**Bài 1: Security Testing – Giới Thiệu**

Security Testing được thực hiện để phát hiện ra các lổ hổng bảo mật trong hệ thống để bảo vệ dữ liệu và bảo trì chức năng.

Serial học này sẽ chỉ cho bạn các khái niệm cốt lõi của Security Testing (Kiễm thử bảo mật) and mổi phần chứa đựng các chủ đề liên quan với các ví dụ hữu ích.

Trong các ví dụ mình sẽ demo vài phương pháp tấn công và cách phòng chóng.

**Security Testing là cái gì**

Security Testing (ST) là một kỹ thuật kiễm tra để xác định nếu một hệ thống thông tin được bảo vệ và bảo trì như dự định. Bằng việc thực hiện ST, không bảo đảm hệ thống sẽ được bảo mật tuyệt đối nhưng quan trọng để giúp giảm thiểu bị tấn công từ bên ngoài ở mức có thể nhất. Nó cũng nhằm mục đích xác minh 6 nguyên tắc cơ bản được liệt kê như sau:

* **Confidentiality (bảo mật)**
* **Integrity (toàn vẹn)**
* **Authentication (chứng thực)**
* **Authorization (ủy quyền)**
* **Availability (tiện lợi)**
* **Non-repudiation**

**Example**

Nhận ra một lổ hổng bảo mật trong một ứng dụng web liên quan tới nhiều bước  phức tạp and một tư duy sáng tạo, nhưng việc thực hiện một bài kiễm tra đơn giản như dưới đây có thể giúp giảm nguy cơ bảo mật. Dưới đây là một ST cơ bản mà bất kỳ ai cũng có thể thực hiện trên bất kỳ ứng dụng web:

1. Log vào ứng dụng web bằng thông tin có giá trị
2. Log out ứng dụng web
3. Click nút BACK của trình duyệt. Kiễm tra nếu bạn được yêu cầu log in một lần nữa hoặc nếu bạn có thể đi trở lại trang đã được log vào thành công trước đó.

**Điều kiện để học tutorial này**

Bạn phải có kiến thức cơ bản về software testing (kiễm thử phần mềm) và các khái niệm liên quan.

Nếu chưa có? Đừng lo lắng, mình sẽ đi lại các kiến thức cơ bản trong những bài tiếp theo trước khi bước vào phần trọng tâm của serial này là Hacking and Preventing.