System Administration Homework 4 – Web Server

austin

Environments

❑ HTTP Server

- NGINX and Apache are both allowed
- PHP-FPM and PHP are both allowed
- The TA has only tested all specs on NGINX+PHP-FPM currently
- The content of pages that should display messages should satisfy:
  - Can be distinguished by eyes
  - Contain your Student ID

Environments

- ❑ Networks
  - Intranet: Only one host other than your machine can access, which can be one of:
    - ➢ A VM with a host-only adapter connecting to the same network of the original machine
    - ➢ The host OS connecting to the machine using host-only adapter
    - ➢ One machine that is connected to your own private network
    - ➢ 140.113.235.0/24 (If you have a public IP)
  - Public: The addresses that can be accessed from either:
    - ➢ The whole world: An public IP
    - ➢ The Wireguard VPN (10.113.0.0/16)

Outline

❑ HTTP Server
- Virtual Host (5%)
- Access Control (5%)
- Hiding server information (5%)
- HTTPS (20%)
- PHP (5%)

❑ MySQL
- Preparation for Nextcloud (10%)

❑ HTTP Application
- Basic app router (10%)
- WebSocket Handling (10%)
- Nextcloud (10%)
- Personal webpage (10%)

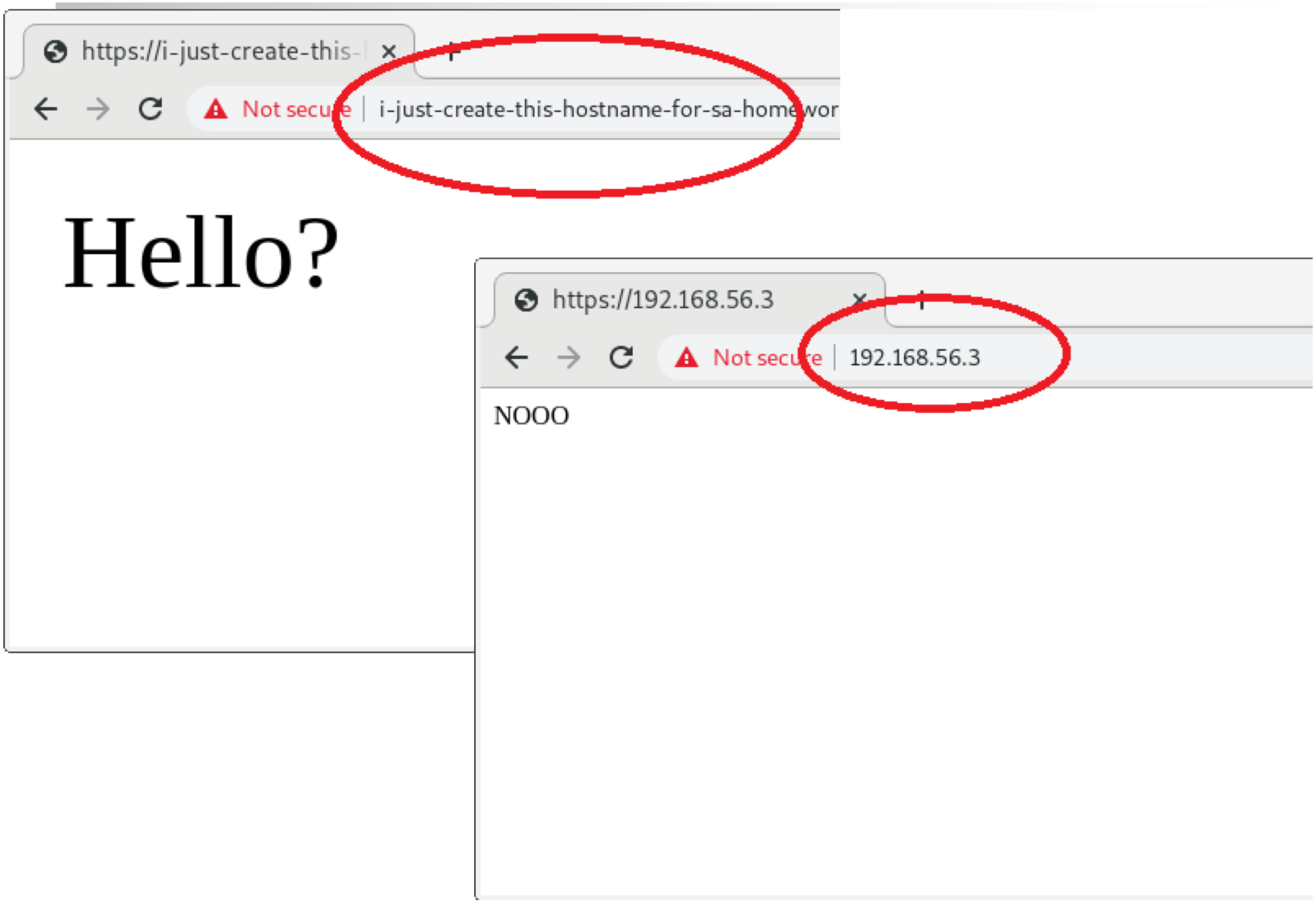
❑ DEMO (10%)

HTTP Server

Virtual Host

- ❑ Setup a name-based virtual host
- ❑ Show different content when connecting using domain name/IP (5%)
- ❑ You can get a domain name from:
  - https://www.nctu.me
  - https://www.noip.com

Virtual Host



https://i-just-create-this-

Not secure | i-just-create-this-hostname-for-sa-homewor

Hello?

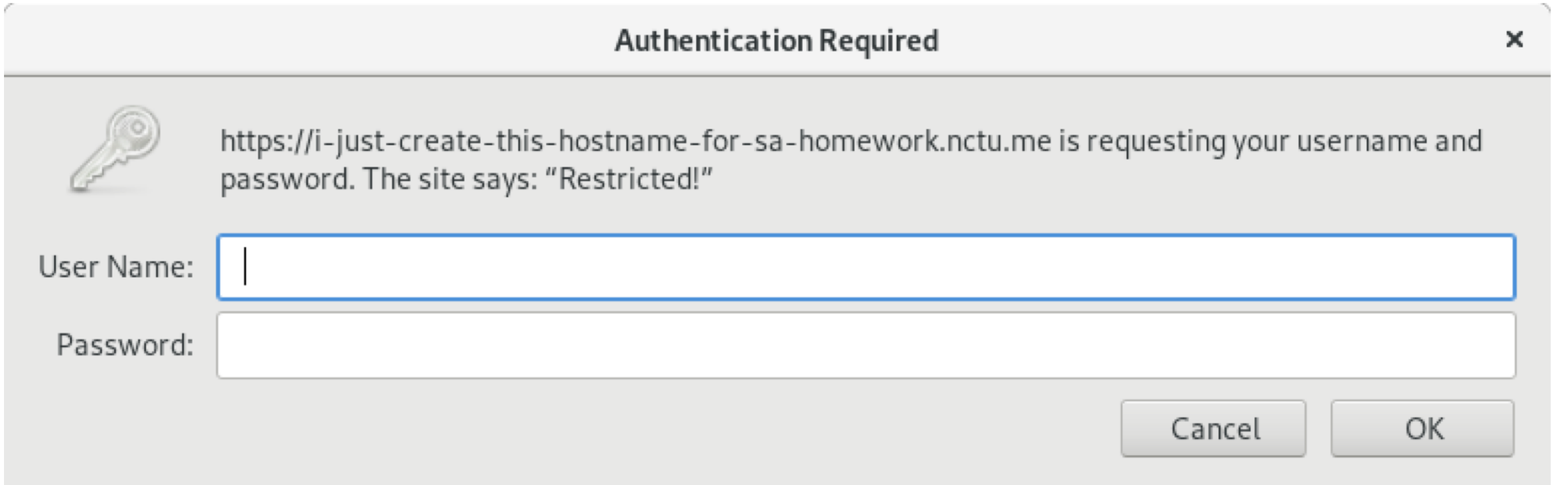
https://192.168.56.3

Not secure | 192.168.56.3

NOOO

Access Control

- ❑ Place a webpage on https://{your-intranet-IP}/private
- ❑ When accessing from intranet, it must show after passing Basic Auth authentication with username `admin` and password `{your-student-ID}` (3%)
- ❑ Access from public network should be denied (return 403) (2%)



Authentication Required

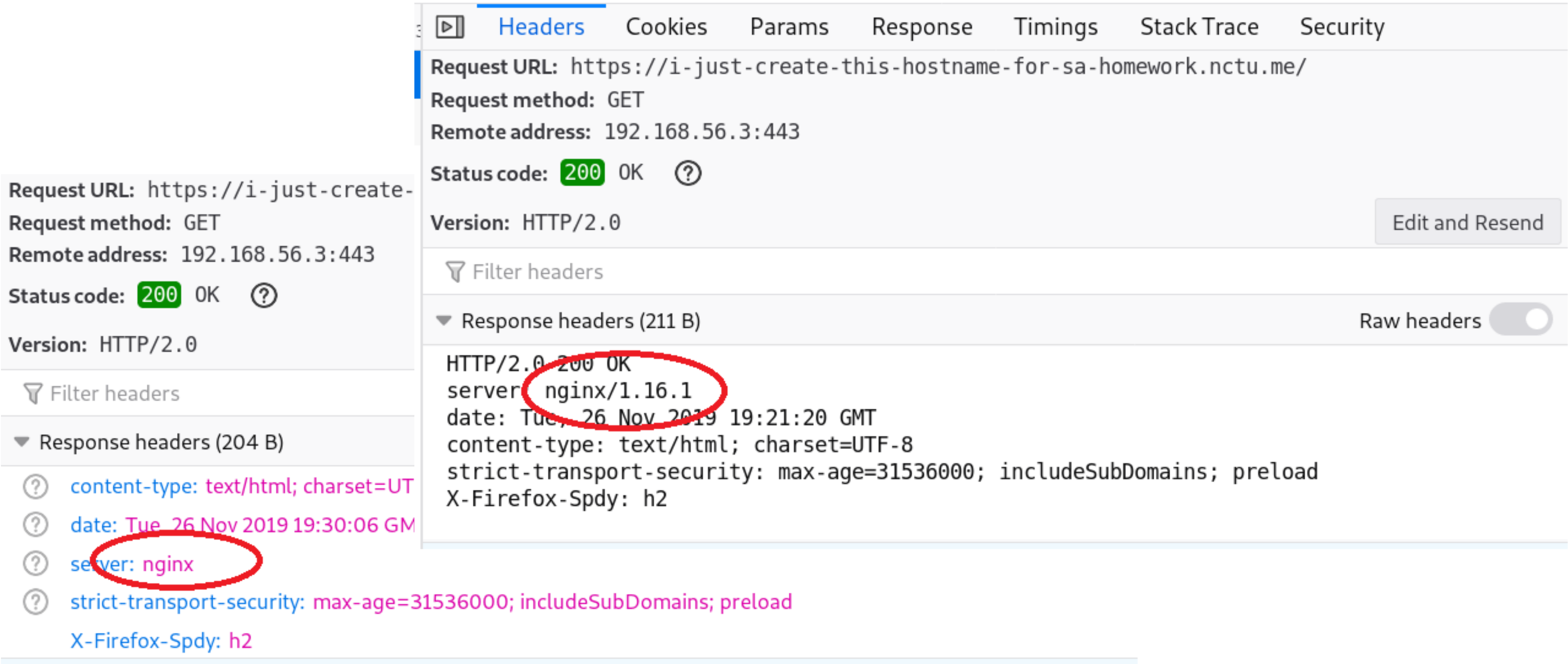
https://i-just-create-this-hostname-for-sa-homework.nctu.me is requesting your username and password. The site says: "Restricted!"

User Name:

Password:

Hiding Server Information

- ❑ Hide NGINX/Apache version in header (5%)



Request URL: https://i-just-create-this-hostname-for-sa-homework.nctu.me/
Request method: GET
Remote address: 192.168.56.3:443
Status code: 200 OK
Version: HTTP/2.0

Response headers (211 B)

```
HTTP/2.0 200 OK
server: nginx/1.16.1
date: Tue, 26 Nov 2019 19:21:20 GMT
content-type: text/html; charset=UTF-8
strict-transport-security: max-age=31536000; includeSubDomains; preload
X-Firefox-Spdy: h2
```

Request URL: https://i-just-create-
Request method: GET
Remote address: 192.168.56.3:443
Status code: 200 OK
Version: HTTP/2.0

Response headers (204 B)

```
content-type: text/html; charset=UT
date: Tue, 26 Nov 2019 19:30:06 GM
server: nginx
strict-transport-security: max-age=31536000; includeSubDomains; preload
X-Firefox-Spdy: h2
```

HTTPS

❑ Enable HTTPS (5%)

- Self-signed certificate is allowed
- Supply `–k` option when testing with `curl`

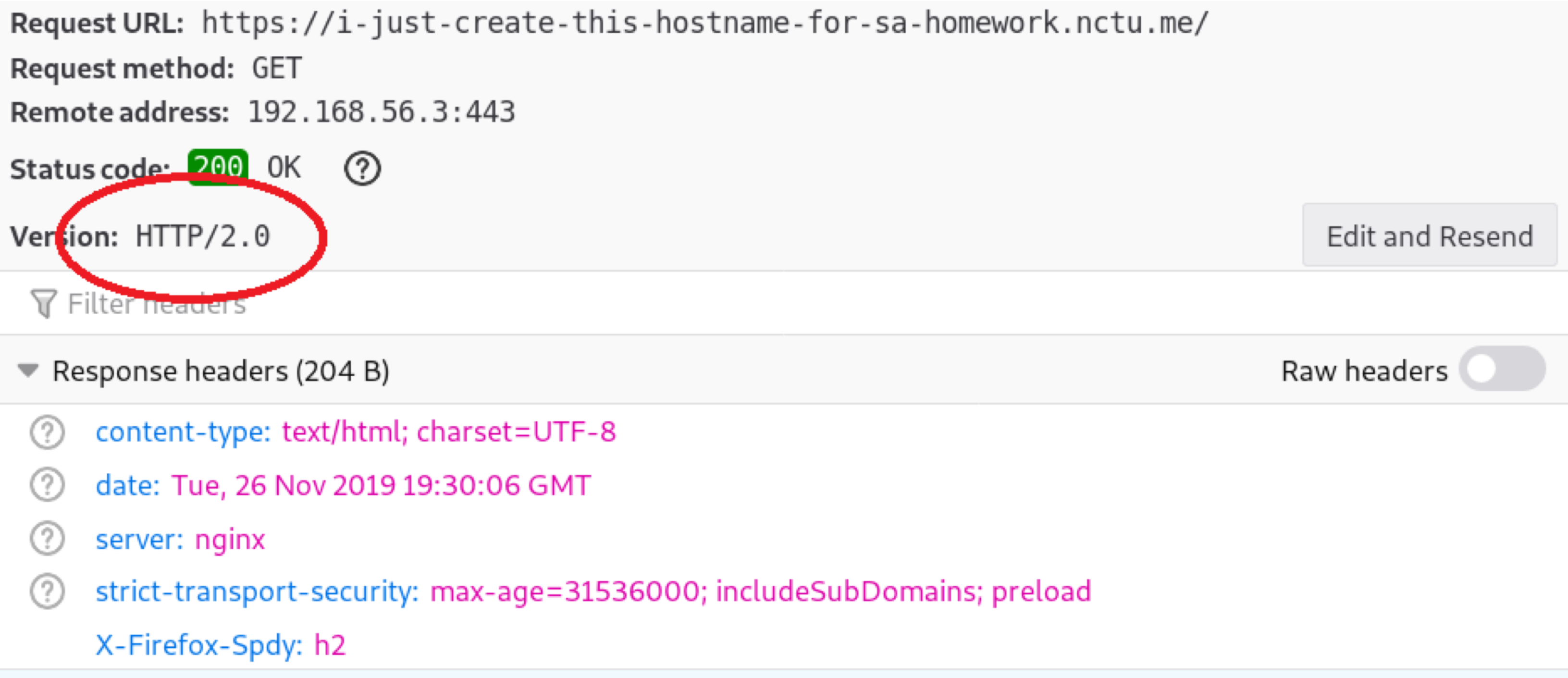
❑ Redirect to HTTPS automatically when attempting to connect to HTTP (5%)

❑ Enable HSTS (5%)

❑ Enable HTTP2 on pages connected with HTTPS (5%)

- Can be tested with `curl --http2`
- Ensure that the server only provides ciphers not ‘blacklisted’ by http2

HTTPS



Request URL: https://i-just-create-this-hostname-for-sa-homework.nctu.me/

Request method: GET

Remote address: 192.168.56.3:443

Status code: 200 OK

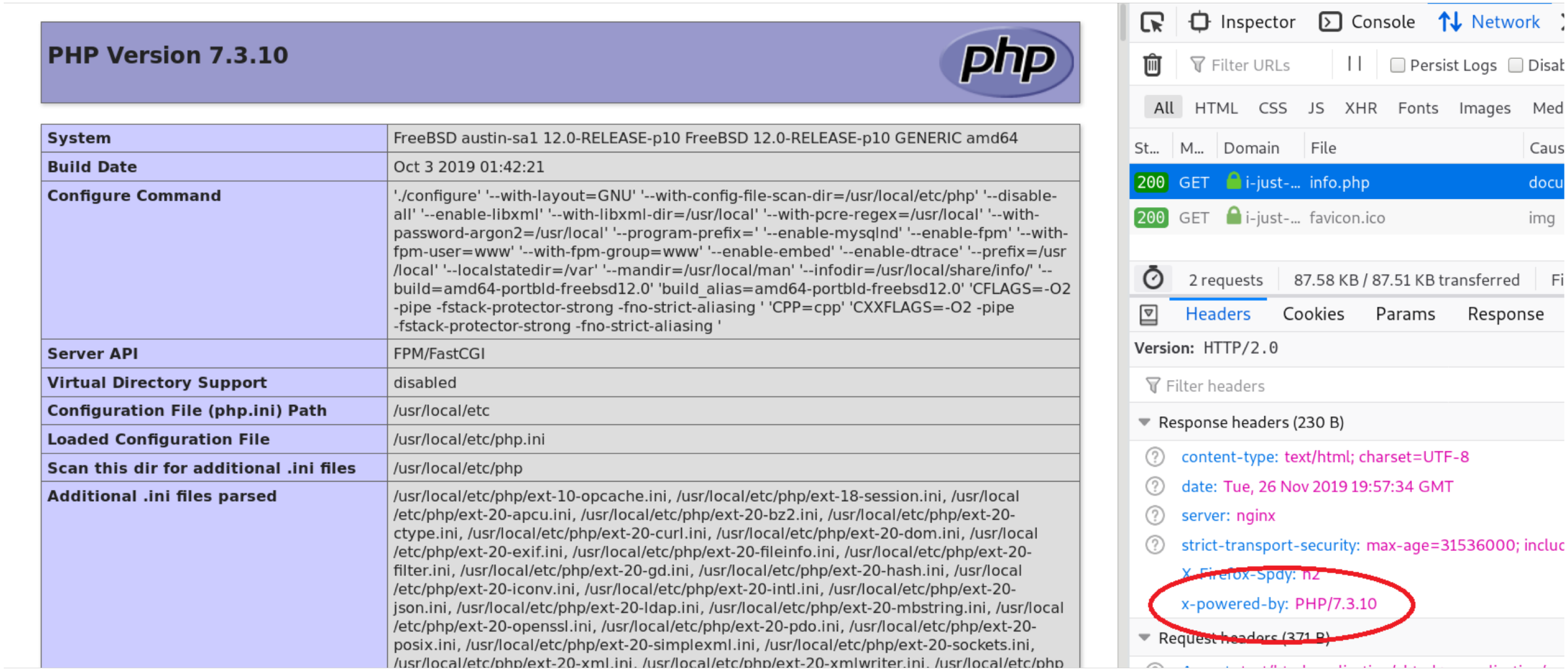
Version: HTTP/2.0

Response headers (204 B)

```
content-type: text/html; charset=UTF-8
date: Tue, 26 Nov 2019 19:30:06 GMT
server: nginx
strict-transport-security: max-age=31536000; includeSubDomains; preload
X-Firefox-Spdy: h2
```

PHP/PHP-FPM

- ❑ Set up PHP such that access to `https://{your-domain}/info-{your-student-ID}.php` gives response of `phpinfo()` (3%)
- ❑ Hide PHP version information in header (2%)
- ❑ Use PHP7 or higher, or you won’t get the points for this part



PHP Version 7.3.10

System	FreeBSD austin-sa1 12.0-RELEASE-p10 FreeBSD 12.0-RELEASE-p10 GENERIC amd64
Build Date	Oct 3 2019 01:42:21
Configure Command	'./configure' '--with-layout=GNU' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--with-libxml-dir=/usr/local' '--with-pcre-regex=/usr/local' '--with-password-argon2=/usr/local' '--program-prefix=' '--enable-mysqlnd' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--enable-embed' '--enable-dtrace' '--prefix=/usr/local' '--localstatedir=/var' '--mandir=/usr/local/man' '--infodir=/usr/local/share/info/' '--build=amd64-portbld-freebsd12.0' 'build_alias=amd64-portbld-freebsd12.0' 'CFLAGS=-O2 -pipe -fstack-protector-strong -fno-strict-aliasing ' 'CPP=cpp' 'CXXFLAGS=-O2 -pipe -fstack-protector-strong -fno-strict-aliasing '
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc
Loaded Configuration File	/usr/local/etc/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php
Additional .ini files parsed	/usr/local/etc/php/ext-10-opcache.ini, /usr/local/etc/php/ext-18-session.ini, /usr/local/etc/php/ext-20-apcu.ini, /usr/local/etc/php/ext-20-bz2.ini, /usr/local/etc/php/ext-20-ctype.ini, /usr/local/etc/php/ext-20-curl.ini, /usr/local/etc/php/ext-20-dom.ini, /usr/local/etc/php/ext-20-exif.ini, /usr/local/etc/php/ext-20-fileinfo.ini, /usr/local/etc/php/ext-20-filter.ini, /usr/local/etc/php/ext-20-gd.ini, /usr/local/etc/php/ext-20-hash.ini, /usr/local/etc/php/ext-20-iconv.ini, /usr/local/etc/php/ext-20-intl.ini, /usr/local/etc/php/ext-20-json.ini, /usr/local/etc/php/ext-20-ldap.ini, /usr/local/etc/php/ext-20-mbstring.ini, /usr/local/etc/php/ext-20-openssl.ini, /usr/local/etc/php/ext-20-pdo.ini, /usr/local/etc/php/ext-20-posix.ini, /usr/local/etc/php/ext-20-simplexml.ini, /usr/local/etc/php/ext-20-sockets.ini, /usr/local/etc/php/ext-20-xml.ini, /usr/local/etc/php/ext-20-xmlwriter.ini, /usr/local/etc/php

St...	M...	Domain	File	Caus
200	GET	i-just-...	info.php	docu
200	GET	i-just-...	favicon.ico	img

2 requests 87.58 KB / 87.51 KB transferred Fi

Version: HTTP/2.0

Response headers (230 B)

```
content-type: text/html; charset=UTF-8
date: Tue, 26 Nov 2019 19:57:34 GMT
server: nginx
strict-transport-security: max-age=31536000; incluc
X-Firefox-Spdy: h2
x-powered-by: PHP/7.3.10
```

Request headers (371 B)

MySQL

MySQL: Prepare for Nextcloud

- ❑ Set the transaction isolation levels to READ-COMMITED (3%)
- ❑ Bonus: Explain what this and other isolation levels mean (+5%)
- ❑ Create a MySQL user named 'nc' and a database named 'nextcloud', which satisfies:
  - The password of the user is your student ID (3%)
  - This user can only login from localhost (2%)
  - This user only have full privileges on database 'nextcloud' (2%)

HTTP Applications

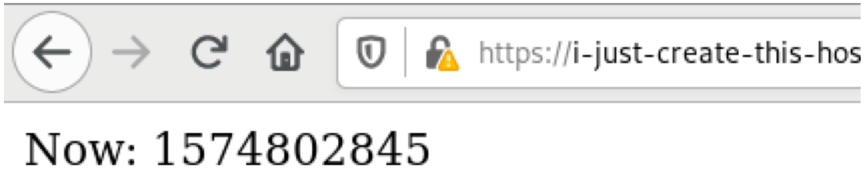
Basic App Router

- ❑ You can have only one file `index.php` in the root at the path https://{your-domain}/app , then rewrite all the request under this path to this file(You need to write php script)
- ❑ There are three path displaying different contents:
  - https://{your-domain}/app
    - ➢ Display `route: /`
  - https://{your-domain}/app/{A}+{B} (A, B are integers)
    - ➢ Display `result: {value of A+B}`
  - https://{your-domain}/app?name={string}
    - ➢ Display `Hello, {string}`
- ❑ (10%)

WebSocket

❑ A sample program:

- https://medium.com/@cn007b/super-simple-php-websocket-example-ea2cd5893575
- This program crashes at client refresh, so just use it for test or demo
- You can use other WebSocket program you want



https://i-just-create-this-hos

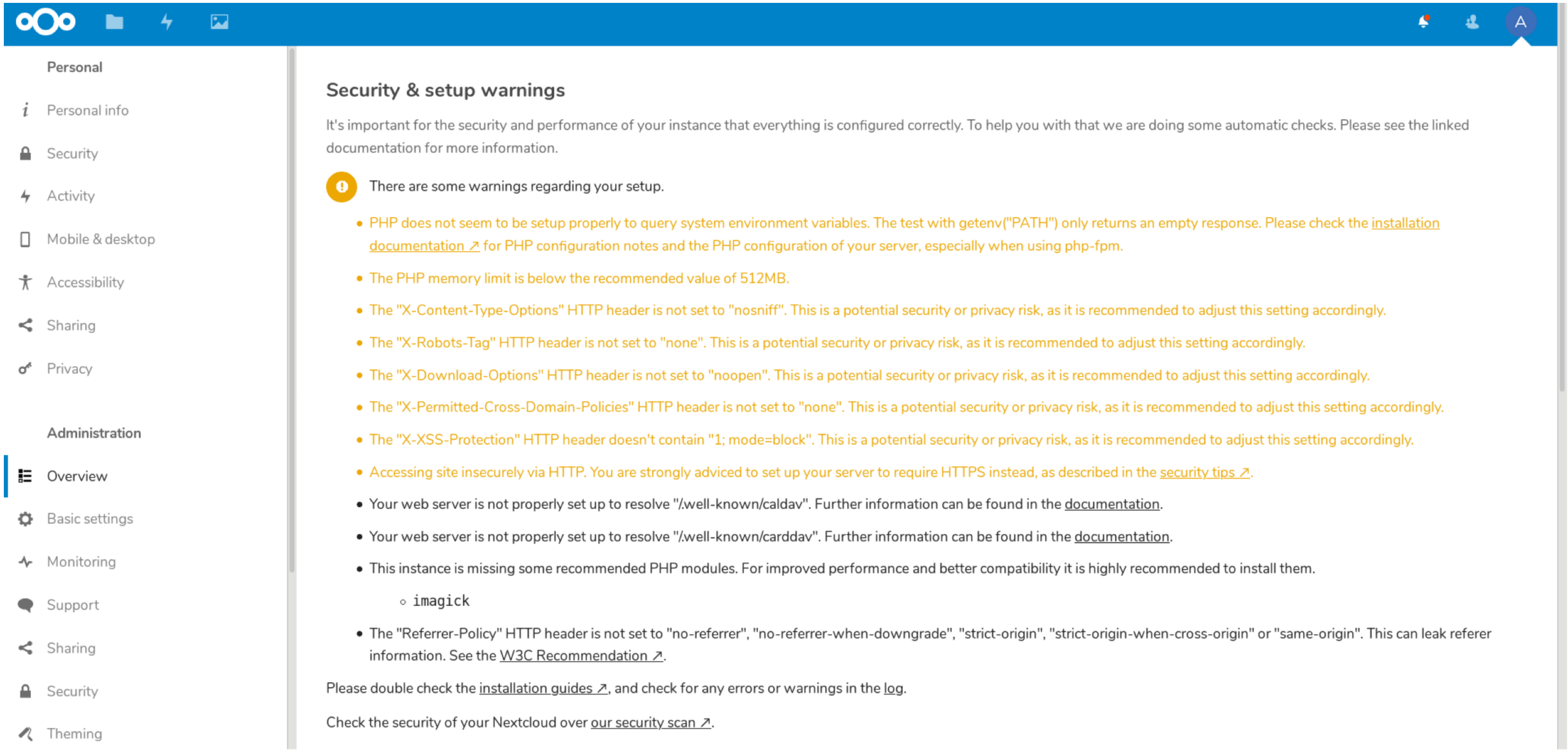
Now: 1574802845

WebSocket

- ❑ You don’t need to support HTTP2 for WebSocket connection
- ❑ You can use HTTP for this path if you cannot make it connected on port 443
- ❑ Configure your HTTP server such the program run appropriately that when accessing http(s)://{your-domain}/wsdemo
  - Connect WebSocket on port other than 80, 443 (ws://) (3%)
  - Connect WebSocket on port 80 (ws://) (+3%)
  - Connect WebSocket on port 443 (wss://) (+4%)

Nextcloud

- You can either install by pkg (v16) or download the latest version (v17)
- Install on path https://{your-domain}/nextcloud
- Use the database and user created in MySQL part
- (10%)
- Bonus: Fix all the warnings in Settings/Overview page (10%)



Security & setup warnings

It's important for the security and performance of your instance that everything is configured correctly. To help you with that we are doing some automatic checks. Please see the linked documentation for more information.

There are some warnings regarding your setup.

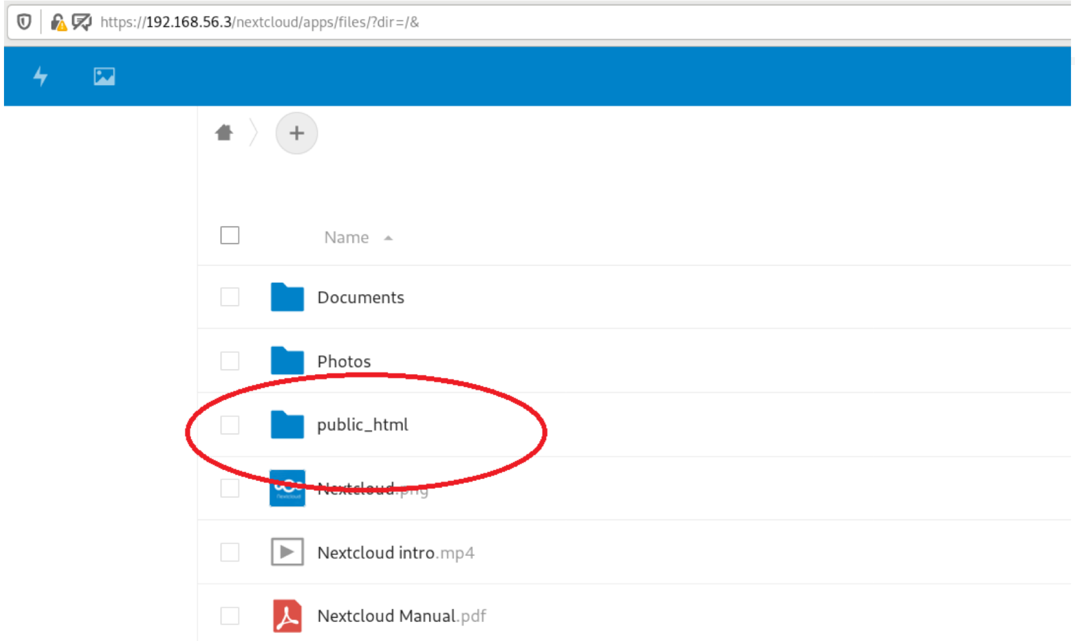
- PHP does not seem to be setup properly to query system environment variables. The test with getenv("PATH") only returns an empty response. Please check the installation documentation ↗ for PHP configuration notes and the PHP configuration of your server, especially when using php-fpm.
- The PHP memory limit is below the recommended value of 512MB.
- The "X-Content-Type-Options" HTTP header is not set to "nosniff". This is a potential security or privacy risk, as it is recommended to adjust this setting accordingly.
- The "X-Robots-Tag" HTTP header is not set to "none". This is a potential security or privacy risk, as it is recommended to adjust this setting accordingly.
- The "X-Download-Options" HTTP header is not set to "noopen". This is a potential security or privacy risk, as it is recommended to adjust this setting accordingly.
- The "X-Permitted-Cross-Domain-Policies" HTTP header is not set to "none". This is a potential security or privacy risk, as it is recommended to adjust this setting accordingly.
- The "X-XSS-Protection" HTTP header doesn't contain "1; mode=block". This is a potential security or privacy risk, as it is recommended to adjust this setting accordingly.
- Accessing site insecurely via HTTP. You are strongly adviced to set up your server to require HTTPS instead, as described in the security tips ↗.
- Your web server is not properly set up to resolve "/.well-known/caldav". Further information can be found in the documentation.
- Your web server is not properly set up to resolve "/.well-known/carddav". Further information can be found in the documentation.
- This instance is missing some recommended PHP modules. For improved performance and better compatibility it is highly recommended to install them.
    - `imagick`
- The "Referrer-Policy" HTTP header is not set to "no-referrer", "no-referrer-when-downgrade", "strict-origin", "strict-origin-when-cross-origin" or "same-origin". This can leak referer information. See the W3C Recommendation ↗.

Please double check the installation guides ↗, and check for any errors or warnings in the log.

Check the security of your Nextcloud over our security scan ↗.

Personal Webpage

- ❑ Each user in Nextcloud can put static(PHP is not needed) contents(img, html, css, js, etc.) in the `public_html` directory under their home
- ❑ When accessing https://{your-domain}/sites/~{username}/ , it should show whatever {username} put in his `public_html`, with index `index.html`
- ❑ (10%)



https://192.168.56.3/nextcloud/apps/files/?dir=/&

□ Name

□ Documents

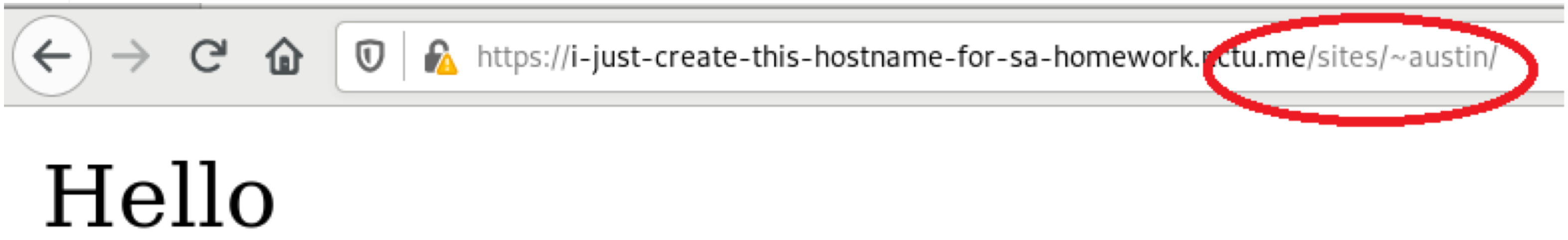
□ Photos

□ public_html

□ Nextcloud.png

□ Nextcloud intro.mp4

□ Nextcloud Manual.pdf



https://i-just-create-this-hostname-for-sa-homework.nctu.me/sites/~austin/

Hello

Deadline

- 2019/12/19
- You do not need to submit anything

Help!

- Email to ta@nasa.cs.nctu.edu.tw
- New E3 https://e3new.nctu.edu.tw/
- Office hour: 3GH at EC318