Homework 5a:
Installing Webservers

Apache (or Lighttpd)

MySQL

PHP

CGI and Dynamic Pages

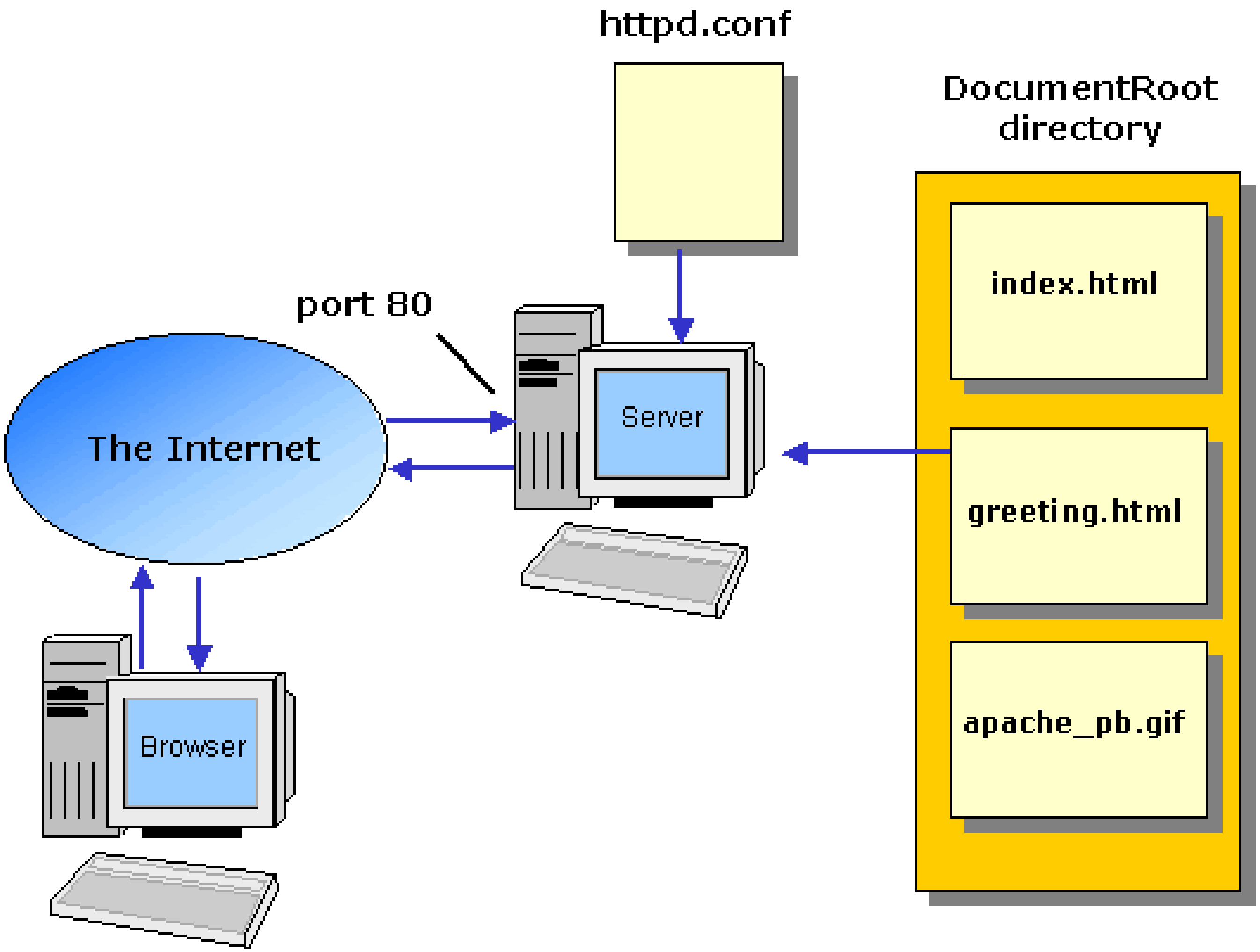
Outline

- ❑ Introductions
  - Apache
  - MySQL
  - PHP
  - Certificate Authentication
- ❑ Installation
  - Apache + MySQL + PHP
- ❑ Administration
  - Apache
  - MySQL
- ❑ Appendix
  - Installing lighttpd
  - CA

Apache

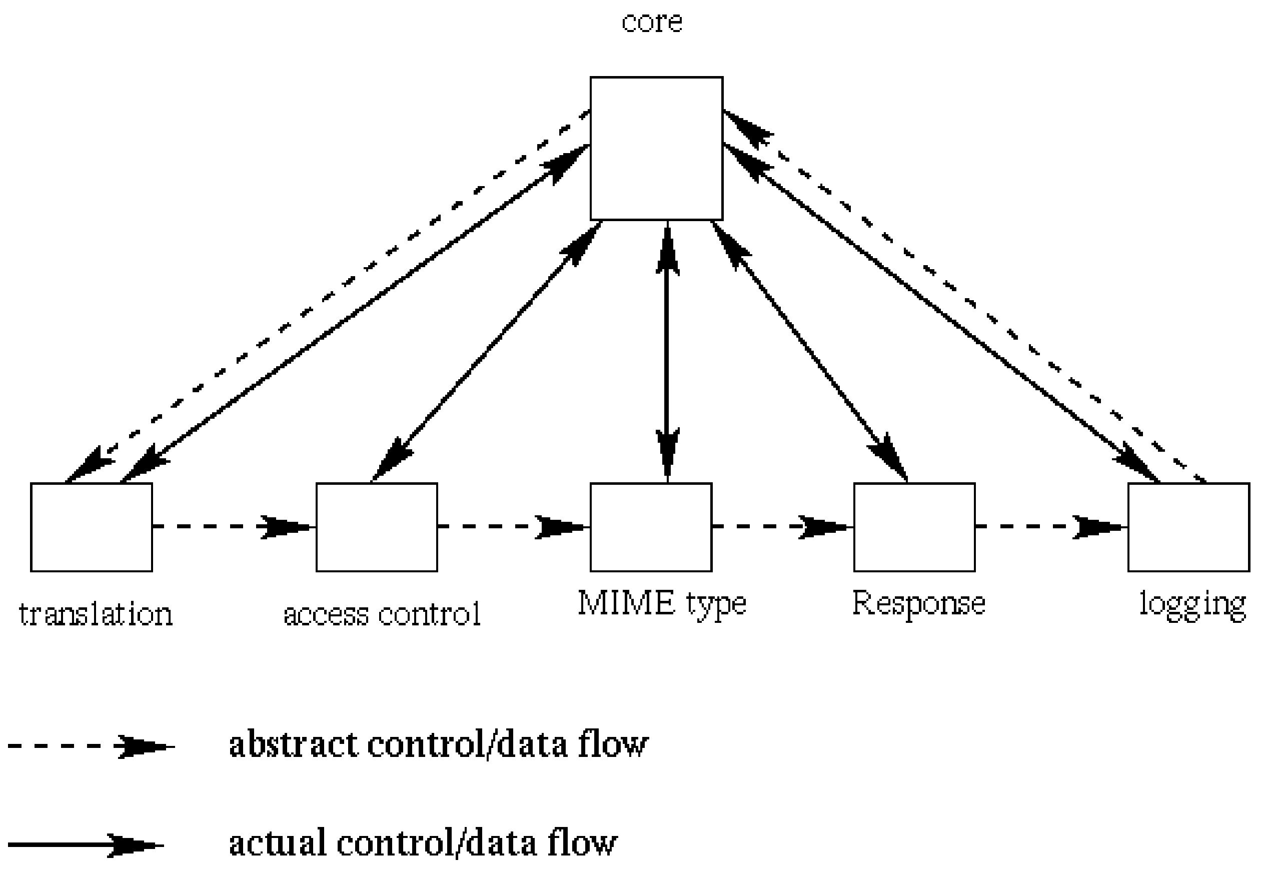
- ❑ Official: http://www.apache.org/
- ❑ Web httpd server that
  - HTTP/1.1 compliant web server
  - Modular design
  - Can be customised by writing modules using Apache module API
  - Freely available cross many platforms
- ❑ Two main parts
  - core
    - ➢ Implement basic functions
  - Modules
    - ➢ Extend or override the functionality of the server
    - ➢ Example:
      - – Access control, logging, CGI, proxy, cache control, PHP…

How Apache Works – request and response

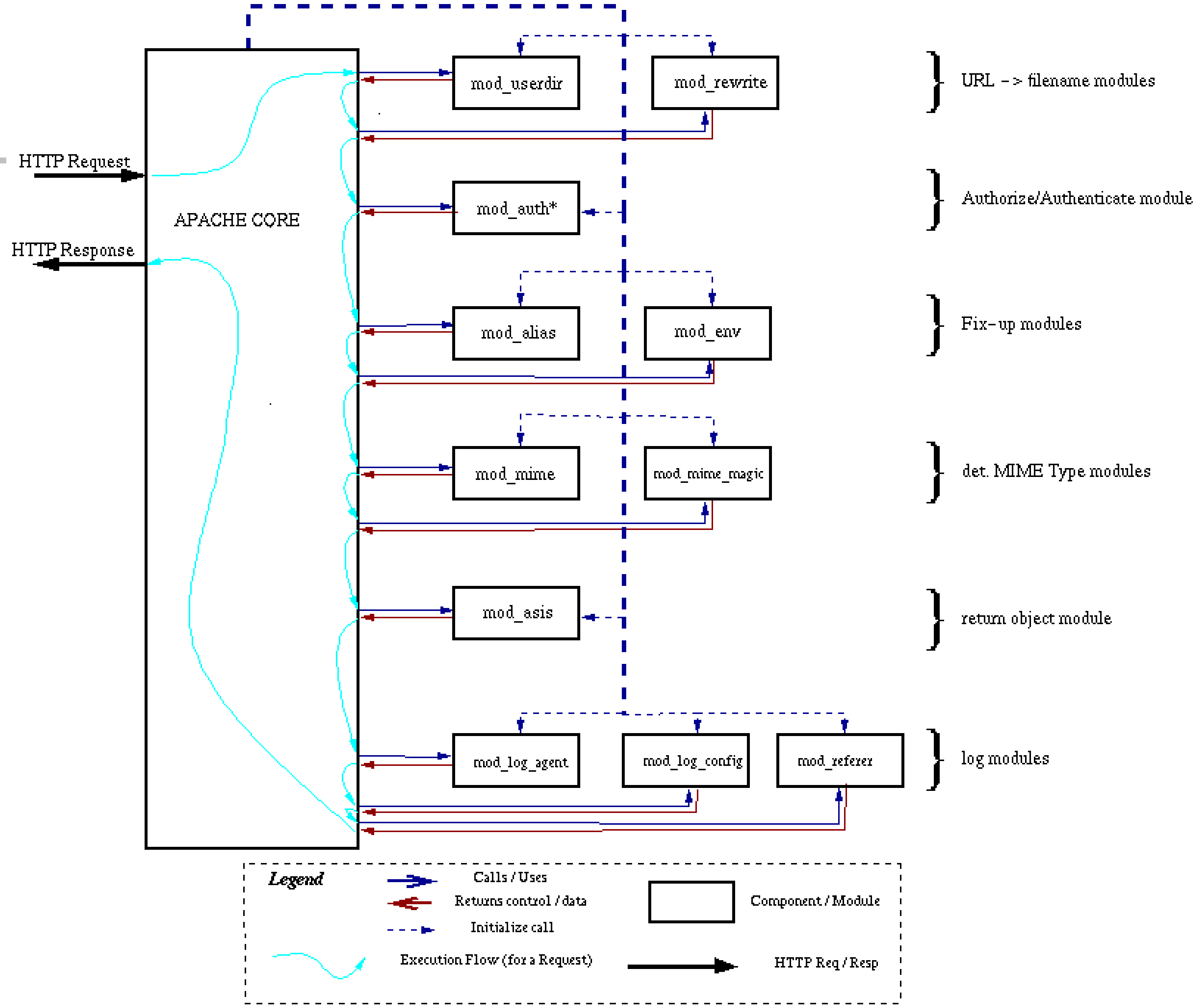


How Apache Works – Each request-response

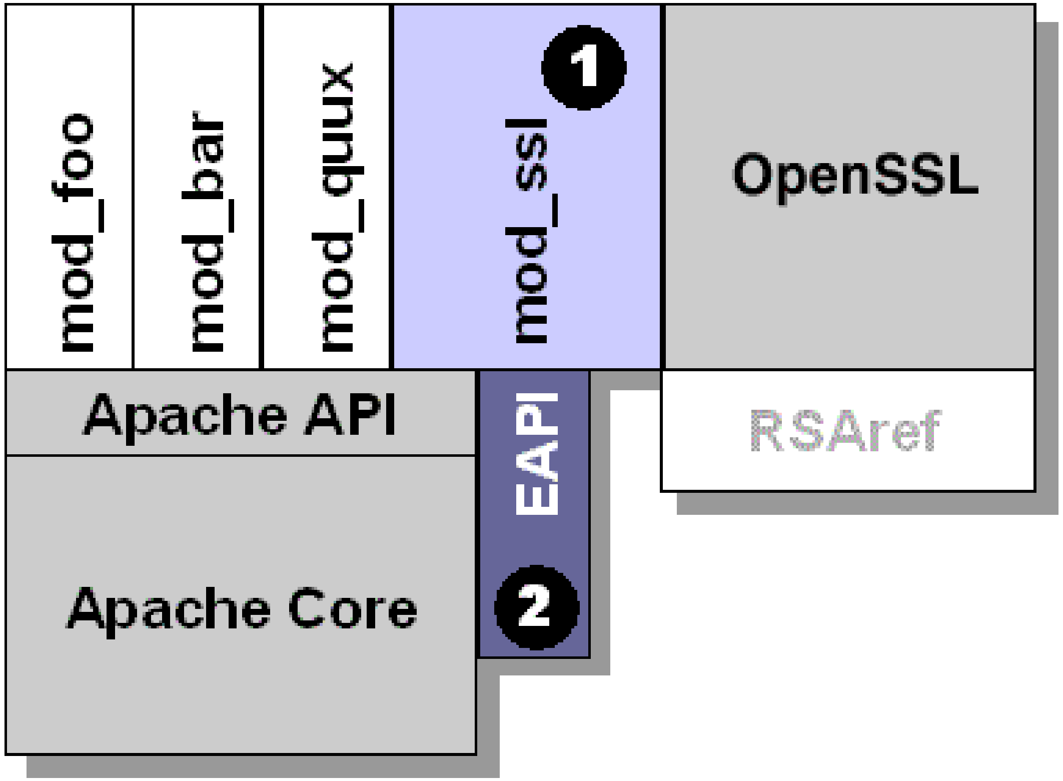
❑ Apache breaks client request into several steps which are implemented as modules



Apache Detail



Apache with mod_ssl



MySQL (1)

- ❑ Official Site: http://www.mysql.com
- ❑ SQL (Structured Query Language)
  - The most popular computer language used to create, modify, retrieve and manipulate data from relational database management systems.
  - Introduction to SQL: http://www.1keydata.com/tw/sql/sql.html
- ❑ A multithreaded, multi-user, SQL Database Management System.
- ❑ MySQL is owned and sponsored by a Swedish company MySQL AB.

MySQL (2)

❑ Characteristics:

- Writing in C/C++, tested by many compilers, portable to many systems.
- Providing APIs for C/C++, Java, Perl, PHP, Python, Ruby, Tcl, …etc.
- Supporting AIX, FreeBSD, HP-UX, Linux, Mac OS, Solaris, Windows, …etc.
- Multi-threaded kernel, supporting systems with multiple CPUs.
- Optimized algorithm for SQL Query.
- Multi-Language (coding) Supports.
- Lots of connecting method: TCP/IP, ODBC, JDBC, Unix domain socket.
- Free Software
- Popular for web applications

PHP

❑ PHP: Hypertext Preprocessor

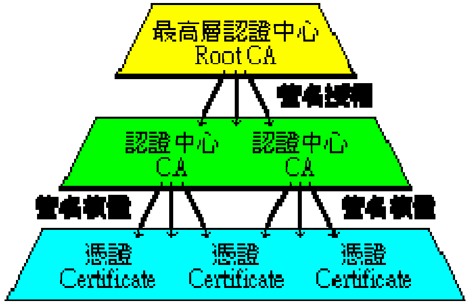
- A widely-used Open Source general-purpose scripting language.
- Originally designed to create dynamic web pages, PHP's principal focus is server-side scripting.
- PHP scripts can be embedded into HTML.
- The LAMP architecture has become popular in the Web industry as a way of deploying inexpensive, reliable, scalable, secure web applications.
  - ➢ PHP is commonly used as the P in this bundle alongside Linux, Apache and MySQL.
  - ➢ FAMP replaces Linux with FreeBSD, WAMP replaces Linux with Windows.

Certificate Authority (1)

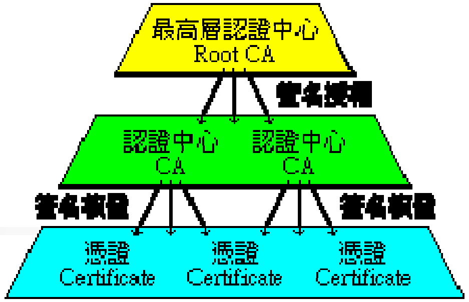
❑ Certificate

- 憑證的原文是 Certificate ，是附上所有人 (owner) 的資料（公司名稱、伺服器名稱、個人真實姓名、連絡 E-mail 、通訊地址等資料），後面加上數位簽名的 Public Key 。憑證上會附有幾個數位簽名，代表這些簽名的人，確認過這個 Public Key 的所有人，和憑證上所載的資料相符，沒有假造。

- 在 X.509 中，最下層每一個合格的憑證 (Certificate) 上，會有一個認證中心 (CA) 的簽名，表示這個認證中心 (CA) 檢查過，確認憑證上的所有者資料無誤。當程式碰到沒見過的憑證時，只要檢查憑證上認證中心 (CA) 的簽名無誤，即代表這個認證中心 (CA) 查核過這個憑證 (Certificate) ，憑證上的資料無誤。



Certificate Authority (2)



❑ Certificate Authority

- 認證中心的原文是 CA ，是 Certificate Authority 的縮寫，在微軟繁體中文 WINDOWS 上翻譯成憑證授權。認證中心是 X.509 的一環。認證中心也是一種憑證，上面附有認證中心本身的資料，但不是用來加解密，而是用來簽發憑證，證明憑證所有人和憑證上所載的資料無誤。

- 每一個合格的認證中心 (CA) 上，會有一個管轄它的最高層認證中心 (Root CA) 的簽名，表示最高層認證中心授權給它，可以簽發別人的憑證。當程式碰到沒見過的憑證，憑證上簽名的認證中心 (CA) 也沒見過時，只要檢查認證中心上附的最高層認證中心 (Root CA) 的簽名無誤，即代表這個最高層認證中心 (Root CA) ，認為這個認證中心 (CA) 的憑證簽發過程很仔細，檢查資料很詳實，所以授權給它，准許它可以簽發憑證 (Certificate) 。所以這個認證中心 (CA) 簽發的憑證 (Certificate) ，憑證上的資料也沒有問題。

- Reference: http://www.imacat.idv.tw/tech/sslcerts.htm

Installation

In this exercise …

❑ What to install

- We want to install Apache + PHP + MySQL + mod_ssl

❑ Install sequence

- Install MySQL
- Install openssl and apache
- Install PHP
- Test PHP in apache

Install Sequence – MySQL

❑ Steps

- # cd/usr/ports/databases/mysql51-server/
- # make WITH_XCHARSET=all install clean

❑ Add into rc.conf

- mysql_enable="YES"

❑ Start up

- # /usr/local/etc/rc.d/mysql-server start

Install Sequence – Openssl and Apache

❑ Steps

- cd /usr/ports/security/openssl
- make install clean

- cd /usr/ports/lang/python
- Make options: WITHOUT_IPV6=yes

- cd /usr/ports/converters/libiconv
- Make options: WITH_EXTRA_PATCHES=yes

- cd /usr/ports/www/apache22/
- make WITH_CHARSET=utf8 WITH_XCHARSET=all WITH_MPM=worker WITH_THREADS=yes WITH_SUEXEC=yes WITH_BERKELEYDB=db4 WITH_STATIC_SUPPORT=yes WITH_ALL_STATIC_MODULES=yes install clean

❑ Add into /etc/rc.conf

- apache22_enable="YES"

❑ Start up

- /usr/local/etc/rc.d/apache22 start

Install Sequence – PHP

- ❑ Steps
  - # cd /usr/ports/lang/php5
  - # make install clean
    - ➢ Remenber to choose Apache module
- ❑ Install php5-extensions
  - # cd /usr/ports/lang/php5-extensions
  - # make install clean
    - ➢ Choose what you need

Install Sequence – test PHP in apache (1)

- Edit httpd.conf to support php
  - % cd /usr/loca/apache/conf
  - % mkdir /www ; mkdir /www/data
  - % Edit httpd.conf

```
<IfModule mime_module>
…
AddType application/x-httpd-php .php .phtml .php5
AddType application/x-httpd-php-source .phps
…
</IfModule>
```

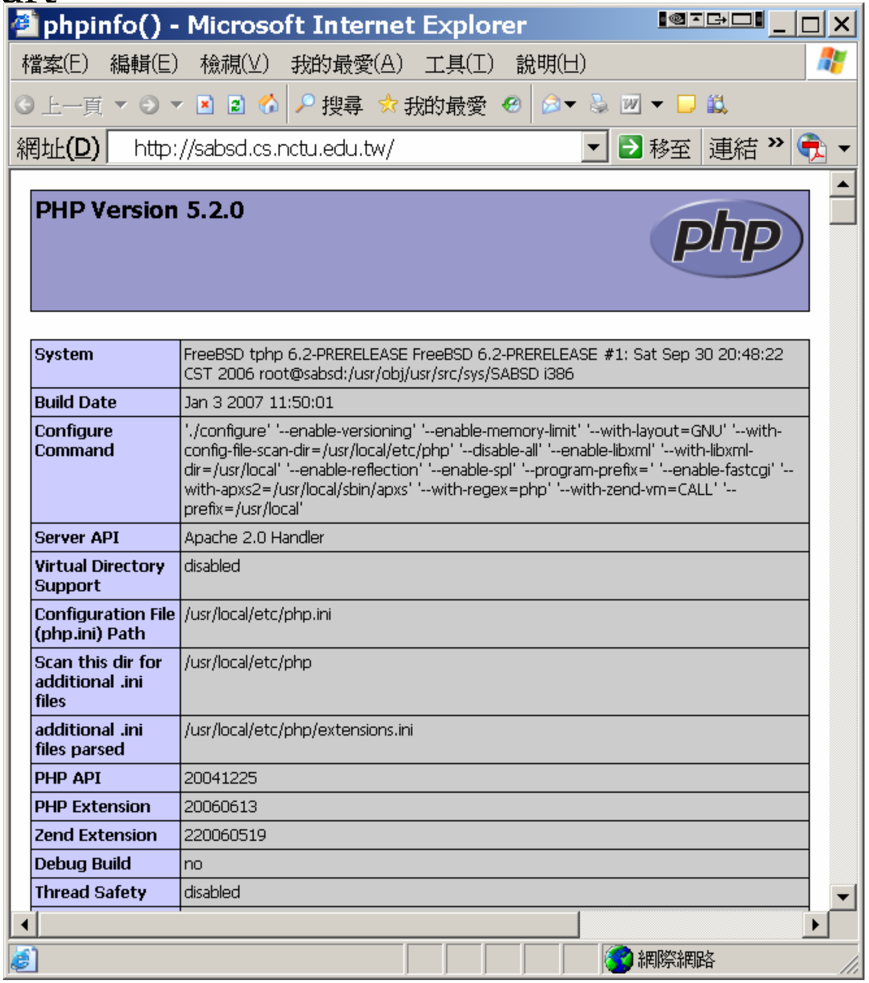
```
ServerName sabsd.cs.nctu.edu.tw
# DocumentRoot "/usr/local/www/apache22/data"
DocumentRoot "/www/data“
…
# <Directory "/usr/local/www/apache22/data ">
<Directory "/www/data">
```

```
<IfModule mod_dir.c>
   DirectoryIndex index.php index.html index.htm
</IfModule>
```

Install Sequence – test PHP in apache (2)

- ❑ Restart httpd
  - /usr/local/etc/rc.d/apache22 restart
- ❑ Test PHP
  - % Edit /www/data/index.php

```
<?
        phpinfo();
?>
```


phpinfo() - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D)
http://sabsd.cs.nctu.edu.tw/
移至
連結
網際網路

PHP Version 5.2.0

System	FreeBSD tphp 6.2-PRERELEASE FreeBSD 6.2-PRERELEASE #1: Sat Sep 30 20:48:22 CST 2006 root@sabsd:/usr/obj/usr/src/sys/SABSD i386
Build Date	Jan 3 2007 11:50:01
Configure Command	'./configure' '--enable-versioning' '--enable-memory-limit' '--with-layout=GNU' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--with-libxml-dir=/usr/local' '--enable-reflection' '--enable-spl' '--program-prefix=' '--enable-fastcgi' '--with-apxs2=/usr/local/sbin/apxs' '--with-regex=php' '--with-zend-vm=CALL' '--prefix=/usr/local'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php
additional .ini files parsed	/usr/local/etc/php/extensions.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled

Administration

Apache configuration

- ❑ Location
  - The default location of apache (in ports) is /usr/local/etc/apache22
  - Major configuration file: httpd.conf
    - ➢ Other configuration files could be included. (setting in httpd.conf)
- ❑ Two types
  - Global configurations
    - ➢ Global setting
    - ➢ Server specific setting
    - ➢ Virtual host setting
  - Directory Configuration
    - ➢ Local setting for certain directory

Apache configuration – Global Configuration

❑ Global setting

- ServerType standalone
- Timeout 300
- KeepAlive On
- KeepAliveRequests 100
- StartServers 5

❑ Server configuration

- Port 80
- ServerAdmin chwong@sabsd.cs.nctu.edu.tw
- ServerName sabsd.cs.nctu.edu.tw
- DocumentRoot "/www/data"

Apache configuration – Directory Configuration (1)

- Configuration parameters
  - Options
    - All (turn on all options except multiview)
    - ExecCGI (To allow executions of AddHandler)
    - FollowSymLinks (access files outside this directory)
    - Indexs (generate file-list for browsing)
(when there is no DirectoryIndex files)
    - MultiViews (multi-language support)
  - AllowOverride
    - All (Read .htaccess)
    - None (ignoring .htaccess)
  - Deny/Allow
    - IP/DN (control access to this directory)
  - Order
    - Solve collision of deny and allow rules

```
<Directory "/www/data">
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        Allow from all
</Directory>
```

Apache configuration – Directory Configuration (2)

```
# User home directories
#Include etc/apache22/extra/httpd-userdir.conf
```

```
UserDir public_html
UserDir disabled root toor daemon operator bin tty kmem games news man
sshd bind proxy _pflogd _dhcp uucp pop www nobody mailnull smmsp
#
# Control access to UserDir directories.  The following is an example
# for a site where these directories are restricted to read-only.
#
<Directory /home/*/public_html>
    AllowOverride FileInfo AuthConfig Limit Indexes
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    <Limit GET POST OPTIONS>
        Order allow,deny
        Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS>
        Order deny,allow
        Deny from all
    </LimitExcept>
</Directory>
```

Apache configuration – Directory Configuration (3)

```
<IfModule alias_module>
  Alias /icons/ "/usr/local/www/apache22/icons/"

  <Directory "/usr/local/www/apache22/icons">
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
  </Directory>

  Alias /manual/ "/usr/local/apache/htdocs/manual/"

  <Directory "/usr/local/apache/htdocs/manual">
    Options Indexes FollowSymlinks MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
  </Directory>
</IfModule>
```

Apache configuration – Virtual Host

❑Name-Base

- Singe IP, several hostnames

```
NameVirtualHost 140.113.51.24

<VirtualHost 140.113.51.24>
ServerName www.snmg.com.tw
DocumentRoot "/www"
</VirtualHost>

<VirtualHost 140.113.51.24>
ServerName mail.snmg.com.tw
DocumentRoot "/home/sywang"
</VirtualHost>

<VirtualHost 140.113.51.24>
ServerName csie.snmg.com.tw
Redirect / http://www.csie.nctu.edu.tw/
</VirtualHost>
```

❑IP-Base

- several IPs

```
<VirtualHost 140.113.50.33:80>
Port 80
ServerAdmin webmaster@sun3.csie.nctu.edu.tw
DocumentRoot /www/csie
ServerName sun3.csie.nctu.edu.tw
ErrorLog logs/csie-error_log
TransferLog logs/csie-access_log
</VirtualHost>

<VirtualHost 140.113.70.25:80>
Port 80
ServerAdmin webmaster@sun3.ee.nctu.edu.tw
DocumentRoot /www/ee
ServerName sun3.ee.nctu.edu.tw
ErrorLog logs/ee-error_log
TransferLog logs/ee-access_log
</VirtualHost>
```

Apache configuration – .htaccess (1)

- ❑ .htaccess
  - Allow admin to use one file to control access to certain directory
- ❑ Usage
  - Modify httpd.conf
  - Create .htaccess file
  - Generate password database
  - Test

Apache configuration – .htaccess (2)

❑ Example

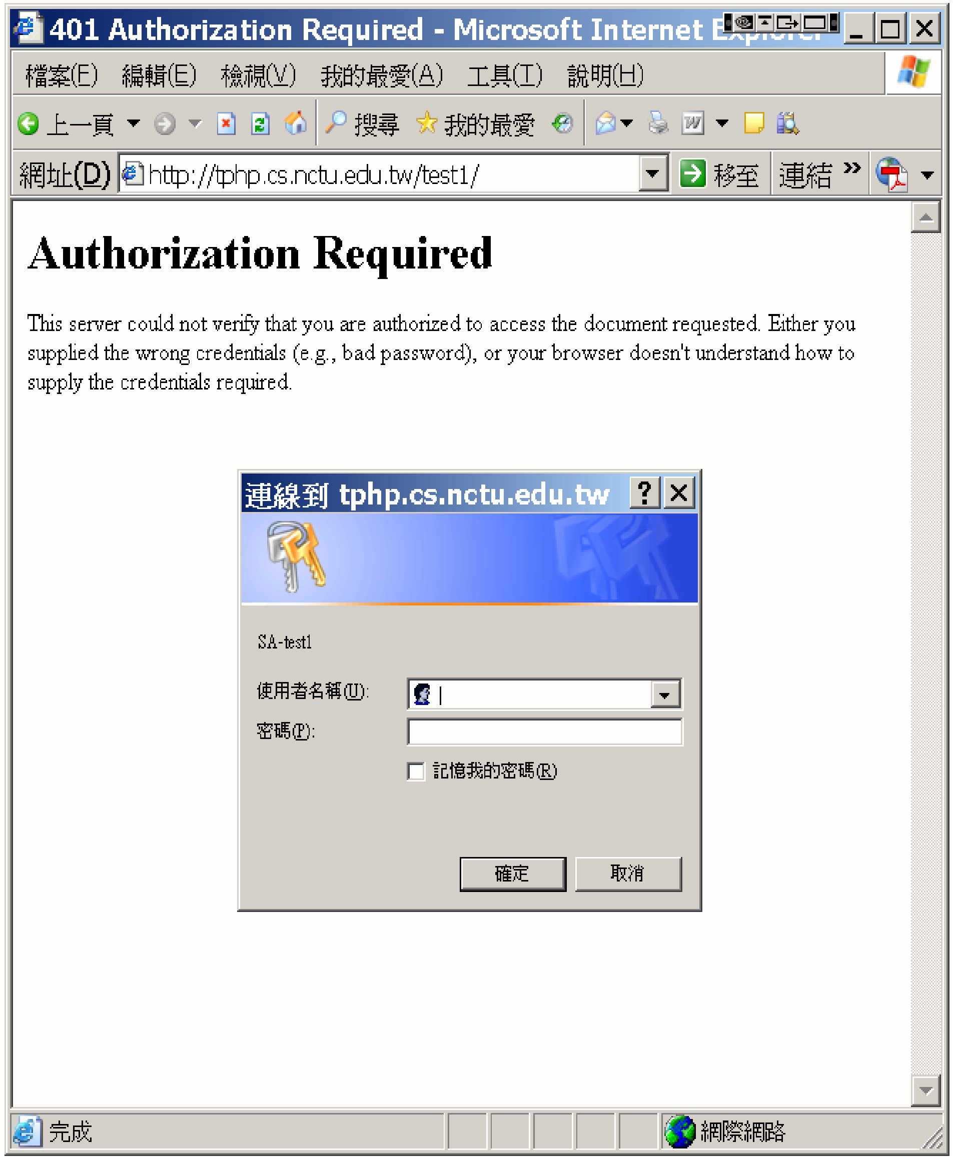
- Modify httpd.conf
- Create .htaccess file
- Generate password file

```
<Directory "/www/data/test1">
   Options Indexes FollowSymLinks MultiViews ExecCGI
   AllowOverride All
   Order allow,deny
   Allow from all
</Directory>
```

```
chwong@sabsd [3:02pm] /www/data/test1> cat .htaccess
AuthName "SA-test1"
AuthType "Basic"
AuthUserFile “/www/data/test1/.htpasswd”
require valid-user
```

```
chwong@sabsd [2:58pm] /> /usr/local/apache/bin/htpasswd -c ./.htpasswd SA-user1
New password:
Re-type new password:
Adding password for user SA-user1
```

Apache configuration – .htaccess (3)


401 Authorization Required - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D)
移至
連結
完成
網際網路

http://tphp.cs.nctu.edu.tw/test1/

Authorization Required

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

連線到 tphp.cs.nctu.edu.tw

SA-test1

使用者名稱(U):

密碼(P):

☐ 記憶我的密碼(R)

Apache configuration – log

❑ Rotate your log using newsyslog

Apache configuration – Certificate Authority (1)

- ❑ Flow
  - Generate random seed
  - Generate RootCA
    - ➢ Generate private key of RootCA
    - ➢ Fill the Request of Certificate.
    - ➢ Sign the certificate itself.
  - Generate certificate of Web Server
    - ➢ Generate private key of Web Server
    - ➢ Fill the Request of certificate
    - ➢ Sign the certificate using RootCA
  - Modify apache configuration ➔ restart apache

Apache configuration – Certificate Authority (2)

- Generate random seed
  - ➢ openssl rand -out rnd-file num
    - – Ex. openssl rand -out /etc/ssl/RootCA/private/.rnd 1024
  - ➢ chmod go-rwx rnd-file
    - – Ex. chmod go-rwx /etc/ssl/RootCA/private/.rnd

Apache configuration – Certificate Authority (3)

- Generate RootCA
  - ➢ Generate private key of RootCA
    - – openssl genrsa -des3 -rand rnd-file -out rootca-key-file num

```
% openssl genrsa -des3 -rand /etc/ssl/RootCA/private/.rnd \
    -out /etc/ssl/RootCA/private/rootca.key.pem 2048
```

Note: phrase are asked (something like password)

    - – chmod go-rwx rootca-key-file

```
% chmod go-rwx /etc/ssl/RootCA/private/rootca.key.pem
```

Apache configuration – Certificate Authority (4)

- Generate RootCA
  - ➢ Generate private key of RootCA
  - ➢ Fill the Request of Certificate.
    - – openssl req -new -key rootca-key-file -out rootca-req-file

      ```
      % openssl req -new -key /etc/ssl/RootCA/private/rootca.key.pem \
          -out /etc/ssl/RootCA/private/rootca.req.pem
      ```

    - – chmod go-rwx rootca-req-file

      ```
      % chmod go-rwx /etc/ssl/RootCA/private/rootca.req.pem
      ```

```
Enter pass phrase for rootca-key-file:

Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:HsinChu
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NCTU
Organizational Unit Name (eg, section) []:CS
Common Name (eg, YOUR name) []:sabsd.cs.nctu.edu.tw
Email Address []:chwong@cs.nctu.edu.tw

A challenge password []: (不需要密碼，直接 Enter)
An optional company name []: (直接 Enter)
```

Apache configuration – Certificate Authority (5)

- Generate RootCA
  - ➢ Generate private key of RootCA
  - ➢ Fill the Request of Certificate.
  - ➢ Sign the certificate itself.
    - – openssl x509 -req -days #_of_days -sha1 \
      -extfile path_of_openssl.cnf -extensions v3_ca \
      -signkey rootca-key-file -in rootca-req-file -out rootca-crt-file

      ```
      % openssl x509 -req -days 5109 -sha1 -extfile /etc/ssl/openssl.cnf -extensions
          v3_ca -signkey /etc/ssl/RootCA/private/rootca.key.pem -in
          /etc/ssl/RootCA/private/rootca.req.pem -out
          /etc/ssl/RootCA/private/rootca.crt.pem
      ```
    - – rm -f rootca-req-file

      ```
      %rm -f /etc/ssl/RootCA/private/rootca.req.pem
      ```
    - – chmod go-rwx rootca-crt-file
      - » %chmod go-rwx /etc/ssl/RootCA/private/rootca.crt.pem

Apache configuration – Certificate Authority (6)

- Generate certificate of Web Server
  - Generate private key of Web Server
    - openssl genrsa -out host-key-file num

      %openssl genrsa -out /etc/ssl/sabsd/private/sabsd.key.pem 1024
    - chmod go-rwx host-key-file

      %chmod go-rwx /etc/ssl/sabsd/private/sabsd.key.pem
  - Fill the Request of certificate
    - openssl req -new -key host-key-file -out host-req-file

      % openssl req -new -key /etc/ssl/sabsd/private/sabsd.key.pem -out /etc/ssl/sabsd/private/sabsd.req.pem
    - chmod go-rwx host-req-file

      % chmod go-rwx /etc/ssl/sabsd/private/sabsd.req.pem

Apache configuration – Certificate Authority (7)

- Generate certificate of Web Server
  - Generate private key of Web Server
  - Fill the Request of certificate
  - Sign the certificate using RootCA
    - Tramsmit host-req-file to Root CA, and do following steps in RootCA
    - openssl x509 -req -days #_of_days -sha1 -extfile path_of_openssl.cnf \
      -extensions v3_ca -CA rootca-crt-file -CAkey rootca-key-file \
      -CAserial rootca-srl-file -CAcreateserial -in host-req-file -out host-crt-file

      ```
      % openssl x509 -req -days 361 -sha1 -extfile /etc/ssl/openssl.cnf -extensions v3_ca
          -CA /etc/ssl/RootCA/private/rootca.crt.pem -CAkey
          /etc/ssl/RootCA/private/rootca.key.pem -CAserial
          /etc/ssl/RootCA/private/rootca.srl -CAcreateserial -in
          /etc/ssl/sabsd/private/sabsd.req.pem -out /etc/ssl/sabsd/private/sabsd.crt.pem
      ```
    - rm -f host-req-file (in both RootCA and Web Server)

      ```
      % rm -f /etc/ssl/sabsd/private/sabsd.req.pem
      ```
    - Transmit host-crt-file back to Web Server

Apache configuration – Certificate Authority (8)

- Modify apache configuration → restart apache

```
##
## SSL Virtual Host Context
##
<VirtualHost _default_:443>
#   General setup for the virtual host
DocumentRoot /www/data
<Directory "/www/data">
    Options Indexes FollowSymLinks
    AllowOverride All
    Order allow,deny
    Allow from all
</Directory>
ServerName sabsd.cs.nctu.edu.tw:443
ServerAdmin chwong@sabsd.cs.nctu.edu.tw
ErrorLog /var/log/httpd/sabsd.cs-error.log
CustomLog /var/log/httpd/sabsd.cs-access.log common

SSLEngine on
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:!SSLv2:+EXP:+eNULL
SSLCertificateFile /etc/ssl/sabsd/sabsd.crt.pem
SSLCertificateKeyFile /etc/ssl/sabsd/private/sabsd.key.pem
```

Administrating MySQL (1)

- ❑ Config file
  - Copy config file
    - ➢ % cd /usr/local/share/mysql
    - ➢ % sudo cp my-huge.cnf /etc/my.cnf
  - Edit /etc/my.cnf
- ❑ Start up
  - Add into rc.conf
    - ➢ mysql_enable="YES"
  - # /usr/local/etc/rc.d/mysql-server start

Administrating MySQL (2)

- ❑ Test
  - % mysql –u root –p
    - ➢ The initial password for root is empty

```
chwong@sabsd:/var/log> mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2 to server version: 4.1.7-log

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+----------+
| Database|
+----------+
| mysql    |
| test     |
+----------+
2 rows in set (0.27 sec)

mysql> exit
Bye
```

Administrating MySQL (3)

```
mysql> SELECT Host, User From mysql.user;
+-------------------------+------+
| Host                    | User |
+-------------------------+------+
| localhost               |      |
| localhost               | root |
| sabsd.cs.nctu.edu.tw    |      |
| sabsd.cs.nctu.edu.tw    | root |
+-------------------------+------+
```

❑ Securing initial accounts

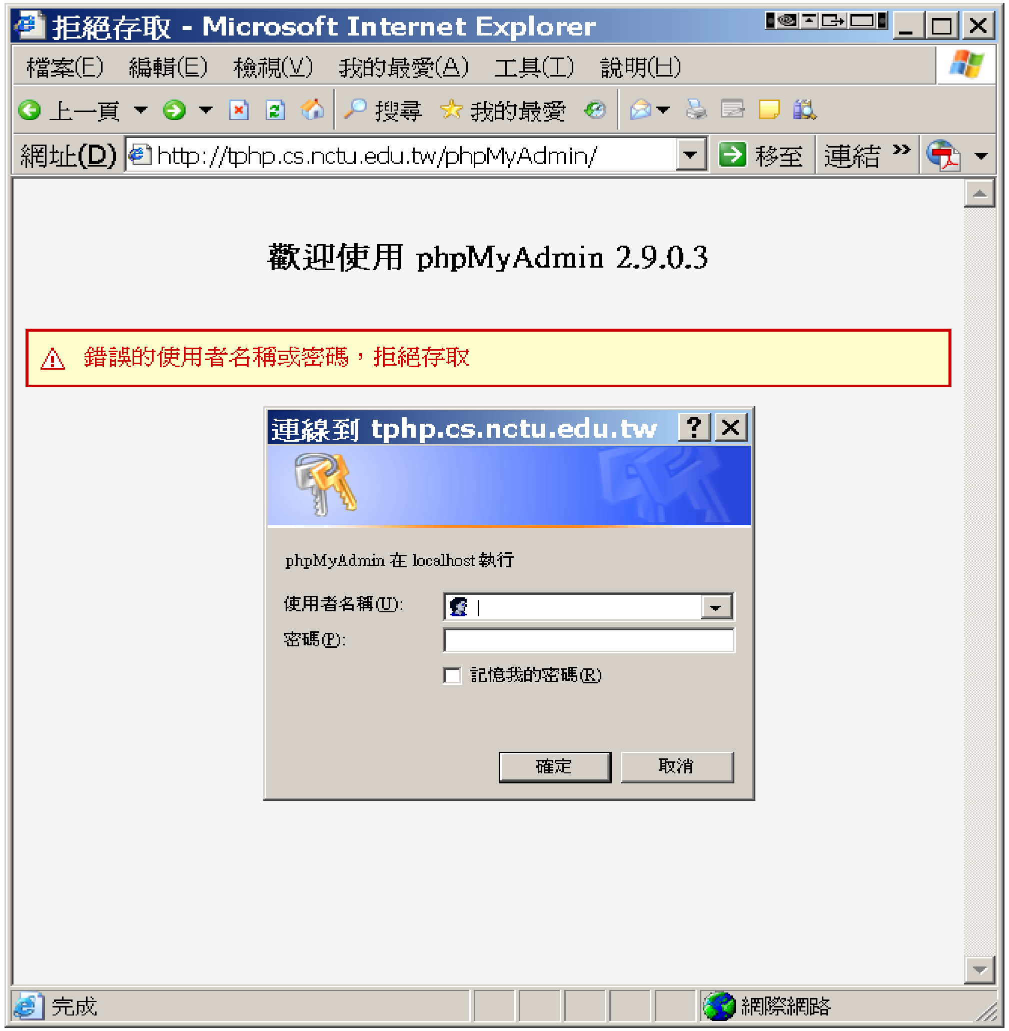
- Two initial accounts
  - root
  - anonymous

```
chwong@sabsd:~> mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4 to server version: 4.1.7-log

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> UPDATE mysql.user SET Password = PASSWORD(‘user123') WHERE User = '';
Query OK, 2 rows affected (0.26 sec)
Rows matched: 2  Changed: 2  Warnings: 0

mysql> UPDATE mysql.user SET Password = PASSWORD(‘root123') WHERE User = 'root';
Query OK, 2 rows affected (0.00 sec)
Rows matched: 2  Changed: 2  Warnings: 0

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

Administrating MySQL – Using phpMyAdmin (1)

- ❑ phpMyAdmin can manage a whole MySQL server as well as a single database.
- ❑ Official Site: http://www.phpmyadmin.net/
- ❑ Characteristics
  - Browser-based, Supporting PHP5, MySQL 4.1 and 5.0, Open Source
- ❑ Installation Steps
  1. Download latest version from official site
  2. Unzip the archived file.
  3. Read documents: Documentation.html
  4. copy config.sample.inc.php → config.inc.php
     - Change auth type to http
     - Remove configuration about Advanced Feature (something start with ‘pma’)
  - Browse the phpMyAdmin, and login.

Administrating MySQL – Using phpMyAdmin (2)



拒絕存取 - Microsoft Internet Explorer

網址(D) http://tphp.cs.nctu.edu.tw/phpMyAdmin/

歡迎使用 phpMyAdmin 2.9.0.3

⚠ 錯誤的使用者名稱或密碼，拒絕存取

連線到 tphp.cs.nctu.edu.tw

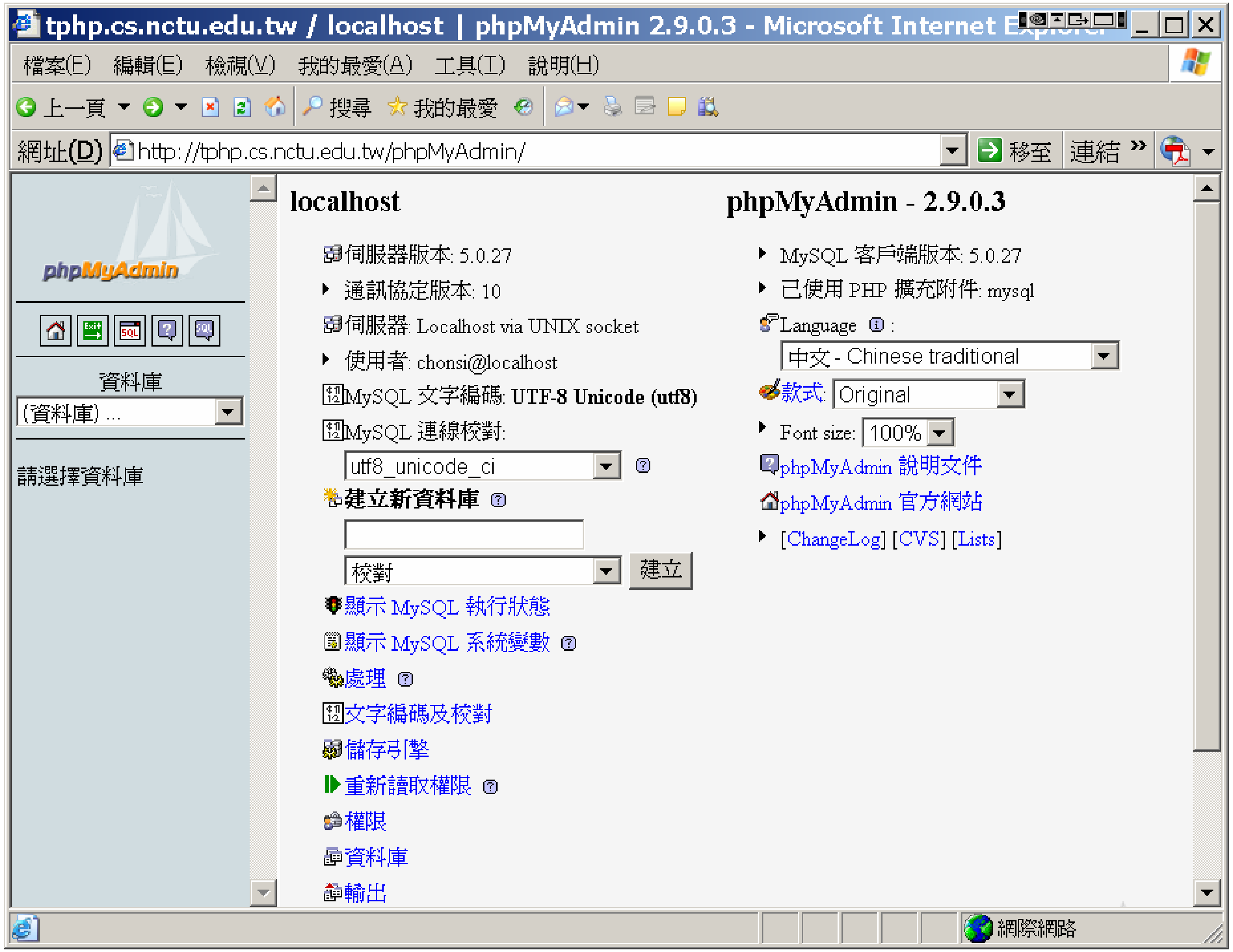
phpMyAdmin 在 localhost 執行

使用者名稱(U):

密碼(P):

□ 記憶我的密碼(R)

Administrating MySQL – Using phpMyAdmin (3)



tphp.cs.nctu.edu.tw / localhost | phpMyAdmin 2.9.0.3 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D) http://tphp.cs.nctu.edu.tw/phpMyAdmin/
移至
連結
phpMyAdmin
資料庫
(資料庫) ...
請選擇資料庫
網際網路

localhost

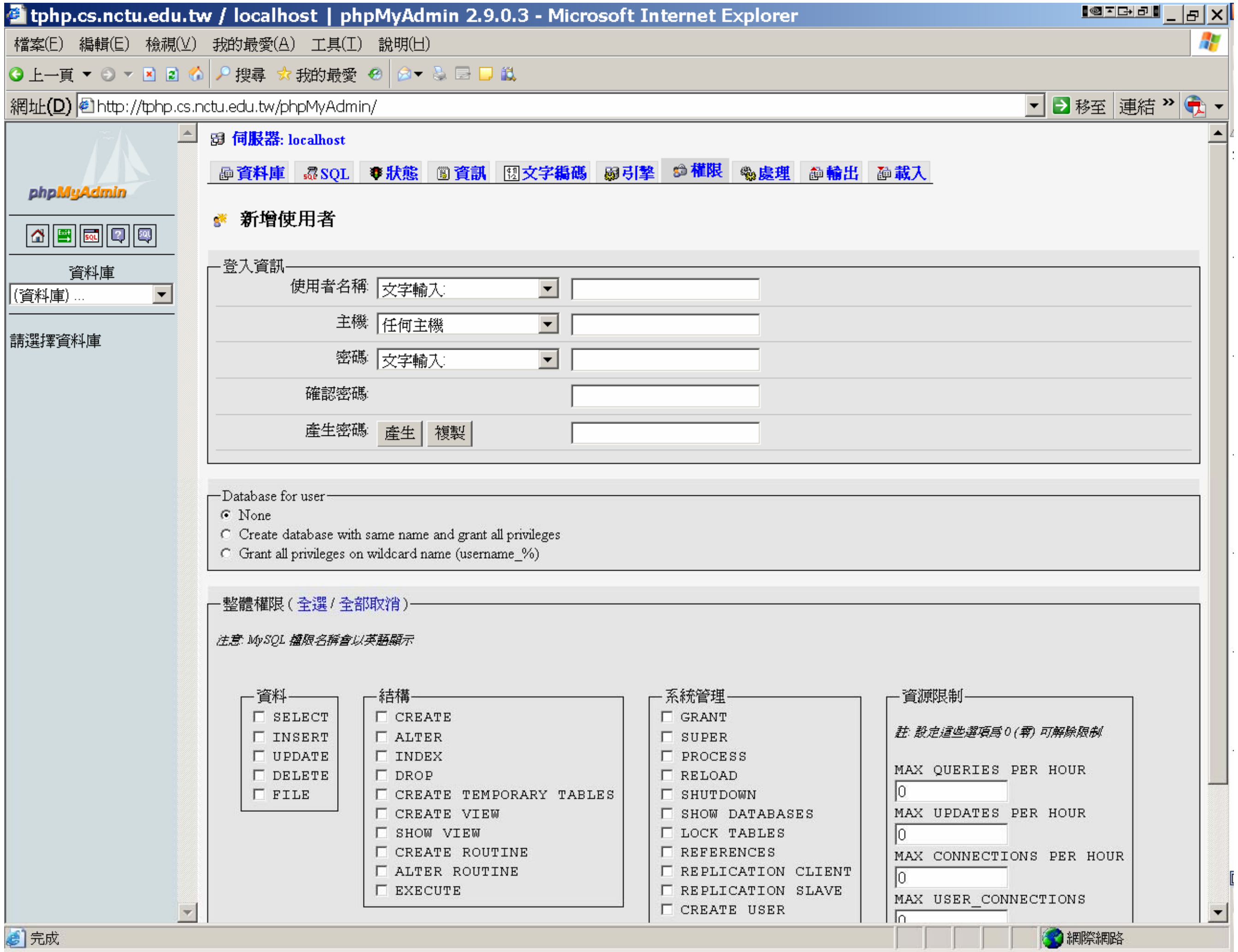
- 伺服器版本: 5.0.27
- 通訊協定版本: 10
- 伺服器: Localhost via UNIX socket
- 使用者: chonsi@localhost
- MySQL 文字編碼: **UTF-8 Unicode (utf8)**
- MySQL 連線校對: utf8_unicode_ci
- **建立新資料庫**
  - 校對 建立
- 顯示 MySQL 執行狀態
- 顯示 MySQL 系統變數
- 處理
- 文字編碼及校對
- 儲存引擎
- 重新讀取權限
- 權限
- 資料庫
- 輸出

phpMyAdmin - 2.9.0.3

- MySQL 客戶端版本: 5.0.27
- 已使用 PHP 擴充附件: mysql
- Language: 中文 - Chinese traditional
- 款式: Original
- Font size: 100%
- phpMyAdmin 說明文件
- phpMyAdmin 官方網站
- [ChangeLog] [CVS] [Lists]

Administrating MySQL – Using phpMyAdmin (4)

- ❑ Create another user with limited privilege



tphp.cs.nctu.edu.tw / localhost | phpMyAdmin 2.9.0.3 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://tphp.cs.nctu.edu.tw/phpMyAdmin/
移至 連結
phpMyAdmin
資料庫
(資料庫) ...
請選擇資料庫
伺服器: localhost
資料庫 SQL 狀態 資訊 文字編碼 引擎 權限 處理 輸出 載入
完成
網際網路

新增使用者

登入資訊

使用者名稱:	文字輸入:	
主機:	任何主機	
密碼:	文字輸入:	
確認密碼:		
產生密碼:	產生 複製	

Database for user

- ● None
- ○ Create database with same name and grant all privileges
- ○ Grant all privileges on wildcard name (username_%)

整體權限 (全選 / 全部取消)

注意: MySQL 權限名稱會以英語顯示

資料

- □ SELECT
- □ INSERT
- □ UPDATE
- □ DELETE
- □ FILE

結構

- □ CREATE
- □ ALTER
- □ INDEX
- □ DROP
- □ CREATE TEMPORARY TABLES
- □ CREATE VIEW
- □ SHOW VIEW
- □ CREATE ROUTINE
- □ ALTER ROUTINE
- □ EXECUTE

系統管理

- □ GRANT
- □ SUPER
- □ PROCESS
- □ RELOAD
- □ SHUTDOWN
- □ SHOW DATABASES
- □ LOCK TABLES
- □ REFERENCES
- □ REPLICATION CLIENT
- □ REPLICATION SLAVE
- □ CREATE USER

資源限制

註: 設定這些選項為 0 (零) 可解除限制

MAX QUERIES PER HOUR: 0

MAX UPDATES PER HOUR: 0

MAX CONNECTIONS PER HOUR: 0

MAX USER_CONNECTIONS: 0

Appendix: Installing lighttpd

Installing lighttpd (1)

- ❑ Official: http://www.lighttpd.net/
- ❑ 安裝
  - # cd /usr/ports/www/lighttpd
  - # make install clean
- ❑ Supporting PHP
  - 修改lighttpd的設定檔/usr/local/etc/lighttpd.conf

將「“mod_fastcgi”,」前面的註解(#字號)刪除

將

```
fastcgi.server= ( “.php”=>
( "localhost" =>
(
"socket" => "/tmp/php-fastcgi.socket",
"bin-path" => "/usr/local/bin/php-cgi"
)
)
)
```

這八行的註解刪除

Installing lighttpd (2)

❑ SSL support

- #### SSL engine
- ssl.engine = “enable”
- ssl.pemfile = “/path/server.pem”

❑ Virtual Hosting

- Simple Virtual-Hosting

```
#simple-vhost.server-root   = "/home/weigon/wwwroot/servers/"
#simple-vhost.default-host  = "grisu.home.kneschke.de"
#simple-vhost.document-root = "/pages/“
```

- Enhanced Virtual-Hosting
  - ➢ http://trac.lighttpd.net/trac/wiki/Docs%3AModEVhost

❑ 其餘可按需求更改設定

Installing lighttpd (3)

❑ 在/etc/rc.conf檔案中加入：

- lighttpd_enable="YES"

❑ 手動啓動

- /usr/local/etc/rc.d/lighttpd start

Appendix: CA

What is a CA ?

- ❑ *Certificate Authority* (認證中心)
- ❑ Trusted server which signs certificates
- ❑ One private key and relative public key
- ❑ Tree structure of X.509
  - *Root CA*

What is a CA ? (c.2)

- ❑ Root CA (最高層認證中心)
  - Micro$oft 翻譯成「根目錄授權憑證」
  - 通常 Root CA 不會直接用來簽發憑證，而是授權給一些中間的認證中心，讓這些中間的認證中心來簽發憑證
  - Root CA 自己幫自己簽名
    - ➢ 沒有再上層可以為他簽名
  - 認可最高層認證中心
    - ➢ 經由 secure channel 安裝 Root CA 的憑證
  - Root CA 只能由一些著名可靠的公司來擔任
    - ➢ 無法再向上查驗，所以不可隨便加進系統信任的 Root CA

What is a CA ? (c.3)

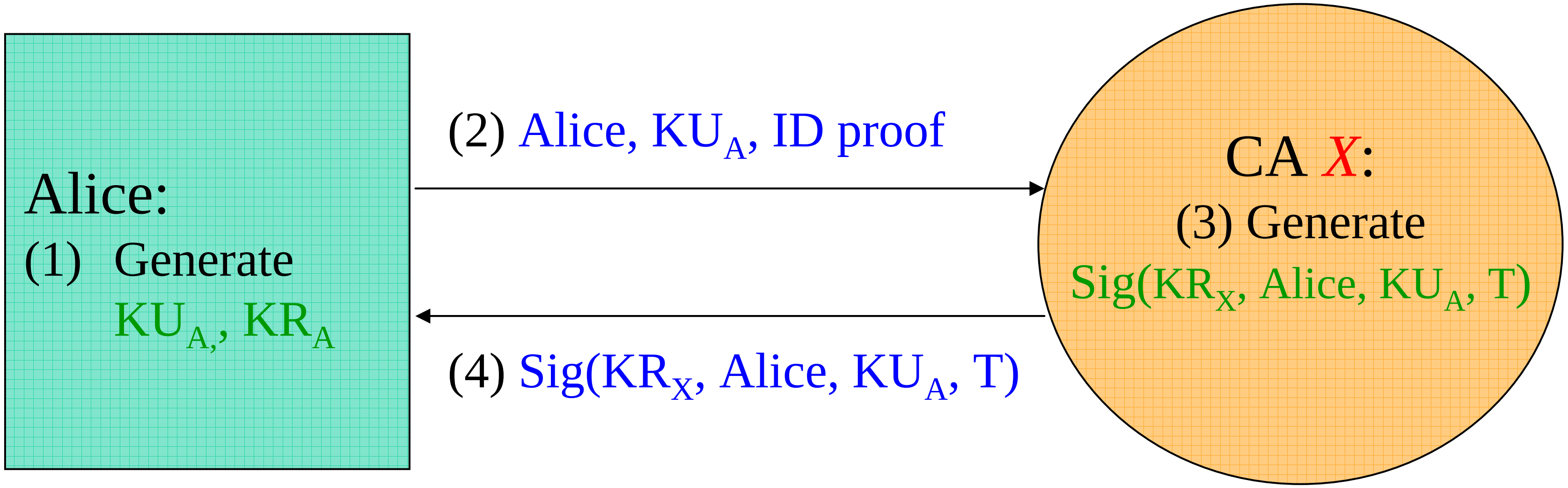
❑ Tree structure of CA
- 每個合格的 CA，都會有一個管轄它的最高層 CA 的簽名，表示 Root CA 授權給它，可以簽發別人的憑證
- 當程式碰到沒見過的憑證，憑證上簽名的 CA 也沒見過時，只要檢查 Root CA 的簽名無誤，就接受這個憑證

❑ Cost of certificate
- HiTrust : NT *$30,000* / per year / per host
- Myself : NT *$0*

Certificate

- ❑ 電子憑證 / 公開金鑰憑證 / 網路身份證
- ❑ A certificate is issued by a CA *X*
- ❑ A certificate of a user A consists:
  - The name of the issuer CA *X*
  - His/her public key KU_A
  - The signature $Sig(KR_X, A, KU_A)$ by the CA *X*
  - The expiration date
  - Applications
    - ➢ Encryption / Signature

Certificate (c.1)



Alice:

(1) Generate $KU_{A,}$, KR_A

(2) Alice, KU_A, ID proof

CA *X*:

(3) Generate

Sig(KR_X, Alice, KU_A, T)

(4) Sig(KR_X, Alice, KU_A, T)

$\text{Cert}_{A,X}$=[Alice, KU_A, Sig(KR_X, Alice, KU_A)]

Note: CA does not know KR_A

Certificate (c.2)

❑ Guarantee of CA and certificate

- Guarantee the public key is of *someone*
- *Someone* is not guaranteed to be *safe*

❑ Security of transmitting DATA

- Transmit *session key* first
  - ➢ *Public crypto system*
- Transmit DATA by session key
  - ➢ *Symmetric crypto system*