Tên: Lê Hải Đăng

MSSV: 20110243

**KIỂM TRA LÝ THUYẾT PHẦN TỰ LUẬN (70%)**

**Môn: An toàn thông tin**

1. ***(3 điểm)* Trình bày giải pháp để đảm bảo an toàn cho ứng dụng Web?**

Lỗ hổng (vulnerability) được hiểu là những điểm yếu có thể bị khai thác bởi các tác nhân xấu để thực hiện các hành động không cho phép (unauthorized actions) trong: Police, Design, Implementation, Operation.

Các lỗ hổng có thể cho phép kẻ tấn công chạy mã, truy cập bộ nhớ của hệ thống, cài đặt phần mềm độc hại và đánh cắp, phá hủy hoặc sửa đổi những dữ liệu nhạy cảm.

Ứng dụng web nào cũng có điểm yếu, nên ứng dụng web nào cũng có thể bị tấn công.

Trước hết, các lỗ hổng phần mềm được xác định bởi 3 yếu tố:

* Existence: tồn tại lỗ hổng.
* Access: khả năng kết nối của kẻ tấn công đến lỗ hổng.
* Exploit: khả năng khai thác lỗ hổng thông qua các công cụ hoặc kỹ thuật nhất định nào đó.

Để có thể tìm được giải pháp phù hợp đảm bảo an toàn cho ứng dụng Web, đầu tiên, ta cần tiến hành phân tích các nguyên nhân gây ra lỗ hổng:

* Độ phức tạp: Các hệ thống phức tạp làm tăng xác suất của lỗ hổng, sai sót trong cấu hình hoặc truy cập ngoài ý muốn. Nó đồng nghĩa với việc hệ thống càng phức tạp thì lỗ hổng càng nhiều.
* Tính phổ biến: Các loại mã, phần mềm, hệ điều hành và phần cứng có tính phổ biến (Microsoft, Windows,…) sẽ làm tăng khả năng kẻ tấn công có thể khai thác và tìm thấy hoặc có thông tin về các lỗ hổng đã biết.
* Mức độ kết nối: Thiết bị càng được kết nối nhiều thì khả năng xuất hiện lỗ hổng càng cao vì hầu hêý những lỗ hổng này xuất hiện trong quá trình kết nổi.
* Quản lý bảo mật kém: Những mật khẩu yếu có thể bị phá bằng tấn công brute-force và việc sử dụng lại mật khẩu có thể biến một vi phạm dữ liệu trở thành nhiều vụ vi phạm xảy ra.
* Lỗi hệ điều hành: Giống như bất kỳ phần mềm nào khác, hệ điều hành cũng có thể có lỗ hổng. Các hệ điều hành không an toàn – chạy mặc định và để tất cả mọi người dùng có quyền truy cập đầy đủ sẽ có thể cho phép virus và phần mềm độc hại thực thi các lệnh.
* Sử dụng Internet: Internet có rất nhiều loại phần mềm gián điệp và phần mềm quảng cáo có thể được cài đặt tự động trên máy tính. Những loại phần mềm này có thể tồn tại mã độc hoặc virus,… tấn công độc hại đến người dùng.
* Lỗi phần mềm: Lập trình viên có thể vô tình hoặc cố ý để lại một lỗi có thể khai  
  thác trong phần mềm. Do đó lỗi phần mềm sẽ luôn có và có thể khai thác.
* Đầu vào của người dùng không được kiểm tra: Nếu trang web hoặc phần mềm cho rằng tất cả đầu vào đều an toàn, chúng có thể thực thi các lệnh SQL ngoài ý muốn.
* Con người: Lỗ hổng lớn nhất trong bất kỳ tổ chức nào là con người đằng sau hệ  
  thống đó (do con người giám sát, thiết kế, thực thi và vận hành). Tấn công phi kỹ thuật (social engineering) là mối đe dọa lớn nhất đối với đa số các tổ chức. Với những nguy cơ đó, hệ thống không thể đảm bảo an toàn tuyệt đối, do đó ta cần cố gắng đảm bảo mỗi khâu an toàn nhất có thể để đảm bảo liên hệ giữa các lớp.

Dựa vào nguyên nhân gây ra lỗ hổng mà có các giải pháp phù hợp:

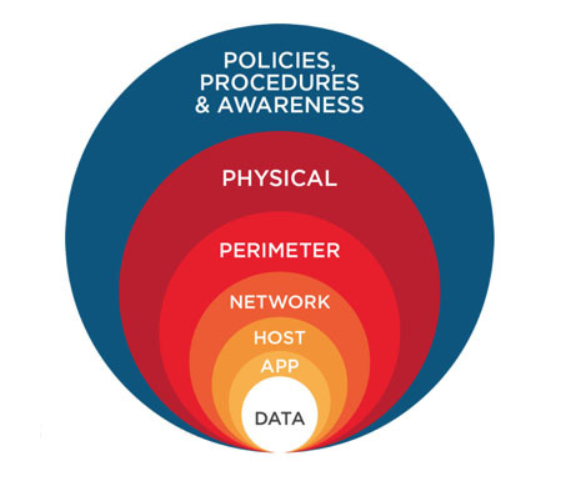
* Hệ thống phức tạp, khó quản lí, kiểm soát: Phân chia hệ thống thành các phần  
  chuyên biệt để dễ dàng quản lí và cài đặt.
* Quản lý các thiết bị kết nối, tránh trường hợp nhiều thiết bị kết nối, dễ gây ra lỗ  
  hổng bằng cách đặt giới hạn số thiết bị.
* Dựa trên các nguyên tắc về quyền tối thiểu: Mỗi chương trình hoặc user chỉ nên  
  được cấp quyền đủ để truy cấp, tránh việc cấp dư quyền.
* Tăng cường quản lí mật khẩu, sử dụng strong password - mật khẩu có tính bảo mật cao, hạn chế sử dụng một loại mật khẩu cho nhiều tài khoản các nhau. Đồng thời, sử dụng PAM (Privileged Account/Access Management) để quản lý hệ thống server của các admin, tránh trường hợp xảy ra sự cố với admin.
* Trên ứng dụng, đánh giá sự tồn tại của các lỗ hổng trên hệ thống, qua đó xem xét khả năng hình thành lỗ hổng. Thông qua các điểm yếu nhận định nó có thể được khai thác cho mục đích tấn công hay không.
* Kiểm soát các lỗ hổng thông qua:
  + Các công cụ quét lỗ hỏng bảo mật như Acunetix, Nexpose, Retina,….
  + Đối với Buffer Overflow:
    - Stack Guard: kiểm tra khi có thay đổi giá trị so với ban đầu dẫn đến xảy ra Buffer Overflow thì thông báo đến người dùng.
    - Stack Shield: sao lưu giá trị return address, sau khi thực thi, nếu giá trị Stack Shiled không thay đổi thì không sao, ngược lại thì xảy ra buffer overflow.
    - Random Space: Random địa chỉ lưu.
    - Ngăn không cho thực hiện lệnh trên vùng Memory.

Để hiệu quả hơn, chúng ta cần phải biết cách quản lý lỗ hổng. Quản lý lỗ hổng là một hoạt động theo chu kỳ trong việc xác định, phân loại, khắc phục và giảm thiểu các lỗ hổng bảo mật. Các yếu tố cơ bản của quản lý lỗ hổng bao gồm phát hiện lỗ hổng, đánh giá lỗ hổng và khắc phục. Các phương pháp phát hiện lỗ hổng bao gồm:

* Quét lỗ hổng
* Kiểm thử xâm nhập
* Google hack

Khi một lỗ hổng được tìm thấy, nó sẽ trải qua quá trình đánh giá lỗ hổng như sau:

* Xác định các lỗ hổng: Phân tích các lần quét hệ thống mạng, kết quả pentest, nhật ký tường lửa và kết quả quét lỗ hổng để tìm ra sự bất thường cho thấy một cuộc tấn công mạng có thể lợi dụng lỗ hổng đó.
* Xác minh lỗ hổng: Xác định xem lỗ hổng đã được nhận diện có thể bị khai thác hay không và phân loại mức độ nghiêm trọng của việc khai thác đó để hiểu mức độ rủi ro
* Giảm thiểu các lỗ hổng: Xác định các biện pháp đối phó và cách đo lường hiệu quả của chúng trong trường hợp không có bản vá.
* Khắc phục lỗ hổng: Cập nhật phần mềm hoặc phần cứng bị ảnh hưởng nếu có thể.

Ngày nay, các website thường được triển khai ở một máy chủ thông qua các nhà cung cấp dịch vụ. Cơ sở dữ liệu của website cũng được triển khai thông qua các dịch vụ đám mây, đồng thời các website sẽ thường xuyên được truy cập bởi nhiều người dùng có kết nối Internet. Vì vậy, để đảm bảo an toàn cho ứng dụng web, phải đảm bảo an toàn ở nhiều tầng khác nhau, hay còn được gọi là *“Defense in depth”*

**1. Data**

Đầu tiên, là bảo mật ở tầng Data, đó là Database security ( bảo mật cơ sở dữ liệu ). Nếu hệ thống cơ sở dữ liệu được đặt trên các cơ sở dữ liệu đám mây, phải đảm bảo tính bảo mật từ các nhà cung cấp dịch vụ. Nếu hệ thống cơ sở dữ liệu được đặt trên các cơ sở lưu trữ riêng của công ty, phải đảm bảo an ninh từ các tác nhân vật lý lẫn thông qua môi trường mạng.

Phải thường xuyên backup dữ liệu, có thể lưu trữ dữ liệu ở trên đám mây lẫn ở phía local ( máy chủ ). Phòng khi sự cố xảy ra, ta có thể phục hồi dữ liệu kiệp thời, đảm bảo tính sẵn sàng cho dữ liệu.

Hạn chế truy cập vào cơ sở dữ liệu ở một số người dùng. Chỉ cấp quyền truy cấp nếu đã xác thực ( authenticated ) và đặc quyền của người đó cho phép truy xuất tới dữ liệu ( authorization ). Ngăn chặn việc sửa đổi cơ sở dữ liệu đối với những người dùng chưa được xác thuật. Sử dụng yếu tố đặc quyền ít nhất ( least privilage)

**2. Application**

Tiếp theo, là bảo mật ở tầng application, ở phía website tương tác với các người dùng. Phải có các cài đặt để xác thực người dùng và các đặc quyền của yêu cầu truy cập thông qua AAA (Authentication, authorization, auditing ). Đảm bảo tính toàn vẹn, bảo mật, sẵn sàng của dữ liệu.

Phải kiểm tra đầu vào của dữ liệu, sử dụng các công cụ lọc dữ liệu, phòng chống tấn công SQL Injection vào database

Kiểm thử lại ứng dụng, sử dụng những đoạn code sạch, tránh xảy ra bug hoặc lỗ hổng để hacker có thể khai thác

Có thể mua chứng chỉ SSL, Với tiêu chuẩn này, dữ liệu truyền tải giữa máy chủ và trình duyệt của người dùng sẽ được đảm bảo riêng tư hoàn toàn, đảm bảo tuyệt đối thông tin.

**3. Host**

Bất cứ một website nào khi được triển khai ( deploy ), sẽ được cài đặt ở một web server nào đó. Và web server thực chất là một máy chủ sử dụng hệ điều hành window, linux,.. Vì thế, phải tiến hành bảo mật hệ điều hành, đặc biệt là khi website được triển khai ở 1 server mà bản thân hoặc công ty tự thiết kế

Máy chủ phải được cài đặt các phần mềm bảo vệ, chống virus, tắt bớt các dịch vụ và phần mềm không cần thiết để phòng chống mã độc. Thường xuyên cập nhật các bản vá. Hạn chế các lỗ hổng ở hệ điều hành để hacker khó có thể xâm nhập

Sử dụng các thiết bị phát hiện xâm nhập (IDS) và phòng chống xâm nhập (IPS). Tường lừa ứng dụng web (WAF), để đảm bảo tính toàn vẹn của dữ liệu và phát hiện các mối đe dọa kiệp thời. Tăng thêm băng thông hoặc mua thêm máy chủ để đảm bảo tính sẵn sàng cho người dùng.

**4. Internal Network, perimeter**

Sử dụng các thiết bị bảo vệ như firewall để kiểm tra truy cập . Mã hóa dữ liệu được truyền đi, xác thực yêu cầu truy cập

Phòng chống DDOS, giám sát lưu lượng mạng, tạo một ACL ( access control list ) trong tường lửa để chặn các ip tấn công

**5. Physical**

Bên cạnh bảo mật về phần mềm. Nếu ứng dụng web sử dụng một server riêng cần phải bảo mật vật lý đối với các máy chủ, đề phòng các cuộc tấn công vào máy chủ.

**6. Policies, Procedure, Awareness**

Cài đặt các quy tắc cho mật khẩu, nếu là một website lớn, phải nâng cao nhận thức cho nhân viên. Tạo một môi trường an toàn, tránh việc xâm nhập xuất phát từ nội bộ.

Khi kẻ tấn công vượt qua được 1 tầng, sẽ phải đối mặt với tầng kế tiếp trong defense in depth, điều này giúp tăng thời gian xâm nhập đồng thời phát hiện và phòng chống kiệp thời các mối đe dọa

1. ***(4 điểm)* Trình bày các nguyên tắc để đảm bảo an toàn cho dữ liệu?**

Một hệ thống phải đảm bảo 03 tính chất (CIA) mới được gọi là bảo mật:

* Bí mật (Confidentiality): chỉ các thực thể được ủy quyền mới có quyền truy cập vào dữ liệu.
* Toàn vẹn (Integrity): dữ liệu sẽ không được sửa đổi khi không được cho phép.
* Sẵn sàng (Availability): các tài nguyên và dữ liệu luôn sẵn sàng để truy cập khi thực tể được cấp quyền.

Một hệ thống thường được bảo vệ theo Defense in Depth (bảo vệ theo chiều sâu, bảo vệ theo từng layer). Các cơ chế bảo vệ được phân lớp để đảm bảo dữ liệu và thông tin có giá trị an toàn, và tùy theo quy mô hoạt động, mối quan tâm và nguồn lực mà hệ thống sẽ được bảo vệ như thế nào:

* Data > Application > Host > LAN > Border Gateway > Physical Security > Human.
* Khi xây dựng một hệ thống CNTT, thì bảo mật hệ thống phải đạt được mục tiêu: Ngăn chặn (prevention) – Phát hiện (detection) – Phục hồi (recovery).
* Nguyên tắc đóng gói trong đảm bảo an toàn thông tin: Thường xuyên backup dữ liệu hoặc update phiên bản cho phần mềm.
* Nguyên tắc cách ly trong đảm bảo an toàn thông tin: Giảm các tấn công bề mặt, tiêu biểu như các cổng kết nối,…
* Ngăn chặn các mối đe dọa đã biết đến. Ngăn chặn các mối đe dọa chưa được biết đến, có thể kể đến zero-day,... và có thể kiểm tra thông qua sandbox.
* Đồng thời, sử dụng PAM (Privileged Account/Access Management) để quản lý hệ thống server của các admin, tránh trường hợp xảy ra sự cố với admin.
* Sử dụng các chuẩn an toàn ISO 27001/27002, COBIT, ITIL, RMF, CSA STAR,...để tuân thủ khi xây dựng hệ thống.
* Đặc biệt, an ninh mạng còn có thể tuân theo các mô hình:
  + CIA (Confidentiality – Integrity – Availability): Bí mật – Toàn vẹn – Sẵn sàng.
  + PPT (People – Process – Technology): Con người – Tiến trình – Công nghệ.
  + AAA (Authentication - Authorization - Accounting): Xác thực - Phân quyền - Ghi nhận

Ngoài ra chúng ta có thể đảm bảo an toàn dữ liệu phải đảm bảo 04 nguyên tắc sau:

* Authentication
* Authorization
* Access control
* Accounting

**1. Authentication**

Là về việc xác thực dữ liệu truy cập, như quá trình đăng nhập. Hệ thống thường sẽ kiểm tra tên người dùng và mật khẩu để xác minh danh tính. Sau khi đã xác thực thành công, người dùng sẽ được cấp quyền truy xuất đến dữ liệu.

Ngăn chặn việc truy cập dữ liệu từ những người dùng chưa được xác thực. Đảm bảo tính bảo mật, toàn vẹn của dữ liệu.

Ví dụ: Nếu một tài khoản không có quyền admin, sẽ không thể thực hiện những hành động như quyền xóa, sửa dữ liệu người dùng.

Cài đặt các chính sách bảo mật như mật khẩu người dùng phải đủ mạnh để tránh các cuộc tấn công như brute force, dictionary attack,..

Việc xác thực người dùng có thể dựa trên nhiều yếu tố.

* Something you know: Mật khẩu, mã OTP
* Something you are: Vân tay, nhận diện khuông mặt, giọng nói
* Something you have: E-Token, thẻ điện tử, chứng chỉ điện tử

Dù sử dụng cách xác thực nào (OTP,SSO), đều phải đảm bảo tính đúng đắn của quá trình đăng nhập. Đảm bảo cung cấp đặc quyền ít nhất (Least privilage) cho người dùng.

**2. Authorization**

Là quá trình xảy ra sau khi hệ thống xác thực thành công. Xác định xem người dùng được xác thực có quyền truy cập vào các tài nguyên cụ thể hay không. Cung cấp các quyền truy cập cho người dùng về:

* Roles: Chia người dùng thành nhiều vai trò khác nhau, mỗi vai trò được truy cập vào một số tài nguyên cụ thể.
* Groups: Phân người dùng vào các nhóm, từ đó quản lý các nhóm người dùng và dữ liệu họ có thể truy cập.

Ngoài ra còn căn cữ vào vị trí, thời gian,.. để cung cấp đặc quyền cho người dùng.

Quá trình authorization nhằm đảm báo tính toàn vẹn của dữ liệu, không cho phép việc sửa đổi dữ liệu đối với những người dùng không có quyền truy cập.

**3. Access Control**

Là quá trình cung cấp đặc quyền cho người sử dụng để cho phép họ truy cập vào các tài nguyên hệ thống. Bao gồm:

* Mandatory access control ( MAC ): Chỉ có người quản lý hệ thống mới có quyền truy cập tài nguyên.
* Discretionary access control ( DAC ): Chỉ những người là chủ sở hữu tài nguyên mới có thể truy cập tài nguyên
* Role-Based access control ( RBAC ): Cấp quyền truy cập thông qua vai trò của người dùng
* Rule-Based access control: Cấp quyền truy cập thông qua các quy tắc được thiết lập
* Attribute-based access control: Cấp quyền truy cập thông qua các tiêu chí mà người quản lý cấp cho người dùng

Để đảm bảo an toàn cho thông tin, cần phải cài đặt access control ở nhiều phương diện: cơ sở dữ liệu, máy chủ, ứng dụng,..

Thiết lặp các ACL ( access control list ), để có cái nhìn tổng quát về phía người dùng. Đồng thời dựa vào ACL có thể ngăn chặn các mối nguy hại thông qua việc ngăn chặn các ip ở phía firewall

Thông qua các phần mềm quản lý, nhờ vào access control, dữ liệu được đảm bảo an toàn từ phía các người sử dụng

**4. Accounting**

Là quá trình ghi nhận, theo dõi thông tin truy cập của người dùng. Đó là thông tin về tên người dùng, quyền của họ trong hệ thống. Nhờ vào điều này, ta có thể nhanh chóng phát hiện các truy cập trái phép đến dữ liệu, ngăn chặn các đối tượng có mưu đồ xấu tấn công vào hệ thống dữ liệu. Đảm bảo tính toàn vẹn dữ liệu của chúng ta

Ngoài ra, cũng cần phải có các biện pháp bảo vệ dữ liệu như:

* Sao lưu dữ liệu
* Cài đặt, cập nhật các phần mềm diệt virus
* Gỡ bỏ file, dịch vụ, ứng dụng không cần thiết
* Cập nhật hệ điều hành
* Cài đặt, cấu hình tường lửa
* Đặt mật khẩu truy cập bằng phương thức mã hóa
* Tránh sử dụng internet công cộng