

Module 13

Tấn Công Trang Web

Những Nội Dung Chính Trong Chương Này

GUI Web Hacking

Tấn Công Dựa Trên URL

Những Điểm Yếu Thông Dụng Của Ứng Dụng Web

Các Công Cụ Tấn Công Ứng Dụng Web

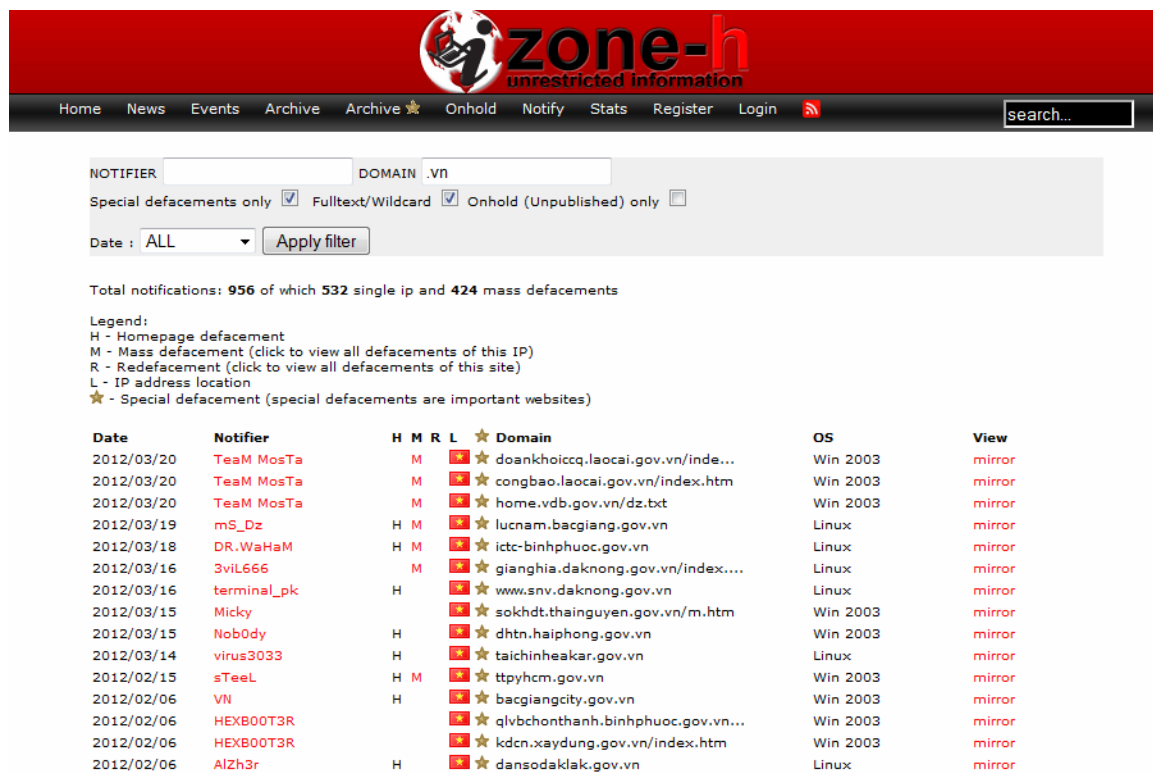
Google Hacking

Phương Pháp Tăng Cường An Ninh Cho Trang Web

Các Kỹ Thuật Bẻ Khóa Mật Khẩu Của Trang Web

Web application hay ứng dụng web là các chương trình chạy trên các web server như <http://vncert.gov.vn/> và được phân loại theo các chức năng của ứng dụng như Forum là trang web về diễn đàn, chia sẻ thông tin, CMS / Blog là những web site của cấp nội dung, thông tin hay các trang về mạng xã hội, những ứng dụng quản lý công việc, quản lý khách hàng hay kinh doanh trực tuyến.

Hacker đặc biệt quan tâm đến các trang web của những tổ chức lớn hay các site của cơ quan nhà nước như những tên miền .gov.vn ở Việt Nam. Ngoài ra, các hacker ngày nay bên cạnh ý thích trình diễn, khoe khoang còn hành động vì mục tiêu kinh tế nên họ hay đưa các trang thương mại điện tử vào danh sách ưu tiên của họ, vì ở đó có những thông tin quan trọng như thẻ tín dụng của khách hàng, các tài khoản ngân hàng trực tuyến ... Sau khi tấn công, các hacker hay khoe chiến tích trên trang zone-h tại địa chỉ <http://www.zone-h.org/> , đây được xem như là một bảng phong thần của các trang web như hình minh họa sau là danh sách các trang web có tên miền .vn đã bị tấn công và có khả năng chưa được vá hay nhận biết.



Date	Notifier	H	M	R	L	Domain	OS	View
2012/03/20	TeaM MosTa				M	doankhoicq.laocai.gov.vn/inde...	Win 2003	mirror
2012/03/20	TeaM MosTa				M	congbao.laocai.gov.vn/index.htm	Win 2003	mirror
2012/03/20	TeaM MosTa				M	home.vdb.gov.vn/dz.txt	Win 2003	mirror
2012/03/19	mS_Dz	H	M			lucnam.bacgiang.gov.vn	Linux	mirror
2012/03/18	DR.WaHaM	H	M			ictc-binhphuoc.gov.vn	Linux	mirror
2012/03/16	3vIL666				M	gianghia.daknong.gov.vn/index....	Linux	mirror
2012/03/16	terminal_pk				H	www.snv.daknong.gov.vn	Linux	mirror
2012/03/15	Micky					sokhdt.thainguyen.gov.vn/m.htm	Win 2003	mirror
2012/03/15	Nob0dy				H	dhtn.haiphong.gov.vn	Win 2003	mirror
2012/03/14	virus3033				H	taichinheakar.gov.vn	Linux	mirror
2012/02/15	sTeel	H	M			ttpyhcm.gov.vn	Win 2003	mirror
2012/02/06	VN				H	bacgiangcity.gov.vn	Win 2003	mirror
2012/02/06	HEXB00T3R					qlvbchonthanh.binhphuoc.gov.vn...	Win 2003	mirror
2012/02/06	HEXB00T3R					kdcn.xaydung.gov.vn/index.htm	Win 2003	mirror
2012/02/06	AlZh3r				H	dansodaklak.gov.vn	Linux	mirror

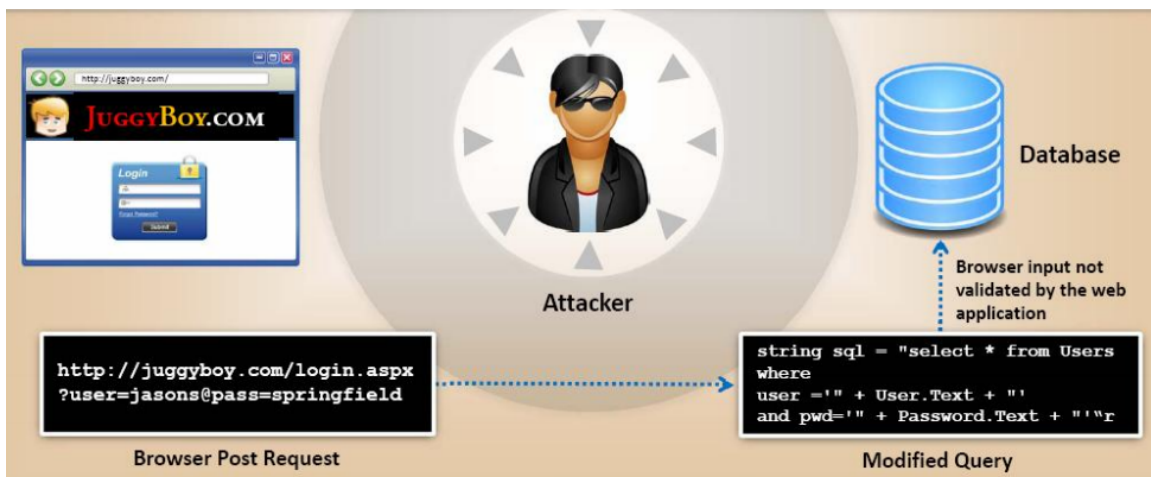
Hình 13.1 – Các trang web Việt Nam bị tấn công và công bố trên zone-h.org

Đa số các ứng dụng web ngày nay hoạt động theo mô hình client / server với các trình duyệt web như Firefox, IE, Chrome là web client còn những máy chủ web là phía server như Apache, IIS, TomCat .Những công nghệ phổ biến để xây dựng các web site hiện nay là ASP, PHP, JavaScript ... Mỗi kỹ thuật có những điểm mạnh và yếu riêng cho nên khi tấn công hacker điều phải nghiên cứu cẩn thận để xác định chính xác các hệ điều hành, máy chủ web, công nghệ triển khai web site để đưa ra phương án tấn công hiệu quả. Các hình thức tấn công ứng dụng web thông dụng mà chúng ta cần biết đó là :

- Thao tác trực tiếp trên ứng dụng thông qua giao diện web trực quan (GUI) của nó gọi là GUI Web Hacking.
- Tiến hành khai thác với Uniform Resource Identify hay còn gọi là URL (URL Hacking)
- Khai thác các thành phần của HTTP mà không có trong URL

GUI Web Hacking

Là việc thao tác trực tiếp trên giao diện web application hay sử dụng các công cụ audit website như Havij, WebAcunetix ... mà trong các bài học sau chúng ta sẽ trình bày. Các bạn có thể xem hình ảnh minh họa một khái thác để tìm kiếm lỗi SQL Injection trên trang web mẫu của FoundStone như hình sau ...



Hình 13.2 – Gui Web Hacking

Trên hình minh họa các attacker nhập trực tiếp giá trị 'OR 1=1— nhằm vượt qua cơ chế kiểm soát của ứng dụng nếu việc kiểm tra tính hợp lệ của các giá trị INPUT không được thực hiện đầy đủ. Đây là một trong những lỗi thông dụng nhất mà các website thường mắc phải và được attacker rất quan tâm

Tấn Công Dựa Trên URL

Các HTTP method là những hành động được tiến hành tại ứng dụng web và web client. are the type of action performed on the target resource. Trong HTTP RFC có định nghĩa các hành động này và ứng dụng WEBDAV trên nên máy chủ IIS của Windows có bổ sung một số phương pháp khác nhưng nhìn chung các ứng dụng web sử dụng 2 hàm sau : GET và POST. GET dùng để yêu cầu thông tin, còn POST để gửi thông tin và cả POST

và GET đều có thể gửi thông tin đến server với một điểm khác biệt quan trọng giữa chúng là GET để data trong URL trong khi đó POST đặt dữ liệu (data) trong phần body (thân) của request và không hiển thị trong URL. Vì vậy POST được dùng để submit dữ liệu đến web application như khi chúng ta cung cấp thông tin tên, địa chỉ khi đăng ký mua hàng trực tuyến là đang sử dụng hàm POST. Tuy vậy, việc không hiển thị thông tin của POST không hẳn là bảo vệ dữ liệu tốt hơn GET, đây cũng là một trong những điểm thường gây nhầm lẫn đối với người dùng, vì với các hacker thì việc tìm kiếm thông tin được che dấu bởi POST không phải là vấn đề quá khó khăn.



Hình 13.3 – Minh họa tấn công dựa trên URL

HTTP header thường được dùng để lưu trữ các thông tin mở rộng như các giáo thức vận chuyển hay những yếu tố bảo mật liên quan gồm có :

- Authorization xác định có hay không những cơ chế bảo mật kèm theo yêu cầu như là Basic authentication, Certificate ...
- Cache-control xác định có lưu cache các yêu cầu này trên một máy chủ trung gian hay không.
- Referer Liệt kê source URI .
- Cookies được dùng để lưu trữ thẻ bài (token) trong quá trình xác thực dựa trên phiên làm việc của client.

Sau đây là một ví dụ về các hàm được sử dụng bởi công cụ netcat kết nối đến máy chủ `www.test.com` server trên TCP port 80 (port chuẩn cho giao thức HTTP; HTTPS là TCP 443), và yêu cầu của kết nối này là lấy về tập tin `/test.html`. Đường dẫn đầy đủ của yêu cầu này là <http://www.test.foo/test.html>.

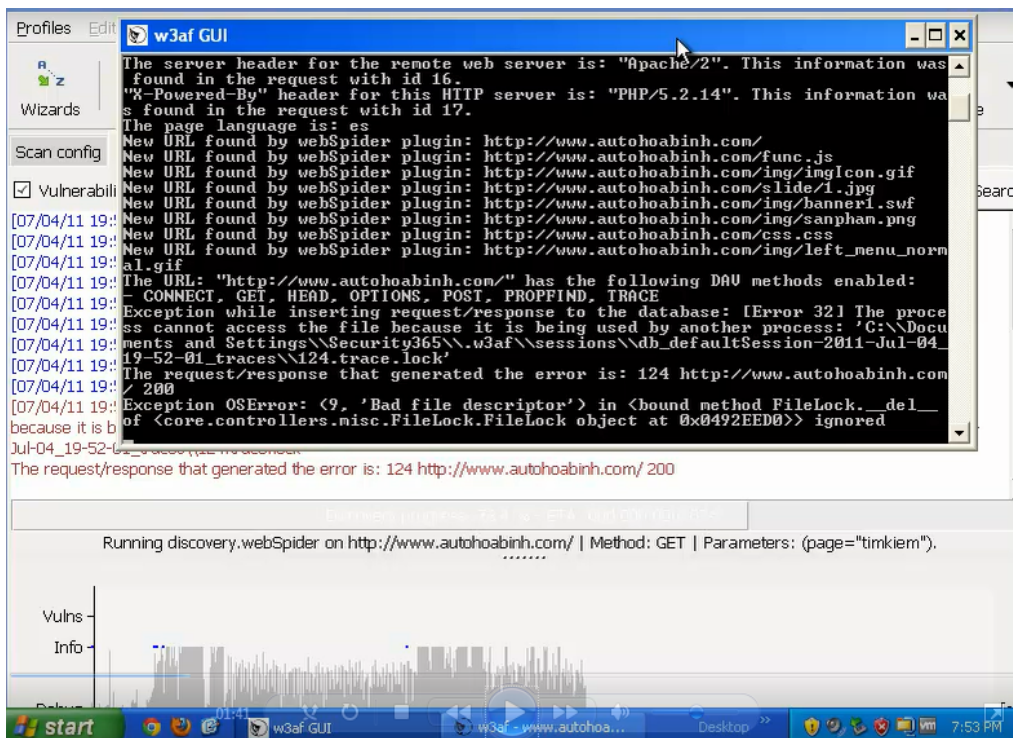
```
www.test.foo [10.124.72.30] 80 (http) open
GET /test.html HTTP/1.0
HTTP/1.1 200 OK
Date: Mon, 04 Feb 2002 01:33:20 GMT
Server: Apache/1.3.22 (Unix)
Connection: close
Content-Type: text/html
<HTML><HEAD><TITLE>TEST.FOO</TITLE>etc.
```

Trong ví dụ này các bạn có thể thấy hàm GET trong yêu cầu từ client được sử dụng bởi netcat và đáp ứng trả về trong phần header của máy chủ là Server: Apache/1.3.22 (Unix), còn phần dữ liệu (response body data) nằm trong khung (BODY)

`<HTML><HEAD><TITLE>TEST.FOO</TITLE>`.

Tuy nhiên dù cho hacker sử dụng những phương pháp tấn công nào thì như đã trình bày mục tiêu chính của họ vẫn là những thông tin có trong các trang web này, có thể đó là những công văn hay tài liệu quan trọng, hoặc là thông tin về khách hàng của trang web như danh sách email, số thẻ tín dụng. Và để đạt được mục tiêu hacker cần tiến hành quy trình tấn công theo đúng trình tự như sau :

- **Scanning** : Quét lỗi trang web, tìm kiếm các thông tin hữu ích về máy chủ.
- **Information Gathering** : Tập trung các thông tin chính,
- **Test** : Thử nghiệm một số phương án.
- **Planning Attack** : Hoạch định phương án tấn công như dùng proxy nào, sử dụng công cụ gì để tấn công.
- **Luanching Attack** : Khởi động cuộc tấn công



Hình 13.4 - Audit trang web với W3AF

Lưu ý video minh họa này chỉ dùng cho mục đích đào tạo, nghiên cứu. Không được ứng dụng thực tế. Xem demo tại đây : <http://www.youtube.com/watch?v=ugIxUtbFH-o&feature=youtu.be>

Những Điểm Yếu Thông Dụng Của Ứng Dụng Web.

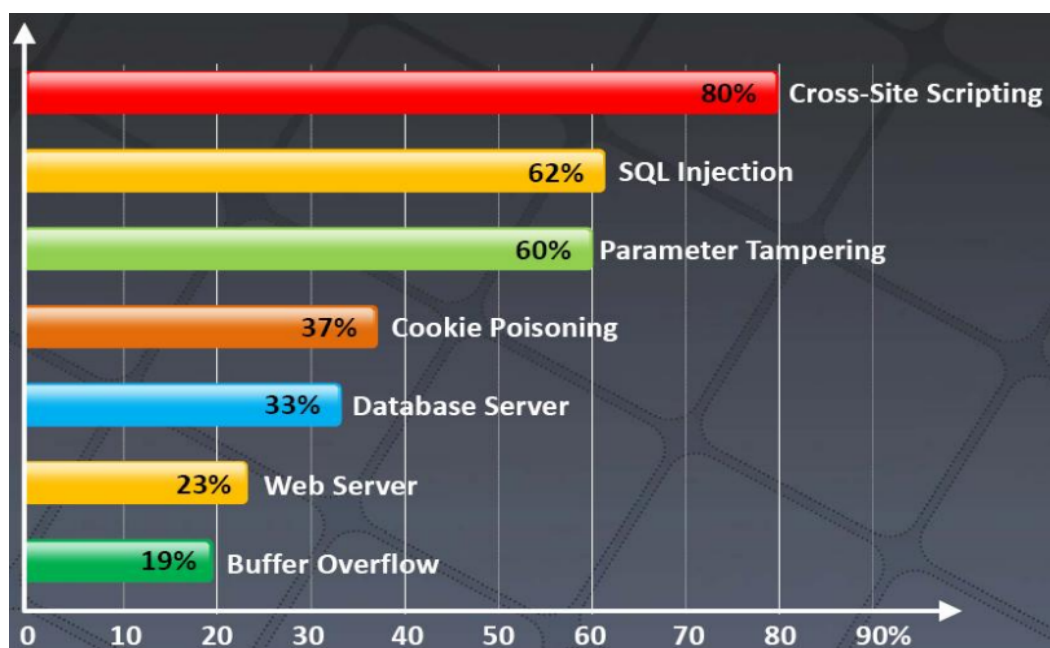
Có nhiều mối nguy hiểm mà các trang web có thể mắc phải, những mối đe dọa hàng đầu mà chúng ta thường nghe đến là SQL injection, XSS, Authentication Hijacking.. Trong vai trò CEH chúng ta cần nắm ý nghĩa của các lỗi này và một số công cụ khai thác thịnh hành :

- **Cross-site scripting** : Lỗi này cho phép hacker thực thi các đoạn mã nguy hiểm thông qua các khung tiếp nhận dữ liệu của trang web như ô tìm kiếm.
- **SQL injection** : Một lỗi có tỉ lệ bị hacker tận dụng rất cao, cho phép hacker chạy các câu lệnh SQL từ trình duyệt và xem nội dung của các bảng, cột chứa thông tin quan trọng. Các bạn có thể tham khảo video minh họa kèm theo ở phần trên.
- **Buffer Overflow** : Một số lượng lớn các dữ liệu hời đến ứng dụng web thông qua các biểu mẫu gây nên tràn bộ đệm.
- **Cookie poisoning và Authentication hijacking** : Hacker đánh cắp cookie của một phiên làm việc giữa web client và web server, sau đó truy cập vào khu vực

riêng tư của người sử dụng, demo
http://www.youtube.com/watch?v=zLdB3UgDi_I

- **Directory travelsal / Unicode** : Hacker truy vấn hệ thống tập tin và thư mục hệ thống thông qua trình duyệt web hay windows explorer.

Sau đây là danh sách các lỗi bảo mật của *web application* mà hacker thường tận dụng để tấn công do mà tài liệu CEH công bố, trong đó dẫn đầu là những lỗi liên quan đến *XSS (Cross-Site Scripting)*, tiếp theo sau là *SQL Injection*, *Parameter Tampering*, *Cookie Poisoning* ...



Hình 13.4 – Các lỗi ứng dụng web hay bị tấn công

Ngoài danh sách trên, các bạn có thể tham khảo thêm các nguồn thông tin về 10 lỗi bảo mật thông dụng do OWASP thống kê tại <https://www.owasp.org/index.php/Vietnam> , trong danh sách đang tin cậy này chúng ta nhận thấy có đôi chút khác biệt về tỉ lệ giữa những lỗi hay bị ảnh hưởng như xếp đầu bảng là SQL Injection (được gọi là lỗi nhúng mã) nhưng nhìn chung thì các lỗi liên quan đến SQL injection, XSS, hư hỏng cơ chế chứng thực và quản lý phiên làm việc là những mối quan tâm mà các bạn nên đặt lên hàng đầu.

OWASP Top 10 – 2007	OWASP Top 10 – 2010 (Mới)
A2 – Lỗi nhúng mã	A1 – Lỗi nhúng mã
A1 – Thực thi mã script xấu (XSS)	A2 – Thực thi mã script xấu (XSS)
A7 – Hư hỏng cơ chế chứng thực và quản lý phiên làm việc	A3 – Hư hỏng cơ chế chứng thực và quản lý phiên làm việc
A4 – Đối tượng tham chiếu thiếu an toàn	A4 – Đối tượng tham chiếu thiếu an toàn
A5 – Giả mạo yêu cầu (CSRF)	A5 – Giả mạo yêu cầu (CSRF)
<từng là T10 2004 A10 – Cấu hình hệ thống không an toàn>	A6 – Sai sót cấu hình an ninh(NEW)
A8 – Lưu trữ mật mã không an toàn	A7 – Lưu trữ mật mã không an toàn
A10 – Sai sót hạn chế truy cập	A8 – Sai sót hạn chế truy cập
A9 – Thiếu bảo vệ lớp vận chuyển	A9 – Thiếu bảo vệ lớp vận chuyển
< không ở trong T10 2007>	A10 – Chuyển hướng và chuyển tiếp thiếu thẩm tra(NEW)
A3 – Thực thi tập tin độc	<không nằm trong T10 2010>
A6 – Thất thoát thông tin và xử lý lỗi không đúng cách	<không nằm trong T10 2010>

Hình 13.5 – Danh sách 10 lỗi ứng dụng web hàng đầu

Các Công Cụ Tấn Công Ứng Dụng Web

Acunetix Web Security Scanner Ứng dụng hàng đầu phải kể đến đó là Web Acunetix Scanner, một chương trình thương mại dùng cho việc tìm kiếm các lỗi bảo mật của web site như XSS, SQL injection, Directory Traversal ...

Havji Là chương trình tự động khai thác lỗi SQL injection mà chúng tôi có minh họa qua video hướng dẫn, đây là công cụ miễn phí được đa số các hacker sử dụng hiện nay để tấn công và xem các thông tin trong cơ sở dữ liệu.

Burpsuite Gồm nhiều công cụ mạnh mẽ từ quét lỗi trang web cho đến các chức năng proxy, chặn dữ liệu trong quá trình truyền sau đó thay đổi và gửi về máy chủ.

BlackWidow Có thể scan và tạo lập sơ đồ của trang web.

Teleport Pro Có khả năng toàn bộ nội dung của một trang web để xem offline

Google Hacking

Google hacking là kỹ năng tìm kiếm nâng cao với công cụ tìm kiếm của Google nhằm xác định các thông tin nhạy cảm của mục tiêu. Nếu không được cấu hình chặt chẽ thì các thông tin như mật khẩu đăng nhập, các tài liệu riêng tư có thể bị hacker đánh cắp chỉ với ứng dụng tìm kiếm Google. Có nhiều tài liệu về chủ đề này được đề cập tại trang web

<http://johny.ihackstuff.com> hay chuyên trang <http://www.exploit-db.com/google-dorks/> cung cấp những cụm từ tìm kiếm nhằm xác định các điểm nhạy cảm của trang web.



Hình 13.6 - Trang web cung cấp những cụm từ tìm kiếm liên dùng cho việc khai thác

Những Phương Pháp Tăng Cường An Ninh Cho Web

Trước đây, hãng Microsoft đã tổ chức một cuộc thi cho phép các hacker tấn công vào hệ thống ứng dụng và máy chủ web được xây dựng trên nền tảng của hãng như cơ sở dữ liệu SQL Server, hệ điều hành Windows, nền tảng lập trình ASP. Cuộc thi này có tên là Open hack và chỉ sau một thời gian ngắn phát động cuộc thi ban tổ chức đã ghi nhận có đến hơn 40.000 đợt tấn công, tuy nhiên các hacker không cách nào xâm nhập được vào hệ thống máy chủ hay gây tổn hại đến các trang web mục tiêu mà ban tổ chức đã dựng lên. Vậy họ đã sử dụng quy trình kiện toàn bảo mật cho ứng dụng web như thế nào mà đem đến sự vững chắc như vậy? Tất cả những điều này đã được các kỹ sư của Microsoft tiết lộ trong tài liệu hướng dẫn tăng cường an ninh cho web application có tên gọi là “Improving Web Application Security: Threats and Countermeasures” tại địa chỉ : <http://msdn.microsoft.com/en-us/library/ff649874.aspx> , đây cũng là tài liệu mà tôi đã dùng để hướng dẫn trong chương trình bảo mật ứng dụng web cho Tập đoàn EVN tại Đồ Sơn, Hải Phòng và cuối năm 2011.

Sau đây là một số hướng dẫn để tăng cường an ninh cho ứng dụng web mà chúng ta cần quan tâm :

- *Cross-site scripting* : Để phòng tránh dạng tấn công này ta cần kiểm tra tính hợp lệ của các dữ liệu đầu vào, các cookie, những yêu cầu truy vấn hay các thông tin ẩn kỹ càng. Dùng công cụ quét lỗi chuyên dụng cho trang web như Web Acunetix Scanner để phát hiện xem có những lỗi XSS trên website.
- *SQL injection / Command injection* : Đóng vai trò hacker để tiến hành quét lỗi SQL injection trên trang web với công cụ như W3AF (Web Application Attack and Audit Framework, download tại <http://w3af.sourceforge.net/>). Và kiểm tra các biến người dùng chặt chẽ, áp dụng các cơ chế lọc ký tự đặc biệt qua tập tin .htaccess hay các module chuyên dùng cho việc phòng chống SQL injection.

- *Cookie poisoning* : Không lưu trữ mật khẩu trong cookie, thiết lập thời gian tồn tại và cơ chế xác thực thích hợp cho các cookie.
- *Buffer overflow* : Kiểm tra kích thước của các biên do người dùng cung cấp để chương trình không bị vượt quá khả năng kiểm soát, có xử lý các tình huống ngoại lệ đầy đủ ngăn không cho hacker lợi dụng chèn những chỉ thị độc.
- *Authentication hijacking* : Sử dụng SSL để mã hóa dữ liệu truyền.
- *Directory traversal / Unicode* : Cần cài đặt các bản vá lỗi và cập nhật đầy đủ, thiết lập quyền truy cập thư mục và tập tin chặt chẽ theo nguyên tắc least privilege (chỉ cấp quyền vừa đủ cho người dùng dựa trên nhu cầu)

Các Kỹ Thuật Bẻ Khóa Mật Khẩu Của Trang Web

Là một CEH chúng ta cần nắm rõ một số kỹ thuật mà các hacker thường dùng để bẻ khóa mật khẩu của ứng dụng web. Bao gồm các phương pháp xác thực mà ứng dụng web sử dụng, thế nào là password cracker cũng như xác định và phân loại các kỹ thuật password-cracking để có những biện pháp phòng chống thích hợp. Chúng ta sẽ đề cập đến những khái niệm trong phần tiếp sau đây.

Các Dạng Xác Thực Của Web Server Và Web Application

Web server và web application hỗ trợ nhiều phương pháp xác thực khác nhau. Phổ biến nhất là xác thực dựa trên HTTP với hai dạng HTTP authentication là : basic và digest. Trong mô hình xác thực cơ bản (basic), quá trình xác thực HTTP sẽ gửi các thông tin tài khoản và mật khẩu dưới dạng cleartext (không mã hóa) trong khi đó với digest authentication thì mô hình xác thực của HTTP sẽ tiến hành băm thông tin tài khoản, ngoài ra giữa client và server cần tiến hành một bước thử thách gọi là challenge-response nhằm nâng cao tính an toàn cho quá trình giao dịch.

Rõ ràng, khi thông tin được gửi dưới dạng *cleartext* thì tính an toàn rất thấp về hacker sẽ dễ dàng đánh cắp mật khẩu cùng tên đăng nhập bằng các công cụ sniffer.

Ngoài hai phương pháp trên thì trong mô hình xác thực của máy chủ và ứng dụng web còn hỗ trợ NTLM (mô hình xác thực trên nền tảng của hệ điều hành Windows), sử dụng chứng chỉ điện tử như khi chúng ta dùng giao thức https:// hay sử dụng thẻ bài và cao cấp nhất là cơ chế xác thực sinh trắc học dựa trên các đặc điểm nhận dạng của người dùng như vân tay, giọng nói, võng mạc ...

Trong các cơ chế xác thực trên thì NTLM sử dụng Internet Explorer và IIS webserver , vì cơ chế này hoạt động trên nền tảng của Windows cho nên rất thích hợp cho các quá trình kiểm tra trong các hệ thống nội bộ hay mạng intranet dùng hệ điều hành Windows. Đối với các hệ thống máy chủ như Windows Server 2000/2003/2008 thì có thể tận dụng

Keberos để nâng cao tính an toàn cho quá trình xác thực của ứng dụng hay máy chủ web. Trong khi đó, xác thực dựa trên chứng chỉ điện tử hay certificate dùng các x.509 certificate để triển khai cặp khóa public và private key. Ở đây chúng ta không đi sâu vào công nghệ này nhưng các bạn cần lưu ý đây là một trong công nghệ thịnh hành trong việc xác thực người dùng với máy chủ hay ứng dụng web.

Còn đối với xác thực bằng token như SecureID mà chúng ta thường thấy triển khai tạo các ngân hàng trong quá trình chuyển khoản trực tuyến, mỗi khi cần đăng nhập hay thực hiện giao dịch chúng ta sẽ nhận một mã số được gửi đến hay phát sinh ngẫu nhiên trên một thiết bị phần cứng, và khi nhập chính xác thông tin này chúng ta mới được đăng nhập hay xử lý giao dịch. Ví dụ như thiết bị SecureID của ngân hàng TechComBank.

Password Cracker Là Gì ?

Password cracker là những chương trình được thiết kế để bẻ khóa mật khẩu hay vô hiệu hóa cơ chế kiểm tra của ứng dụng. Các công cụ này thường sử dụng các kỹ thuật dò mật khẩu dựa trên từ điển hay dùng kỹ thuật quét cạn để phá mật khẩu.

Trong quá trình bẻ khóa mật khẩu thông qua từ điển cracker (ta dùng thuật ngữ này thay cho hacker) sẽ tạo một danh sách các mật khẩu tiềm năng trong dữ liệu của từ điển, thông qua các chương trình tạo từ điển mật khẩu hay tải những từ điển được tạo sẵn từ internet. Sau đó các mật khẩu này sẽ được mã hóa hay băm với các thuật toán hash thường được dùng trong quá trình băm các mật khẩu như MD5. Và để bẻ khóa mật khẩu của ứng dụng thì các mật khẩu đã được xử lý trong từ điển được so sánh với mật khẩu thực sự cho đến khi xảy ra sự trùng khớp (máy chủ hay ứng dụng xác thực thành công) thì quá trình bẻ khóa hoàn tất. Các mật khẩu bị bẻ khóa thường được lấy trong tập tin SAM (Security Account Manager) hay tập tin /etc/passwd trên các máy chủ web dùng hệ điều hành linux (khi hacker tấn công vào các trang web họ sẽ upload các trojan như c99, rv57 để tải về tập tin này).

Nhưng phương pháp dò từ điển này khó thành công với những mật khẩu mạnh, vì không thể tập hợp đủ các dữ liệu cần thiết cũng như thời gian tiến hành không thực tế. Trong những trường hợp đó phương pháp dò mật khẩu theo kỹ thuật quét cạn hay brute-force sẽ được áp dụng. Brute-force sẽ thử tất cả các tình huống kết hợp của những ký tự để tạo ra mật khẩu. Lấy ví dụ đơn giản nếu như mật khẩu chỉ được tạo ra từ 3 ký tự 1,2,3 thì chỉ có tối đa 8 kết quả vì vậy công cụ chỉ cần so sánh tối đa 8 lần là tìm ra mật khẩu gốc. Tuy nhiên, trong thực tế các mật khẩu sẽ phức tạp hơn nhiều cho nên quá trình bẻ khóa diễn ra lâu hay nhanh phụ thuộc vào độ mạnh của thuật toán và cấu hình phần cứng của máy chủ dùng để bẻ khóa. Chương trình thông dụng trong lĩnh vực này thường được đề cập trong CEH chính là L0phtCrack, Join the ripper, Ophcrack ... Những ứng dụng mạnh mẽ thường kết hợp cả hai phương pháp dò mật khẩu trên và kỹ thuật này gọi là Hybrid.

Tổng Kết

Trong chương này chúng ta đã thảo luận về những mối đe dọa hàng đầu đồng với sự an toàn của ứng dụng web qua thống kê của tài liệu CEH hay trong danh sách 10 mối nguy hiểm hàng đầu của OWASP. Với những mối đe dọa hay dạng tấn công nguy hiểm cần có những cách thức khắc phục riêng, nhưng trước tiên chúng ta cần phải tiến hành hardening cho các hệ thống máy chủ để kiện toàn bảo mật ứng dụng web.

Về các kỹ thuật bề khóa mật khẩu các bạn cần phân biệt hai tình huống chính là bề khóa dựa trên từ điển khác với bề khóa quét cạn như thế nào. Và để phòng chống bị bề khóa mật khẩu thì các quản trị viên cần áp dụng các chính sách mật khẩu mạnh với độ dài mật khẩu ít nhất là 8 ký tự, có sự kết hợp giữa chữ hoa, chữ thường, số kèm các ký tự đặc biệt. Ngoài ra, phải bật các chế độ audit, ghi nhật ký thích hợp để có thể dò tìm những tình huống bị tấn công. Đặc biệt, hãy sao lưu cẩn thận để phòng khi có rủi ro xảy ra thì vẫn có thể phục hồi dữ liệu, đưa hệ thống vào hoạt động nhanh chóng.