Die Kunst des Google-Hackings (Pentesting Stage 1: Intel)

Vorbemerkung

- Google-Hacks sind **nicht** verboten, da die Daten für jeden aus dem Internet zu erreichen sind.
- Daher sind Google-Hacks keine ‚Hacks' im eigentlichen Sinne, vielmehr handelt es sich um **‚kreatives' Suchen** mit bestimmten Parametern.
- **Strafbar** wird es dann, wenn die Daten für Unsinn missbraucht werden (z.B. eingriff in die Heizungssteuerung)

Wieso funktioniert Googele-Hacking?

- Durch eine fehlende, bzw. falsch eingerichtete **robots.txt** indiziert Google Seiten, die nicht für das indizieren vorgesehen sind bzw. sein sollten.
  Lesebefehl: https://en.wikipedia.org/wiki/Robots_exclusion_standard

- Heute betrifft dies vor allem viele **IoT-Devices**, die unzureichend konfiguriert sind und so ‚offen' im Netz hängen.
  Für IoT-Devices ist **shodan.io** eine andere gute Quelle.

Grundregeln der Google-Suche

- Google ist **nicht** Case-sensitiv (Ausnahme: OR-Operator)

- ***** (Asterisk) ist kein Wildcard innerhalb eines Wortes (*.mp3) – es ist ein Ersatz für einen normalen Suchbegriff („*** ist die Mutter von ***“).

- Google ignoriert allgemeine Begriffe (where, is, where, if, …).
  where a=1 wird gesucht als **a=1**
  Will man diese Begriffe suchen, muss man sie in „“ (Anführungszeichen) setzen oder ein **+** voranstellen.

Boolsche Operatoren bei der Suche

- **AND (+)** ist redundant und wird von Google vorgegeben:
  `veganes Essen` liefert das selbe Ergebnis wie
  `veganes AND essen`

- **NOT (-)** schliesst Begriffe aus:
  `Gebrauchtwagen AND Diesel NOT Volkswagen`

- **OR (|)** Zeigt Ergebnisse, auf die einer der Suchbegriffe auftaucht
  `Gebrauchtwagen AND Diesel AND BMW OR FORD`

Basisparameter 1

- **„SUCHBEGRIFF 1 SUCHBEGRIFF 2 …“**
  Alle Wörter innerhalb der „“ werden exakt in dieser Form und Reihenfolge gesucht

- **site:**$DOMAIN **SUCHBEGRIFF**
  Die Suche wird nur auf eine spezielle Domain beschränkt

- **intitle:SUCHBEGRIFF**
  Der Seitentitel muss das Suchwort enthalten (z.B. ‚index of‘)

Basisparameter 2

- **`inurl:SUCHBEGRIFF`**
  Die URL der Seite muss das Suchwort enthalten (z.B. ‚pictures‘)

- **`filetype:SUCHBEGRIFF`**
  Beschränkt die Suche auf Dokumente eines bestimmten Formats (z.B. ‚jpg‘-Bilder)

- **`related:`**`$DOMAIN`
  Sucht Seiten, deren Inhalt ähnlich der der angegebenen Domain sind.

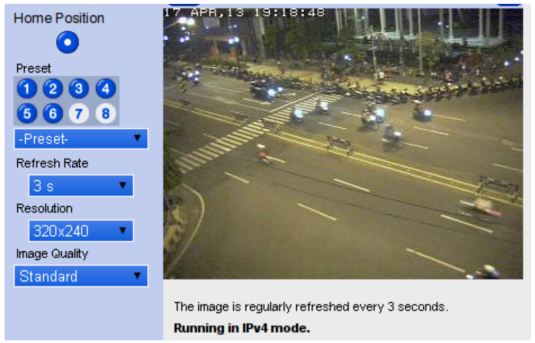
KEEP CALM AND START YOUR (SEARCH) ENGINES!

Wichtige Befehle

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Kameras

- `intitle:"Live View / - AXIS“`
- `inurl:"sample/LvAppl/“`
- `inurl:"viewerframe?mode=refresh“`
- `intitle:"Network Camera“ inurl:"/ViewerFrame?Mode=Refresh“`
- `intitle:"Toshiba Network Camera" user login`



Dokumente

- `intitle:"Lebenslauf" "Telefon *" "Adresse *"inurl:"`

Lebenslauf

Persönliche Daten

Name	Wille
Vorname	Melanie
Adresse	Spaniagasse 5c 9490 Vaduz Fürstentum Liechtenstein
E-Mail	melanie_wille@hotmail.com
Telefon P	00423 233 28 68
Telefon M	079 722 61 15
Geburtsdatum	25. Dezember 1989
Heimatort	Grabs, SG
Zivilstand	ledig

Schulische Ausbildung

2009 – 2012	Pädagogische Hochschule des Kantons St. Gallen (PHSG, Studiengang Kindergarten und Primarschule), Diplomtyp B (1.-6 Klasse)
2001- 2009	Gymnasium Marianum Vaduz, Matura Profil Lingua mit Schwerpunkt alte Sprachen (Italienisch und Latein)
1996 – 2001	Primarschule Ebenholz, Vaduz

Praktische Tätigkeit

02.2012	Praktikum Integrationsklasse St.Gallen

Dokumente 2

- Gängige Office-Formate
  - **für Word: filetype:doc OR filetype:docx**
  - **für Excel: filetype:xls OR filetype:xlsx**
  - **für Powerpoint: filetype:ppt OR filetype:pptx**
  - **für PDF: filetype:pdf**
- Gern auch zusammen mit Begriffen wie
  „Vertraulich OR intern“
- Gute Quelle auch hier:
  https://de.wikipedia.org/wiki/Kategorie:Liste_(Dateinamenserweiterungen)

Medien

- Musik `intitle:"Index of /" +mp3 eminem`
- Videos `intitle:"Index of /" +avi`
- Bücher `intitle:"Index of /" +epub`
- ISOs `intitle:"Index of /" +iso`

Schwachstellen

- Webserver bekannter Releasestände
  `intitle:index of "Apache/2.4.7 (Ubuntu) Server"`

- Outlook Web-Applications (OWA), die auf Exchange aufbauen
  `inurl:https://owa`

- Der Klassiker: Wordpress
  - `"index of" inurl:wp-content/`
  - `"inurl:"/wp-content/plugins/wp-shopping-cart/“`
  - `"inurl:wp-content/plugins/wp-dbmanager/"`

Weiterführendes:

- Google-Dorks-Database:
  https://www.exploit-db.com/google-hacking-database/

- Wikipedia:
  https://en.wikipedia.org/wiki/Google_hacking