**Bài 1: youtube-trailer**

Mô tả: xem ping ctf 2023 trailer và tìm flag

https://www.youtube.com/watch?v=siZPvEGrtNY

Bật developer tools lên 🡪 vào mục Inspector 🡪 Ctrl+ F, nhập ping{

**Flag: ping{hello\_welcome\_to\_ping\_ctf}**

**Bài 2: internet-explorer**

Mô tả: Bạn có thể chạy Internet Explorer trên Linux?

Gợi ý cho mình thêm User-Agent.

Bài này lúc đầu mình brute force User-Agent nhưng nó sẽ không khả thi vì Internet Explorer là 1 trình duyệt web của Microsoft và không chạy được trên Linux.

Thử User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

🡪Ứng dụng báo “I see IE but no Linux...”

Mình nghĩ sẽ thay đổi windows thành linux:

Mozilla/4.0 (compatible; MSIE 8.0; Linux x86\_64; Trident/4.0)

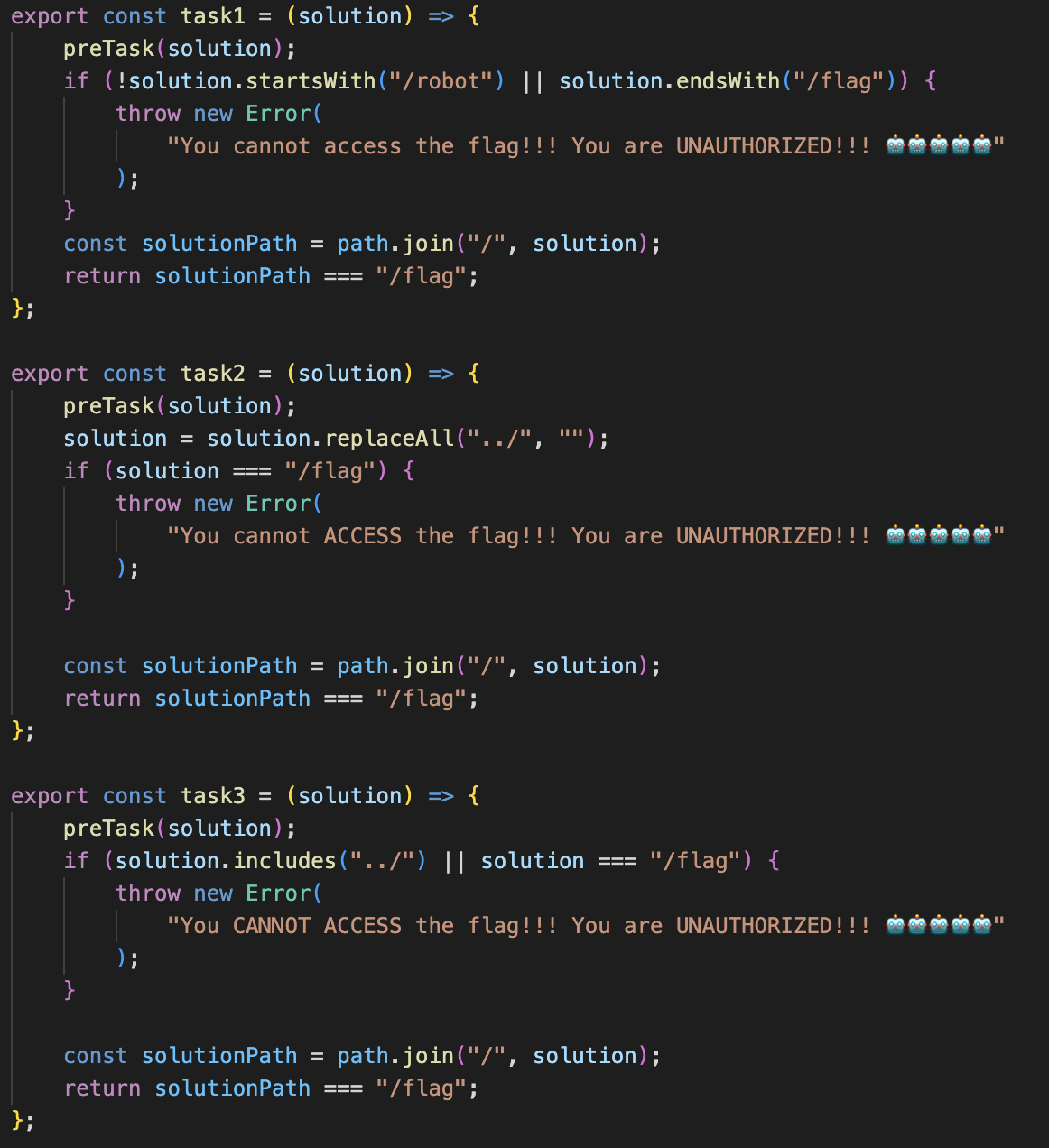
**Flag: ping{ping{the\_best\_browser\_ever\_made111}}**

**Bài 3: path-traversal-101**

Bài cho source để làm. Có hai file đáng chú ý là : index.js và tasks.js

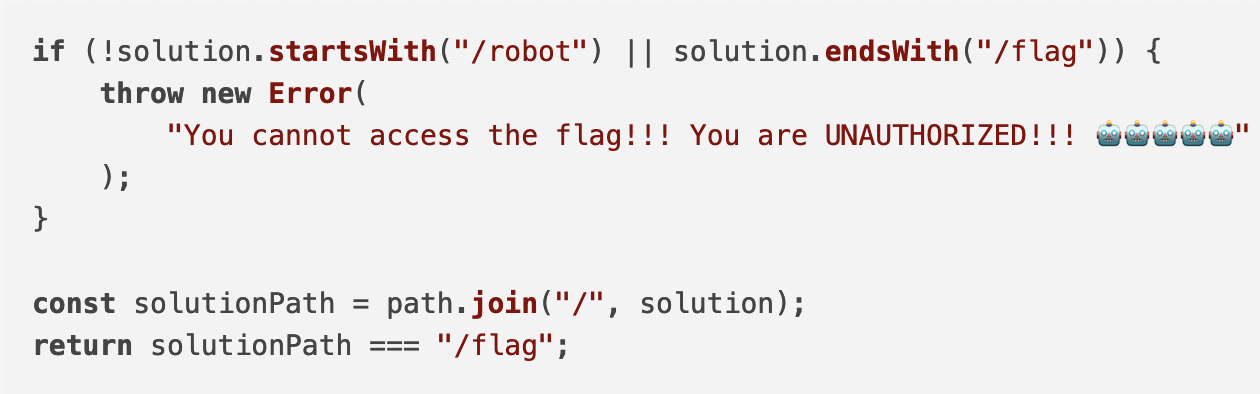


Mình phải làm được 3 nhiệm vụ mới nhận được flag. Mỗi nhiệm vụ ứng dụng sẽ cấp 1 phiên khác nhau. Nội dung của các nhiệm vụ ở trong file tasks.js



Muốn có được cookie của nhiệm vụ đầu tiên, bạn phải thêm User-Agent: robot, phương thức GET /%F0%9F%A4%96 🡪Set-Cookie: token=73361b7e-08f1-4fbb-81a6-6f74afd71e2c

Nhiệm vụ đầu tiên:



Mình dùng tham số solution trong phương thức Post. Yêu cầu:

* Bắt đầu với /robot
* Không được kết thúc với /flag

Hàm join giúp nối các phân đoạn thành 1 đường dẫn hoàn chỉnh, sau cùng, solutionPath phải bằng /flag.

Nhiều khi mình thấy ứng dụng bị lỗi, solution để /flag ở cuối nhưng không báo lỗi.

Không hiển thị “Try again!” khi mình trả lời sai.

Solution: /robot/../flag/.

Mình học được:

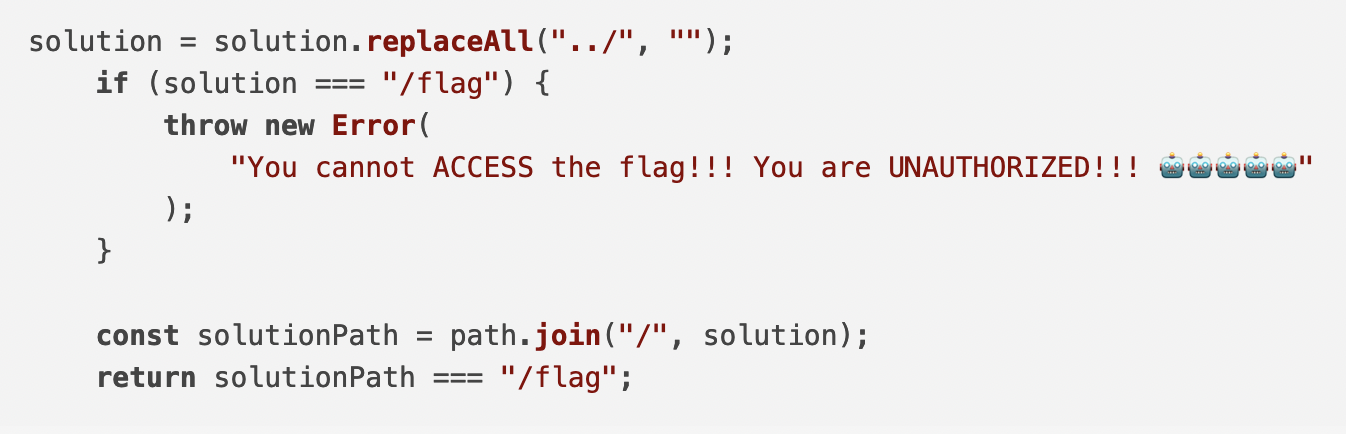
* **// 🡪 /**
* **Không nhất thiết phải là ./ hay ../, để . hay .. cũng được**

Mình cũng không thạo code javascript lắm. Đọc mãi mới hiểu.

Trong quá trình làm, mình có mô phỏng code trên nodejs online: https://www.tutorialspoint.com/execute\_nodejs\_online.php

Token không thay đổi, khi payload bạn đúng nó sẽ tự động hiển thị chall tiếp theo.

Nhiệm vụ thứ hai:

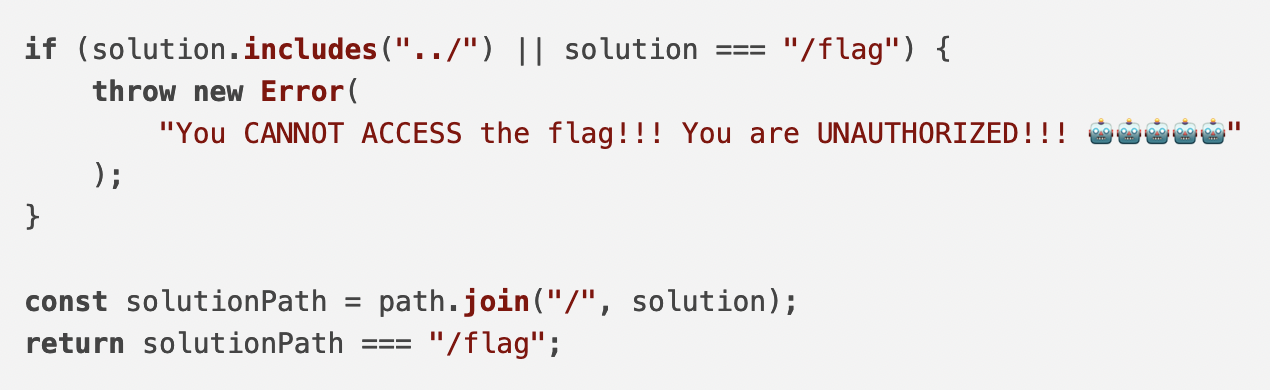


Yêu cầu:

* thay thế ../ thành rỗng
* Không được bằng /flag

Solution: ./flag/.

Nhiệm vụ thứ ba:



Solution giống với task2: ./flag/.

**Flag: ping{p4th\_tr4V3Rs4L\_06c22f693acd46015891c98cb72f45e3}**