TakeMeTour's Job Quest 2020 Edition

Back-end Questions

1. Explain First-party cookie & Third-party cookie

First-party cookie คือ cookie ที่ถูกสร้างขึ้นและใช้งานเฉพาะเว็บที่เราเข้าใช้งาน

Third-party cookie คือ cookie ที่ถูกสร้างและบันทึกข้อมูลของคุณด้วยโดยเว็บไซต์ใดๆก็ได้ และสามารถแบ่ง cookie ของเราให้กับเว็บอื่นๆได้ใช้งานอย่างอิสระ

2. Explain CAP Theorem.

CAP Theorem ถูกคิดค้นโดย Eric Brewer กล่าวคือ distributed database ทั้งหมดจะมีคุณสมบัติได้เพียง 2 จากทั้งหมด 3 อย่างตามด้านล่างเท่านั้น

Consistency [C] หมายถึง ทุกครั้งที่เราอ่านข้อมูลจาก database จะได้ผลลัพธ์ล่าสุดหรือไม่ก็ error ไปเลยเท่านั้น

Availability [A] หมายความว่า ถ้าเราดึงข้อมูลจาก database เราจะได้ผลลัพธ์กลับมาเสมอ (ไม่ error)

Partition Tolerance [P] — คือการที่ระบบสามารถทำงานต่อไปได้ หากมี node ใด node หนึ่งใน distributed database ขาดการติดต่อหรือล่มอยู่

3. Considering two queries

```
const searchIds = ['1', '2', '3', ...];

const query1 = await Product.find({ id: { $in: searchIds } });

const query2 = await Promise.all(searchIds.map(searchId => Product.find({ id: searchId })));
```

Which one is faster.

ตอบ:

```
const query2 = await Promise.all(searchIds.map(searchId => Product.find({ id: searchId })));
```

4. Explain XSS / SQL Injection / Man in the Middle Attack, and how to prevent each attack type.

Cross Site Scripting (XSS)

เป็นการฝั่ง Code Javascrip เข้าไปใน เว็บไซน์และเมื่อผู้ใช้โหลดหน้าเว็บไปก็อาจจะโดนขโมยข้อมูลบางอย่างไป หรือโดนบังคับให้ทำอะไรบางอย่างที่เป็นผู้ดีต่อผู้โจมตี

วิธีป้องกัน

- ลดการใช้ JavaScript และ พัฒนาเว็บโดยอาศัย framework
- ใช้การ encoding ข้อมูลก่อนแสดงผล
- ไม่แสดงข้อมูลสำคัญ inspect เช่น user password หรือฝั่ง user password ลงใน cookie

SQL Injection

ส่วนของฐานข้อมูล ซึ่งการทำงานร่วมกับฐานข้อมูล จะต้องใช้คำสั่ง SQL (Structured Query Language) ในการทำงาน สำหรับคำสั่ง SQL เป็นโครงสร้างคำสั่งพื้นฐาน เช่น Select, Insert, Update หรือ Delete จากตารางข้อมูลที่กำหนดไว้ ซึ่งในบางครั้ง ผู้จัดสร้างเว็บไซต์เขียนแบบฟอร์มสำหรับรับข้อมูลไม่รัดกุมเพียงพอ อาจเกิดความพยายามส่งคำสั่ง SQL แทรกเข้าไปในระบบ

วิธีป้องกัน

- แยกตัวแปร query ออกมาเป็นส่วนๆและใช้ style formatting แทนการใส่ค่าไปตรงๆ
- ใส่ encode ลงในคำสั่ง SQL

Man In The Middle (MITM) คือ เทคนิคการโจมตีของแฮคเกอร์ที่จะปลอมเป็นคนกลางเข้ามาแทรกสัญญาณการรับส่งข้อมูลระหว่างผู้ใช้ (เบราว์เซอร์) และเซิร์ฟเวอร์ โดยใช้โปรแกรมดักฟังข้อมูลของเหยื่อ แล้วแฮกเกอร์ก็เป็นตัวกลางส่งผ่านข้อมูลให้ระหว่างเบราว์เซอร์กับเซิร์ฟเวอร์ วิธีการทำอย่างหนึ่งคือ การส่งข้อมูล MAC Address ของเครื่องของแฮกเกอร์ไปให้กับเครื่องของผู้ใช้โดยแจ้งว่าเป็น MAC Address ของ Gateway ของระบบเครือข่าย หลังจากนั้นเมื่อเครื่องเหยื่อรับ MAC Address ดังกล่าวไปใส่ไว้ใน ARP Table cached แล้ว กระบวนการส่งข้อมูลจากเบราว์เซอร์ของเครื่องเหยื่อจะถูกส่งผ่านไปยังเครื่องแฮกเกอร์ก่อนที่จะส่งไปยังเครื่องเซิร์ฟเวอร์

วิธีป้องกัน

- การโจมตีด้วยวิธี Man In The Middle นั้นประสบความสำเร็จง่ายและตรวจจับได้ยาก เนื่องจากผู้ถูกโจมตีส่วนใหญ่มักจะไม่รู้ตัวและค่อนข้างละเลยในเรื่องของความปลอดภัย ดังนั้น วิธีการป้องกันที่ดีที่สุดคือสร้างความ

ตระหนักในเรื่องของความปลอดภัยให้กับผู้ใช้ เช่น ตรวจสอบความถูกต้องของใบรับรองของเว็บไซต์ทุกครั้งที่ต้องทำธุรกรรมทางอิเล็กทรอนิกส์

5. Explain the different between using `callback` / `Promise` / `async await`. When to use and when not to.

Callback คือ callback คือ function ที่จะถูกเรียกหลัง function อื่นทำงานเสร็จ ทำให้การทำงานเป็นแบบ synchronous Callback เหมาะกับงานประเภทที่ สามารถถูกเรียกได้มากกว่า 1 ครั้งและไม่ต้องการหยุดรอ Callback ไม่เหมาะกับงานที่มีความซับซ้อนเพราะจะทำให้เกิด callback hell ทำให้อ่าน Code ยากและดัก Error ได้ยาก หรือเปลี่ยนแปลงได้ยาก

Promise คือ จะคล้ายกับ Callback แต่จะทำงานแบบ asynchronous Promise จะทำงานแบบเป็นลำดับชั้น Promise เหมาะกับงานการเรียกเป็นลำดับชั้น ข้อดีคือทำให้ Code เราไม่อยู่ภายใต้ {} หลายๆชั้นทำให้เราไล่ Code ได้ง่าย Promise ไม่เหมาะกับงานที่เป็นการเรียงลำดับเป็นขั้นเป็นตอน

async await คือ การ พัฒนาจาก Promise การทำงานจะเป็นรูปแบบ asynchronous และ เราสามารถกำหนดได้ว่าตรงไหนหยุดหรือไม่หยุดรอซึ่งแตกต่างจาก Promise ที่จะหยุดรอเป็นลำดับ async await เหมาะกับงานที่ต้องการความถูกต้อง เช่น การ Select ข้อมูลจาก Database หรือ การทำงานที่ต้องใช้การประมวลผล async await ไม่เหมาะกับงานที่ต้องจัดการ Error เนื่องจาก จัดการค่อนข้างยากไม่มีการ callback หรือ then จะต้องใช้ try/catch แทน

6. Explain how HTTP protocol works.

เครื่องลูกข่าย Client		เครื่องแม่ข่าย Server
สร้าง HTTP Request String		เปิด TCP Server Socket รอรับ Request
เปิด TCP Socket		เปิด TCP Socket รับการสื่อสารจากเครื่องลูก
ส่ง HTTP Request		รับ HTTP Request
รอการประมวลผล หากรอนานเกินไปจะเกิด Timeout		ตีความ ประมวลผล
		สร้าง HTTP Response
รับ HTTP Response		ส่ง HTTP Response กลับไปยังเครื่องลูก
แสดงผลจาก HTTP Response	ปิด TCP Socket	ปิด TCP Socket
จบการทำงาน		รอรับ Request อื่นๆ ต่อไป
–	–	–

รูปจาก https://swiftlet.co.th/learn/http-protocol/

HTTP ย่อมาจาก Hypertext Transfer Protocol เป็นโปรโตคอล (Protocol) สื่อสารที่ทำงานอยู่ในระดับ Application Layer บนโปรโตคอล TCP/IP มีรูปแบบดังนี้

1. เป็นโปรโตคอลหลักที่ใช้ในการแลกเปลี่ยนข้อมูล (HTML) กันระหว่าง Web Server และ Web Client (Browser)
2. ใช้ URL (Uniform Resoure Locator) ในการเข้าถึงเว็ปไซต์ (Web Site) ซึ่งจะขึ้นต้นด้วย http:// ตามด้วยชื่อของเว็ปไซต์
3. ทำงานที่พอร์ต (port) 80 (มาตรฐาน)
4. ส่งข้อมูลเป็นแบบ Clear text คือ ไม่มีการเข้ารหัสข้อมูลในระหว่างการส่ง (None-Encryption) จึงสามารถถูกดักจับได้ และอ่านข้อมูลนั้นรู้เรื่อง