# Chapter 9

# Usernames, Passwords, and Secret Stuff, Oh My!

**Solutions in this chapter:**

- **Searching for Usernames**
- **Searching for Passwords**
- **Searching for Credit Card Numbers, Social Security Numbers, and More**
- **Searching for Other Juicy Info**
- **List of Sites**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

# Introduction

This chapter is not about finding sensitive data during an assessment as much as it is about what the "bad guys" might do to troll for the data. The examples presented in this chapter generally represent the lowest-hanging fruit on the security tree. Hackers target this information on a daily basis. To protect against this type of attacker, we need to be fairly candid about the worst-case possibilities. We won't be *overly* candid, however. We don't want to give the bad guys any ideas they don't already have.

We start by looking at some queries that can be used to uncover usernames, the less important half of most authentication systems. The value of a username is often overlooked, but as we've already discussed, an entire multimillion-dollar security system can be shattered through skillful crafting of even the smallest, most innocuous bit of information.

Next, we will take a look at queries that are designed to uncover passwords. Some of the queries we look at reveal encrypted or encoded passwords, which will take a bit of work on the part of an attacker to use to his or her advantage. We also take a look at queries that can uncover *cleartext* passwords. These queries are some of the most dangerous in the hands of even the most novice attacker. What could make an attack easier than handing a username and cleartext password to an attacker?

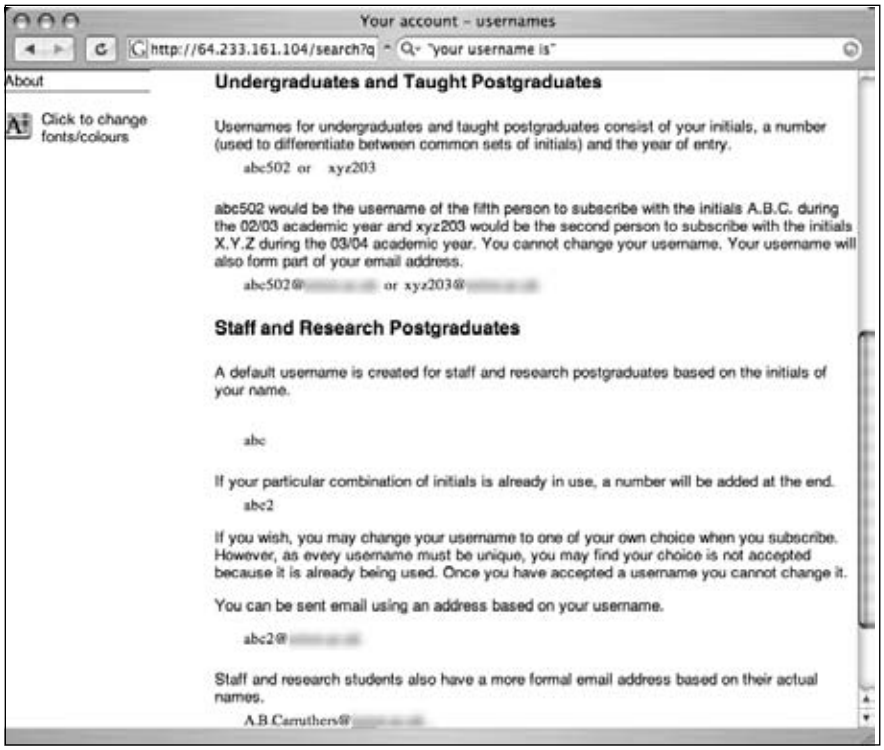
We wrap up this chapter by discussing the *very real* possibility of uncovering highly sensitive data such as credit card information and information used to commit identity theft, such as Social Security numbers. Our goal here is to explore ways of protecting against this very real threat. To that end, we don't go into details about uncovering financial information and the like. If you're a "dark side" hacker, you'll need to figure these things out on your own, or make the wise decision to turn to the light side of the force.

# Searching for Usernames

Most authentication mechanisms use a username and password to protect information. To get through the "front door" of this type of protection, you'll need to determine usernames as well as passwords. Usernames also can be used for social engineering efforts, as we discussed earlier.

Many methods can be used to determine usernames. In the "Database Digging" chapter, we explored ways of gathering usernames via database error messages. In the "Tracking Down Web Servers" chapter, we explored Web server and application error messages that can reveal various information, including usernames. These indirect methods of locating usernames are helpful, but an attacker could target a usernames directory with a simple query like *"your username is"*. This phrase can locate help pages that describe the username creation process, as shown in Figure 9.1.

**Figure 9.1** Help Documents Can Reveal Username Creation Processes




An attacker could use this information to postulate a username based on information gleaned from other sources, such as Google Groups posts or phone listings. The usernames could then be recycled into various other phases of the attack, such as a worm-based spam campaign or a social-engineering attempt. An attacker can gather usernames from a variety of sources, as shown in the sample queries listed in Table 9.1.

**Table 9.1** Sample Queries That Locate Usernames

| Query | Description |
|---|---|
| *inurl:admin inurl:userlist* | Generic userlist files |
| *inurl:admin filetype:asp inurl:userlist* | Generic userlist files |
| *inurl:php inurl:hlstats intext: Server Username* | Half-life statistics file, lists username and other information |
| *filetype:ctl inurl:haccess.ctl Basic* | Microsoft FrontPage equivalent(?)of htaccess shows Web user credentials |
| *filetype:reg reg intext:"internet account manager"* | Microsoft Internet Account Manager can reveal usernames and more |

Continued

**Table 9.1 continued** Sample Queries That Locate Usernames

| Query | Description |
|---|---|
| *filetype:wab wab* | Microsoft Outlook Express Mail address books |
| *filetype:mdb inurl:profiles* | Microsoft Access databases containing (user) profiles. |
| *index.of perform.ini* | mIRC IRC ini file can list IRC usernames and other information |
| *inurl:root.asp?acs=anon* | Outlook Mail Web Access directory can be used to discover usernames |
| *filetype:conf inurl:proftpd.conf –sample* | PROFTP FTP server configuration file reveals username and server information |
| *filetype:log username putty* | PUTTY SSH client logs can reveal usernames and server information |
| *filetype:rdp rdp* | Remote Desktop Connection files reveal user credentials |
| *intitle:index.of .bash_history* | UNIX bash shell history reveals commands typed at a bash command prompt; usernames are often typed as argument strings |
| *intitle:index.of .sh_history* | UNIX shell history reveals commands typed at a shell command prompt; usernames are often typed as argument strings |
| *"index of " lck* | Various lock files list the user currently using a file |
| *+intext:webalizer +intext:Total Usernames +intext:"Usage Statistics for"* | Webalizer Web statistics page lists Web usernames and statistical information |
| *filetype:reg reg HKEY_CURRENT_ USER username* | Windows Registry exports can reveal usernames and other information |

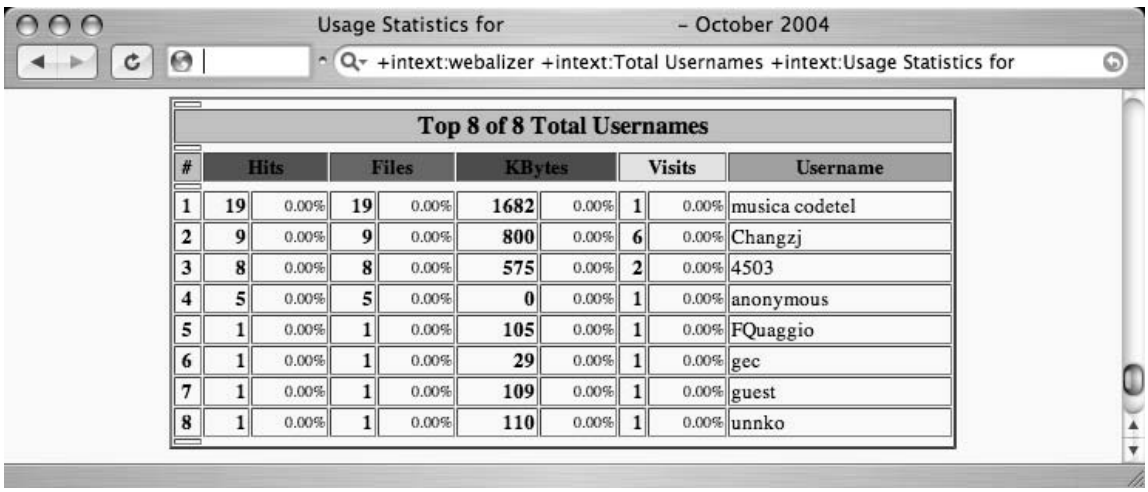
## Underground Googling

### Searching for a Known Filename

Remember that there are several ways to search for a known filename. One way relies on locating the file in a directory listing, like *intitle:index.of install.log.* Another, often better, method relies on the *filetype* operator, as in *filetype:log inurl:install.log*. Directory listings are not all that common. Google will crawl a link to a file in a directory listing, meaning that the *filetype* method will find *both* directory listing entries as well as files crawled in other ways.

In some cases, usernames can be gathered from Web-based statistical programs that check Web activity. The Webalizer program shows all sorts of information about a Web server's usage. Output files for the Webalizer program can be located with a query such as *+intext:webalizer +intext:"Total Usernames" +intext:"Usage Statistics for"*. Among the information displayed is the username that was used to connect to the Web server, as shown in Figure 9.2. In some cases, however, the usernames displayed are not valid or current, but the "Visits" column lists the number of times a user account was used during the capture period. This enables an attacker to easily determine which accounts are more likely to be valid.

**Figure 9.2** The Webalizer Output Page Lists Web Usernames

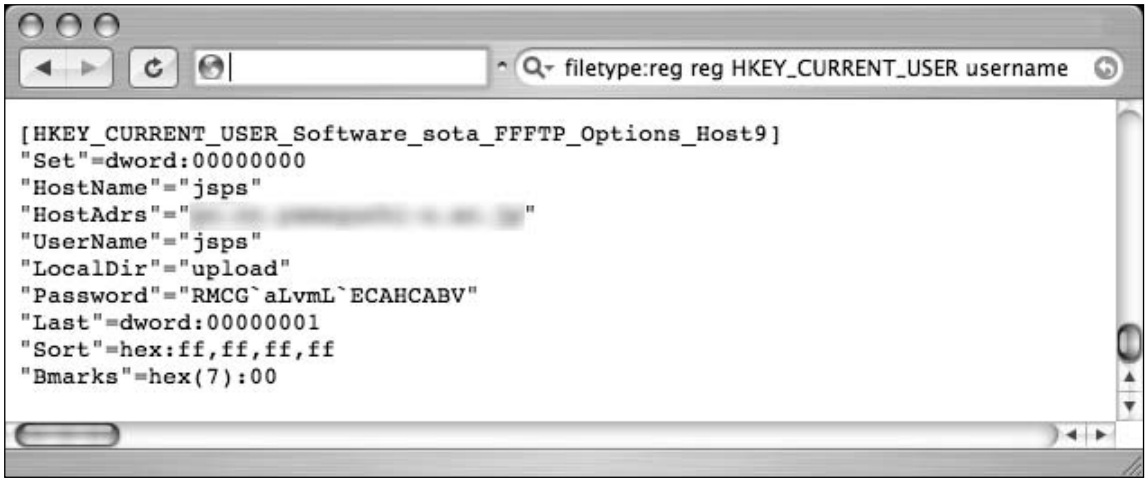



**Top 8 of 8 Total Usernames**

| # | Hits | | Files | | KBytes | | Visits | | Username |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 19 | 0.00% | 19 | 0.00% | 1682 | 0.00% | 1 | 0.00% | musica codetel |
| 2 | 9 | 0.00% | 9 | 0.00% | 800 | 0.00% | 6 | 0.00% | Changzj |
| 3 | 8 | 0.00% | 8 | 0.00% | 575 | 0.00% | 2 | 0.00% | 4503 |
| 4 | 5 | 0.00% | 5 | 0.00% | 0 | 0.00% | 1 | 0.00% | anonymous |
| 5 | 1 | 0.00% | 1 | 0.00% | 105 | 0.00% | 1 | 0.00% | FQuaggio |
| 6 | 1 | 0.00% | 1 | 0.00% | 29 | 0.00% | 1 | 0.00% | gec |
| 7 | 1 | 0.00% | 1 | 0.00% | 109 | 0.00% | 1 | 0.00% | guest |
| 8 | 1 | 0.00% | 1 | 0.00% | 110 | 0.00% | 1 | 0.00% | unnko |

The Windows registry holds all sorts of authentication information, including usernames and passwords. Though it is unlikely (and fairly uncommon) to locate live, exported Windows registry files on the Web, at the time of this writing there are nearly 200 hits on the query *filetype:reg HKEY_CURRENT_USER username,* which locates Windows registry files that contain the word *username* and in some cases passwords, as shown in Figure 9.3.

**Figure 9.3** Generic Windows Registry Files Can Reveal Usernames and Passwords




As any talented attacker or security person will tell you, it's rare to get information served to you on a silver platter. Most decent finds take a bit of persistence, creativity, intelligence, and just a bit of good luck. For example, consider the Microsoft Outlook Web Access portal, which can be located with a query like *inurl:root.asp?acs=anon*. There are few hits for this query, even though there lots of sites run the Microsoft Web-based mail portal. Regardless of how you might locate a site running this e-mail gateway, it's not uncommon for the site to host a public directory (denoted "Find Names," by default), as shown in Figure 9.4.

**Figure 9.4** Microsoft Outlook Web Access Hosts a Public Directory

The public directory allows access to a search page that can be used to find users by name. In most cases, wildcard searching is not allowed, meaning that a search for * will not return a list of all users, as might be expected. Entering a search for a space is an interesting idea, since most user descriptions contain a space, but most large directories will return an error message reading "This query would return too many addresses!" Applying a bit of creativity, an attacker could begin searching for individual common letters, such as the "Wheel of Fortune letters" *R, S, T, L, N, and E*. Eventually one of these searches will most likely reveal a list of user information like the one shown in Figure 9.5.

**Figure 9.5** Public Outlook Directory Searching for Usernames

Once a list of user information is returned, the attacker can then recycle the search with words contained in the user list, searching for the words *Voyager, Freshmen, or Campus*, for example. Those results can then be recycled, eventually resulting in a nearly complete list of user information.

# Searching for Passwords

Password data, one of the "Holy Grails" during a penetration test, should be protected. Unfortunately, many examples of Google queries can be used to locate passwords on the Web, as shown in Table 9.2.

**Table 9.2** Queries That Locate Password Information

| Query | Description |
|---|---|
| filetype:config config intext: appSettings "User ID" | .Net Web Application configuration may contain authentication information |
| filetype:netrc password | .netrc file may contain cleartext passwords |
| intitle:"Index of" passwords modified | "Password" directories |
| inurl:/db/main.mdb | ASP-Nuke database files often contain passwords |
| filetype:bak inurl:"htaccess\|passwd\| shadow\|htusers" | BAK files referring to passwords or usernames |
| filetype:log "See `ipsec —copyright" | BARF log files reveal ipsec data |
| inurl:"calendarscript/users.txt" | CalenderScript passwords |
| inurl:ccbill filetype:log data | CCBill log files may contain authentication |
| inurl:cgi-bin inurl:calendar.cfg | CGI Calendar (Perl) configuration file reveals information including passwords for the program. |
| inurl:chap-secrets -cvs | chap-secrets file may list usernames and passwords |
| enable password \| secret "current configuration" -intext:the | Cisco "secret 5" and "password 7" passwords |
| intext:"enable secret 5 $" | Cisco enable secrets |
| intext:"enable password 7" | Cisco router config files |
| [WFClient] Password= filetype:ica | Citrix WinFrame-Client may contain login information |
| inurl:passlist.txt | Cleartext passwords. No decryption required! |

Continued

**Table 9.2 continued** Queries That Locate Password Information

| Query | Description |
|---|---|
| filetype:cfm "cfapplication name" password | ColdFusion source code mentioning "passwords" |
| intitle:index.of config.php | Config.php files |
| inurl:config.php dbuname dbpass | config.php files |
| inurl:server.cfg rcon password | Counter strike rcon passwords |
| ext:inc "pwd=" "UID=" | Database connection strings |
| ext:asa \| ext:bak intext:uid intext:pwd -"uid..pwd" database \| server \| dsn | Database credentials in ASA and BAK files |
| filetype:ldb admin | Database lock files may contain credential info |
| filetype:properties inurl:db intext: password | db.properties file contains usernames, decrypted passwords |
| filetype:inc dbconn | Dbconn.inc files contain the username and password a website uses to connect to a database. |
| filetype:pass pass intext:userid | dbman password files |
| allinurl:auth_user_file.txt | DCForum's password file |
| "powered by ducalendar" -site:duware.com | ducalendar database may reveal password data |
| "Powered by Duclassified" -site:duware.com | Duclassified database may reveal password data |
| "powered by duclassmate" -site:duware.com | duclassmate database may reveal password data |
| "Powered by Dudirectory" -site:duware.com | dudirectory database may reveal password data |
| "powered by dudownload" -site:duware.com | dudownload database may reveal password data |
| "Powered by DUpaypal" -site:duware.com | Dupaypal database may reveal password data. |
| intitle:dupics inurl:(add.asp \| default.asp \| view.asp \| voting.asp) -site:duware.com | dupics database may reveal password data |
| eggdrop filetype:user user | Eggdrop config files |
| "Powered By Elite Forum Version *.*" | Elite forums database contains authentication information |

Continued

**Table 9.2 continued** Queries That Locate Password Information

| Query | Description |
|---|---|
| intitle:"Index of" pwd.db | Encrypted pwd.db passwords |
| ext:ini eudora.ini | Eudora INI file may contain usernames and encrypted passwords |
| inurl:filezilla.xml -cvs | filezilla.xml contains passwords data |
| filetype:ini inurl:flashFXP.ini | FlashFXP configuration file may contain FTP passwords |
| filetype:dat inurl:Sites.dat | FlashFXP FTP passwords |
| inurl:"Sites.dat"+"PASS=" | FlashFXP Sites.dat server configuration file |
| ext:pwd inurl:(service \| authors \| administrators \| users) "# -FrontPage-" | Frontpage sensitive authentication-related files |
| filetype:url +inurl:"ftp://" +inurl:"@" | FTP bookmarks, some of which contain plaintext login names and passwords |
| intitle:index.of passwd passwd.bak | Generic PASSWD files |
| inurl:zebra.conf intext:password -sample -test -tutorial -download | GNU Zebra enable passwords (plain text or encrypted) |
| intext:"powered by EZGuestbook" | HTMLJunction EZGuestbook database reveals authentication data |
| intitle:"Index of" ".htpasswd" htpasswd.bak | htpasswd password files |
| intitle:"Index of" ".htpasswd" "htgroup" -intitle:"dist" -apache -htpasswd.c | htpasswd password files |
| filetype:htpasswd htpasswd | htpasswd password files |
| "http://*:*@www" bob:bob | HTTP web authentication information |
| "liveice configuration file" ext:cfg -site:sourceforge.net | Icecast liveice.cfg file which may contain passwords |
| "sets mode: +k" | IRC channel keys |
| signin filetype:url | Javascript user validation mechanisms may contain cleartext usernames and passwords |
| LeapFTP intitle:"index.of./" sites.ini modified | LeapFTP client configuration file may reveal authentication information |
| inurl:lilo.conf filetype:conf password -tatercounter2000 -bootpwd -man | LILO boot passwords |
| "Powered by Link Department" | Link management script contains encrypted admin passwords and session data |

Continued

**Table 9.2 continued** Queries That Locate Password Information

| Query | Description |
|---|---|
| "your password is" filetype:log | log files containing the phrase (Your password is). |
| "admin account info" filetype:log | logs containing admin server account information |
| intitle:index.of master.passwd | master.passwd files |
| allinurl: admin mdb | Microsoft Access "admin" databases |
| filetype:mdb inurl:users.mdb | Microsoft Access "user databases" |
| filetype:xls username password email | Microsoft Excel spreadsheets containing the words username, password and email |
| intitle:index.of administrators.pwd | Microsoft Front Page administrative usernames and passwords. |
| filetype:pwd service | Microsoft Frontpage service info |
| inurl:perform.ini filetype:ini | mIRC IRC passwords |
| inurl:perform filetype:ini | mIRC potential connection data |
| filetype:cfg mrtg "target[*]" -sample -cvs -example | Mrtg.cfg SNMP configuration file may reveal public and private community strings |
| intitle:"index of" intext:connect.inc | MySQL database connection information |
| intitle:"Index of" .mysql_history | mysql history files |
| intitle:"index of" intext:globals.inc | MySQL user/password information |
| "Your password is * Remember this for later use" | NickServ registration passwords |
| filetype:conf oekakibbs | Oekakibss configuration files may reveal passwords |
| filetype:conf slapd.conf | OpenLDAP slapd.conf file contains configuration data including the root password |
| inurl:"slapd.conf" intext:"credentials" -manpage -"Manual Page" -man: -sample | OpenLDAP slapd.conf file contains configuration data including the root password |
| filetype:dat wand.dat | Opera web browser "magic wand" stored cerdentials |
| inurl:pap-secrets -cvs | pap-secrets file may list usernames and passwords |
| filetype:dat inurl:pass.dat | Pass.dat files may reveal passwords |
| index.of passlist | Passlist password files |

Continued

**Table 9.2 continued** Queries That Locate Password Information

| Query | Description |
|---|---|
| filetype:dat "password.dat" | Password.dat files can contain plaintext usernames and passwords |
| filetype:log inurl:"password.log" | Password.log files can contain cleartext usernames and passwords |
| filetype:pem intext:private | PEM private key files |
| intitle:index.of people.lst | people.lst files |
| intitle:index.of intext:"secring.skr"\| "secring.pgp"\|"secring.bak" | PGP secret keyrings |
| inurl:secring ext:skr \| ext:pgp \| ext:bak | PGP secret keyrings |
| filetype:inc mysql_connect OR mysql_pconnect | PHP .inc files contain authentication information |
| filetype:inc intext:mysql_connect | PHP .inc files contain usernames, passwords |
| ext:php intext:"$dbms""$dbhost" "$dbuser""$dbpasswd""$table_ prefix""phpbb_installed" | phpBB mySQL connection information |
| intitle:"phpinfo()" +"mysql. default_password" +"Zend Scripting Language Engine" | phpinfo files may contain default mysql passwords |
| inurl:nuke filetype:sql | PHP-Nuke or Postnuke database dumps may contain authentication data |
| "parent directory" +proftpdpasswd | ProFTPd User names and password hashes from web server backups |
| filetype:conf inurl:psybnc.conf "USER.PASS=" | psyBNC configuration files may contain authentication info |
| intitle:rapidshare intext:login | Rapidshare login passwords. |
| inurl:"editor/list.asp" \| inurl: "database_editor.asp" \| inurl: "login.asa" "are set" | Results Database Editor usernames/ passwords |
| ext:yml database inurl:config | Ruby on Rails database link file |
| ext:ini Version=4.0.0.4 password | servU FTP Daemon ini file may contain usernames and passwords |
| filetype:ini ServUDaemon | servU FTP Daemon INI files may contains setting, session and authentication data |
| filetype:ini inurl:"serv-u.ini" | Serv-U INI file may contain username and password data |

Continued

**Table 9.2 continued** Queries That Locate Password Information

| Query | Description |
|---|---|
| intitle:"Index of" sc_serv.conf sc_ serv content | Shoutcast sc_serv.conf files often contain cleartext passwords |
| intitle:"Index of" spwd.db passwd -pam.conf | spwd.db password files |
| filetype:sql "insert into" (pass\|passwd\|password) | SQL dumps containing cleartext or encrypted passwords |
| filetype:sql ("passwd values" \| "password values" \| "pass values" ) | SQL file password references |
| filetype:sql ("values * MD5" \| "values * password" \| "values * encrypt") | SQL files may contain encrypted passwords |
| filetype:sql +"IDENTIFIED BY" -cvs | SQL files mentioning authentication info |
| filetype:sql password | SQL files mentioning authentication info |
| filetype:reg reg HKEY_CURRENT_ USER SSHHOSTKEYS | SSH host keys stored in Windows Registry |
| inurl:"GRC.DAT" intext:"password" | Symantec Norton Anti-Virus Corporate Edition data file contains encrypted passwords |
| filetype:inf sysprep | Sysprep.inf files contain all information for a Windows information including administrative passwords, IP addresses and product IDs |
| server-dbs "intitle:index of" | teamspeak server admin files |
| filetype:ini wcx_ftp | Total commander FTP passwords |
| intitle:index.of trillian.ini | Trillian INI files contain passwords. |
| ext:txt inurl:unattend.txt | unattend.txt files contain all information for a Windows information including administrative passwords, IP addresses and product IDs |
| index.of.etc | Unix /etc directories |
| intitle:"Index of..etc" passwd | Unix /etc/passwd files |
| intitle:Index.of etc shadow | UNIX /etc/shadow password files |
| ext:passwd -intext:the -sample -example | Various passwords |
| filetype:bak createobject sa | VBScript database connection backups |
| inurl:ventrilo_srv.ini adminpassword | ventrilo passwords for many servers |

Continued

**Table 9.2 continued** Queries That Locate Password Information

| Query | Description |
|---|---|
| filetype:reg reg +intext: WINVNC3 | vnc passwords |
| !Host=*.* intext:enc_UserPassword=* ext:pcf | VPN profiles often contain authentication data |
| inurl:vtund.conf intext:pass -cvs | vtund configuration files can contain usernames and passwords |
| filetype:mdb wwforum | Web Wiz Forums database contains authentication information |
| intext:"powered by Web Wiz Journal" | Web Wiz Journal ASP Blog database contains administrative information |
| "AutoCreate=TRUE password=*" | Website Access Analyzer passwords |
| filetype:pwl pwl | Windows Password List files |
| filetype:reg reg +intext: "defaultusername" +intext: "defaultpassword" | Windows registry keys which reveal passwords |
| filetype:ini ws_ftp pwd | WS_FTP.ini file contains weakly encrypted passwords |
| "index of/" "ws_ftp.ini" "parent directory" | WS_FTP.ini file contains weakly encrypted passwords |
| inurl:"wvdial.conf" intext: "password" | wvdial.conf may contain phone numbers, usernames and passwords |
| inurl:/wwwboard | WWWBoard "passwd.txt" authentication configuration files |
| wwwboard WebAdmin inurl: passwd.txt wwwboard\|webadmin | WWWBoard password files |
| "login: *" "password= *" filetype:xls | xls files containing login names and passwords |
| inurl:/yabb/Members/Admin.dat | YaBB forums Administrator password |

In most cases, passwords discovered on the Web are either encrypted or encoded in some way. In most cases, these passwords can be fed into a password cracker such as John the Ripper from www.openwall.com/john to produce plaintext passwords that can be used in an attack. Figure 9.6 shows the results of the search *ext:pwd inurl:_vti_pvt inurl:(Service | authors | administrators)*, which combines a search for some common Microsoft FrontPage support files.

**Figure 9.6** Encrypted or Encoded Passwords

Exported Windows registry files often contain encrypted or encoded passwords as well. If a user exports the Windows registry to a file and Google subsequently crawls that file, a query like *filetype:reg intext:"internet account manager"* could reveal interesting keys containing password data, as shown in Figure 9.7.

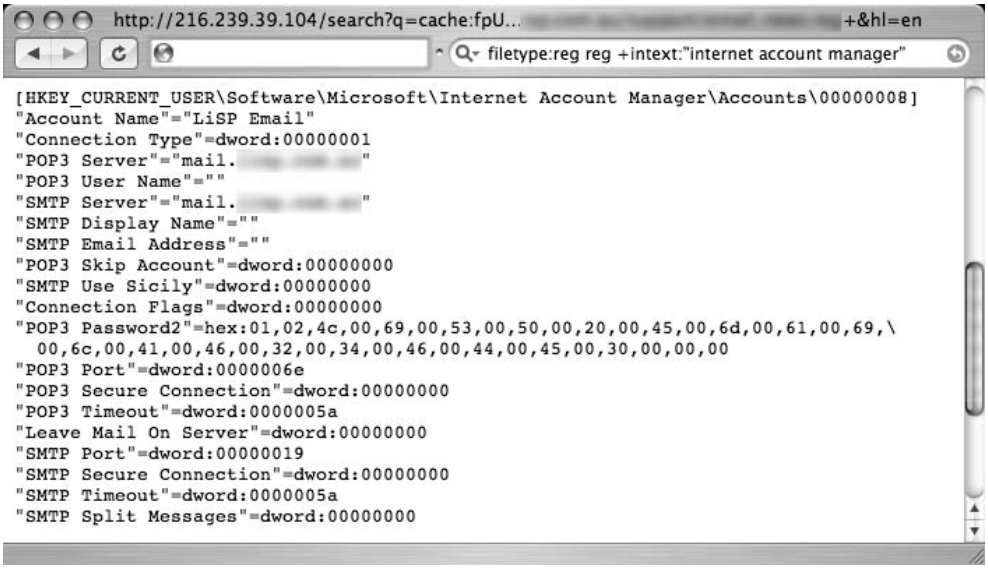



**Figure 9.7** Specific Windows Registry Entries Can Reveal Passwords