You found that on Google?

Gaining awareness about "Google Hackers"
Johnny Long
johnny@ihackstuff.com
Who’s Johnny?

- Since this is a Google talk, let’s ask google:
About DC3

- Who does Johnny really work for?
What this is about

- We’ll be talking about how hackers can use Google to locate vulnerable targets and sensitive information
- This process has been termed “Google hacking”
- We will be blowing through the basics
  - After all, this is BLACKHAT! =)
This is not new.

- Although search engine ‘hacking’ is not new, it’s potent and often overlooked.

**The Problem of Search Engines and "Sekrit" Data**

Posted by Hemos on Mon Nov 26, '01 11:43 AM

from the how-to-choose-data dept.

Nos. writes: "CNet is reporting that not only Google but other search engines are finding password and credit card numbers while doing its indexing. An interesting quote from the article by Google: 'We define public as anything placed on the public Internet and not blocked to search engines in any way. The primary burden falls to the people who are incorrectly exposing this information. But at the same time, we’re certainly aware of the problem, and our development team is exploring different solutions behind the scenes.'" As the article outlines, this has been a problem for a long time -- and with no easy solution in sight.
Advanced Operators

- Google advanced operators help refine searches
- Advanced operators use a syntax such as the following:
  - `operator:search_term`

- Notice that there's no space between the operator, the colon, and the search term.
Crash course in advanced operators
Advanced Google Searching

- **FILETYPE:php**
- **INTITLE:“I hack stuff”**
- **INTEXT:“Google Masters”**
- **NUMRANGE:33334-33336**
Google Hacking Basics

INURL:admin
INURL:orders
FILETYPE:php

osCommerce
om/catalog/admin/orders.php+filety
Google Hacking Basics

- It's all in the results....
Search Characters

- Some characters to keep in mind:
  - (+) force inclusion of something common
  - (-) exclude a search term
  - (" ) use quotes around search phrases
  - ( . ) a single-character wildcard
  - (*) any word
  - ( | ) boolean 'OR'
  - Parenthesis group queries ("master card" | mastercard)
Google Info Gathering Techniques
Site Crawling

- To find every web page Google has crawled for a specific site, use the site: operator
Server Crawling

- To locate additional servers, subtract common hostnames from the query
Directory Listings

- Directory listings can be a source of great information
Directory Listings

- Directory listings can provide server version information
Default Server Pages

- Web servers with default pages can serve as juicy targets

intitle:test.page.for.apache "it worked"
Default Server Pages

- Netscape FastTrack
Default Server Pages

- Netscape Enterprise Server
Default Server Pages

- IIS - Windows 2000

intitle:"Welcome to Windows 2000 Internet Services"
Default Server Pages

- IIS - Windows XP
Default Server Pages

- IIS 4.0
Default Server Pages

- Generic IIS
Default Documents

- Servers can also be profiled via default manuals and documentation
Server Profiling

- There are more ways to profile servers. Here are a few ways. I’m glad someone’s keeping a list somewhere… =)
Error Messages

- Server profiling is easy with some error messages
Error Messages

- CGI environment vars provide a great deal of information
- The generic way to find these pages is by focusing on the trail left by the googlebot crawler

“HTTP_USER_AGENT=Googlebot”
Error Messages

- after a generic search, we can narrow down to the fields we find more interesting
Error Messages

- Error messages may be one of the more evil Google hacking finds. They can pop up ANYWHERE!
Login Portals

- Very generic queries can be used to find login portals
Login Portals

- Another very generic query
Login Portals

- Coldfusion Admin Page

intitle:"ColdFusion Administrator Login"
Login Portals

- Windows Remote Desktop

`intitle: "Remote Desktop Web Connection"`
Login Portals

- Citrix Metaframe

inurl:citrix/metaframe.exp/default/login.asp
Login Portals

- MS Outlook Web Access

Intitle:"Microsoft Outlook Web Access"
Login Portals

- Now, if these are meant to be public, then fine. Why SSL on the connection? Hmmm...
Login Portals

• So, the question becomes “Is the directory search public on purpose?”
But using Google for HACKING? ‘cmon...

- It might seem a stretch to say that Google can be used for hacking...
Hacking for Dummies

- Password Cracking 101

"Welcome to **" "Your password is **"
Hacking for Dummies

- Ehhh... PBX Hacking with Google? =)

1. Dial Audix at campus locations using only last four digits from inside any campus. If calling from an outside line, dial the following numbers:
   - ITS Building - 2501 661-5596
   - Annex - 683-2695
   - CAAT - 683-2795
   - STARR - 488-5895
   - WESL - 447-6695
   - NAH - 683-3195
   - PHARR - 283-3880

2. Audix will prompt you to enter your extension followed by the # sign.

3. Audix will prompt you to enter your password followed by the # sign. The first time your password is just # sign. Press #. After two tries hang up and start over.

4. Audix will tell you that you need to record your name. Press 1 to start. Say your first and last name. Press 1 to stop and # to approve. If you don't like how it sounds Press 1 to rerecord.

5. If a password is required, Audix will tell you how many digits your password

"Welcome to *" "Your password is *

"Welcome to *" "Your password is *

"Welcome to *" "Your password is *"
Hacking for Dummies

- This search finds sites that allow an interesting option....

Inurl:(browse|top_rated|power_search|hot|create_admin_user) +"powered by indexu"
Hacking for Dummies

• ...the ability to delete the old Administrator account and recreate it with default passwords! Point, click, OWN!
Hacking for Dummies

- Another example: These pages....
Hacking for Dummies

- let you set up your own free email account. Point, click, SPAM.

Click here if you want setup your mail with Outlook or any Mailer program.
Click here if you're looking for free Eurofil Webhosting.
Hacking for Dummies

- “Look, Ma, cleartext passwords!”
- Guess the query (hint: filetype/inurl)
**Hacking for Dummies**

- This search finds “PHP Shell” installations.

[Google Search: intitle:"PHP Shell *" "Enable stderr" filetype:php]

---

**PHP Shell**

PHP Shell. Warning: `chdir()` [function.chdir]: SAFE MODE Restriction in effect. ... Command: `Enable stderr` - trapping? Output: Copyright © 2000, Martin Geisler. ...

---

**PHP Shell 1.7**


---

**PHP Shell**

PHP Shell. Current working directory: Root/data/members/free/tripod/uk/i/o/w/nwbuy/htdocs/.

---

**PHP Shell**

File Format: Unrecognized - View as HTML.

* We'll register the variables as globals: `?if (empty($HTTP_POST_VARS)) extract($HTTP_POST_VARS); if (!empty($HTTP_GET_VARS)) extract ... Enable stderr-trapping? *
Hacking for Dummies

- What exactly is “PHP Shell?” Let’s try a few benign UNIX commands...
Hacking for Dummies

- Oooh... hey! A web-based command shell! Handy! Oh... look at that password file!
Hacking for Dummies

- Poking around a bit more… What’s wap? Wireless??!!
Hacking for Dummies

- Wha-HAY! This ain’t wireless! (This kiddie smells REAL pay dirt!)
Hacking for Dummies

• WOOOO HOOO!!! JACKPOT! BRIT-NAY PICS!!!! =PppPP
Vulnerability Trolling
Vulnerability Trolling

- Many attackers find vulnerable targets via Google
- A typical security advisory may look like this:

![Security Tracker Alert Example](image-url)
Vulnerability Trolling

- A quick browse of the vendor's website reveals a demo of the product
Vulnerability Trolling

- The demo page suggests one method for finding targets
Vulnerability Trolling

- A quick intitle: search suggests more vectors...
Vulnerability Trolling

- This search finds the documentation included with the product
- These sites are probably poorly configured
Vulnerability Trolling

- Other searches are easy to discover as well...
Vulnerability Trolling

- Other searches are easy to discover as well...
Vulnerability Trolling

- Many times, a good search string is much simpler to come up with. Guess search strings for this advisory:
Vulnerability Trolling

- The search is very intuitive...
Traditional Hacking Techniques
Google Style!
CGI Scanning

- In order to locate web vulnerabilities on a larger scale, many attackers will use a ‘CGI’ scanner.
- Most scanners read a data file and query target web servers looking for the vulnerable files.
CGI Scanning

- A CGI scanner’s vulnerability file...
  /iisadmpwd/
  /iisadmpwd/achg.htr
  /iisadmpwd/aexp.htr
  /iisadmpwd/aexp2.htr
  /iisadmpwd/aexp2b.htr

- can be converted to Google queries in a number of different ways:
  intitle:index.of /iisadmpwd/
  intitle:index.of /iisadmpwd/achg.htr
  intitle:index.of /iisadmpwd/aexp.htr
  intitle:index.of /iisadmpwd/aexp2.htr
  intitle:index.of /iisadmpwd/aexp2b.htr
CGI Scanning

- Regardless of the age of the vulnerability, there are usually vulnerable targets
Port Scanning

- Although port numbers are sometimes found in the url, there's no easy way to scan just for a port number... the results are much too copious.
- There are way too many bad results for this query:

![Google Search: inurl:5800](image-url)
Port Scanning

- We can use creative queries to find services that listen on known ports.
- VNC Desktop, port 5800
Port Scanning

- Webmin, port 10000
Port Scanning

- Another way is to find the port in the url, but not in the text:
Port Scanning

- Another way is to find the port in the url, but not in the text:
Port Scanning

- As an option to scanning for ports directly, Google can be used to find sites to do the scan for you
- Consider the Network Query Tool
Port Scanning

- NQT allows web users to perform traceroutes, rdns lookups and port scans.
- This is the NQT program checking port 80 on www.microsoft.com:

![Network Query Tool](image-url)
Port Scanning

- Google can be used to locate servers running the NQT program, nqt.php
- Once servers are harvested, they can be used to perform port scans (usually through a web proxy)
- NQT also allows remote posts, so that more than one port can be checked at a time from an html form you create...
Automation
Automation

- Google's stand on automation: "Use our API or don't do it."
- API vs. Non-API
Tools - Athena

- Athena: http://www.buyukada.co.uk/projects/athena/
Tools - Gooscan

- Gooscan by some johnny guy...

Gooscan Results

<table>
<thead>
<tr>
<th>Search</th>
<th>Link</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>intitle:&quot;500 Internal Server Error&quot; &quot;server at&quot;</td>
<td>link</td>
<td>1490</td>
</tr>
<tr>
<td>&quot;mySQL error with query&quot;</td>
<td>link</td>
<td>587</td>
</tr>
<tr>
<td>&quot;You have an error in your SQL syntax near&quot;</td>
<td>link</td>
<td>52200</td>
</tr>
<tr>
<td>inurl:search.php vbulletin</td>
<td>link</td>
<td>178000</td>
</tr>
<tr>
<td>inurl:footer.inc.php</td>
<td>link</td>
<td>496</td>
</tr>
<tr>
<td>inurl:info.inc.php</td>
<td>link</td>
<td>50</td>
</tr>
<tr>
<td>&quot;Powered by mnoGoSearch - free web search engine software&quot;</td>
<td>link</td>
<td>1450</td>
</tr>
<tr>
<td>inurl:Custva.asp</td>
<td>link</td>
<td>157</td>
</tr>
<tr>
<td>&quot;YaBB SE Dev Team&quot;</td>
<td>link</td>
<td>284000</td>
</tr>
</tbody>
</table>

filetype:htpasswd

gooscan by j0hnny

http://johnny.ihackstuff.com
Tools

- Site Digger by Foundstone:
  www.foundstone.com/resources/proddesc/sitedigger.htm

if (unanswered_emails > 2) {screenshot = NULL};

Seriously though, they did plug my site in their docs, so thanks guys. =)
Poking, Prodding and Pummeling SQL
Poking SQL

- Gathering SQL usernames is simple with this search.
Poking SQL

- This query will locate SQL schemas on the web
Poking SQL

- This is a complete database schema dump, essentially a complete database backup

```
# Dumping data for table 'config'

INSERT INTO config VALUES ( 'last_update', '');

# Table structure for table 'creatures'

CREATE TABLE creatures ('id' int(11) DEFAULT '0' NOT NULL auto_increment, 'name' varchar(255) NOT NULL, 'owner' int(11) DEFAULT '0' NOT NULL, 'carnivore' enum('Y','N') DEFAULT 'Y' NOT NULL, 'weight' int(11) DEFAULT '0' NOT NULL, 'speed' int(11) DEFAULT '0' NOT NULL,

"# Dumping data for table"
```
Poking SQL

* In addition, this query finds the words ‘username’ and ‘password’ inside the SQL dump
Poking SQL

- This potent query finds SQL dumps with either 'username', 'user', 'users' or 'password' as a table name
Prodding SQL

- This search can be used by an attacker to find SQL injection targets

```
ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1
ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1
ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1
ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1
ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1
ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1
ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1
```

"ORA-00933: SQL command not properly ended"
Prodding SQL

• ...another SQL injection target...

"Unclosed quotation mark before the character string"
Prodding SQL

- ..and another...

"Unclosed quotation mark before the character string"
Prodding SQL

- In most cases, there’s nothing better for an SQL injector than a complete line of SQL source code...

```sql
The error occurred in D:\INET\fun_site\_NEW\_f_main.cfm: line 87
Called from D:\INET\fun_site\_NEW\_f_index.cfm: line 13
Called from D:\INET\fun_site\_NEW\_f_index.cfm: line 14
Called from D:\INET\fun_site\_NEW\_f_index.cfm: line 200
85: SELECT id, thumbnail, big, small, property
86: FROM wallpapers
87: WHERE id = #ListGetAt(pic, 1)#
88: </cfquery>
89: </cfloop>
```

intitle:"Error Occurred" "The error occurred in"
Prodding SQL

- ...except for really really *long* lines of SQL code.
Pummeling SQL

- This graphical front-end to SQL is misconfigured to allow anyone admin access

inurl:main.php Welcome to phpMyAdmin
Pummelling SQL

- Big SQL dumpage... Wicked cool query...

```
intitle:"Error Occurred While Processing Request" +WHERE (SELECT|INSERT) filetype:cfm
```
Pummeling SQL

- the mysql_connect function makes a database query with a supplied username and password! (Other functions do this as well. Search for the function.)
- This file should not be on the web

```php
<?php
$host = "";
$user = "cs3projo";
$password = "tTnM76mx5"
$database = "cs3projo"

mysql_connect($host, $user, $password);
@mysql_select_db($database) or die ("I cannot?
?>
```
SQL Passwords

- Question: What’s the SQL syntax that can be used to set a password?
- (TWO WORDS)
- Answer: “IDENTIFIED BY”
Pummelling SQL

- Here’s a simple way to go after “IDENTIFIED BY”
Pummelling SQL

- The hardcore Google hacker’s version:
Pummelling SQL

- Another curious way to go after SQL passwords.
Google Hacking “Security People”
Certificates

- Security conscious people use certificates...
Private Certificates

- PRIVATE keys. AOL Keyword: PRIVATE!
Locating Nessus Scans

- Lots of hits, but we have samples and garbage...

“This file was generated by Nessus”
Nessus Scans

- Every now and then you get something interesting.
- This ‘corporate’ scan was found on a personal site.
Locating ISS Scans

- Same deal, lots of samples, but then a few gems. How about navy.mil? (be good kids, it’s gone now =)

"This report lists" "identified by Internet Scanner"
ISS Scans

- Test scans always lack realistic details, like usernames that match accounts on matching mail servers.... Wait... this ain’t no test scan...
IDS Data: ACID

- SNORT IDS data delivered graphically, served up fresh
SSH Host Keys

- Guess the Google query…

```
ProxyPort=dword:00000000
ProxyUsername=""
ProxyPassword=""
ProxyTelnetCommand="connect %host %port\n"
ProxySOCKSVersion=dword:00000005
NoMouseReporting=dword:00000000
NoRemoteResize=dword:00000000
NoAltScreen=dword:00000000
NoRemoteWinTitle=dword:00000000
NoDelBackspace=dword:00000000
NoRemoteCharset=dword:00000000
Printer=""
BugIgnore1=dword:00000000
BugPlainFW1=dword:00000000
BugREAl=dword:00000000
BugSHMAC2=dword:00000000
BugDeriveKey2=dword:00000000
BugRSAAP2=dword:00000000
BugDHEG2=dword:00000000

[HKEY_CURRENT_USER\SOFTWARE\SimonTatham\PuTTY\SshHostKeys]
galaxy.uci.agh.edu.pl=0x23,0xac4e3526930d5921fb499a0b4600355b4dffe3be5af4d4cc9b910
\r\nrs1222:galaxy.uci.agh.edu.pl=0x23,0xac4e3526930d5921fb499a0b4600355b4dffe3be5af4d4cc9b910

Display a menu
```
PGP Private Keys
Hacking ‘hackers’… you know? IRC users??
Accessing IRC

- Finding a temporary IRC bounce is easy. These sites offer a web-based IRC client.
Accessing IRC

- Some of these sites are even kind enough to let you connect to any irc server you want.
Pillaging IRC

- Lots of leeto hackers use psybnc for bouncing irc connections.... Not so leeto if the config file lands on the web....
Pillaging IRC

- Wanna become someone on IRC? Let’s find their nickserv registration passwords.

"Your password is * Remember this for later use"
Pillaging IRC

• *sigh*

```
[04:36 PM] <RobertoFrog> how do i register my nick?
[04:36 PM] <Sumthing> magic
[04:36 PM] <Sumthing> =D
[04:36 PM] <+Lucylnyo> o___O
[04:36 PM] <Sumthing> type /msg nickserv register password
[04:36 PM] <Sumthing> i think
[04:37 PM] <Sumthing> i haven't registered anything in forever
[04:37 PM] *** Sumthing is now known as Frank
[04:37 PM] <+Lucylnyo> o___O
[04:37 PM] *** Lucylnyo is now known as Kayley
[04:37 PM] <RobertoFrog> hmm.. i guess i will use froggy as my password
[04:37 PM] <+Kayley> Hi Frank
[04:37 PM] <+Yosho> /ns register <password>
[04:37 PM] <+Kayley> o___O
[04:37 PM] * Kinzu unf$s Kayley
[04:37 PM] <+Kayley> @@
[04:37 PM] <+Yosho> easier
[04:37 PM] @@ Xerin> hmm
[04:37 PM] <Frank> hiyo Kayley
-NickServ- Nickname RobertoFrog registered under your account:
RobertoFro@*.ade0409.ade.iprimus.net.au
-NickServ- Your password is froggy - remember this for later use.
```

"Your password is * Remember this for later use"
Getting Sensitive
Locked out!

- Some sites lock down sensitive data..

- However, the Google cache image still remains.
Credit card info on the web?

- How can this happen? Let’s take a tour of some of the possibilities...
Court Documents

• Court cases sometimes give TONS of detail about cases, especially fraud.
Court Documents

account number:

account #:

account #:

account #:

Bank #
Court Documents

- How much detail is too much detail? =)
Court Documents

- Of course, fraud accounts are closed pretty quickly, no?

<table>
<thead>
<tr>
<th>BANK</th>
<th>ACCOUNT NUMBER</th>
<th>ACCOUNT NAME</th>
<th>AMOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>t Bank</td>
<td>05: 13</td>
<td>High Risk</td>
<td>$1</td>
</tr>
<tr>
<td></td>
<td>13: 23</td>
<td>High Risk</td>
<td>$2</td>
</tr>
<tr>
<td></td>
<td>90: 97</td>
<td>High Risk</td>
<td>$7</td>
</tr>
<tr>
<td>Bank</td>
<td>71: 02</td>
<td>High Risk</td>
<td>$2</td>
</tr>
<tr>
<td>Bank</td>
<td>101: 96</td>
<td>High Risk</td>
<td>$3</td>
</tr>
<tr>
<td></td>
<td>28: 27</td>
<td>High Risk</td>
<td>$11</td>
</tr>
<tr>
<td></td>
<td>63: 91</td>
<td>High Risk</td>
<td>$2</td>
</tr>
<tr>
<td></td>
<td>90: 10</td>
<td>High Risk</td>
<td>$2</td>
</tr>
</tbody>
</table>
A tale of a corn snake

- Is this for real? Either way it's pretty sad...
Getting shell.. the easy way

- Now I’ve heard the term ‘using your credit card online’ but this is ridiculous!

---

**applying for a shell acct**

*To:* ping-yonk@ping-yonk.org
*Subject:* applying for a shell acct
*From:* ping-yonk@ping-yonk.org
*Date:* Sat, 09 Oct 1999 04:40:28 GMT

hi there i am interested to buy a shell acct for my son.
i m 2 busy because of some reasons. This is my only way to communicate with my son... so i want 2 buy a shell acct using my creditcard

the login name and password will be:
login name: mysonacct
password: q77q77

Down here will be the details about me.
name: leong x. yonk
-Residence: Fortuna, CA, 95540

tel#: 512-3456
Billing Information:
Name on card: leong x. yonk
credit card #: 4123899160798162
expiration date: 01/00
type of card: visa

Thank you and I hope to hear from you soon.
Some people just don’t get it....

Questions & Offers Board
Our Questions & Offers board is the place to view questions and offers between other buyers and the seller. Please review this board before you make an offer or ask the seller a question.

Questions & Offers between [Name] and the Seller

**Question**: hi there here is my credit card details below : name on card : [Name] card number : [Number] expire date : 10/05 CVV2 number : [CVV2] card type : Visa name on card : [Name] card number : [Number] expire date : 02/05 cyy2 number : [CVV2] card type : Visa please let me know if you finished charge my credit card. thanks

**Answer**: Ok, I will attempt to charge your card first thing tomorrow when I am back at the office. Also, what address do you want this shipped to? Thanks
Some people just don’t get it....

<table>
<thead>
<tr>
<th>Cash Accounts</th>
<th>Account Number</th>
<th>Available Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>PettyCash</td>
<td>000-7300xxx</td>
<td>$50</td>
</tr>
<tr>
<td></td>
<td>000-7646xxx</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200-2233xxx</td>
<td>$20,000</td>
</tr>
<tr>
<td></td>
<td>600-7593xxx</td>
<td></td>
</tr>
<tr>
<td></td>
<td>600-7442xxx</td>
<td></td>
</tr>
</tbody>
</table>
Getting serialz... wha-hay!! and MORE!

- This is a very generous person. He’s willing to give his software serial numbers and his credit card info to the whole world. Generosity like this could change the world.
Police Crime reports

• Two questions:
• Are police reports public record?
  • YES.
• Are they on the web?
  • YES.
• Many states have begun placing campus police crime reports on the web. Students have a right to know what crimes take place on campus.
Crime shouldn’t pay...

- I’m thinking there should be a process for filtering these reports.

- A few might fall through the cracks....
Expense Reports

- It's not uncommon for expense reports to be generated. This one is for a county.
Expense Reports

- Bank account numbers...
Expense Reports

- Bank loan information... $20,000 + transactions
Expense Reports

- Oh boy…

<table>
<thead>
<tr>
<th>Description</th>
<th>Date</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>STAPLERS</td>
<td>2019</td>
<td>$12.34</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$15.78</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$20.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$25.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$30.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$35.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$40.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$45.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$50.00</td>
</tr>
<tr>
<td>LONG DISTANCE</td>
<td>2019</td>
<td>$10.00</td>
</tr>
<tr>
<td>VISA</td>
<td>2019</td>
<td>$10.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$15.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$20.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$25.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$30.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$35.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$40.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$45.00</td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td>$50.00</td>
</tr>
</tbody>
</table>
Expense Reports...

- Somebody has to pay for all this stuff....
Expense Reports

• That’s one heck of a video series…. $300+
Credit cards... Google hacker’s gold...

- The legend of finding credit cards online is true...
- I just get bored sifting through them all....
Credit card listings
Credit card listings
Credit card listings
Credit Listings
Pick a card any card...

- We proudly accept...
Credit Validation

Question: What keeps someone from using a pilfered credit card number and expiration date to make an online purchase?

• Answer: That little code on the back of the card.
• Bonus question: What’s that code called?
• Answer: A “CVV” code.
Credit Card Numbers, Expiration Date and CVV numbers, oh my!
That’s not all....

- Credit cards are sooo 1990’s =)
Getting more personal

• Question: What’s the one 9 digit number you shouldn’t give to ANYONE?
• Answer: SSN
• Bonus question: What can you do with someone’s SSN?
• Answer: Steal their identity.

• How do SSN’s get on the web? Let’s take a look at some possibilities.
SSN’s in source code

- Well, they could be hardcoded into a healthcare system... and uhmmm... put on the web...
Crime shouldn’t pay...

- Remember the police reports? Since the credit card accounts in them are no good, maybe we should troll them some more....
SSN’s - Police Reports
SSN’s

- Students have a right to know...
Social Security Numbers

- Many privacy violations are self-inflicted...
Social Security Numbers

- Schools are notorious... Grades posted w/ student’s SSN's
Social Security Numbers

- Schools again...
Social Security Numbers

- Once you get a lock on a grade list, the results fan out as you explore the site.
Social Security Numbers

- More schools
Social Security Numbers

- ...and more schools.
Social Security Numbers

- In order to make the most out of a pilfered SSN, you need some more details, like names… These usually get blocked…

File Not Found
We're sorry, but the document or address you have requested is not available. Please make sure you have typed the name and/or URL correctly, or report the error to: pagemaster@...

Note: This uses special security software that monitors suspicious network traffic and behavior.
Social Security Numbers

- ...unless Google’s caches grabs them first...
Social Security Numbers

- Schools seem to be very bad about posting names and SSNs together with grade postings.
A tale of one city

- A city document outlining residents who are in debt to the city... A little report of names, addresses, amount owed and SSN numbers...
A tale of one city

- Or perhaps more than a little report...
A tale of one city

- Hundreds of city residents’ personal information posted to the web... 90% including SSN and address.
Prevention

- Do not put sensitive data on your web site, even temporarily
- Proactively check your web presence with Google on a regular basis
- Use sites like http://johnny.ihackstuff.com to keep up on the latest “Google Hacks”
Prevention

- Use site: queries against each of your web hosts
- Don’t forget about hosts that do not have DNS names. Site scan IP addresses and FQDN’s.

- Scan each result page, ensuring that each and every page it supposed to be in Google’s database
Prevention

- Automate your scans with tools like Athena or sitedigger by Foundstone.
Prevention

- Visit the ‘Search Engine Hacking’ forum or the Googledorks database on my web site, http://johnny.ihackstuff.com
About DC3

- Who does Johnny really work for?
Final words

• Be on the lookout for “Google Hacking for Pen Testers” by Syngress Publishing.

• Thanks to my company, CSC and to DC3. They make my research possible. Shouts to strikeforce, the ‘TIP and all those in the security community who have provided me a helping hand.

• Thanks to the Google Masters List: MURFIE, The Psyko (stevew@security-forums.com), crash_monkey, MILKMAN (milkman@b4b0.org), zoro25, l00m, Deadlink, wasabi (sangu1s) and Peefy.
Thanks

• Thanks to God for the gift of life.
• Thanks to my wife for the gift of love.
• Thanks to my kids for the gift of laughter.
• Thanks to my friends for filling in the blanks.