

Google Reveals Cryptographic Secrets

Emin İslam Tatlı
tatli@th.informatik.uni-mannheim.de

Department of Computer Science, University of Mannheim

1. Kryptowochende, 01-02 July 2006

Outline

- 1 Google Hacking
- 2 Cryptographic Secrets
- 3 Automatic Tools
- 4 Countermeasures

Motivation

- Google has the index size over 20 billion entries
 - try to search `-"fgkdfgjisdgjsiod"`
- We use google to search anything
- But hackers also use google to search something
 - called **Google Hacking**
 - vulnerable servers, files and applications, files containing usernames-passwords, sensitive directories, online devices, etc.
 - Google Hacking Database [1] \Rightarrow 1413 entries in 14 groups (by July 2006)
- What about Cryptographic Secrets?
- In this talk, we find out cryptographic secrets with google

Advanced Search Parameters

- [all]inurl
- [all]intext
- [all]intitle
- site
- ext, filetype
- symbols: "-", "|", "."

Examples of Google Hacking I

Unauthenticated programs

```
"PHP Version" intitle:phpinfo inurl:info.php
```

Applications containing SQL injection & path modification vulnerabilities

- "advanced guestbook * powered" inurl:addentry.php
- intitle:"View Img" inurl:viewimg.php

Security Scanner Reports

```
"Assessment Report" "nessus" filetype:pdf
```

Examples of Google Hacking II

Private data listings

- `"index of private|privat|özel"`
- `phone address email intitle:"Curriculum Vitae"`

Database applications&error files

- `"Welcome to phpmyadmin ***" "running on * as root@*" intitle:phpmyadmin`
- `"mysql error with query"`

Examples of Google Hacking III

Online Devices

- `inurl:"hp/device/this.LCDispatcher"`
- `intitle:liveapplet inurl:LvAppl`
- `"Please wait....." intitle:"SWW link"`

Cryptographic Secrets

- 1 Hashed Passwords
- 2 Secret Keys
- 3 **Public Keys**
- 4 Private Keys
- 5 Encrypted Messages
- 6 Signed Messages

Hashed Passwords

Hashed passwords in dump files

- `"create table" "insert into"`
`"pass|passwd|password" (ext:sql | ext:dump |`
`ext:dmp)`
- `intext:"password|pass|passwd"`
`intext:"md5|sha1|crypt" (ext:sql | ext:dump |`
`ext:dmp)`

Secret Keys

Secret keys in Kerberos

- `inurl:"kdc.conf" ext:conf`
- `inurl:"slave_datatrans" OR inurl:"from_master"`

Java keystores

- `keystore ext:ks`

Public Keys

PGP public keys

- "BEGIN PGP PUBLIC KEY BLOCK" (ext:txt | ext:asc | ext:key)

Public keys in certificates

- "Certificate:Data:Version" "BEGIN CERTIFICATE"
(ext:crt | ext:asc | ext:txt)

Private Keys

PGP private keys

- "BEGIN (DSA|RSA)" ext:key
- "BEGIN PGP PRIVATE KEY BLOCK" inurl:txt|asc
- "index of" "secring.gpg"

Encrypted Messages

PGP encrypted files

- `-"public|pubring|pubkey|
signature|pgp|and|or|release" ext:gpg`

More encrypted files

- `-intext:"and" (ext:enc | ext:axx)`

XML encrypted elements

- `"ciphervalue" ext:xml`

Signed Messages

Signed emails

- "BEGIN PGP SIGNED MESSAGE" "From" "Date"
"Subject" (ext:eml | ext:txt | ext:asc)

File signatures

- -"and|or" "BEGIN PGP SIGNATURE" ext:asc

PGP signed messages

- "BEGIN PGP SIGNED MESSAGE" -"From" (ext:txt |
ext:asc | ext:xml)

Automatic Tools

- 1 Gooscan
- 2 Sitedigger
- 3 Goolink
- 4 AdvancedDork
- 5 Google Advanced Operation Toolbar

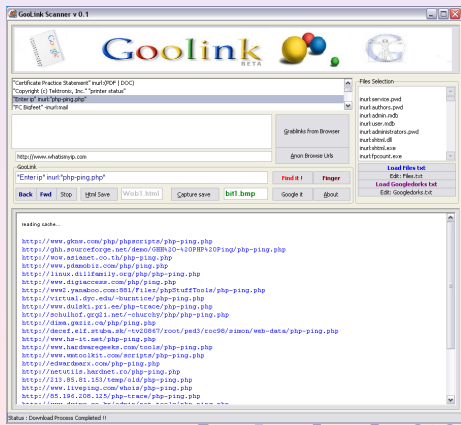
Gooscan [7]

- a Unix/Linux script to check google hacking queries against your system
- uses GHD [1]
- to execute:

```
$ gooscan -t www.google.de -q "BEGIN (DSA|RSA)  
ext:key" -s de -o output.html
```


Goolink [5]

- Goolink queries Google for a particular chosen search from GHD



AdvancedDork [2]

- not specific to google hacking
- a Firefox extension for google searches

The screenshot shows a Firefox browser window with search results for the term "güvenlik". The first result is titled "Saldırı Ağaçları" by Emin İslam Tatlı, discussing Bruce Schneier's "attack trees". The second result is "Türkçe İçin Doğal Dil İşleme Çalışması" by Ünal Çakıroğlu. The AdvancedDork extension menu is open, showing options like "Add to Kaboodle", "Copy", "Select All", "Search Web for 'güvenlik'", "Stumble Search for 'güvenlik'", "Tag this page as 'güvenlik'", "Tag This Page...", "This Frame", "View Selection Source", "Properties", and "Web Developer". The menu also displays metadata fields: "intitle:", "inurl:", "intext:", "site:", and "ext:". The background text in the search results is partially obscured by the menu.

Google Advanced Operations Toolbar [3]

- a Firefox extension
- provides a shortcut of Google's advanced search functions

güvenlik site:www.teknoturk.org - Google Search - Mozilla Firefox

File Edit View Go Bookmarks Tools Help del.icio.us

Back Forward Reload Stop Home Kaboodle Add To Kaboodle del.icio.us tag this Send Money

Getting Started Latest Headlines SALSA WebHome < Main < ... Neophyte Google heise online - My-IP-S...

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resizer Tools View Source Options

Stumble! All I like it! Search or Tag here Menu

güvenlik site: URL: www.teknoturk.org Search

Google

Web

TeknoTurk.org - Yazı K
Güvenlik. Saldırı Açışları -
Albert Levi, 28/3/2004. Gü
www.teknoturk.org/docking/

Zavallı Savunmasız İnter
DoS atakları tanım itibarıyla
tıpkı 17 Ağustos depreminde
www.teknoturk.org/docking/

Elektronik Saldırı Tespi

Groups News Froogle Maps more »

teknoturk.org Search Advanced Search Preferences

Results 1 - 10 of about 50 from www.

13/8/2005. Deveküşü Sendromu: E-posta Örneği
ayar ve iletişim ...
k.htm - 11k - Cached - Similar pages

lan Şubat (2000) ağı ...
lik geçtiği değildir. Ancak son aylardaki ataklar,
fi, ...
azi.htm - 15k - Cached - Similar pages

Guard G
Hırsız Ala
Detaylı bil
www.guar
Kursun C
Kürşun ge
Battaniye
www.acar

Security Measures

- 1 Use automatic tools to check your system

Security Measures

- 1 Use automatic tools to check your system
- 2 Use Robot Exclusion Standart (robots.txt)

Security Measures

- 1 Use automatic tools to check your system
- 2 Use Robot Exclusion Standart (robots.txt)
- 3 Install and manage Google Honeypot [4]

Conclusion

- Cryptography requires secrets to be kept secret
- Google indexes your secrets and makes public
- Take the required security countermeasures and protect your secrets

References I

-  Google Hacking Database. <http://johnny.ihackstuff.com>
-  AdvancedDork- A Firefox extension for google searches.
<http://johnny.ihackstuff.com>
-  Google Advanced Operation Toolbar.
<https://addons.mozilla.org/firefox/1258/>
-  Google Hack HoneyPot Project. <http://ghh.sourceforge.net>
-  Goolink- Security Scanner.
www.ghacks.net/2005/11/23/goolink-scanner-beta-preview/
-  SiteDigger v2.0 - Information Gathering Tool.
<http://www.foundstone.com>

References II



Gooscan - Google Security Scanner.
<http://johnny.ihackstuff.com>