Google Hacking - The Basics

Maniac
• What exactly is Google Hacking?

• Google Hacking involves using the Google search engine to identify vulnerabilities in websites.
Hacking - The Basics

• Ok, so you use Google to find all of this stuff, but how do you?

  • Google supports a multitude of operators and modifiers that add a ton of power to google searching.
• Mmmmmmm....operators and modifiers! I want them!
Hacking - The Basics

- cache:

  - Syntax: cache:URL [highlight]

  - The cache operator will search through google’s cache and return the results based on those documents. You can alternatively tell cache to highlight a word or phrase by adding it after the operator and URL.
Hacking - The Basics

- **link:**
  - Syntax: link:URL
  - Sites that have a hyperlink to the URL specified will be returned in the search results.
The related operator will return results that are “similar” to the page that was specified.

• Syntax: related:URL
Hacking - The Basics

- **info:**
  - Syntax: `info:URL`
  - This tag will give you the information that Google has on the given URL.
Hacking - The Basics

- **site:**

  - Syntax: site:Domain

  - This modifier will restrict results to those sites within the domain given.
Hacking - The Basics

- allintitle:

- Syntax: allintitle: oper1 [oper2] [oper3] [etc..]

- Google will restrict the results to those that have all of the words entered after the modifier within the title. NOTE: This modifier does not play well
• intitle:

• Syntax: intitle:operator

• Google will return only results that match the word or phrase entered after the modifier within the title of the page.
allinurl:

Syntax: allinurl: oper1 [oper2] [oper3] [etc...]

This modifier is similar to allintitle: in that it will use the rest of the query and look for all the words or phrases in the URL that was specified. NOTE: Also like allintitle:, this modifier doesn’t play well with others.
Hacking - The Basics

- inurl:

  - Syntax: inurl:operator

- Here is the single operator version of allinurl:. Will return anything that has the operator in the URL.
Hacking - The Basics

• allintext:

  • Syntax: allintext: oper1 [oper2] [oper3] [etc...]

  • Just like not using any operators....
Hacking - The Basics

• intext:
  
  • Syntax: intext:operator
  
  • Ok, ok, I’ll let you guess on this one.

![Google Search](https://i.imgur.com/123456.png)
Hacking - The Basics

• Are you done yet? That seemed like a lot, and what the hell was with all the apple stuff?

  • Almost there. Now it's time to start mixing and matching these modifiers and operators.

    • The four most commonly used will be intitle:, intext:, inurl:, and filetype:

    • Also note, you can use OR and + and - signs.
Hacking - The Basics

• mixing in intext:, inurl:, and intitle: and looking for default drupal sites that haven’t been configured yet.

• -inurl:drupal.org intext: "Welcome to your new Drupal-powered website." intitle:drupal
Hacking - The Basics

- "display printer status" intitle:"Home"
Hacking - The Basics

• Whoa! a Xerox printer!
"#mysql dump" filetype:sql 21232f297a57a5a743894a0e4a801fc3

sesiones enum('S','N') DEFAULT 'N' NOT NULL,
usuarios enum('S','N') DEFAULT 'N' NOT NULL,
configuracion enum('S','N') DEFAULT 'N' NOT NULL,
estadisticas enum('S','N') DEFAULT 'N' NOT NULL,
super enum('S','N') DEFAULT 'S' NOT NULL,
PRIMARY KEY (id),
UNIQUE id_admin_2 (id),
KEY id_admin (id)
);

# Dumping data for table 'administradores'
#

INSERT INTO administradores (id, login, password, nombre, estado, sesiones, usuarios, configuracion, estadisticas, super) VALUES ('1', 'Administrador', '21232f297a57a5a743894a0e4a801fc3', 'Nombre Administrador', 'N', 'N', 'N', 'N', 'S');

21232f297a57a5a743894a0e4a801fc3 is the MD5sum for admin
1 General

This document is the Comodo Certification Practice Statement (CPS) and outlines the legal, commercial and technical principles and practices that Comodo employ in providing certification services that include, but are not limited to approving, issuing, using and managing of Digital Certificates and in maintaining a X.509 Certificate-based public key infrastructure (PKIX) in accordance with the Certificate Policies determined by Comodo. It also defines the underlying certification processes for Subscribers and describes Comodo’s™ repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the Comodo PKI.

1.1 Comodo

Comodo is a Certification Authority (CA) that issues high quality and highly trusted digital certificates to entities including private and public companies and individuals in accordance with this CPS. In its role as a CA Comodo performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing a digital certificate.
Hacking - The Basics

- "Network Vulnerability Assessment Report"

```
Session name: PIX Firewall

Total records generated: 11
  high severity: 0
  low severity: 7
  informational: 4

Start time: 21.03.
Finish time: 21.03.
Elapsed: 0 day

Summary of scanned hosts
```
"Thank you for your order" + receipt filetype:pdf
"robots.txt" + "Disallow:" filetype:txt

User-agent: *
Disallow: /cgi-bin
Disallow: /search
Disallow: /query.html
Disallow: /help
Disallow: /robots.txt
Disallow: /360pics/text
Disallow: /911/911day/text
Disallow: /911/heroes/text
Disallow: /911/messages/text
Disallow: /911/patriotism/text
Disallow: /911/patriotism2/text
Disallow: /911/progress/text
Disallow: /911/remembrance/text
Disallow: /911/response/text
Disallow: /911/sept112002/text
Disallow: /911/text
Disallow: /QA-test/text
"phpMyAdmin" "running on" inurl:"main.php"
Hacking - The Basics

- "phone * * *" "address *" "e-mail" intitle:"curriculum vitae"

**CURRICULUM VITAE**

**BIOGRAPHICAL**

**NAME:** James M. Lynch, MD

**HOME ADDRESS:** 127 Pheasant Drive
Pittsburgh, PA 15238

**BIRTH DATE:** November 2

**BIRTH PLACE:** Washington

**BUSINESS ADDRESS:** Department of Surgery
Children's Hospital of Pittsburgh
3705 Fifth Avenue
Pittsburgh, PA 15213

**CITIZENSHIP:** U.S.A.

**SOCIAL SECURITY:** 042-40-9236
"social security number" "phone * * *" "address *" "e-mail *" intitle:"curriculum vitae" filetype:pdf site:.edu
Hacking - The Basics

- **ext:vmx vmx**

```bash
#!/opt/vmware-player/vmware
config.version = "8"
virtualHW.version = "4"
memsize = "128"
ide0:0.present = "FALSE"
ide0:0.fileName = ""
ide1:0.present = "TRUE"
ide1:0.fileName = "dsl-1.5.iso"
ide1:0.deviceType = "cdrom-image"
floppy0.startConnected = "FALSE"
floppy0.fileName = "~/home/jgeorg/Download/Abbilder/fdos1440.img"
ethernet0.present = "TRUE"
sound.present = "TRUE"
sound.virtualDev = "es1371"
displayName = "DamnSmallLinux-1.5"
guestOS = "linux"
vrnam = "dsl-1.5.nvram"

floppy0.present = "TRUE"
usb.present = "TRUE"
```
Hacking - The Basics

- filetype:QBW qbw

Results 11 - 20 of about 301 for filetype:QBW qbw. (0.16 seconds)

CSCServer.CC.Edu/JohnsonP/Csc201/Larry.Qbw
File Format: Unrecognized - View as HTML
Supplemental Result - Similar pages

www.Psats.ORG/QuickBooksPro2003FileWithDCEDChartof...
File Format: Unrecognized - View as HTML
Supplemental Result - Similar pages

www.FourKidsPlay.com/My%20Documents/AmTel-2004.QBW
File Format: Unrecognized - View as HTML
Supplemental Result - Similar pages

†v*Ali*D**A*T#*1YYYY*MAUl ...
File Format: Unrecognized - View as HTML
qbw:browser?relativeURL=y&url=components/Services/find. ... qbw:browser?
url=https://Site.quickbooks.com/edit/1&showtoolbar=no&unique=https://Site. ...
### Hacking - The Basics

- filetype:xls inurl:"email.xls"

---

**Sheet1**

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Abby Kavner</td>
<td></td>
<td>University of California, Los Angeles</td>
<td></td>
<td><a href="mailto:akavner@igpp.ucla.edu">akavner@igpp.ucla.edu</a></td>
</tr>
<tr>
<td>2</td>
<td>Agnes L Mao</td>
<td></td>
<td>Carnegie Institution of Washington</td>
<td></td>
<td><a href="mailto:amao@gl.ciw.edu">amao@gl.ciw.edu</a></td>
</tr>
<tr>
<td>3</td>
<td>Alexandre Corgne</td>
<td></td>
<td>Carnegie Institution of Washington</td>
<td></td>
<td><a href="mailto:a.corgne@gl.ciw.edu">a.corgne@gl.ciw.edu</a></td>
</tr>
<tr>
<td>4</td>
<td>Ann Lattimore</td>
<td></td>
<td>Stony Brook University</td>
<td></td>
<td><a href="mailto:alattimore@notes.cornell.edu">alattimore@notes.cornell.edu</a></td>
</tr>
<tr>
<td>5</td>
<td>Arianna E. Gleason</td>
<td></td>
<td>University of California, Berkeley</td>
<td></td>
<td><a href="mailto:arianna@lpl.arizona.edu">arianna@lpl.arizona.edu</a></td>
</tr>
<tr>
<td>6</td>
<td>Bruce Buffett</td>
<td></td>
<td>University of Chicago</td>
<td></td>
<td><a href="mailto:buffett@geosci.uchicago.edu">buffett@geosci.uchicago.edu</a></td>
</tr>
<tr>
<td>7</td>
<td>Carl B. Agee</td>
<td></td>
<td>University of New Mexico</td>
<td></td>
<td><a href="mailto:agee@unm.edu">agee@unm.edu</a></td>
</tr>
<tr>
<td>8</td>
<td>Charles Martin</td>
<td></td>
<td>Stony Brook University</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Charles T. Browitt</td>
<td></td>
<td>University of Arizona</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Hacking - The Basics

• intitle:"Index of" finances.xls

<table>
<thead>
<tr>
<th>Name</th>
<th>Last_modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td>23-Mar-2005 12:07</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Finances.xls</td>
<td>23-Mar-2005 12:07</td>
<td>15k</td>
<td></td>
</tr>
<tr>
<td>Letter.doc</td>
<td>23-Mar-2005 12:07</td>
<td>21k</td>
<td></td>
</tr>
</tbody>
</table>
• WOW! That was a lot of good finds! Where can I find more info on googlehacking?

• http://johnny.ihackstuff.com