Xin chào cô, xin chào tất cả các bạn

Em tên là Ngô Anh Long và hôm nay em xin thay mặt nhóm số 1, lên tổng kết lại về chủ đề an toàn an ninh mạng và vấn đề được tìm hiểu là TOP 10 những lỗi bảo mật nguy hại nhất năm 2013 (TOP 10 OWASP)

Nội dung bài tổng kết đi qua 2 phần,

Phần 1:

Điểm qua những thông tin về an toàn, an ninh mạng

\_ Thực tế trên thế giới và ở Việt Nam

\_ Hậu quả về những lỗi bảo mật an ninh mạng

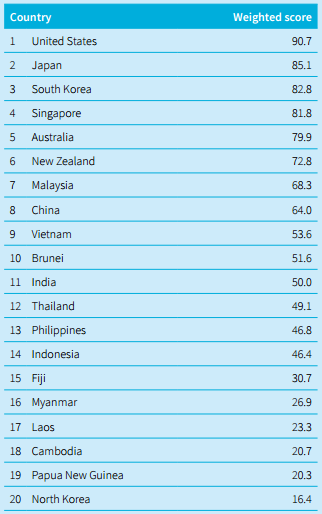
Và phần 2:

TOP 10 các lỗi bảo mật nguy hại trên các ứng dụng WEB

\_ Khái niệm

\_ Cách phòng tránh

Đầu tiên, ta cùng theo dõi **bảng xếp hạng các quốc gia khu vực châu Á - Thái Bình Dương bảo đảm an ninh mạng năm 2015 do Viện Chính sách chiến lược Úc (ASPI) vừa công bố:**



Mỹ vẫn là quốc gia có mức độ bảo mật thông tin cao nhất khu vực, tiếp đến là Nhật Bản, Hàn Quốc và Singapore

Thật vui mừng là Việt Nam đứng thứ 9 trong danh sách này, nhưng, liệu chúng ta có an toàn không ?

Chắc chắn rồi, KHÔNG!

Trong năm 2014 thì Việt Nam đã có tới 4676 trang web bị tấn công, trong đó có các website của chính phủ, hay các website giáo dục, mà trường ta cũng không nằm ngoài số đó, hãy cùng điểm qua một số tin nổi bật

1. **Sau sự kiện cổ động viên Malaysia tấn công cổ động viên Việt Nam tại sân vận động Shah Alam tối 7-12-2014 (vì chiến thắng của đội tuyển bóng đá Việt Nam trước đội tuyển Malaysia), thì ngay sau đó nhiều trang web của Việt Nam đã bị tấn công mạng**

Trong danh sách đó, có website của Công ty VNPT Technology đã bị các hacker Malaysia tấn công và thay đổi giao diện trang chủ

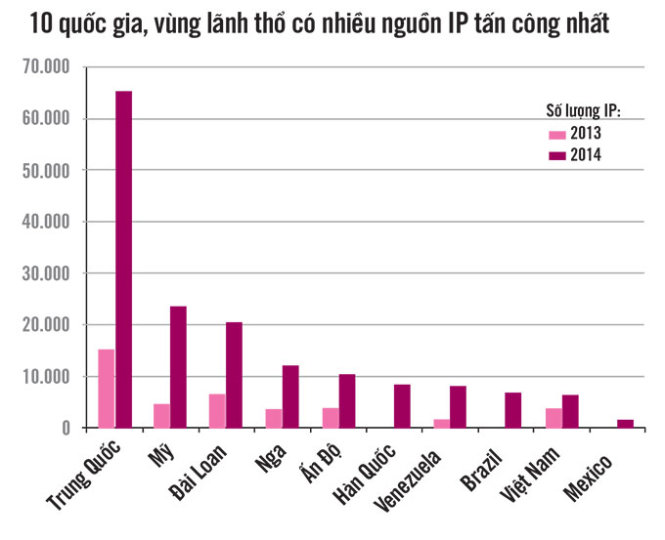
Hay là chính web site của liên đoàn bóng đá việt nam (VFF.org.vn) bị tấn công nắm quyền kiểm soát máy chủ website



1. Vào tháng 10, tháng 11 năm ngoái ta còn nhớ, hàng loạt các báo nổi tiếng như Dantri.com.vn, Giadinh.net.vn, VCCorp.vn, GameK.vn, tấn công Ddos hay sử dụng mã độc cố gắng xóa cơ sở dữ liệu của họ.

Vậy các hacker này ở đâu ra thế ?

Ta hãy cùng xem bảng thống kê 10 quốc gia và vùng lãnh thổ có nguồn IP tấn công nhiều nhất

****

**Chắc chắn rồi, Trung Quốc, nổi tiếng với việc sử dụng và đào tạo các hacker của mình để ăn cắp bí mật kinh doanh, khai thác khoáng sản, sở hữu trí tuệ trên thế giới đứng thứ nhất. Tiếp sau đó là Mỹ, Đài loan.**

**Trong bảng xếp hạng này, Việt Nam cũng đứng thứ 9**

**Vậy hacker này họ đã dùng cách gì, làm như thế nào để tấn công các website này, ta cùng tìm hiểu TOP 10 các vấn đề bảo mật nghiêm trọng nhất (TOP 10 OWASP)**

A10 : Chuyển hướng hoặc chuyển tiếp không an toàn:

Là Chuyển hướng và chuyển hướng không an toàn là liên kết từ trang web tin cậy

sẽ đưa người dùng đến một trang web không tin cậy để lừa đảo hoặc thu thập thông tin

từ người dùng

**Ví dụ như:**

<https://acounts.google.com/ServiceLogin?hl=en&continue=https://www.google.com>

Thì hacker có thể tạo ra một liên kết dạng như:

<https://acounts.google.com/ServiceLogin?hl=en&continue=https://evil.com>

để lừa người dùng tới địa chỉ nào đó

**Lỗi này thì có khả năng khai thác trung bình, không phổ biến, rất dễ phát hiện nhưng rất nhiều người bị mắc lỗi do không để ý hoặc không biết đường dẫn có nguy hiểm không**

**Lỗi chuyển hướng không an toàn này, hiện nay ta có thể dùng tool frontpage của Microsoft đẻ phát hiện, tuy nhiên hầu như các trình duyệt web hiện nay cũng tích hợp chức năng cảnh báo người dùng**

**A9: Tấn công sử dụng các thành phần lỗ hổng đã biết:**

**Cách tấn công này, thường tấn công vào các website quan trọng nhưng vẫn sử dụng các công nghệ cũ(**thư viện, framework, plug-in và các module phần mềm **). Các website chính phủ, hay trường học ở VN là 1 ví dụ**

**Phương pháp tấn công**: Hacker xác định điểm yếu thông qua scan hoặc phân tích bằng tay

**A8: Giả mạo yêu cầu:**

**Với cách này,các hacker sẽ sử dụng quyền chứng thực từ trình duyệt của người sử dụng tới các trang web, sau đó sử dụng quyền chứng thực này để giả mạo yêu cầu của người dùng vào mục đích của hacker**

**Lỗi này giống lỗi A2(**Sai lầm trong kiểm tra định danh và phiên làm việc

**)**

**Tuy nhiên lỗi A2 thường được che giấu trong email lỗi này lại thường được giấu trong các thành phần của một trang web**

**Ví dụ như, hacker có thể có thể chèn vào sau một đoạn bức ảnh trong một bản tin như sau:**

X là một admin của một trang web đen và Y là người thường sử dụng trang web đen đó. X là một người có ý đồ xấu, nên chèn vào sau một vài bức ảnh trên web trong thuộc tính src, của mình đoạn code có dạng như sau:

<img src="<http://examplebank.com/app/transferFunds?amount=1500&destinationAccount=>... >

Y vừa giao dịch đăng nhập tài khoản vào ngân hàng example để kiểm tra tài khoản xong và vào website của X như thường ngày

Thì người dùng Y sẽ chuyển 1500$ cho tài khoản X. Tất nhiên lúc này người dùng còn chưa hết thời session trên web

A7: Mất kiểm soát mức độ truy cập chức năng:

Hầu hết các trang web đều có 1 hàm phân quyền cho người dùng. Nhưng nếu hàm đó không được đồng bộ thì kẻ tấn công sẽ lợi dụng điều này để làm lợi cho mình.

Ví dụ như: trên trang web zing.mp3 người bình thường chỉ được tải nhạc 128kbp với đường link:

[**http://mp3.zing.vn/bai-hat/Rang-Em-Mai-O-Ben-Bich-Phuong/ZW7WFD9B.html**](http://mp3.zing.vn/bai-hat/Rang-Em-Mai-O-Ben-Bich-Phuong/ZW7WFD9B.html)

**Nhưng hàm phân quyền của Zing không tốt: nên ta muốn tải nhạc vip chỉ cần**

**Copy mã bài hát vào sau đường link http://mp3.zing.vn/download/vip/song/ và paste vào trình duyệt**

**http://mp3.zing.vn/download/vip/song/** **ZW7WFD9B**

**A6: Lộ dữ liệu nhạy cảm**

**Lỗi này không phổ biến, khó phát hiện, nhưng ảnh hưởng thì rất nặng nề.**

Bằng cách này hacker sẽ tìm các khóa, lấy các bản sao dữ liệu không được mã hóa, hoặc truy cập dữ liệu qua các kênh có thể tự động giải mã.

**Để lấy :** dữ liệu nhạy cảm như hồ sơ y tế, thông tin, dữ liệu cá nhân, thẻ tín dụng

**A5: Sai sót trong cấu hình an ninh**

**A4: lỗi bảo mật đối tượng tham chiếu thiếu an toàn**

**Các trang web thường tương tác với người dùng thông qua các dữ liệu mà người dùng đưa vào, qua các editText, để biết họ là ai, họ cần gì, từ đó website lấy các đoạn text để xử lí xem họ cần gì.**

**Tuy nhiên thì một vài website lại không kiểm tra đầu vào kĩ, các hacker có thể lợi dụng điều này để làm những điều xấu. Đó là cách thực hiện chung của A3 chèn mã script xấu và A1 Tiêm nhiễm mã độc**

**A3:**  Là một kiểu tấn công cho phép hacker chèn vào những đoạn script độc hại (thông thường là javascript hoặc HTML) vào website và sẽ được thực thi ở trình duyệt người dùng.

**Cookie** : Hacker có thể lấy được cookie của người dùng và dùng thông tin trong cookie để giả mạo phiên truy cập.

**Keylogging** : Hacker có thể ghi lại những thao tác gõ phím của người dùng bắng cách sử dụng sự kiện addEventListenner trong javascript sau đó sẽ phân tích dữ liệu đó và tìm ra các mật khẩu hay mã ngân hàng.

**Phishing**: Hacker có thể thay đổi giao diện website bằng cách thay đổi cấu trúc HTMLtrong trang web để đánh lừa người dùng,khi đó chúng có thể tạo các forrm đăng nhập giả để lấy mật khẩu.

**A1 Tiêm nhiễm mã độc: Hacker có thể chèn vào những đoạn mã SQL xấu nhằm chiếm quyền điều khiển, xóa cơ sở dữ liệu, ăn cắp trong csdl những thông tin nhạy cảm.Điều này đã được thực hiện trong vụ tấn công VCCorp. Kẻ tấn công liên tục chiếm quyền điều khiển và cố gắng xóa mọi dữ liệu trong csdl**

**Đi qua 10 lỗi bảo mật trên, để phòng tránh tối ưu nhất các lỗi nghiêm trọng này ta cần:**

**\_ Sử dụng các phần mềm diệt virut khi sử dụng máy tính cá nhân**

**\_ Cẩn thận, chú ý, kiểm tra đầu vào dữ liệu, quyền truy nhập chặt chẽ trước khi thực thi**

**\_ Sử dụng các tool bảo mật để lập trình an toàn**

**\_ Không vào các web đen, web xấu**

**\_ Không tò mò click vào các link lạ**

**\_ Không cài đặt và sử dụng các phần mềm không tin tưởng**

**\_ Không đặt mật khẩu quá dễ dàng và thay mật khẩu thường xuyên**

**Bên trên là bài tổng kết về chủ đề Network security mà nhóm được phân công tìm hiểu, các bạn quan tâm tìm hiều có thể tới thăm link gitbook.com của bọn mình để được biết rõ hơn.**

**Bài tổng kết chủ đề của bọn mình tới đây là kết thúc. Cảm ơn cô và các bạn đã lắng nghe**