**Bài 3: Security Testing – Hacking Web Applications**

**Kỹ thuật PenetrationTesting**

**Penetration Testing là gì:**

Thường được gọi tắt là **PenTesting.**

Có thể hiểu một cách nôm na là chúng ta đánh trận giả, tức là test thâm nhập vào hệ thống để tìm ra các lổ hổng bảo mật. Không phải là tấn công thật vào website để hack.

Ý nghĩa như thế này: Khi thâm nhập thử nghiệm cần phải có sự cho phép của người sở hữu hệ thống. Nếu không, bạn sẽ là hacking hệ thống, và đó là bất hợp pháp. Nói cách khác: Sự khác biệt giữa thử nghiệm thâm nhập(pentesting) và hack là  bạn có sự cho phép của chủ sở hữu hệ thống ..

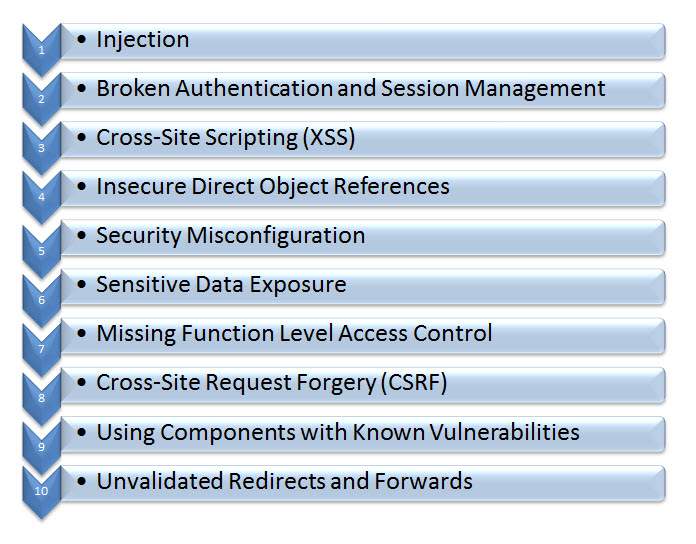
Có nhiều phương pháp khác nhau mà chúng ta có thể sử dụng để thực hiện PenTesting.

* PTES – Penetration Testing Execution Standard.
* OSSTMM – Open Source Security Testing Methodology Manual.
* OWASP – Testing Techniques – Open Web Application Security Protocol.

Trong số này thì OWASP hoạt động rất tích cực và có nhiều cộng đồng đóng góp. Chúng ta sẽ tập trung vào kỹ thuật OWASP.

**OWASP**

Team OWASP đã đưa ra 10 lỗ hổng bảo mật phổ biến trong trang web trong những năm gần đây. Dưới đây là danh sách những sai sót của bảo mật phổ biến trong ứng dụng web. Chúng ta sẽ bàn luận chi tiết tất cả các kỹ thuật này trong các bài học tiếp theo.



**Thực Hành**

Để hiểu rõ từng kỹ thuật, chúng ta hãy làm việc với một ứng dụng mẩu. Chúng ta sẽ thực hiện tấn công vào “WebGoat”, Ứng dụng J2EE được phát triển rõ ràng với các lổ hổng bảo mật cho mục đích học tập.

Các bạn có thể truy cập đường link sau để cài đặt ứng dụng mẩu WebGoat.

<https://github.com/WebGoat/WebGoat/wiki/Installation-(WebGoat-6.0)>

Hoặc có thể truy cập vào chính trang chủ WebGoat để chọn phiên bản và source cài đặt. Vì WebGoat có hổ trợ nhiều ngôn ngữ, .Net có, PHP có …Ở đây AD sử dụng Java.

Nếu các bạn chưa từng biết java, đừng lo lắng AD sẽ chỉ cho các bạn cách đơn giản nhất để chạy ứng dụng này.

Chỉ cần download WebGoat-6.0.1-war-exec.jar sau đó từ terminal gõ lệnh:

java –jar WebGoat-6.0.1-war-exec.jar

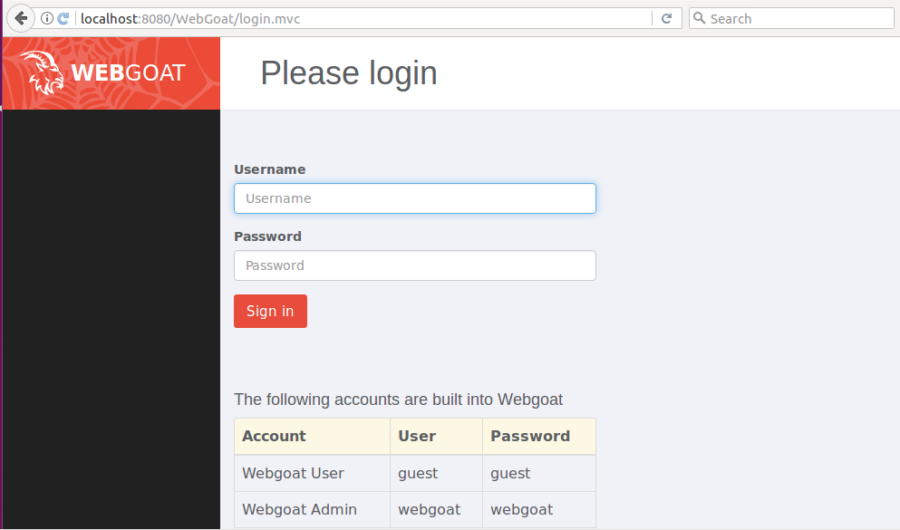
Dĩ nhiên là máy của bạn đã cài đặt java. Nếu các bạn chưa biết cài java như thế nào thì hãy ra google gõ : install java Ubuntu là có ngay. À quên nữa với môn học này chúng ta sẽ sử dụng Linux (Ubuntu) để thực hành nha các bạn, còn nếu bạn nào muốn dùng Window thì hãy tiếp tục với sự quen thuộc của bạn, tuy nhiên nếu gặp khó khan trong qua trình cài đặt hoặc bất cứ vấn đề gì làm trở ngại bạn theo học môn này thì hãy email cho AD nhé.

<http://dammelaptrinh.com/contact> truy cập link này và gửi thư cho AD.

Sauk hi run câu lệnh java –jar WebGoat-6.0.1-war-exec.jar và không có vấn đề gì thì các bạn trở ra trình duyệt gõ truy cập ứng dung:

<http://localhost:8080/WebGoat/attack>

bạn sẽ thấy màn hình như sau:



Xin chúc mừng bạn đã setup thành công ứng dụng mẩu.

Từ màn hình login chúng ta có thể sử dụng các acc được cung cấp sẳn để login vào hệ thống.

Có 2 acc cơ bản cho phiên bản này là : guest/guest và webgoat/webgoat tương ứng với username/pass.

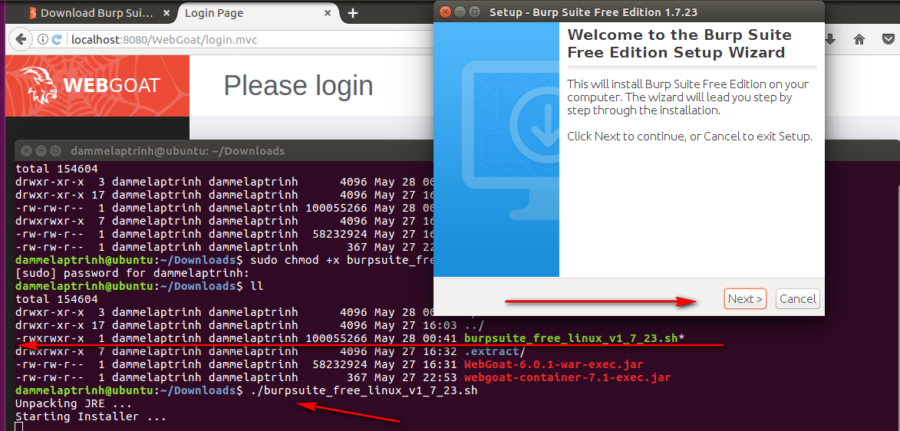
**Web Proxy**

Để đánh chặn lưu lượng giữa client(Browser) và Server(System, nơi mà ứng dụng web WebGoat được cài đặt), chúng ta sẽ phải sữ dụng một web proxy. Chúng ta sẽ sử dụng Burp Proxy và bạn có thể download nó tại:

<http://portswigger.net/burp/download.html>

Nếu bạn dùng Linux thì down file .sh về, window thì chọn file .exe.

Như đầu bài AD sẽ dùng Linux để thực hiện serial này, do vậy bây giờ bạn hãy mở một terminal mới ra và tiến hành chạy file .sh vừa down về để cài đặt, sài version free là đủ cho serial của chúng ta. Nên nhớ cấp quyền cho file thực thi. Quan sát hình cho dể thôi người ơi.

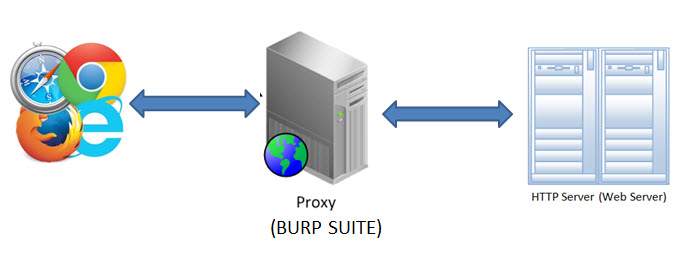


Next next vài phát là hoàn tất cài đặt thôi .

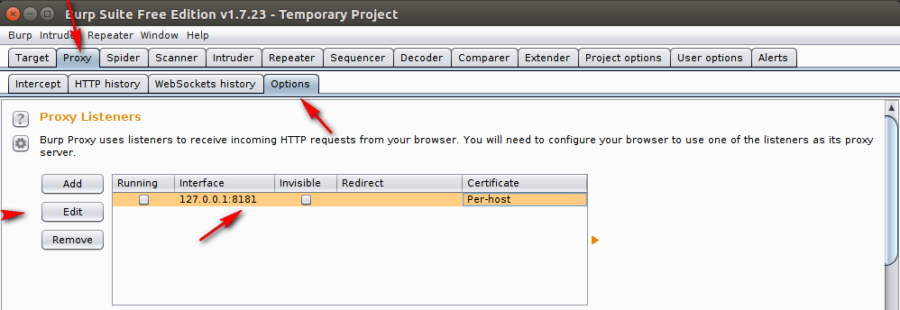
Bây giờ mở Burp ra các bạn chọn cấu hình mặc định rồi next vì là lần đầu nên có cấu hình gì đâu mà chọn.

**CONFIGURING BURP PROXY**

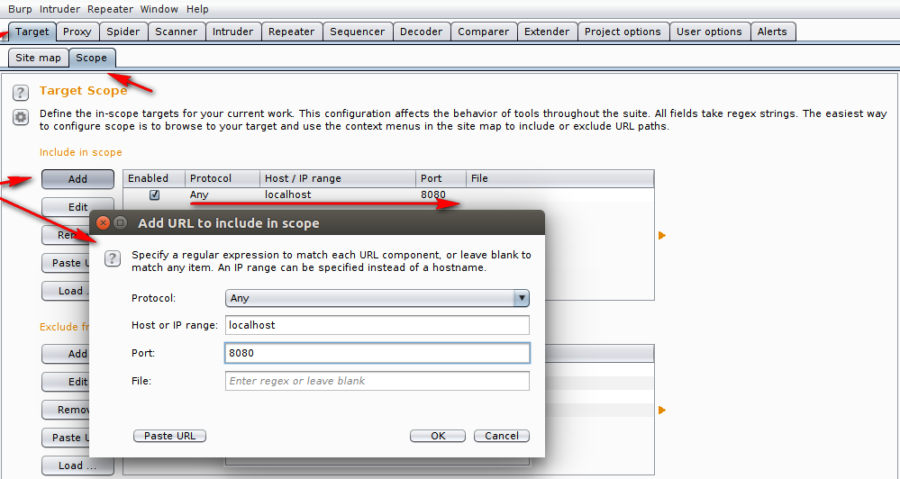
Burp proxy có thể đánh chặn mổi gói thông tin gửi và nhận bởi browser và server. Giúp chúng ta thay đổi nội dung trước khi client gửi thông tin tới Web-Server.



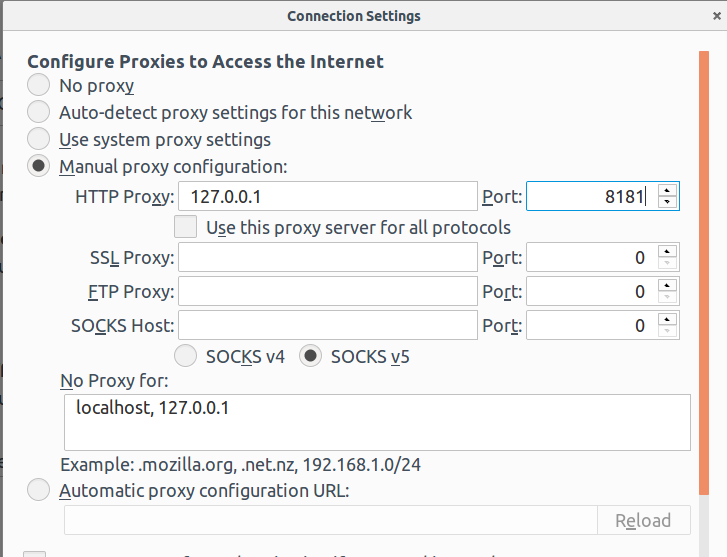
1. WebGoat của chúng ta đã dành port 8080 rồi giờ thì ta cho Burp chạy port 8181 vì mặc định Burp cũng chơi port 8080. Thực hiện như hình dưới nhé.



1. Chúng ta phải đảm bảo rằng Burp nó lắng nghe port 8080 mà WebGoat đang hoạt động để nó ăn cắp traffic, dùng từ ăn cắp như sắp thành tội phạm vậy, hehe gọi là đánh chặn traffic nha các bạn.Làm theo hình nào.



1. Sau cùng làm cho trình duyệt của bạn lắng nghe port 8181 (Burp Proxy port), như vậy là tụi nó sẽ lắng nghe nhau hehe. Do đó chúng ta đã cấu hình Web proxy để đánh chặn traffic giữa client(browser) và server(Webserver).



Cái này là firefox, còn chrome hay trình duyệt khác thì cũng đơn giản thôi ạ, mình không đưa hết vô, các bạn tự xử nhé.

1. Hình ảnh sau giúp bạn hiểu workflow cho các bước cấu hình trên.

