System Administration HW4

- Web Server/Services

yoychen, blzhuang

Environment setup

You can choose one of following options

- Plan A: FreeBSD Server with Public IP
- Plan B: 使用 VirtualBox 開兩台 FreeBSD server (bsd1, bsd2)，兩台 VM 皆須設定兩個網卡 (NAT 及同一張 host-only network adapter)，bsd1 為安裝作業用機器，bsd2 為測試作業部份 spec 用機器
  - http://hadoopspark.blogspot.tw/2016/03/blog-post.html
  - https://askubuntu.com/questions/198452/no-host-only-adapter-selected

Requirements

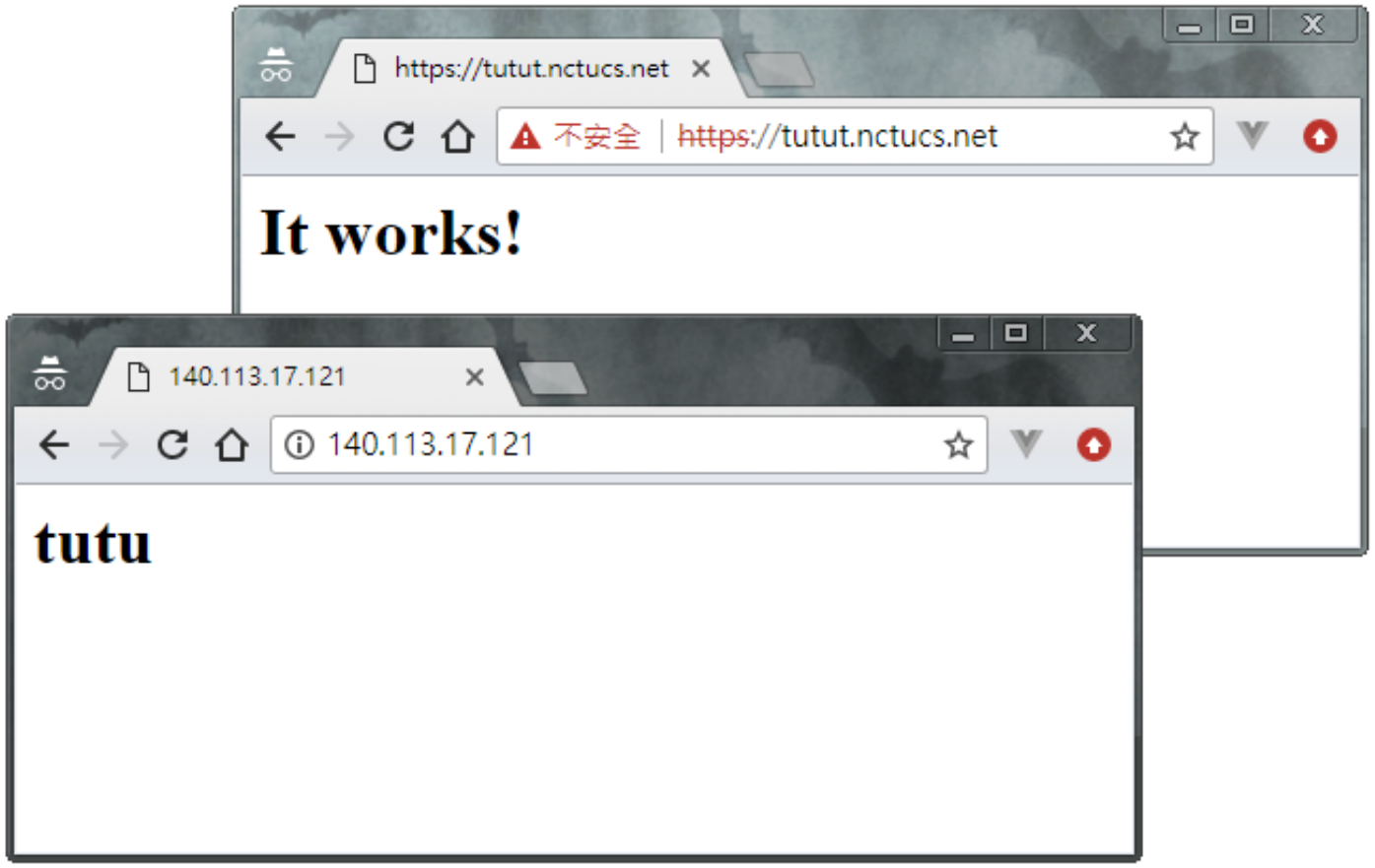
- Web Service
  - Virtual Host (5%)
  - Hide Server Token (5%)
  - HTTPS (30%)
  - Access Control / Rewrite (10%)
  - PHP (10%)
- Database
  - MySQL / MariaDB (10%)
- HTTP Application
  - phpMyAdmin (5%)
  - Wordpress (5%)
  - Basic PHP router (10%)
- DEMO (10%)

Apache

Apache - Virtual Host

- Setup a name-based virtual hosts in Apache.
- 使用 ip 和 Domain 瀏覽網站根目錄會看到不同內容 (5%)
- You can get domain names from:
  - https://www.nctucs.net/
    - https://nctu.me/
  - https://www.noip.com/

Apache - Virtual Host



Apache - Hide Server Token

- 瀏覽 php 網頁時，Response header 中不包含 php 相關資訊 (1%)
- 網站的 Response header 只顯示沒有版本的 Apache 資訊可以得到 (2%)，如果完全隱藏 Apache 資訊或是偽裝成其他 web service 的名字則得 (4%)

Apache - Hide Server Token

只顯示不帶版本號的 Apache 資訊，以及隱藏 php 相關資訊 (3%)

```
root@tutu:/usr/local/etc/apache24 # curl -Ik https://tutut.nctucs.net/phpinfo-0656000.php
HTTP/1.1 200 OK
Date: Mon, 27 Nov 2017 19:21:01 GMT
Server: Apache
Strict-Transport-Security: max-age=31536000;includeSubdomains; preload
Content-Type: text/html; charset=UTF-8
```

偽裝成其他 web service 資訊，以及隱藏 php 相關資訊 (5%)

```
root@tutu:/usr/local/etc/apache24 # curl -Ik https://tutut.nctucs.net/phpinfo-0656000.php
HTTP/1.1 200 OK
Date: Mon, 27 Nov 2017 19:22:46 GMT
Server: Microsoft-IIS/6.0
Strict-Transport-Security: max-age=31536000;includeSubdomains; preload
Content-Type: text/html; charset=UTF-8
```

Apache - HTTPS

使用 domain 瀏覽時

- ❑啟用 HTTPS (5%)
  - 可使用 self-signed certificate
  - 未啟用 HTTPS (-5%)
  - self-signed certificate 如果要使用 curl 做測試，記得加 -k 喔
- ❑HTTP auto redirect HTTPS (5%)
  - 未啟用 HTTPS 不給分
- ❑啟用 HSTS (10%)
  - 僅驗證 HTTPS 回傳的 header
- ❑所有 https 頁面皆啟用 HTTP/2 (10%)

Apache - HTTPS

啟用 https，如果是 self-signed certificate，顯示 `不安全` 是正常的

將 HTTP 自動導向 HTTPS

```
➜  ~ curl -IL --http2 http://sahw4-apache.bingluen.tw
HTTP/1.1 301 Moved Permanently
Date: Thu, 23 Nov 2017 19:24:02 GMT
Server: NCTU CSCC WEB Server
Location: https://sahw4-apache.bingluen.tw/
Content-Type: text/html; charset=iso-8859-1

HTTP/2 200
date: Thu, 23 Nov 2017 19:24:02 GMT
server: NCTU CSCC WEB Server
strict-transport-security: max-age=31536000;includeSubdomains; preload
last-modified: Thu, 23 Nov 2017 18:27:33 GMT
etag: "99-55eaa96ee58c6"
accept-ranges: bytes
content-length: 153
content-type: text/html
```

Apache - HTTPS

啟用 HTTP/2

```
➜  ~ curl -I --http2 https://sahw4-apache.bingluen.tw
HTTP/2 200
date: Thu, 23 Nov 2017 19:19:34 GMT
server: NCTU CSCC WEB Server
strict-transport-security: max-age=31536000;includeSubdomains; preload
last-modified: Thu, 23 Nov 2017 18:27:33 GMT
etag: "99-55eaa96ee58c6"
accept-ranges: bytes
content-length: 153
content-type: text/html
```

開啟 HSTS

```
➜  ~ curl -I --http2 https://sahw4-apache.bingluen.tw
HTTP/2 200
date: Thu, 23 Nov 2017 19:19:34 GMT
server: NCTU CSCC WEB Server
strict-transport-security: max-age=31536000;includeSubdomains; preload
last-modified: Thu, 23 Nov 2017 18:27:33 GMT
etag: "99-55eaa96ee58c6"
accept-ranges: bytes
content-length: 153
content-type: text/html
```

Apache - Access Control

使用 ip 瀏覽網頁時

如果您的環境是 Plan A:

❑僅 140.113.235.0/24 可瀏覽 http://{your apache server ip} (回傳200)、其他 IP (包含 localhost) 禁止瀏覽 (請回傳 403) (5%)

- 可以登入 linux1~6, bsd1~6 來測試

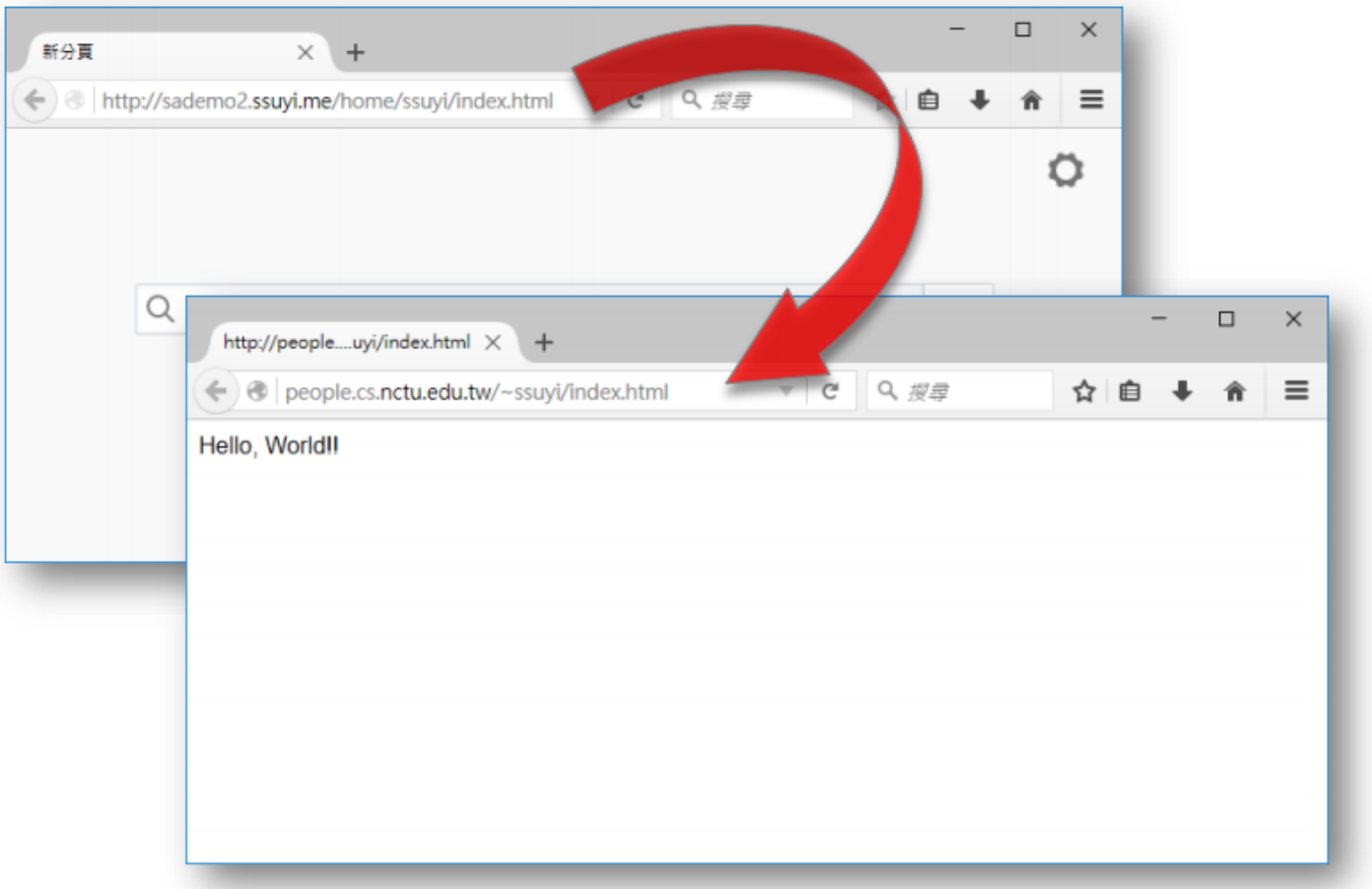
如果您的環境是 Plan B:

❑僅 bsd2 的 ip 可瀏覽 http://{your apache server ip} (回傳200)、其他 IP (包含 localhost) 禁止瀏覽 (請回傳 403) (5%)

- 可以使用 curl 做測試

Apache - Rewrite

- 瀏覽 https://{your domain}/home/[a-zA-Z0-9]+/.* 會轉址到 http://people.cs.nctu.edu.tw/~[a-zA-Z0-9]+/.* (5%)



Apache - PHP 7

- PHP 版本為 7 以上 (5%)
- 瀏覽 https://{your domain}/phpinfo-{your student ID number}.php，會顯示 php info 頁面 (5%)

Apache - PHP 7

php info 頁面，php 安裝版本為 7.1

System	FreeBSD tutu.cs.nctu.edu.tw 11.1-RELEASE FreeBSD 11.1-RELEASE #0 r321309: Fri Jul 21 02:08:28 UTC 2017 root@releng2.nyi.freebsd.org:/usr/obj/usr/src/sys/GENERIC amd64
Build Date	Nov 17 2017 07:06:25
Configure Command	'./configure' '--with-layout=GNU' '--localstatedir=/var' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--enable-mysqlnd' '--with-libxml-dir=/usr/local' '--with-pcre-regex=/usr/local' '--program-prefix=' '--disable-cli' '--disable-cgi' '--with-apxs2=/usr/local/sbin/apxs' '--enable-dtrace' '--prefix=/usr/local' '--mandir=/usr/local/man' '--infodir=/usr/local/info/' '--build=amd64-portbld-freebsd11.0' 'build_alias=amd64-portbld-freebsd11.0' 'CFLAGS=-O2 -pipe -fstack-protector -fno-strict-aliasing' 'CPPFLAGS=' 'CPP=cpp'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc

Database

Database

- MySQL/MariaDB 擇一
- 限制 root 僅本機可以登入 (5%)

如果您的環境是 Plan A:

- 建立 user sysadm-ta，密碼為 {your student ID}，並限制只有 140.113.235.0/24 可連線 (5%)
  - 此 User 僅能存取 sysadm 資料庫
  - 此 User 可以對 sysadm 進行 INSERT, SELECT, UPDATE, CREATE

如果您的環境是 Plan B:

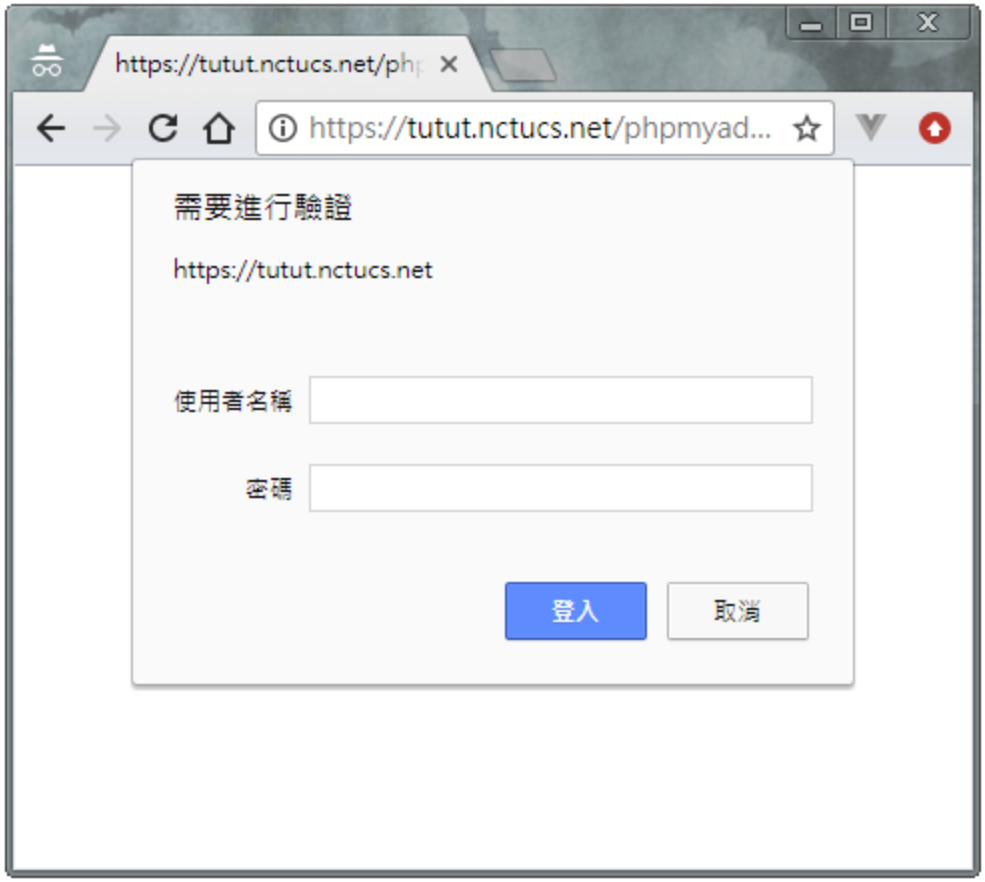
- 建立 user sysadm-ta，密碼為 {your student ID}，並限制只有 bsd2 的 ip 可連線 (5%)
  - 此 User 僅能存取 sysadm 資料庫
  - 此 User 可以對 sysadm 進行 INSERT, SELECT, UPDATE, CREATE

HTTP Application

phpMyAdmin

- 存取位置必須為 https://{your domain}/phpmyadmin-{your student ID number} 若非該位置 phpMyAdmin 部份不計分
- 啟用 Access Control (5%)
  - Plan A: 140.113.235.0/24 可直接看到 phpmyadmin 登入畫面
  - Plan B: bsd2 的 ip 可直接看到 phpmyadmin 登入畫面
  - 其他位置需要經過 Basic Auth 認證才能看到 phpmyadmin 登入畫面
    - Basic Auth Username: Sysadm
    - Basic Auth Password: {your student ID number}

phpMyAdmin


https://tutut.nctucs.net/ph
https://tutut.nctucs.net/phpmyad...
需要進行驗證
https://tutut.nctucs.net
使用者名稱
密碼
登入
取消

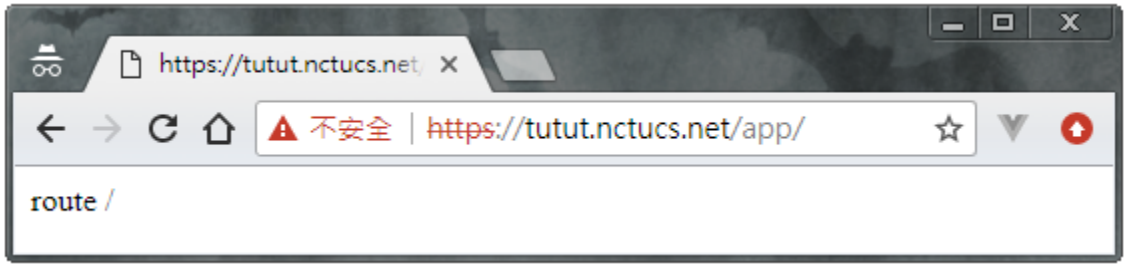
Wordpress

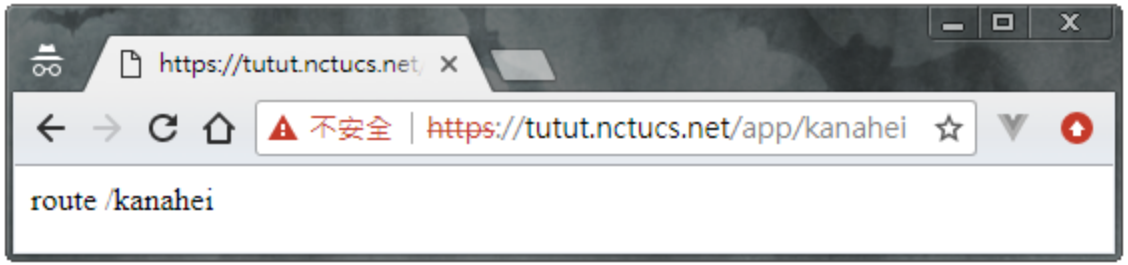
- 存取位置為 https://{your domain}/wordpress-{your student ID number}
- 可以閱覽、新增、刪除、修改文章 (5%)

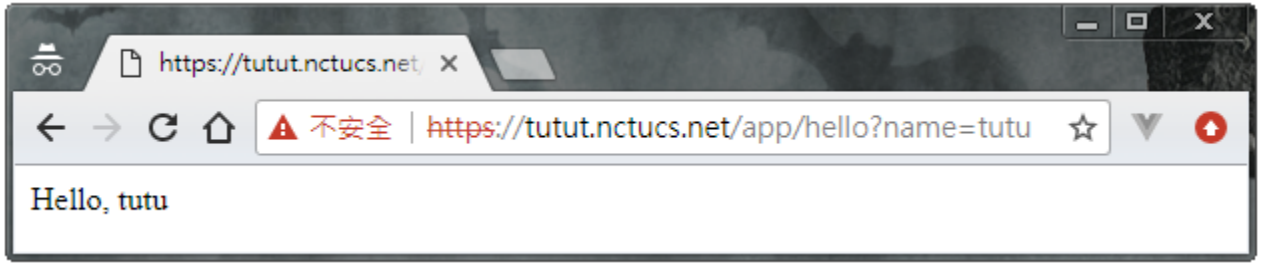
Basic PHP router

- 於網站根目錄建立資料夾 app，裡面只能有一個檔案，檔名為 index.php，請調整 apache 設定及撰寫 index.php，來達到以下三個要求 (10%)
  - 瀏覽 https://{your domain}/app/，回傳網頁內容 route /
  - 瀏覽 https://{your domain}/app/{string}，回傳網頁內容 route /{string}
  - 瀏覽 https://{your domain}/app/hello?name={string}，回傳網頁內容 Hello, {string}

Apache - PHP 7


https://tutut.nctucs.net
不安全
https://tutut.nctucs.net/app/
route /


https://tutut.nctucs.net
不安全
https://tutut.nctucs.net/app/kanahei
route /kanahei


https://tutut.nctucs.net
不安全
https://tutut.nctucs.net/app/hello?name=tutu
Hello, tutu

Demo (10%)

- 隨機抽作業中幾項服務，請解釋如何設定及原理

Bonus

- 憑證使用 let's encrypt 或其他合格第三方憑證簽發 (5%)
- 通過 SSL Lab 獲得 A+ (10%)

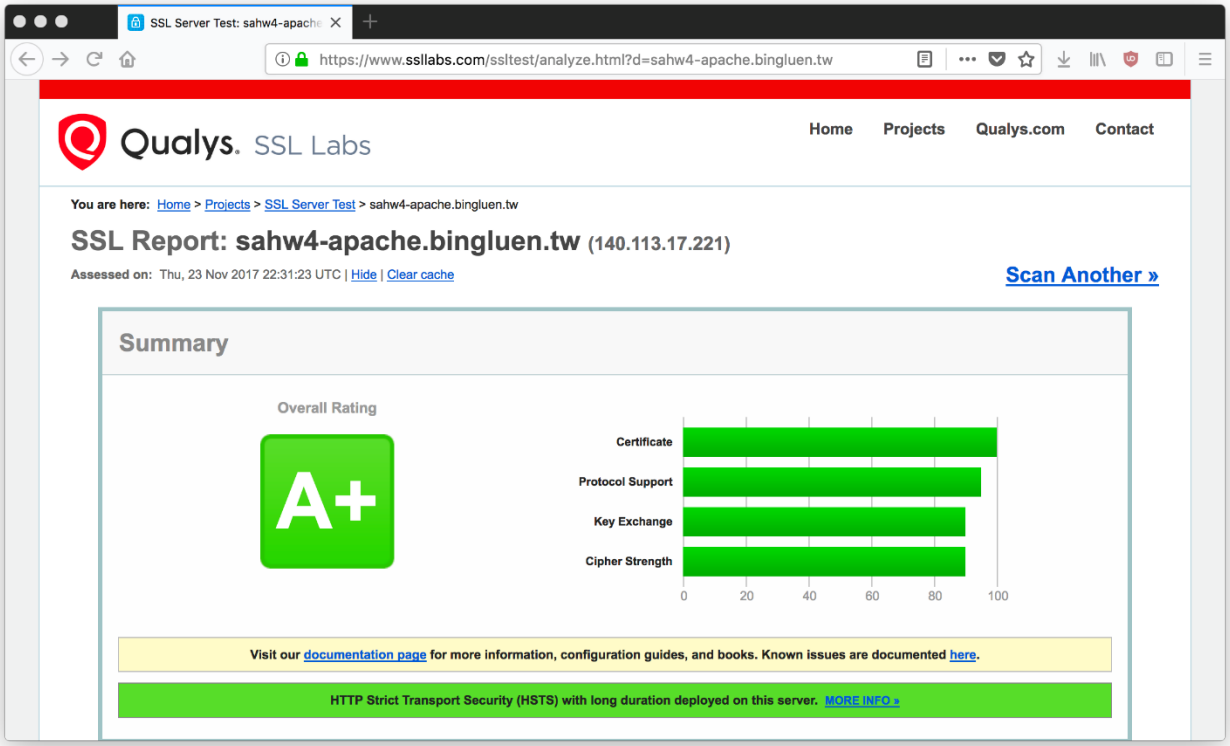
Bonus

採用 let's encrypt 或 其它合格憑證頒發機構簽發之憑證

StartCom、沃通以及其旗下憑證機構不屬於合格憑證頒發機構

Bonus

通過 SSL Lab 測試 https://www.ssllabs.com/ 獲得 A+ 評等



Deadline

- 2017/12/13 23:59
- You do not need to submit anything

How to hand in

- DEMO 2017/12/14 (四) 18:30 ~ 22:30
  - 如果當天無法來，最晚於 2017/12/10 23:59 前寄信說明並提出 DEMO 日期之前可以來提早 DEMO 的時段
  - 如沒有特殊原因 (病假需要提出相關證明)，不開放補 DEMO

Help

- Email ta@nasa.cs.nctu.edu.tw
- Goto CSCC to ask professional 3F!