**Bài tập về Juice Shop 1 sao**

**Mục lục**

[1. Score Board 1](#_Toc16831)

[2. DOM XSS 2](#_Toc4711)

[3. DOM XSS 3](#_Toc3411)

[4. Privacy Policy 4](#_Toc20053)

[5. Bully Chatbot 5](#_Toc19629)

[6. Confidential Document 6](#_Toc18809)

[7. Error Handling 7](#_Toc30662)

[8. Exposed Metrics 8](#_Toc6720)

[9. Mass Dispel 10](#_Toc6243)

[10. Missing Encoding 11](#_Toc25654)

[11. Outdated Allowlist 13](#_Toc2359)

[12. Repetitive Registration 15](#_Toc12090)

[13. Web3 Sandbox 18](#_Toc13008)

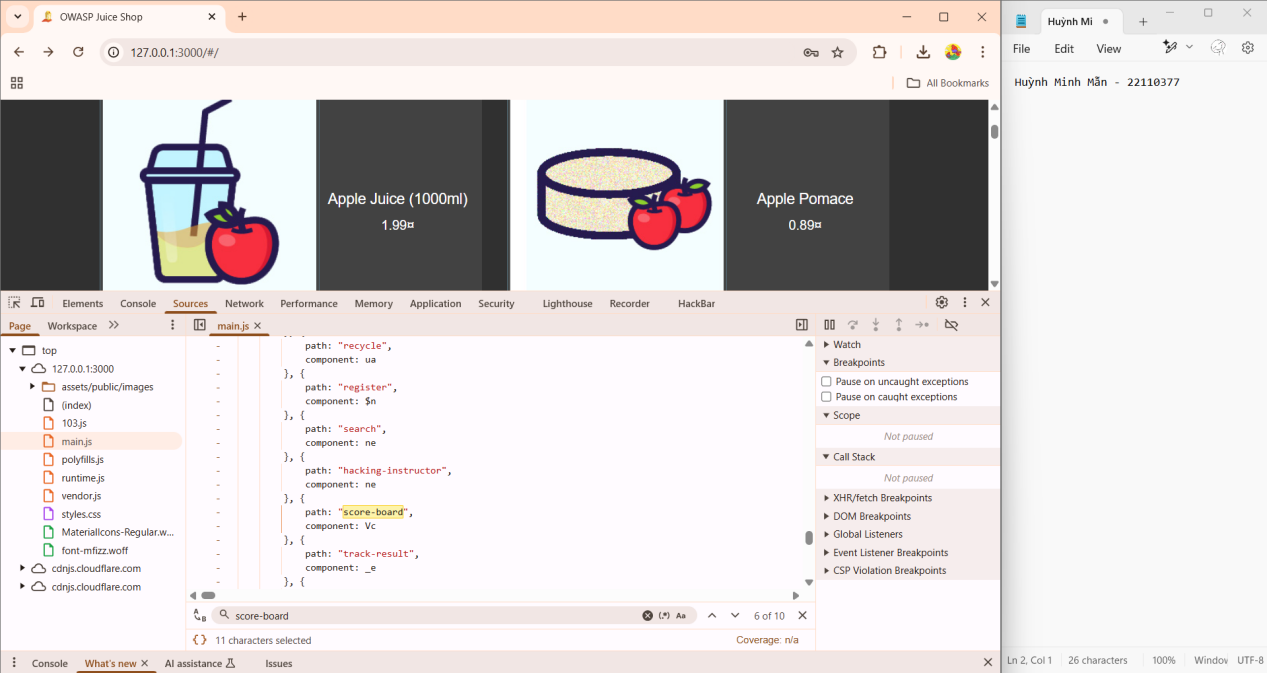
[14. Zero Stars 19](#_Toc26909)

1. **Score Board**

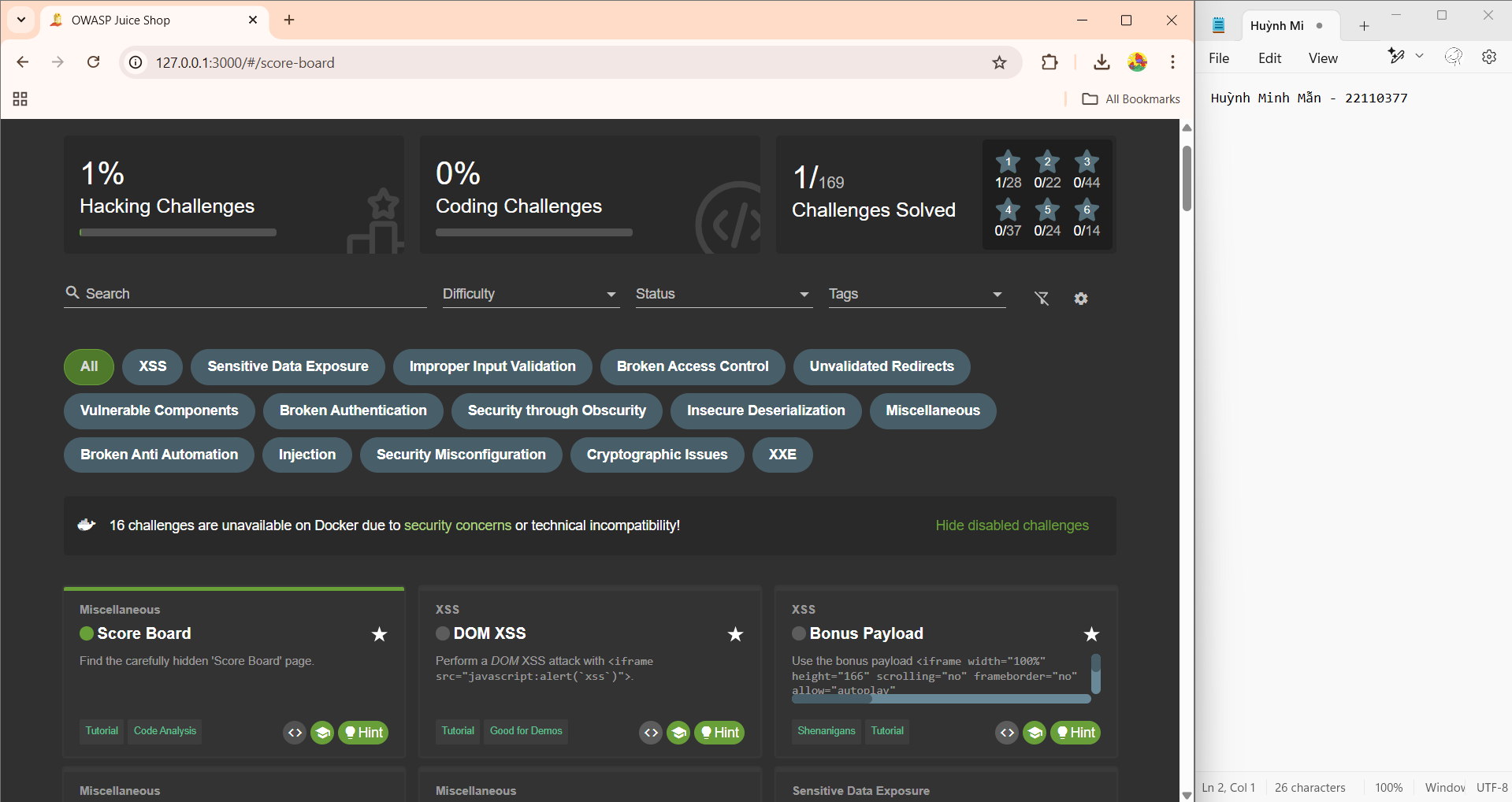
**Find the carefully hidden 'Score Board' page.**

Trang Score-board là một trang hiển thị danh sách các thử thách bảo mật trong Juice Shop, giúp người dùng theo dõi tiến trình thực hiện các thử thách.

Để hoàn thành bài này, ta cần biết đường dẫn vào trang score-board. Đầu tiên ta mở Inspect (F12), sau đó vào tab sources, vào main.js tìm kiếm “score-board” và sau đó thấy được đường dẫn path.



Tiến hành dán path vào phía sau url đang có, lập tức trang Score-board sẽ hiện lên, bài tập hoàn thành.



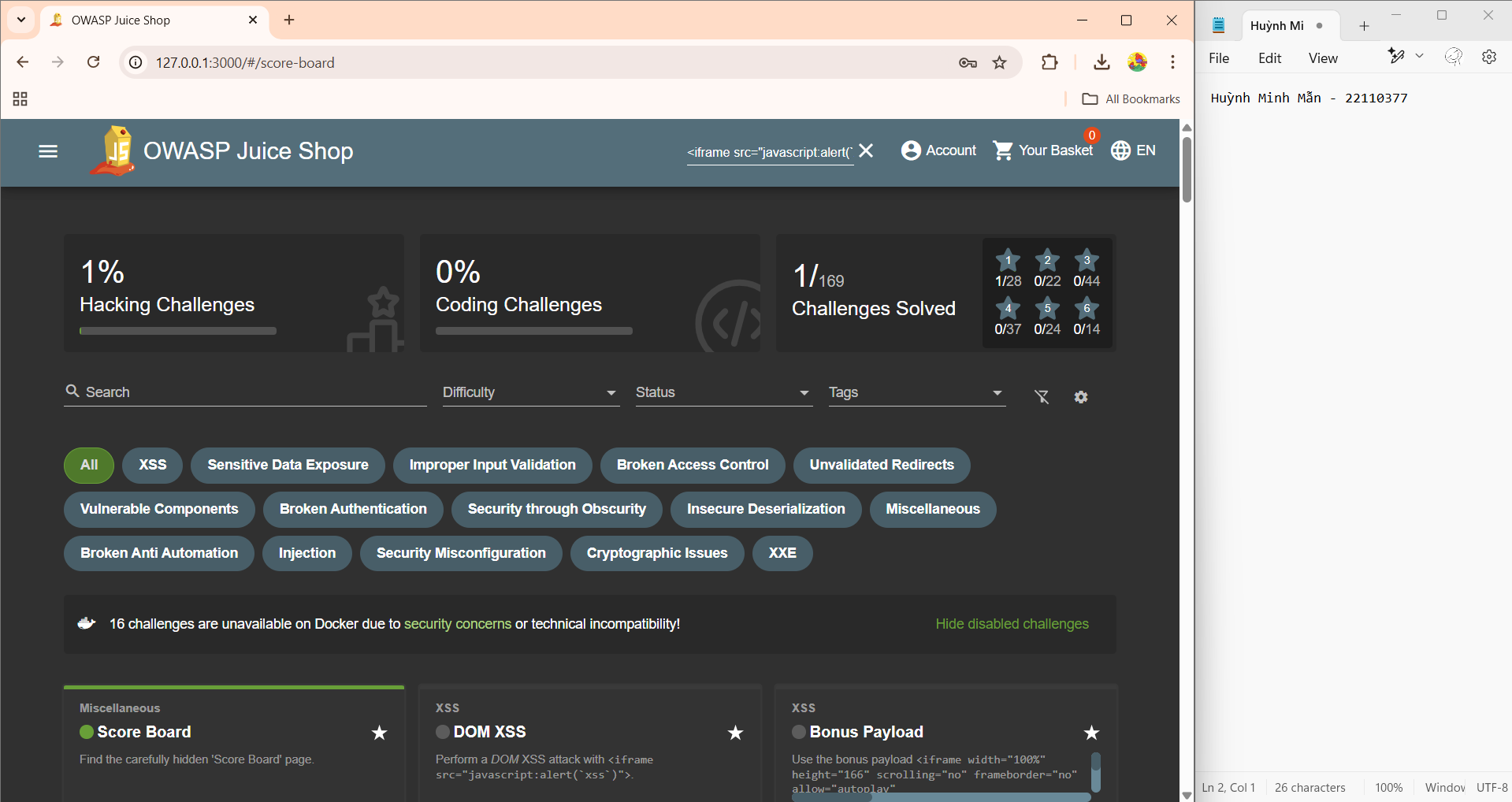
1. **DOM XSS**

**Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.**

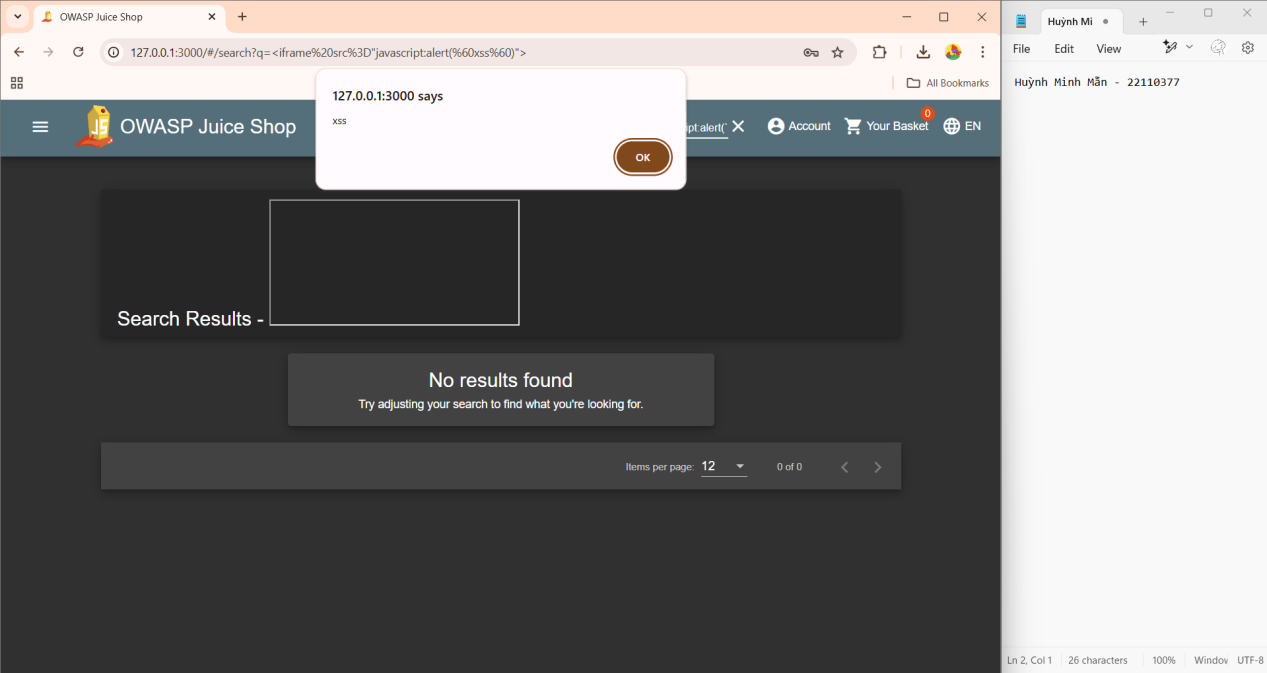
DOM XSS (Cross-Site Scripting dựa trên DOM) là một dạng tấn công XSS xảy ra khi JavaScript trên trang web xử lý dữ liệu đầu vào từ người dùng mà không có kiểm tra hoặc mã hóa an toàn, dẫn đến việc kẻ tấn công có thể thực thi mã JavaScript độc hại trên trình duyệt của nạn nhân.

Đầu tiên, ta truy cập Juice Shop và tìm vị trí nhập liệu có thể bị tấn công, cụ thể ở đây là thanh tìm kiếm để nhập nhập dữ liệu.

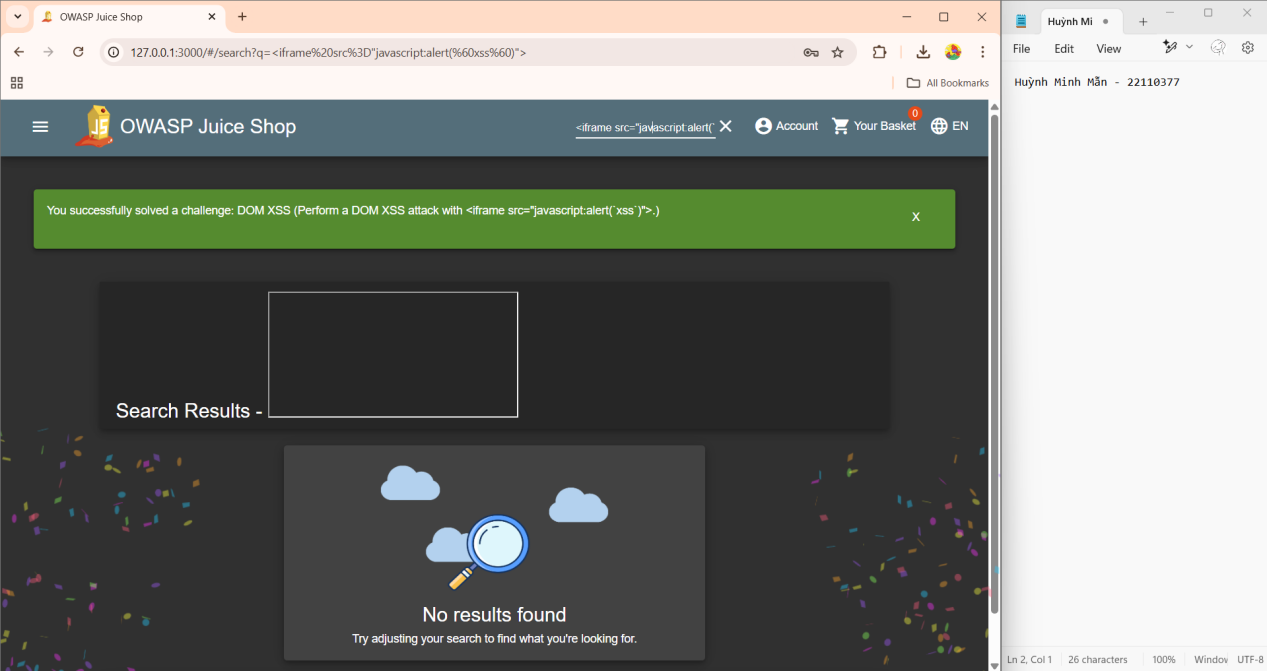
Nhập payload: *<iframe src="javascript:alert(`xss`)">*



Nếu trang web không xử lý đúng dữ liệu đầu vào, đoạn mã trên sẽ được thực thi ngay khi được nhập vào, hiển thị một hộp thoại cảnh báo (alert).



Khi hộp thoại hiện ra, nghĩa là tấn công thành công, bài tập được hoàn thành.



1. **DOM XSS**

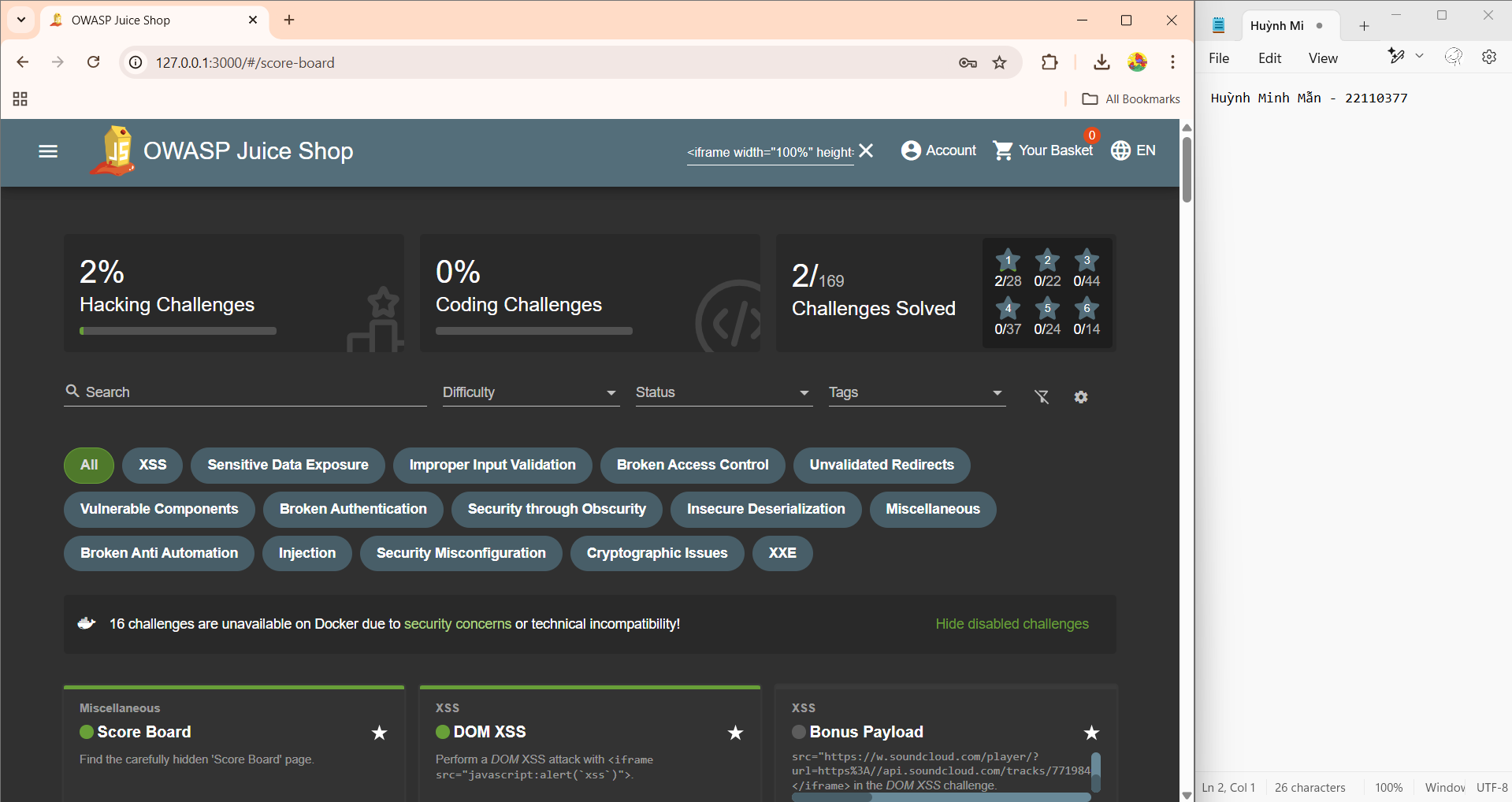
**Use the bonus payload <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto\_play=true&hide\_related=false&show\_comments=true&show\_user=true&show\_reposts=false&show\_teaser=true"></iframe> in the DOM XSS challenge.**

Bài tập này là một biến thể nâng cao của tấn công DOM XSS. Thay vì hiển thị một hộp thoại alert, chúng ta sẽ nhúng một iframe chứa nội dung từ SoundCloud để kiểm tra xem trang web có xử lý không đúng dữ liệu đầu vào hay không.

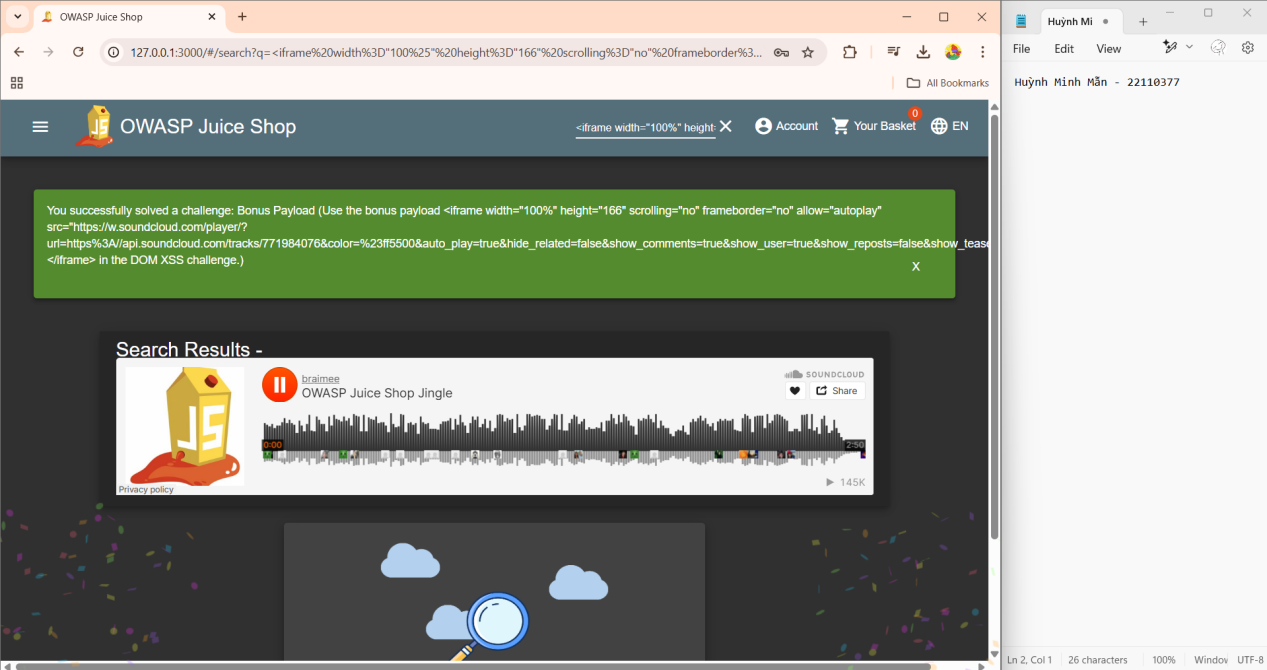
Đầu tiên, ta truy cập Juice Shop và tìm vị trí nhập liệu có thể bị tấn công, cụ thể ở đây là thanh tìm kiếm để nhập nhập dữ liệu.

Nhập payload: *<iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto\_play=true&hide\_related=false&show\_comments=true&show\_user=true&show\_reposts=false&show\_teaser=true"></iframe>*

Nếu trang web không xử lý đúng dữ liệu đầu vào, iframe sẽ được nhúng và phát nhạc tự động



Khi nhạc phát thành công, nghĩa là tấn công đã hoạt động, bài tập hoàn thành.

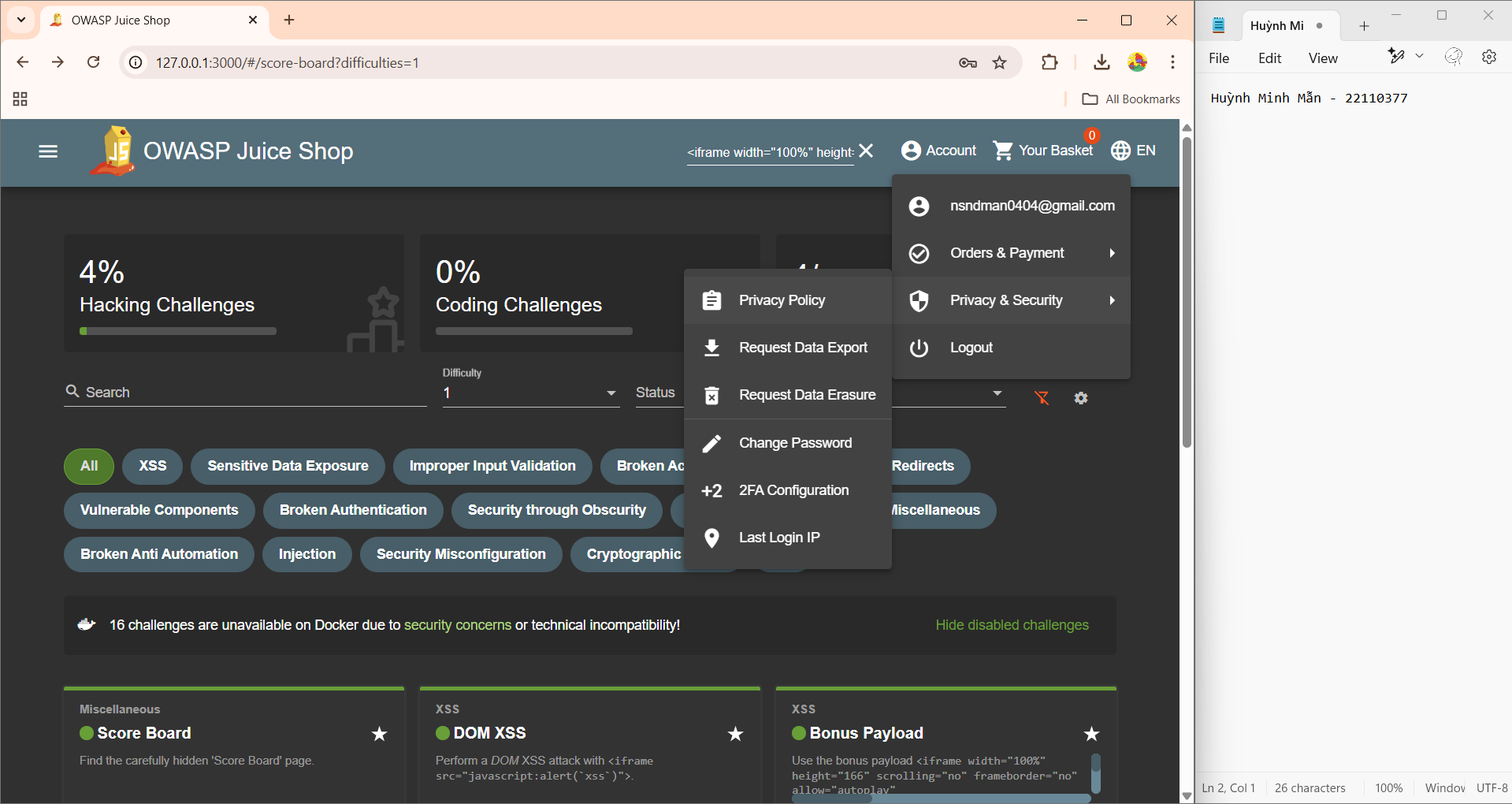


1. **Privacy Policy**

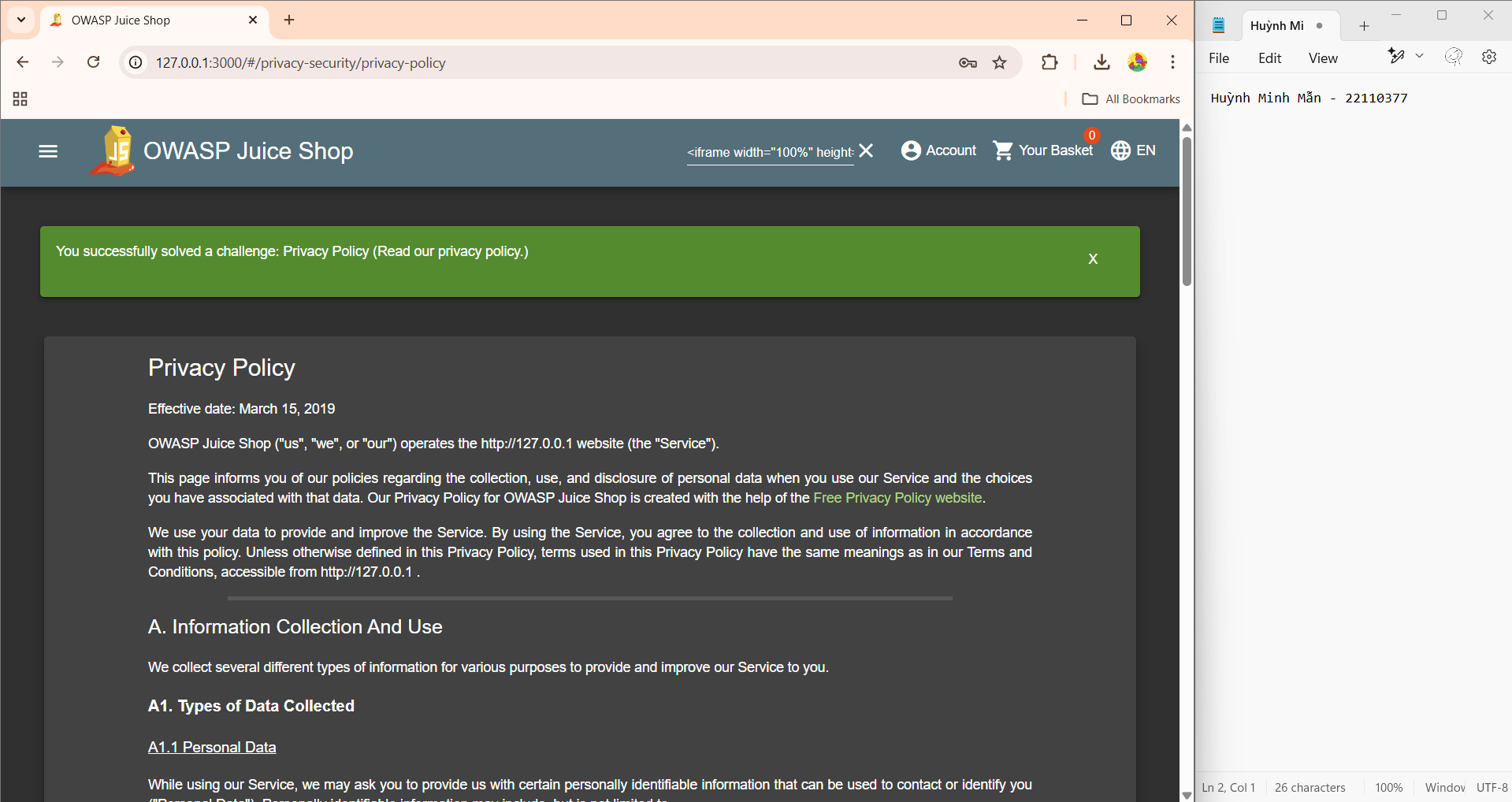
**Read our privacy policy.**

Bài tập này yêu cầu người dùng tìm và đọc trang chính sách bảo mật (Privacy Policy) của Juice Shop. Đây là một bài tập đơn giản, giúp làm quen với cách tìm kiếm và truy cập các trang thông tin trong ứng dụng web.

Đầu tiên, ta kiểm tra giao diện trang web để tìm liên kết đến Privacy & Security.



Khi trang Privacy Policy mở ra, tiến hành đọc và bài tập sẽ được đánh dấu là hoàn thành.

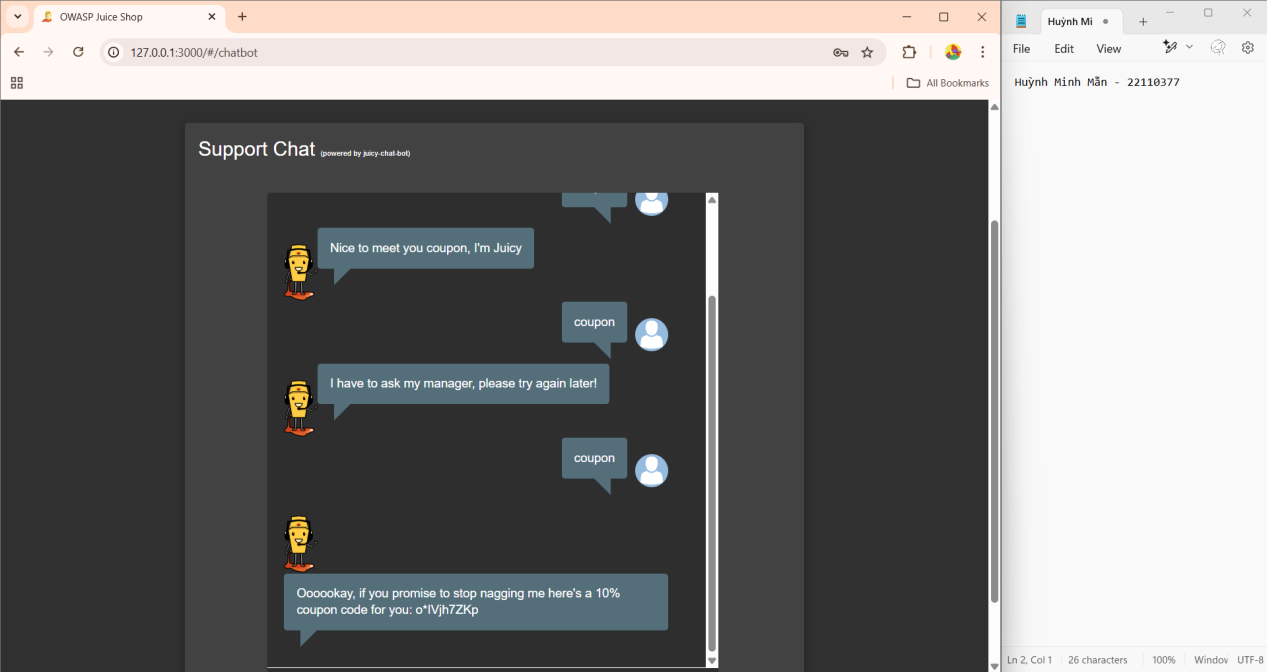


1. **Bully Chatbot**

**Receive a coupon code from the support chatbot.rivacy Policy**

Bài tập này yêu cầu người dùng khai thác chatbot hỗ trợ của Juice Shop để nhận được một mã giảm giá (coupon code). Đây là một tình huống phổ biến trong thực tế khi chatbot có thể bị lạm dụng hoặc dễ bị thao túng để tiết lộ thông tin không mong muốn.

Đầu tiên, tìm và mở chatbot hỗ trợ trên trang web. Tiếp theo ta spam vào đoạn chat ký tự “coupon” cho đến khi chatbot cung cấp mã giảm giá, bài tập sẽ được đánh dấu là hoàn thành.

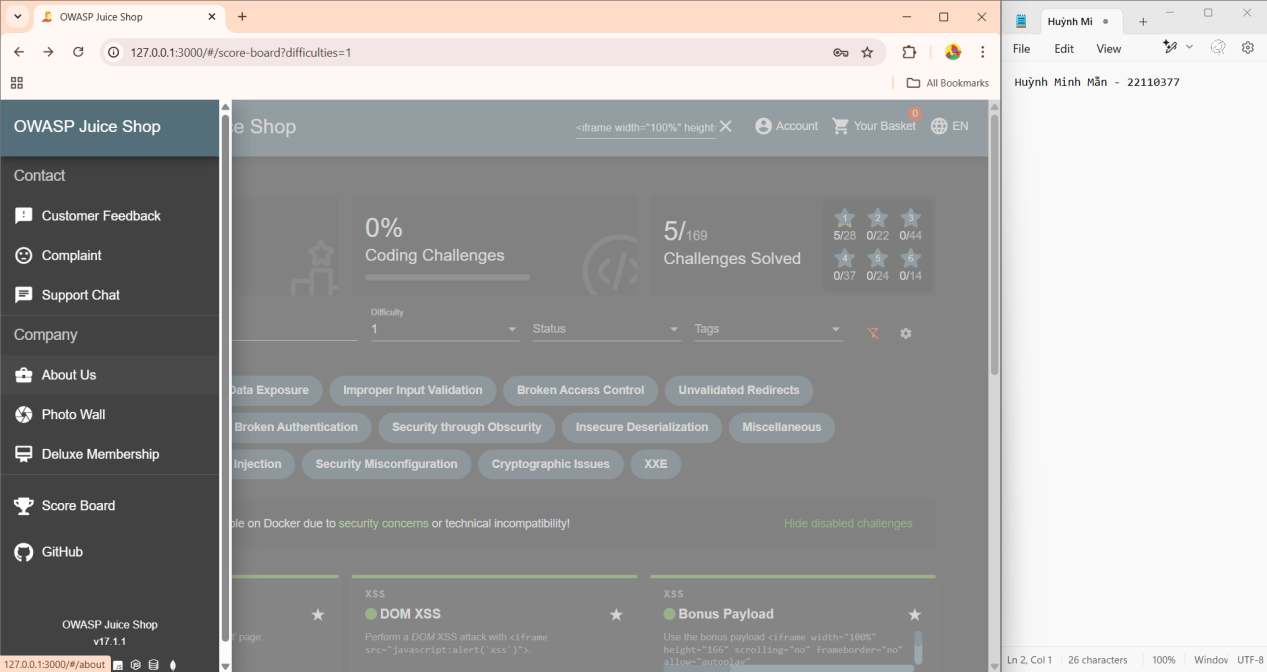


1. **Confidential Document**

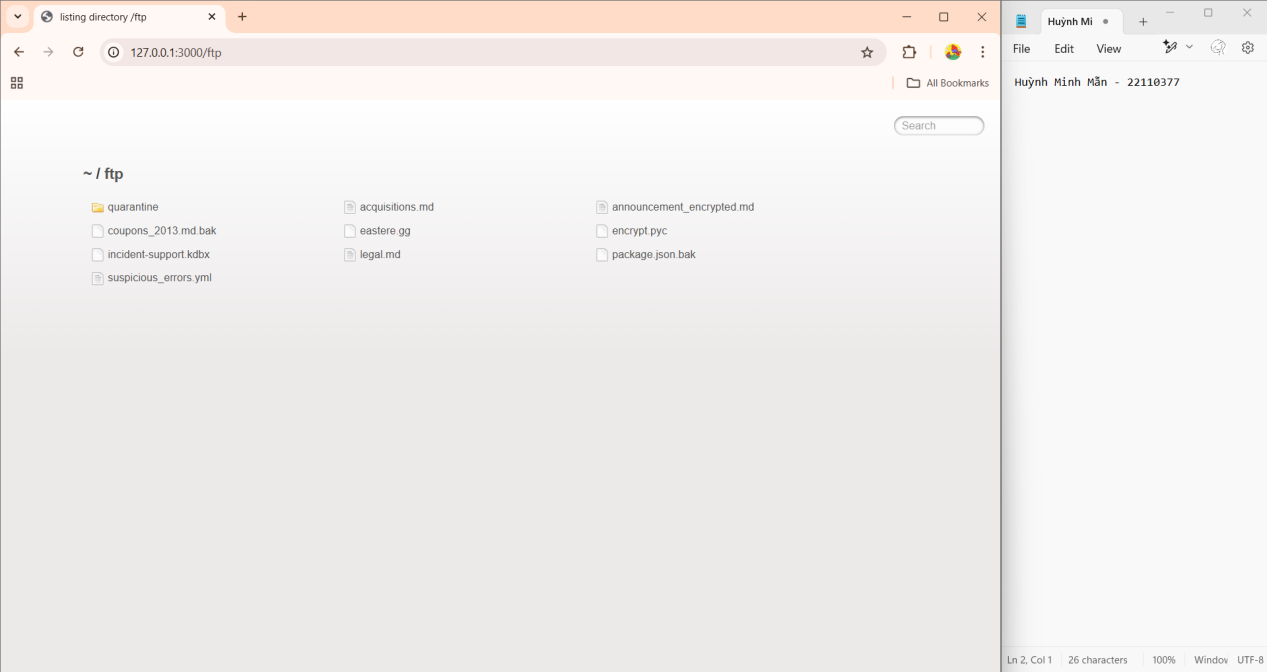
**Access a confidential document.**

Bài tập này yêu cầu người dùng truy cập vào một tài liệu mật trong hệ thống Juice Shop. Một cách khai thác phổ biến là tìm các thư mục hoặc endpoint chưa được bảo vệ đúng cách để truy xuất tệp tin nhạy cảm.

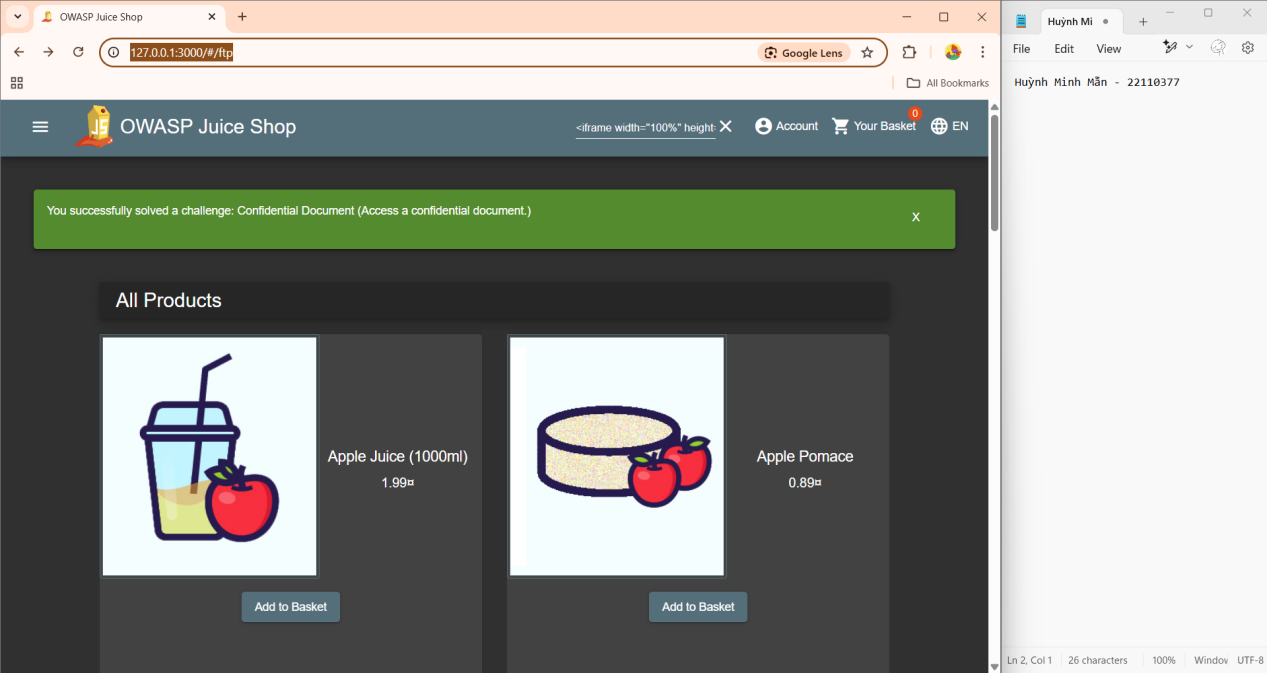
Đầu tiên, ta thử truy cập thư mục FTP nội bộ qua url: <http://127.0.0.1:3000/ftp>, một trang trắng chứa danh sách các tệp tin sẽ hiện ra.



Trong danh sách tệp tin, tìm kiếm một tệp có vẻ quan trọng, chẳng hạn như acquisitions, nhấp vào tệp đó để tải về hoặc mở nội dung.



Khi mở thành công tệp **acquisitions**, hệ thống sẽ đánh dấu bài tập là hoàn thành.

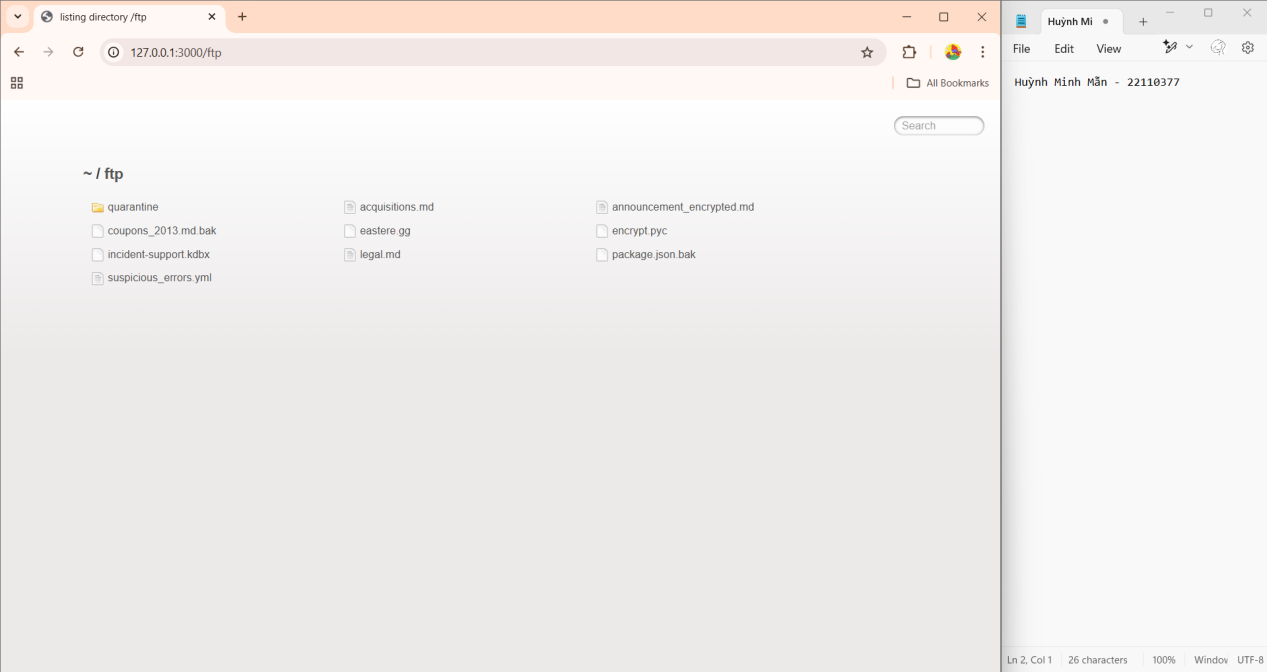


1. **Error Handling**

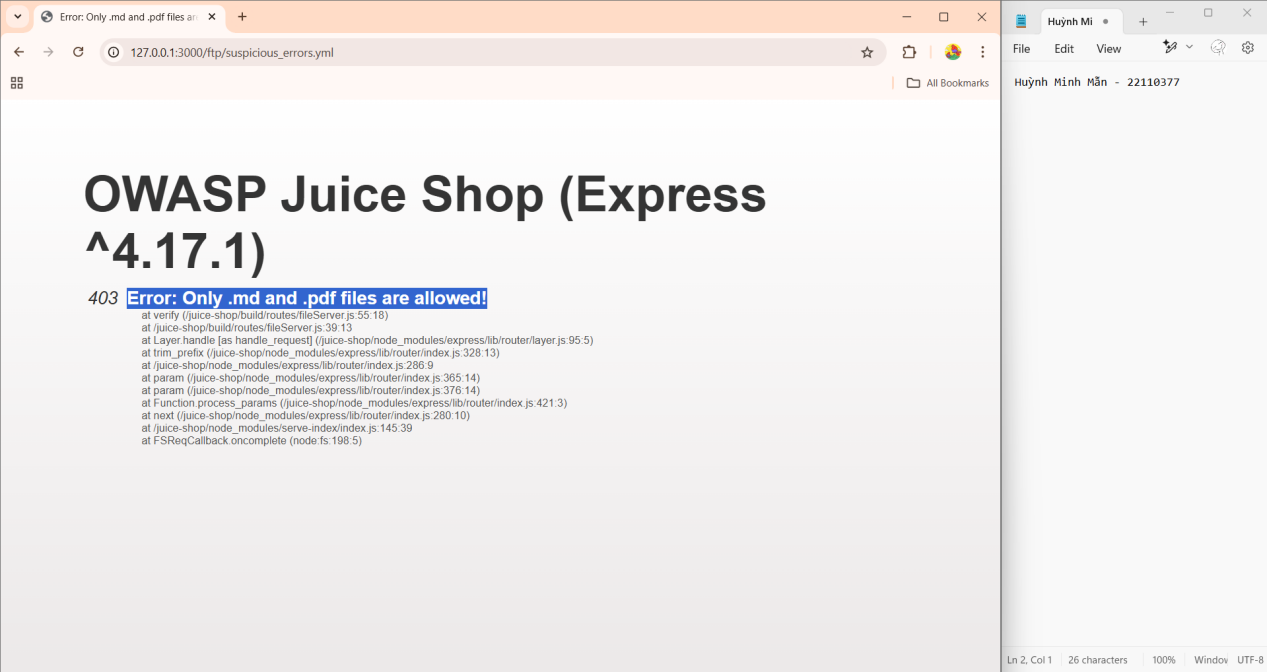
**Provoke an error that is neither very gracefully nor consistently handled.**

Bài tập này yêu cầu người dùng tạo ra một lỗi trong hệ thống Juice Shop và quan sát cách ứng dụng xử lý lỗi đó. Nếu lỗi không được xử lý một cách trơn tru hoặc không nhất quán, bài tập sẽ hoàn thành.

Các bước làm cũng tương tự như bài 6 Confidential Document, ta cũng truy cập vào trang <http://127.0.0.1:3000/ftp> sau đó truy cập vào tài liệu lỗi suspicious\_errors.yml.



Khi truy cập thành công, hệ thống sẽ đánh dấu bài tập là hoàn thành.



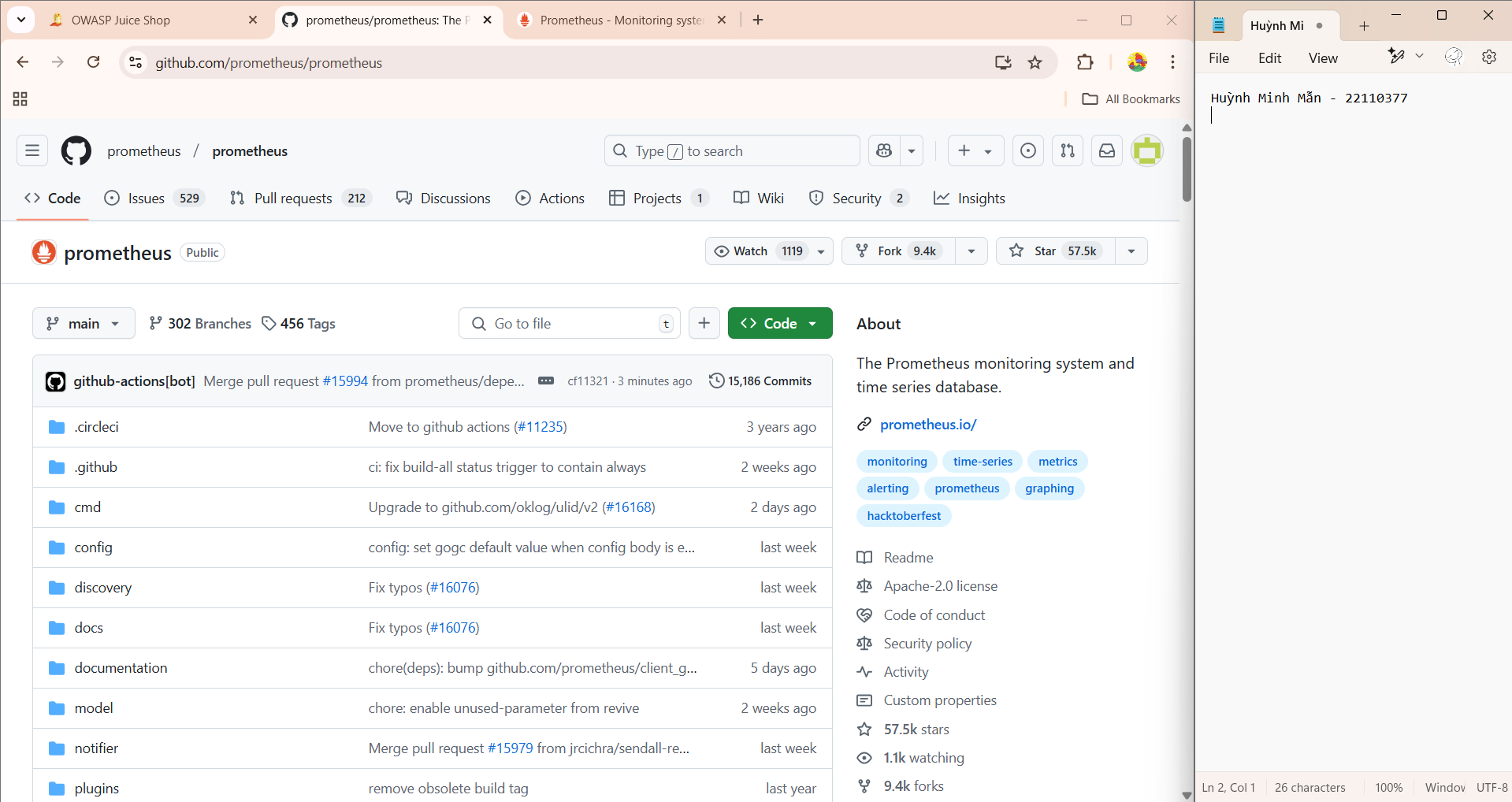
1. **Exposed Metrics**

**Find the endpoint that serves usage data to be scraped by a popular monitoring system.**

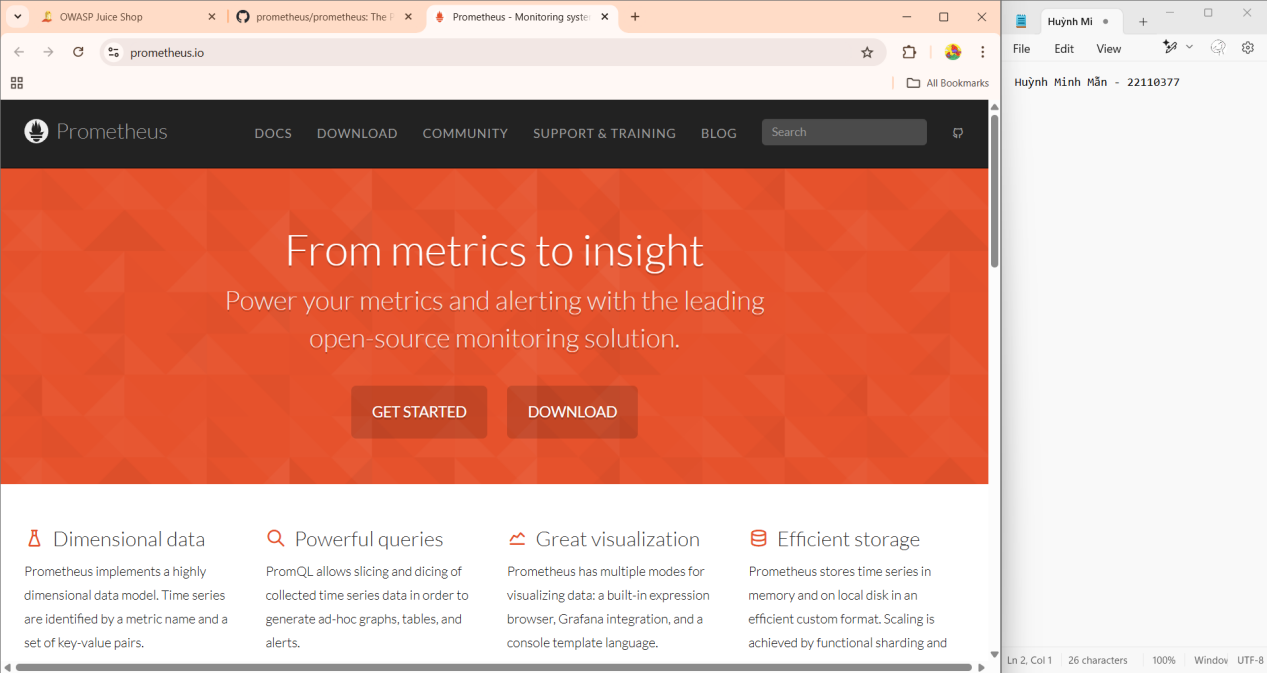
Bài tập này yêu cầu người dùng tìm ra một endpoint cung cấp dữ liệu giám sát hệ thống, thường được sử dụng bởi các công cụ như Prometheus để thu thập thông tin về hiệu suất và trạng thái của ứng dụng.

Đầu tiên, truy cập vào trang GitHub của Prometheus tại

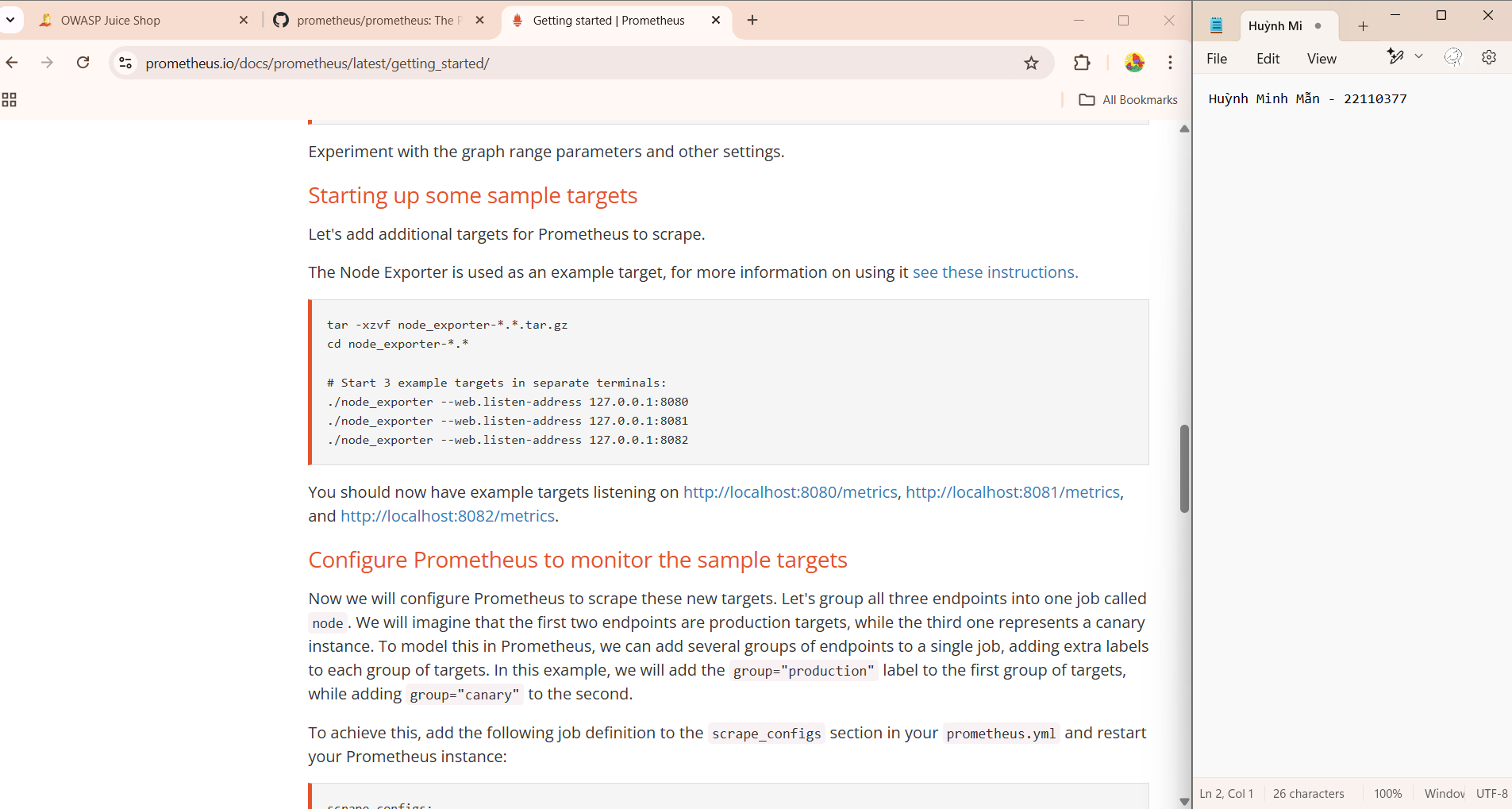
<https://github.com/prometheus/prometheus>



Nhấp vào liên kết trang chủ của Prometheus ứng với url: <https://prometheus.io/>



Nhấn GET STARTED, cuộn xuống để tìm phần hướng dẫn về /metrics, đây là endpoint mặc định của Prometheus để thu thập dữ liệu.

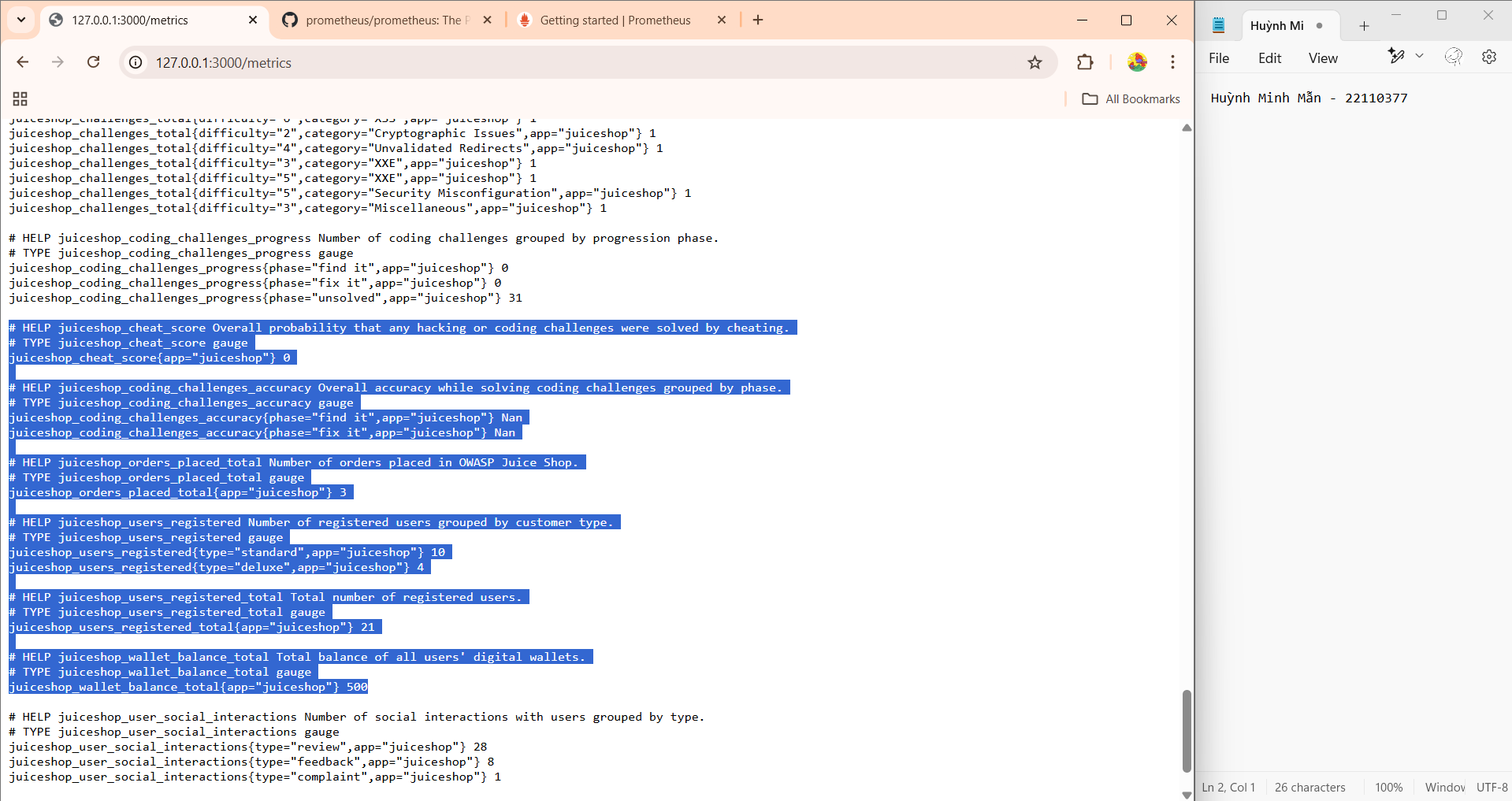


Kéo xuống phía dưới sẽ thấy ../metrics, thêm ../metrics vào url:

<http://127.0.0.1:3000/metrics>

Nếu truy cập thành công, bạn sẽ thấy một trang hiển thị dữ liệu dạng text, chứa các thông số như CPU, bộ nhớ, số lượng request, v.v.

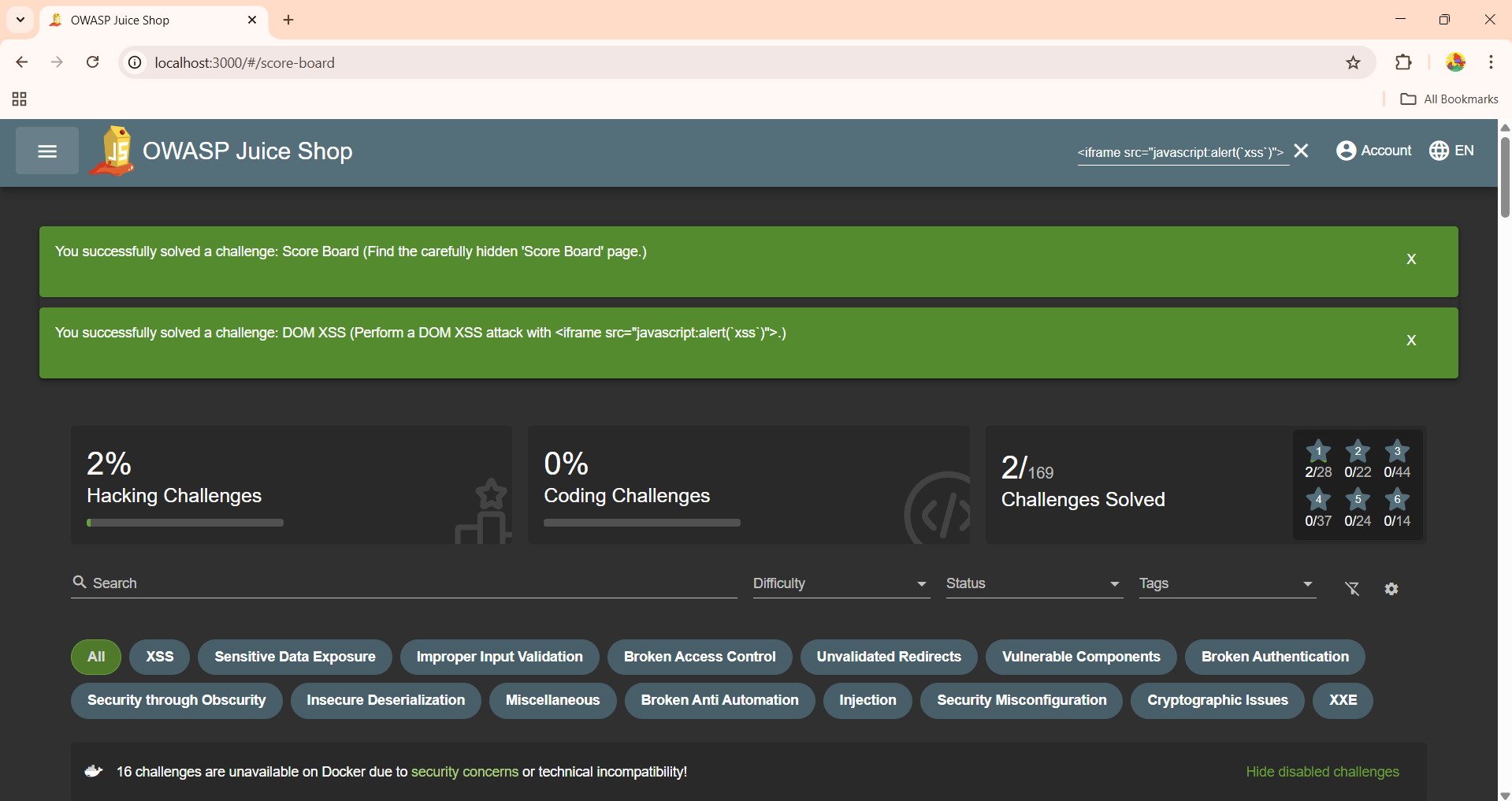
Sau khi mở trang /metrics, quay lại Juice Shop và bài tập sẽ được đánh dấu là hoàn thành.



1. **Mass Dispel**

Bài tập này yêu cầu người dùng đóng tất cả thông báo xuất hiện trên giao diện Juice Shop cùng một lúc.

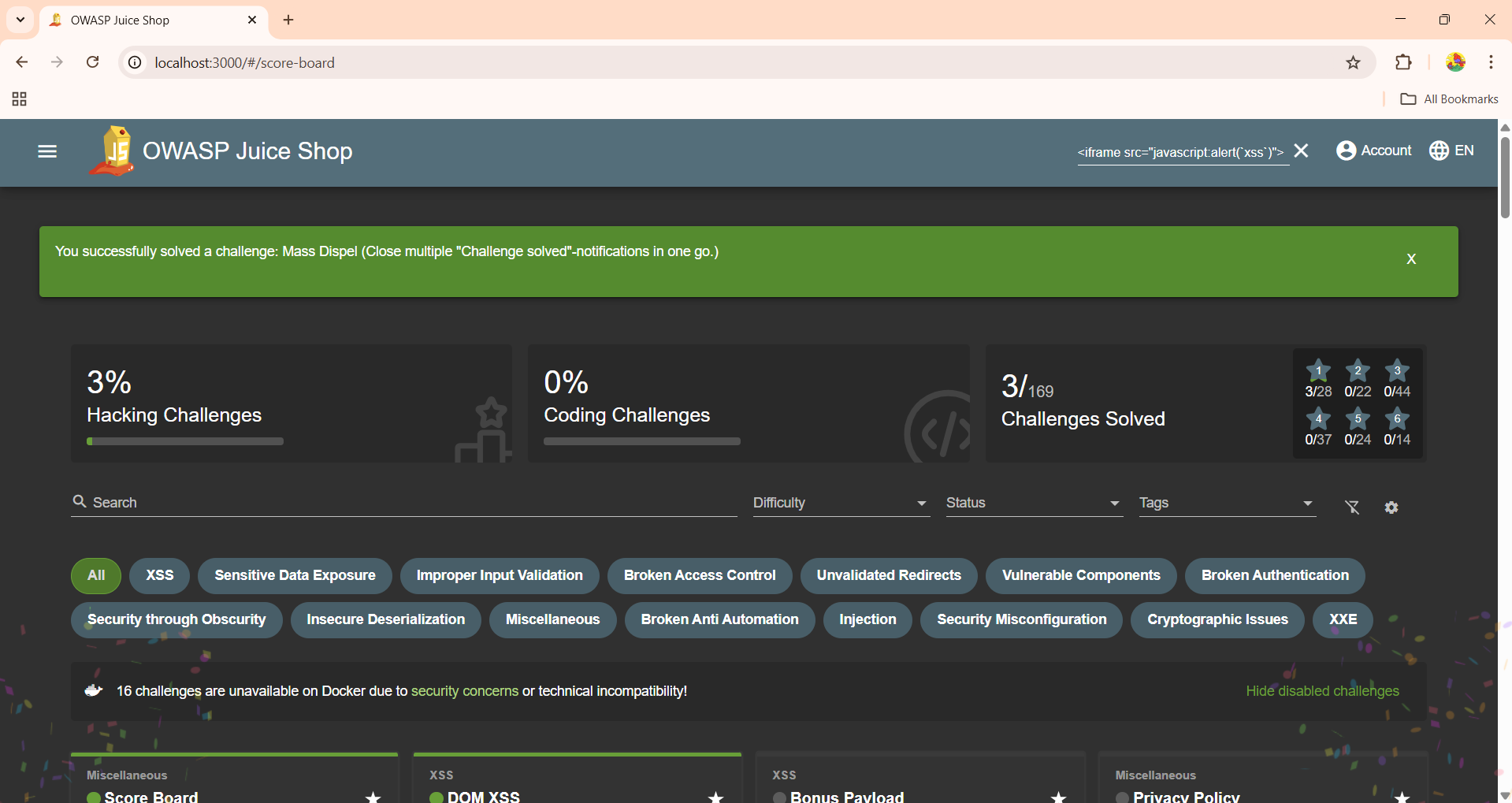
Khi thực hiện các thử thách trong Juice Shop, hệ thống sẽ hiển thị các thông báo xác nhận (toasts/alerts) ở góc trên màn hình.



Nhấn tổ hợp phím Shift + X để kích hoạt chế độ xóa hàng loạt.

Nhấp vào dấu X trên bất kỳ thông báo nào.

Ngay lập tức, tất cả các thông báo sẽ bị đóng, và bài tập sẽ được đánh dấu hoàn thành.

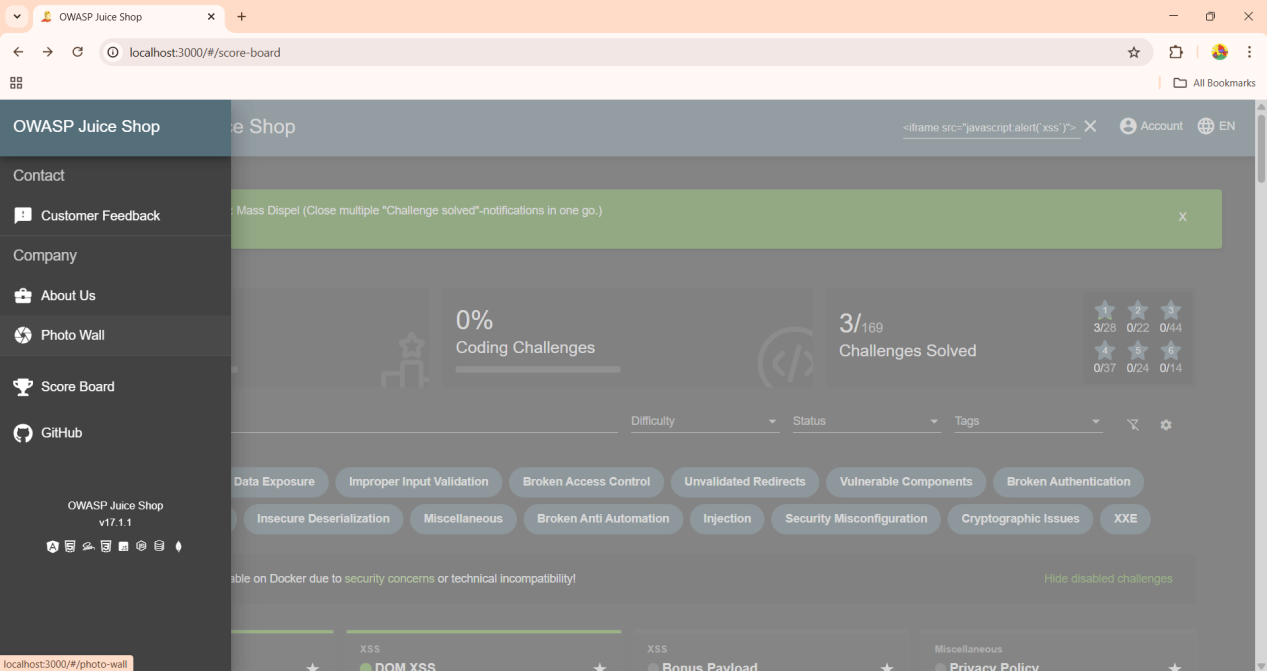


1. **Missing Encoding**

**Retrieve the photo of Bjoern's cat in "melee combat-mode".**

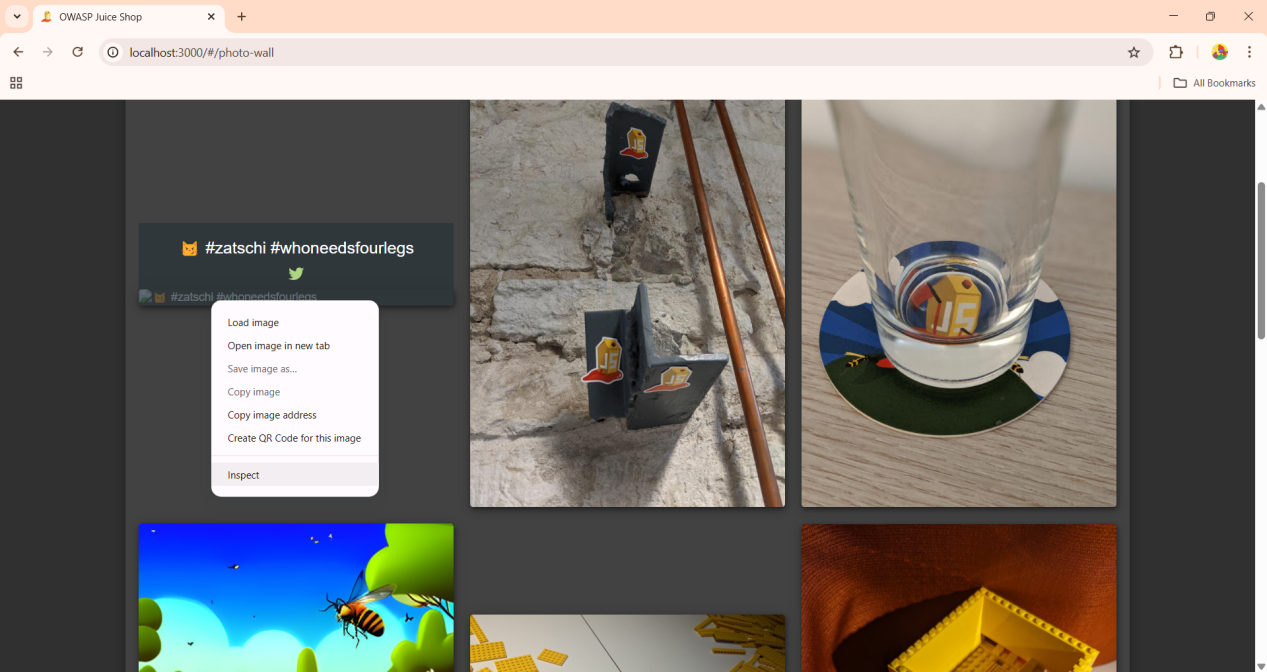
Bài tập này yêu cầu người dùng lấy ảnh của Bjoern's cat trong chế độ "melee combat-mode" bằng cách khai thác lỗi URL encoding.

Đầu tiên, ta truy cập vào phần Photo Wall, nơi hiển thị danh sách các hình ảnh được tải lên.

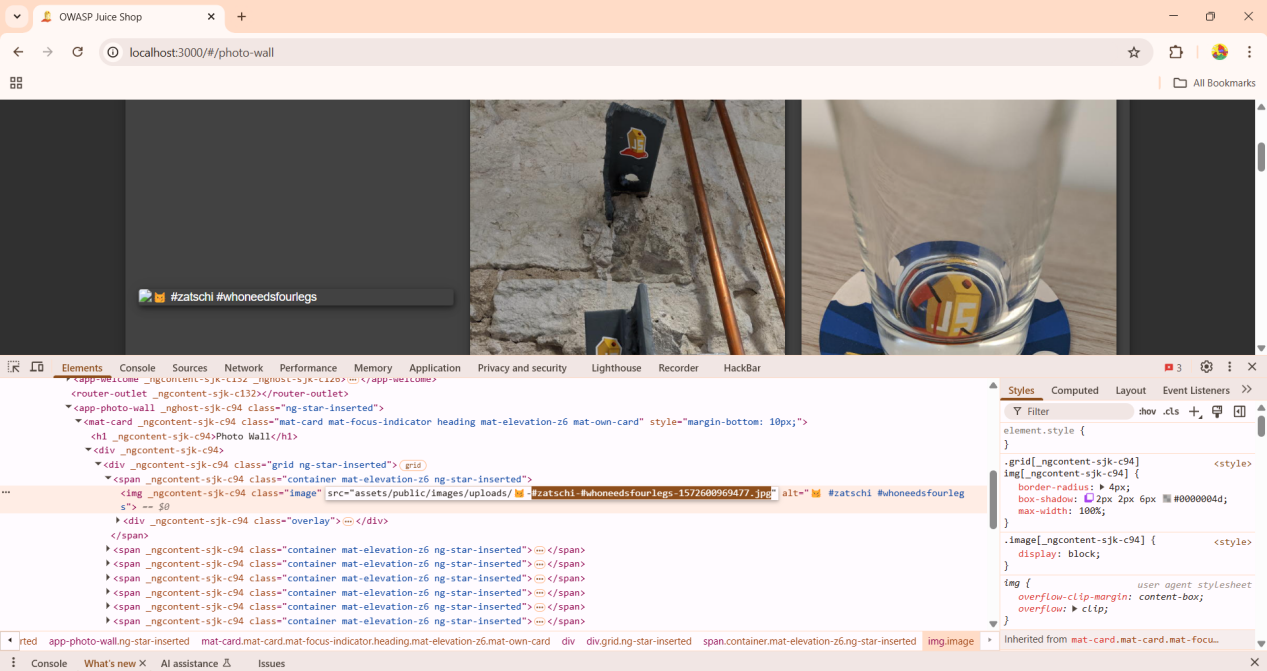


Nhấp chuột phải vào tiêu đề của một ảnh có tên chứa ký tự #, sau đó chọn Inspect (F12).

Trong thẻ HTML, ta sẽ thấy URL của ảnh chứa dấu # trong đường dẫn.

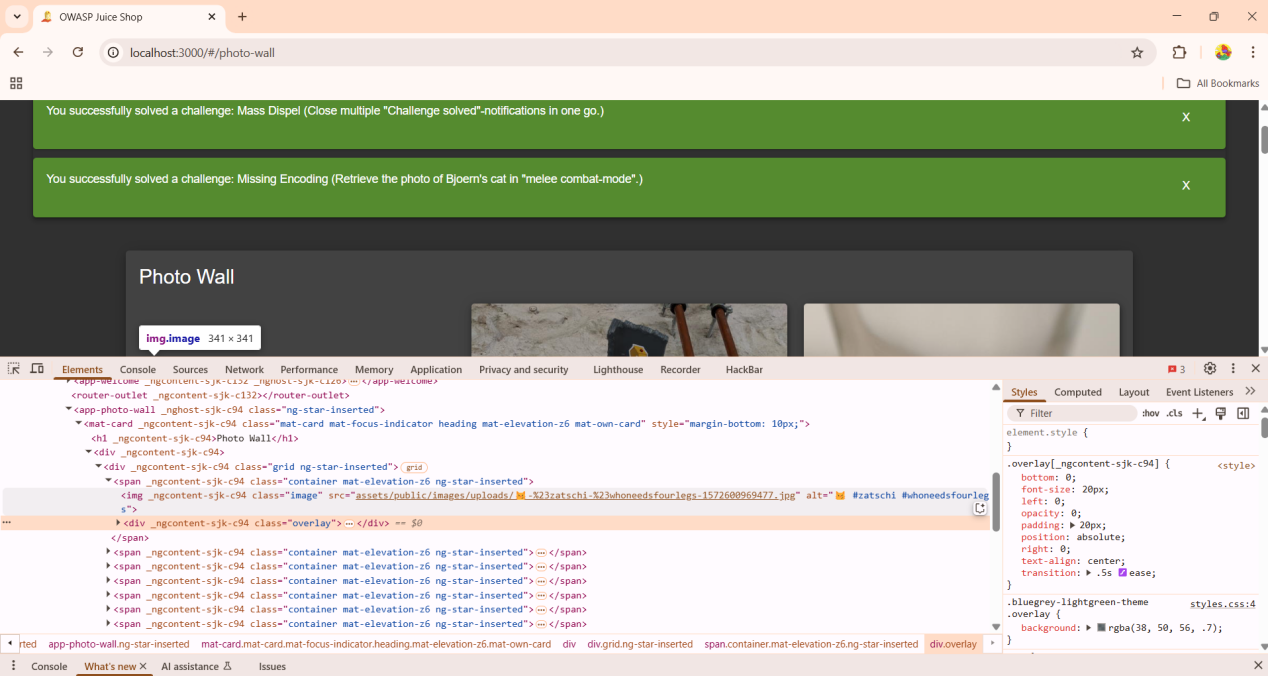


Xóa 2 dấu # trong đường dẫn.



Thay thế dấu # bằng %23 (vì %23 là mã URL encoding của ký tự #).

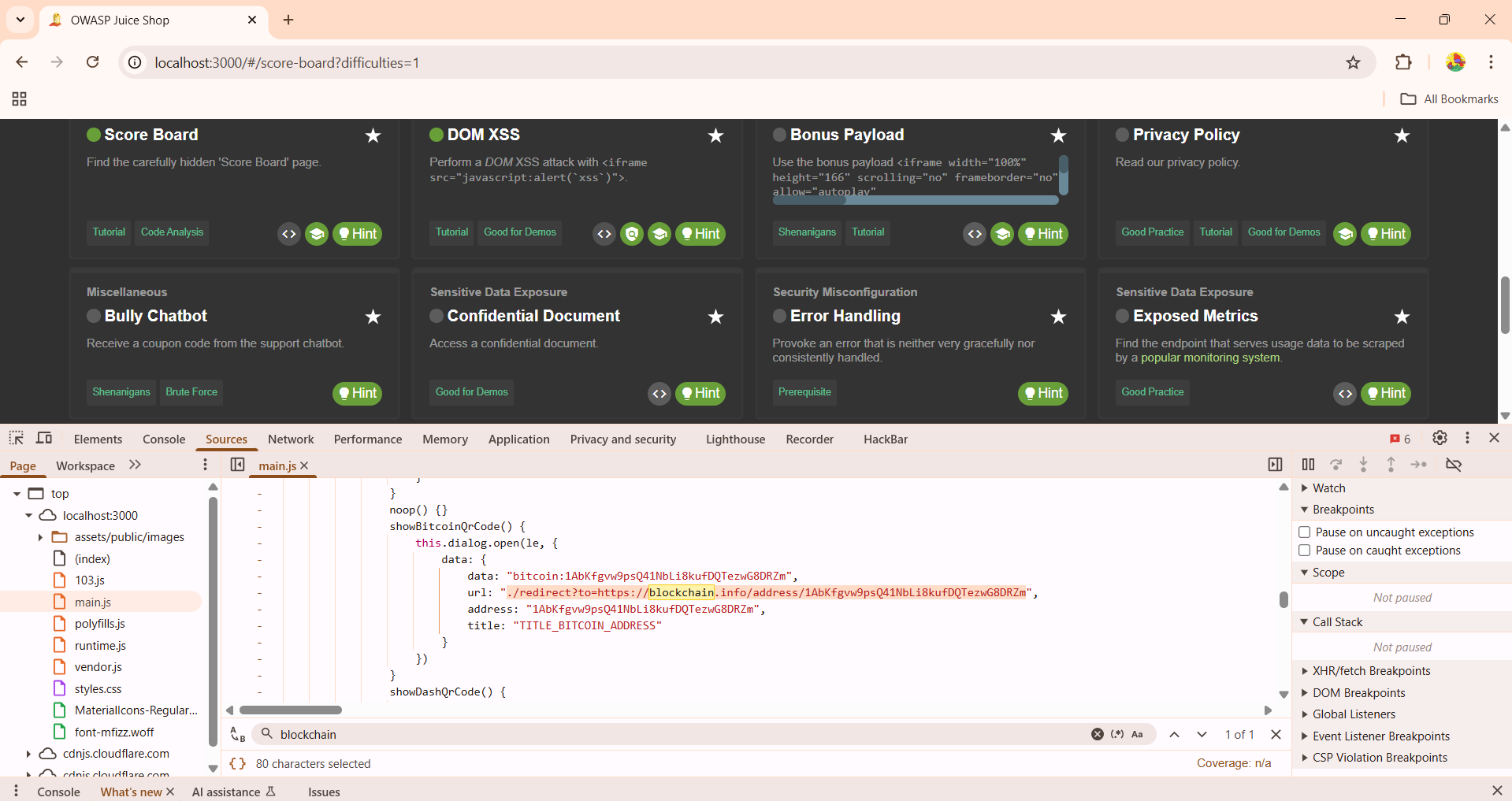
Nhấn Enter để tải lại trang với URL đã chỉnh sửa. Nếu ảnh xuất hiện đúng cách, hệ thống sẽ đánh dấu bài tập hoàn thành.



1. **Outdated Allowlist**

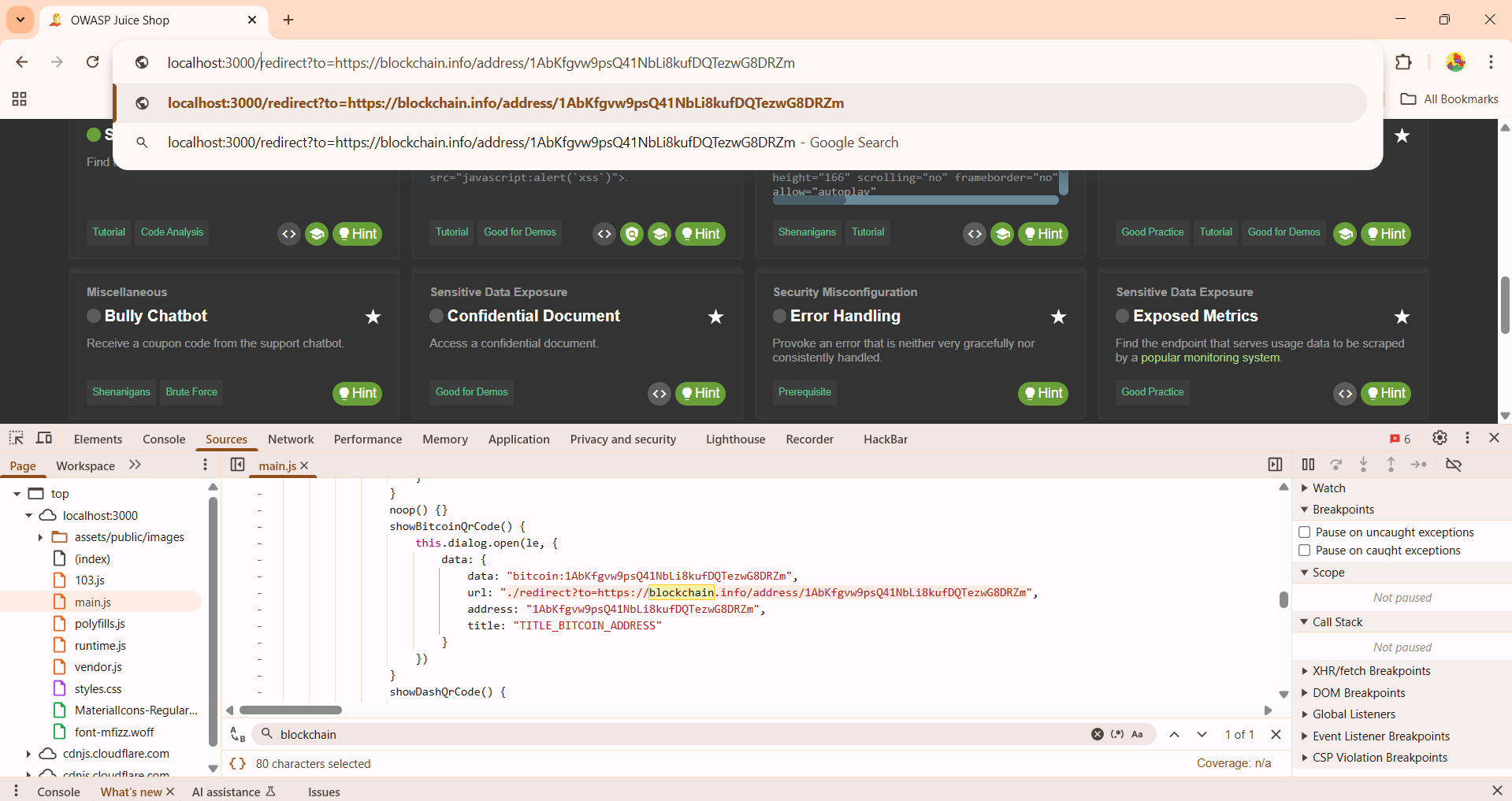
Bài tập này yêu cầu người dùng khai thác một lỗ hổng liên quan đến allowlist URL redirect, để truy cập một trang bên ngoài từ Juice Shop.

Đầu tiên, nhấn F12 để mở Inspect, vào tab Sources, tìm tệp main.js, tìm kiếm từ khóa "blockchain", kết quả sẽ hiển thị một URL ./redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm.

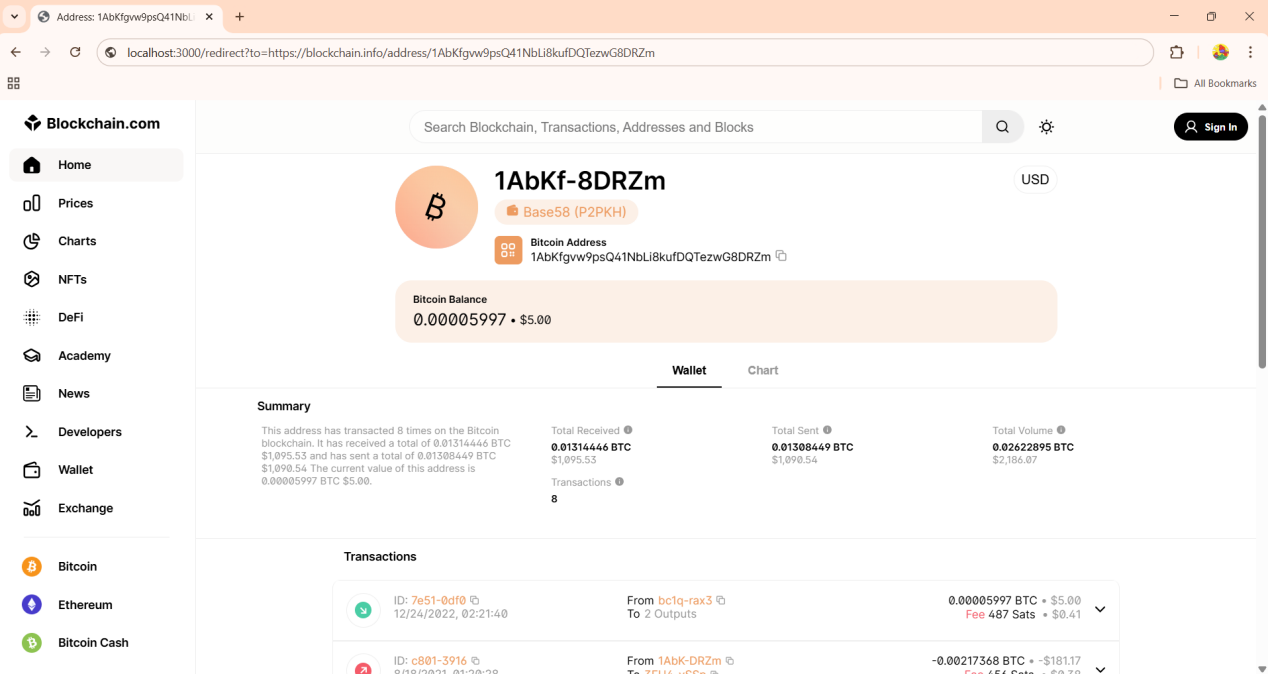


Truy cập vào Score Board và sao chép URL hiện tại:

<http://localhost:3000/#/score-board?difficulties=1> thay thế bằng URL khai thác [http://localhost:3000/redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm](http://localhost:3000/redirect?to=https:/blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm)

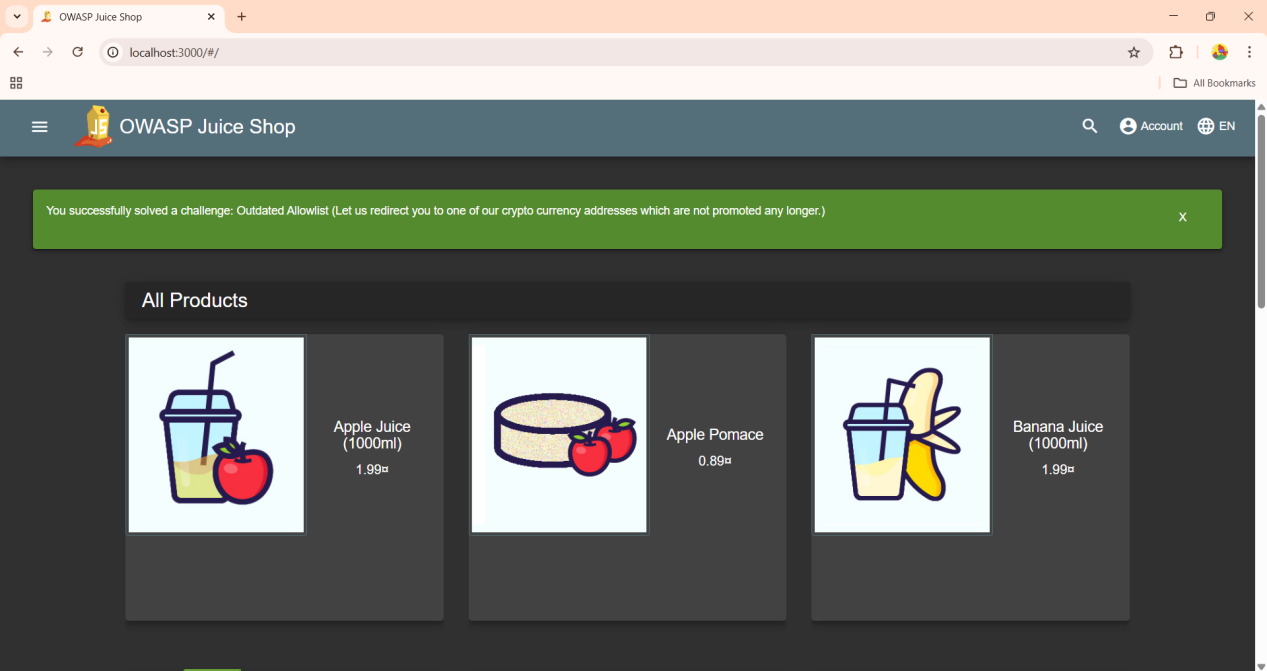


Sau khi nhấn Enter để truy cập, một trang web bên ngoài (blockchain.info) sẽ xuất hiện.



Quay lại trang Juice Shop <http://localhost:3000/#/>

Bài tập sẽ được đánh dấu là hoàn thành.

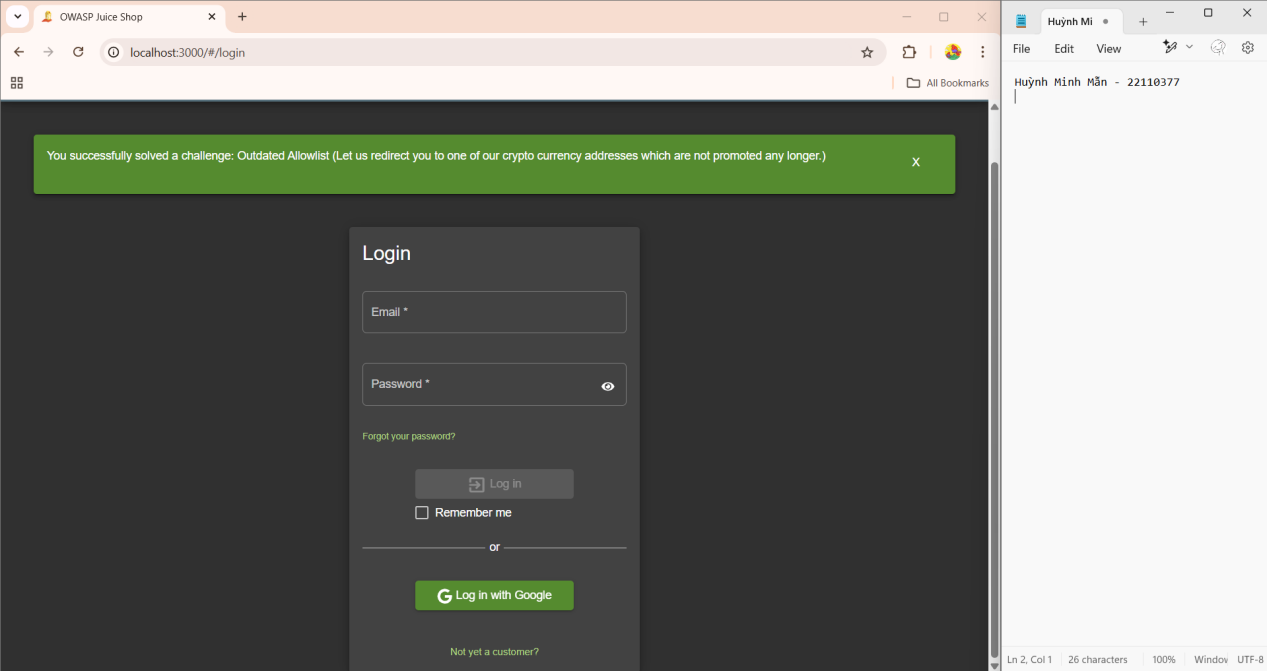


1. **Repetitive Registration**

Bài tập này yêu cầu người dùng khai thác lỗ hổng liên quan đến đăng ký trùng lặp, bằng cách đăng ký lại một tài khoản đã tồn tại theo cách đặc biệt để vượt qua hệ thống kiểm tra.

Truy cập Account trên giao diện.

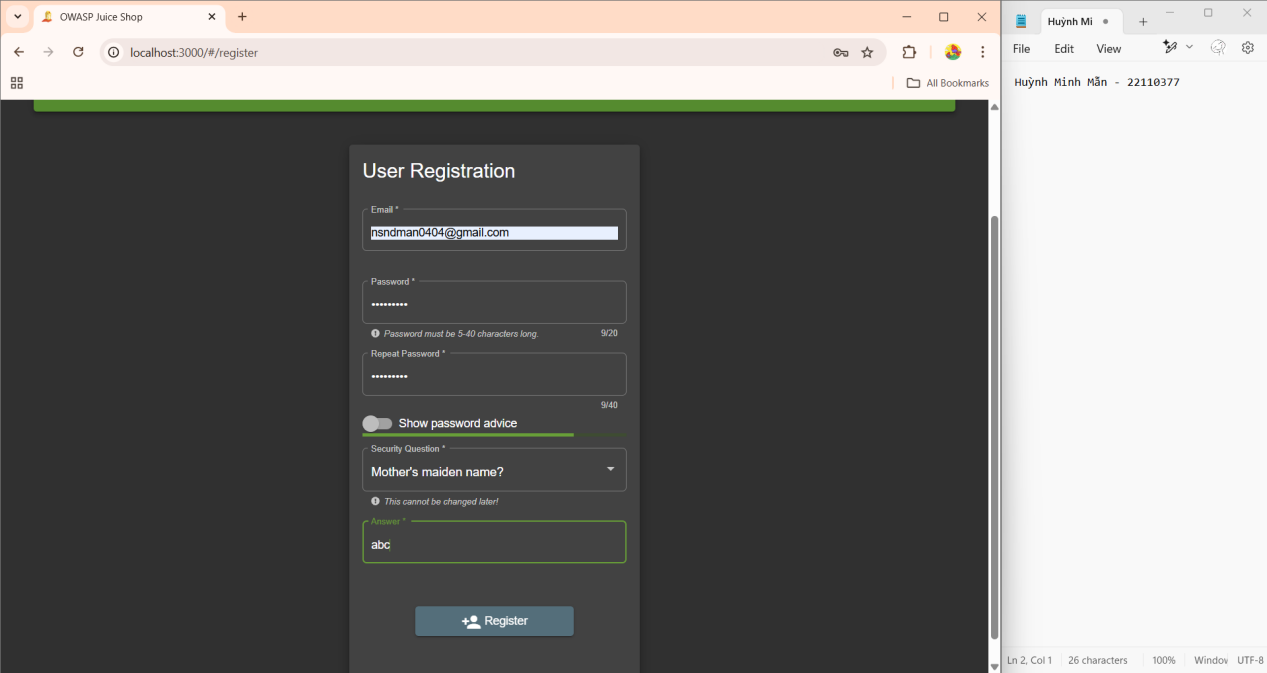
Nhấn Login, sau đó chọn Not yet a customer? để tạo tài khoản.



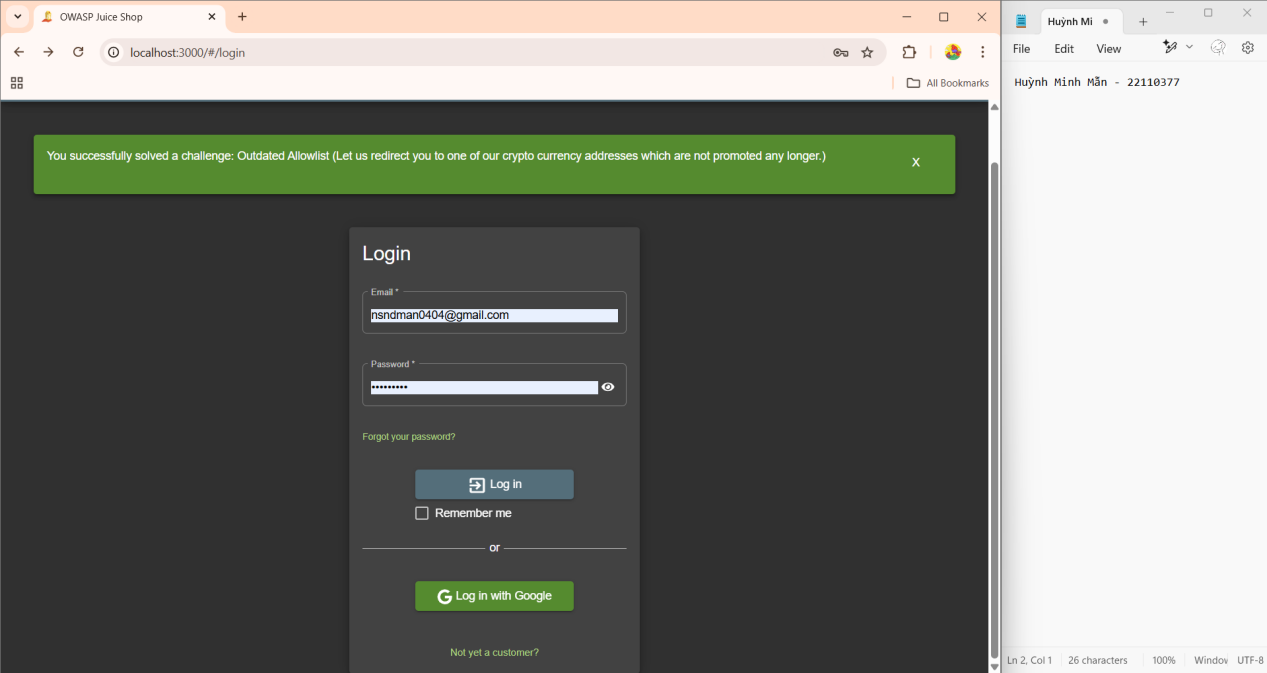
Ấn vào Not yet a customer?

Đăng ký 1 tài khoản

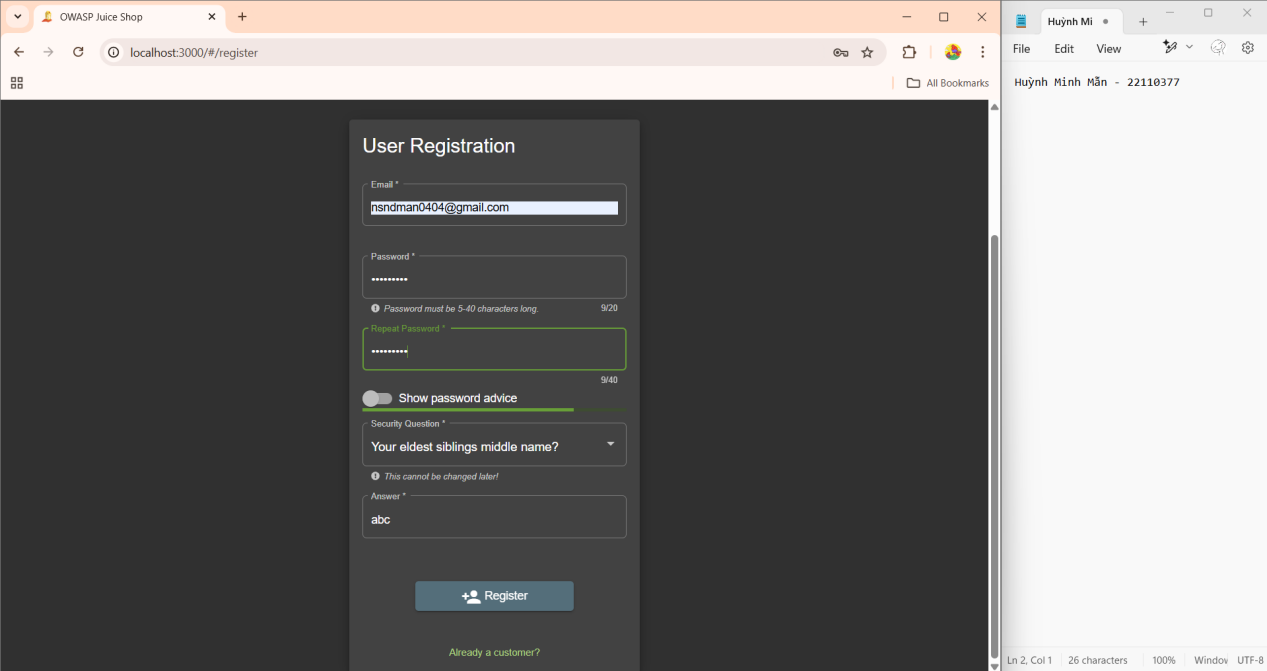
Nhấn Register để tạo tài khoản thành công.



Tiến hành login với tài khoản vừa đăng ký



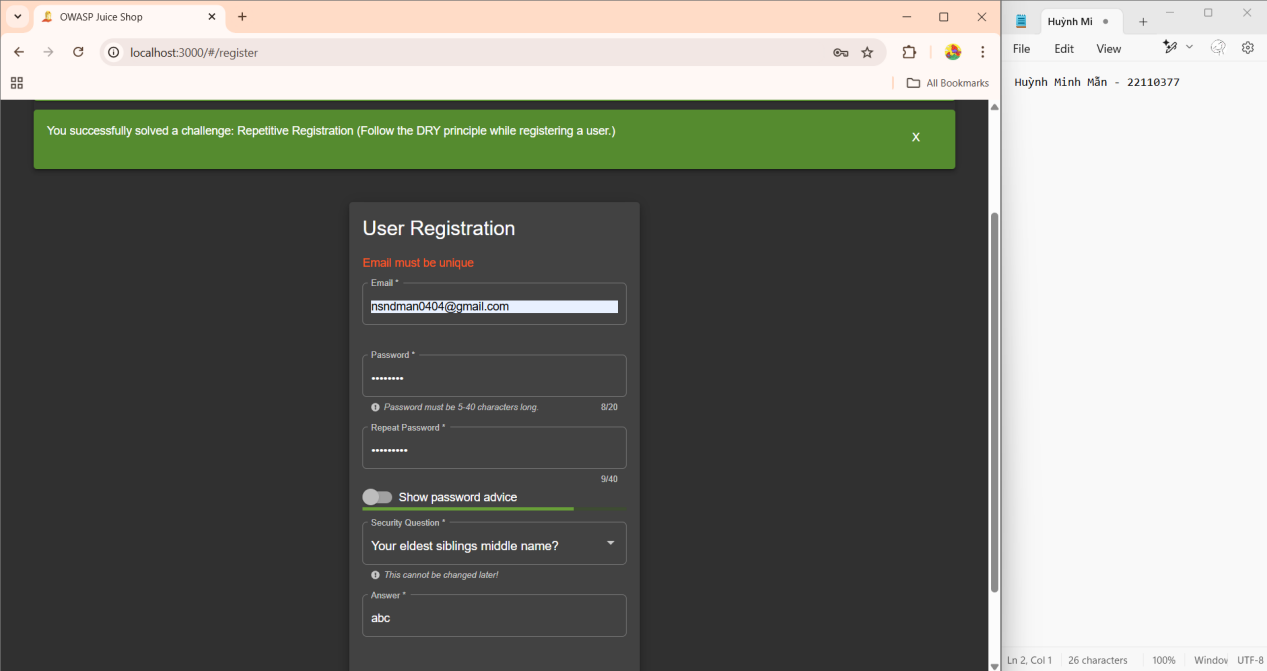
Tiếp tục đăng ký tài khoản với thông tin tài khoản vừa tạo



Tiếp tục đăng ký tài khoản với cùng địa chỉ email vừa tạo (nsndman0404@gmail.com).

Hệ thống sẽ báo Email must be unique.

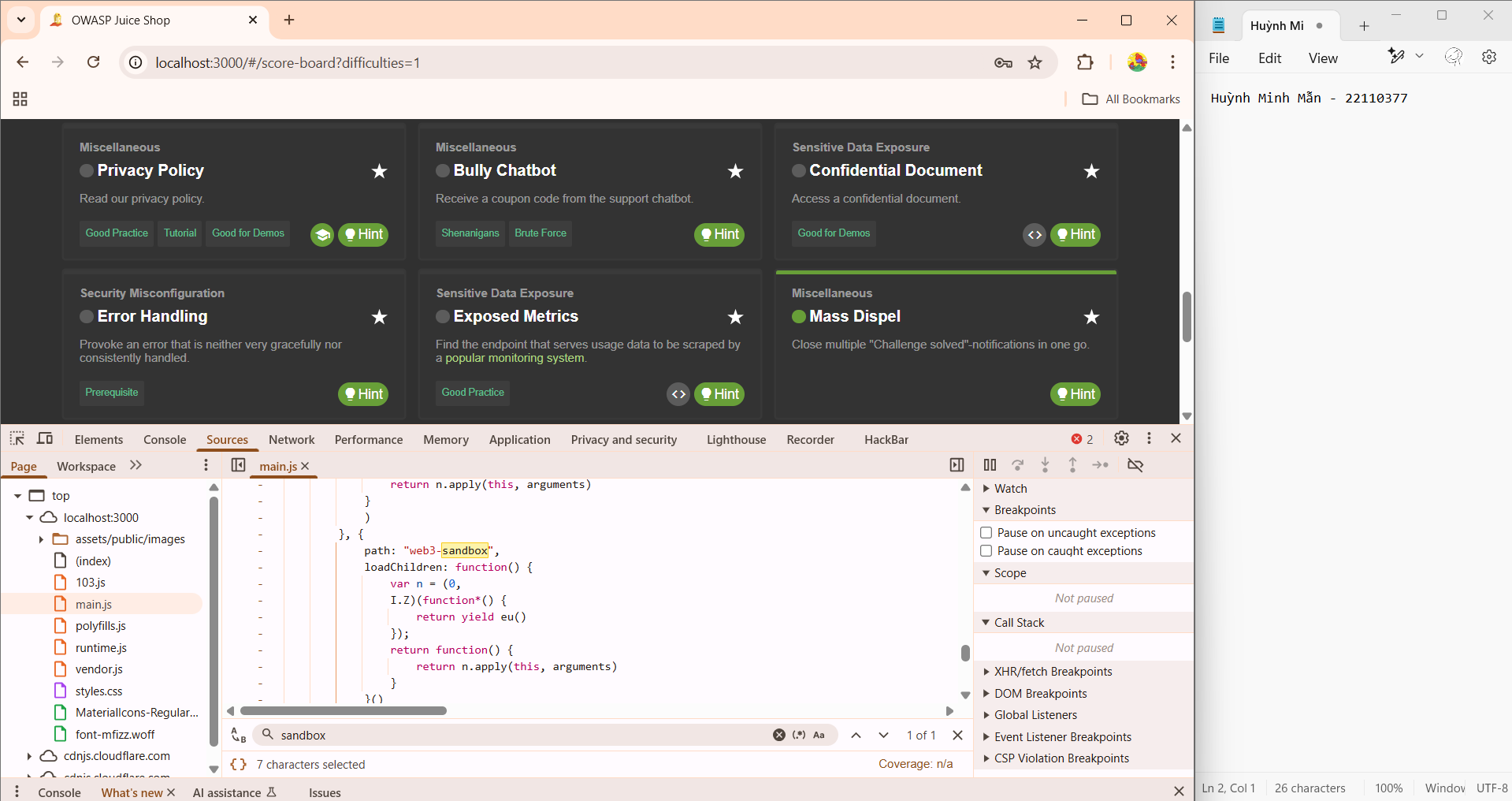
Khai thác lỗi bằng cách thay đổi mật khẩu: nhập mật khẩu mới nhưng Password và Repeat Password phải khác nhau, nhấn Register. Nếu hệ thống chấp nhận đăng ký (mặc dù mật khẩu không khớp), bài tập sẽ được đánh dấu hoàn thành.



1. **Web3 Sandbox**

Bài tập này yêu cầu người dùng tìm ra trang Web3 Sandbox ẩn trong hệ thống, thông qua phân tích mã nguồn của trang web.

Đầu tiên, mở DevTools bằng cách nhấn F12, chuyển đến tab Sources.

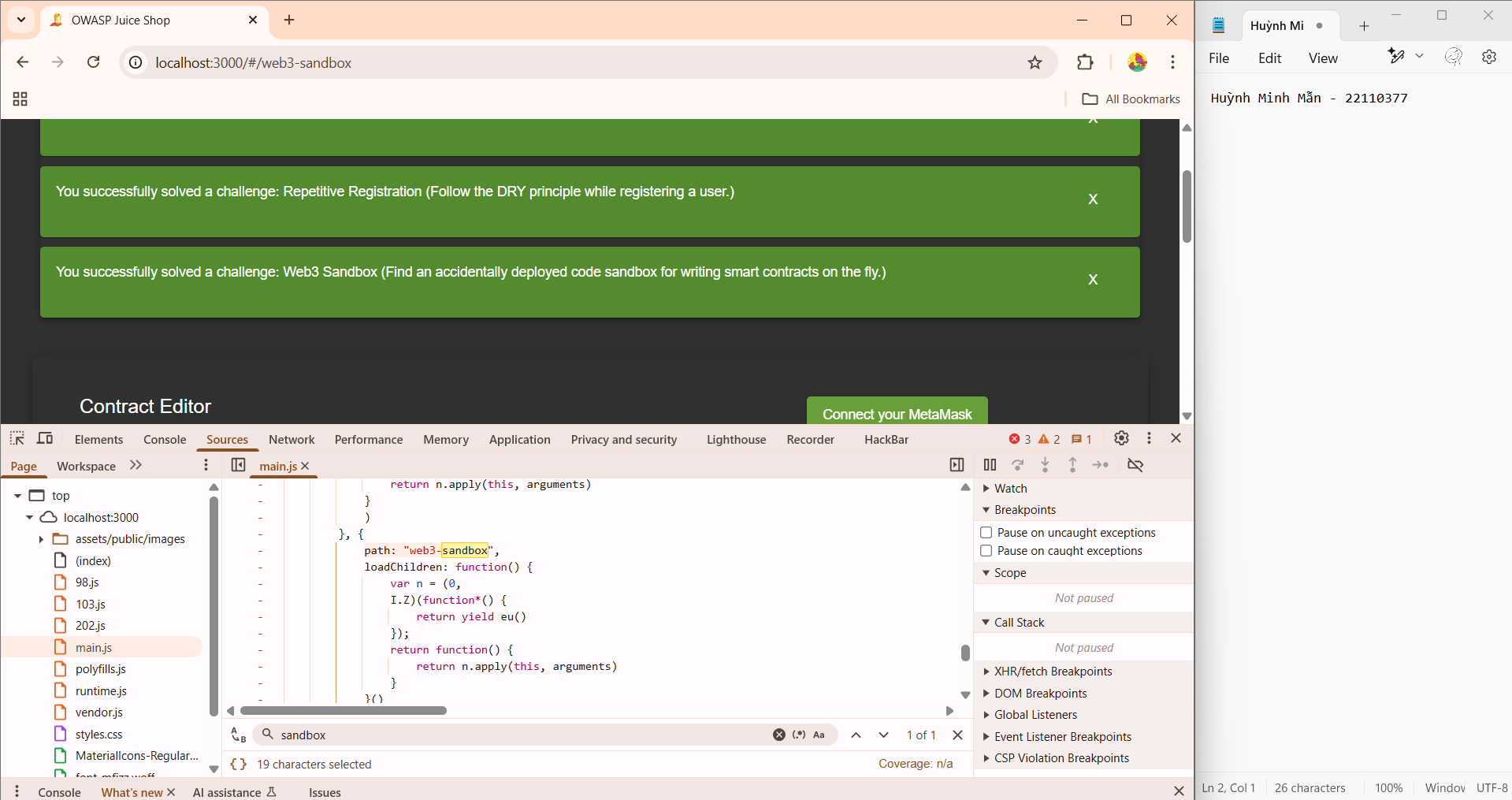
Tìm tệp main.js, sử dụng Ctrl + F để tìm kiếm từ khóa "sandbox". 

Lúc này ta thấy đường dẫn path được tìm thấy là path: "web3-sandbox", ta copy đường dẫn trên vào url đang có:

<http://localhost:3000/#/score-board?difficulties=1> ->

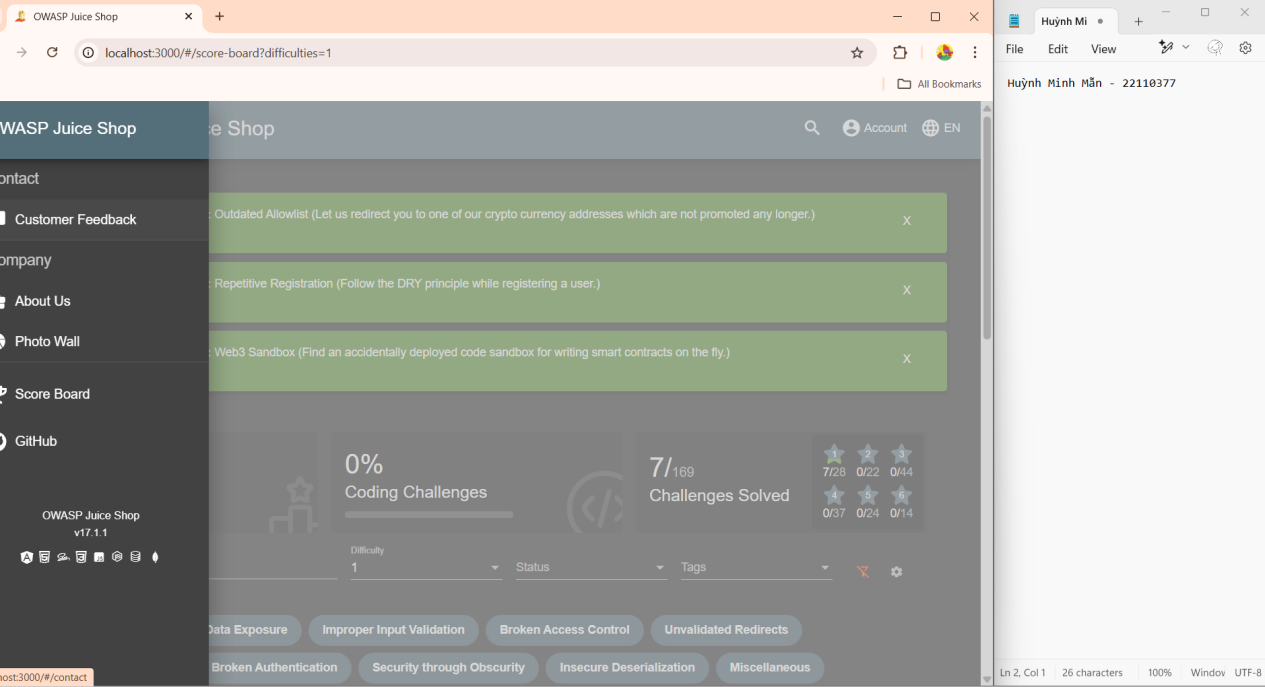
[http://localhost:3000/#/web3-sandbox](http://localhost:3000/#/score-board?difficulties=1)

Nhấn Enter, và trang Web3 Sandbox sẽ mở ra, bài tập được hoàn thành.

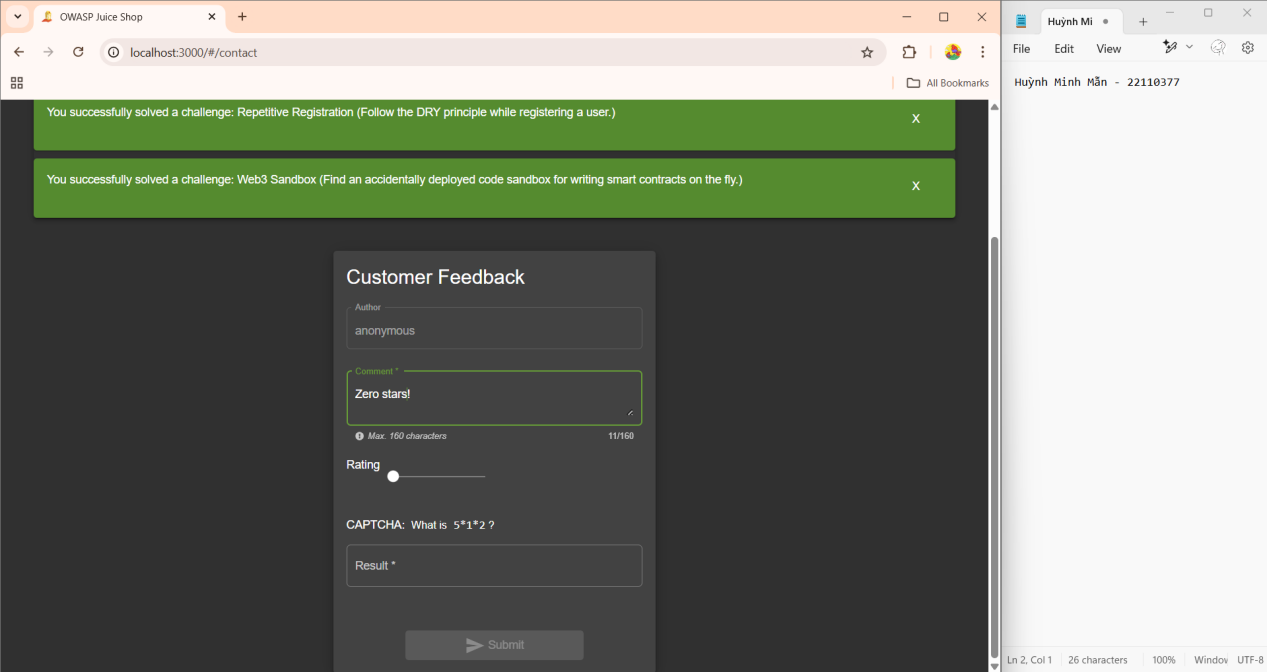


1. **Zero Stars**

Bài tập này yêu cầu người dùng gửi đánh giá với nội dung "Zero stars!", dù hệ thống không cho phép.

Truy cập vào Customer Feedback trên giao diện. 

Với comment ta nhập “Zero stars!” và captcha nhập đáp án sau khi tính toán



Mở DevTools (F12), sau đó: dùng công cụ chọn phần tử (Ctrl + Shift + C), trỏ vào nút Submit, tìm thuộc tính disabled="true" trong HTML của nút này.

Xóa thuộc tính disabled="true" để kích hoạt nút Submit.



Nhấn Submit, bài tập hoàn thành.

