Gefährliches Google – Suche nach sensiblen Daten

Michał Piotrowski

Der Artikel wurde in der Ausgabe 4/2005 des Magazins *hakin9* publieziert.

Das *hakin9* Magazin, Wydawnictwo Software, ul. Piaskowa 3, 01-067 Warschau, Polen *de@hakin9.org*

Gefährliches Google – Suche nach sensiblen Daten

Michał Piotrowski

Daten, die geschützt sein sollten, werden sehr oft öffentlich zugänglich gemacht. Es sind die Nutzer selbst, die sie unbewusst – aufgrund von Vernachlässigung oder Unwissenheit – veröffentlichen. Der Effekt ist, dass die sensiblen Daten im Internet zum Greifen nahe sind. Es reicht Google zu verwenden.

Google beantwortet ca. 80% aller Anfragen im Netz, und ist damit die am häufigsten und am liebsten verwendete Suchmaschine. Es verdankt dies nicht nur dem außergewöhnlich effektiven Suchalgorithmus, sondern auch den sehr komplexen Möglichkeiten der Anfragenstellung. Wir sollten jedoch nicht vergessen, dass das Internet ein sehr dynamisches Medium ist, weshalb die, durch Google gelieferten, Ergebnisse nicht immer aktuell sind. Es kommt vor, dass manche gefundenen Webseiten sehr veraltet sind, und gleichzeitig viele ähnliche durch den Googlebot nicht besucht wurden (Script-Automat, der die WWW-Ressourcen durchkämmt und indexiert).

Die wichtigsten und gebräuchlichsten Operatoren zur Verfeinerung der Suche, inklusive ihrer Beschreibung und ihrem Effekt, wurden in Tabelle 1 aufgelistet. Die Stellen in Dokumenten, auf die sich jene Operatoren während der Durchsuchung der Netz-Ressourcen beziehen (am Beispiel der Webseite des Magazins *hakin9*), stellt Abbildung 1 dar. Das sind nur einige Beispiele – durch eine geschickt gestellte Anfrage an Google kann man viel interessantere Informationen gewinnen.

In diesem Artikel erfahren Sie...

- wie man mit Hilfe von Google nach Datenbanken mit personenbezogenen Informationen und nach anderen sensiblen Daten sucht,
- wie man Informationen über angriffsanfällige Systeme und Web Dienste erhält,
- wie man mit Google öffentlich zugängliche Netzgeräte findet.

Was Sie vorher wissen/können sollten...

- wie man einen Internet-Browser benutzt,
- man sollte Grundwissen über das HTTP-Protokoll besitzen.

Über den Autor

Michał Piotrowski ist Magister der Informatik. Er besitzt langjährige Erfahrung als Netz- und Systemadministrator. Seit über drei Jahren arbeitet er als Sicherheitsinspektor. Im Moment ist er Spezialist für die Sicherheit einer der größten Finanzinstitutionen Polens. Seine Leidenschaft ist Freie Software.

Tabelle 1. *Abfrageoperatoren in Google*

Operator	Bestimmung	Beispiel der Verwendung
`site`	beschränkt die Ergebnisse auf die Seiten, die sich in einer bestimmten Domain befinden	`site:google.com fox` findet alle Seiten aus der Domain **.google.com*, die in ihrem Text das Wort *fox* enthalten
`intitle`	beschränkt die Ergebnisse auf die Dokumente, die die im Titel gegebene Phrase enthalten	`intitle:fox fire` findet Seiten, die das Wort *fox* im Titel und *fire* im Text enthalten
`allintitle`	beschränkt die Ergebnisse auf die Dokumente, die alle im Titel gegebenen Phrasen enthalten	`allintitle:fox fire` findet alle Seiten, die die Wörter *fox* und *fire* im Titel enthalten; funktioniert ähnlich wie `intitle:fox intitle:fire`
`inurl`	beschränkt die Ergebnisse auf die Seiten, die die in der URL-Adresse gegebene Phrase enthalten	`inurl:fox fire` findet Seiten, die das Wort *fire* im Text und *fox* in der URL-Adresse enthalten
`allinurl`	beschränkt die Ergebnisse auf die Seiten, die alle in der URL-Adresse gegebenen Phrasen enthalten	`allinurl:fox fire` findet Seiten, die die Wörter *fox* und *fire* in der URL-Adresse enthalten; funktioniert ähnlich wie `inurl:fox inurl:fire`
`filetype, ext`	beschränkt die Ergebnisse auf die Dokumente vom gewünschten Typ	`filetype:pdf fire` liefert die das Wort *fire* enthaltenden PDF-Dokumente, `filetype:xls fox` liefert die das Wort *fox* enthaltenden *Excel-Dokumente*
`numrange`	beschränkt die Ergebnisse auf die Dokumente, die eine Zahl aus dem gegebenen Zahlenbereich in ihrem Content enthalten	`numrange:1-100 fire` liefert Seiten, die eine Zahl aus dem Bereich 1 bis 100 und das Wort *fire* enthalten. Dasselbe Ergebnis erreicht man mit der Anfrage: `1..100 fire`
`link`	beschränkt die Ergebnisse auf die Seiten, die die Links zur gegebenen Lokalisierung enthalten	`link:www.google.de` liefert Dokumente, die mindestens einen Link zur Seite *www.google.de* enthalten
`inanchor`	beschränkt die Ergebnisse auf die Seiten mit den Links, die die in der Beschreibung gegebene Phrase enthalten	`inanchor:fire` liefert Dokumente, die die Links mit dem Wort *fire* in der Beschreibung (nicht in der URL-Adresse, auf die sie hinweisen, sondern in dem unterstrichenen Teil des Textes) enthalten
`allintext`	beschränkt die Ergebnisse auf die Dokumente, die die im Text gegebene Phrase enthalten und gleichzeitig diese Phrase im Titel, den Links und den URL-Adressen nicht enthalten	`allintext:"fire fox"` liefert Dokumente, die die Phrase *fire fox* nur im Text enthalten
`+`	erzwingt das häufige Auftreten der gegebenen Phrase in den Ergebnissen	`+fire` ordnet die Ergebnisse nach der Anzahl des Auftretens vom Wort *fire*
`-`	erzwingt das Nichtauftreten der gegebenen Phrase in den Ergebnissen	`-fire` liefert Dokumente, die das Wort *fire* nicht enthalten, zurück
`""`	erlaubt die Suche nach den ganzen Phrasen, nicht nur nach Wörtern	`"fire fox"` liefert Dokumente, die die Phrase *fire fox* enthalten
`.`	wird mit einem einzelnen Zeichen ersetzt	`fire.fox` liefert Dokumente, die die Phrasen *fire fox*, *fireAfox*, *fire1fox*, *fire-fox* etc. enthalten
`*`	wird mit einem einzelnen Wort ersetzt	`fire * fox` liefert Dokumente, die die Phrasen fire the *fox*, *fire in fox*, *fire or fox* etc. enthalten
`|`	logisches OR	`"fire fox" | firefox` liefert Dokumente, die die Phrase *fire fox* oder das Wort *firefox* enthalten

Wir suchen nach einem Opfer

Dank der Google-Suchmaschine kann man nicht nur zu öffentlich zugänglichen Internet-Ressourcen gelangen, sondern auch zu denjenigen, die unbekannt bleiben sollten. Wenn wir eine entsprechende Suchanfrage stellen, bekommen wir oft wirklich erstaunliche Ergebnisse. Fangen wir mit etwas Einfachem an.

Stellen wir uns vor, dass in einem allgemein verwendeten Programm eine Lücke entdeckt wurde. Nehmen wir weiterhin an, dass sie den Server *Microsoft IIS* Version 5.0 betrifft und ein Angreifer ein paar Server mit dieser Software finden will, um sie zu attackieren. Selbstverständlich könnte er zu diesem Zweck einen Scanner benutzen, aber er bevorzugt es, Google zu verwenden – er tippt also die folgende Abfrage ein: `"Microsoft-IIS/5.0 Server at" intitle:index.of` und bekommt als Resultat Links zu den gesuchten Servern, genauer zu aufgelisteten Inhalten der Verzeichnisse, die sich auf diesen Servern befinden. Der Grund hierfür ist, dass die Software *IIS* (und viele andere) in der Standardkonfiguration zu manchen dynamisch generierten Webseiten Banner hinzufügen, die eigene Namen und Version enthalten (man sieht dies auf Abbildung 2).

Das ist ein Beispiel einer Information, die an sich nicht gefährlich ist; aus diesem Grund wird sie sehr häufig ignoriert und in der Standardkonfiguration gelassen. Leider ist sie auch eine Information, die unter gewissen Bedingungen für den Angreifer eine wesentliche Bedeutung haben kann. Mehr Beispiele für Suchanfragen an Google nach anderen Servertypen enthält Tabelle 2.

Andere Methode zum Finden der konkreten Version der WWW-Server: man kann nach Standardseiten suchen, die mit ihnen geliefert und nach der erfolgreichen Konfiguration zugänglich gemacht werden. Es mag seltsam erscheinen, aber im Netz befindet sich eine Menge von Servern, deren Default-Inhalt nach der Installation nicht geändert

Abbildung 1. *Verwendung der Operatoren in der Suche – am Beispiel des Schaufensters des Magazins hakin9*

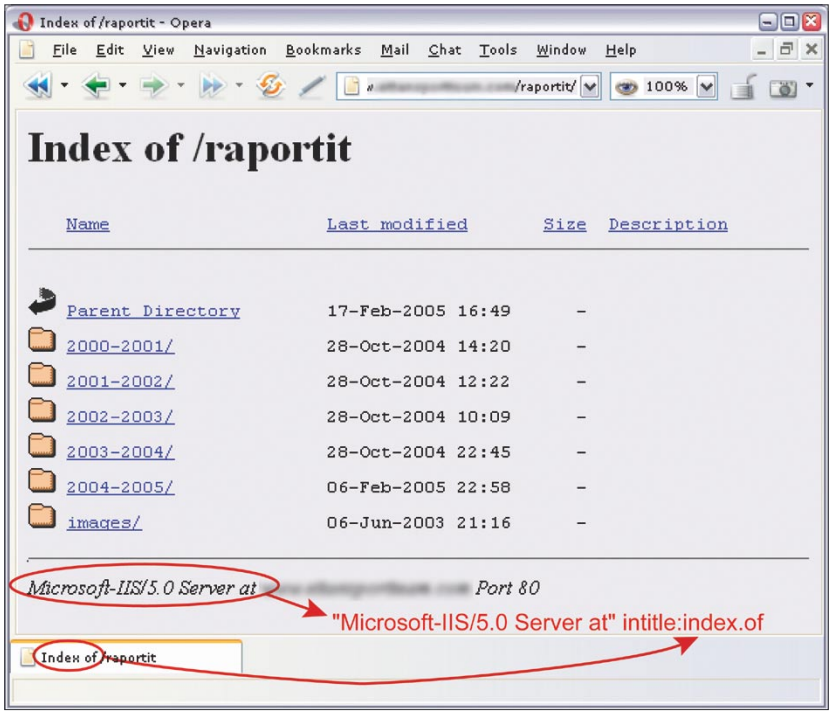


Abbildung 2. *Server IIS 5.0 wird mit Hilfe vom Operator intitle gefunden*

wurde. Dies sind oft schwach gesicherte, vergessene Geräte, die ein einfaches Ziel für die Einbrecher darstellen. Man kann sie finden, indem man die in der Tabelle 3 aufgelisteten Anfragen anwendet.

Diese Methode ist sehr einfach und gleichzeitig nützlich. Mit ihrer Hilfe bekommt man den Zugang zu einer immensen Anzahl von verschiedenen Netzservern oder Betriebssystemen, die die Applikationen verwenden, in denen Fehler gefunden und von faulen Administratoren nicht beseitigt wurden. Als Beispiel nehmen wir zwei ziemlich populäre Programme: *WebJeff Filemanager* und *Advanced Guestbook*.

Das erste Programm ist ein webbasierter Dateimanager, der

Tabelle 2. *Google – Suchanfragen nach verschiedenen Typen von WWW-Servern*

Suchanfrage	Server
`"Apache/1.3.28 Server at" intitle:index.of`	*Apache* 1.3.28S
`"Apache/2.0 Server at" intitle:index.of`	*Apache* 2.0
`"Apache/* Server at" intitle:index.of`	beliebige Version von *Apache*
`"Microsoft-IIS/4.0 Server at" intitle:index.of`	*Microsoft Internet Information Services* 4.0
`"Microsoft-IIS/5.0 Server at" intitle:index.of`	*Microsoft Internet Information Services* 5.0
`"Microsoft-IIS/6.0 Server at" intitle:index.of`	*Microsoft Internet Information Services* 6.0
`"Microsoft-IIS/* Server at" intitle:index.of`	beliebige Version von *Microsoft Internet Information Services*
`"Oracle HTTP Server/* Server at" intitle:index.of`	beliebige Version eines *Oracle*-Servers
`"IBM _ HTTP _ Server/* * Server at" intitle:index.of`	beliebige Version eines IBM Servers
`"Netscape/* Server at" intitle:index.of`	beliebige Version eines *Netscape*-Servers
`"Red Hat Secure/*" intitle:index.of`	beliebige Version eines *Red Hat Secure*-Servers
`"HP Apache-based Web Server/*" intitle:index.of`	beliebige Version eines HP-Servers

Tabelle 3. *Abfragen nach Standardseiten von WWW-Servern nach der Installation*

Abfrage	Server
`intitle:"Test Page for Apache Installation" "You are free"`	*Apache* 1.2.6
`intitle:"Test Page for Apache Installation" "It worked!" "this Web site!"`	*Apache* 1.3.0–1.3.9
`intitle:"Test Page for Apache Installation" "Seeing this instead"`	*Apache* 1.3.11–1.3.33, 2.0
`intitle:"Test Page for the SSL/TLS-aware Apache Installation" "Hey, it worked!"`	*Apache* SSL/TLS
`intitle:"Test Page for the Apache Web Server on Red Hat Linux"`	*Apache* im Red Hat-System
`intitle:"Test Page for the Apache Http Server on Fedora Core"`	*Apache* im Fedora-System
`intitle:"Welcome to Your New Home Page!" Debian`	*Apache* im Debian-System
`intitle:"Welcome to IIS 4.0!"`	*IIS* 4.0
`intitle:"Welcome to Windows 2000 Internet Services"`	*IIS* 5.0
`intitle:"Welcome to Windows XP Server Internet Services"`	*IIS* 6.0

das Hochladen der Dateien an den Server und das Erstellen, Anzeigen, Löschen und Modifizieren der sich auf dem Server befindenden Dateien ermöglicht. Leider enthält *WebJeff Filemanager* in der Version 1.6 einen Fehler, der das Ablesen jeder beliebigen Datei aus dem Server, zu welchem die den WWW-Dämon startenden Benutzer den Zugang besitzen, möglich macht. Es reicht also, dass der Eindringling im anfälligen System die Adresse */index.php3?action=telecharger&fichier=/etc/passwd* eintippt und den Inhalt der Datei */etc/passwd* bekommt (siehe Abbildung 3). Selbstverständlich nutzt der Angreifer die Google-Suchmaschine um den anfälligen Server zu finden, indem er die Abfrage: `"WebJeff-Filemanager 1.6" Login` stellt.

Die zweite Applikation – *Advanced Guestbook* – ist ein in PHP geschriebenes Programm, das die SQL-Datenbank benutzt, mit derer Hilfe man die Gästebücher in die WWW-Services hinzufügen kann. In April 2004 wurde eine Information über eine Lücke in der Version 2.2 von diesem Programm veröffentlicht. Diese Lücke (dank des SQL-Codes – siehe Artikel *SQL Injection Angriffe mit PHP und MySQL in hakin9 3/2005*) ermöglicht den Zugang zum Administrationspaneel. Es reicht die Login-Seite vom Paneel zu finden (siehe Abbildung 4) und sich da einzulogen, wobei man das Feld *username* leer lässt und im Feld *password* `') OR ('a' = 'a` eintippt oder umgekehrt – man lässt das Feld *password* leer und schreibt im Feld *username* schreibt `? or 1=1 –` hinein. Unser Angreifer kann an Google eine der folgenden Anfragen stellen, um anfällige Schaufenster im Netz zu finden: `intitle:Guestbook "Advanced Guestbook 2.2 Powered"` oder

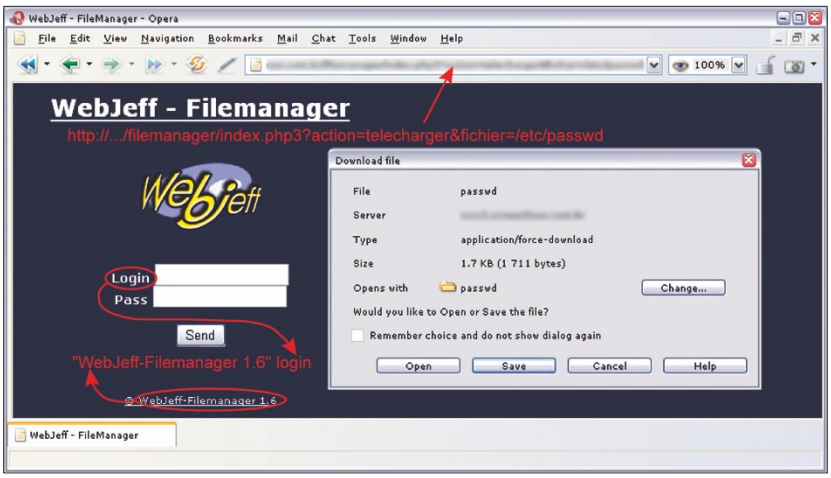


Abbildung 3. *Anfällige Version des Programms WebJeff Filemanager*

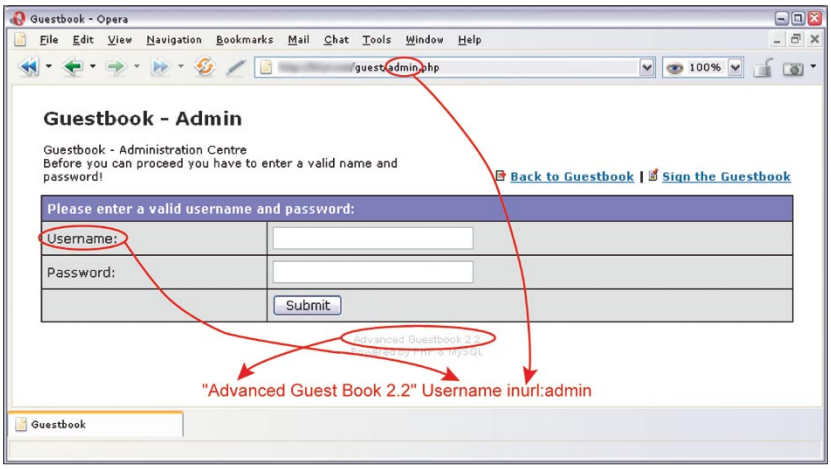


Abbildung 4. *Advanced Guestbook – Login-Seite*

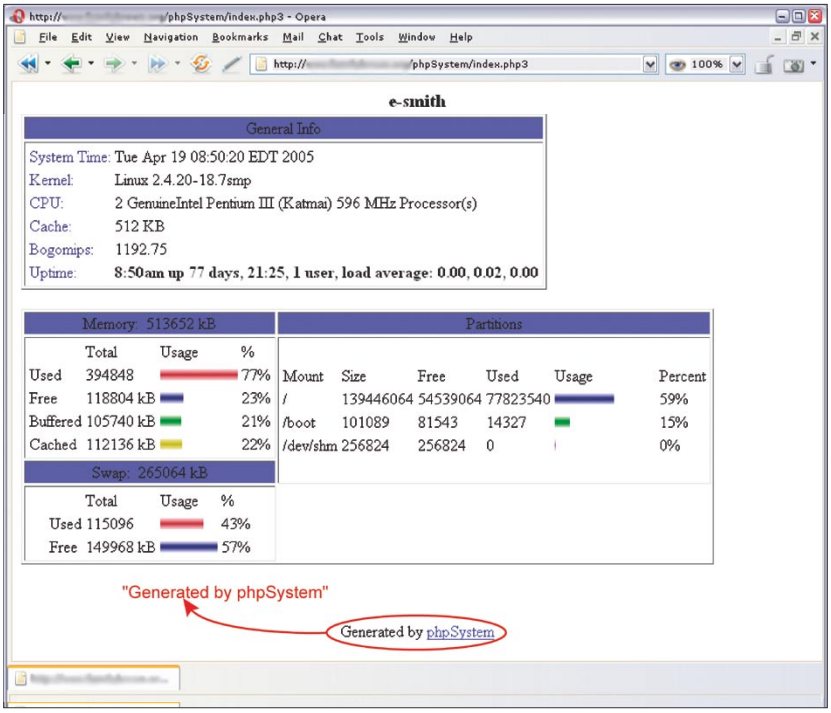


Abbildung 5. *Statistiken über phpSystem*

`"Advanced Guestbook 2.2" Username inurl:admin`.

Der oben beschriebene Datenklau lässt sich verhindern, wenn ein Administrator kontinuierlich die Informationen über alle Programme, die er in von ihm betreuten Service verwendet, überwacht und die Programm-Updates durchführt, falls ein Fehler in einem von ihnen aufgetreten ist. Die zweite Sache, um die man sich kümmern sollte, ist das Entfernen von Banner, Programmnamen und Programmversionsnummern aus allen Webseiten oder Dateien, in denen sie vorkommen.

Informationen über Netze und Systeme

Fast jeder Angriff auf ein Rechnersystem wird durch eine Zielklärung eingeleitet. Gewöhnlich beruht das darauf, dass die Rechner gescannt werden – es wird versucht die funktionierenden Dienste, den Typ vom Betriebssystem und die Version der Provisioning-Software zu bestimmen. Am häufigsten werden zu diesem Zweck Scanner vom Typ *Nmap* oder *amap* verwendet, aber es existiert noch eine andere Option. Viele Administratoren installieren WWW-Applikationen, die kontinuierlich Statistiken über die Systemarbeit erstellen, über die Belegung der Festplatte informieren, die Listen mit den gestarteten Prozessen oder sogar System-Logfiles enthalten.

Für einen Einbrecher sind das sehr wertvolle Informationen. Es reicht, dass er Google nach Statistiken des *phpSystem*–Programms fragt: `"Generated by phpSystem"`; so bekommt er Seiten, die zur auf Abbildung 5 dargestellten Seite ähnlich sind. Man kann auch nach den durch das *Sysinfo*-Script generierten Seiten fragen `intitle:"Sysinfo * " intext:"Generated by Sysinfo * written by The Gamblers."`; die viel mehr Informationen über das System enthalten (Abbildung 6).

Es gibt ganz viele Möglichkeiten (Beispiele für die Anfragen nach Statistiken und Informationen, die durch die populärsten Programme erstellt wurden, enthält Tabelle 4).

Der Erwerb solcher Erkenntnisse kann den Eindringling zur Durchführung eines Angriffs auf ein gefundenes System ermutigen und ihm dann bei der Wahl der entsprechenden Tools oder Exploits helfen. Aus diesem Grund müssen wir dafür sorgen, dass der Zugang zu den Programmen geschützt bleibt und eine Kennworteingabe verlangt wird, wenn wir diejenigen Programme verwenden, die das Monitoring unserer Rechner-Ressourcen ermöglichen.

Wir suchen nach Fehlern

Die HTTP-Fehler-Meldungen können für einen Einbrecher äußerst wertvoll sein – gerade aus diesen Informationen kann man eine Vielzahl von Daten bezüglich des Systems sowie bezüglich der Konfiguration und des Aufbaus der Datenbanken gewinnen. Zum Beispiel, um durch die *Informix*-Datenbank generierte Fehler zu finden, reicht es an die Suchmaschine die folgende Anfrage zu stellen: `"A syntax error has occurred" filetype:ihtml`. Im Resultat findet der Einbrecher die Meldungen, die die Informationen über die Konfiguration der Datenbanken, Dateistruktur im System und manchmal auch die Passwörter (siehe Abbildung 7), enthalten. Um die Suchergebnisse auf die Seiten mit den Passwörtern einzuschränken, kann man die Anfrage `"A syntax error has occurred" filetype:ihtml intext:LOGIN` ein wenig modifizieren.

Ebenso interessante Informationen kann man aus den Fehlern der *MySQL*-Datenbanken gewinnen. Man sieht das am Beispiel der Anfrage `"Access denied for user" "Using password"` – Abbildung 8 stellt eine der auf diese Weise gefundenen Seiten dar. Andere Beispiele für die Anfragen, die solche Fehler ausnutzen, befinden sich in Tabelle 5.

Die einzelne Methode zum Schutz unserer Systeme vor der Veröffentlichung der Fehler ist vor allem die schnelle Beseitigung von Anomalien. Weiterhin ist es sehr

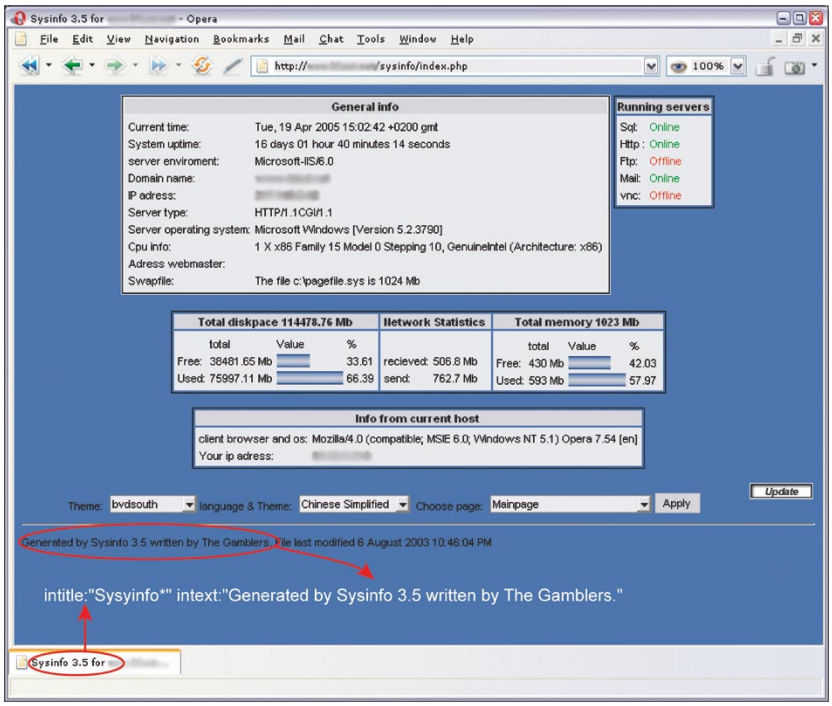


Abbildung 6. *Statistiken über Sysinfo*

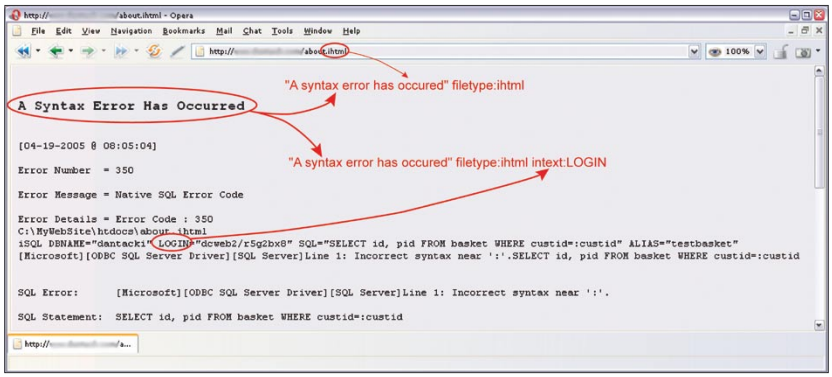


Abbildung 7. *Verwendung von Fehlern der Informix-Datenbanken*

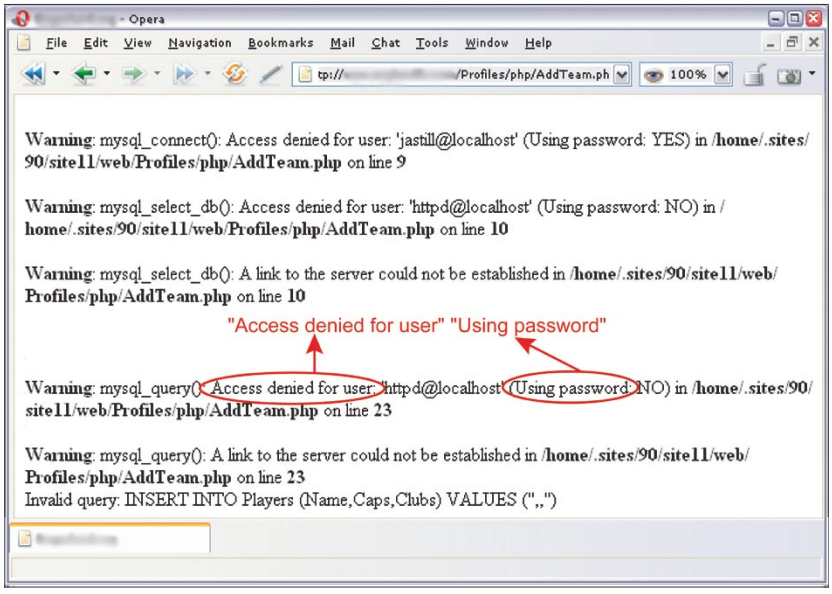


Abbildung 8. *Fehler der MySQL-Datenbank*

Tabelle 4. *Programme, die Statistiken über die Systemarbeit erstellen*

Anfrage	Informationstyp
"Generated by phpSystem"	Typ und Version des Betriebssystems, Hardware-Konfiguration, eingeloggte Benutzer, geöffnete Verbindungen, Belegung der Speicher und der Festplatten, Mount-Punkte
"This summary was generated by wwwstat"	Statistiken über die Arbeit des WWW-Servers, Dateistruktur im System
"These statistics were produced by getstats"	Statistiken über die Arbeit des WWW-Servers, Dateistruktur im System
"This report was generated by WebLog"	Statistiken über die Arbeit des WWW-Servers, Dateistruktur im System
intext:"Tobias Oetiker" "traffic analysis"	Statistiken über die Systemarbeit in Form von MRTG-Diagrammen, Netzkonfiguration
intitle:"Apache::Status" (inurl:server-status | inurl:status.html | inurl:apache.html)	Serverversion, Typ des Betriebssystems, Liste der Tochterprozesse und aktuelle Verbindungen
intitle:"ASP Stats Generator *.*" "ASP Stats Generator" "2003-2004 weppos"	Aktivität des WWW-Servers, viele Informationen über die Besucher
intitle:"Multimon UPS status page"	Statistiken über die Arbeit der UPS-Geräte
intitle:"statistics of" "advanced web statistics"	Statistiken über die Arbeit des WWW-Servers, Informationen über die Besucher
intitle:"System Statistics" +"System and Network Information Center"	Statistiken über die Systemarbeit in Form von MRTG-Diagrammen, Hardware-Konfiguration, funktionierende Dienste
intitle:"Usage Statistics for" "Generated by Webalizer"	Statistiken über die Arbeit des WWW-Servers, Informationen über die Besucher, Dateistruktur im System
intitle:"Web Server Statistics for ****"	Statistiken über die Arbeit des WWW-Servers, Informationen über die Besucher
inurl:"/axs/ax-admin.pl" -script	Statistiken über die Arbeit des WWW-Servers, Informationen über die Besucher
inurl:"/cricket/grapher.cgi"	MRTG-Diagramme von der Arbeit der Netzinterfaces
inurl:server-info "Apache Server Information"	Version und Konfiguration des WWW-Servers, Typ des Betriebssystems, Dateistruktur im System
"Output produced by SysWatch *"	Typ und Version des Betriebssystems, eingeloggte Benutzer, Belegung der Speicher und der Festplatten, Mount-Punkte, aktivierte Prozesse, System-Logfiles

gut, wenn wir über Möglichkeiten verfügen, das Konfigurieren der Software auf solche Weise, dass die Informationen über Fehler in den speziell dafür bestimmtem Dateien gespeichert und nicht an die für die Benutzer zugänglichen Seiten geschickt werden.

Wir sollten nicht vergessen, dass selbst wenn wir die Fehler ziemlich schnell beseitigen (und damit erreichen, dass die via Google gezeigten Seiten nicht mehr aktuell sind), sich der Eindringling dennoch eine Kopie der Webseite ansehen kann, die in dem *Cache* der Google-Suchmaschine gespeichert wird. Es reicht, dass er auf der Liste der Suchergebnisse einen Link zur Schaufensterkopie anklickt. Zum Glück werden, aufgrund der immensen Anzahl an Internet-Ressourcen, die Kopien der Webseiten nur für kurze Zeit im Google-*Cache* gehalten.

Wir suchen nach Passwörtern

Im Netz kann man eine Vielzahl von Passwörtern zu Ressourcen aller Art finden – E-Mail-Konten, FTP-Server oder sogar Shell-Konten. Dies folgt hauptsächlich aus der Unwissenheit der Benutzer, die unbewusst ihre Kennwörter in den öffentlich zugänglichen Stellen anlegen oder auch aus der Nachlässigkeit der Software-Hersteller, die entweder die Benutzerdaten nicht angemessen bewahren oder die Nutzer nicht darüber informieren, dass die Standardkonfiguration ihrer Produkte modifiziert werden muss.

Betrachten wir das Beispiel von *WS_FTP* – vom gut bekannten und allgemein verwendeten FTP-Client, der ähnlich zu den meisten Provisioning-Softwares das Mer-

ken der Passwörter zu den Konten ermöglicht. *WS_FTP* speichert die Konfiguration und die Informationen über die Benutzerkonten in der *WS_FTP.ini*–Datei. Leider ist es nicht uns allen bewusst, dass jeder, der den Zugang zur Konfiguration des FTP-Clients erreicht, gleichzeitig den Zugang zu unseren Ressourcen besitzt. Zwar sind die in der *WS_FTP.ini*–Datei gelagerten Passwörter verschlüsselt, aber das sind nicht die ausreichenden Schutzmaßnahmen – hat ein Einbrecher die Konfigurationsdatei, dann kann er die Tools, die die Entschlüsselung der Passwörter ermöglichen, verwenden oder das *WS_FTP*-Programm einfach installieren und es mit unserer Konfiguration starten. Und auf welche Weise kann ein Einbrecher zu Tausenden von Konfigurationsdateien des *WS_FTP*-Clients gelangen? Via Google selbstverständlich. Dank der Anfragen `"Index of/" "Parent Directory" "WS_FTP.ini"` oder `filetype:ini WS_`

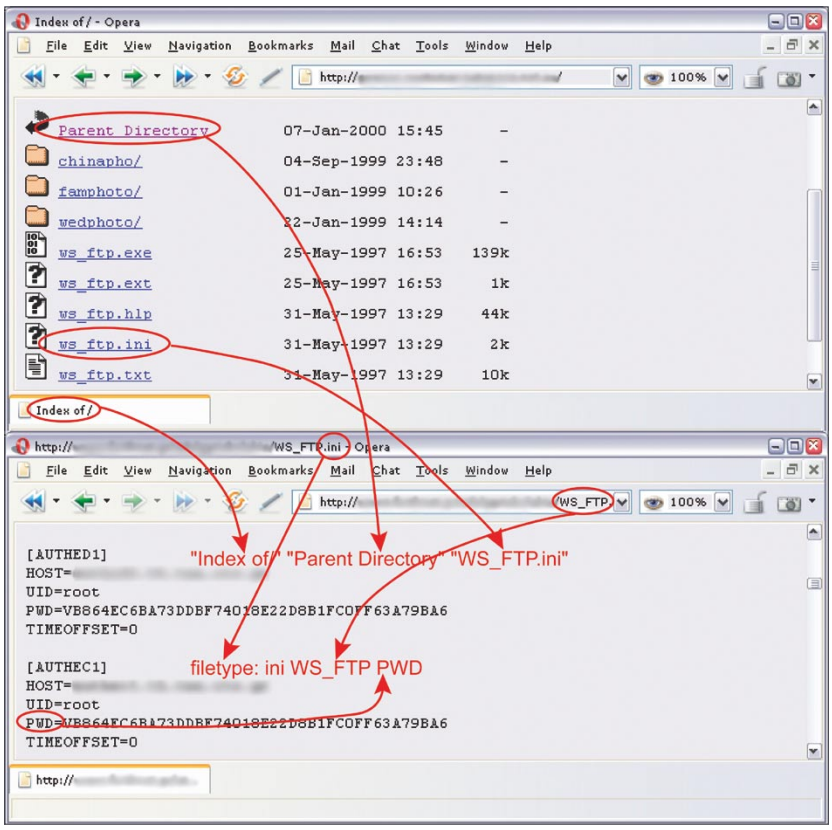


Abbildung 9. *Konfigurationsdatei des WS_FTP-Programms*

Tabelle 5. *Fehlermeldungen*

Anfrage	Resultat
`"A syntax error has occurred" filetype:ihtml`	Fehler der *Informix*-Datenbank – sie können Funktionsnamen, Dateinamen, Informationen über die Dateistruktur, Fragmente des SQL-Codes und Passwörter enthalten
`"Access denied for user" "Using password"`	Fehler bei Autorisierung – sie können Benutzernamen, Funktionsnamen, Informationen über die Dateistruktur und Fragmente des SQL-Codes enthalten
`"The script whose uid is " "is not allowed to access"`	PHP-Fehler, die mit der Zugangskontrolle verbunden sind – sie können Dateinamen, Funktionsnamen, Informationen über die Dateistruktur enthalten
`"ORA-00921: unexpected end of SQL command"`	Fehler der *Oracle*-Datenbank – sie können Dateinamen, Funktionsnamen und Informationen über die Dateistruktur enthalten
`"error found handling the request" cocoon filetype:xml`	Fehler des *Cocoon*-Programms – sie können die Versionsnummer von *Cocoon*, Dateinamen, Funktionsnamen und Informationen über die Dateistruktur enthalten
`"Invision Power Board Database Error"`	Fehler des *Invision Power Board* – Diskussionsforums – sie können Funktionsnamen, Dateinamen, Informationen über die Dateistruktur im System und Fragmente des SQL-Codes enthalten
`"Warning: mysql_query()" "invalid query"`	Fehler der *MySQL*-Datenbank – sie können Benutzernamen, Funktionsnamen, Dateinamen und Informationen über die Dateistruktur enthalten
`"Error Message : Error loading required libraries."`	Fehler des CGI-Scripts – sie können Informationen über den Typ des Betriebssystems und der Software-Version, Benutzernamen, Dateinamen und Informationen über die Dateistruktur im System enthalten
`"#mysql dump" filetype:sql`	Fehler der *MySQL*-Datenbank – sie können Informationen über die Struktur und den Inhalt der Datenbank enthalten

Tabelle 6. *Passwörter – Beispiele für die Anfragen an Google*

Anfrage	Resultat
`"http://*:*@www" site`	Passwörter zur Seite *site*, geschrieben in der Form: *http://username:password@www...*
`filetype:bak inurl:"htaccess|passwd|shadow|htusers"`	Backups der Dateien, die Informationen über Benutzernamen und Passwörter enthalten können
`filetype:mdb inurl:"account|users|admin|administrators|passwd|password"`	Dateien vom Typ *mdb*, die Informationen über Passwörter enthalten können
`intitle:"Index of" pwd.db`	*pwd.db* – Dateien können Benutzernamen und verschlüsselte Passwörter enthalten
`inurl:admin inurl:backup intitle:index.of`	Verzeichnisse, die in ihrem Namen die Wörter *admin* und *backup* enthalten können
`"Index of/" "Parent Directory" "WS_FTP.ini" filetype:ini WS_FTP PWD`	Konfigurationsdateien des *WS_FTP*-Programms, die Passwörter zu den FTP-Servern enthalten können
`ext:pwd inurl:(service|authors|administrators|users) "# -FrontPage-"`	Dateien, die Passwörter des *Microsoft FrontPage* – Programms enthalten
`filetype:sql ("passwd values ****" | "password values ****" | "pass values ****" )`	Dateien, die SQL-Code und in Datenbanken enthaltene Passwörter enthalten
`intitle:index.of trillian.ini`	Konfigurationsdateien des *Trillian*-Messengers
`eggdrop filetype:user user`	Konfigurationsdateien von *Eggdrop*-IRCbot
`filetype:conf slapd.conf`	Konfigurationsdateien der *OpenLDAP*-Applikation
`inurl:"wvdial.conf" intext:"password"`	Konfigurationsdateien des *WV Dial*-Programms
`ext:ini eudora.ini`	Konfigurationsdateien des *Eudora*-Mailprogramms
`filetype:mdb inurl:users.mdb`	*Microsoft Access*-Dateien, die Informationen über die Konten enthalten können
`intext:"powered by Web Wiz Journal"`	WWW-Dienste, die die *Web Wiz Journal*-Applikation benutzen, die in der Standardkonfiguration das Herunterladen der Datei mit dem Passwort ermöglichen; anstelle der Default-Adresse *http:///<host>/journal/ schreibt man http:///<host>/journal/journal.mdb* hinein
`"Powered by DUclassified" -site:duware.com "Powered by DUcalendar" -site:duware.com "Powered by DUdirectory" -site:duware.com "Powered by DUclassmate" -site:duware.com "Powered by DUdownload" -site:duware.com "Powered by DUpaypal" -site:duware.com "Powered by DUforum" -site:duware.com intitle:dupics inurl:(add.asp | default.asp | view.asp | voting.asp) -site:duware.com`	WWW-Dienste, die die Applikationen *DUclassified*, *DUcalendar*, *DUdirectory*, *DUclassmate*, *DUdownload*, *DUpaypal*, *DUforum* oder *DUpics* verwenden, die in der Standardkonfiguration das Herunterladen der Datei mit dem Passwort ermöglichen; anstelle der Default-Adresse (für *DUclassified*) *http:///<host>/duClassified/* schreibt man *http:///<host>/duClassified/_private/duclassified.mdb* hinein
`intext:"BiTBOARD v2.0" "BiTSHiFTERS Bulletin Board"`	WWW-Dienste, die die *Bitboard2*–Applikation verwenden, die in der Standardkonfiguration das Herunterladen der Datei mit dem Passwort ermöglicht; anstelle der Default-Adresse *http:///<host>/forum/forum.php* schreibt man *http:///<host>/forum/admin/data_passwd.dat* hinein

`FTP PWD` bekommt er eine Vielzahl von Links zu für ihn interessanten Daten, die wir ihm selbst aufgrund unserer Unwissenheit in die Hände legen (Abbildung 9).

Ein anderes Beispiel ist eine webbasierte Applikation mit dem Namen *DUclassified*, die das Hinzufügen und die Verwaltung der Werbungen in Internet-Services ermöglicht. In der Standardkonfiguration dieses Programms werden Benutzernamen, Passwörter und andere Daten in der *duclassified.mdb* gelagert – in einer Datei, die sich im nicht geschützten *_private* – Unterverzeichnis befindet. Es reicht nun einen *DUclassifield* verwendenden Dienst mit der Adresse z.B. *http:///<host>/duClassified/* zu finden und sie auf *http:///<host>/duClassified/_private/duclassified.mdb* zu ändern, um die Dateien mit den Passwörtern zu erhalten und damit einen unbe-

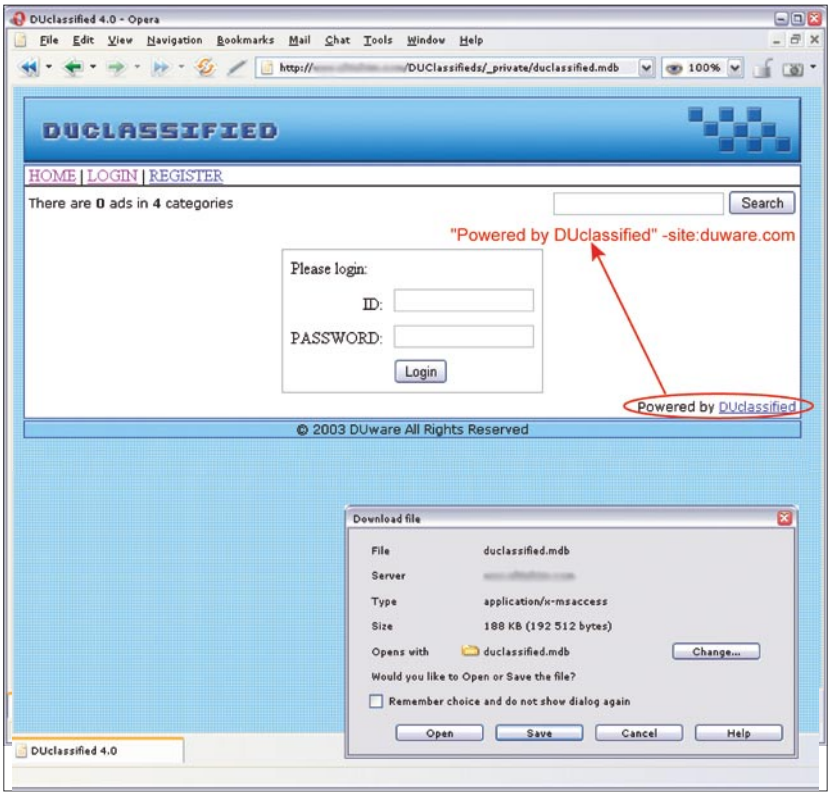
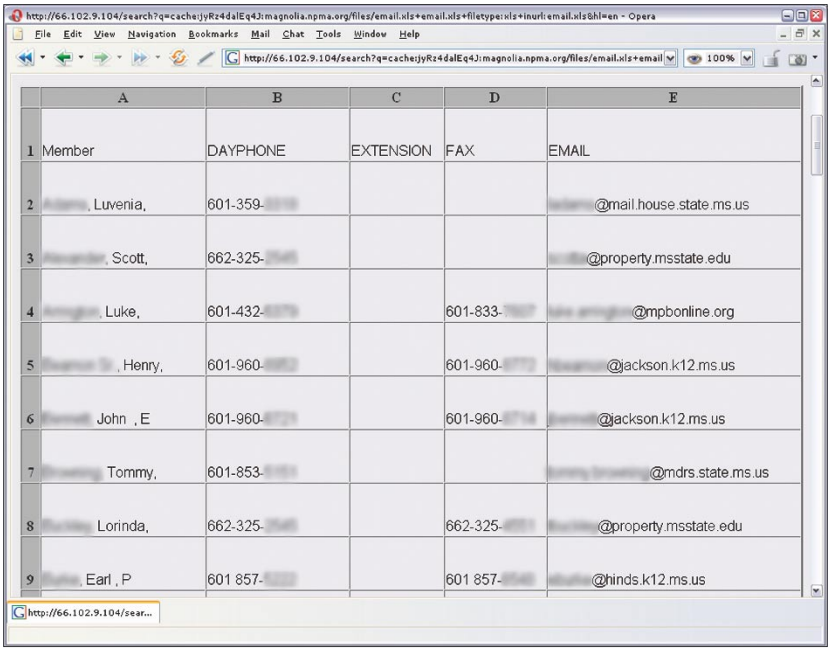


Abbildung 10. *Standardmäßig konfiguriertes Duclassified-Programm*



	A	B	C	D	E
1	Member	DAYPHONE	EXTENSION	FAX	EMAIL
2	, Luvenia,	601-359-			@mail.house.state.ms.us
3	, Scott,	662-325-			@property.msstate.edu
4	, Luke,	601-432-		601-833-	@mpbonline.org
5	, Henry,	601-960-		601-960-	@jackson.k12.ms.us
6	John , E	601-960-		601-960-	@jackson.k12.ms.us
7	Tommy,	601-853-			@mdrs.state.ms.us
8	Lorinda,	662-325-		662-325-	@property.msstate.edu
9	Earl , P	601 857-		601 857-	@hinds.k12.ms.us

Abbildung 11. *Dank Google gefundenes elektronisches Adressbuch*

Im Internet

- *http://johnny.ihackstuff.com/ – das größte Kompendium der Informationen über Google Hacking,*
- *http://insecure.org/nmap/ – Nmap*-Netzscanner,
- *http://thc.org/thc-amap/ – amap*-Scanner.

schränkten Zugang zur Applikation (dies wird an Abbildung 10 gezeigt). In der Suche nach Schaufenstern, die die erwähnte Applikation benutzen, kann wiederum die folgende an Google gestellte Anfrage helfen: `"Powered by DUclassified" -site:duware.com` (um die das Herstellerschaufenster betreffenden Ergebnisse zu vermeiden). Was interessant ist, der Hersteller von *DUclassified* – die Firma DUware – hat einige andere Applikationen erstellt, die auch gegen ähnliche Missbräuche anfällig sind.

Theoretisch wissen wir alle, dass man die Passwörter weder an den Bildschirm ankleben noch unter der Tastatur verstecken sollte. Währenddessen schreiben ziemlich viele Leute die Passwörter in die Dateien hinein und legen sie in den Heimverzeichnissen an, die, trotz unserer Erwartungen, vom Internet her erreichbar sind. Dazu bekleiden noch viele von ihnen Funktionen wie Netzadministrator oder ähnliche, wodurch diese Dateien beachtliche Größen erreichen. Es ist schwer eine konkrete Regel anzugeben, nach der man solche Daten wieder findet, aber die Kombination der Wörter *account*, *users*, *admin*, *administrators*, *passwd*, *password* etc. ist nützlich. In der Verbindung mit den Dateitypen *.xls*, *.txt*, *.doc*, *.mdb* und *.pdf*. Es lohnt sich auch auf die Verzeichnisse mit den Wörtern *admin*, *backup* oder mit ähnlichen Namen aufmerksam zu machen: `inurl:admin intitle:index.of`. Beispiele für die Anfragen nach den mit Passwörtern verbundenen Daten kann man in Tabelle 6 finden.

Um den Eindringlingen den Zugang zu unseren Passwörtern zu erschweren, müssen wir vor allem daran denken, wo und warum wir sie zuweisen, wie sie aufbewahrt werden und was mit ihnen geschieht. Wenn wir uns um einen Internet-Dienst kümmern, sollten wir die Konfiguration der verwendeten Applikationen analysieren, schwach geschützte oder sensible Daten wieder finden und sie entsprechend schützen.

Personenbezogene Daten und sensible Dokumente

Sowohl in der EU als auch in den Vereinigten Staaten existieren entsprechende Rechtsregelungen, die als Ziel haben, unsere Privatsphäre zu schützen. Leider kommt es vor, dass sensible Dokumente aller Art mit unseren Daten an öffentlich zugängliche Orte gelegt oder durch das Netz ohne entsprechende Verschlüsselung geschickt werden. Es reicht, dass ein Eindringling den Zugang zu unserer elektronischen Post mit unserem Lebenslauf bekommt, das wir während der Suche nach Arbeit abgeschickt haben, dann lernt er unsere Adresse, Telefonnummer, Geburtsdatum, Ausbildungsverlauf, Wissen und Erfahrung kennen.

Im Internet kann man eine Menge von Dokumenten dieses Typs finden. Um sie zu entdecken, muss man die folgende Anfrage stellen: `intitle:"curriculum vitae" "phone * * *" "address *" "e-mail"`. Es ist auch einfach die Daten, wie die Listen mit den Nachnamen, Telefonnummern und E-Mail-Adressen zu finden (Abbildung 11). Dies folgt aus der Tatsache, dass fast alle Internet-Benutzer verschiedene elektronische Adressbücher erstellen – für einen durchschnittlichen Eindringling sind sie von geringer Bedeutung, aber schon ein geschickter Soziotechniker wird wissen, wie man in ihnen enthaltene Daten verwenden kann, vor allem wenn sie Kontakte im Bereich eines Unternehmens betreffen. Ziemlich nützlich ist zum Beispiel die Anfrage: `filetype:xls inurl:"email.xls"`, die alle Kalkulationsbögen mit dem Namen *email.xls* wiederfindet.

Ähnlich sieht die Situation mit den Instant Messengern und den in ihnen gespeicherten Kontaktlisten aus – nachdem ein Einbrecher so eine Aufstellung erreicht hat, kann er versuchen, sich als einer unserer Freunde auszugeben. Was interessant ist, man kann ziemlich viele solcher Informationen in Amtsdokumenten aller Art finden – Polizeiberichte, Gerichtsschreiben oder sogar Beschreibungen des Krankheitsverlaufs.

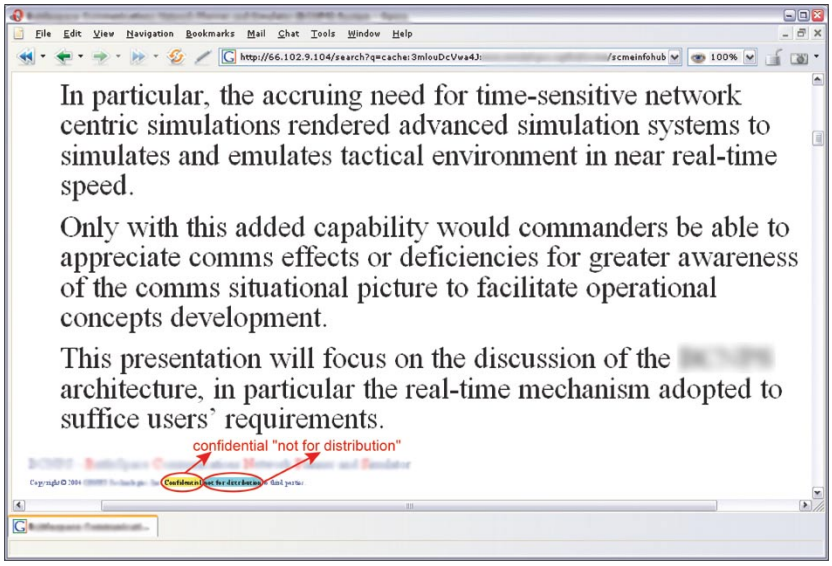


Abbildung 12. *Mittels der Suchmaschine gefundenes geschütztes Dokument*

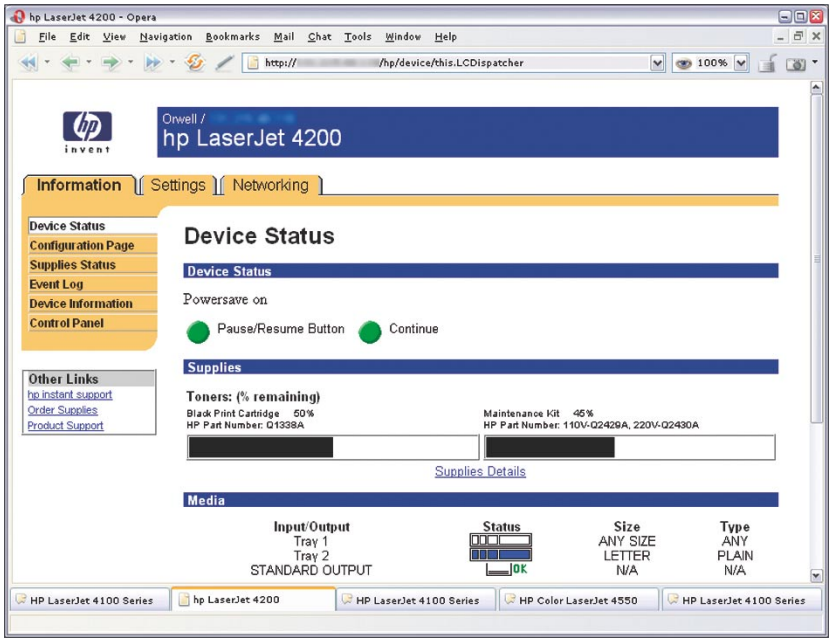


Abbildung 13. *Via Google gefundene Konfigurationsseite eines HP-Druckers*

Im Netz kann man auch Dokumente finden, die mit einer Geheimhaltungsklausel versehen wurden, also geschützte Informationen enthalten. Dies können Projektpläne, technische Dokumentationen, verschiedene Fragebögen, Berichte, Präsentationen und viele andere Dokumente eines Unternehmens sein. Man kann sie finden, weil sie sehr oft das Wort *confidential*, die Phrase *Not for distribution* oder ähnliche enthalten (siehe Abbildung 12). Tabelle 7 enthält ein paar Beispiele von Anfragen nach Dokumenten, die personenbezogene Daten oder sensible Informationen enthalten können.

Ähnlich wie im Falle der Passwörter, um die Bekanntmachung unserer privaten Informationen zu verhindern, können wir ausschließ-

lich Vorsichtsmaßnahmen treffen und über die veröffentlichten Daten herrschen. Firmen und Institutionen sollten (in vielen Fällen sogar müssen) entsprechende Reglements, Prozeduren und den inneren Informationsverkehr bestimmende Verhaltensweisen, Verantwortung und Konsequenzen für die Nichtbefolgung der Vorschriften bearbeiten und einführen.

Netzgeräte

Viele Administratoren nehmen den Schutz von Geräten wie Netzdruckern oder Webcams nicht ernst. So kann ein schlecht geschützter Drucker ein Zufluchtsort sein, der zuerst von einem Einbrecher erobert werden, und dann zur Durchführung eines Angriffs gegen übrige Systeme innerhalb oder außerhalb des Netzes dienen kann. Internet-Webcams sind selbstverständlich nicht so gefährlich, man kann sie eher als Spaß betrachten, jedoch ist es nicht schwer sich eine Situation vorzustellen, in der solche Daten von Bedeutung sein könnten (Industriespionage, Raubüberfall). Anfragen nach Druckern und Webcams enthält Tabelle 8. Abbildung 13 stellt die im Netz gefundene Konfigurationsseite eines Druckers dar. ■

Tabelle 7. *Suche nach personenbezogenen Daten und sensiblen Dokumenten*

Abfrage	Resultat
`filetype:xls inurl:"email.xls"`	*email.xls*-Dateien, die die Daten mit Telefonnummern und Adressen enthalten können
`"phone * * *" "address *" "e-mail" intitle:"curriculum vitae"`	CV-Dokumente
`"not for distribution" confidential`	mit der *confidential*-Klausel versehene Dokumente
`buddylist.blt`	Kontaktliste des *AIM*-Messengers
`intitle:index.of mystuff.xml`	Kontaktliste des *Trillian*-Messengers
`filetype:ctt "msn"`	Kontaktliste des *MSN*-Messengers
`filetype:QDF QDF`	Datenbank des Finanzprogramms *Quicken*
`intitle:index.of finances.xls`	*finances.xls*-Dateien, die Informationen über Bankkonten, Finanzaufstellungen und Kreditkartennummer enthalten können
`intitle:"Index Of" -inurl:maillog maillog size`	*maillog*-Dateien, die E-Mails enthalten können
`"Network Vulnerability Assessment Report" "Host Vulnerability Summary Report" filetype:pdf "Assessment Report" "This file was generated by Nessus"`	Berichte über die Untersuchung der Netzsicherheit, Penetrationstesten etc.

Tabelle 8. *Charakteristische Zeichenfolgen für Netzgeräte*

Anfrage	Gerät
`"Copyright (c) Tektronix, Inc." "printer status"`	PhaserLink-Drucker
`inurl:"printer/main.html" intext:"settings"`	Brother HL-Drucker
`intitle:"Dell Laser Printer" ews`	Della-Drucker mit der EWS-Technologie
`intext:centreware inurl:status`	Drucker Xerox Phaser 4500/6250/8200/8400
`inurl:hp/device/this.LCDispatcher`	HP-Drucker
`intitle:liveapplet inurl:LvAppl`	Canon Webview-Webcams
`intitle:"EvoCam" inurl:"webcam.html"`	Evocam-Webcams
`inurl:"ViewerFrame?Mode="`	Panasonic Network Camera-Webcams
`(intext:"MOBOTIX M1" | intext:"MOBOTIX M10") intext: "Open Menu" Shift-Reload`	Mobotix-Webcams
`inurl:indexFrame.shtml Axis`	Axis-Webcams
`SNC-RZ30 HOME`	Sony SNC-RZ30-Webcams
`intitle:"my webcamXP server!" inurl:":8080"`	über die WebcamXP Server-Applikation verfügbare Webcams
`allintitle:Brains, Corp. Camera`	über die mmEye-Applikation verfügbare Webcams
`intitle:"active webcam page"`	Webcams mit USB-Interface