BỘ CÔNG THƯƠNG

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP TP.HCM

KHOA CÔNG NGHỆ THÔNG TIN

TIỂU LUẬN 2

ĐỀ TÀI: GIẢI PHÁP TĂNG CƯỜNG BẢO MẬT CHO HỆ THỐNG QUẢN LÝ THÔNG TIN SINH VIÊN CỦA ĐẠI HỌC ABC Ở THÀNH PHỐ HỒ CHÍ MINH.

Học phần: Nhập môn An toàn thông tin

Mã học phần: 404

Lớp học phần: DHKHMT17

GVHD: TS Ngô Hữu Dũng

Nhóm 4

TP. HỒ CHÍ MINH, THÁNG 05 NĂM 2024

Danh sách thành viên thực hiện

STT	Họ tên SV	MSSV	Ghi chú
1	Phúc Lâm		Nhóm trưởng
2	Quế Trân		
3	Tuấn Anh		
4	Quang Danh		
5	Minh Thuận		
6	Phương Khánh		
7	Hồ Điệp		

MỤC LỤC

CHƯƠNG I. GIỚI THIỆU HỆ THỐNG

1.1. Giới thiệu hệ thống thông tin

Hệ thống quản lý thông tin sinh viên của các Trường Đại học ABC ở Thành phố Hồ Chí Minh là một nền tảng ứng dụng web toàn diện, được thiết kế để hiệu quả hóa việc lưu trữ, quản lý và truy cập thông tin liên quan đến các sinh viên của trường. Được xây dựng với mục tiêu tạo ra một môi trường tương tác và tiện lợi cho cả sinh viên, giáo viên và nhân viên quản lý, hệ thống này bao gồm nhiều tính năng và chức năng chính.

Trong số các tính năng đó, hệ thống cho phép lưu trữ hồ sơ cá nhân của sinh viên, bao gồm thông tin cá nhân cơ bản, lịch sử học tập và kết quả đạt được... Các điểm thi của sinh viên được cập nhật và lưu trữ một cách chính xác, cho phép sinh viên theo dõi tiến trình học tập của bản thân thông qua một giao diện trực quan và dễ sử dụng.

Ngoài ra, hệ thống cung cấp các chức năng liên quan đến quản lý lịch học và đăng ký học phần. Sinh viên có thể dễ dàng xem lịch học, đăng ký hoặc hủy đăng ký các khóa học, và kiểm tra trạng thái học phần thông qua hệ thống. Điều này không chỉ giúp tăng cường tính tự chủ cho sinh viên trong quản lý học tập của mình mà còn giảm thiểu các thủ tục hành chính cho phía nhà trường.

Hệ thống cũng tích hợp một module quản lý hồ sơ tốt nghiệp, cho phép sinh viên theo dõi tiến trình và đáp ứng các yêu cầu cần thiết để tốt nghiệp. Các thông tin về hoạt động học tập và sự kiện của sinh viên cũng được cập nhật thường xuyên, giúp sinh viên không bỏ lỡ bất kỳ thông tin quan trọng nào từ trường.

Tổng thể, Hệ thống quản lý thông tin sinh viên các Trường Đại học ABC ở Thành phố Hồ Chí Minh là một giải pháp công nghệ hiện đại, được thiết kế để cung cấp một trải nghiệm quản lý học tập đơn giản, hiệu quả và tiện lợi cho cả sinh viên và quản lý giáo dục. Hệ thống đảm bảo tính minh bạch, an toàn thông tin và tối ưu trong việc quản lý và trao đổi thông tin giáo dục, phục vụ tốt cho nhu cầu đa dạng của cộng đồng đại học.

1.2. Mô tả chức năng của hệ thống

Dưới đây là một số tính năng chính:

- Cổng giảng viên: Thông tin về lịch dạy, lịch thi, thông tin của giảng viên,...
- Công sinh viên: Thông tin về lịch học, lịch thi, thông tin cá nhân của sinh viên,...
- Tra cứu điểm rèn luyện: Đăng ký tham gia hoạt động và xem điểm rèn luyện.
- Đăng ký email IUH: Dành cho sinh viên đang học tập tại trường có nhu cầu sử dụng.
- Công LLKH của CBVC: Tra cứu, cập nhật lý lịch của cán bộ viên chức.
- Liên hệ - Phản hồi: Các liên hệ phản hồi góp ý về dịch vụ CNTT trong toàn trường.

1.3. Thực trạng an toàn thông tin của hệ thống

1.3.1. Phân tích:

Có ba loại người dùng trong hệ thống: giáo viên, quản trị viên và sinh viên. Tuy nhiên, không có các biện pháp bảo mật đủ mạnh để đảm bảo rằng chỉ những người có quyền truy cập hợp lệ mới có thể tiếp cận dữ liệu nhạy cảm như điểm thi. Cùng với đó, có thể mất thông tin và dữ liệu cá nhân của sinh viên nói chung và giảng viên nói riêng.

Do thiếu biện pháp bảo mật đủ mạnh, thiếu kiểm soát truy cập, có thể xảy ra các vấn đề nghiêm trọng. Như một giáo viên hoặc sinh viên không có quyền truy cập vào điểm thi có thể lấy trộm hoặc thay đổi dữ liệu; một tin tặc lấy trộm tất cả thông tin sinh và đêm rao bán trên những web đen không chính thống.

Những điều trên có thể gây ra sự thiếu minh bạch và tin cậy trong hệ thống quản lí sinh viên, ảnh hưởng đến kết quả học tập và đánh giá của sinh viên. Mất an toàn thông tin, dữ liệu cá nhân của toàn thể nhân viên Trường Đại học ABC.

1.3.2. Thực trạng của hệ thống

- Thiếu kiểm soát truy cập: Hệ thống không có cơ chế xác thực chặt chẽ, dẫn đến nguy cơ lỗi truy cập và sửa đổi dữ liệu nhạy cảm.
- Dữ liệu không được mã hóa: Dữ liệu nhạy cảm không được bảo vệ, dễ bị truy cập trái phép và rò rỉ thông tin cá nhân của sinh viên.

- Thiếu giám sát và phát hiện sớm: Hệ thống không có cơ chế giám sát và báo cáo sự kiện, không cảnh báo khi có hành vi không mong muốn, tăng nguy cơ xâm nhập.
- Sử dụng mật khẩu yếu: Người dùng thường sử dụng mật khẩu yếu, dễ đoán, làm tăng khả năng bị tấn công và tiếp cận trái phép.
- Thiếu bảo mật trong giao tiếp: Dữ liệu giao tiếp không được mã hóa, tạo cơ hội cho kẻ tấn công đánh cắp thông tin trong quá trình truyền tải.

CHƯƠNG 2. ĐỀ XUẤT GIẢI PHÁP

Hiện tại Trường Đại học ABC ở Thành phố Hồ Chí Minh nên cân nhắc việc áp dụng các biện pháp bảo mật bổ sung, tăng cường bảo mật năng cao. Cùng với đó có thể sử dụng thêm công nghệ blockchain để lưu trữ dữ liệu sinh viên một cách an toàn và sử dụng trí tuệ nhân tạo để phát hiện các hoạt động gian lận.

Việc đảm bảo an toàn cho hệ thống quản lý thông tin sinh viên là điều cần thiết để bảo vệ thông tin cá nhân, minh bạch trong điểm số của sinh viên, duy trì sự tin tưởng vào Trường Đại học ABC ở Thành phố Hồ Chí Minh. Bằng các cách thực hiện các biện pháp phòng ngừa phù hợp, Trường Đại học có thể giúp giữ an toàn cho dữ liệu của sinh viên và giảm thiểu rủi ro vi phạm dữ liệu.

Để đảm bảo sự minh bạch và an toàn về thông tin cá nhân của sinh viên nói chung và giảng viên nói riêng, chúng tôi xin đề xuất một số biện pháp:

2.1. Đề xuất giải pháp chung

Đề xuất cải thiện bao gồm:

1. *Tạo chính sách bảo mật:*
   - Xác định và mô tả rõ ràng các quy định và nguyên tắc bảo mật mà tổ chức cần tuân thủ.
   - Bao gồm các quy định về quyền truy cập, mật khẩu mạnh, mã hóa dữ liệu, quản lý thiết bị và phần mềm bảo mật, quản lý rủi ro, và các biện pháp phòng ngừa và ứng phó sự cố.

- Thực hiện việc giám sát và đánh giá định kỳ để đảm bảo tuân thủ chính sách và làm cập nhật khi cần thiết.

2. *Đào tạo và nâng cao nhận thức:*
   - Tổ chức các khóa đào tạo định kỳ về an ninh thông tin cho giáo viên và sinh viên, bao gồm tất cả sinh viên đang còn theo học tại Trường, giảng viên còn công tác.
   - Cung cấp cho sinh viên và nhân viên đào tạo về các biện pháp an ninh mạng tốt nhất, bao gồm cách tạo mật khẩu mạnh, cách xác định email lừa đảo và cách bảo vệ thông tin cá nhân.
   - Tổ chức các chiến dịch nâng cao nhận thức về an ninh mạng để giúp mọi người nhận thức được các mối đe dọa tiềm ẩn và biết cách bảo vệ bản thân.
   - Tập trung vào việc giáo dục về những mối đe dọa thông tin phổ biến, cách phát hiện và phản ứng lại với các cuộc tấn công, và tầm quan trọng của việc bảo vệ thông tin cá nhân và nhạy cảm.
3. *Áp dụng cơ chế xác thực hai yếu tố (2FA):*
   - Yêu cầu sinh viên, giáo viên cung cấp ít nhất hai phương tiện xác thực khác nhau (ví dụ: mật khẩu và mã OTP được gửi qua điện thoại di động) để truy cập vào hệ thống.
   - Tăng cường tính bảo mật bằng cách yêu cầu hacker phải có thông tin xác thực không chỉ là mật khẩu mà còn là một phương tiện xác thực khác.
4. *Mã hóa dữ liệu:*
   - Áp dụng các thuật toán mã hóa mạnh mẽ để bảo vệ dữ liệu nhạy cảm trong quá trình truyền tải và lưu trữ.
   - Đảm bảo rằng dữ liệu được mã hóa đúng cách và chỉ có người được ủy quyền mới có thể giải mã dữ liệu.
5. *Triển khai công cụ giám sát và ghi log hoạt động:*
   - Cài đặt các công cụ giám sát để theo dõi hoạt động trên hệ thống và phát hiện các hành vi không bình thường hoặc đáng ngờ.
   - Ghi lại các sự kiện và hoạt động quan trọng để giúp phân tích và điều tra sự cố và cuộc tấn công.

6. *Thực hiện kiểm định bảo mật định kỳ:*
   - Thực hiện các kiểm tra bảo mật định kỳ để đảm bảo rằng hệ thống không có lỗ hổng bảo mật mới nảy sinh.
   - Khắc phục các lỗ hổng bảo mật ngay khi chúng được phát hiện để đảm bảo tính bảo mật liên tục.

2.2. Đề xuất giải pháp riêng

1. Tăng cường cơ chế quản lý truy cập

- Xây dựng hệ thống phân quyền truy cập cơ động giúp đảm bảo rằng người dùng chỉ có quyền truy cập vào những tài nguyên và chức năng cần thiết cho công việc của họ.
- Nguyên tắc "nguyên tắc của sự ít đặc quyền" (principle of least privilege) đảm bảo rằng mỗi người dùng chỉ được cấp quyền truy cập tối thiểu cần thiết để thực hiện công việc của họ, giảm thiểu rủi ro truy cập trái phép.

2. Thực hiện chính sách mật khẩu mạnh

- Yêu cầu người dùng sử dụng mật khẩu có độ phức tạp cao (bao gồm ký tự chữ cái in hoa và thường, số, ký tự đặc biệt) để tăng cường tính bảo mật.
- Thực hiện đổi mật khẩu định kỳ giúp đảm bảo rằng mật khẩu không bị lạc hậu và nguy cơ bị tấn công giảm đi.
- Sử dụng các biện pháp bảo vệ mật khẩu như mã hóa và salt để bảo vệ mật khẩu khỏi các cuộc tấn công dò mật khẩu.

3. Triển khai giao thức mã hóa trong quá trình giao tiếp

- Sử dụng giao thức mã hóa như HTTPS (cho trang web) hoặc SSH (cho truy cập từ xa) để mã hóa dữ liệu trong quá trình truyền tải giữa máy tính của sinh viên và máy chủ.
- Mã hóa dữ liệu giúp đảm bảo tính bảo mật của thông tin được truyền tải qua mạng và ngăn chặn kẻ tấn công từ việc đánh cắp thông tin.

4. Xây dựng hệ thống cảnh báo

- Thiết lập các cảnh báo tự động để thông báo cho người quản trị khi phát hiện các hoạt động không bình thường hoặc đáng ngờ trong hệ thống.
- Cảnh báo tự động giúp phát hiện và phản ứng nhanh chóng với các mối đe dọa hoặc cuộc tấn công, giúp giảm thiểu thời gian phản ứng và hậu quả của các sự cố bảo mật.

5. Thực hiện kiểm soát và giám sát việc sử dụng mật khẩu

- Giám sát và ghi log các hoạt động liên quan đến mật khẩu, như các lần đăng nhập không thành công hoặc việc đổi mật khẩu.
- Theo dõi và ghi log các hoạt động liên quan đến mật khẩu giúp phát hiện và ngăn chặn các hành vi đe dọa, như tấn công dò mật khẩu hoặc sử dụng mật khẩu bất hợp pháp.

CHƯƠNG 3. KẾT LUẬN

Việc áp dụng các giải pháp trên sẽ giúp củng cố an toàn thông tin cho hệ thống quản lý thông tin sinh viên của Trường Đại học ABC ở Thành phố Hồ Chí Minh, đảm bảo tính bảo mật và quyền riêng tư của thông tin sinh viên. Đây là bước quan trọng trong việc nâng cao chất lượng quản lý thông tin và đảm bảo sự tin cậy của hệ thống trong môi trường đại học.

Tất cả các giải pháp bảo mật thông tin được đề cập đều đóng vai trò cực kỳ quan trọng trong việc củng cố tính an toàn cho hệ thống quản lý thông tin sinh viên của Trường Đại học ABC ở Thành phố Hồ Chí Minh. Bằng việc triển khai những biện pháp này, trường không chỉ đảm bảo sự bảo mật cho thông tin quan trọng của sinh viên mà còn thể hiện cam kết đạo đức và trách nhiệm của mình đối với việc bảo vệ quyền riêng tư và thông tin cá nhân của cộng đồng sinh viên.

Phân quyền truy cập linh hoạt và minh bạch là nền tảng của một hệ thống bảo mật hiệu quả. Bằng cách xác định rõ ràng quyền hạn và trách nhiệm của từng người dùng, Trường Đại học ABC đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào thông tin cần thiết, giảm thiểu nguy cơ truy cập trái phép và lưu trữ thông tin của sinh viên một cách an toàn.

Chính sách mật khẩu mạnh cùng việc yêu cầu đổi mật khẩu định kỳ đóng vai trò quan trọng trong việc tạo ra một môi trường an toàn trực tuyến. Bằng cách khuyến khích việc sử dụng mật khẩu phức tạp và thực hiện việc đổi mật khẩu định kỳ, Trường Đại học ABC giúp bảo vệ tài khoản của sinh viên khỏi các cuộc tấn công dò mật khẩu và đảm bảo tính bảo mật liên tục của hệ thống.

Mã hóa dữ liệu trong quá trình truyền tải và lưu trữ không chỉ là một biện pháp bảo mật mà còn là một cam kết đối với tính riêng tư của sinh viên. Bằng cách sử dụng các giao thức mã hóa mạnh mẽ, Trường Đại học ABC đảm bảo rằng dữ liệu của sinh viên sẽ luôn được bảo vệ, ngay cả khi chúng được truyền tải qua mạng Internet.

Cảnh báo tự động và giám sát hoạt động giúp phát hiện kịp thời các hành vi không bình thường và đáng ngờ trong hệ thống. Bằng cách cung cấp khả năng phản ứng nhanh chóng đối với các sự cố bảo mật, Trường Đại học ABC xây dựng một môi trường an toàn và tin cậy cho sinh viên và nhân viên.

Cuối cùng, việc nâng cao chất lượng quản lý thông tin không chỉ giúp cải thiện hiệu suất hoạt động mà còn là một cam kết với sự phát triển bền vững của cả trường và cộng đồng sinh viên. Bằng cách thúc đẩy tính bảo mật và quản lý thông tin chất lượng, Trường Đại học ABC khẳng định vai trò lãnh đạo của mình trong việc đảm bảo sự an toàn và tin cậy của thông tin sinh viên và giúp hình thành một môi trường học tập và nghiên cứu tốt nhất cho tất cả mọi người.

TÀI LIỆU THAM KHẢO

- Giáo trình: Chương 4. Chính sách ATTT
- https://classin.vn/bao-mat-du-lieu-trong-he-thong-quan-ly-hoc-tap/
- https://locker.io/passwords/blog/bao-mat-du-lieu-cho-sinh-vien