Homework 4
Web Services

tcyuan yiyuchang

交大資工系資訊中心

Computer Center of Department of Computer Science, NCTU

Outline

- HTTP Server (50%)
  - Virtual Hosts (5%)
  - Access Control (5%)
  - HTTPS & HTTP2 (20%)
  - Hiding Server Information (5%)
  - Harden and Secure Web Server (10%)
  - PHP / PHP-FPM (5%)
- Database (10%)
  - MySQL for Wordpress (10%)
- HTTP Application (40%)
  - Basic App Route (15%)
  - Websocket (15%)
  - WordPress (10%)

HTTP Server

Virtual Host (5%)

- Setup a name-based virtual host
- Show different contents based on different incoming donaim / IP
  - Your Domain Name: {ID}.nctu.cs
  - Your IP: 10.113.0.{ID}
    - {ID} is your wireguard ID

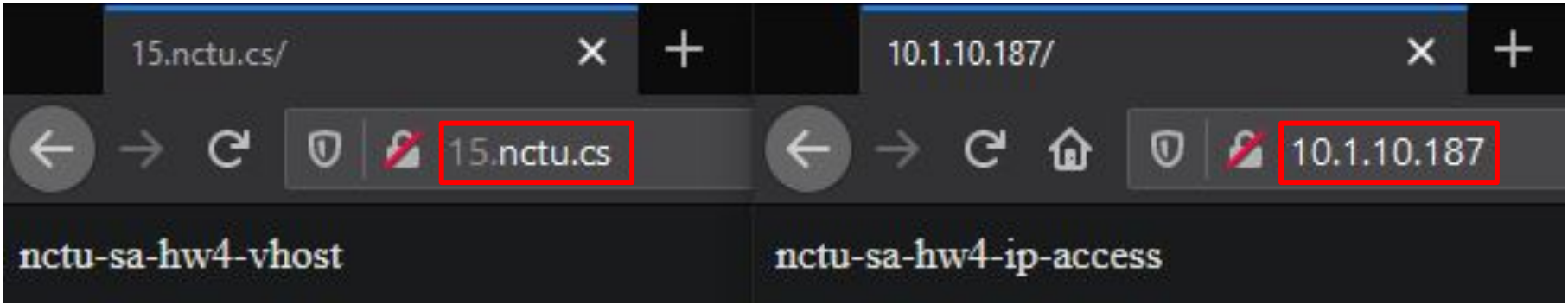
Hint:

You can use hosts file to map ip to your domain

On FreeBSD: /etc/hosts

On Windows: C:\Windows\System32\drivers\etc\hosts

Virtual Host (5%) (Cont'd)

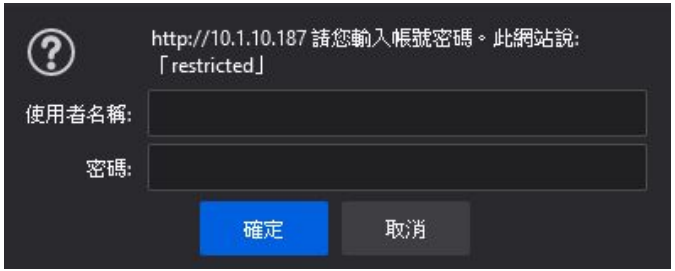


We will judge your work by 10.113.0.{ID} and {ID}.nctu.cs
Be sure to adjust your configurations accordingly

Access Control (5%)

- There is a secret webpage on http://10.113.0.{ID}/private
  - Deny access with domain. Only allow ip connection.
- When the webpage is accessed from 10.113.0.254, the user is asked to enter credentials
  - Username: admin
  - Password: Your {IP} without dots. e.g. 10113015
- When the webpage is accessed from any other location or accessed with domain:
  - 403 Forbidden or 404 Not Found
  - EVEN from the localhost, your'll have to return 403 or 404

Access Control (5%) (Cont'd)



ATTENTION

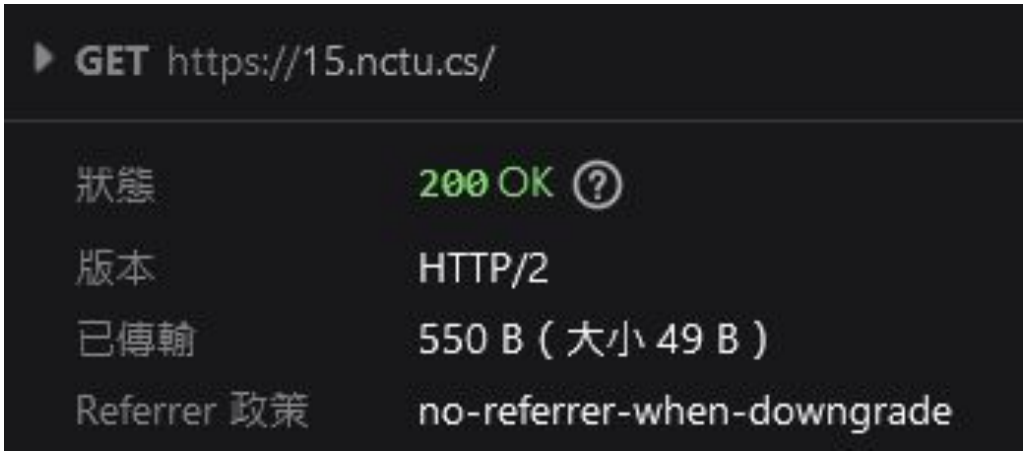
- We will judge everything starting from this page with your domain
- Please make sure you have adjusted your configurations

HTTPS (20%)

- Enable HTTPS (8%)
  - Please sign your own certificate on your domain
- Redirect all HTTP requests to HTTPS (2%)
- Enable HSTS (HTTP Strict Transport Security) (5%)

HTTPS (20%) (Cont'd)

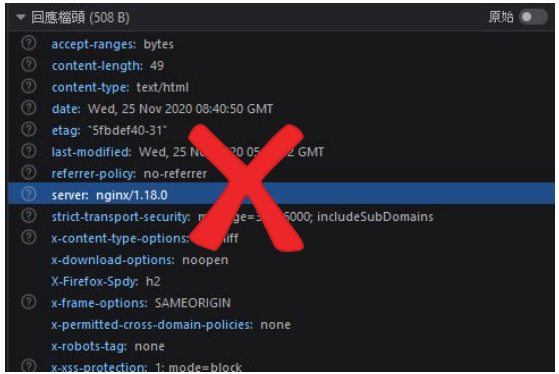
- Enable HTTP2 with HTTPS (5%)
  - Ensure that the server only provides ciphers not 'blacklisted' by http2

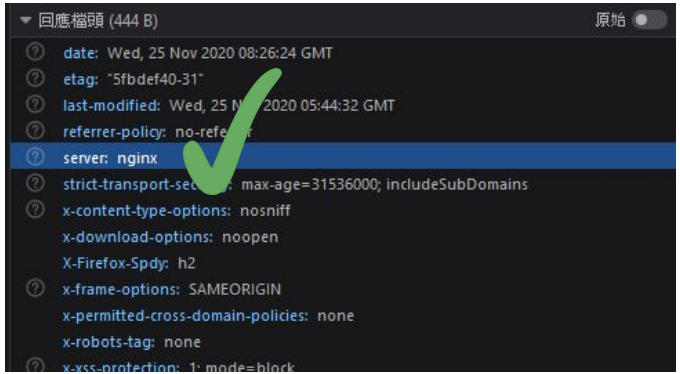


Hint: Using curl to test http2 requires special configurations

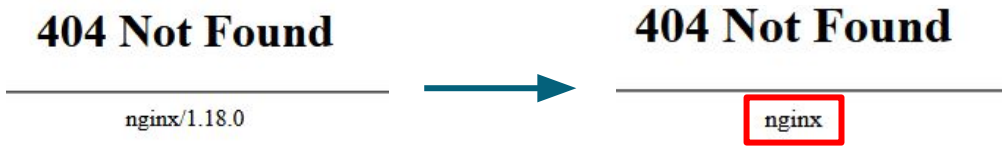
Hiding Server Information (5%)

- Hide NGINX/Apache version in header





- Do not show server version when there is an error



Harden and Secure Web Server (10%)

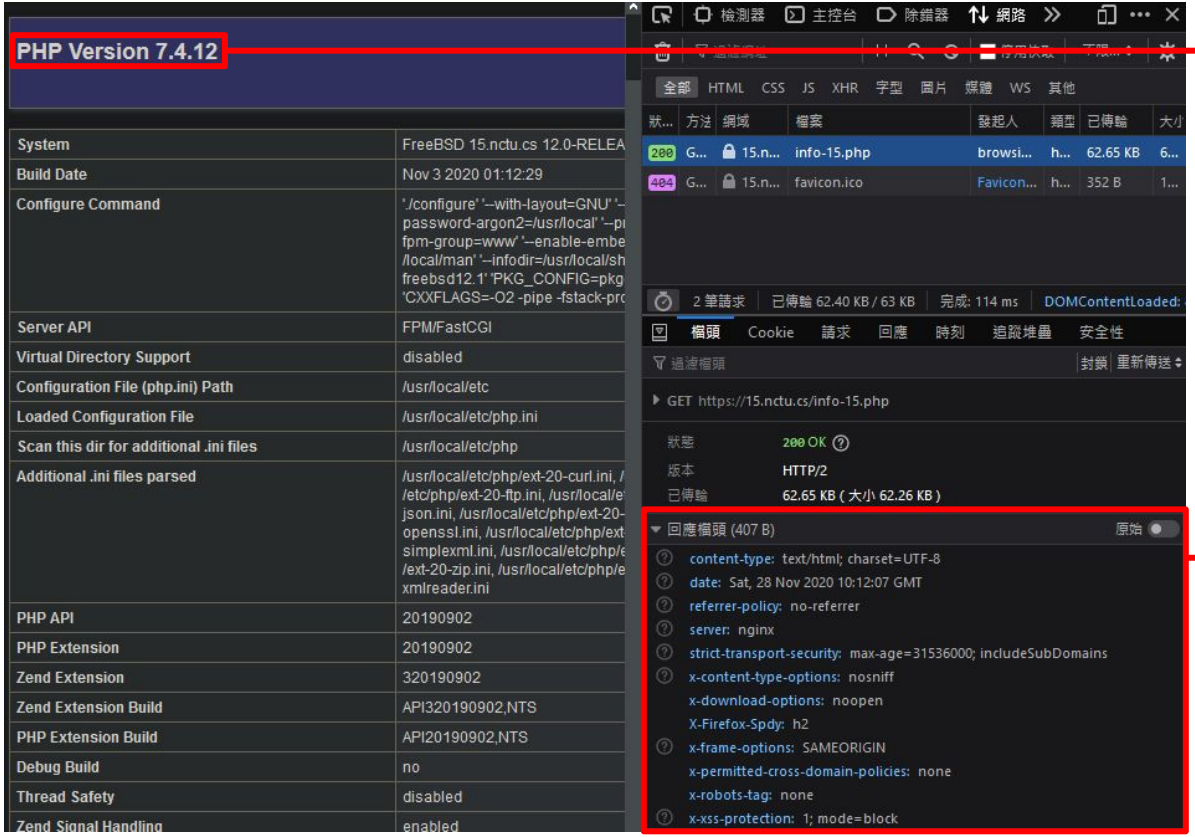
- CORS and Headers (7%)
  a. Allow only four HTTP methods: GET, HEAD, POST, OPTIONS
     - Other methods can allow Cross-Site Tracking attack and potentially allow a hacker to steal the cookie information.
     - Please refer to CORS
       - allow-origin: $ID.nctu.cs
       - allow methods: GET, POST, HEAD , OPTIONS
  b. *iframe* from this domain can only be accessed within this domain
  c. Enable X-XSS-Protection
- Allow only TLS 1.2 and above (3%)

Requirement: You must use CORS to complete a. and b.

PHP / PHP-FPM (5%)

- Set up PHP and create https://{ID}.nctu.cs/info-{ID}.php
  - This is a php info page
- Hide PHP version information in header
  - But the version is shown in PHP info page
- Use PHP 7 (7.3 or higher)

PHP / PHP-FPM (5%) (Cont'd)



PHP info page
(version >= 7.3)

Hide php version in header

Database

Setup MySQL for Wordpress (10%)

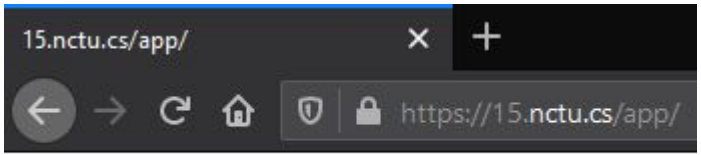
- Create a “mortal” account (3%)
  - Username: *wdpress*
  - Password: Your {IP} without dots. e.g. 10113015
  - Can only login from localhost
- Secure MySQL (4%)
  - Allow root login only from localhost
    - Password: 10113015
  - Remove test database
- Create a database called *wordpress* (3%)
  - ONLY *root* and *wdpress* have FULL privileges
  - User *wdpress* have FULL privleges ONLY on this database

HTTP Applications

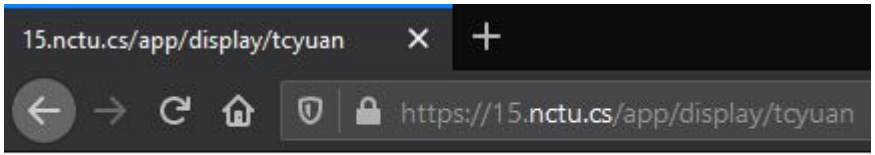
Basic App Router (15%)

- Use only ONE file: index.php to complete this app route
- Parse the URL and display different results accordingly (8%)
  - https://{ID}.nctu.cs/app
    - Display: App route enabled
  - https://{ID}.nctu.cs/app/display/{username} (username is a string)
    - Display: Display: {username}
  - https://{ID}.nctu.cs/app/calculate/{A}+{B} (A & B are integers)
    - Display: Result: {value of A + B}

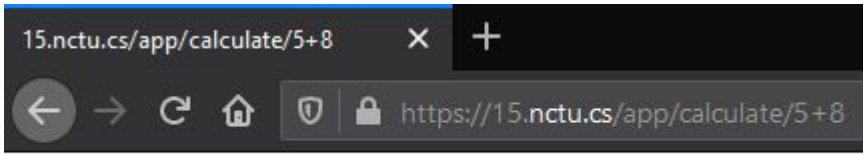
Basic App Router (15%) - Example



App route enabled



Display: tcyuan



Result: 13

Basic App Router (15%) (cont'd)

- Redirect from URL parameters (7%)
  - https://{ID}.nctu.cs/app?vid=sXp2FwMYbQc
    - This will redirect to
      - https://youtu.be/sXp2FwMYbQc
  - https://{ID}.nctu.cs/app?vid=FBp4QhLqiKs&time=14
    - This will redirect to
      - https://youtu.be/FBp4QhLqiKs?t=14

WebSocket (15%)

- A WebSocket is a persistent connection between a client and server
- Use websocket to keep logging your ping value to 1.1.1.1
  - Show one ping value per second for 3seconds
  - The connection is closed after three messages transmitted
  - Please check the example page for the format
- Create a new domain {ID}_ws.nctu.cs without HSTS
  - So you can access ws

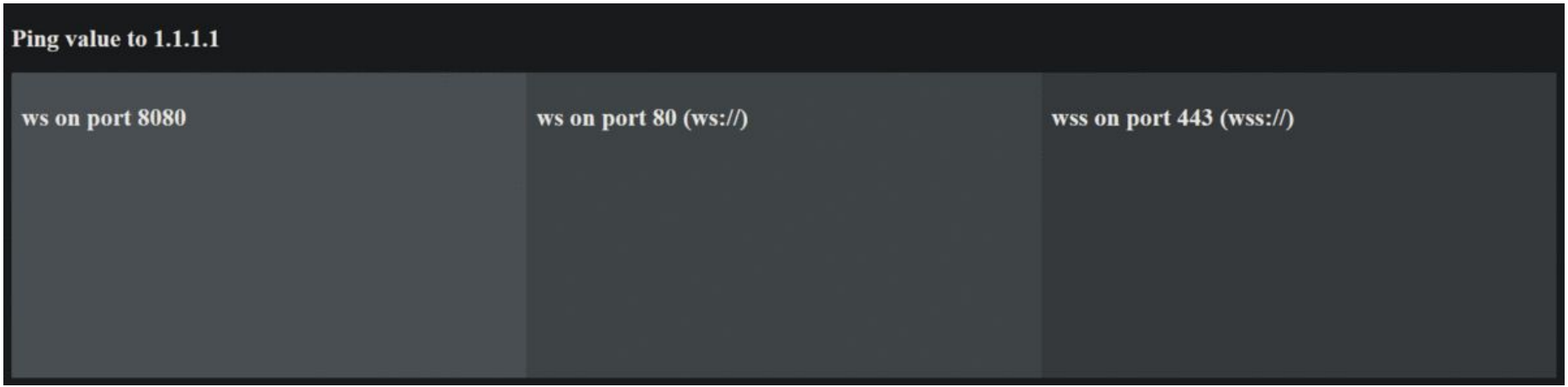
Hint: [websocketd]

WebSocket (15%) (cont'd)

- Create a webpage
  - http://{ID}_ws.nctu.cs/wsdemo
  - To connect to
    - ws://{ID}_ws.nctu.cs:8080 (3%)
    - ws://{ID}_ws.nctu.cs/wsconnect on port 80 (6%)
    - wss://{ID}.nctu.cs/wsconnect on port 443 (6%)
- And show your results side by side on that webpage

Hint: You might need to trust your self-signed certificate to see wss on your browser

WebSocket (15%) (Example)



https://imgur.com/a/GLLFRKm

WordPress (10%)

- Download and install the latest version (5%)
  - https://wordpress.org/latest.zip
  - Install Traditional Chinese (繁體中文) version wordpress
  - Should be accessed from https://{ID}.nctu.cs/wordpress
- Please create a new post (5%)
  - Title: 系計中徵才中!
  - Content: 歡迎加入系計中助教的行列
  - Url: https://{ID}.nctu.cs/wordpress/welcome-cscc/

Hint: Check out “Permalinks” settings.

Hints

1. You can use Apache or NGINX to complete this homework
2. Although you can not test your setup in 10.113.0.x network, you can use ip from another interface or you can use port forwarding
3. If you find your system too slow, please consider adding more RAM to it
4. If wss or https is not working, make sure you have trusted the self-signed certificate
5. Deadline: 2020/12/16 23:59

Help me! TA!

- TA office hours: 3 GH at EC 324 (PC Lab) or by appointment (mail us)
  - We do not accept walk-ins except for TA office hours
- Questions about this homework
  - Ask them on https://groups.google.com/g/nctunasa
  - When posting a question, be sure to include all information you think others would need
    - including but not limiting to your ID, setups, configurations and / or what you have done to trace the error / problem
  - We MIGHT give out hints on google group
    - Be sure to join the group :D
  - Do not mail us unless it's personal or that you're making an appointment

Good Luck!