Google Hacks toàn tập

Giới thiệu

Tôi đã nghĩ về việc công bố bài báo này từ lâu nhưng vì thiếu thời gian nên tôi đã không thể hoàn thành nó. Tôi đã bổ sung và cập nhật bài báo này khi tôi đã mệt mỏi với công việc nghiên cứu hàng ngày.

Google là máy tìm kiếm mạnh mẽ và phổ biến nhất thế giới,nó có khả năng chấp nhận những lệnh được định nghĩa sẵn khi nhập vào và cho những kết quả không thể tin được.Điều này cho phép những người dùng có dã tâm như tin tặc, crackers, và script kiddies v.v... sử dụng máy tìm kiếm Google để thu thập những thông tin bí mật và nhạy cảm, những cái mà không thể nhìn thấy qua những tìm kiếm thông thường.

Trong bài báo này tôi sẽ làm rõ những điểm dưới đây mà những người quản trị hoặc chuyên gia bảo mật phải đưa vào tài khoản

để phòng chống những thông tin bí mật bị phơi bày.

- Những cú pháp tìm kiếm nâng cao với Google
- Tìm kiếm những Site hoặc Server(máy chủ) dễ bị tấn công sử dụng những cú pháp nâng cao của Google
- Bảo mật cho servers hoặc sites khỏi sự tấn công của Google

Những cú pháp tìm kiếm nâng cao với Google

Dưới đây thảo luận về những lệnh đặc biệt của Google và tôi sẽ giải thích từng lệnh một cách ngắn gọn và nói rõ nó được sử dụng như thế nào để tìm kiếm thông tin.

[intitle:]

Cú pháp "**intitle:**" giúp Google giới hạn kết quả tìm kiếm về những trang có chứa từ đó trong tiêu đề. Ví dụ, **"intitle:** *login password***"** (không có ngoặc kép) sẽ cho kết quả là những link đến những trang có từ "*login*" trong tiêu đề, và từ "*password*" nằm ở đâu đó trong trang.
Tương tự, nếu ta muốn truy vấn nhiều hơn một từ trong tiêu đề của trang thì ta có thể dùng "**allintitle:"** thay cho "**intitle**" để có kết quả là những trang có chứa tất cả những từ đó trong tiêu đề. Ví dụ như dùng "**intitle:** *login* **intitle:** *password*" cũng giống như truy vấn "**allintitle:** *login password*".

[**inurl:**]

Cú pháp "**inurl:**" giới hạn kết quả tìm kiếm về những địa chỉ URL có chứa từ khóa tìm kiếm. Ví dụ: "**inurl:** *passwd"* (không có ngoặc kép) sẽ cho kết quả là những link đến những trang có từ "*passwd*" trong URL.
Tương tự, nếu ta muốn truy vấn nhiều hơn một từ trong URL thì ta có thể dùng "**allinurl:**" thay cho "**inurl**" để được kết quả là những URL chứa tất cả những từ khóa tìm kiếm.Ví dụ: "**allinurl:** *etc/passwd*" sẽ tìm kiếm những URL có chứa "*etc*" và "*passwd*". Ký hiệu gạch chéo ("/") giữa các từ sẽ bị Google bỏ qua.

[**site:**]

Cú pháp "**site:**" giới hạn Google chỉ truy vấn những từ khóa xác định trong một site hoặc tên miền riêng biệt. Ví dụ: "*exploits* **site:***hackingspirits.com*" (không có ngoặc kép) sẽ tìm kiếm từ khóa "*exploits*" trong những trang hiện có trong tất cả các link của tên miền "*hackingspirits.com"*. Không có khoảng trống nào giữa **"site:"** và **"tên miền".**

[**filetype:**]

Cú pháp "**filetype:**" giới hạn Google chỉ tìm kiếm những files trên internet có phần mở rộng riêng biệt (Ví dụ: doc, pdf hay ppt v.v...). Ví dụ : "**filetype:***doc* **site:***gov confidential*" (không có ngoặc kép) sẽ tìm kiếm những file có phần mở rộng là ".doc" trong tất cả những tên miền của chính phủ có phần mở rộng là "*.gov"* và chứa từ "confidential"(bí mật) trong trang hoặc trong file ".doc". Ví dụ . Kết quả sẽ bao gồm những liên kết đến tất cả các file văn bản bí trên các site của chính phủ.

[**link:**]

Cú pháp **"link:"** sẽ liệt kê những trang web mà có các liên kết đến đến những trang web chỉ định. Ví dụ :

chuỗi "**link:***www.securityfocus.com*" sẽ liệt kê những trang web có liên kết trỏ đến trang chủ SecurityFocus.

Chú ý không có khoảng trống giữa "link:" và URL của trang Web.

[**related:**]

Cú pháp "related:" sẽ liệt kê các trang Web "tương tự" với trang Web chỉ định. Ví dụ :

"related:www.securityfocus.com" sẽ liệt kê các trang web tương tự với trang chủ Securityfocus. Nhớ rằng không có khoảng trống giữa "related:" và URL của trang Web.

[**cache:**]

Truy vấn "**cache:**" sẽ cho kết quả là phiên bản của trang Web mà mà Google đã lưu lại. Ví dụ:

“**cache:***www.hackingspirits.com*” sẽ cho ra trang đã lưu lại bởi Google's.
Nhớ rằng không có khoảng trống giữa "cache:" và URL của trang web.
Nếu bạn bao gồm những từ khác trong truy vấn, Google sẽ điểm sáng những từ này trong văn bản đã được lưu lại.
Ví dụ: “**cache:***www.hackingspirits.com guest*” sẽ cho ra văn bản đã được lưu lại có từ "*guest*" được điểm sáng.

[**intext:**]
Cú pháp “**intext:**” tìm kiếm các từ trong một website riêng biệt. Nó phớt lờ các liên kết hoặc URL và tiêu đề của trang.
Ví dụ: “**intext:***exploits”* (không có ngoặc kép) sẽ cho kết quả là những liên kết đến những trang web có từ khóa tìm kiếm là "*exploits*" trong các trang của nó.

[**phonebook:**]
“**phonebook**” tìm kiếm thông tin về các địa chỉ đường phố ở Mỹ và số điện thoại. Ví dụ:
“**phonebook:***Lisa+CA*” sẽ liệt kê tất cả các tên người có từ “*Lisa*” trong tên và ở “*California (CA)*”. Cú pháp này có thể được sử dụng như là một công cụ tuyệt vời của tin tặc trong trường hợp ai đó muốn tìm kiếm thông tin cá nhân cho công việc xã hội.

Truy vấn các site hoặc server dễ bị tấn công sử dụng các cú pháp nâng cao của Google

Những cú pháp truy vấn nâng cao thảo luận ở trên thực sự có thể giúp người ta chính xác hóa các tìm kiếm và có được những gì họ thực sự tìm kiếm.

Bây giờ Google trở thành một máy tìm kiếm thông minh, những người dùng có ác ý không hề bận tâm khai thác khả năng của nó để đào bới những thông tin bí mật từ internet mà chỉ có sự truy cập giới hạn. Bây giờ tôi sẽ thảo luận những kỹ thuật này một cách chi tiết làm thế nào để những người dùng ác tâm đào bới thông tin trên internet sử dụng Google như một công cụ.

Sử dụng cú pháp “Index of ” để tìm kiếm các site cho phép duyệt chỉ mục

Một webserver(máy chủ web) cho phép duyệt chỉ mục nghĩa là bất kỳ ai có thể duyệt các thư mục của webserver như các thư mục nội bộ thông thường. Ở đây tôi sẽ thảo luận làm thế nào để sử dụng cú pháp "index of" để có một danh sách các liên kết đến webserver cho phép duyệt thư mục.

Cách này trở thành một nguồn dễ dàng cho việc thu thập thông tin của tin tặc. Tưởng tưởng nếu họ nắm được các file mật khẩu hoặc các file nhạy cảm khác mà bình thưởng không thể thấy được trên internet.

Dưới đây là vài Ví dụ sử dụng để có được quyền truy cập vào rất nhiều thông tin nhạy cảm dễ dàng hơn rất nhiều:

Index of /admin

Index of /passwd

Index of /password

Index of /mail

"Index of /" +passwd

"Index of /" +password.txt

"Index of /" +.htaccess

"Index of /secret"

"Index of /confidential"

"Index of /root"

"Index of /cgi-bin"

"Index of /credit-card"

"Index of /logs"

"Index of /config"

Tìm kiếm các site hoặc server dễ bị tấn công sử dụng cú pháp “inurl:” hoặc “allinurl:”

a. Sử dụng **“allinurl:**winnt/system32/**”** (không có ngoặc kép) sẽ liệt kê tất cả các liên kết đến server mà cho phép truy cập đến những thư mục giới hạn như “system32” qua web. Nếu bạn đủ may mắn thì bạn có thể có quyền truy cập đến file cmd.exe trong thư mục “system32”. Một khi bạn có quyền truy cập đến file “cmd.exe” và có thể thực thi nó thì bạn có thể tiến lên xa hơn leo thang quyền của bạn khắp server và làm hại nó.

b. Sử dụng **“allinurl:**wwwboard/passwd.txt**”**(không có ngoặc kép) trong Google search sẽ liệt kê tất cả các liên kết đến server mà dễ bị tấn công vào “tính dễ bị tấn công mật khẩu WWWBoard”. Để biết thêm về tính dễ bị tấn công này bạn có thể vào link sau đây:
http://www.securiteam.com/exploits/2BUQ4S0SAW.html

c. Sử dụng **“inurl:**.bash_history**”** (không có ngoặc kép) sẽ liệt kê tất cả các liên kết đến server mà cho phép truy cập vào file “.bash_history” qua web. Đây là một file lịch sử dòng lệnh. File này bao gồm danh sách các lệnh được thực thi bởi quản trị viên,
, và đôi khi bao gồm cả thông tin nhạy cảm như mật khẩu
gõ vào bởi quản trị viên. Nếu file này bị làm hại
và nếu nó bao gồm mật khẩu đã mã hóa của hệ thống unix (or *nix)
thì nó có thể dễ dàng bị crack bởi phương pháp “John The

Ripper”.

d. Sử dụng “**inurl:**config.txt” (không có ngoặc kép) sẽ liệt kê tất cả các liên kết đến các máy chủ cho phép truy cập vào file “config.txt”
qua giao diện web. File này bao gồm các thông tin nhạy cảm,
bao gồm giá trị bị băm ra của mật khẩu quản trị và sự xác thực quyền truy cập cơ sở dữ liệu. Ví dụ: Hệ thống quản lý học tập Ingenium
là một ứng dụng Web cho các hệ thống Windows phát triển bởi Click2learn, Inc. Hệ thống quản lý học tập Ingenium
phiên bản 5.1 và 6.1 lưu các thông tin nhạy cảm không an tòan trong file config.txt. Để biết thêm thông tin vào liên kết sau:
http://www.securiteam.com/securitynews/6M00H2K5PG.html

Những tìm kiếm tương tự khác dùng “inurl:” hoặc “allinurl:” kết hợp với các cú pháp khác:

inurl:admin filetype:txt
inurl:admin filetype:db
inurl:admin filetype:cfg
inurl:mysql filetype:cfg
inurl:passwd filetype:txt
inurl:iisadmin
inurl:auth_user_file.txt
inurl:orders.txt
inurl:"wwwroot/*."
inurl:adpassword.txt
inurl:webeditor.php
inurl:file_upload.php
inurl:gov filetype:xls "restricted"

index of ftp +.mdb allinurl:/cgi-bin/ +mailto

Tìm kiếm các site hoặc server dễ bị tấn công dùng "intitle:" hoặc "allintitle:"

a. Sử dụng [**allintitle:** "index of /root"] (không có ngoặc vuông) sẽ liệt kê các liên kết đến các webserver(máy chủ Web) cho phép truy cập vào các thư mục giới hạn như "root" qua giao diện web. Thư mục này đôi khi bao gồm các thông tin nhạy cảm mà có thể dễ dàng tìm được tqua những yêu cầu Web đơn giản.

b. Sử dụng [**allintitle:** "index of /admin"] (không có ngoặc vuông) sẽ liệt kê các liên kết đến các website cho phép duyệt chỉ mục các thư mục giới hạn như "admin" qua giao diện web. Hầu hết các ứng dụng web đôi khi sử dụng tên như "admin" để lưu quyền admin trong đó. Thư mục này đôi khi bao hàm các thông tin nhạy cảm mà có thể dễ dàng tìm được qua các yêu cầu Web đơn giản.

Những tìm kiếm tương tự dùng "intitle:" hoặc "allintitle:" kết hợp với các cú pháp khác

intitle:"Index of" .sh_history

intitle:"Index of" .bash_history

intitle:"index of" passwd

intitle:"index of" people.lst

intitle:"index of" pwd.db

intitle:"index of" etc/shadow

intitle:"index of" spwd

intitle:"index of" master.passwd

intitle:"index of" htpasswd

intitle:"index of" members OR accounts

intitle:"index of" user_carts OR user_cart

allintitle: sensitive filetype:doc

allintitle: restricted filetype :mail

allintitle: restricted filetype:doc site:gov

Những truy vấn tìm kiếm thú vị khác

Để tìm những site dễ bị tấn công bằng phương pháp Cross-Sites Scripting (XSS):

allinurl:/scripts/cart32.exe

allinurl:/CuteNews/show_archives.php

allinurl:/phpinfo.php

Để tìm những site dễ bị tấn công bằng phương pháp SQL Injection:

allinurl:/privmsg.php

allinurl:/privmsg.php

Bảo mật các server hoặc site khỏi sự tấn công của Google

Dưới đây là những phương pháp bảo mật mà các quản trị viên và các chuyên gia bảo mật phải đưa vào tài khoản để bảo mật những thông tin then chốt khỏi rơi vào không đúng chỗ:

- Cài những bản vá bảo mật mới nhất cho các ứng dụng cũng như hệ điều hành chạy trên máy chủ.
- Đừng để những thông tin nhạy cảm và then chốt trên máy chủ mà không có hệ thống xác nhận hợp lệ mà có thể bị truy cập trực tiếp bởi bất kỳ ai trên internet.
- Không cho phép duyệt thư mục trên webserver. Duyệt thư mục chỉ nên được cho phép với các thư mục web bạn muốn cho bất kỳ ai trên internet truy cập.

- Nếu bạn tìm thấy bất kỳ liên kết nào đến server hoặc site giới hạn của bạn trong kết quả của Google search thì nó phải được xóa đi. Vào liên kết sau để biết thêm chi tiết:
http://www.google.com/remove.html
- Không cho phép truy cập dấu tên vào webserver qua internet
vào các thư mục hệ thống giới hạn.
- Cài các công cụ lọc như URLScan cho các máy chủ chạy
IIS như là webserver.

Kết luận

Đôi khi tăng sự phức tạp trong hệ thống tạo ra những sự cố mới. Google trở lên phức tạp hơn có thể được sử dụng bởi bất kỳ anh Tom,
anh Dick & Harry nào đó trên internet để đào bới những thông tin nhạy cảm mà thông thường không thể nhìn thấy hoặc với đến bởi bất kỳ ai.
Người ta không thể ngăn cản ai đó ngừng tạo ra những giả mạo vì vậy những lựa chọn duy nhất còn lại cho những chuyên gia bảo mật và quản trị hệ thống là bảo vệ hệ thống của họ và làm khó khăn hơn từ sự xâm hại không mong muốn.

Về tác giả

Không có nhiều điều để tôi có thể nói về chính tôi. Nói một cách ngắn gọn,
Tôi dành hầu hết thời gian để nghiên cứu về sự dễ bị tấn công,
một tách càfê và internet. Đó là tất cả về tôi.
Để biết thêm về tôi xin mời vào www.hackingspirits.com

D
ebasis Mohanty
www.hackingspirits.com
Email: debasis_mty@yahoo.com

Bạn có thể thấy tôi tại:

http://groups.yahoo.com/group/Ring-of-Fire

Nhận xét và góp ý xin gửi cho debasis_mty@yahoo.com.
