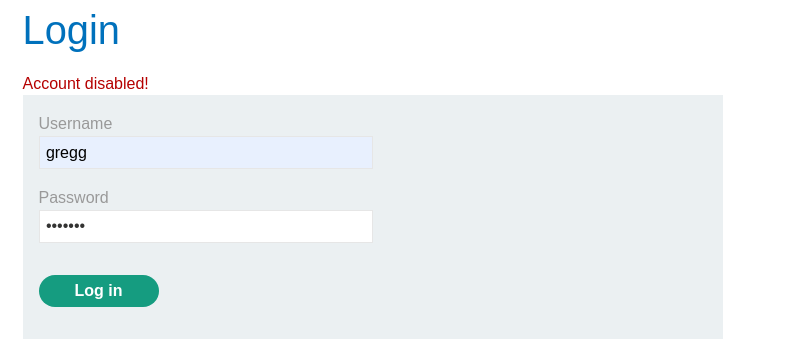
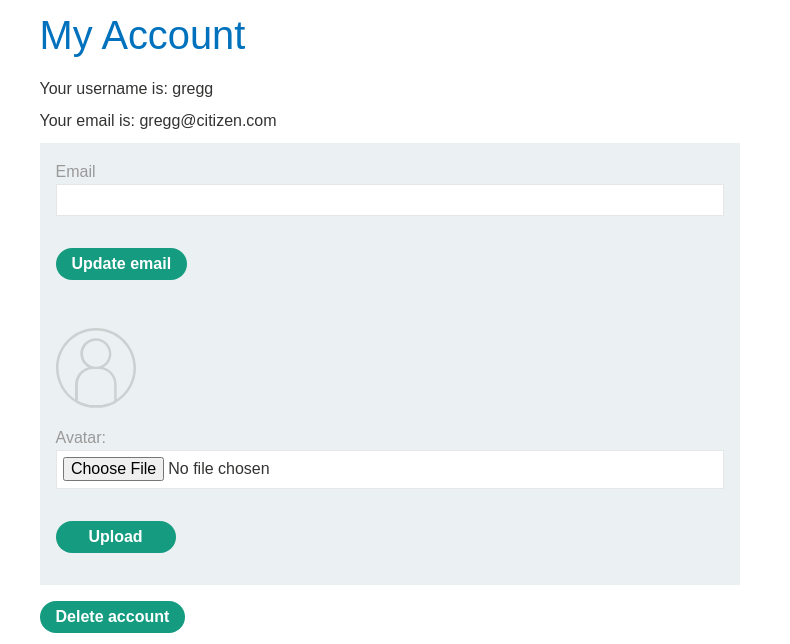
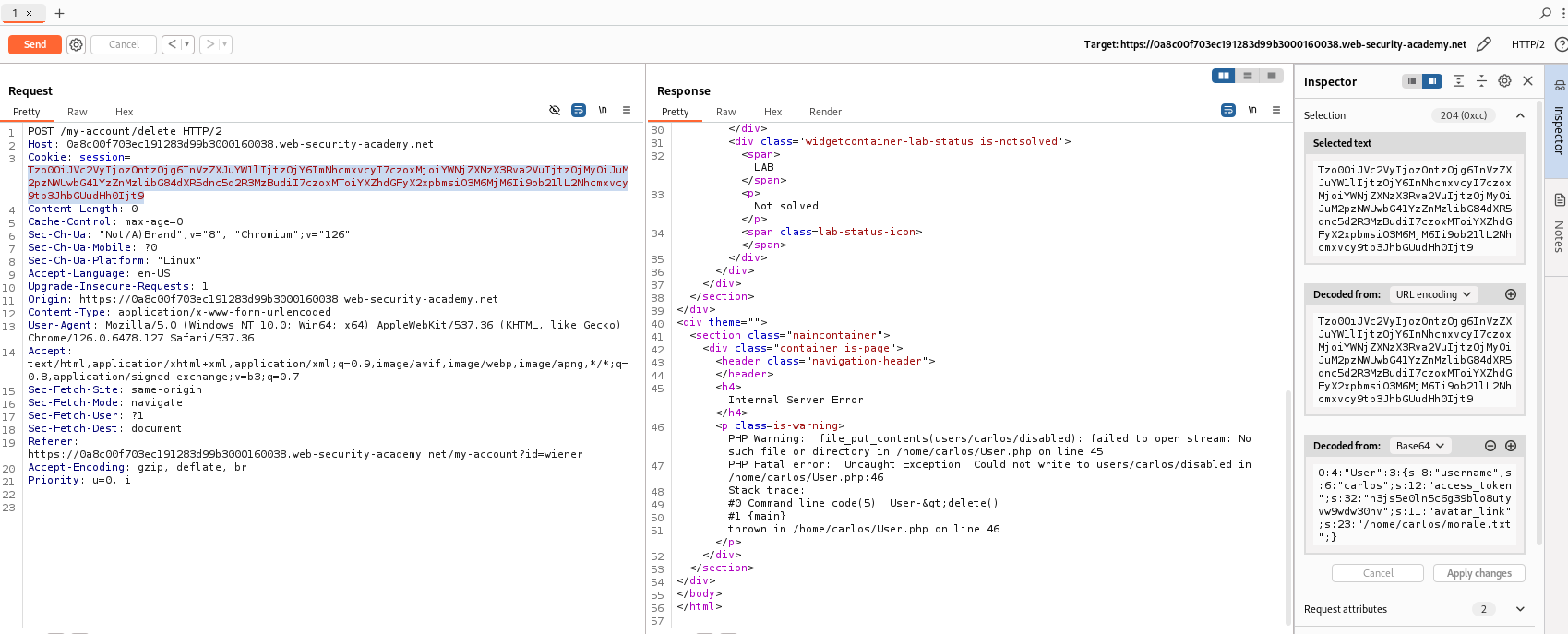
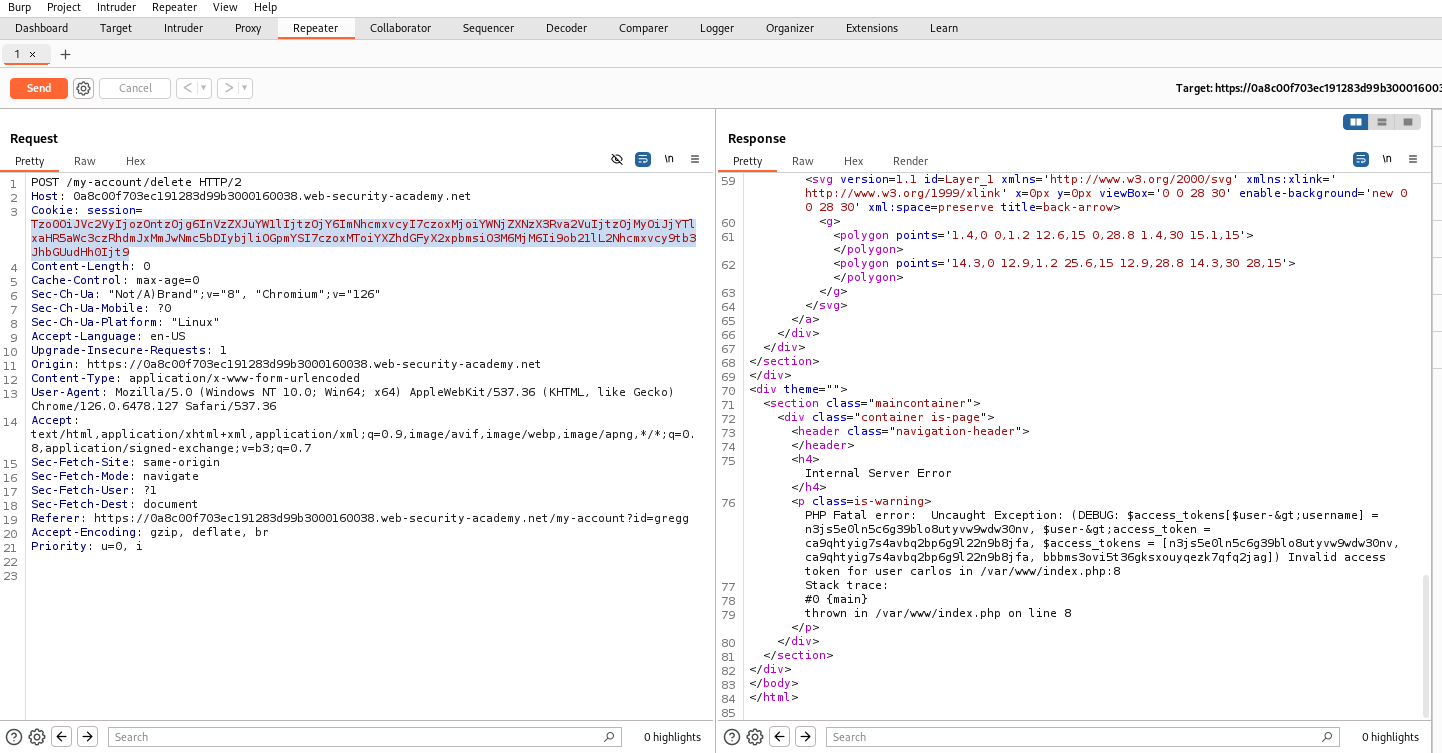
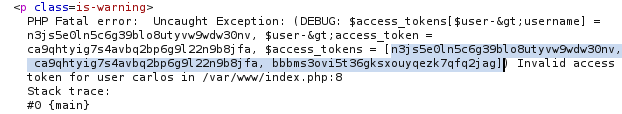
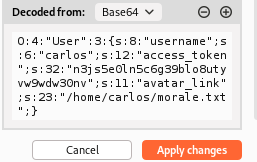
# Lab3: Using application functionality to exploit insecure deserialization

1. **NỘI DUNG CHỦ ĐỀ**
   1. **Đặc điểm và nguyên tắc hoạt động**
   * Tấn công này lợi dụng cơ chế session dựa trên serialization để thực hiện các hành động nguy hiểm thông qua dữ liệu được serialized.
   * Tin tặc có thể chỉnh sửa đối tượng serialized trong cookie để thực hiện các hoạt động không mong muốn như xóa tệp, thực thi mã độc.
   * Nguyên tắc hoạt động: Khi ứng dụng deserializes dữ liệu không an toàn từ người dùng, tin tặc có thể thay đổi dữ liệu đó để gây ra các hành động không mong muốn trên máy chủ.
   1. **Phương pháp ngăn chặn**
   * Kiểm tra và xác thực dữ liệu được deserialized trước khi sử dụng.
   * Sử dụng cơ chế mã hóa và chữ ký số để đảm bảo tính toàn vẹn của dữ liệu.
   * Hạn chế quyền truy cập của người dùng và thực hiện kiểm tra quyền truy cập ở phía máy chủ.
   * Sử dụng các thư viện hoặc frameworks bảo mật để quản lý quy trình serialization/deserialization an toàn.
2. **Các bước thực hiện bài Lab**
   1. **Mục tiêu**

Khai thác lỗ hổng trong cơ chế session của ứng dụng để xóa tệp morale.txt trong thư mục của người dùng Carlos.

* 1. **Thực hiện**
     + Đăng nhập tài khoản: gregg:rosebud
     + 
     + Click vào btn Delete để lấy session trong Burp suite
     + 
     + Send to repeater để giải và sửa mã: chuyển user thành carlos, và avartarlinks:11:"avatar\_link";s:23:"/home/carlos/morale.txt"
     + 
     + Sau khi sửa apply changes và send lại yêu cầu thì nó sẽ cho ra các access token mới
     + 
     + 
     + Ta thay mã đó vào session đã được giải bởi base64
     + 
  2. **Kết quả**

Đã xóa thành công tệp morale.txt của người dùng Carlos thông qua việc khai thác lỗ hổng deserialization.

