Google dangereux – à la recherche des informations confidentielles

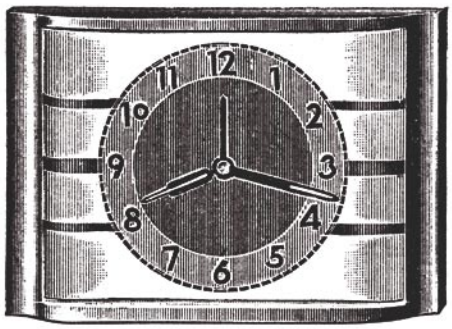
Michał Piotrowski

Article publié dans le numéro 4/2005 du magazine *hakin9*

Magazine *hakin9*, Wydawnictwo Software, ul. Lewartowskiego 6, 00-190 Warszawa, *fr@hakin9.org*

Google dangereux – à la recherche des informations confidentielles

Michał Piotrowski



Des informations qui doivent être protégées sont très souvent disponibles au grand public. Elles sont mises à disposition inconsciemment – suite à la négligence ou l'ignorance de simples utilisateurs. Le résultat est que ces données confidentielles peuvent se trouver à la portée de mains de tout le monde sur Internet. Il suffit pour cela d'utiliser Google.

Google répond à environ 80 pourcent de toutes les questions posées et par conséquent, c'est le moteur de recherche le plus utilisé. Cela est dû non seulement à son mécanisme de génération de résultats très efficace mais aussi à de grandes possibilités au niveau des questions posées. Il ne faut pas pourtant oublier qu'Internet est un média très dynamique et que les résultats de recherche présentés par Google ne sont pas toujours d'actualités. Il arrive que certaines pages trouvées soient vieilles et que plusieurs pages ayant un contenu similaire n'aient pas été visitées par Googlebot (script ayant pour but de rechercher et d'indexer les ressources Web).

Les opérateurs de précision les plus importants et les plus utiles, y compris leur description et le résultat de leur fonctionnement, sont présentés dans le Tableau 1. Les endroits des documents auxquels ils se réfèrent lors de recherche de ressources réseau (sur l'exemple du site de la revue *hakin9*) sont visibles sur la Figure 1. Ce ne sont que des exemples – une question mieux construite dans Google permettra d'obtenir de meilleurs résultats et en conséquent des informations beaucoup plus intéressantes.

Cet article explique...

- comment rechercher des informations confidentielles en utilisant Google,
- comment trouver des informations sur des systèmes et des services réseaux vulnérables aux attaques,
- comment trouver dans Google des périphériques réseaux disponibles au grand public.

Ce qu'il faut savoir...

- savoir utiliser un navigateur Web,
- avoir un savoir-faire de base sur le protocole HTTP.

À propos de l'auteur

Michał Piotrowski a plusieurs années d'expérience en tant qu'administrateur des réseaux et des systèmes d'information. Depuis plus de 3 ans, il travaille en tant qu'inspecteur de sécurité. Il est expert en matière de sécurité des réseaux téléinformatiques dans l'un des établissements financiers en Pologne. Il passe son temps libre à programmer et à s'occuper de la cryptographie.

Tableau 1. *Opérateurs de requêtes dans Google*

Opérateur	Description	Exemple d'utilisation
`site`	limite les résultats aux pages se trouvant dans un domaine défini	`site:google.com fox` trouvera toutes les pages contenant le mot *fox* dans leur texte et se trouvant dans le domaine **.google.com*
`intitle`	limite les résultats aux documents contenant une phrase donnée dans le titre	`intitle:fox fire` trouvera les pages contenant le mot *fox* dans le titre et *fire* dans le texte
`allintitle`	limite les résultats aux documents contenant toutes les phrases données dans le titre	`allintitle:fox fire` trouvera toutes les pages contenant les mots *fox* et *fire* dans le titre ; son fonctionnement est similaire à celui de `intitle:fox intitle:fire`
`inurl`	limite les résultats aux pages contenant une phrase donnée dans l'adresse URL	`inurl:fox fire` trouvera les pages contenant les mot *fire* dans le texte et *fox* dans l'adresse URL
`allinurl`	limite les résultats aux pages contenant toutes les phrases données dans l'adresse URL	`allinurl:fox fire` trouvera les pages contenant les mots *fox* et *fire* dans l'adresse URL ; son fonctionnement est similaire à celui de `inurl:fox inurl:fire`
`filetype, ext`	limite les résultats à un type de document donnée	`filetype:pdf fire` retournera les documents PDF contenant le mot *fire* et `filetype:xls fox` retournera les documents *Excel* contenant le mot *fox*
`numrange`	limite les résultats aux documents contenant dans leur texte le nombre d'une page définie	`numrange:1-100 fire` retournera les pages comprises entre 1 et 100 contenant le mot *fire*. Le même résultat peut être obtenu en posant la question : `1..100 fire`
`link`	limite les résultats aux pages contenant des liens vers une page donnée	`link:www.google.fr` retournera les documents contenant au moins un lien vers la page *www.google.fr*
`inanchor`	limite les résultats aux pages avec un lien contenant dans sa description une phrase donnée	`inanchor:fire` retournera les documents contenant les liens possédant le mot *fire* dans sa description (non dans l'adresse URL vers laquelle ils conduisent mais dans la partie soulignée du texte représentant le lien)
`allintext`	limite les résultats aux documents contenant dans le texte une phrase donnée sans se soucier du titre, des liens et des adresses URL	`allintext:"fire fox"` retournera les documents contenant la phrase *fire fox* seulement dans le texte
`+`	impose une présence fréquente de la phrase donnée dans les résultats	`+fire` met les résultats en ordre conformément à la fréquence de présence du mot *fire*.
`-`	impose la non présence de la phrase donnée dans les résultats	`-fire` retournera les documents ne contenant pas le mot *fire*.
`""`	permet de rechercher toutes les phrases et pas seulement que les mots	`"fire fox"` retournera les documents contenant la phrase *fire fox*
`.`	est remplacé par un caractère unique	`fire.fox` retournera les documents contenant les phrases *fire fox*, *fireAfox*, *fire1fox*, *fire-fox* etc.
`*`	est remplacé par un mot unique	`fire * fox` retournera les documents contenant les phrases *fire the fox*, *fire in fox*, *fire or fox* etc.
`|`	OR logique	`"fire fox" | firefox` retournera les documents contenant la phrase *fire fox* ou le mot *firefox*

Figure 1. *Utilisation d'opérateurs de recherche sur l'exemple du site de hakin9*

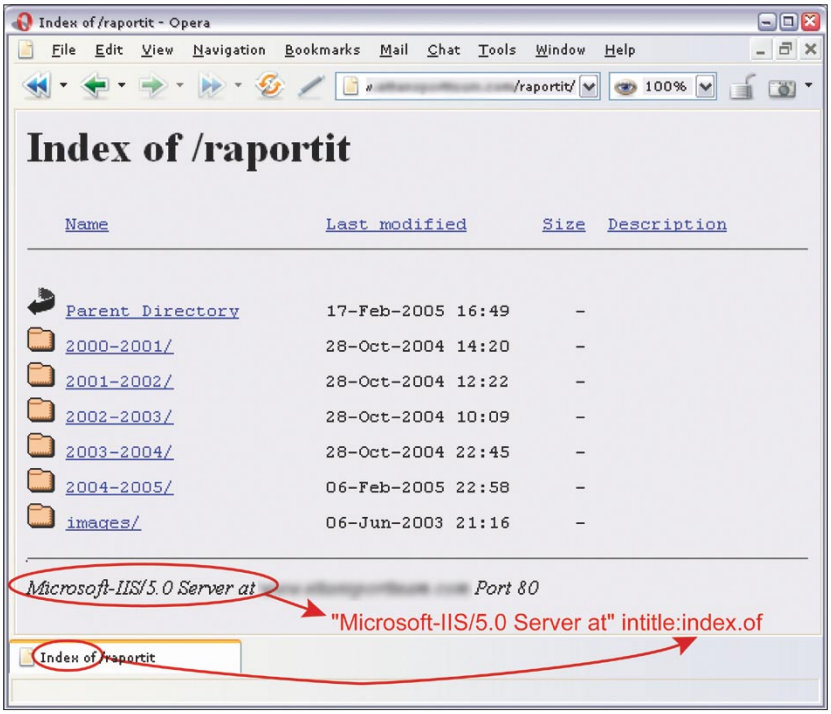


Figure 2. *Recherche de serveur IIS 5.0 à l'aide de l'opérateur intitle*

Chercher une victime

Grâce à Google, il est possible non seulement de trouver des ressources Internet visant plutôt le grand public mais aussi des ressources dites confidentielles et donc privées. Si vous posez une question appropriée, il se peut que vous receviez de surprenants résultats. Commençons par quelque chose de simple.

Imaginez qu'un trou de sécurité est trouvé dans un logiciel communément utilisé. Admettons qu'il concerne le serveur Microsoft IIS en version 5.0 et que l'objectif d'un agresseur potentiel soit de trouver quelques machines équipées de ce logiciel afin de les attaquer. Bien sûr, il pourrait utiliser à cette fin un scanner mais il préfère choisir Google – il tape alors la question suivante : `"Microsoft-IIS/5.0 Server at" intitle:index.of`. En conséquence, il reçoit des liens vers des serveurs recherchés et plus précisément aux contenus listés des répertoires disponibles sur ces serveurs. Il est ainsi vu que dans la configuration standard, les logiciels IIS (et beaucoup d'autres) ajoutent à certaines pages générées dynamiquement des bannières publicitaires contenant leur nom et le numéro de la version (voir la Figure 2).

C'est un exemple d'information non dangereuse en elle-même ; vu qu'elle est très souvent ignorée et laissée dans la configuration standard. Malheureusement, c'est aussi une information qui dans certains cas peut devenir très importante pour l'agresseur. Pour plus de questions standard à poser dans Google concernant les autres types de serveurs, reportez-vous au Tableau 2.

Une autre méthode pour trouver les versions données de serveurs Web consiste à rechercher les pages standard fournies avec les serveurs et disponibles après l'installation. Cela peut paraître bizarre mais sur le réseau, il y a plein de serveurs dont le contenu par défaut n'a pas été modifié après l'installation. Très souvent, ce sont des machines oubliées et protégées de façon insuffisante qui s'avère être une cible facile pour les intrus. Pour en trouver, il suffit de poser les questions présentées dans le Tableau 3.

Cette méthode est très simple et à la fois utile. Elle permet d'obtenir l'accès à un grand nombre de différents services réseaux et systèmes d'exploitation utilisant des applications où il y a des erreurs qui ont été détectées et que les administrateurs paresseux ou inconscients n'ont pas supprimées. Prenons comme exemple deux logiciels assez populaires : *WebJeff Filemanager* et *Advanced Guestbook*.

Le premier d'entre eux est un gestionnaire de fichiers Web permettant d'envoyer des fichiers sur des serveurs. De plus, grâce à ce logiciel, il est possible de créer,

Focus

Tableau 2. *Google – questions concernant les différents types de serveurs Web*

Question	Serveur
`"Apache/1.3.28 Server at" intitle:index.of`	*Apache* 1.3.28
`"Apache/2.0 Server at" intitle:index.of`	*Apache* 2.0
`"Apache/* Server at" intitle:index.of`	n'importe quelle version d'*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`	n'importe quelle version de *Microsoft Internet Information Services*
`"Oracle HTTP Server/* Server at" intitle:index.of`	n'importe quelle version de serveur *Oracle*
`"IBM_HTTP_Server/* * Server at" intitle:index.of`	n'importe quelle version de serveur IBM
`"Netscape/* Server at" intitle:index.of`	n'importe quelle version de serveur *Netscape*
`"Red Hat Secure/*" intitle:index.of`	n'importe quelle version de serveur *Red Hat Secure*
`"HP Apache-based Web Server/*" intitle:index.of`	n'importe quelle version de serveur HP

Tableau 3. *Questions sur les pages standard après l'installation des serveurs Web*

Question	Serveur
`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* d'un système Red Hat
`intitle:"Test Page for the Apache Http Server on Fedora Core"`	*Apache* d'un système Fedora
`intitle:"Welcome to Your New Home Page!" Debian`	*Apache* d'un système Debian
`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

de consulter, de supprimer et même de modifier tous fichiers présents sur le serveur concerné. Malheureusement, *WebJeff Filemanager* en version 1.6 a une erreur permettant de lire le contenu de n'importe quel fichier se trouvant sur le serveur auquel peut accéder l'utilisateur démarrant un navigateur Web. Il suffit donc que l'intrus tape dans le système vulnérable l'adresse */index.php3?action=telecharger&fichier=/etc/passwd* pour qu'il obtienne le contenu du fichier */etc/passwd* (voir la Figure 3). Bien sûr, pour trouver les serveurs vulnérables, l'agresseur utilisera Google en posant la question : `"WebJeff-Filemanager 1.6" Login`.

La deuxième application – *Advanced Guestbook* – est un logiciel écrit en PHP utilisant la base de données SQL permettant d'ajouter des messages laissés par les visiteurs au livre d'or du site visité. En avril 2004, l'information concernant un trou de sécurité dans la version 2.2 de ce logiciel permettant (grâce à la possibilité d'insérer le code SQL – voir l'article *Attaques par injection SQL avec PHP et MySQL* dans *hakin9* n° 3/2005) d'obtenir l'accès au panneau de configuration. Il suffit de trouver la page d'ouverture de session au panneau (voir la Figure 4) et d'ouvrir la session en laissant le champ *username* vide et de taper dans le champ *password* `') OR ('a' = 'a` ou à l'inverse – laisser le champ *password* vide et taper `? or 1=1 –` dans le champ *username*. Pour trouver sur le réseau les sites vulné-

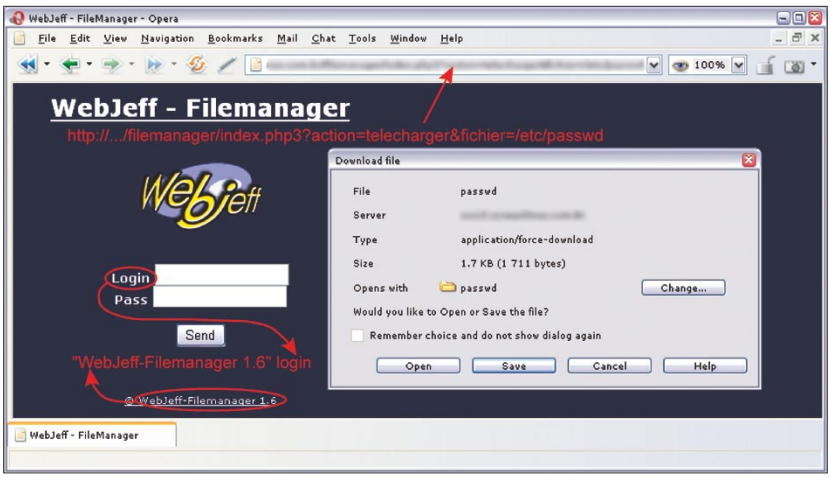


Figure 3. *Version vulnérable du logiciel WebJeff Filemanager*

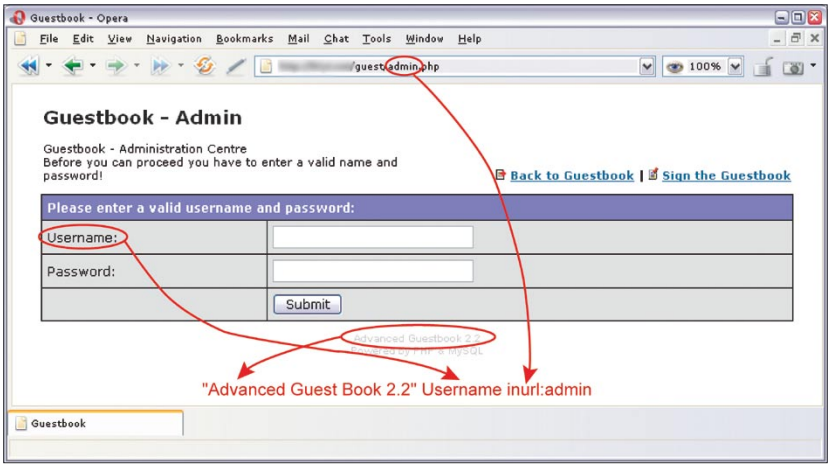


Figure 4. *Advanced Guestbook – page d'ouverture de session*

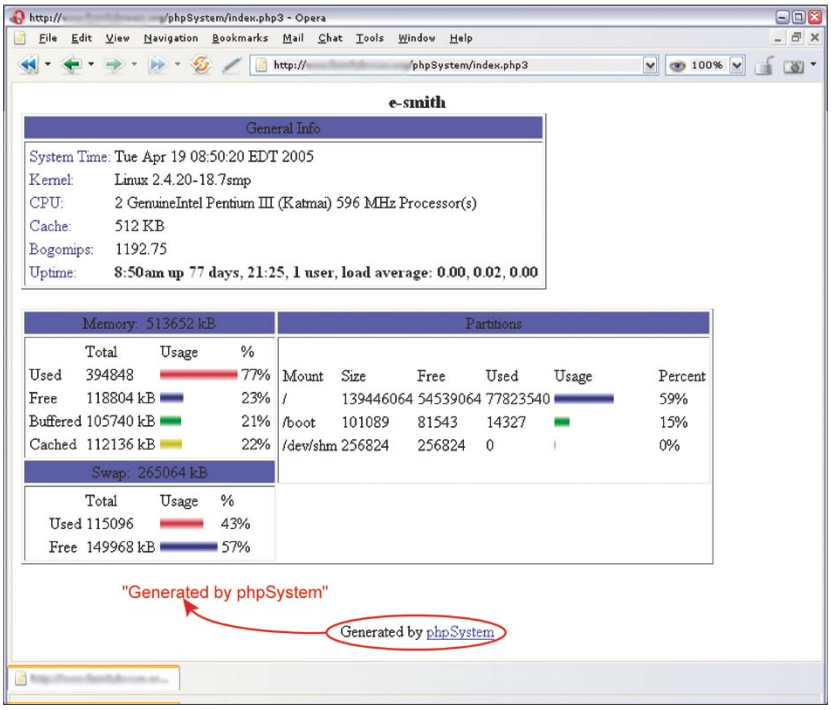


Figure 5. *Statistiques de phpSystem*

rables, l'agresseur potentiel peut poser au moteur de recherche Google l'une des questions suivantes : `intitle:Guestbook "Advanced Guestbook 2.2 Powered"` ou `"Advanced Guestbook 2.2" Username inurl:admin`.

Pour prévenir à une éventuelle attaque, l'administrateur doit être constamment au courant sur les éventuelles failles de sécurité trouvées des logiciels utilisés et appliquer le plus rapidement possible les correctifs de sécurité. La seconde chose qu'il est conseillé de faire est de supprimer les bannières publicitaires, les noms et les numéros des versions des logiciels de toutes les pages ou fichiers sensibles d'en contenir.

Informations sur les réseaux et les systèmes

Presque chaque attaque contre un système informatique est précédée de son étude. En règle générale, cela consiste à scanner les ordinateurs – c'est un essai ayant pour but de définir les services en marche, un type de système d'exploitation utilisé et la version du logiciel utilitaire. Pour cela, on utilise le plus souvent les scanners de type *Nmap* ou *amap* mais il existe encore une option à choisir. Plusieurs administrateurs installent des applications Web générant sans arrêt les statistiques de travail du système, informant sur l'encombrement des disques durs et contenant les listes des processus démarrés et même les journaux système.

Pour un intrus, ce sont des informations très précieuses. Il suffit qu'il demande à Google de trouver les statistiques du logiciel *phpSystem* : `"Generated by phpSystem"` et il obtiendra des pages similaires à la page présentée sur la Figure 5. Il peut également demander d'afficher les pages générées par le script *Sysinfo* : `intitle:"Sysinfo * " intext:"Generated by Sysinfo * written by The Gamblers."` qui contiennent beaucoup plus d'informations sur le système (Figure 6).

Focus

Les possibilités sont ici nombreuses (des questions concernant des statistiques et des informations générées par des logiciels très populaires se trouvent dans le Tableau 4). Le fait d'obtenir des informations de ce type peut encourager l'intrus à réaliser une attaque contre un système trouvé et peut l'aider à choisir les outils ou les exploits appropriés. Donc si vous utilisez des logiciels permettant de surveiller les ressources de votre ordinateur, veillez à ce que l'accès y soit sécurisé et qu'il exige un mot de passe.

À la recherche des erreurs

Les messages d'erreur HTTP peuvent être très précieux pour l'intrus – c'est grâce à ces informations que l'on peut obtenir beaucoup de précisions sur le système, sa configuration et la structure de ses bases de données. À titre d'exemple, pour trouver des erreurs générées par la base *Informix,* il suffit de poser au moteur de recherche la question suivante : `"A syntax error has occurred" filetype:ihtml`. En conséquence, l'intrus trouvera les messages contenant des informations sur la configuration de la base de données, la répartition des fichiers dans le système et parfois les mots de passe (voir la Figure 7). Pour limiter les résultats seulement aux pages contenant les mots de passe, il suffit de modifier un peu la question posée : `"A syntax error has occurred" filetype:ihtml intext:LOGIN`.

Des informations aussi intéressantes peuvent être obtenues à partir des erreurs de la base de

Tableau 4. *Logiciels générant des statistiques de travail du système*

Question	Type d'informations
`"Generated by phpSystem"`	le type et la version du système d'exploitation, la configuration matérielle, les utilisateurs logués, les connexions ouvertes, l'encombrement de la mémoire et des disques durs, les points de montage
`"This summary was generated by wwwstat"`	les statistiques de travail du serveur Web, la répartition des fichiers dans le système
`"These statistics were produced by getstats"`	les statistiques de travail du serveur Web, la répartition des fichiers dans le système
`"This report was generated by WebLog"`	les statistiques de travail du serveur Web, la répartition des fichiers dans le système
`intext:"Tobias Oetiker" "traffic analysis"`	les statistiques de travail du système sous forme de diagrammes MRTG, la configuration du réseau
`intitle:"Apache::Status" (inurl:server-status | inurl:status.html | inurl:apache.html)`	la version du serveur, le type du système d'exploitation, la liste des processus fils et les connexions actuelles
`intitle:"ASP Stats Generator *.*" "ASP Stats Generator" "2003-2004 weppos"`	l'activité du serveur Web, beaucoup d'informations sur les visiteurs
`intitle:"Multimon UPS status page"`	les statistiques de travail des périphériques UPS
`intitle:"statistics of" "advanced web statistics"`	les statistiques de travail du serveur Web, les informations sur les visiteurs
`intitle:"System Statistics" +"System and Network Information Center"`	les statistiques de travail du système sous la forme des diagrammes MRTG, la configuration matérielle, les services en marche
`intitle:"Usage Statistics for" "Generated by Webalizer"`	les statistiques de travail du serveur Web, les informations sur les visiteurs, la répartition des fichiers dans le système
`intitle:"Web Server Statistics for ****"`	les statistiques de travail du serveur Web, les informations sur les visiteurs
`inurl:"/axs/ax-admin.pl" -script`	les statistiques de travail du serveur Web, les informations sur les visiteurs
`inurl:"/cricket/grapher.cgi"`	les diagrammes MRTG concernant le travail des interfaces réseau
`inurl:server-info "Apache Server Information"`	la version et la configuration du serveur Web, le type du système d'exploitation, la répartition des fichiers dans le système
`"Output produced by SysWatch *"`	le type et la version du système d'exploitation, les utilisateurs logués, l'encombrement de la mémoire et des disques durs, les points de montage, les processus démarrés, les journaux système

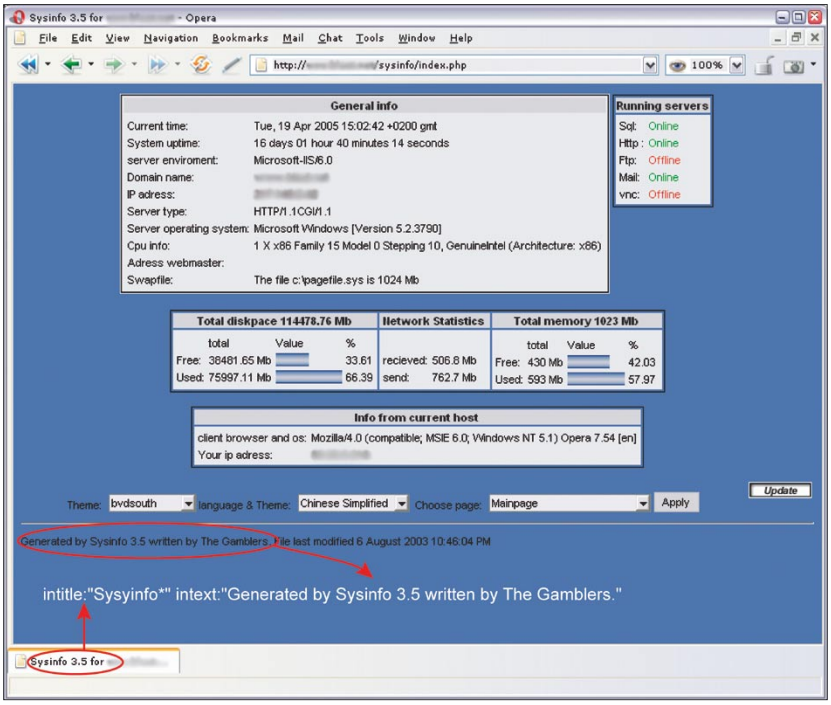


Figure 6. *Statistiques de Sysinfo*

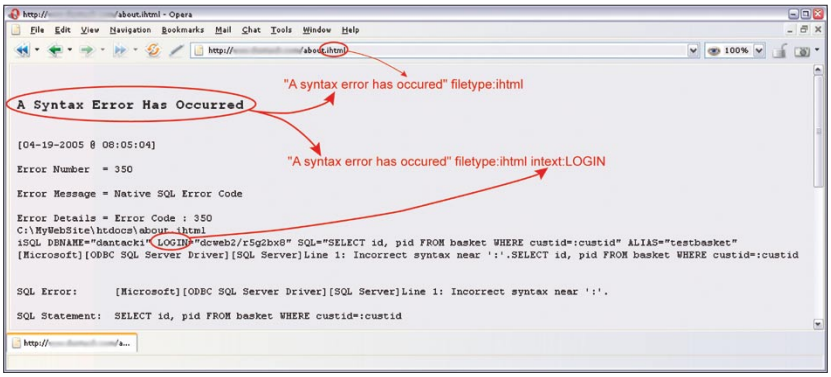


Figure 7. *Utilisation d'erreurs de la base de données Informix*

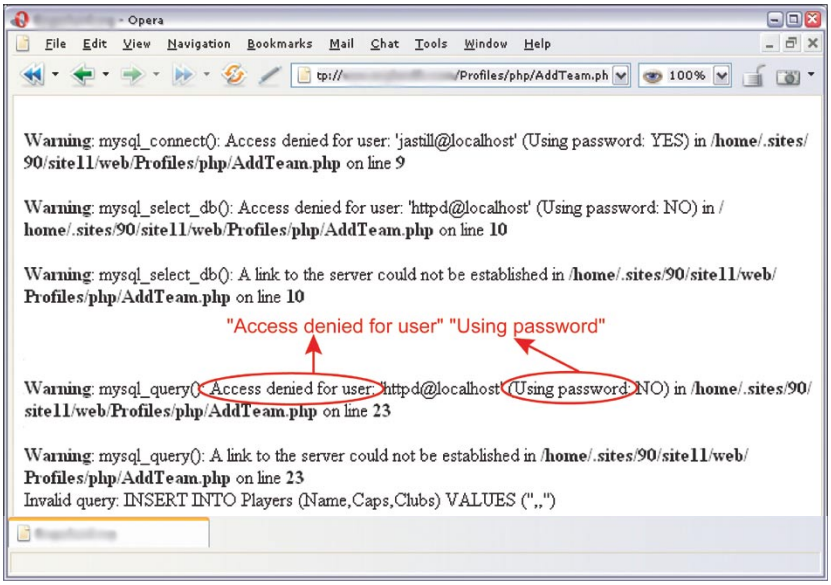


Figure 8. *Erreur de la base MySQL*

données *MySQL*. Cela se voit sur l'exemple de la question `"Access denied for user" "Using password"` – la Figure 8 représente l'une des pages trouvées à l'aide de cette méthode. Pour consulter les autres exemples de questions utilisant des erreurs de ce type, reportez-vous au Tableau 5.

La seule méthode pour protéger vos systèmes contre l'information publique sur les erreurs consiste avant tout à modifier rapidement les configurations standards et si cela est possible, à configurer les logiciels de sorte que les messages d'erreur soient enregistrées dans les fichiers destinés à cette fin et non à les envoyer vers les pages disponibles aux utilisateurs.

N'oubliez pas que même si vous supprimez les erreurs (et que les pages affichées par Google ne seront plus d'actualités par la suite), l'intrus peut voir toujours la copie de la page stockée par le *cache* du moteur de recherche Google. Il suffit qu'il clique sur le lien donné par la liste de résultats pour être conduit vers la copie du site. Heureusement, prenant en compte une grande quantité de ressources Web, les copies sont stockées dans le *cache* durant un temps restreint.

Chercher les mots de passe

Sur le réseau, on peut trouver une multitude de mots de passe destinée à des ressources de tous types – des comptes courrier, des serveurs FTP ou même des comptes shell. Cela est dû notamment au manque de savoir-faire des utilisateurs qui mettent inconsciemment leur mots de passe dans des endroits accessibles au grand public et à la négligence d'éditeurs de logiciels qui, d'une part protègent les données utilisateur de façon inappropriée, et, d'autre part, ne les informent pas sur la nécessité de modifier la configuration standard de leurs produits.

Prenons comme exemple *WS_FTP*, client FTP connu et utilisé fréquemment qui tout comme la plu-

part des logiciels utilitaires permet de mémoriser les mots de passe des comptes. *WS_FTP* enregistre sa configuration et les informations sur les comptes utilisateur dans le fichier *WS_FTP.ini*. Malheureusement, tout le monde ne se rend pas compte du fait que chaque personne qui aura l'accès à la configuration du client FTP pourra accéder en même temps à nos ressources. Il est vrai que les mots de passe stockés dans le fichier *WS_FTP.ini* sont cryptés mais malgré tout, cela ne reste pas suffisant – possédant le fichier de configuration, l'intrus pourra utiliser les outils permettant de déchiffrer les mots de passe ou d'installer tout simplement le logiciel *WS_FTP* et de le démarrer dans votre configuration. Mais comment peut-il accéder aux milliers de fichiers de configuration du client *WS_FTP* ? En utilisant Google bien évidemment. En posant les questions `"Index of/" "Parent Directory" "WS_FTP.ini"` ou `filetype:ini WS_FTP PWD`, il obtiendra

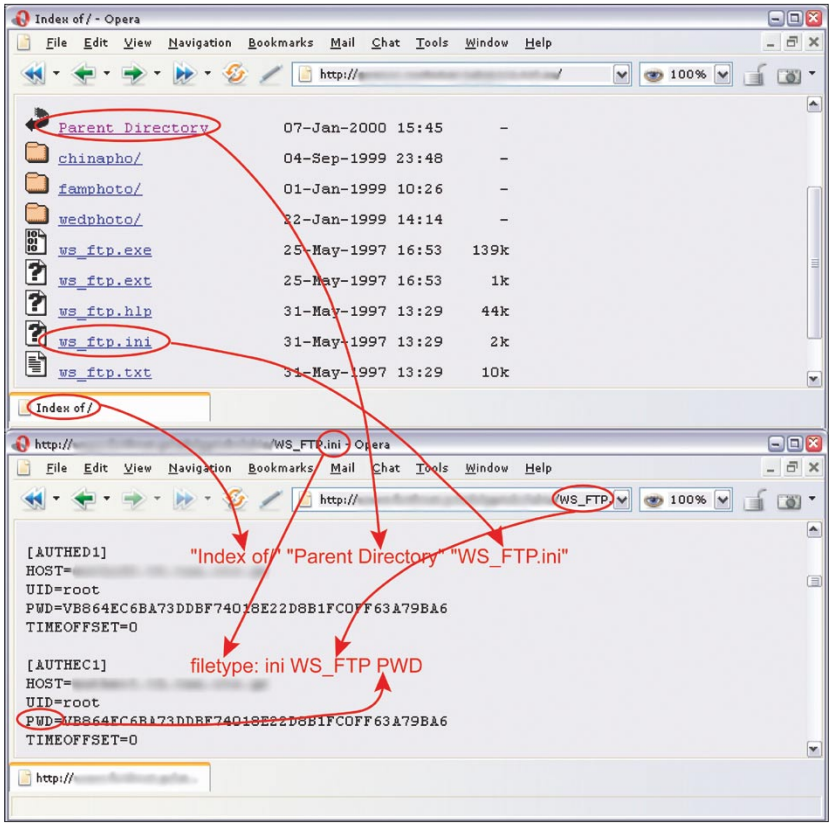


Figure 9. *Fichier de configuration du logiciel WS_FTP*

Tableau 5. *Messages d'erreur*

Question	Résultat
`"A syntax error has occurred" filetype:ihtml`	les messages d'erreur de la base *Informix* – ils peuvent contenir les noms des fonctions ou de fichiers, des informations sur la répartition des fichiers, des fragments du code SQL et des mots de passe
`"Access denied for user" "Using password"`	les erreurs d'authentification – ils peuvent contenir des noms d'utilisateur, des noms des fonctions, des informations sur la répartition de fichiers et de fragments de code SQL
`"The script whose uid is " "is not allowed to access"`	les messages d'erreur PHP liés au contrôle d'accès – ils peuvent contenir des noms de fichiers ou de fonctions et des informations sur la répartition des fichiers
`"ORA-00921: unexpected end of SQL command"`	les messages d'erreur de la base *Oracle* – ils peuvent contenir des noms de fichiers ou de fonctions et des informations sur la répartition des fichiers
`"error found handling the request" cocoon filetype:xml`	les messages d'erreur du logiciel *Cocoon* – ils peuvent contenir le numéro de la version *Cocoon*, des noms de fichiers ou de fonctions et des informations sur la répartition des fichiers
`"Invision Power Board Database Error"`	les messages d'erreur du forum de discussion *Invision Power Board* – ils peuvent contenir des noms de fonctions et de fichiers, des informations sur la répartition de fichiers dans le système et des fragments du code SQL
`"Warning: mysql_query()" "invalid query"`	les messages d'erreur de la base *MySQL* – ils peuvent contenir des noms d'utilisateur, des noms de fonctions des fichiers et des informations sur la répartition des fichiers
`"Error Message : Error loading required libraries."`	les messages d'erreur des scripts CGI – ils peuvent contenir des informations sur le type du système d'exploitation et la version du logiciel, des noms d'utilisateur, des noms de fichiers et des informations sur la répartition de fichiers dans le système
`"#mysql dump" filetype:sql`	les messages d'erreur de la base *MySQL* – ils peuvent contenir des informations sur la structure et le contenu de la base de données

plusieurs liens vers les données qui l'intéressent (Figure 9).

L'application Web nommée *DUclassified* permettant d'ajouter et de gérer les publicités dans les services Internet est un autre exemple. Dans la configuration standard, les noms d'utilisateur, les mots de passe et les autres données sont stockés dans le fichier *duclassified.mdb* situé dans un sous-répertoire *_private* non sécurisé contre la lecture. Il suffit alors de trouver un service utilisant *DUclassifield* avec une adresse *http://<host>/*

Tableau 6. *Mots de passe – exemples de questions dans Google*

Question	Résultat
`"http://*:*@www" site`	les mots de passe pour la page « site » enregistrés comme « `http://username:password@www...` »
`filetype:bak inurl:"htaccess|passwd|shadow|htusers"`	les copies de sauvegarde de fichiers pouvant contenir des informations sur des noms d'utilisateurs et des mots de passe
`filetype:mdb inurl:"account|users|admin|administrators|passwd|password"`	les fichiers de type *mdb* qui peuvent contenir des informations sur les mots de passe
`intitle:"Index of" pwd.db`	les fichiers *pwd.db* peuvent contenir des noms d'utilisateurs et des mots de passe cryptés
`inurl:admin inurl:backup intitle:index.of`	les répertoires nommés *admin* et *backup*
`"Index of/" "Parent Directory" "WS_FTP.ini" filetype:ini WS_FTP PWD`	les fichiers de configuration du logiciel *WS_FTP* pouvant contenir des mots de passe pour des serveurs FTP
`ext:pwd inurl:(service|authors|administrators|users) "# -FrontPage-"`	des fichiers contenant des mots de passe du logiciel *Microsoft FrontPage*
`filetype:sql ("passwd values ****" | "password values ****" | "pass values ****" )`	des fichiers contenant des codes SQL et des mots de passe ajoutés à la base de données
`intitle:index.of trillian.ini`	des fichiers de configuration du logiciel de messagerie instantanée *Trillian*
`eggdrop filetype:user user`	des fichiers de configuration de l'ircbot *Eggdrop*
`filetype:conf slapd.conf`	des fichiers de configuration de l'application *OpenLDAP*
`inurl:"wvdial.conf" intext:"password"`	des fichiers de configuration du logiciel *WV Dial*
`ext:ini eudora.ini`	des fichiers de configuration du logiciel de messagerie électronique *Eudora*
`filetype:mdb inurl:users.mdb`	des fichiers *Microsoft Access* pouvant contenir des informations sur des comptes
`intext:"powered by Web Wiz Journal"`	des services Web utilisant l'application *Web Wiz Journal* permettant dans la configuration standard de télécharger un fichier contenant les mots de passe ; au lieu de l'adresse par défaut *http://<host>/journal/*, il faut taper *http://<host>/journal/journal.mdb*
`"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`	des services Web utilisant les applications *DUclassified*, *DUcalendar*, *DUdirectory*, *DUclassmate*, *DUdownload*, *DUpaypal*, *DUforum* ou *DUpics* qui, dans la configuration standard, permettent de télécharger un fichier contenant les mots de passe ; au lieu de l'adresse par défaut (pour *DUclassified*) *http://<host>/duClassified/*, il faut taper *http://<host>/duClassified/_private/duclassified.mdb*
`intext:"BiTBOARD v2.0" "BiTSHiFTERS Bulletin Board"`	des services Web utilisant l'application *Bitboard2* permettant, dans la configuration standard, de télécharger un fichier contenant les mots de passe ; au lieu de l'adresse par défaut *http://<host>/forum/forum.php*, il faut taper *http://<host>/forum/admin/data_passwd.dat*

Focus

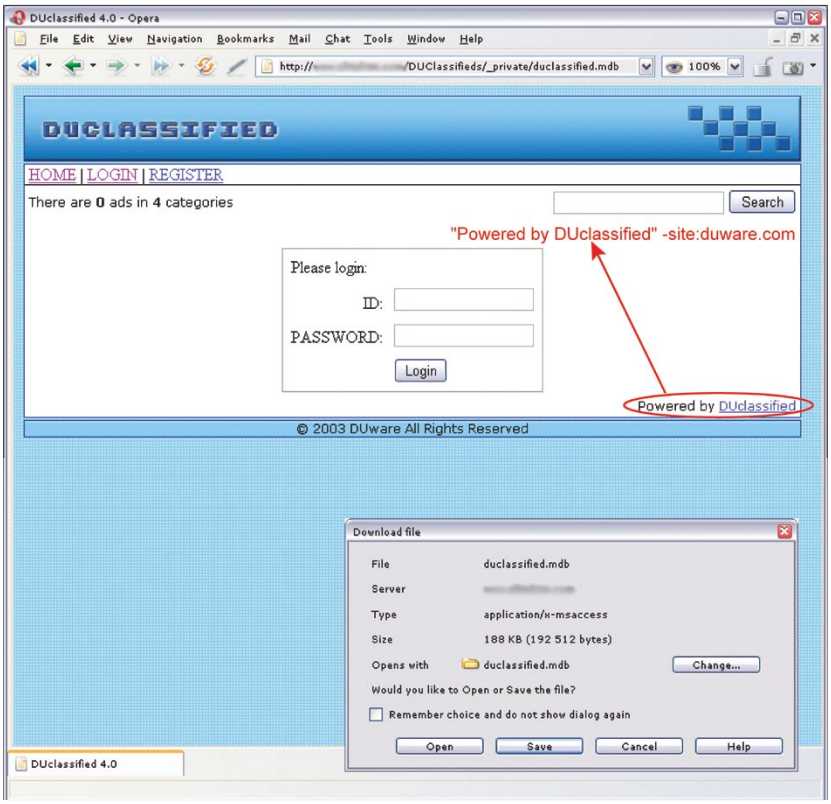
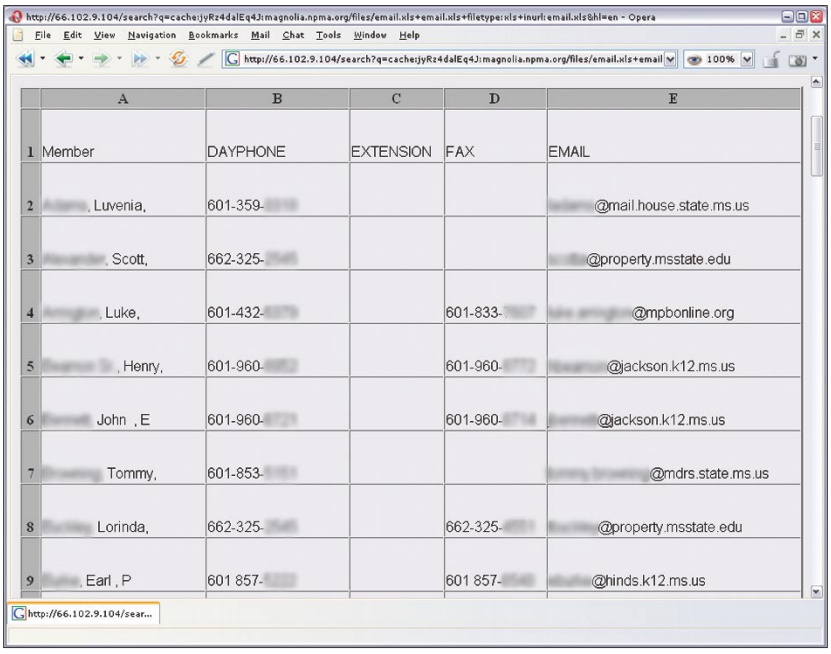


Figure 10. *Logiciel DUclassified dans la configuration standard*



	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

Figure 11. *Carnet d'adresses électronique obtenu grâce à Google*

Sur Internet

- *http://johnny.ihackstuff.com* – l'archive d'informations sur *Google hacking* la plus importante,
- *http://insecure.org/nmap/* – le scanner réseau *Nmap*,
- *http://thc.org/thc-amap/* – le scanner *amap*.

duClassified/ et de la remplacer par *http://<host>/duClassified/_private/duclassified.mdb* pour obtenir un fichier avec les mots de passe et, par conséquent, un accès illimité à l'application (voir la Figure 10). Pour trouver les sites utilisant l'application décrite, essayez de taper la question suivante dans Google : `"Powered by DUclassified" -site:duware.com` (pour éviter les résultats concernant le site de l'éditeur). Ce qui est intéressant c'est que l'éditeur *DUclassified* – la société DUware – a créé d'autres applications vulnérables à ce type d'opérations.

En théorie, tout le monde sait qu'il ne faut pas coller les mots de passe sur le moniteur ou les cacher sous le clavier. Cependant, beaucoup d'utilisateurs enregistrent leurs mots de passe dans des fichiers à l'intérieur de leurs dossiers personnels étant eux-mêmes, contrairement aux attentes, disponibles depuis Internet. En outre, beaucoup d'entre sont des administrateurs réseaux et c'est pourquoi, ces fichiers sont d'une importance capitale. Difficile de trouver une règle pour rechercher ce type de données mais les combinaisons de mots du type : *account*, *users*, *admin*, *administrators*, *passwd*, *password* etc. peuvent apporter de bons résultats notamment pour les types de fichiers suivant :*.xls*, *.txt*, *.doc*, *.mdb* et *.pdf*. Il est également conseillé de s'intéresser aux répertoires nommés avec les mots *admin*, *backup* ou d'autres mots similaires : `inurl:admin intitle:index.of`. Pour voir des questions concernant les mots de passe, reportez-vous au Tableau 6.

Pour rendre aux intrus l'accès à vos mots de passe plus difficile, vous devez tout d'abord penser où et pourquoi vous les tapez, comment ils sont stockés et comment ils sont utilisés. Si vous surveillez un service Internet, vous devez analyser la configuration des applications utilisées, trouver les données exposées au danger ou mal protégées et les sécuriser de façon appropriée.

Tableau 7. *Recherche des données personnelles et des documents confidentiels*

Question	Résultat
`filetype:xls inurl:"email.xls"`	des fichiers *email.xls* pouvant contenir des adresses
`"phone * * *" "address *" "e-mail" intitle:"curriculum vitae"`	des documents CV
`"not for distribution" confidential`	des documents avec la clause *confidential*
`buddylist.blt`	des listes de contacts du logiciel de messagerie instantanée *AIM*
`intitle:index.of mystuff.xml`	des listes de contacts du logiciel de messagerie instantanée *Trillian*
`filetype:ctt "msn"`	des listes de contacts *MSN*
`filetype:QDF QDF`	la base de données du logiciel financier *Quicken*
`intitle:index.of finances.xls`	des fichiers *finances.xls* pouvant contenir des informations sur des comptes bancaires, des rapports financiers et des numéros de cartes de crédit
`intitle:"Index Of" -inurl:maillog maillog size`	des fichiers *maillog* pouvant contenir des messages e-mail
`"Network Vulnerability Assessment Report" "Host Vulnerability Summary Report" filetype:pdf "Assessment Report" "This file was generated by Nessus"`	des rapports sur l'étude de la sécurité des réseaux, des tests de pénétration, etc.

Tableau 8. *Séquences caractéristiques pour les périphériques réseaux*

Question	Périphérique
`"Copyright (c) Tektronix, Inc." "printer status"`	les imprimantes PhaserLink
`inurl:"printer/main.html" intext:"settings"`	les imprimantes Brother HL
`intitle:"Dell Laser Printer" ews`	les imprimantes Della basées sur la technologie EWS
`intext:centreware inurl:status`	les imprimantes Xerox Phaser 4500/6250/8200/8400
`inurl:hp/device/this.LCDispatcher`	les imprimantes HP
`intitle:liveapplet inurl:LvAppl`	les caméras Canon Webview
`intitle:"EvoCam" inurl:"webcam.html"`	les caméras Evocam
`inurl:"ViewerFrame?Mode="`	les caméras Panasonic Network Camera
`(intext:"MOBOTIX M1" | intext:"MOBOTIX M10") intext: "Open Menu" Shift-Reload`	les caméras Mobotix
`inurl:indexFrame.shtml Axis`	les caméras Axis
`SNC-RZ30 HOME`	les caméras Sony SNC-RZ30
`intitle:"my webcamXP server!" inurl:":8080"`	les caméras disponibles via l'application *WebcamXP Server*
`allintitle:Brains, Corp. camera`	les caméras disponibles via l'application *mmEye*
`intitle:"active webcam page"`	les caméras dotées de l'interface USB

Données personnelles et documents confidentiels

Aussi bien que dans les pays faisant parti de l'Union Européenne qu'aux États-Unis, il existe des régulations juridiques ayant pour but de protéger la confidentialité des utilisateurs. Malheureusement, il arrive que les différents documents confidentiels contenant vos données soient mis dans des endroits accessibles au grand public ou envoyés via le réseau sans être pour autant sécurisés. Il suffit donc que l'intrus obtienne l'accès au courrier électronique contenant votre Curriculum Vitae envoyé pour la recherche d'un emploi pour qu'il connaisse votre adresse, votre numéro de téléphone, votre date de naissance, votre niveau d'étude, vos centres d'intérêts et votre expérience professionnelle.

Sur le réseau, il y a plein de documents de ce type. Pour les

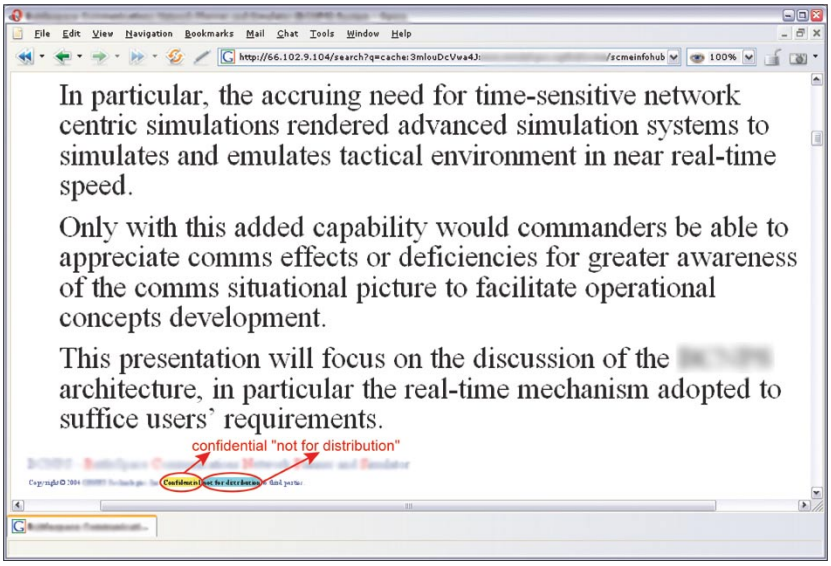


Figure 12. *Un document confidentiel trouvé par le moteur de recherche*

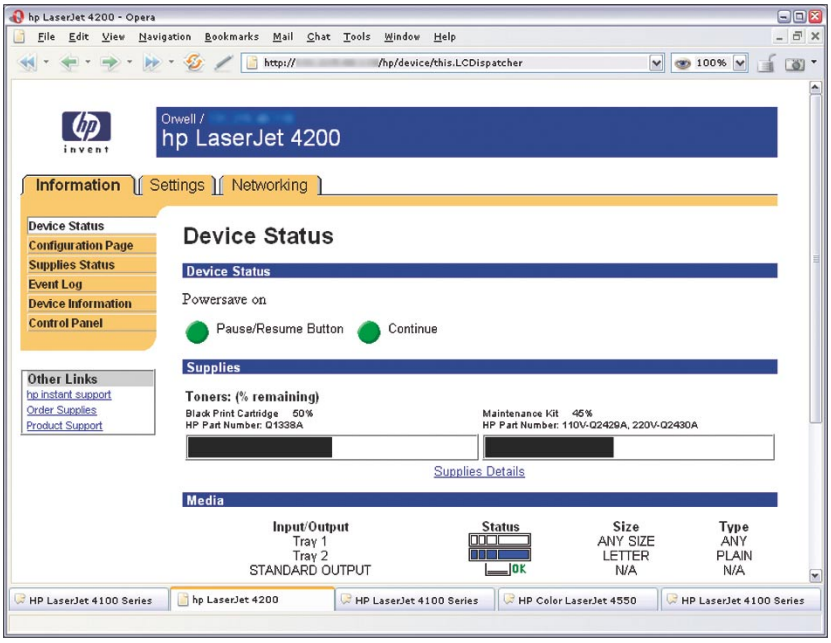


Figure 13. *Page de configuration de l'imprimante HP trouvée par Google*

trouver, il faut poser la question suivante : `intitle:"curriculum vitae" "phone * * *" "address *" "e-mail"`. Il est également facile de trouver des adresses sous forme de listes de noms, de numéros de téléphones et d'adresses e-mail (Figure 11). Cela résulte du fait que presque tous les utilisateurs d'Internet créent différents types de carnets d'adresses électroniques – ceux-ci sont peu importants pour un intrus moyen mais un manipulateur habile (*social engineering*) sera capable d'utiliser au mieux ces données, notamment si celles-ci concernent les contacts dans le cadre d'une société. Dans ce cas, il est conseillé de taper la question : `filetype:xls inurl:"email.xls"` permettant de trouver des feuilles de calcul nommées *email.xls*.

La même situation concerne les logiciels de messagerie instantanée et les listes de contacts enregistrées. Quand une liste de ce type tombe entre les mains d'un intrus, celui-ci pourra essayer de se faire passer pour vos amis. Ce qui est intéressant, c'est qu'un grand nombre de données personnelles se trouvent dans des documents officiels – des rapports de la police, des notes judiciaires ou même dans des cartes de maladie.

Sur Internet, il y a également des documents privés possédant une clause de confidentialité. Ce sont des plans de projets, des documentations techniques, de différentes enquêtes, rapports, présentations et beaucoup d'autres documents à utilisation interne. Il est facile de les trouver car ils contiennent souvent le mot *confidential*, la phrase *Not for distribution,* etc. (voir la Figure 12). Le Tableau 7 comprend quelques questions concernant ces documents souvent privés ou confidentiels.

Tout comme dans le cas des mots de passe, pour éviter la divulgation au public d'informations privées, il faut rester prudent et surveiller les données publiées. Les sociétés et les institutions doivent élaborer et mettre en œuvre des réglementations appropriées, des procédures, des principes de sécurité et préparer son personnel pour faire face à ce problème.

Périphériques réseaux

Plusieurs administrateurs ne prennent pas au sérieux la sécurité des périphériques tels que les imprimantes réseaux ou les caméras Web. Pourtant, une imprimante mal sécurisée peut devenir la première cible à attaquer par l'intrus qu'il utilisera ensuite pour réaliser des attaques contre d'autres systèmes sur le réseau. Les caméras Internet ne sont pas très dangereuses et peuvent être considérées comme un divertissement mais il n'est pas difficile d'imaginer la situation où les données de ce type auraient de l'importance (une espièglerie industrielle, un vol à main armée). Les questions sur les imprimantes et les caméras se trouvent dans le Tableau 8 et la Figure 13 représente la page de configuration de l'imprimante trouvée sur le réseau. ■