Hacking with Google for fun and profit!

October 2004

Robert Masse & Jian Hui Wang
Agenda

- Google Introduction & Features
- Google Search Technique
- Google Basic Operators
- Google Advanced Operators
- Google Hacking
  - Digging for “vulnerability gold”
  - Identifying operating systems
  - Vulnerability scanning
  - Proxying
- Protect your information from Google
Google Hacking

- Google Search Technique
  - Just put the word and run the search
- You need to audit your Internet presence
  - One database, Google almost has it all!
- One of the most powerful databases in the world
- Consolidate a lot of info
- Usage:
  - Student …
  - Business …
  - Al’Qaeda …
    - One stop shop for attack, maps, addresses, photos, technical information
Google Hacking

- Google Advance Search
  - A little more sophisticated …..
Google Operators:
- Operators are used to refine the results and to maximize the search value. They are your tools as well as hackers’ weapons.

Basic Operators:
+ , -, ~ , ., *, “”, |, OR

Advanced Operators:
- allintext:, allintitle:, allinurl:, bphonebook:, cache:, define:, filetype:, info:, intext:, intitle:, inurl:, link:, phonebook:, related:, rphonebook:, site:, numrange:, daterange
Google Hacking

- **Basic Operators**
  - (+) force inclusion of something common
  - Google ignores common words (where, how, digit, single letters) by default:
    Example: StarStar Wars Episode +I
  - (-) exclude a search term
    Example: apple –red
  - (““) use quotes around a search term to search exact phrases:
    Example: “Robert Masse”
  - Robert masse without “” has the 309,000 results, but “robert masse” only has 927 results. Reduce the 99% irrelevant results
Google Hacking

- **Basic Operators**
  - (\sim) search synonym:
    - Example: \sim food
  - Return the results about food as well as recipe, nutrition and cooking information
  - (.) a single-character wildcard:
    - Example: m.trix
  - Return the results of M@trix, matrix, metrix……
  - (*) any word wildcard
Google Hacking

• Advanced Operators: “Site:”
  – Site: Domain_name
  – Find Web pages only on the specified domain. If we search a specific site, usually we get the Web structure of the domain
  – Examples:
    site:ca
    site:gosecure.ca
    site:www.gosecure.ca
usr/bin/perl    # Runs a number of concurrent nmap processes and ...
#!/usr/bin/perl    # Runs a number of concurrent nmap processes and stores the
results in # a specified directory in xml, human and machine formats. ...
www.gosecure.ca/SecInfo/tools/multimap.pl - 10k - Cached - Similar pages

GoSecure: Information Security Experts
VULNERABILITIES & EXPLOITS DETAILS. Multiple Browsers Frame Injection Vulnerability.
www.gosecure.ca/cgi-bin/detailvul_flash.cgi?id=244 - 17k - Cached - Similar pages

GoSecure: Information Security Experts
VULNERABILITIES & EXPLOITS DETAILS. SSH URI Handler Code Execution. Source:
http://www.securiteam.com/securitynews/archive.html
Date: 2004-06-22. Summary. ...
www.gosecure.ca/cgi-bin/detailvul_flash.cgi?id=221 - 18k - Cached - Similar pages

www.gosecure.ca/cgi-bin/detailvul_flash.cgi?id=209
Similar pages
Google Hacking

- **Advanced Operators: “Filetype:”**
  - Filetype: extension_type
  - Find documents with specified extensions
  - The supported extensions are:
    - HyperText Markup Language (html)
    - Adobe Portable Document Format (pdf)
    - Adobe PostScript (ps)
    - Lotus 1-2-3
      (wk1, wk2, wk3, wk4, wk5, wki, wks, wku)
    - Lotus WordPro (lwp)
    - MacWrite (mw)
    - Text (ans, txt)
    - Microsoft PowerPoint (ppt)
    - Microsoft Word (doc)
    - Microsoft Works (wks, wps, wdb)
    - Microsoft Excel (xls)
    - Microsoft Write (wri)
    - Rich Text Format (rtf)
    - Shockwave Flash (swf)
    - Text (ans, txt)
  - Note: We actually can search asp, php and cgi, pl files as long as it is text-compatible.
  
Example: Budget filetype: xls
Google Hacking

• Advanced Operators
  – A budget file we found ……. 
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Nondefense:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>International affairs</td>
<td>33.1</td>
<td>29.9</td>
<td>25.1</td>
<td>24.7</td>
<td>25.9</td>
<td>26.7</td>
<td>23.6</td>
<td>18.5</td>
</tr>
<tr>
<td>General science, space and technology:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General science and basic research</td>
<td>3.0</td>
<td>3.0</td>
<td>4.2</td>
<td>4.1</td>
<td>4.4</td>
<td>4.5</td>
<td>4.5</td>
<td>4.2</td>
</tr>
<tr>
<td>Space and other technology</td>
<td>7.4</td>
<td>14.3</td>
<td>22.5</td>
<td>26.4</td>
<td>29.9</td>
<td>26.7</td>
<td>22.3</td>
<td>18.5</td>
</tr>
<tr>
<td>Total General science, space and technology</td>
<td>10.3</td>
<td>17.4</td>
<td>26.7</td>
<td>30.6</td>
<td>34.3</td>
<td>31.1</td>
<td>26.8</td>
<td>22.7</td>
</tr>
<tr>
<td>Energy</td>
<td>3.9</td>
<td>3.7</td>
<td>3.7</td>
<td>4.4</td>
<td>3.8</td>
<td>4.2</td>
<td>5.0</td>
<td>4.6</td>
</tr>
<tr>
<td>Natural resources and environment</td>
<td>13.7</td>
<td>14.4</td>
<td>14.5</td>
<td>14.9</td>
<td>16.0</td>
<td>16.4</td>
<td>16.5</td>
<td>15.4</td>
</tr>
<tr>
<td>Agriculture</td>
<td>2.2</td>
<td>2.6</td>
<td>2.7</td>
<td>2.8</td>
<td>3.1</td>
<td>3.4</td>
<td>3.4</td>
<td>3.8</td>
</tr>
<tr>
<td>Commerce and housing credit</td>
<td>8.1</td>
<td>7.8</td>
<td>6.4</td>
<td>8.6</td>
<td>9.5</td>
<td>11.2</td>
<td>10.2</td>
<td>4.7</td>
</tr>
<tr>
<td>Transportation:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ground transportation</td>
<td>0.4</td>
<td>0.4</td>
<td>0.4</td>
<td>0.4</td>
<td>0.5</td>
<td>0.6</td>
<td>0.8</td>
<td>1.4</td>
</tr>
<tr>
<td>Air transportation</td>
<td>4.4</td>
<td>4.4</td>
<td>4.4</td>
<td>4.6</td>
<td>4.6</td>
<td>4.9</td>
<td>5.0</td>
<td>5.4</td>
</tr>
<tr>
<td>Water and other transportation</td>
<td>3.7</td>
<td>3.6</td>
<td>3.4</td>
<td>3.7</td>
<td>3.4</td>
<td>3.7</td>
<td>4.0</td>
<td>3.8</td>
</tr>
<tr>
<td>Total Transportation</td>
<td>8.6</td>
<td>8.4</td>
<td>8.1</td>
<td>8.6</td>
<td>8.5</td>
<td>9.3</td>
<td>9.8</td>
<td>10.6</td>
</tr>
<tr>
<td>Community and regional development</td>
<td>2.6</td>
<td>3.0</td>
<td>5.0</td>
<td>5.7</td>
<td>5.5</td>
<td>5.3</td>
<td>6.6</td>
<td>7.2</td>
</tr>
<tr>
<td>Education, training, employment and social services:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td>3.8</td>
<td>4.3</td>
<td>4.5</td>
<td>5.4</td>
<td>11.7</td>
<td>17.2</td>
<td>19.2</td>
<td>17.5</td>
</tr>
<tr>
<td>Training, employment and social services</td>
<td>1.7</td>
<td>1.9</td>
<td>2.3</td>
<td>4.2</td>
<td>9.2</td>
<td>12.3</td>
<td>14.6</td>
<td>14.2</td>
</tr>
<tr>
<td>Total Education, training, employment and social services</td>
<td>5.6</td>
<td>6.2</td>
<td>6.8</td>
<td>9.6</td>
<td>20.9</td>
<td>29.5</td>
<td>33.8</td>
<td>31.7</td>
</tr>
</tbody>
</table>
Google Hacking

- Advanced Operators “Intitle:”
  - Intitle: search_term
  - Find search term within the title of a Webpage
  - Allintitle: search_term1 search_term2 searchTerm3
  - Find multiple search terms in the Web pages with the title that includes all these words
  - These operators are specifically useful to find the directory lists
  - Example:

    Find directory list:
    Intitle: Index.of “parent directory”
## Index of /images

<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>29-Jul-2004 16:36</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Actions/</td>
<td>12-Dec-2003 14:44</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Animation/</td>
<td>07-Aug-2004 12:18</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Balls/</td>
<td>12-Dec-2003 14:44</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Box/</td>
<td>12-Dec-2003 14:44</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>ButSmall/</td>
<td>12-Dec-2003 14:44</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Buttons/</td>
<td>12-Dec-2003 14:44</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Diamonds/</td>
<td>12-Dec-2003 14:44</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>FancyLines/</td>
<td>12-Dec-2003 14:44</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Icons/</td>
<td>12-Dec-2003 14:44</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Images.html</td>
<td>12-Dec-2003 14:30</td>
<td>10k</td>
<td>-</td>
</tr>
<tr>
<td>Images.m4</td>
<td>16-Apr-2002 20:25</td>
<td>14k</td>
<td>-</td>
</tr>
</tbody>
</table>
Google Hacking

• Advanced Operators “Inurl:”
  – Inurl: search_term
  – Find search term in a Web address
  – Allinurl: search_term1 search_term2 search_term3
  – Find multiple search terms in a Web address
  – Examples:
    Inurl: cgi-bin
    Allinurl: cgi-bin password
Web Results 1 - 10 of about 44,400 for allinurl:cgi-bin password. (0.68 seconds)

Index of /dda/cgi-bin/password
Index of /dda/cgi-bin/password. Name Last modified
Size Description Parent directory Empty directory
www.cib.nig.ac.jp/dda/cgi-bin/password - 1k - Cached - Similar pages

Password protector dirs free web hosting cgi-bin at ncsm.org
More search results. Password protector dirs free web hosting cgi-bin info. ... Lot of information about dirs hosting protector password cgi-bin web free. ...
www.ncsm.org/.../password-protector-dirs-free-web-hosting-cgi-bin.html - 4k - Cached - Similar pages
Advanced Operators “Intext:”

- Intext: search_term
- Find search term in the text body of a document.
- Allintext: search_term1 search_term2 search_term3
- Find multiple search terms in the text body of a document.
- Examples:
  - Intext: Administrator login
  - Allintext: Administrator login
Administrator login

Username

password

submit
Google Hacking

- Advanced Operators: “Cache:”
  - Cache: URL
  - Find the old version of Website in Google cache
  - Sometimes, even the site has already been updated, the old information might be found in cache
  - Examples:
    Cache: www.gosecure.com
This is Google's cache of [Website URL] as retrieved on 31 Jul 2004 00:41:33 GMT. Google's cache is the snapshot that we took of the page as we crawled the web. The page may have changed since that time. Click here for the current page without highlighting. This cached page may reference images which are no longer available. Click here for the cached text only.
To link to or bookmark this page, use the following URL: [URL to link]

Google is not affiliated with the authors of this page nor responsible for its content.

Security that drives business results.
La sécurité au service de vos objectifs d’affaires.
Google Hacking

• Advanced Operators
  – <number1>..<number2>
  – Conduct a number range search by specifying two numbers, separated by two periods, with no spaces. Be sure to specify a unit of measure or some other indicator of what the number range represents
  – Examples:
    Computer $500..1000
    DVD player $250..350
Google Hacking

- Advanced Operators: “Daterange:”
  - Daterange: <start_date>-<end date>
  - Find the Web pages between start date and end date
  - Note: start_date and end date use the Julian date
  - The Julian date is calculated by the number of days since January 1, 4713 BC. For example, the Julian date for August 1, 2001 is 2452122
  - Examples:
    2004.07.10=2453196
    2004.08.10=2453258
  - Vulnerabilities date range: 2453196-2453258
Common **Vulnerabilities** and Exposures

Common **Vulnerabilities** and Exposures (CVE) is a list or dictionary that provides common names for publicly known information security **vulnerabilities** and ... www.cve.mitre.org/ - 13k - 8 Aug 2004 - Cached - Similar pages

**SANS Top 20 Vulnerabilities - The Experts Consensus**

... Pentagon hacking incident and the easy and rapid spread of the Code Red and NIMDA worms can be traced to exploitation of unpatched **vulnerabilities** on this list ...


**{ PivX Solutions, LLC }**

... It tries to exploit 7 different **vulnerabilities** to infect Windows machines, ranging from the Messenger Service buffer overrun, the uPnP overflow, LSASS as well ...


Sponsored Links

**Vulnerability Database**

Easy-to-use & validated info.
Free and updated daily.

www.secunia.com

**DIGEV 2004**

1st International Digital Evidence Web Conference. You're invited!

www.digev2004.com

**Network Security**

Free info on network security, software, and enterprise solutions
Google Hacking

• Advanced Operators “Link:”
  – Link: URL
  – Find the Web pages having a link to the specified URL
  – Related: URL
  – Find the Web pages that are “similar” to the specified Web page
  – info: URL
  – Present some information that Google has about that Web page
  – Define: search_term
  – Provide a definition of the words gathered from various online sources
  – Examples:
    Link: gosecure.ca
    Related: gosecure.ca
    Info: gosecure.ca
Information security is about people

By Robert Masse
Special to Globe and Mail Update

Front Lines is a guest viewpoint section offering perspectives on current issues and events from people working on the front lines of Canada's technology industry. Robert Masse is the president of GoSecure Inc., a Montreal information security services firm, and a former security consultant for KPMG.

One morning I pulled on hat and sweater bearing the logo of a well-known telecom company, printed up a fake work order, and headed off to the offices of one of my clients.
GoSecure

Google can show you the following information for this URL:

- Show Google’s cache of www.gosecure.ca
- Find web pages that are similar to www.gosecure.ca
- Find web pages that link to www.gosecure.ca
- Find web pages that contain the term "www.gosecure.ca"
Tip: Try removing quotes from your search to get more results.

Definitions of **Network Security** on the Web:

Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. Network security includes providing for data integrity.

[www.tsl.state.tx.us/id/pubs/compsecurity/glossary.html](http://www.tsl.state.tx.us/id/pubs/compsecurity/glossary.html)

Security procedures and controls that protect a network from: (a) unauthorized access, modification, and information disclosure; and (b) physical impairment or destruction.


Managing the physical and logical accessibility of your network resources. Physical includes safeguarding the actual equipment; logical includes controlling customers' access to network resources.

Advanced Operators “phonebook:”
- Phonebook
- Search the entire Google phonebook
- rphonebook
- Search residential listings only
- bphonebook
- Search business listings only
- Examples:
  Phonebook: robert las vegas (robert in Las Vegas)
  Phonebook: (702) 944-2001 (reverse search, not always work)
  The phonebook is quite limited to U.S.A
### Business Phonebook

<table>
<thead>
<tr>
<th>Business Name</th>
<th>Address</th>
<th>Phone Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Century Vision Center, <strong>Robert</strong> Pearson Od</td>
<td>Las Vegas, NV 89101</td>
<td>(702) 944-2001, Yahoo Maps, MapQuest</td>
</tr>
<tr>
<td>Eob, Head Start Centers, <strong>Robert</strong> Jones Gardens</td>
<td>Las Vegas, NV 89115</td>
<td>(702) 433-3770, Yahoo Maps, MapQuest</td>
</tr>
<tr>
<td>Clark County Of, Constable <strong>Robert</strong> Bobby G Gronauer</td>
<td>Las Vegas, NV 89101</td>
<td>(702) 385-2436, Yahoo Maps, MapQuest</td>
</tr>
<tr>
<td>Clark County Of, Constable <strong>Robert</strong> Bobby G Gronauer, Las Vegas Township</td>
<td>Las Vegas, NV 89101</td>
<td>(702) 455-4099, 309 S 3rd St, Yahoo Maps, MapQuest</td>
</tr>
<tr>
<td>American Family Insurance, Career Opportunities, Harrison <strong>Robert</strong></td>
<td>Las Vegas, NV 89109</td>
<td>(702) 732-4708, Yahoo Maps, MapQuest</td>
</tr>
</tbody>
</table>

### Residential Phonebook

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Phone Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Robert</strong></td>
<td>Las Vegas, NV 89121</td>
<td>(702) 433-6314, Yahoo Maps, MapQuest</td>
</tr>
<tr>
<td>Enrique <strong>Robert</strong></td>
<td>Las Vegas, NV 89102</td>
<td>(702) 792-9312, Yahoo Maps, MapQuest</td>
</tr>
<tr>
<td>F S <strong>Robert</strong></td>
<td>Las Vegas, NV 89101</td>
<td>(702) 631-2034, Yahoo Maps, MapQuest</td>
</tr>
<tr>
<td>Howard <strong>Robert</strong></td>
<td>Las Vegas, NV 89101</td>
<td>(702) 760-6896, Yahoo Maps, MapQuest</td>
</tr>
</tbody>
</table>

**More business listings... (Removal info)**
Century Vision Center, Robert Pearson Od - (702) 944-2001 - Las Vegas, NV 89101 - Yahoo! Maps - MapQuest

Century Vision Center, Ronald Dutton Od - (702) 944-2001 - Las Vegas, NV 89101 - Yahoo! Maps - MapQuest

Century Vision Center - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - Yahoo! Maps - MapQuest

Century Vision Center, Michael Crutchfield Od - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - Yahoo! Maps - MapQuest

Cohen David B MD - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - Yahoo! Maps - MapQuest

Crutchfield Michael Od - (702) 944-2001 - 8230 W Sahara Ave Infocus, Las Vegas, NV 89101 - Yahoo! Maps - MapQuest

Dutton Ronald Od - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - Yahoo! Maps - MapQuest

Somers William Od - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - Yahoo! Maps - MapQuest
Google, Friend or Enemy?

- Google is everyone’s best friend (yours or hackers)
- Information gathering and vulnerability identification are the tasks in the first phase of a typical hacking scenario
- Passitive, stealth and huge data collection
- Google can do more than search
- Have you used Google to audit your organization today?
Google Hacking

- What can Google can do for a hacker?
  - Search sensitive information like payroll, SIN, even the personal email box
  - Vulnerabilities scanner
  - Transparent proxy
Google Hacking

- Salary
  - Salary filetype: xls site: edu
<table>
<thead>
<tr>
<th>Desired Salary Action</th>
<th>Enter Base Salary</th>
<th>Timebase or Adjustment</th>
<th>Adjusted Salary</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full-Time to Part-time AY</td>
<td>$6,000</td>
<td>1</td>
<td>$3,600.00</td>
<td>Base Salary X Timebase</td>
</tr>
<tr>
<td>Full-Time to Part-Time 12 month</td>
<td>$6,900</td>
<td>1</td>
<td>$4,140.00</td>
<td>Base Salary X Timebase</td>
</tr>
<tr>
<td>AY to 12 Month (15% Increase)</td>
<td>$6,000</td>
<td>+15.0%</td>
<td>$6,900.00</td>
<td>Base Salary X 1.15</td>
</tr>
<tr>
<td>12 Month to AY (Minus 15%)</td>
<td>$6,900</td>
<td>-15.0%</td>
<td>$6,000.00</td>
<td>Base Salary divided by 1.15</td>
</tr>
<tr>
<td>Difference-in-Pay Leave (7/1/02)</td>
<td>$6,000</td>
<td>-$3035</td>
<td>$2,965.00</td>
<td>Base Salary minus minimum of Rank 2</td>
</tr>
</tbody>
</table>
Google Hacking

- Security social insurance number
  - Intitle: Payroll intext: ssn filetype: xls site: edu
<table>
<thead>
<tr>
<th>Name</th>
<th>SSN</th>
<th>Rate</th>
<th>Worked</th>
<th>Worked</th>
<th>Pay</th>
<th>Tax</th>
<th>Tax</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kristy Cole</td>
<td>071-74-1069</td>
<td>12.50</td>
<td>26.0</td>
<td>0.0</td>
<td>325.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jose Herrera</td>
<td>031-57-4273</td>
<td>11.75</td>
<td>40.0</td>
<td>3.0</td>
<td>522.88</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brooke Hoover</td>
<td>382-24-77</td>
<td>14.20</td>
<td>22.0</td>
<td>0.0</td>
<td>312.40</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Google Hacking

• Security Social Insurance Number
  – Payroll intext: Employee intext: ssn  iletype: xls
<table>
<thead>
<tr>
<th>Employee #1</th>
<th>Time Card</th>
<th>Employee #4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Number: 521-32-0678</td>
<td>Social Security Number: 521-32-0678</td>
<td></td>
</tr>
<tr>
<td>Status: Single</td>
<td>Exemptions: 0</td>
<td>Marital Status: Single</td>
</tr>
<tr>
<td>Deductions:</td>
<td>Hospital: $15.00</td>
<td>Other: $25.00</td>
</tr>
</tbody>
</table>
Google Hacking

• Financial Information
  – Filetype: xls “checking account” “credit card” -intext: Application -intext: Form (only 39 results)
<table>
<thead>
<tr>
<th>Date</th>
<th>Amount</th>
<th>Description</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/6/99</td>
<td>1350.00</td>
<td>Mortgage payment</td>
<td>11150.00</td>
</tr>
<tr>
<td>7/6/99</td>
<td>1236.82</td>
<td>Car insur</td>
<td>9913.18</td>
</tr>
<tr>
<td>7/10/99</td>
<td></td>
<td>OTC Deposits</td>
<td>10258.18</td>
</tr>
<tr>
<td>7/13/99</td>
<td>16.00</td>
<td>Internet Connection</td>
<td>10242.18</td>
</tr>
<tr>
<td>7/13/99</td>
<td>211.36</td>
<td>Pedernales electric</td>
<td>10030.82</td>
</tr>
<tr>
<td>7/13/99</td>
<td></td>
<td>OTC Deposits</td>
<td>11016.38</td>
</tr>
<tr>
<td>7/14/99</td>
<td>54.21</td>
<td>SW Bell Tel</td>
<td>10962.17</td>
</tr>
<tr>
<td>7/15/99</td>
<td>315.00</td>
<td>Flying trip to New Orleans 7 hrs @ $45</td>
<td>10647.17</td>
</tr>
</tbody>
</table>
Google Hacking

- Financial Information
  - Intitle: “Index of” finances.xls (9)
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Amount</th>
<th>Type</th>
<th>Note</th>
<th>Item breakdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/27</td>
<td>Car service for flashing lights</td>
<td>$69.50</td>
<td>Debit - Temporary Payment</td>
<td>Grocery</td>
<td>$0.00</td>
</tr>
<tr>
<td>5/27</td>
<td>Dad's repayment for car service</td>
<td>$4.60</td>
<td>Cash</td>
<td>Personal</td>
<td>$705.00</td>
</tr>
<tr>
<td>5/30</td>
<td>Shampoo and fish tank tubing</td>
<td>$25.00</td>
<td>Check</td>
<td>Personal</td>
<td>Books</td>
</tr>
<tr>
<td>5/31</td>
<td>First Pres offering through May</td>
<td>$75.00</td>
<td>Check</td>
<td>Personal</td>
<td>Transportation</td>
</tr>
<tr>
<td>6/7</td>
<td>Gas for Rachel's car</td>
<td>$27.00</td>
<td>Check</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>6/5</td>
<td>Dinner at Brat Stop w/ Mom and Dad</td>
<td>$35.20</td>
<td>Debit</td>
<td>Dinner</td>
<td>Gifts</td>
</tr>
<tr>
<td>6/6</td>
<td>Kitten supplies</td>
<td>$256.20</td>
<td>Debit</td>
<td>Personal</td>
<td>Non-PSU</td>
</tr>
<tr>
<td>6/8</td>
<td>Plane ticket to NYC</td>
<td>$7,244.00</td>
<td>Debit</td>
<td>Transportation</td>
<td>Misc</td>
</tr>
<tr>
<td>6/10</td>
<td>Reservation deposit for Tuckaway Heights</td>
<td>$100.00</td>
<td>Check</td>
<td>Apartment</td>
<td>Total</td>
</tr>
<tr>
<td>6/12</td>
<td>Metra ticket to Chicago</td>
<td>$5.00</td>
<td>Cash</td>
<td>Transportation</td>
<td></td>
</tr>
<tr>
<td>6/12</td>
<td>Food at Blues Fest</td>
<td>$3.50</td>
<td>Cash</td>
<td>Dining</td>
<td></td>
</tr>
<tr>
<td>6/12</td>
<td>Blues Fest keychain</td>
<td>$5.00</td>
<td>Cash</td>
<td>Personal</td>
<td></td>
</tr>
<tr>
<td>6/12</td>
<td>Dinner at Giordano's w/ Joy, Neighbor, Vince</td>
<td>$10.00</td>
<td>Cash</td>
<td>Dining</td>
<td></td>
</tr>
<tr>
<td>6/12</td>
<td>Gas for Rachel's car</td>
<td>$15.00</td>
<td>Debit</td>
<td>Transportation</td>
<td></td>
</tr>
<tr>
<td>6/15</td>
<td>Garage sale proceeds from Mom</td>
<td>$25.00</td>
<td>Check</td>
<td>Cash Gift</td>
<td></td>
</tr>
<tr>
<td>6/15</td>
<td>Initial shots for Cat</td>
<td>$29.00</td>
<td>Check</td>
<td>Cat</td>
<td></td>
</tr>
<tr>
<td>6/15</td>
<td>Deposit for Tuckaway Heights (minus reserv. dep.)</td>
<td>$305.00</td>
<td>Check</td>
<td>Apartment</td>
<td></td>
</tr>
<tr>
<td>6/16</td>
<td>2-year Vine Line subscription renewal</td>
<td>$44.00</td>
<td>Check</td>
<td>Personal</td>
<td></td>
</tr>
</tbody>
</table>

Check reimbursement is still a deposit
withdrawal considered part of deposit when cash back is taken

Separate PSFCU and 5/3 somehow!!!
Google Hacking

• Personal Mailbox
  – Intitle: Index.of inurl: Inbox (456) (mit mailbox)
<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>17-Mar-2004 15:00</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>#1</td>
<td>17-Mar-2004 14:21</td>
<td>2k</td>
<td></td>
</tr>
<tr>
<td>#10</td>
<td>17-Mar-2004 14:45</td>
<td>2k</td>
<td></td>
</tr>
<tr>
<td>#11</td>
<td>17-Mar-2004 14:45</td>
<td>3k</td>
<td></td>
</tr>
<tr>
<td>#12</td>
<td>17-Mar-2004 14:45</td>
<td>3k</td>
<td></td>
</tr>
<tr>
<td>#13</td>
<td>17-Mar-2004 14:45</td>
<td>2k</td>
<td></td>
</tr>
<tr>
<td>#14</td>
<td>17-Mar-2004 14:34</td>
<td>10k</td>
<td></td>
</tr>
<tr>
<td>#15</td>
<td>17-Mar-2004 14:45</td>
<td>3k</td>
<td></td>
</tr>
<tr>
<td>#16</td>
<td>17-Mar-2004 14:34</td>
<td>51k</td>
<td></td>
</tr>
<tr>
<td>#17</td>
<td>17-Mar-2004 15:16</td>
<td>2k</td>
<td></td>
</tr>
<tr>
<td>#18</td>
<td>17-Mar-2004 15:16</td>
<td>2k</td>
<td></td>
</tr>
<tr>
<td>#19</td>
<td>17-Mar-2004 15:16</td>
<td>3k</td>
<td></td>
</tr>
<tr>
<td>#2</td>
<td>17-Mar-2004 14:21</td>
<td>2k</td>
<td></td>
</tr>
<tr>
<td>#20</td>
<td>17-Mar-2004 15:16</td>
<td>3k</td>
<td></td>
</tr>
<tr>
<td>#21</td>
<td>17-Mar-2004 15:16</td>
<td>2k</td>
<td></td>
</tr>
<tr>
<td>#22</td>
<td>17-Mar-2004 14:58</td>
<td>10k</td>
<td></td>
</tr>
<tr>
<td>#23</td>
<td>17-Mar-2004 15:16</td>
<td>3k</td>
<td></td>
</tr>
<tr>
<td>#24</td>
<td>17-Mar-2004 14:58</td>
<td>51k</td>
<td></td>
</tr>
<tr>
<td>#25</td>
<td>17-Mar-2004 15:26</td>
<td>2k</td>
<td></td>
</tr>
</tbody>
</table>
Google Hacking

• Personal Mailbox
  – After several clicks, got the private email messages
Return-Path: <kspivey@ux1.sp.cs.cmu.edu>
Delivered-To: mws@ux1.sp.cs.cmu.edu
Received: from EDRC.CMU.EDU ([128.2.203.42]) by ux1.sp.cs.cmu.edu id aal1848:
           17 Mar 2004 7:15 EST
Received: from MX5.andrew.cmu.edu ([128.2.10.116]) by edrc.cmu.edu id aa04183:
           17 Mar 2004 7:14 EST
Received: from mx5.toho-u.ac.jp (c=67-166-49-63.client.comcast.net [67.166.49.63])
           by mx5.andrew.cmu.edu (8.12.10/8.12.10) with SMTP id i2HEC0mN017771
           for <mws@andrew.cmu.edu>; Wed, 17 Mar 2004 07:14:09 -0500
Message-ID: <97d00c0d0c9f$7356556f30$a9bc033d@med.toho-u.ac.jp>
From: "Kelvin Spivey" <kspivey@ux1.sp.cs.cmu.edu>
To: mws@andrew.cmu.edu
Subject: More efficient than viagra
MIME-Version: 1.0
Content-Type: text/html:
   charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
X-MIME-Autoconverted: from 8bit to quoted-printable by mx5.andrew.cmu.edu id i2HEC0mN017771
X-UIDL: becfd0f4e73d42d3d94cda6e8b477f3

<BODY><P>Generic cialis (Regalis), at cheap prices.<BR>
Most places charge $20, we charge $5. Quite a difference.<BR></P>
Cialis is known as a Super-V=EDagra or Weekend-V=EDagra because its effects start sooner and last much longer.<BR></P>
<P>Your easy-to-use solution is here: <A HREF="http://www.mega-health.net/cia/?oxygen">http://www.mega-health.net/cia/?oxygen</A></P>
<P>The link below is for those who hate spam...</P>
</BODY>
Google Hacking

- Personal Mailbox
  - Intitle: Index.of inurl: Inbox (inurl: User OR inurl: Mail) (220)
Google Hacking

- Confidential Files
  - “not for distribution” confidential (1,760)
A ONCE Network Proposal to CN

Proposal: “Executive Summit Series” focused on the Business Implications of Web Services.

SUMMARY
Google Hacking

- Confidential Files
  - “not for distribution” confidential filetype: pdf
    (marketing info) (456)
An Introduction to AIMMS

Clearing the US Energy Market

part II/II

Gertjan de Lange
Chief Commercial Officer

Peter Nieuwesteeg
AIMMS Consultant at Areva
Google Hacking

- OS Detection
- Use the keywords of the default installation page of a Web server to search.
- Use the title to search
- Use the footer in a directory index page
Google Hacking

- OS Detection-Windows
  - “Microsoft-IIS/5.0 server at”
Index of /legislacoes/parecer_jurid_arquivos

<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>08-Mar-2004 16:37</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>filelist.xml</td>
<td>03-Oct-2002 10:10</td>
<td>1k</td>
<td></td>
</tr>
<tr>
<td>header.htm</td>
<td>03-Oct-2002 10:10</td>
<td>4k</td>
<td></td>
</tr>
<tr>
<td>image001.gif</td>
<td>03-Oct-2002 10:10</td>
<td>11k</td>
<td></td>
</tr>
</tbody>
</table>

Microsoft-IIS/5.0 Server at www. [IP Address] Port 80
Google Hacking

- OS Detection - Windows
  - Default web page?
  - Intitle: “Welcome to Windows 2000 Internet Services”
Welcome to IIS 5.0
Internet Information Services (IIS) for Microsoft Windows 2000 brings the power of Web computing to Windows. With IIS, you can easily share files and printers and create applications to securely publish information to improve the way your organization works. IIS is a secure platform for building and deploying eCommerce solutions. IIS also makes it easy to bring mission-critical business applications to the Web.

Windows 2000 with IIS scales to meet your needs. You can:

- Set up a personal Web server.
- Share information within your team.
- Access databases.
- Create an enterprise intranet.

IIS integrates proven Internet standards with Windows, so that using the Web does not mean

Integrated Management
You can manage IIS through the Windows 2000 Computer Management console, or by using scripting. If you have installed Windows 2000 Server or Windows 2000 Advanced Server, the Administration Web site can also be used to manage IIS.

You can also right-click on a directory, and you can share its contents via the Web, as well as configure the most common IIS settings.

Online Documentation
The award-winning IIS online documentation includes an index, full-text search, and printing by node or by individual topic. You can:

- Get help with tasks.
- Learn about server operation.
- Consult reference material.
Google Hacking

- OS Detection – Apache 1.3.11-1.3.26
  - Intitle: Test.Page.for.Apache seeing.this.instead
It Worked!

If you can see this, it means that the installation of the Apache software on this system was successful. You may now add content to this directory and replace this page.

If you are seeing this instead of the content you expected, please contact the administrator of the site involved. If you send mail about this to the authors of the Apache software, who almost certainly have nothing to do with this site, your message will be ignored.

The Apache documentation has been included with this distribution.

You are free to use the image below on an Apache-powered web server. Thanks for using Apache!
Google Hacking

- OS Detection-Apache SSL enable
  - Intitle: Test.page “SSL/TLS-aware” (127)
Hey, it worked!
The SSL/TLS-aware Apache webserver was successfully installed on this website.

If you can see this page, then the people who own this website have just installed the Apache Web server software and the Apache Interface to OpenSSL (mod_ssl) successfully. They now have to add content to this directory and replace this placeholder page, or else point the server at their real content.

ATTENTION!
If you are seeing this page instead of the site you expected, please contact the administrator of the site involved. (Try sending mail to <webmaster@domain>.) Although this site is running the Apache software it almost certainly has no other connection to the Apache Group, so please do not send mail about this site or its contents to the Apache authors. If you do, your message will be ignored.

The Apache online documentation has been included with this distribution. Especially also read the mod_ssl User Manual carefully.

Your are allowed to use the images below on your SSL-aware Apache Web server.
Thanks for using Apache, mod_ssl and OpenSSL.
Google Hacking

• Search Passwords
  – Search the well known password filenames in URL
  – Search the database connection files or configuration files to find a password and username
  – Search specific username file for a specific product
• Search Passwords
  – Inurl: etc inurl: passwd
MiniUnix/./etc/.passwd

Find at most 5 related files. Search

including files from this version of Unix.

root::0:1::/
sys:2:2::/usr/sys:
bin:3:1::/bin:
c:10:1::/usr/c:
man:3:1::/usr/man:
adm:3:1::/usr/adm:
s1:3:1::/src/source/s1:
s2:3:1::/src/source/s2:
s3:3:1::/src/source/s3:
s4:3:1::/src/source/s4:
s5:3:1::/src/source/s5:
s6:3:1::/src/source/s6:
s7:3:1::/src/source/s7:
s8:3:1::/src/source/s8:
#
root::0:0:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:0:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:0:System &:/usr/sbin/nologin
bin:*:3:7:0:0:Binaries Commands and Source:/usr/sbin/nologin
tty:*:4:65533:0:0:Tty Sandbox:/usr/sbin/nologin
kmem:*:5:65533:0:0:KMem Sandbox:/usr/sbin/nologin
games:*:7:13:0:0:Games pseudo-user:/usr/games:/usr/sbin/nologin
news:*:8:8:0:0:News Subsystem:/usr/sbin/nologin
man:*:9:9:0:0:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:0:0:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:0:0:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:0:0:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:0:0:Bind Sandbox:/usr/sbin/nologin
proxy:*:62:62:0:0:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64:0:pflogd privsep user:/var/empty:/usr/sbin/nologin
uucp:*:66:66:0:0:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:0:0:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80:0:0:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
nobody:*:65534:65534:0:0:Unprivileged user:/nonexistent:/usr/sbin/nologin
Google Hacking

- Search Passwords
  - Intitle: “Index of..etc” passwd
<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>01-Nov-2002</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>group</td>
<td>31-Oct-2002</td>
<td>1k</td>
<td>-</td>
</tr>
<tr>
<td>localtime</td>
<td>30-Oct-2002</td>
<td>1k</td>
<td>-</td>
</tr>
<tr>
<td>nsswitch.conf</td>
<td>31-Oct-2002</td>
<td>2k</td>
<td>-</td>
</tr>
<tr>
<td>passwd</td>
<td>31-Oct-2002</td>
<td>1k</td>
<td>-</td>
</tr>
</tbody>
</table>

Apache/1.3.24 Server at ftp.cs.concordia.ca Port 80
Google Hacking

- Search Passwords
  - "# -FrontPage-" inurl: service.pwd (then crack it)
# -FrontPage-
ekendall:bYld1Sr73NLKo
louisa:5zm94d7cdDFiQ
Google Hacking

- Search Passwords
  - Inurl: admin.pwd filetype: pwd
mdneauto:DglNlhTHy9Sis:2025:100:Michael Floodman:/home/mdneauto:/bin/false
Google Hacking

- Search Passwords
  - Filetype: inc dbconn
var $ERR_DESC; //Oracle Error Desc.

var $str;

function my_conn() { //Create database connection using bg-id
    $this->i = 0;
    $this->c = @$OCIpllogon ("poweroftwo", "fourby10", "prod") or die ("Could not connect");
}

function my_err() {
    $err = OCIError($this->sqlstmt);
    $this->ERR = $err["code"];  
    $this->ERR_DESC = $err["message"];}
Google Hacking

- Search Passwords
  - Filetype: inc intext: mysql_connect
<?php
require_once("common.inc") ;

function dbConnect() {
    $dbHandle = @mysql_connect("localhost", "rbrooks", "2167") ;
    if (!$dbHandle) {
        showDBError("Unable to connect to the database management system") ;
        exit() ;
    }
    if (!mysql_select_db("tmob")) {
        showDBError("Unable to connect to the TexasMob database") ;
        exit() ;
    }
}

//
Google Hacking

- Search Passwords
  - Filetype: ini +ws_ftp +pwd (get the encrypted passwords)
LONGDATE=0
sndaf=C:\WSFTP\error.wav
sndcs=C:\WSFTP\connect.wav
sndcf=C:\WSFTP\error.wav
sndts=C:\WSFTP\complete.wav
sndtf=C:\WSFTP\error.wav
soundflags=30
LSORT=1
RSORT=1
UseFindExec=0
balloon=0
DateFmt=0
RETAIN=1

[]
HOST=
UID=anonymous
TIMEOFFSET=0

[Netconnect-Public]
HOST=seq.clan.lib.ri.us
UID=getpfw
PWD=V213D0609B1CA8B0AA8B65AB6FFEA4575A2796B72AC6E
LOCDIR=c:\
TIMEOFFSET=0
rdir0="/export/ftp/pub"
ldir0=c:\

[MARCHIVE]
HOST=ftp.marcive.com
UID=anonymous
PWD=V5DBA8DDA00A5795C15B248A18750A1D7A567706DAF7C4A7B9DAA39A3AFA7B140ADAF7673BAB645BDC3
TIMEOFFSET=0
DIR="/output/ftp/clfhdtth"
rdir0="/output/ftp/clfhdtth"
rdir1="/output"
ldir0=c:\
TYPE=6016
rdir2="/"
LOCDIR=c:\
ldir1=C:\CDR\Disc1\wsftp
Google Hacking

- Search Passwords
  - Filetype: log inurl: “password.log”
name: = "jbhunt"; password: = "jbhunt"; URL: = "http://home.nc.rr ..."
name: = "jbhunt"; password: = "jbhunt"; URL: = "http://home.nc.rr.com/clay123/ref23.html";
Beth Haas name: = "BHaas"; password: = "Beth Haas"; URL: = "http ...
home.nc.rr.com/clay123/password.log - 2k - Supplemental Result - Cached - Similar pages

name: = "tad"; password: = "homepage"; URL: = "<a href="http://www ..."
END_FILE
dob.tnc.edu.tw/authorHD/1/password.log - 1k - Cached - Similar pages

name: = "momo"; password: = "momo"; URL: = "password.htm ..."
name: = "momo"; password: = "momo"; URL: = "password.htm"; END_FILE
jason123.uhome.net/password.log - 1k - Supplemental Result - Cached - Similar pages

name: = "23202"; password: = "ilgt"; URL: = "address.htm"; name ...
name: = "23202"; password: = "ilgt"; URL: = "address.htm"; name: = "23203"; password: = "ilgt"; URL: = "address.htm"; name: = "23204"; password: = "ilgt"; URL ...
www.lib.nchu.edu.tw/groups/group21/password.log - 9k - Cached - Similar pages

name: = "admin"; password: = "computer"; URL: = "http://members ...
name: = "admin"; password: = "computer"; URL: = "http://members.tripod.de/Rick_Cooper/fr.htm";
name: = "paul"; password: = "papst"; URL: = "http://members ...
mitglied.lycos.de/Rick_Cooper/mnr/password.log - 2k - Supplemental Result - Cached - Similar pages
Google Hacking

• Search Username
Top 1 of 1 Total Usernames

<table>
<thead>
<tr>
<th>#</th>
<th>Hits</th>
<th>Files</th>
<th>KBytes</th>
<th>Visits</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0.00%</td>
<td>16</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

Top 15 of 2514 Total User Agents

<table>
<thead>
<tr>
<th>#</th>
<th>Hits</th>
<th>User Agent</th>
</tr>
</thead>
</table>
Google Hacking

- License Key
  - Filetype: lic lic intext: key (33) (license key)
Google Hacking

- Cookies Syntax
  - Filetype: inc inc intext: setcookie -cvs -examples -sourceforge -site: php.net (120) (cookie schema)
<?
//Cookie for name, web and email in news-trnk v1.2.2 tnka@linux-sottises.net
if($param_name && $save!="1"){
    $name=$param_name;
    $email=$param_email;
    $web=$param_web;
}elseif($save=="1"){
    setcookie("param_name", "", time()-100000);
    setcookie("param_email", "", time()-100000);
    setcookie("param_web", "", time()-100000);
    setcookie("param_name", $name, time()+315360000);
    setcookie("param_email", $email, time()+315360000);
    setcookie("param_web", $web, time()+315360000);
}
Google Hacking

- Sensitive Directories Listing
  - Powerful buzz word: Index of
  - Search the well known vulnerable directories names
Google Hacking

- Sensitive Directories Listing
  - “index of cgi-bin” (3590)
Index of /cgi-bin/

<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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>forum-admin.pl</td>
<td>18-Jan-2000 10:24</td>
<td>13K</td>
<td></td>
</tr>
<tr>
<td>forum.pl</td>
<td>18-Jan-2000 10:24</td>
<td>18K</td>
<td></td>
</tr>
<tr>
<td>tutkimus/</td>
<td>16-Oct-2002 09:36</td>
<td>4K</td>
<td></td>
</tr>
</tbody>
</table>
Google Hacking

- Sensitive Directories Listing
  - Intitle: “Index of” cfide (coldfusion directory)
Index of /CFIDE/

<table>
<thead>
<tr>
<th>Directory</th>
<th>Size</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application.cfm</td>
<td>199</td>
<td>05/19/02 07:39 PM</td>
</tr>
<tr>
<td>administrator/</td>
<td>dir</td>
<td>08/21/03 06:07 PM</td>
</tr>
<tr>
<td>classes/</td>
<td>dir</td>
<td>08/21/03 06:07 PM</td>
</tr>
<tr>
<td>componentutils/</td>
<td>dir</td>
<td>08/21/03 06:07 PM</td>
</tr>
<tr>
<td>debug/</td>
<td>dir</td>
<td>08/21/03 06:07 PM</td>
</tr>
<tr>
<td>install.cfm</td>
<td>4038</td>
<td>05/19/02 07:39 PM</td>
</tr>
<tr>
<td>probe.cfm</td>
<td>8061</td>
<td>05/19/02 07:39 PM</td>
</tr>
<tr>
<td>scripts/</td>
<td>dir</td>
<td>08/21/03 06:07 PM</td>
</tr>
</tbody>
</table>
Google Hacking

- Sensitive Directories Listing
  - Intitle: index.of.winnt
GoSecure Inc.

03/07/2007
Google Hacking

• Sensitive Directories Listing
  – Intitle: “index of” iissamples (dangerous iissamples) (32)
## Index of /glides/iissamples/homepage

<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>13-Nov-2003 11:56</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>WS_FTP.LOG</td>
<td>13-Jan-2001 18:31</td>
<td>4k</td>
<td></td>
</tr>
<tr>
<td>bullet.gif</td>
<td>13-Jan-2001 18:31</td>
<td>1k</td>
<td></td>
</tr>
<tr>
<td>default.asp</td>
<td>13-Jan-2001 18:31</td>
<td>1k</td>
<td></td>
</tr>
<tr>
<td>file.gif</td>
<td>13-Jan-2001 18:31</td>
<td>1k</td>
<td></td>
</tr>
<tr>
<td>global.asa</td>
<td>13-Jan-2001 18:31</td>
<td>1k</td>
<td></td>
</tr>
<tr>
<td>guestbk.asp</td>
<td>13-Jan-2001 18:31</td>
<td>6k</td>
<td></td>
</tr>
<tr>
<td>myfiles.asp</td>
<td>13-Jan-2001 18:31</td>
<td>4k</td>
<td></td>
</tr>
<tr>
<td>signbook.asp</td>
<td>13-Jan-2001 18:31</td>
<td>7k</td>
<td></td>
</tr>
<tr>
<td>sub.inc</td>
<td>13-Jan-2001 18:31</td>
<td>9k</td>
<td></td>
</tr>
<tr>
<td>theme.inc</td>
<td>13-Jan-2001 18:31</td>
<td>1k</td>
<td></td>
</tr>
<tr>
<td>themes/</td>
<td>13-Nov-2003 11:56</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
Google Hacking

- Sensitive Directories Listing
  - Inurl: iissamples (1080)
The format of QUERY_STRING is invalid.
The format of QUERY_STRING is invalid.
Google Hacking

• Database Manipulation
  – Different database applications leave different signatures on the database files
Google Hacking

- Database Manipulation
  - “Welcome to phpMyAdmin” AND “Create new database” -intext: “No Priviledge” (find a page that might have privilege to update mysql)
Welcome to phpMyAdmin 2.5.7-pl1

MySQL 3.23.49 running on localhost as seven@localhost

MySQL
- Create new database [Documentation]
- Show processes [Documentation]
- Databases
- Export

phpMyAdmin
- Language (*) : English (en-iso-8859-1)
- phpMyAdmin documentation
- Official phpMyAdmin Homepage
  - [ChangeLog] [CVS] [Lists]

The $cfg['PmaAbsoluteUri'] directive MUST be set in your configuration file!
Google Hacking

- Database Manipulation
  - “Welcome to phpMyAdmin” AND “Create new database” (after several hits, we got this)
SQL-query on database **avbase2**:
Google Hacking

- Database Manipulation
  - “Select a database to view” intitle: “filemaker pro” (94) Filemaker
These FileMaker Pro databases are shared by IAC.

Select a database to view:

- piconelectures.FP3
- DIPENDENTIIAC.FP3
- newcnr.FP3
- preprintdb.FP3
- preprintiac.fp3
- pizzaiac.FP3
- Staff2.FP3
- financestaff.FP3
- registro.FP3
- tecnoareastaff.FP3
- SCIENTIFICCOMMITTEE.FP3
- STAFF.FP3
- preprintdb.FP3
- seminari.FP3
- quadernifinale.fp3
Google Hacking

- Database Manipulation
  - After several clicks and you can query the table
<table>
<thead>
<tr>
<th>Nome</th>
<th>Cognome</th>
<th>telefono</th>
<th>email</th>
<th>Paginaw</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rita</td>
<td>Abbondanza</td>
<td>+39-0688470276</td>
<td><a href="mailto:abbondanza@iac.rm.cnr.it">abbondanza@iac.rm.cnr.it</a></td>
<td></td>
</tr>
<tr>
<td>Massimiliano</td>
<td>Adamo</td>
<td>+39-0688470235</td>
<td><a href="mailto:adamo@iac.rm.cnr.it">adamo@iac.rm.cnr.it</a></td>
<td></td>
</tr>
<tr>
<td>Piero</td>
<td>Barone</td>
<td>+39-0688470237</td>
<td><a href="mailto:barone@iac.rm.cnr.it">barone@iac.rm.cnr.it</a></td>
<td></td>
</tr>
<tr>
<td>Massimo</td>
<td>Bernaschi</td>
<td>+39-0688470229</td>
<td><a href="mailto:massimo@iac.rm.cnr.it">massimo@iac.rm.cnr.it</a></td>
<td></td>
</tr>
<tr>
<td>Michiel</td>
<td>Bertsch</td>
<td>+39-064402627</td>
<td><a href="mailto:bertsch@iac.rm.cnr.it">bertsch@iac.rm.cnr.it</a></td>
<td></td>
</tr>
<tr>
<td>Stefano</td>
<td>Bianchini</td>
<td>+39-0688470255</td>
<td><a href="mailto:bianchini@iac.rm.cnr.it">bianchini@iac.rm.cnr.it</a></td>
<td></td>
</tr>
<tr>
<td>Massimiliano</td>
<td>Caramia</td>
<td>+39-0688470222</td>
<td><a href="mailto:caramia@iac.rm.cnr.it">caramia@iac.rm.cnr.it</a></td>
<td></td>
</tr>
<tr>
<td>Giuliana</td>
<td>Caringi</td>
<td>+39-0688470205</td>
<td><a href="mailto:direzio@iac.rm.cnr.it">direzio@iac.rm.cnr.it</a></td>
<td></td>
</tr>
</tbody>
</table>
Google Hacking

• Database Manipulation
  – “# Dumping data for table (username|user|users|password)” -site: mysql.com –cvs (289) (backup data of mysqldump)
Process_priv enum('N','Y') NOT NULL default 'N',
File_priv enum('N','Y') NOT NULL default 'N',
Grant_priv enum('N','Y') NOT NULL default 'N',
References_priv enum('N','Y') NOT NULL default 'N',
Index_priv enum('N','Y') NOT NULL default 'N',
Alter_priv enum('N','Y') NOT NULL default 'N',
Show_db_priv enum('N','Y') NOT NULL default 'N',
Super_priv enum('N','Y') NOT NULL default 'N',
Create_tmp_table_priv enum('N','Y') NOT NULL default 'N',
Lock_tables_priv enum('N','Y') NOT NULL default 'N',
Execute_priv enum('N','Y') NOT NULL default 'N',
Repl_slave_priv enum('N','Y') NOT NULL default 'N',
Repl_client_priv enum('N','Y') NOT NULL default 'N',
ssl_type enum('', 'ANY', 'X509', 'SPECIFIED') NOT NULL default '',
ssl_cipher blob NOT NULL,
x509_issuer blob NOT NULL,
x509_subject blob NOT NULL,
max_questions int(11) unsigned NOT NULL default '0',
max_updates int(11) unsigned NOT NULL default '0',
max_connections int(11) unsigned NOT NULL default '0',
PRIMARY KEY (Host,User)
) TYPE=MyISAM COMMENT='Users and global privileges';

-- Dumping data for table `user`

INSERT INTO user VALUES ('localhost', 'root', '', '', '', '', '', '', '', '', '', '', '', ',
INSERT INTO user VALUES ('localhost', 'typo3', '', '', '', '', '', '', '', '', '', '', '', '')
Database Manipulation
  – “# Dumping data for table (username|user|users|password)” –site: mysql.com -cvs
-- MySQL dump 8.22
--
-- Host: localhost  Database: cis233j
-- Server version 3.23.51-max-nt

Drop Database if exists cis233j;
Create Database cis233j;
use cis233j;

-- Table structure for table 'users'

CREATE TABLE users (    UserKey int(9) NOT NULL auto_increment,    UserName varchar(15) NOT NULL default '',    Password varchar(15) NOT NULL default '',    Active tinyint(1) default '1',    PRIMARY KEY (UserKey) ) TYPE=MyISAM;

-- Dumping data for table 'users'

INSERT INTO users VALUES (1,'Greg','biffle',1);
INSERT INTO users VALUES (2,'Doug','pbmaster',1);
INSERT INTO users VALUES (3,'Stevn','linuxmaster',1);
INSERT INTO users VALUES (4,'Skip','vpmaster',1);
Google Hacking

- Database Manipulation
  - “# Dumping data for table (username|user|users|password)” -site: mysql.com –cvs
INSERT INTO `user` VALUES (1, 'sarah', '3defa3cb554b108470027b017af8116', 'admin@actionpoint.net', 'Sarah', 'Coleman', 'sarah', '20040806092330', '20040806092514');
INSERT INTO `user` VALUES (2, 'sarah', '3defa3cb554b108470027b017af8116', 'sarah@kyelani.com', 'Sarah', 'Coleman', 'sarah', '20040806000223', '20040806004017');

# Table structure for table `user2collection`
#
CREATE TABLE `user2collection`(
`user_id` int(11) NOT NULL default '0',
`collection_id` int(11) NOT NULL default '0',
PRIMARY KEY (`user_id`, `collection_id`)
) TYPE=MyISAM COMMENT='Assign users to groups';

# Dumping data for table `user2collection`
#
INSERT INTO `user2collection` VALUES (1, 1);
INSERT INTO `user2collection` VALUES (2, 2);

There are two users in the database right now for testing, one admin (me) and one user (also me - in disguise)

Now when content is delivered, Harry's system checks for a permission named in table 'permission', which *seems* to have to go through four different tablas to get a true or false
Google Hacking

- Sensitive System Information
  - Network security reports have lists of vulnerabilities for your system
  - Configuration files often contain the application parameters inventory
Google Hacking

• Network Security Report (ISS)
  – “Network Host Assessment Report” “Internet Scanner” (iss report) (13)
Network Host Assessment Report

Name

Report Description

This report provides detailed network host configuration and vulnerability information. It identifies all services and vulnerabilities associated with each assessible system.

Session Name: R & D Section 6
File Name: Session2_000413
Comment: Weekly Scan

Session ID: 13
Template: Comprehensive
Termination Status: Finished

Scan Summary Information

Hosts Scanned: 3
Hosts Active: 3
Hosts Inactive: 0

Scan Start: 2000/04/13 18:15:20
Scan End: 2000/04/13 18:17:02
Elapsed: 00:01:42
Google Hacking

- Network Security Report (ISS)
  - “Host Vulnerability Summary Report” (ISS report) (25)
# Host Vulnerability Summary Report

**Report Description**

This report displays summary information detailing the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggests corrective action. Vulnerabilities are classified as high, medium, and low. High risk vulnerabilities are those which provide unauthorized access to the host, and possibly, the network.

<table>
<thead>
<tr>
<th>Session Name:</th>
<th>R &amp; D Section 6</th>
<th>Session ID:</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name:</td>
<td>Session2_000413</td>
<td>Template:</td>
<td>Comprehensive</td>
</tr>
<tr>
<td>Comment:</td>
<td>Weekly Scan</td>
<td>Termination Status:</td>
<td>Finished</td>
</tr>
</tbody>
</table>

## Scan Summary Information

- **Hosts Scanned:** 3
- **Hosts Active:** 3
- **Hosts Inactive:** 0
- **Scan Start:** 2000/04/13 18:15:20
- **Scan End:** 2000/04/13 18:17:02
- **Elapsed:** 00:01:42

<table>
<thead>
<tr>
<th>DNS Name</th>
<th>Host IP Address</th>
<th>Operating System</th>
<th>Vulnerability Name</th>
<th>Severity</th>
</tr>
</thead>
</table>

GoSecure Inc.
Google Hacking

- Network Security Report (nessus)
  - “This file was generated by Nessus” || intitle:”Nessus Scan Report” -site:nessus.org (185)
## Host List

<table>
<thead>
<tr>
<th>Host(s)</th>
<th>Possible Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>charlemagne.dyndns.org</td>
<td>Security hole(s) found</td>
</tr>
</tbody>
</table>

## Analysis of Host

<table>
<thead>
<tr>
<th>Address of Host</th>
<th>Port/Service</th>
<th>Issue regarding Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>charlemagne.dyndns.org</td>
<td>discard (9/tcp)</td>
<td>No Information</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>daytime (13/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>ftp (21/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>telnet (23/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>smtp (25/tcp)</td>
<td>Security notes found</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>time (37/tcp)</td>
<td>Security notes found</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>finger (79/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>www (80/tcp)</td>
<td>Security hole found</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>pop3 (110/tcp)</td>
<td>Security notes found</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>sunrpc (111/tcp)</td>
<td>Security notes found</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>general/tcp</td>
<td>Security hole found</td>
</tr>
<tr>
<td>charlemagne.dyndns.org</td>
<td>general/icmp</td>
<td>Security warning(s) found</td>
</tr>
</tbody>
</table>
Google Hacking

- Network Scanner Report (Snort)
  - “SnortSnarf alert page” (15,500)
SnortSnarf alert page

Source: 218.191.177.52: overview

SnortSnarf v020516.1

Signature section (3371) Top 20 source IPs Top 20 dest IPs

2558 such alerts found using input module SnortFileInput, with sources:

- /var/log/auth.log

Latest: 07:34:21 on 6/7/2004

19 different signatures are present for 218.191.177.52 as a source

- 1 instances of IMRN RTP Rad Login:
Google Hacking

- Network Security Report (Snort)
  - Intitle: “Analysis Console for Intrusion Databases”
    +intext:”by Roman Danyliw” inurl:acid/acid_main.php (13 results, acid alert database)
Added 40 alert(s) to the Alert cache

Queried on: Thu August 12, 2004 17:10:13
Database: snort@ (schema version: 106)

Sensors: 1
Unique Alerts: 116 (17 categories)
Total Number of Alerts: 5550

- Source IP addresses: 997
- Dest. IP addresses: 135
- Unique IP links 1138

- Source Ports: 3333
  - TCP (3126) UDP (254)
- Dest. Ports: 21
  - TCP (10) UDP (0)

Traffic Profile by Protocol

- TCP (86%)
- UDP (11%)
- ICMP (2%)
- Portscan Traffic (0%)

GoSecure Inc.
Google Hacking

- Configuration Files (robots.txt)
  - Robots.txt means to protect your privacy from crawlers
  - But allows you to determine the file system architecture
User-agent: *
Disallow:/cgi-bin
Disallow:/search
Disallow:/query.html
Disallow:/help
Disallow:/360pics/iraq
Disallow:/360pics/text
Disallow:/911/911day/iraq
Disallow:/911/911day/text
Disallow:/911/heroes/iraq
Disallow:/911/heroes/text
Disallow:/911/...
Google Hacking

• A vulnerable targets scanning example
  – Get the new vulnerabilities from advisory
  – Find the signature from vendor Website
  – Google search to find the targets
  – Perform further malicious actions
Google Hacking

• An advisory looks like…….
Smart Guest Book Database Content Disclosure Security Issue

Secunia Advisory: SA12401
Release Date: 2004-08-30

Critical: Moderately critical
Impact: Exposure of sensitive information
Where: From remote
Solution Status: Unpatched

Software: Smart Guest Book 2.x

Select a product and view a complete list of all Patched/Unpatched Secunia advisories affecting it.

Description:
A security issue has been reported in Smart Guest Book, which may allow malicious people to gain knowledge of sensitive information.

The problem is that the database file "SmartGuestbook.mdb" by default is accessible by anyone. This may disclose various information including the administrative username and password by downloading the file from an affected web site.

Solution:
Place the database file in a separate database directory and restrict access to it.

Provided and/or discovered by:
Security .Net Information

Please note: The information, which this Secunia Advisory is based upon, comes from third party unless stated otherwise.

Secunia collects, validates, and verifies all vulnerability reports issued by security research groups, vendors, and others.

Send Feedback to Secunia:
Google Hacking

- Vendor Website Information
Installing Free Smart Guest Book 2.0 for Access Database

A. Contents of the zip file

You will find the following files:

- SmartGuestbook.mdb (Access Database)
- SmartGuestbook.swf (Flash Interface)
- SmartGuestbook.asp (ASP file where the Flash interface is placed)
- SmartGuestbookCode.asp (ASP file accessed by the .swf file)
- scripts.js (JavaScript code)
- badwordfilter.txt (comma delimited bad words list)
- CloseWindow.htm (to automatically close the window)
- Readme.txt (content similar to this page section)

Note: If you have your own site and want a quick installation just follow the 1st and 3rd steps. That's it!

B. Installation steps

1. Important: Place all the above files in a folder called SmartGuestBook under your site root.
   Very Important: Please give the folder write permission (If you don't know how to do this, please contact your site administrator).

2. If your site is being hosted by another site i.e. your site is a freely hosted site, you would have to most probably place the access database file in a specified database folder as assigned by your service provider. You will thus need to make a few changes to the pages to give the correct path to the SmartGuestBook files:
Google Hacking

- Google search......
  - Inurl: smartguestbook.asp
Google Hacking

- The victim’s Website
Google Hacking

- Download the database…… Game over
Google Hacking

- Transparent Proxy
  - Normal surfing on www.myip.nu
www.myip.nu

Your IP address: 126.55
Your Country are: CA Canada
You Browser is: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Tuesday 7th September, 2004
You are the 37615th visitor since 11 May 2003
Google Hacking

- Transparent Proxy
  - When we use Google translation tool to surf www.myip.nu
Your IP address: 216.239.39.5
Your Country: US United States
Your Browser: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322), gzip(gfe) (via translate.google.com)

Tuesday 7th September, 2004
You are the 37610th visitor since 11 May 2003

ip-atlas
Network Query Tool
Network utilis
Subnet Calculator
Who Is

is your .nu name still available?
www.your-name.nu Go!
Google Hacking

- Google Automated Scanning
  - Google doesn’t like the idea about automating Google scan. They issue a free licence limited to 1000 queries/day to Google
  - Gooscan
  - Gooscan is a UNIX (Linux/BSD/Mac OS X) tool that automates queries against Google search appliances, which helps to do the external vulnerability assessment. For more information about this tool, including the ethical implications of its use. See: http://johnny.ihackstuff.com
Google Hacking

- Google Automated Tools
  - SiteDigger
  - SiteDigger searches Google’s cache to look for vulnerabilities, errors, configuration issues, proprietary information, and interesting security nuggets on Web sites. See: [http://www.foundstone.com](http://www.foundstone.com)
Foundstone SiteDigger v1.0

Results | Signatures |

Please enter a domain

Search  Stop  Clear  Export Results

Connecting to Foundstone.com....
Downloading file Schema.xml from Foundstone.com
Downloaded file saved at C:\Program Files\Foundstone\SiteDigger
Signatures successfully updated...............

Enter Google license key: E980ISBQFK1K9zQizzKi5iJ37HA81f

GoSecure Inc.
Google Hacking

- Google Automated Tools
  - Athena
  - Another Google query tool. It supports an open XML configuration format to support multiple search engines (not just Google)
GoSecure Inc.

Web

Results 1 - 10 of about 628 for intitle:index.of:master.passwd (0.23 seconds)

Index of /etc/passwd
Index of /etc/passwd ... 20-Feb-2001 10:11 3k log_orders 31-Jul-2003 13:10 14k
mailform.pl 31-Jul-2003 12:55 4k mailto.cgi 31-Jul-2003 12:55 2k master_passwd 31- ...
gray-world.net/etc/passwd/ - Similar pages

Index of /dist/freebsd/5.2.1/i386/cd2/etc
Index of /dist/freebsd/5.2.1/i386/cd2/etc ... 23-Feb-2004 19:42 106 mail/rc 23-Feb-2004 19:42 1.1K master_passwd 23-Feb ...
www.maxtux.co.uk/dist/freebsd/5.2.1/i386/cd2/etc/- 10k - Cached - Similar pages

Index of /dist/freebsd/4.10/cd2/etc
Index of /dist/freebsd/4.10/cd2/etc ... 22:28 64K mail.rc 25-May-2004 22:28 106 mail/rc
www.maxtux.co.uk/dist/freebsd/4.10/cd2/etc/- 11k - Cached - Similar pages
[ More results from www.maxtux.co.uk ]

Index of /pdoor
Index of /pdoor ... Then you would give it something like this: GET /HTTP/2cat
/etc/master_passwdmail user@blah it will read anything after 'GET / HTTP/2' as ...
cp5.lucidx.com/pdoor/- 3k - Cached - Similar pages

Index of netbsd-help for October, 2002
Index of netbsd-help for October, 2002. From, Subject ... Gan Uesli Starling, passwd & master_passwd from backup. David S. Ro: passwd & master_passwd from backup. ...
**Google Hacking**

- **Google Materials**
  - Googledorks
  - The famous Google Hack Website, it has many different examples of unbelievable things: [http://johnny.ihackstuff.com](http://johnny.ihackstuff.com).
Welcome to the Google Hacking Database (GHDB)!
We call them 'googledorks' (gōl dork, noun, slang): An inept or foolish person as revealed by Google. Whatever you call these fools, you’ve found the center of the Google Hacking Universe! Stop by our forums to see where the magic happens!

Entries by Category

Error Messages (50)
Really retarded error messages that say WAY too much!

Files containing juicy info (125)
No usernames or passwords, but interesting stuff none the less.

Files containing passwords (73)
PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

Files containing usernames (13)
These files contain usernames, but no passwords... Still, google finding usernames on the web..

Footholds (5)
Examples of queries that can help gain a foothold into a web server

Pages containing login portals (46)
These are login pages for various services. Consider them the front door of a site’s more sensitive functions.

Pages containing network or vulnerability data (14)
These pages contain such things as firewall logs, network information, IDS logs... all sorts of fun stuff!

Sensitive Directories (27)
Google’s collection of sites sharing sensitive directories. The files contained in here will vary from sensitive to uber-secret!

Sensitive Online Shopping Info (3)
Examples of queries that can reveal online shopping info like customer data, suppliers, orders, credit info, etc

Various Online Devices (17)
This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.

Vulnerable files (25)
HUNDREDS of vulnerable files that Google can find on web servers...!

Vulnerable Servers (28)
These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section.

Web Server Detection (37)
These links demonstrate Google’s awesome ability to profile web servers...
# Google Hacking

## 10 most popular entries

1. index.of.password
2. "access denied for user" "using password"
3. auth_user_file.txt
4. The Master List
5. allinurl: admin mdb
6. "A syntax error has occurred" filetype:ihtml
7. passlist.txt (a better way)
8. ORA-00921: unexpected end of SQL command
9. Look in my backup directories! Please?
10. config.php

## 10 most recent entries

1. intitle:"Object not found!" intext:"Apache/2.0.* (Linux/SuSE)"
2. inurl:netw_tcp.shtml
3. intitle:"WebJeff - FileManager" intext:"login" intext:Pass|PAse
4. intitle:"EMUMAIL - Login" "Powered by EMU Webmail"
5. intitle:"Open WebMail" "Open WebMail version (2.20|2.21|2.30) "
6. intitle:"error 404" "From RFC 2068 "
7. intitle:"Directory Listing, Index of /*/"
8. "Powered by Caudium Webserver" -caudium.net
9. intitle:"IBM HTTP Server" "Use the Administration Server to configure"
10. intitle:"Lotus Domino Go Webserver:" "Tuning your webserver" -site:ibm.com
Google Hacking

- Google Materials
  - Freshgoo
  - Search Google for the page published on today, yesterday, within the last seven days or last 30 days: [http://www.freshgoo.com/index.php](http://www.freshgoo.com/index.php)
Google Hacking

- Protect Your Data
  - Keep patching your systems and applications
  - Keep your sensitive data off the Web apply authentication
    - (RSA, Clienless VPN)
  - Disable directory browsing
  - Google hack your Website
  - Consider removing your site from Google's index:
  - Use a robots.txt file to against Web crawlers:
Google Hacking References

Google APIS:
www.google.com/apis
Remove:
http://www.google.com/remove.html
Googledorks:
http://johnny.ihackstuff.com/
O’reilly Google Hack:
http://www.oreilly.com/catalog/googlehks/
Google Hack Presentation, Johnnny Long:
http://johnny.ihackstuff.com/modules.php?op=modload&name=ownloads&file=index&req=viewdownload&cid=1
“Autism: Using google to hack:
www.smart-dev.com/texts/google.txt
“Google: Net Hacker Tool du Jour:
http://www.wired.com/news/infostructure/0,1377,57897,00.html
Contact Information:

Robert Masse
rmasse@gosecure.ca
www.GoSecure.ca

407 McGill, suite 900
Montréal, Québec, Canada
H2Y 2G2

514-287-7427