Báo cáo lỗi bảo mật ứng dụng web FAP (FPT University Academic Portal)

Sử dụng thông tin đăng nhập mặc định cho tài khoản phụ huynh của sinh viên K18

Họ và tên	*Huỳnh Ngọc Quang*
Mã số sinh viên	*SE181838*
Trường	Đại học FPT

Contents

I. Giới thiệu

a. Tổng quan

Báo cáo này nhằm đánh giá lổ hông bảo mật của ứng dụng web FAP (FPT University Academic Portal) về việc sử dụng thông tin đăng nhập mặc định cho tài khoản phụ huynh của sinh viên K18.

b. Mục tiêu

Mục tiêu của báo cáo này là phân tích và đề xuất các biện pháp khắc phục để tăng cường bảo mật cho ứng dụng web FAP. Bằng cách tìm hiểu về lỗ hổng bảo mật hiện tại, chúng tôi hy vọng đưa ra những khuyến nghị cụ thể và thiết thực để cải thiện sự bảo mật của ứng dụng này và bảo vệ thông tin cá nhân của người dùng.

c. Phạm vi của báo cáo

Báo cáo này tập trung vào vấn đề chính là sử dụng mật khẩu mặc định cho các tài khoản phụ huynh của sinh viên K18. Chúng tôi sẽ mô tả chi tiết về lỗ hổng này, nhấn mạnh tác động tiềm tàng của chúng và đưa ra các giải pháp để khắc phục vấn đề an ninh này. Tuy nhiên, báo cáo không bao gồm kiểm tra các lỗ hổng khác có thể tồn tại trong ứng dụng web FAP.

d. Cấu trúc của báo cáo

Báo cáo này được chia thành các phần chính để giúp người đọc hiểu rõ vấn đề. Các phần bao gồm: giới thiệu, mô tả ứng dụng web FAP, mô tả lổ hổng dùng thông tin đăng nhập mặc định, nguy cơ, biện pháp khắc phục và kết luận. Mỗi phần sẽ cung cấp thông tin chi tiết và các khuyến nghị tương ứng để giải quyết các vấn đề an ninh trong ứng web FAP

II. Mô tả ứng dụng web FAP

a. Tên ứng dụng

FAP (FPT University Academic Portal).

b. Chức năng

FAP là một cổng thông tin học thuật thiết yếu, cung cấp cho sinh viên một nền tảng để quản lý việc học và tiếp cận thông tin mới nhất từ nhà trường. Thông qua FAP, sinh viên có thể truy cập các dịch vụ học thuật, xem thông tin cá nhân, tra cứu lịch học, kiểm tra điểm số, và nhận thông báo quan trọng từ nhà trường. Phụ huynh cũng có thể thông qua ứng dụng FAP để kiểm tra tình hình học tập của sinh viên.

c. Mô tả chức năng liên quan đến bảo mật

Trong FAP, có một phần đăng nhập dành cho phụ huynh sinh viên, trong đó tài khoản và mật khẩu được trường cung cấp riêng cho từng sinh viên. Tuy nhiên, một vấn đề đáng lo ngại là việc sử dụng mật khẩu mặc định cho tất cả các tài khoản. Điều này có thể dẫn đến nguy cơ nếu sinh viên không nhận thức được về bảo mật và không thực hiện việc thay đổi mật khẩu mặc định, điều này tạo ra nguy cơ cho việc chiếm quyền truy cập từ phía người khác.

III. Mô tả lổ hổng dùng thông tin đăng nhập mặc định.

a. Mô tả lổ hổng

Trên ứng dụng web FAP, các tài khoản và mật khẩu mặc định được cung cấp cho phụ huynh sinh viên quản lý việc học của sinh viên. Tuy nhiên, điểm yếu của phương pháp này là thông tin mật khẩu mặc định này được công khai, mặc dù tên tài khoản của mỗi sinh viên là riêng biệt (được kết hợp từ tên sinh viên và mã số sinh viên) chúng vẫn có thể bị dễ dàng tìm thấy.

b. Hậu quả

Việc sử dụng thông tin đăng nhập mặc định trong FAP có thể tạo điều kiện cho những kẻ tấn công khai thác để chiếm quyền điều khiển tài khoản một cách trái phép. Điều này tạo ra nguy cơ nghiêm trọng về bảo mật và an ninh thông tin.

IV. Nguy cơ

Lỗ hổng Default Credentials trong ứng dụng web FAP tạo ra các nguy cơ sau:

a. Truy cập trái phép

Bằng cách sử dụng tài khoản và mật khẩu mặc định, kẻ tấn công có thể truy cập trái phép vào ứng dụng web FAP và thu thập thông tin quan trọng. Một số thông tin mà kẻ tấn công có thể truy cập:

a. Họ và tên, ngày tháng năm sinh, mã số sinh viên
b. Lịch học từng tuần
c. Điểm chi tiết từng môn
d. Báo cáo tình trạng nộp tiền
e. Bảng điểm quá trình học
f. Lịch thi

Mặc dù tài khoản phụ huynh không có quyền truy cập chi tiết thông tin cá nhân của sinh viên trong ứng dụng web FAP, việc thay đổi mật khẩu mặc định và tăng cường bảo mật vẫn là cần thiết.

b. Xâm nhập hệ thống, rủi ro dữ liệu

Mặc dù tài khoản phụ huynh không có quyền truy cập sâu trong ứng dụng web FAP, thay đổi mật khẩu mặc định và tăng cường bảo mật vẫn là cần thiết để ngăn chặn xâm nhập hệ thống và giảm thiểu rủi ro về an toàn dữ liệu.

V. BIện pháp khắc phục

Để khắc phục lỗ hổng Default Credentials trong ứng dụng web FAP, chúng tôi đề xuất các biện pháp sau:

a. Thay đổi tài khoản và mật khẩu mặc định

Đầu tiên, tài khoản và mật khẩu mặc định của ứng dụng web FAP nên được tạo ra bằng cách sinh ra một chuỗi kí tự ngẫu nhiên. Sau đó, một email thông báo chứa tài khoản mới và hướng dẫn đổi mật khẩu nên được gửi đến tài khoản cá nhân của sinh viên. Khi đăng nhập lần đầu tiên, người dùng sẽ được yêu cầu thay đổi mật khẩu mặc định thành một mật khẩu có độ an toàn cao và dễ nhớ hơn.

b. Đánh giá và kiểm tra bảo mật:

Thực hiện các cuộc đánh giá bảo mật thường xuyên để phát hiện và khắc phục lỗ hổng bảo mật, bao gồm cả lỗ hổng Default Credentials. Kiểm tra xem tài khoản và mật khẩu mặc định có được thay đổi và tạo ra báo cáo để báo cáo về các vấn đề phát hiện được.

c. Đào tạo người dùng

Cung cấp đào tạo bảo mật cho nhân viên và người dùng cuối để tăng cường nhận thức về nguy cơ và cách phòng ngừa sự tấn công từ các tài khoản mặc định

VI. Kết luận

Lỗ hổng Default Credentials trong ứng dụng web FAP tạo ra nguy cơ truy cập trái phép vào hệ thống và làm suy yếu bảo mật. Để khắc phục lỗ hổng này, việc thay đổi tài khoản và mật khẩu mặc định, quản lý tài khoản, đánh giá và kiểm tra bảo mật, cùng với việc đào tạo người dùng là cần thiết. Bằng cách thực hiện các biện pháp này, tổ chức sẽ tăng cường bảo mật cho ứng dụng web FAP và giảm thiểu rủi ro từ các tài khoản mặc định.