**INSECURE BANK**

**REPORT**

1. **SQL Injection**

Tiếp cận trang web, ta được yêu cầu phải đăng nhập để truy cập trang chủ:

A screenshot of a computer

AI-generated content may be incorrect.

*Trang đăng nhập của ứng dụng*

Tuy đã được cung cấp tài khoản john:test, nhưng chúng ta vẫn sẽ kiểm tra xem chức năng login có tồn tại lỗ hổng hay không, ta sẽ kiểm tra SQL injection bằng cách nhập dấu ‘:

A screenshot of a computer

AI-generated content may be incorrect.

*Ứng dụng phản hồi thông báo sai tài khoản*

Ứng dụng trả về thông báo “Invalid username or password”, ta vẫn chưa khẳng định được ứng dụng có lỗ hổng SQL injection hay không, ta sẽ tiến hành sử dụng Burp Suite để thử một payload khác, ở đây là john’-- :

A screenshot of a computer

AI-generated content may be incorrect.

*Sử dụng Burp Suite để gửi request*

Tiến hành xem response bằng trình duyệt thì thấy ta đã đăng nhập thành công:

A screenshot of a computer

AI-generated content may be incorrect.

*Trang chủ của ứng dụng*

Chứng tỏ rằng ứng dụng có lỗ hổng SQL injection ở trang đăng nhập.

1. **IDOR**

A screenshot of a computer

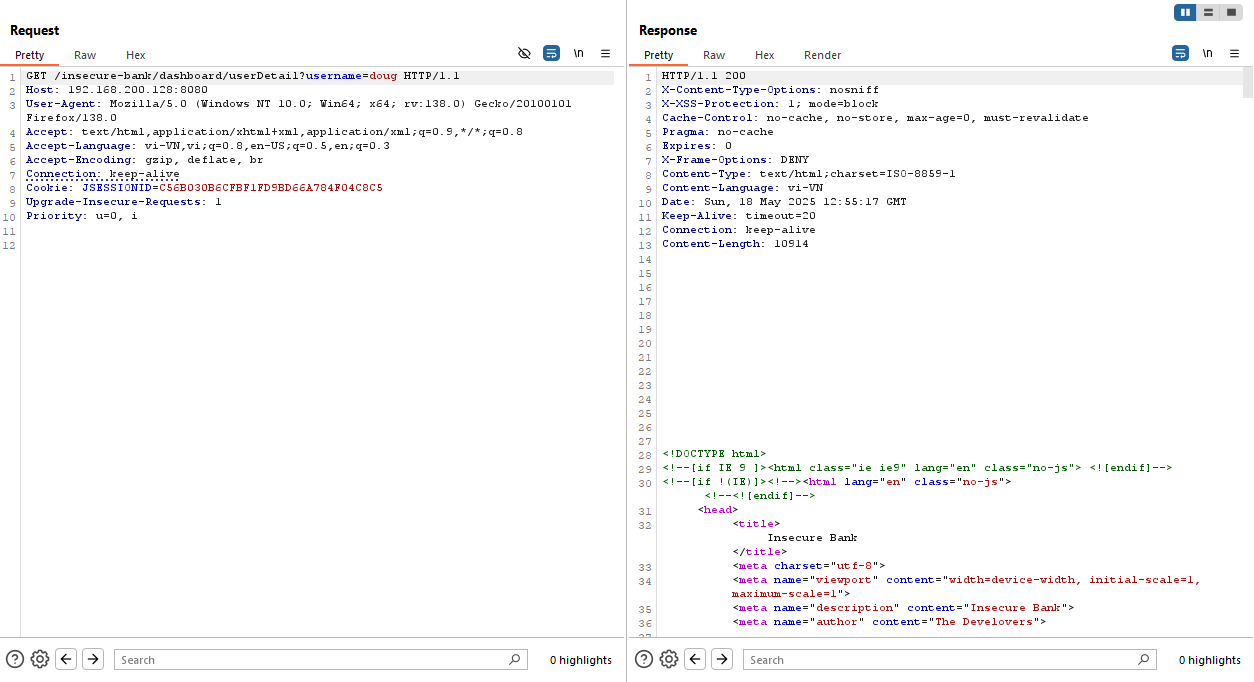
AI-generated content may be incorrect.

*Profile của người dùng*

Ở phần profile, chúng ta thấy có một tham số username ở URL.

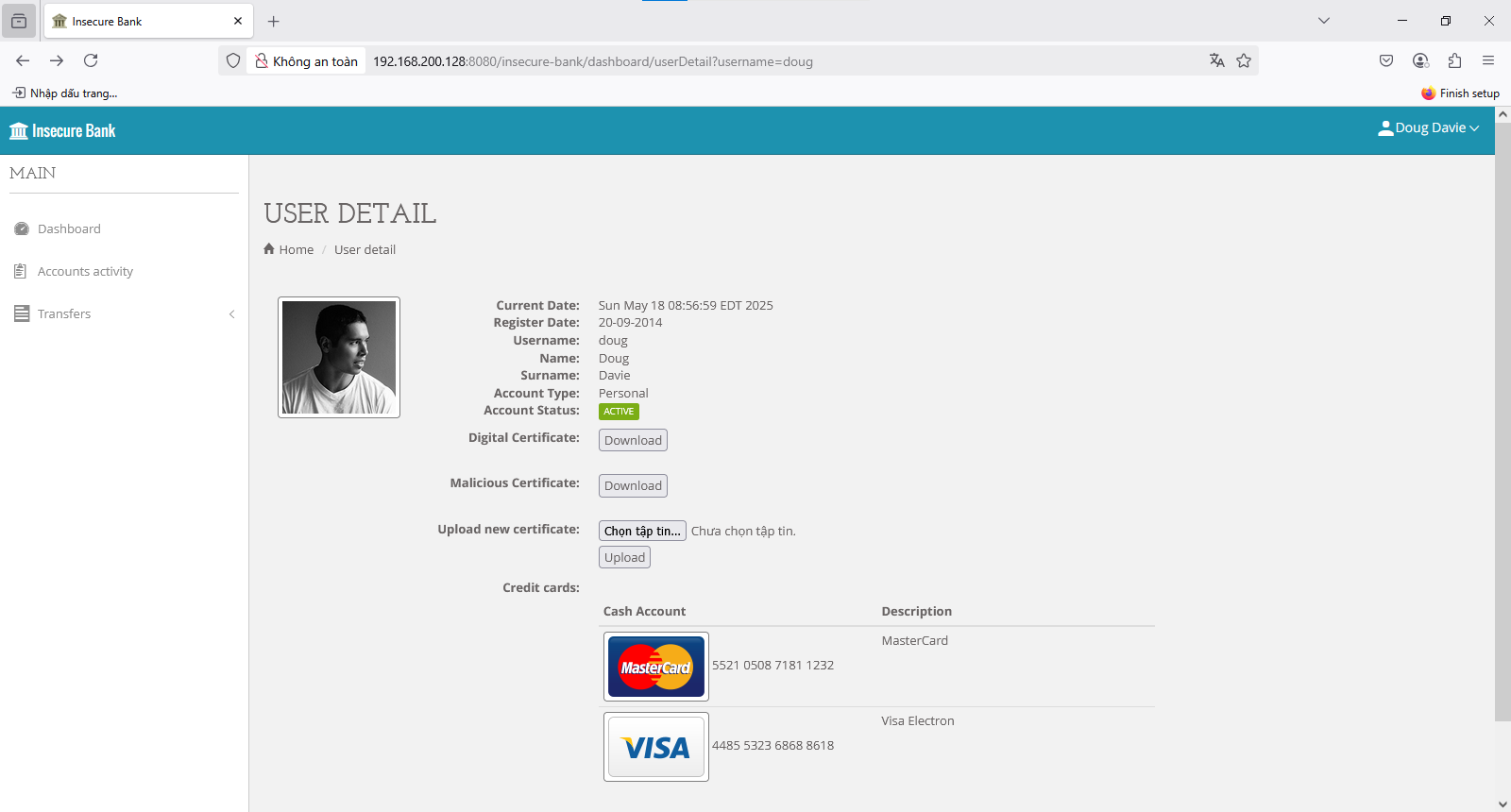
Chúng ta sẽ thực hiện gửi một tên người dùng khác vào tham số này để xem có lỗ hổng IDOR xuất hiện hay không.

Ở đây ta sẽ lấy tên người dùng doug, sử dụng Burp Suite để gửi request:



*Gửi request với Burp Suite*

Kiểm tra response trên trình duyệt:



*Profile của người dùng Doug*

Chúng ta đã thành công truy cập tài khoản của người dùng Doug.

1. **Stored XSS**

Ứng dụng có một chức năng cho phép chúng ta chuyển tiền cho các tài khoản khác:

A screenshot of a computer

AI-generated content may be incorrect.

*Chức năng chuyển tiền*

Ở đây, ta sẽ thử nhập bừa các thông tin để kiểm thử chức năng chuyển tiền này:

A screenshot of a computer

AI-generated content may be incorrect.

*Chức năng chuyển tiền*

Tiến hành nhấn Send, ta được chuyển tới một trang để xác nhận thông tin

A screenshot of a computer

AI-generated content may be incorrect.

*Xác nhận thông tin chuyển tiền*

Thực hiện nhấn Confirm và ta thành công thực hiện chức năng chuyển tiền:

A screenshot of a computer

AI-generated content may be incorrect.

*Chuyển tiền thành công*

Ở đây, ta thấy phần text foo chúng ta nhập vào description được lưu lại ở thông tin của giao dịch.

Chúng ta có thể xem các thông tin giao dịch trong phần Account Activity:

A screenshot of a computer

AI-generated content may be incorrect.

*Lịch sử giao dịch*

Nếu phần description không được xử lí đúng cách, ta có thể thực hiện stored XSS để đánh cắp các thông tin của người dùng mà ta thực hiện chuyển tiền.

Ta sẽ sử dụng Burp Suite để tạo ra một giao dịch khác, ở đây ta có một số tài khoản của một người dùng khác tên là Doug:

A screenshot of a computer

AI-generated content may be incorrect.

*Số tài khoản của người dùng Doug*

Ta sẽ thực hiện chuyển tiền tới tài khoản của người dùng Doug, và payload sẽ là <script>alert(1)</script>:

A screenshot of a computer

AI-generated content may be incorrect.

*Thực hiện gửi request với Burp Suite*

Thực hiện xem response ở trình duyệt và một bảng alert sẽ được hiện ra:

A screenshot of a computer

AI-generated content may be incorrect.

*Xuất hiện alert*

Chứng tỏ rằng phần description tồn tại lỗ hổng XSS, ta có thể thấy phần description của chúng ta không có thông tin, có nghĩa là đoạn script của chúng ta đã được inject vào HTML:

A screenshot of a computer

AI-generated content may be incorrect.

*Xác nhận thông tin giao dịch*

Nhấn confirm và giao dịch chúng ta sẽ thành công:

A screenshot of a computer

AI-generated content may be incorrect.

*Giao dịch thành công*

Khi này, nếu người dùng Doug nhấn vào phần Account Activity, payload XSS sẽ được kích hoạt:

A screenshot of a computer

AI-generated content may be incorrect.

*Payload kích hoạt thành công*

Đây là thông tin giao dịch chúng ta đã chuyển cho người dùng Doug:

A screenshot of a computer

AI-generated content may be incorrect.

*Lịch sử giao dịch của người dùng Doug*