

**Kiểm thử CƠ BẢN**

**LAB 7**



Giảng viên hướng dẫn: **Huỳnh Khắc Duy**

Lớp/Kỳ: SD18303/SPRING2024

Thành viên nhóm :

|  |  |  |
| --- | --- | --- |
| **Chức vụ** | **MSSV** | **Họ và Tên** |
| Trưởng nhóm | PS33069 | Nguyễn Quốc Khánh |
| Thành viên | PS28808 | Lê Đình Mẫn |
| Thành viên | PS28752 | Cao Ngọc Thái |
| Thành viên | PS26461 | Phạm Thế Tình |
| Thành viên | PS28794 | Phạm Văn Thiện |
| Thành viên | PS21469 | Nguyễn Thị Kim Yến |

**Câu 1:**

Dưới đây là một số trường hợp kiểm thử tính năng cho form Login:

1. **Trường hợp 1: Thông tin đăng nhập hợp lệ**
2. **Input:**
   * Username: "validusername"
   * Password: "validpassword"
3. **Kết quả mong đợi:**
   * Chuyển hướng đến màn hình tiếp theo.
4. **Trường hợp 2: Username trống**
5. **Input:**
   * Username: ""
   * Password: "validpassword"
6. **Kết quả mong đợi:**
   * Hiển thị thông báo lỗi "Username không được để trống."
7. **Trường hợp 3: Password trống**
8. **Input:**
   * Username: "validusername"
   * Password: ""
9. **Kết quả mong đợi:**
   * Hiển thị thông báo lỗi "Password không được để trống."
10. **Trường hợp 4: Độ dài Username quá ngắn (dưới 3 ký tự)**
11. **Input:**
    * Username: "ab"
    * Password: "validpassword"
12. **Kết quả mong đợi:**
    * Hiển thị thông báo lỗi "Độ dài Username phải nằm trong khoảng 3 đến 30 ký tự."
13. **Trường hợp 5: Độ dài Username quá dài (trên 30 ký tự)**
14. **Input:**
    * Username: "usernamewithmorethan30characters"
    * Password: "validpassword"
15. **Kết quả mong đợi:**
    * Hiển thị thông báo lỗi "Độ dài Username phải nằm trong khoảng 3 đến 30 ký tự."
16. **Trường hợp 6: Độ dài Password quá ngắn (dưới 6 ký tự)**
17. **Input:**
    * Username: "validusername"
    * Password: "pass"
18. **Kết quả mong đợi:**
    * Hiển thị thông báo lỗi "Độ dài Password phải nằm trong khoảng 6 đến 10 ký tự."
19. **Trường hợp 7: Độ dài Password quá dài (trên 10 ký tự)**
20. **Input:**
    * Username: "validusername"
    * Password: "passwordtoolong"
21. **Kết quả mong đợi:**
    * Hiển thị thông báo lỗi "Độ dài Password phải nằm trong khoảng 6 đến 10 ký tự."
22. **Trường hợp 8: Username hoặc Password không chính xác**
23. **Input:**
    * Username: "invalidusername"
    * Password: "invalidpassword"
24. **Kết quả mong đợi:**
    * Hiển thị thông báo lỗi "Username hoặc Password đã nhập sai."
25. **Trường hợp 9: Kiểm tra sự bảo mật**
26. **Input:**
    * Username: "validusername"
    * Password: "validpassword"
27. **Kết quả mong đợi:**
    * Đảm bảo rằng thông tin đăng nhập không xuất hiện trong log hoặc URL.
28. **Trường hợp 10: Kiểm tra xử lý lỗi không mong muốn**
29. **Input:**
    * Dữ liệu đầu vào không hợp lệ, chẳng hạn như chứa các ký tự đặc biệt hoặc SQL injection.
30. **Kết quả mong đợi:**
    * Xử lý lỗi một cách an toàn và hiển thị thông báo phù hợp.

Lưu ý: Cần thực hiện kiểm thử cả trên giao diện người dùng và phía máy chủ để đảm bảo tính nhất quán và an toàn.

**Câu 2:**

Dưới đây là một số trường hợp kiểm thử tính năng cho chức năng tải ảnh lên (upload photos):

1. **Trường hợp 1: Tải ảnh đúng định dạng và kích thước**
2. **Input:**
   * Chọn một ảnh đúng định dạng (JPEG, GIF, hoặc PNG).
   * Kích thước của ảnh nhỏ hơn 100MB.
3. **Kết quả mong đợi:**
   * Ảnh được tải lên thành công và xuất hiện trên trang web.
4. **Trường hợp 2: Tải ảnh có định dạng không hợp lệ**
5. **Input:**
   * Chọn một ảnh với định dạng không hợp lệ (ví dụ: BMP).
6. **Kết quả mong đợi:**
   * Hiển thị thông báo lỗi "Định dạng ảnh không hợp lệ."
7. **Trường hợp 3: Tải ảnh với kích thước quá lớn**
8. **Input:**
   * Chọn một ảnh với kích thước lớn hơn 100MB.
9. **Kết quả mong đợi:**
   * Hiển thị thông báo lỗi "Kích thước ảnh quá lớn. Vui lòng chọn ảnh có kích thước nhỏ hơn 100MB."
10. **Trường hợp 4: Tải ảnh với cả định dạng và kích thước không hợp lệ**
11. **Input:**
    * Chọn một ảnh với định dạng không hợp lệ (ví dụ: TIFF) và kích thước lớn hơn 100MB.
12. **Kết quả mong đợi:**
    * Hiển thị thông báo lỗi "Định dạng ảnh không hợp lệ và Kích thước ảnh quá lớn. Vui lòng chọn ảnh có định dạng JPEG, GIF hoặc PNG và kích thước nhỏ hơn 100MB."
13. **Trường hợp 5: Tải lên nhiều ảnh cùng một lúc**
14. **Input:**
    * Chọn và tải lên nhiều ảnh cùng một lúc.
15. **Kết quả mong đợi:**
    * Hệ thống xử lý đúng mỗi ảnh và hiển thị thông báo thành công cho từng ảnh.
16. **Trường hợp 6: Tải ảnh với tên tệp lỗi**
17. **Input:**
    * Chọn ảnh và đặt tên tệp ảnh chứa các ký tự không hợp lệ hoặc khoảng trắng.
18. **Kết quả mong đợi:**
    * Hiển thị thông báo lỗi "Tên tệp ảnh không hợp lệ. Vui lòng sử dụng tên không chứa các ký tự đặc biệt hoặc khoảng trắng."
19. **Trường hợp 7: Tải ảnh trong khi hệ thống quá tải**
20. **Input:**
    * Cố gắng tải lên ảnh trong khi hệ thống đang quá tải.
21. **Kết quả mong đợi:**
    * Hiển thị thông báo lỗi "Hệ thống đang quá tải. Vui lòng thử lại sau."
22. **Trường hợp 8: Tải ảnh với lỗi không mong muốn**
23. **Input:**
    * Tải lên ảnh nhưng quá trình tải gặp lỗi không mong muốn.
24. **Kết quả mong đợi:**
    * Xử lý lỗi một cách an toàn và hiển thị thông báo lỗi chính xác.

Lưu ý: Cần kiểm thử cả trên giao diện người dùng và phía máy chủ để đảm bảo tính nhất quán và an toàn.

**Câu 4:**

Trong kiểm thử bảo mật cho form Login, chúng ta cần tập trung vào việc đảm bảo rằng hệ thống không bị lỗ hổng bảo mật và có khả năng chống lại các cuộc tấn công phổ biến. Dưới đây là một số trường hợp kiểm thử bảo mật cho form Login:

1. **Trường hợp 1: SQL Injection**
2. **Input:**
   * Username: "validusername' OR '1'='1'; --"
   * Password: "validpassword"
3. **Kết quả mong đợi:**
   * Hệ thống phải xử lý đúng và không chấp nhận SQL Injection. Người dùng không được đăng nhập vào hệ thống.
4. **Trường hợp 2: XSS (Cross-Site Scripting)**
5. **Input:**
   * Username: "<script>alert('XSS Attack');</script>"
   * Password: "validpassword"
6. **Kết quả mong đợi:**
   * Hệ thống phải xử lý đúng và không cho phép thực hiện mã JavaScript từ người dùng. Người dùng không được thấy thông báo "XSS Attack".
7. **Trường hợp 3: Brute Force Attack**
8. **Input:**
   * Thực hiện nhiều lần đăng nhập không thành công với các tên người dùng và mật khẩu khác nhau.
9. **Kết quả mong đợi:**
   * Hệ thống phải có biện pháp chống lại tấn công Brute Force, ví dụ như việc tạm thời khoá tài khoản sau một số lần thử nghiệm không thành công.
10. **Trường hợp 4: Session Management**
11. **Input:**
    * Đăng nhập bằng một tài khoản, sau đó cố gắng sử dụng session của tài khoản đó ở một thiết bị hoặc trình duyệt khác.
12. **Kết quả mong đợi:**
    * Hệ thống phải quản lý session một cách an toàn và đảm bảo rằng session không thể bị đánh cắp.
13. **Trường hợp 5: Man-in-the-Middle Attack**
14. **Input:**
    * Thử đăng nhập từ một kết nối không an toàn hoặc qua một proxy không đáng tin cậy.
15. **Kết quả mong đợi:**
    * Hệ thống phải hỗ trợ HTTPS và có biện pháp chống lại cuộc tấn công Man-in-the-Middle.
16. **Trường hợp 6: Account Lockout**
17. **Input:**
    * Thử đăng nhập quá số lần cho phép.
18. **Kết quả mong đợi:**
    * Hệ thống phải tạm thời khoá tài khoản sau số lần thử nghiệm không thành công và cung cấp cơ chế mở khóa an toàn.
19. **Trường hợp 7: Session Timeout**
20. **Input:**
    * Đăng nhập, sau đó đợi một khoảng thời gian vượt quá thời gian timeout của session.
21. **Kết quả mong đợi:**
    * Hệ thống phải tự động đăng xuất người dùng sau khoảng thời gian timeout và yêu cầu đăng nhập lại.
22. **Trường hợp 8: CSRF (Cross-Site Request Forgery)**
23. **Input:**
    * Nhập đúng tên người dùng và mật khẩu, nhưng từ một trang web khác gửi yêu cầu đăng nhập.
24. **Kết quả mong đợi:**
    * Hệ thống phải có biện pháp chống lại tấn công CSRF và không chấp nhận yêu cầu từ các nguồn không đáng tin cậy.

Lưu ý: Các kiểm thử bảo mật nên được thực hiện bởi chuyên gia bảo mật và nên điều chỉnh tùy thuộc vào ngữ cảnh cụ thể của ứng dụng và môi trường triển khai.

Top of Form

**Câu 5:**

Trong trường hợp kiểm thử hiệu năng cho chức năng tải ảnh lên, chúng ta cần đảm bảo rằng quá trình tải lên ảnh diễn ra một cách nhanh chóng và hiệu quả, đồng thời kiểm tra sức chịu đựng của hệ thống khi xử lý nhiều tệp ảnh lớn cùng một lúc. Dưới đây là một số trường hợp kiểm thử hiệu năng:

1. **Trường hợp 1: Tải lên ảnh với định dạng JPEG**
2. **Input:**
   * Chọn ảnh với định dạng JPEG.
3. **Kết quả mong đợi:**
   * Quá trình tải lên diễn ra một cách nhanh chóng và hiệu quả.
4. **Trường hợp 2: Tải lên ảnh với định dạng GIF**
5. **Input:**
   * Chọn ảnh với định dạng GIF.
6. **Kết quả mong đợi:**
   * Quá trình tải lên diễn ra một cách nhanh chóng và hiệu quả.
7. **Trường hợp 3: Tải lên ảnh với định dạng PNG**
8. **Input:**
   * Chọn ảnh với định dạng PNG.
9. **Kết quả mong đợi:**
   * Quá trình tải lên diễn ra một cách nhanh chóng và hiệu quả.
10. **Trường hợp 4: Tải lên ảnh với kích thước nhỏ (dưới 1MB)**
11. **Input:**
    * Chọn ảnh với kích thước nhỏ hơn 1MB.
12. **Kết quả mong đợi:**
    * Quá trình tải lên diễn ra một cách nhanh chóng và hiệu quả.
13. **Trường hợp 5: Tải lên ảnh với kích thước lớn (gần 100MB)**
14. **Input:**
    * Chọn ảnh với kích thước gần 100MB.
15. **Kết quả mong đợi:**
    * Hệ thống xử lý tải lên mà không gặp vấn đề và không ảnh hưởng đến hiệu suất của trang web.
16. **Trường hợp 6: Tải lên nhiều ảnh cùng một lúc**
17. **Input:**
    * Chọn và tải lên nhiều ảnh cùng một lúc.
18. **Kết quả mong đợi:**
    * Hệ thống xử lý đúng từng ảnh và không gặp vấn đề về hiệu suất.
19. **Trường hợp 7: Xử lý lỗi khi tải lên ảnh không hợp lệ**
20. **Input:**
    * Chọn ảnh với định dạng không hợp lệ hoặc kích thước quá lớn.
21. **Kết quả mong đợi:**
    * Hệ thống xử lý lỗi một cách nhanh chóng và hiển thị thông báo lỗi phù hợp.
22. **Trường hợp 8: Đánh giá hiệu suất trong điều kiện tải lên đồng thời từ nhiều người dùng**
23. **Input:**
    * Nhiều người dùng cùng lúc thực hiện tải lên ảnh.
24. **Kết quả mong đợi:**
    * Hệ thống vẫn duy trì hiệu suất ổn định và không bị giảm tốc độ đáng kể.

Lưu ý: Đảm bảo sử dụng công cụ đo lường hiệu suất thích hợp để đánh giá và theo dõi hiệu suất của hệ thống trong các trường hợp kiểm thử hiệu năng.