# 1. Điều kiện tiên quyết

Các bài tập khai thác lỗ hổng.

# 2. Giới thiệu

Việc quản lý tài khoản người dùng bao gồm việc xây dựng và áp dụng chính sách đối với định danh người dùng, mật khẩu người dùng và cơ chế phục hồi mật khẩu người dùng, thực hiện phân cấp người dùng. Các hiểm họa an toàn thông tin liên quan đến quản lý tài khoản người dùng gồm:

* Hiểm họa dò đoán thông tin bí mật (Brute-force attacks)
* Hiểm họa chiếm đoạt tài khoản (Acount Hijacking)
* Hiểm họa kỹ nghệ xã hội (Social Engineering)
* Hiểm họa thư rác (Spamming)

Tính an toàn của ứng dụng web được thử nghiệm khi những người dùng đầu tiên đăng nhập và truy xuất tài nguyên website. Có thể có ai đó suy nghĩ rằng mọi việc thật đơn giản: chỉ cần cung cấp một trang đăng nhập để người dùng đệ trình định danh và mật khẩu, nếu nhập đúng thì cấp phép truy cập, còn nếu nhập sai thì từ chối. Trên thực tế, vấn đề không hề đơn giản. Có nhiều việc phải làm xung quanh trang đăng nhập nêu trên để chống lại các hiểm họa mất an toàn thông tin khác nhau. Các hiểm họa liên quan đến quá trình xác thực người dùng có thể kể đến:

* Đánh cắp tài khoản (account hijacking)
* Tấn công người ở giữa (man-in-the-middle)
* Lừa đảo (phishing)
* Truy cập vượt quyền (unauthorized access)
* Rò rỉ thông tin (information leakage)
* Leo thang đặc quyền (privilege escalation)
* Chặn bắt thông tin(sniffing)

### 2.1. Chính sách định danh và mật khẩu

Một chính sách sử dụng mật khẩu an toàn có thể đòi hỏi mật khẩu phải đáp ứng yêu cầu:

 Mật khẩu phải có độ dài tối thiểu là 12 kí tự;

 Không hạn chế độ dài tối đa của mật khẩu;

 Mật khẩu phải bao gồm ít nhất hai nhóm kí tự: chữ hoa, chữ thường, chữ số và kí tự đặc biệt;

 Không được sử dụng từ có trong từ điển để làm mật khẩu

 Không cho phép định danh xuất hiện trong mật khẩu

Việc kiểm tra độ mạnh (độ phức tạp) của mật khẩu có thể được thực hiện bằng cách sử dụng biểu thức chính quy (regular expression).

Việc sử dụng các mật khẩu mạnh sẽ giúp tránh được các hiểm họa dò đoán mật khẩu và đánh cắp tài khoản. Bên cạnh đặt điều kiện cho mật khẩu thì người ta cũng thường đặt điều kiện cho định danh người dùng. Yêu cầu thường gặp là định danh phải có độ dài tối thiểu 3 kí tự, tối đa 25 kí tự, chỉ chứa chữ cái latin, dấu gạch và chữ số và kí tự đầu tiên phải là một chữ cái. Ngoài ra, định danh của người dùng không được trùng với các tên gọi đặc biệt như:

administrator, support, root, postmaster, abuse, webmaster, security... Khi đó, việc kiểm tra tính hợp lệ của định danh cũng có thể được thực hiện tương tự như việc kiểm tra trính chất của mật khẩu trên đây.

### 2.2. Quản lí mật khẩu

Sau khi xác lập thành công định danh và mật khẩu cho người dùng thì ứng dụng web phải thực hiện quản lý mật khẩu một cách an toàn. Việc quản lý mật khẩu bao gồm:

* Lưu trữ mật khẩu
* Xác định hạn sử dụng mật khẩu và lịch sử mật khẩu
* Thay đổi mật khẩu

### 2.3. Cơ chế phục hồi mật khẩu

Có một điều không phải bàn cãi, đó là sớm hay muộn, sẽ có người dùng quên mật khẩu. Do đó, khi xây dựng ứng dụng web thì cần phải xây dựng cả cơ chế để giúp người dùng có thể lấy lại quyền truy cập vào tài khoản. Cơ chế này rất cần thiết cho người dùng, nhưng lại là nguồn gốc của hiểm họa mất an toàn thông tin, nên cần phải được thực hiện một cách cẩn thận, có tính toán. Cũng cần lưu ý rằng, website thường không lưu bản thân mật khẩu người dùng mà chỉ lưu giá trị băm của mật khẩu. Do đó, việc khôi phục mật khẩu không giúp người dùng lấy lại mật khẩu đã dùng mà chỉ có thể cung cấp cho người dùng một mật khẩu mới để đăng nhập vào tài khoản.

Trước đây, nhiều website cho phép người dùng phục hồi mật khẩu nếu trả lời đúng câu hỏi bí mật được thiết lập khi tạo tài khoản. Tuy nhiên, cơ chế khôi phục mật khẩu như thế là kém an toàn. Ngày nay, mật khẩu thường được khôi phục thông qua một kênh thông tin thứ hai: thông thường là qua email, và đối với một số website của tổ chức lớn thì có thể qua tin nhắn SMS.

### 2.4. Xác thực

Trang đăng nhập là điểm cốt lõi trong việc xác thực người dùng ứng dụng web. Trang này là nơi mà người dùng chứng minh tính hợp lệ của mình bằng cách cung cấp định danh và mật khẩu.

Để đảm bảo an toàn cho phần xác thực, một số nội dung được khuyến nghị để thực hiện:

* Thông tin xác thực nhất thiết phải được truyền đến web server bằng phương thức POST thay vì phương thức GET
* Sự thất bại trong xác thực có thể do hai nguyên nhân: định danh không tồn tại, hoặc mật khẩu không đúng. Trong cả hai trường hợp này, ứng dụng web cần trả về chung một thông báo lỗi.
* Khi xây dựng form đăng nhập, đó là không sử dụng các trường ẩn (hidden form fields) để truyền những thông tin nhạy cảm.
* Xây dựng chính sách an toàn thông tin phù hợp để buộc người dùng phải sử dụng mật khẩu có độ phức tạp cao hoặc sử dụng một số giải pháp đơn giản mà hiệu quả: sử dụng mã CAPTCHA, hạn chế số lần đăng nhập thất bại.
* Xác thực người dùng phải được thực hiện qua một kênh an toàn để đảm bảo mật khẩu của người dùng không bị hacker chặn bắt khi truyền đi qua mạng từ trình duyệt người dùng tới web server, cụ thể là sử dụng SSL để mã hóa dữ liệu giữa người dùng và web server trong quá trình xác thực.

Bên cạnh đó cũng cần quan tâm đến việc phát hiện tấn công dò mật khẩu. Có những dấu hiệu cho phép ứng dụng web kết luận có một cuộc tấn công dò mật khẩu đang được thực hiện đối với nó. Các dấu hiệu này gồm:

 Có nhiều đăng nhập thất bại từ một địa chỉ IP

 Đăng nhập với nhiều định danh khác nhau từ một địa chỉ IP

 Đặng nhập sử dụng một định danh từ nhiều địa chỉ IP khác nhau

 Đăng nhập sử dụng định danh hoặc mật khẩu có tính tuần tự

Việc phát hiện ra tấn công sẽ giúp người quản trị có những biện pháp phòng chống bổ sung. Đồng thời, nếu nhận thấy tấn công đó nhằm vào một người dùng nhất định thì cần gửi cảnh báo đến người dùng để họ thực hiện những biện pháp phòng chống cụ thể.

# 3. Kịch bản

Xây dựng một trang web có các chức năng cơ bản để quản lý người dùng và xác thực:

* Đăng ký tài khoản
* Đăng nhập
* Thay đổi mật khẩu
* Khôi phục mật khẩu

# 4. Mục tiêu bài thực hành

Bài tập này nhằm giúp sinh viên:

* Hiểu về cơ chế quản lí tài khoản người dùng và xác thực người dùng trong an toàn ứng dụng web.
* Biết cách thực thi các cơ chế an toàn trong quản lí tài khoản người dùng và xác thực trong ứng dụng web.

# 5. Tổ chức thực hành

Yêu cầu thực hành: thực hành độc lập

Thời gian: 120 phút

# 6. Môi trường thực hành

## *6.1. Phần cứng, phần mềm*

* Yêu cầu phần cứng:

 01 máy tính

 Cấu hình tối thiểu: Intel Core i3, 4GB RAM, 50 GB ổ cứng

* Yêu cầu phần mềm trên máy (tùy từng ngôn ngữ lựa chọn để phát triển ứng dụng mà cài đặt môi trường tương ứng):

 Phần mềm xây dựng web server: IIS/…

 Phần mềm dùng để code: Sublime Text hoặc Visual Studio Code/...

* Yêu cầu kết nối mạng Internet: có

# 7. Các nhiệm vụ cần thực hiện

Trên giao diện của ứng dụng web có cấu trúc tối thiệu gồm các mục như trong bảng phía dưới:

|  |  |
| --- | --- |
| Ảnh của sinh viên | Thông tin về: Số thứ tự của sinh viên trong danh sách lớp  Họ và tên sinh viên  Mã số sinh viên |
| Menu | Nội dung chính |
|  |  |
| Thông tin bản quyền của sinh viên | |

Các chức năng sẽ nằm ở phần “Nội dung chính”.

## Nhiệm vụ 1. Tạo chức năng Đăng ký tài khoản người dùng

Để đăng ký tài khoản người dùng cần nhập những thông tin:

* Tên đăng nhập\*
* Mật khẩu\*
* Nhập lại mật khẩu\*
* Địa chỉ email\*
* Số điện thoại - Địa chỉ Trong đó:

\* là những thành phần bắt buộc phải nhập thông tin

Tên đăng nhập của người dùng là duy nhất trong hệ thống Có áp dụng các chính sách an toàn đối với định danh và mật khẩu.

Áp dụng chính sách lưu trữ mật khẩu an toàn trong cơ sở dữ liệu.

## Nhiệm vụ 2. Tạo chức năng Đăng nhập

Để đăng đăng nhập người dùng cần nhập những thông tin:

* Tên đăng nhập
* Mật khẩu

Trong giao diện của chức năng này sẽ có liên kết tới chức năng Quên mật khẩu.

Phần xác thực tuân thủ các quy tắc an toàn được đề cập trong phần 2.4.

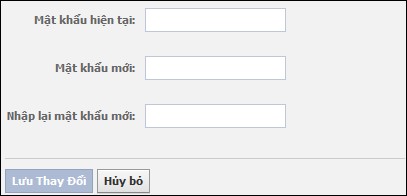
Sau khi đăng nhập thành công sẽ cho phép người dùng thực thi chức năng Thay đổi mật khẩu.

## Nhiệm vụ 3. Tạo chức năng Quên mật khẩu

Yêu cầu người dùng nhập vào email/số điện thoại/một kênh thông tin thứ hai khác, mật khẩu sẽ được sinh và gửi tới người dùng qua kênh thông tin này.

## Nhiệm vụ 4. Tạo chức năng Thay đổi mật khẩu

Chức năng này sẽ có giao diện theo dạng sau:



Chú ý: Kiểm tra chính sách mật khẩu

Sau khi thay đổi thành công cần thông báo cho người dùng biết.

# 8. Đánh giá bài tập

|  |  |  |
| --- | --- | --- |
| **TT** | **Tiêu chí đánh giá** | **Trọng số** |
| 1 | Chức năng đã cài đặt | 70% |
| 2 | Thiết kế: Logic, dễ sử dụng, đẹp | 10% |
| 3 | Tổ chức mã: Tách biệt mã tạo giao diện và mã xử lý nghiệp vụ, tổ chức thư viện, lớp và kế thừa lớp, mô hình MVC | 10% |
| 4 | Phong cách lập trình: Trình bày mã, chú thích mã, … | 10% |
|  | Tổng | 100% |