hakin9

Nebezpečný Google – vyhledávání důvěrných

Michał Piotrowski

Časopis *hakin9*, Software Wydawnictwo,
ul. Piaskowa 3, 01-067 Warszawa, *hakin9@hakin9.org*

Nebezpečný Google – vyhledávání důvěrných informací

Michał Piotrowski

Informace, které by měly být chráněny, jsou velmi často dostupné veřejně. Zpřístupňují je nevědomky, buď z nedbalosti nebo z neznalosti, sami uživatelé. Výsledek je ten, že důvěrná data jsou na dosah ruky, na Internetu. Stačí jen použít Google.

Google vyřizuje kolem 80 procent všech dotazů na Internetu a proto je nejčastěji a nejvíce používaným vyhledávačem. Vděčí za to nejenom výjimečnému mechanismu generování výsledků, ale také velmi pokročilým možnostem zadávání dotazů. Je však také nutné pamatovat na to, že Internet je velmi dynamické médium, díky čemu nejsou výsledky zobrazované Googlem vždy aktuální. Stává se, že některé nalezené strany jsou velmi neaktuální a zároveň mnoho podobných ještě nebylo navštívených Googlebotem (automatický skript procházející a indexující WWW stránky).

Nejdůležitější a nejpotřebnější výběrové operátory, spolu s popisem a výsledkem jejich použití jsou představeny v Tabulce 1, zatímco místa v dokumentech, na které se operátory odkazují při prohledávání síťových zdrojů (na příkladu strany magazínu *hakin9*), ukazuje Obrázek 1. Jsou to pouze příklady – šikovné zadávání dotazů do Googlu umožňuje získání mnohem zajímavějších informací.

Hledáme oběť

Díky vyhledávači Google můžeme najít nejenom obecné internetové zdroje, ale také ty,

Z tohoto článku se naučíte...

- jak s použitím Google hledat privátní databáze a jiné důvěrné informace,
- jak nalézt informace o napadnutelných systémech a síťových službách,
- jak v Google nalézt veřejně dostupná síťová zařízení.

Měl byste vědět...

- umět používat internetový prohlížeč,
- mít základní znalosti o HTTP protokolu.

O autorovi

Michał Piotrowski je magistr informatiky. Má mnohaleté zkušenosti s prací na pozici správce sítě a systémů. Již tři roky pracuje jako manažer bezpečnosti. Momentálně jako manažer bezpečnosti telekomunikačních sítí v jedné z největších finančních institucí v Polsku. Ve volném čase programuje a zabývá se kryptografií, jeho vášní jsou Open Source projekty.

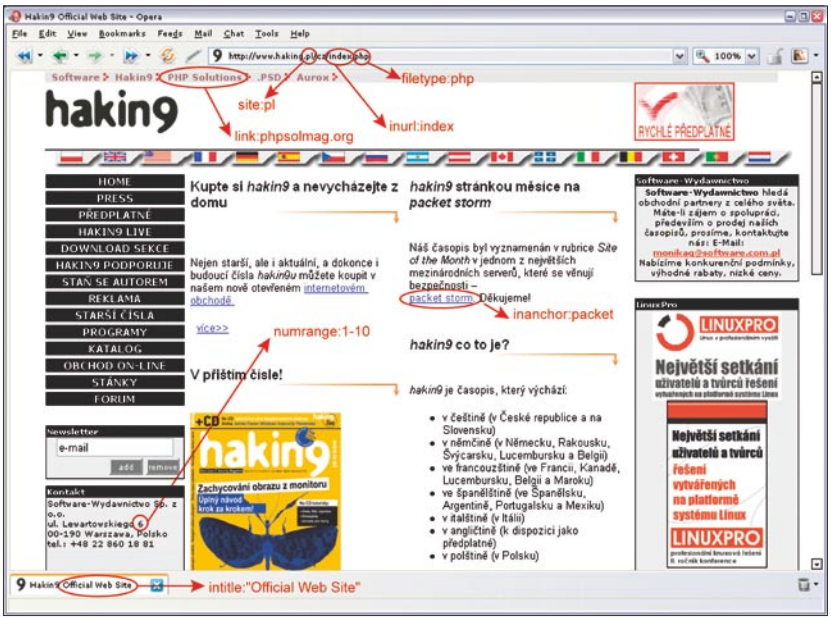
Tabulka 1. *Výběrové operátory Google*

Operátor	Určení	Příklad použití
`site`	omezuje výsledek na strany nacházející se v zadané doméně	`site:google.com fox` najde všechny strany obsahující v textu výraz *fox*, které se nacházejí v doméně **.google.com*
`intitle`	omezuje výsledky na dokumenty obsahující zadaný výraz ve jméně	`intitle:fox fire` najde všechny strany obsahující výraz *fox* ve jméně a *fire* v textu
`allintitle`	omezuje výsledky na dokumenty obsahující všechny zadané řetězce v titulku	`allintitle:fox fire` najde všechny strany obsahující v titulku výrazy *fox* a *fire*; funguje podobně jako `intitle:fox intitle:fire`
`inurl`	omezuje výsledky na strany obsahující zadaný řetězec v URL adrese	`inurl:fox fire` najde strany obsahující v textu výraz *fire* a *fox* v URL adrese
`allinurl`	omezuje výsledky na strany obsahující všechny zadané výrazy v URL adrese	`allinurl:fox fire` najde strany obsahující v URL adrese výrazy *fox* a *fire*; funguje podobně jako `inurl:fox inurl:fire`
`filetype, ext`	omezuje výsledky na dokumenty zadaného typu	`filetype:pdf fire` vrátí dokumenty PDF obsahující výraz *fire* a `filetype:xls fox` vrátí dokumenty tabulkového kalkulátoru *Excel* obsahující *fox*
`numrange`	omezí výsledky na dokumenty obsahující ve svém obsahu číslo ze zadaného rozsahu	`numrange:1-100 fire` vrátí strany obsahující hodnotu z rozsahu od 1 do 100 a výraz *fire*. Stejný efekt je možno získat dotazem: `1..100 fire`
`link`	omezí výsledky na strany obsahující odkazy na zadané umístění	`link:www.google.com` vrátí dokumenty obsahující nejméně jeden odkaz na stranu *www.google.com*
`inanchor`	omezí výsledky na strany s odkazy obsahující v popise zadaný výraz	`inanchor:fire` vrátí dokumenty obsahující odkazy, které mají v popisu výraz *fire* (ne v URL adrese, na kterou odkazují, ale v podtržené části textu)
`allintext`	omezí výsledky na dokumenty obsahující zadaný výraz v textu a současně neobsahující jej v popise, odkazech a URL adrese	`allintext:"fire fox"` vrátí dokumenty, které obsahují výraz *fire fox* pouze v textu
`+`	vynutí častý výskyt zadaného výrazu ve výsledcích	`+fire` třídí výsledky dle počtu výskytů výrazu *fire*
`-`	vynutí nevyskytování se zadaného výrazu ve výsledcích	`-fire` vrátí dokumenty neobsahující výraz *fire*
`""`	umožňuje hledat celé fráze, nejenom výrazy	`"fire fox"` vrátí dokumenty obsahující frázi *fire fox*
`.`	je zástupcem jednoho znaku	`fire.fox` vrátí dokumenty obsahující fráze *fire fox*, *fire-fox*, *fire1fox*, *fire-fox* apod.
`*`	je zástupcem libovolného výrazu	`fire * fox` vrátí dokumenty obsahující frázi *fire the fox*, *fire in fox*, *fire or fox* apod.
`|`	logické OR	`"fire fox" | firefox` vrátí dokumenty obsahující frázi *fire fox* nebo výraz *firefox*

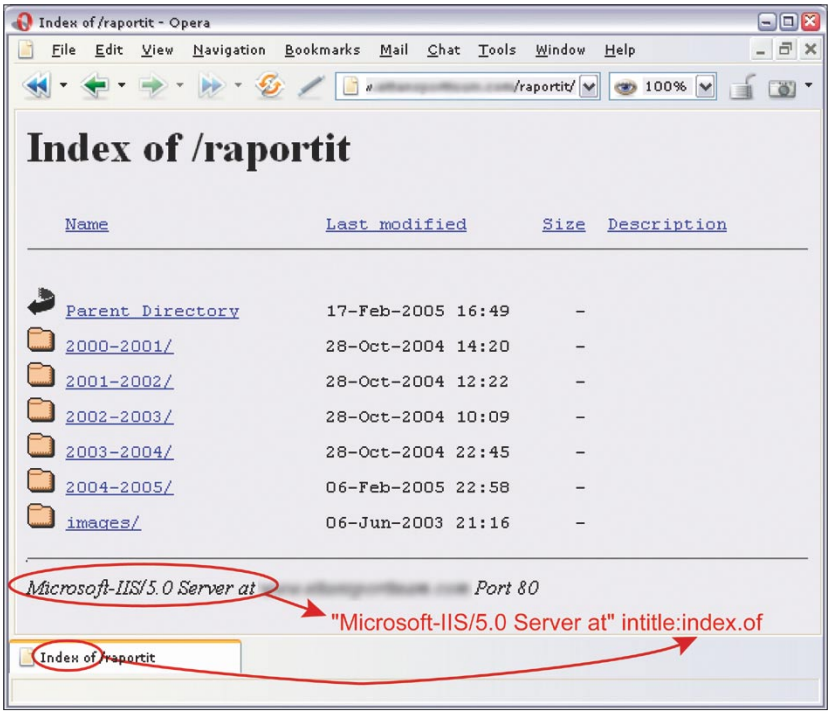
které by neměly být nikdy zobrazeny. Pokud zadáme příslušný dotaz, často dostaneme velmi udivující výsledky. Začněme něčím jednoduchým.

Představme si, že v nějakém běžně používaném programu bude nalezena bezpečnostní díra. Předpokládejme, že se týká serveru *Microsoft IIS* ve verzi 5.0 a že hypotetický útočník chce najít několik počítačů s tímto programem, aby na ně zaútočil. Samozřejmě, že by k tomuto účelu mohl použít nějaký skener, rozhodl se však využít Google, zadá proto následující dotaz: `"Microsoft-IIS/5.0 Server at" intitle:index.of` a ve výsledku dostane odkazy na hledané servery a konkrétně k zobrazeným obsahům adresářů nacházejících se na těchto serverech. Děje se to proto, protože ve standardní konfiguraci *IIS* (a v mnoha jiných) přidává do některých dynamicky generovaných stran bannery obsahující svoje jméno a verzi (je to vidět na Obrázku 2).

Je to příklad informace, která sama o sobě není nebezpečná, z toho důvodu je často ignorována a ve standardní konfiguraci ponechávána. Bohužel je to také informace, která



Obrázek 1. *Použití operátorů ve vyhledávání na příkladu stránek magazínu hakin9*



Obrázek 2. *Našel jsem server IIS 5.0 s použitím operátoru intitle*

může mít za jistých okolností pro útočníka velký význam. Více ukázkových dotazů pro Google na jiné typy serverů obsahuje Tabulka 2.

Jiným způsobem nalezení konkrétní verze WWW serverů je hledání standardních stran, které jsou s nimi distribuovány a dostupné po správné instalaci. Může se to zdát divné, ale na Internetu se nachází množství serverů, jejichž výchozí obsah nebyl po instalaci změněn. Velmi často jsou to slabě zabezpečené, zapomenuté počítače znamenající pro průnikáře snadný cíl. Je možno je najít s použitím dotazů ukázaných v Tabulce 3.

Tato metoda je velmi jednoduchá a zároveň užitečná. S její pomocí je možno získat přístup k ohromnému množství různých síťových služeb nebo operačních systémů používající aplikace, ve kterých byly nalezeny chyby a jež leniví nebo nedůslední správci neodstranili. Za příklad ať nám poslouží dva velmi populární programy : *WebJeff Filemanager* a *Advanced Guestbook*.

První z nich je webový správce souborů umožňující posílání souborů na server a vytváření, prohlížení, mazání a úpravu souborů nacházejících se na serveru. Bohužel, *WebJeff Filemanager* obsahuje ve verzi 1.6 chybu, která umožňuje načtení obsahu libovolného souboru nacházejícího se na serveru, ke kterému má přístup uživatel spouštějící WWW démona. Stačí proto, aby útočník v nezabezpečeném systému napsal adresu */index.php3?action=telecharger&fichier=/etc/passwd* a získá obsah souboru */etc/passwd* (viz Obrázek 3). Samozřejmě, aby útočník nalezl napadnutelné servery, zadá dotaz : `"WebJeff-Filemanager 1.6" Login`.

Druhá aplikace – *Advanced Guestbook* – je v jazyce PHP napsaným programem používajícím SQL databázi, která umožňuje přidávání knihy návštěvníků pro WWW služby. V dubnu 2004 byla zveřejněna informace o bezpečnostním problému týkajícím se verze 2.2 tohoto programu, která umožňuje (díky vstříknutí SQL – viz článek *SQL Injection útoky na PHP a MySQL* v *hakin9* 3/2005) získání přístupu do administrátorského panelu. Stačí nalézt přihlašovací stránku do panelu (viz Obrázek 4) a přihlásit se s ponechaným prázdným polem *username* a v poli *password* zadaným `') OR ('a' = 'a`, nebo naopak, pole *password* ponechat prázdné a do pole *username* zadat `? or 1=1 --`. Náš ukázkový útočník, aby našel napadnutelné systémy na Internetu, může zadat do vyhledávače Google jeden z následujících dotazů: `intitle:Guestbook "Advanced Guestbook 2.2 Powered"` nebo `"Advanced Guestbook 2.2" Username inurl:admin`.

Abychom zabránili popisovanému úniku dat, musí správce průběžně sledovat informace o všech

Tabulka 2. *Google – dotazy na různé typy WWW serverů*

Dotaz	Server
`"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`	libovolná verze *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`	libovolná verze *Microsoft Internet Information Services*
`"Oracle HTTP Server/* Server at" intitle:index.of`	libovolná verze serveru *Oracle*
`"IBM _ HTTP _ Server/* * Server at" intitle:index.of`	libovolná verze serveru *IBM*
`"Netscape/* Server at" intitle:index.of`	libovolná verze serveru *Netscape*
`"Red Hat Secure/*" intitle:index.of`	libovolná verze serveru *Red Hat Secure*
`"HP Apache-based Web Server/*" intitle:index.of`	libovolná verze serveru *HP*

programech, které používá v jím spravovaných službách a provádět aktualizaci v případě vyskytnutí se chyby v kterémkoliv z nich. Druhou věcí, o kterou se musíme postarat, je odstranění bannerů, jmen a čísel verzí programů ze všech stran nebo souborů, ve kterých se objevují.

Informace o sítích a systémech

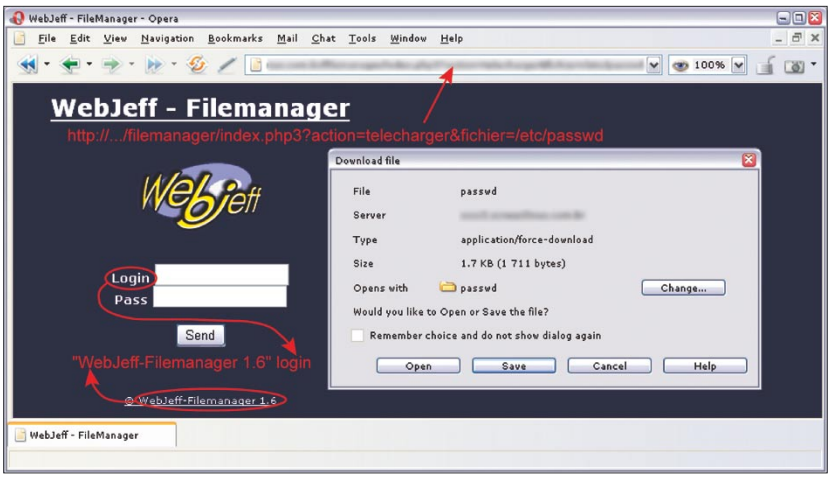
Každému útoku na počítačový systém předchází rozpoznání cíle. Obvykle to spočívá ve skenování počítačů, otestování fungujících služeb, typu operačního systému a verzi služeb programu. Nejčastěji se k tomu používají skenery typu *Nmap* nebo *amap*, ale existuje ještě jedna možnost. Mnoho správců instaluje WWW servery, které za běhu generují statistiky o práci systému, informují o obsazení pevných disků, obsahují seznamy spuštěných procesů nebo i systémové logy.

Pro útočníka jsou to velmi cenné informace. Stačí, pokud se Googlu zeptá na statistiky programu *phpSystem*: `"Generated by phpSystem"` a dostane strany podobné té ukázané na Obrázku 5. Může se také dotázat na strany generované skriptem *Sysinfo*: `intitle:"Sysinfo * " intext:"Generated by Sysinfo * written by The Gamblers."`; které obsahují mnohem více podrobností o systému (Obrázek 6).

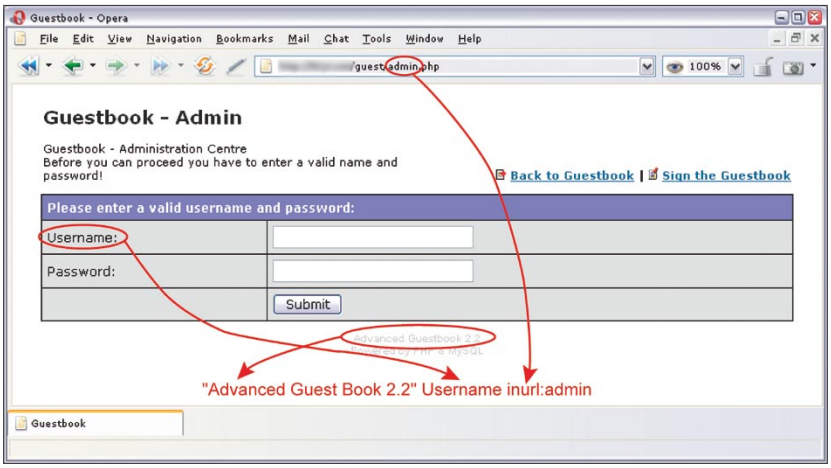
Možností je mnoho (příklady dotazů na statistiky a informace vytvářené nejpopulárnějšími programy obsahuje Tabulka 4). Získání tohoto typu informací může přinutit útočníka k provedení útoku na nalezený systém a pomoci mu s použitím příslušných nástrojů nebo exploitů. Proto se, pokud používáme programy umožňující monitorování zdrojů našich počítačů, musíme postarat

Tabulka 3. *Dotazy na standardní poinstalační strany WWW serverů*

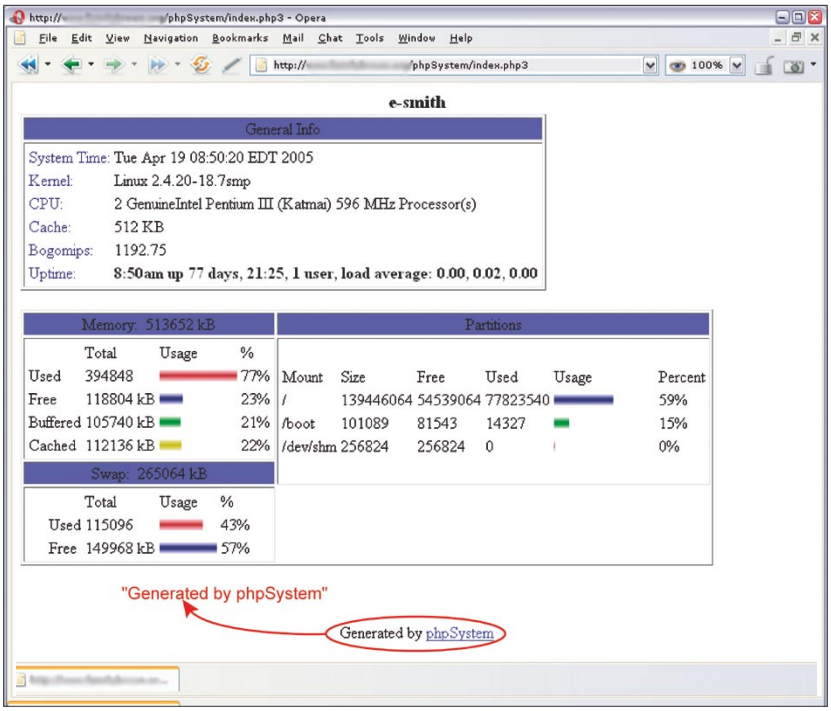
Dotaz	Server
`intitle:"Test Page for Apache Installation" "You are free"`	*Apache* 1.2.6
`intitle:"Test Page for Apache Installation" "It worked!" "this Web site!"`	*Apache* 1.3.0–1.3.9
`intitle:"Test Page for Apache Installation" "Seeing this instead"`	*Apache* 1.3.11–1.3.33, 2.0
`intitle:"Test Page 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* v systému Red Hat
`intitle:"Test Page for the Apache Http Server on Fedora Core"`	*Apache* v systému Fedora
`intitle:"Welcome to Your New Home Page!" Debian`	*Apache* v systému 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



Obrázek 3. *Napadnutelná verze programu WebJeff Filemanager*



Obrázek 4. *Advanced Guestbook – přihlašovací stránka*



Obrázek 5. *Statistiky phpSystem*

o to, aby přístup k nim byl chráněný a vyžadoval zadání hesla.

Hledáme chyby

Hlášení o HTTP chybách mohou být pro útočníky nesmírně cenné – právě z těchto informací je možno získat množství dat o systému a konfiguraci a struktuře databáze. Například abychom našli chyby generované databází *Informix* stačí zadat do vyhledávače následující dotaz: `"A syntax error has occurred" filetype:ihtml`. Ve výsledku útočník dostane hlášení obsahující informace o konfiguraci databáze, umístění souborů v systému a někdy také hesla (viz Obrázek 7). Abychom výsledky omezili jenom na strany obsahující hesla, můžeme trochu poupravit dotaz: `"A syntax error has occurred" filetype:ihtml intext:LOGIN`.

Zajímavé informace je možno získat z chyb databáze *MySQL*. Vidět je to třeba i na příkladě dotazu `"Access denied for user" "Using password"` – Obrázek 8 ukazuje jednu ze stran nalezených tímto způsobem. Jiné ukázkové dotazy využívající tyto chyby se nacházejí v Tabulce 5.

Jediným způsobem ochrany našich systémů před veřejným informováním o chybách je především rychlé odstraňování chyb a pokud tuto možnost máme, nastavení programu tak, aby byly informace o chybách zapisovány do pro tento účel speciálně určených souborů a neposílány na strany dostupné uživatelům.

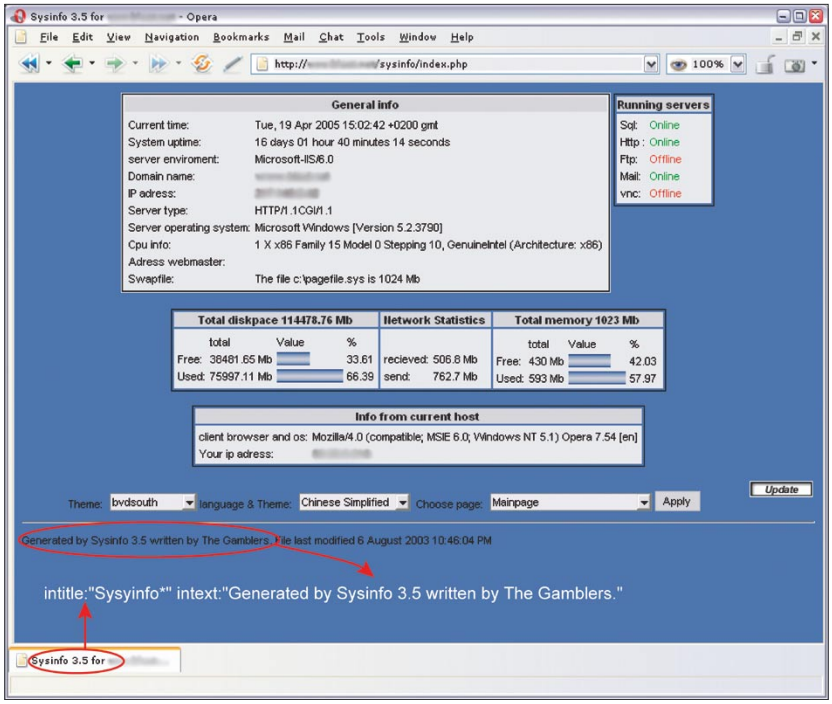
Je nutné při tom pamatovat na to, že i když budeme chyby odstraňovat velmi rychle (a tím vlastně způsobovat, že strany zobrazované Googlem budou již neaktuální), bude si moci útočník prohlédnout kopii strany uchovávanou v *cache* vyhledávače Google. Stačí, že v seznamu s výsledky klikne na odkaz kopie stránek. Naštěstí jsou, vzhledem k velkému množství internetových zdrojů, kopie uchovávané v *cache* pouze krátkou dobu.

Hledáme hesla

Na síti je možno najít množství hesel k různým službám – poštovních účtů, FTP serverů nebo dokonce i k shell

účtům. Vyplývá to hlavně z neznalosti uživatelů, kteří nezodpovědně umisťují hesla na veřejně přístupná místa, ale také z nedbalosti vývojářů programů, kteří buď nedostatečně chrání data uživatelů či je neinformují o nutnosti změny standardních nastavení svých produktů.

Vezměme si za příklad *WS_FTP*, hodně známý a všeobecně používaný FTP klient, který stejně jako většina uživatelských programů umožňuje zapamatovat si hesla pro účty. *WS_FTP* svou konfiguraci a informace o uživatelských účtech ukládá do souboru *WS_FTP.ini*. Bohužel ne všichni si uvědomujeme, že každý, kdo získá přístup ke konfiguraci FTP klienta bude mít současně přístup k našim zdrojům. Je pravda, že hesla ukládaná v souboru *WS_FTP.ini* jsou zašifrována, ale není to dostatečné zabezpečení



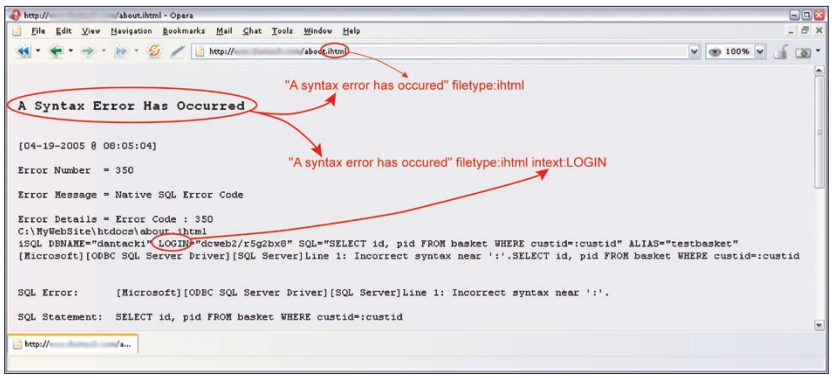
Obrázek 6. *Statistiky Sysinfo*

Tabulka 4. *Programy vytvářející statistiky o fungování systému*

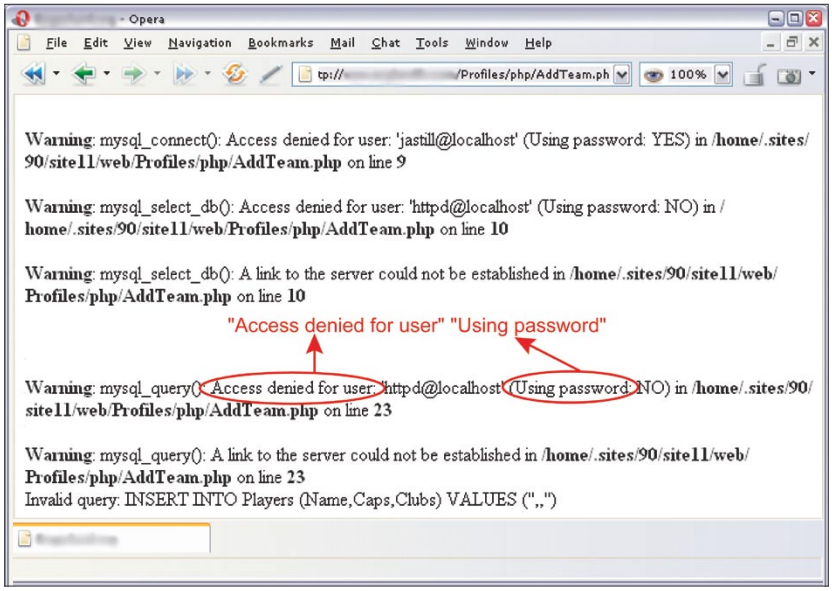
Dotaz	Typ informací
"Generated by phpSystem"	typ a verze operačního systému, hardwarová konfigurace, přihlášení uživatelé, otevřená spojení, zaplněnost paměti a pevných disků, přípojné body
"This summary was generated by wwwstat"	statistiky práce WWW serveru, umístění souborů v systému
"These statistics were produced by getstats"	statistiky práce WWW serveru, umístění souborů v systému
"This report was generated by WebLog"	statistiky práce WWW serveru, umístění souborů v systému
intext:"Tobias Oetiker" "traffic analysis"	statistiky práce systému v podobě MRTG, nastavení sítě
intitle:"Apache::Status" (inurl:server-status | inurl:status.html | inurl:apache.html)	verze serveru, typ operačního systému, seznam procesů a aktivní připojení
intitle:"ASP Stats Generator *.*" "ASP Stats Generator" "2003-2004 weppos"	aktivita WWW serveru, mnoho informací o návštěvnících
intitle:"Multimon UPS status page"	statistiky práce UPS zařízení
intitle:"statistics of" "advanced web statistics"	statistiky práce WWW serveru, informace o návštěvnících
intitle:"System Statistics" +"System and Network Information Center"	statistiky práce systému v podobě MRTG, hardwarová konfigurace, spuštěné služby
intitle:"Usage Statistics for" "Generated by Webalizer"	statistiky práce WWW serveru, informace o návštěvnících, umístění souborů v systému
intitle:"Web Server Statistics for ****"	statistiky práce WWW serveru, informace o návštěvnících
inurl:"/axs/ax-admin.pl" -script	statistiky práce WWW serveru, informace o návštěvnících
inurl:"/cricket/grapher.cgi"	MRTG z práce síťových rozhraní
inurl:server-info "Apache Server Information"	verze a konfigurace WWW serveru, typ operačního systému, umístění souborů v systému
"Output produced by SysWatch *"	typ a verze operačního systému, přihlášení uživatelé, obsazení paměti a pevných disků, přípojné body, spuštěné procesy, systémové logy

– pokud má konfigurační soubor, může útočník použít nástroje pro dešifrování hesla nebo si jen jednoduše nainstalovat program *WS_FTP* a spustit jej s naší konfigurací. A jakým způsobem se může útočník dostat k tisícům konfiguračních souborů klienta *WS_FTP*? Samozřejmě v Googlu. Díky dotazu `"Index of/" "Parent Directory" "WS_FTP.ini"` nebo `filetype:ini WS_FTP PWD` dostane mnoho odkazů na pro něj zajímavá data, která mu díky své neznalosti dáváme do rukou (Obrázek 9).

Jiný příklad je webová aplikace jménem *DUclassified*, která umožňuje přidávání a práci s reklamou na internetových stránkách. Ve standardní konfiguraci tohoto programu jsou jména uživatelů, hesla a jiná data ukládána v souboru *duclassified.mdb*, který se nachází v podadresáři *_private* který není chráněn proti zápisu. Pak již jen stačí najít stránku používající *DUclassifield* s ukázkovou adresou *http://<host>/duClassified/* a změnit ji na *http://<host>/duClassified/_private/duclassified.mdb*, abychom dostali soubor s hesly a naráz i získali neomezený přístup k aplikaci (ukazuje to Obrázek 10). A s nalezením stran, které používají popisovanou aplikaci, nám může pomoci následující do-



Obrázek 7. *Využití chyb databáze Informix*



Obrázek 8. *Chyba databáze MySQL*

Tabulka 5. *Hlášení o chybách*

Dotaz	Výsledek
`"A syntax error has occurred" filetype:ihtml`	Chyby databáze *Informix* – mohou obsahovat jména funkcí, jména souborů, informace o uložení souborů, části SQL kódu nebo hesla.
`"Access denied for user" "Using password"`	chyby ověření – mohou obsahovat jména uživatelů, jména funkcí, informace o umístění souborů a části SQL kódu
`"The script whose uid is " "is not allowed to access"`	chyby PHP spojené s kontrolou přístupu – mohou obsahovat jména souborů, jména funkcí a informace o umístění souborů
`"ORA-00921: unexpected end of SQL command"`	chyby databáze *Oracle* – mohou obsahovat jména souborů, jména funkcí a informace o umístění souborů
`"error found handling the request" cocoon filetype:xml`	chyby programu *Cocoon* – mohou obsahovat číslo verze *Cocoon*, jména souborů, jména funkcí a informace o umístění souborů
`"Invision Power Board Database Error"`	chyby diskuzního fóra *Invision Power Board* – mohou obsahovat jména souborů, jména funkcí a informace o umístění souborů v systému a také části SQL kódu
`"Warning: mysql_query()" "invalid query"`	chyby databáze *MySQL* – mohou obsahovat jména uživatelů, jména souborů, jména funkcí a informace o umístění souborů
`"Error Message : Error loading required libraries."`	chyby CGI skriptů – mohou obsahovat informace o typu operačního systému a verzi programu, jména souborů, jména uživatelů a informace o umístění souborů
`"#mysql dump" filetype:sql`	chyby databáze *MySQL* – mohou obsahovat informace o struktuře a obsahu databáze

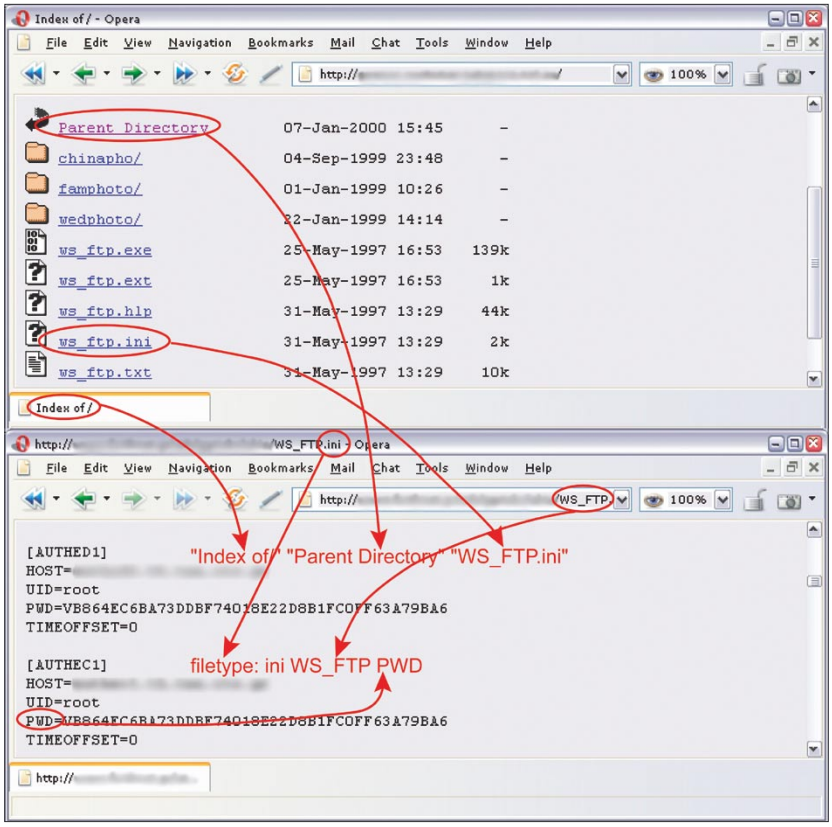
taz zadaný do Googlu: `"Powered by DUclassified" -site:duware.com` (abychom eliminovali výsledky týkající se stran výrobce). Je zajímavé, že výrobce *DUclassified* – firma DUware, vytvořila několik dalších aplikací, které jsou také napadnutelné podobným způsobem.

Teoreticky všichni víme, že nemáme přilepovat hesla na monitor nebo je schovávat pod klávesnicí. Zároveň však mnoho lidí ukládá hesla do souborů a umisťuje je do svých domovských adresářů , které jsou, oproti očekávání, dosažitelné z Internetu. Navíc mnoho z nich plní funkce správců sítí nebo podobných, díky čemu tyto soubory dosahují obrovských velikostí. Je těžké říci konkrétní pravidla pro hledání těchto dat, ale dobré výsledky dosáhnete s kombinací slov *account*, *users*, *admin*, *administrators*, *passwd*, *password* apod. ve spojení s typy souborů *.xls*, *.txt*, *.doc*, *.mdb* a *.pdf*. Je také dobré věnovat pozornost na adresáře obsahující ve jméně slova *admin*, *backup* nebo podobné: `inurl: admin intitle:index.of`. Ukázkové dotazy na data spojená s hesly je možno nalézt v Tabulce 6.

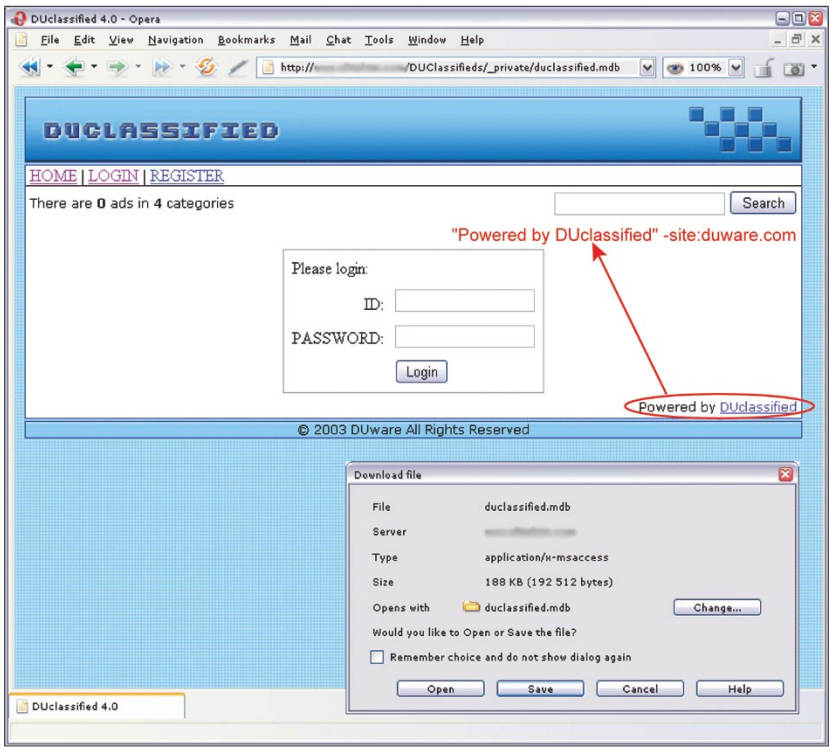
Abychom útočníkům ztížili přístup k našim heslům, musíme především myslet na to, kam a proč je zadáváme, jak jsou uchovávána a co se s nimi děje. Pokud spravujeme internetové stránky, měli bychom zanalyzovat konfiguraci používaných aplikací, najít slabě chráněná nebo citlivá data a příslušně je zabezpečit.

Osobní data a důvěrné dokumenty

Stejně jako v Polsku nebo Evropské unii, tak i ve Spojených státech existují příslušné právní regulace, jejichž cílem je chránit naše soukromí. Bohužel se však stává, že různé důvěrné dokumenty jsou umisťovány ve veřejně přístupných místech nebo posílány po Internetu bez správného zabezpečení. Stačí, když útočník získá přístup k elektronické poště obsahující náš životopis posílaný při hledání práce a zjistí naši adresu, číslo telefonu, datum narození, vzdělání, znalosti a doporučení.



Obrázek 9. *Konfigurační soubor programu WS_FTP*



Obrázek 10. *Standardně nastavený program DUclassified*

Na Internetu je možno najít mnoho dokumentů tohoto typu. Abychom je nalezli, je nutné zadat následující dotaz: `intitle: "curriculum vitae" "phone * * *" "address *" "e-mail"`. Je také

Tabulka 6. *Hesla – ukázkové dotazy v Googlu*

Dotaz	Výsledek
`"http://*:*@www" site`	hesla na stránky *site*, zapsané v podobě *http://username:password@www...*
`filetype:bak inurl:"htaccess|passwd|shadow|htusers"`	záložní kopie souborů, ve kterých se mohou nacházet informace o jménech uživatelů a heslech
`filetype:mdb inurl:"account|users|admin|administrators|passwd|password"`	soubory typu *mdb*, které mohou obsahovat informace o heslech
`intitle:"Index of" pwd.db`	soubory *pwd.db* mohou obsahovat jména uživatelů a zašifrovaná hesla
`inurl:admin inurl:backup intitle:index.of`	adresáře obsahující ve jméně slova *admin a backup*
`"Index of/" "Parent Directory" "WS _ FTP.ini" filetype:ini WS _ FTP PWD`	konfigurační soubory programu *WS_FTP*, které mohou obsahovat hesla pro přístup k FTP serverům
`ext:pwd inurl:(service|authors|administrators|users) "# -FrontPage-"`	soubory obsahující hesla programu *Microsoft FrontPage*
`filetype:sql ("passwd values ****" | "password values ****" | "pass values ****" )`	soubory obsahující SQL kód a hesla pro přístup k databázím
`intitle:index.of trillian.ini`	konfigurační soubory komunikátoru *Trillian*
`eggdrop filetype:user user`	konfigurační soubory ircbota *Eggdrop*
`filetype:conf slapd.conf`	konfigurační soubory aplikace *OpenLDAP*
`inurl:"wvdial.conf" intext:"password"`	konfigurační soubory programu *WV Dial*
`ext:ini eudora.ini`	konfigurační soubory poštovního programu *Eudora*
`filetype:mdb inurl:users.mdb`	soubory *Microsoft Accessu*, které mohou obsahovat informace o účtech
`intext:"powered by Web Wiz Journal"`	WWW stránky používající aplikaci *Web Wiz Journal*, která ve standardní konfiguraci umožňuje stažení souboru obsahujícího hesla; msto výchozí adresy *http://<host>/journal/* je nutno napsat *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`
	WWW stránky, používající aplikace *DUclassified*, *DUcalendar*, *DUdirectory*, *DUclassmate*, *DUdownload*, *DUpaypal*, *DUforum* nebo *DUpics*, které ve standardní konfiguraci umožňují získání souboru obsahujícího hesla; místo výchozí adresy (pro *DUclassified*) *http://<host>/duClassified/* je nutno zadat *http://<host>/duClassified/_private/duclassified.mdb*

`intext:"BiTBOARD v2.0" "BiTSHiFTERS Bulletin Board"`	WWW stránky používající aplikaci *Bitboard2*, které ve standardní konfiguraci umožňují získání souboru obsahujícího hesla; místo výchozí adresy *http://<host>/forum/forum.php* je nutno zadat *http://<host>/forum/admin/data_passwd.dat*

jednoduché najít elektronická data v podobě jmen, čísel telefonů a e-mailových adres (Obrázek 11). Vyplývá to z faktu, že skoro všichni uživatelé Internetu vytvářejí různé elektronické adresáře – mají nevelký význam pro útočníka, ale s použitím sociotechnik bude moci vyzkoušet data v nich obsažená, zvláště pokud se týkají kontaktů v rámci jedné firmy. Velmi dobře se v tom případě hodí například dotaz:

`filetype:xls inurl:"email.xls"`, který najde všechny tabulky se jménem *email.xls*.

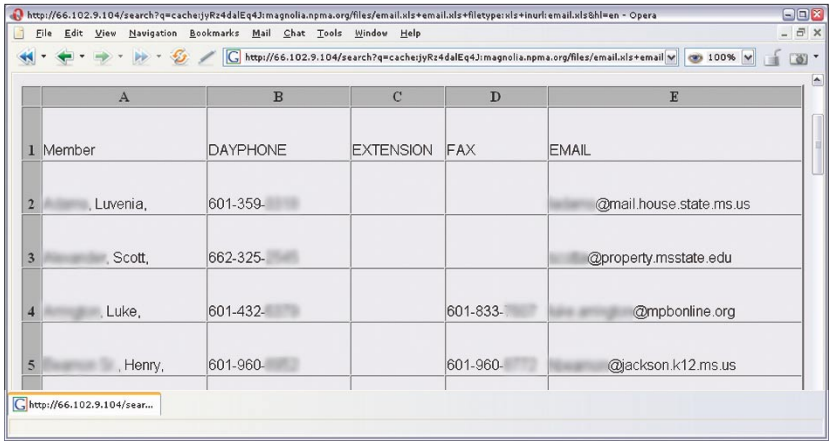
Podobně vypadá situace se síťovými komunikátory a v nich zapsanými kontakty – po získání tohoto seznamu se bude moci útočník pokoušet dostat se k našim přátelům. Je zajímavé, že dost osobních dat je možno najít v různých úředních dokumentech – policejních zpráv, soudních dopisech nebo třeba v chorobopisech.

Na Internetu je možno také nalézt dokumenty, kterým byl přidělen jakýsi stupeň důvěrnosti a které tak proto obsahují chráněné informace. Mohou to být projektové plány, technická dokumentace, různé ankety, hlášení, prezentace a další velké množství jiných vnitřních firemních dokumentů. Je možno je nalézt, protože velmi často obsahují výraz *confidential*, frázi *Not for distribution* nebo podobné (viz Obrázek 12). Tabulka 7 obsahuje několik ukázkových dotazů na dokumenty, které mohou obsahovat osobní data a důvěrné informace.

Stejně jako v případě hesel, abychom zabránili úniku našich osobních informací můžeme jedině zachovávat ostražitost a mít přehled o zveřejňovaných datech. Firmy a instituce by měly (a v mnoha případech i musí) vytvořit a dodržovat příslušné směrnice, procedury a postupy popisující vnitřní oběh informací, odpovědnosti a následky za jejich nedodržování.

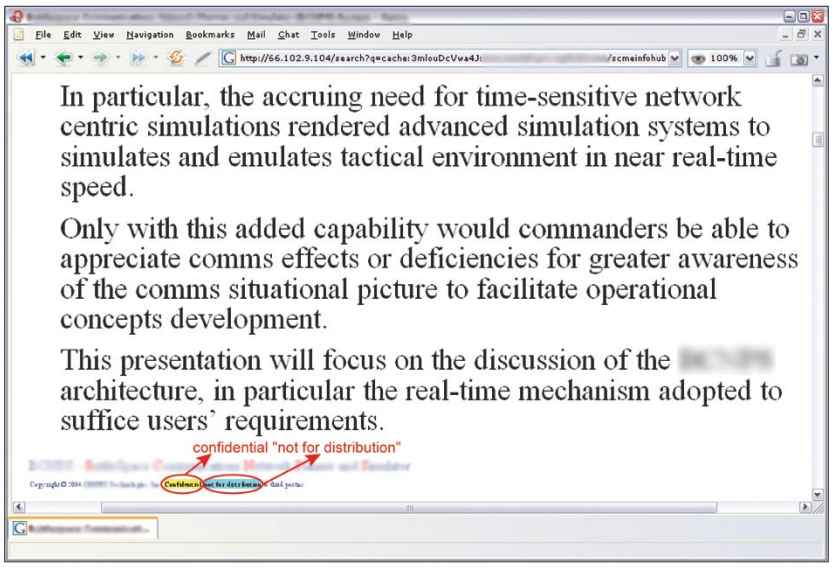
Síťová zařízení

Mnozí správci neberou vážně bezpečnost takových zařízení jako síťové tiskárny nebo webové kamery. Špatně zabezpečená tiskárna může být mostem, který útočník dobývá jako první a pak jej využívá pro provádění útoků na další systémy v síti nebo mimo ní. Webové kamery samozřejmě nejsou až tak nebezpečné, proto je možno se k ní chovat jako k zábavě, ale není těžké si představit situaci, když by taková data měla význam (průmyslová špionáž, přepadení). Dotazy na tiskárny a kamery obsahuje Tabulka 8, zatímco Obrázek 13 ukazuje na Internetu nalezenou stránku konfigurace tiskárny. ■

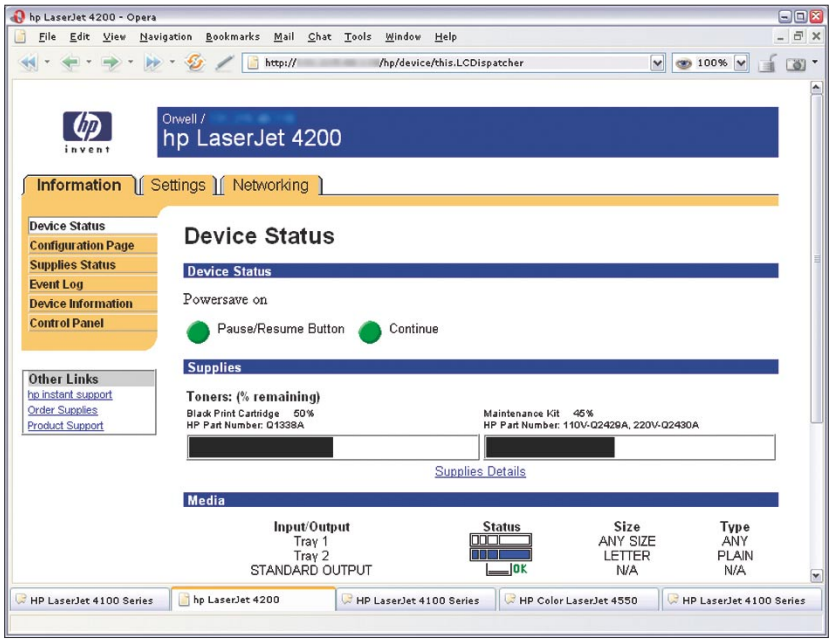


	A	B	C	D	E
1	Member	DAYPHONE	EXTENSION	FAX	EMAIL
2	, Luvenia,	601-359-			@mail.house.state.ms.us
3	, Scott,	662-325-			@property.msstate.edu
4	, Luke,	601-432-		601-833-	@mpbonline.org
5	, Henry,	601-960-		601-960-	@jackson.k12.ms.us

Obrázek 11. *Elektronický adresář získaný díky Google*



Obrázek 12. *Chráněný dokument nalezený vyhledávačem*



Obrázek 13. *Googlem nalezená konfigurační stránka tiskárny HP*

Tabulka 7. *Hledání osobních dat a důvěrných dokumentů*

Dotaz	Výsledek
`filetype:xls inurl:"email.xls"`	soubory *email.xls*, které mohou obsahovat elektronická data
`"phone * * *" "address *" "e-mail" intitle:"curriculum vitae"`	dokumenty s životopisy
`"not for distribution" confidential`	dokumenty opatřené stupněm confidential
`buddylist.blt`	seznamy kontaktů komunikátoru *AIM*
`intitle:index.of mystuff.xml`	seznamy kontaktů komunikátoru *Trillian*
`filetype:ctt "msn"`	seznam kontaktů *MSN*
`filetype:QDF QDF`	databáze finančního programu *Quicken*
`intitle:index.of finances.xls`	soubory *finances.xls*, které mohou obsahovat informace o bankovních kontech, finanční sestavy a čísla kreditních karet
`intitle:"Index Of" -inurl:maillog maillog size`	soubory *maillog*, které mohou obsahovat e-mailové zprávy
`"Network Vulnerability Assessment Report" "Host Vulnerability Summary Report" filetype:pdf "Assessment Report" "This file was generated by Nessus"`	zprávy s výsledky o bezpečnosti sítě, penetračních testů apod.

Tabulka 8. *Charakteristické řetězce pro síťová zařízení*

Dotaz	Zařízení
`"Copyright (c) Tektronix, Inc." "printer status"`	tiskárny PhaserLink
`inurl:"printer/main.html" intext:"settings"`	tiskárny Brother HL
`intitle:"Dell Laser Printer" ews`	tiskárny Dell s technologií EWS
`intext:centreware inurl:status`	tiskárny Xerox Phaser 4500/6250/8200/8400
`inurl:hp/device/this.LCDispatcher`	tiskárny HP
`intitle:liveapplet inurl:LvAppl`	kamery Canon Webview
`intitle:"EvoCam" inurl:"webcam.html"`	kamery Evocam
`inurl:"ViewerFrame?Mode="`	kamery Panasonic Network Camera
`(intext:"MOBOTIX M1" | intext:"MOBOTIX M10") intext: "Open Menu" Shift-Reload`	kamery Mobotix
`inurl:indexFrame.shtml Axis`	kamery Axis
`SNC-RZ30 HOME`	kamery Sony SNC-RZ30
`intitle:"my webcamXP server!" inurl:":8080"`	kamery dostupné skrz aplikaci *WebcamXP Server*
`allintitle:Brains, Corp. camera`	kamery dostupné skrz aplikaci *mmEye*
`intitle:"active webcam page"`	kamery s USB rozhraním