds
```

---

Nmap gives me an abundance of information about address “codesensor.tw,” including but not limited to: alias to codesensor.cs.nctu.edu.tw, IP is 140.113.203.221, port 22 opened for SSH, port 80 opened for HTTP, port 443 opened for HTTPS, runs on CentOS, using Apache, OpenSSH, OpenSSL, and PHP... Since we know what services are provided and their respective versions, we can use the bugs in these specific versions to attack the server.