

Google HaCking

Anthony L@I, CISSP, CISM, CISA

M@rco Leung, SCJP, OCP

0xD8.0x30.0x3.0x12

Presented by Anthony LAI & Marco
Leung, 2005

1

Google HaCking

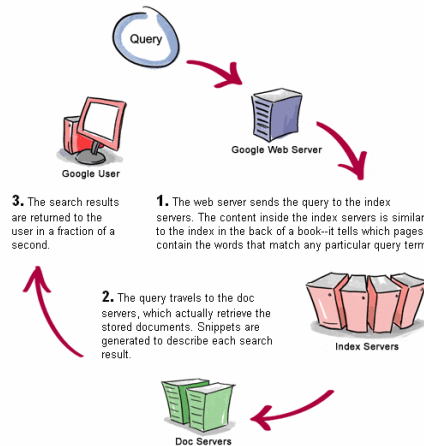
What is that?

- Your developed web application is on the web. Meanwhile, your ignored vulnerabilities and setting are also there ☺
- Google is a great tools for searching like a well-trained anti-drugs dog on the web.
- Reminder: We are not liable for your intrusive and malicious action and intention.

Presented by Anthony LAI & Marco
Leung, 2005

2

How Google works?



Presented by Anthony LAI & Marco
Leung, 2005

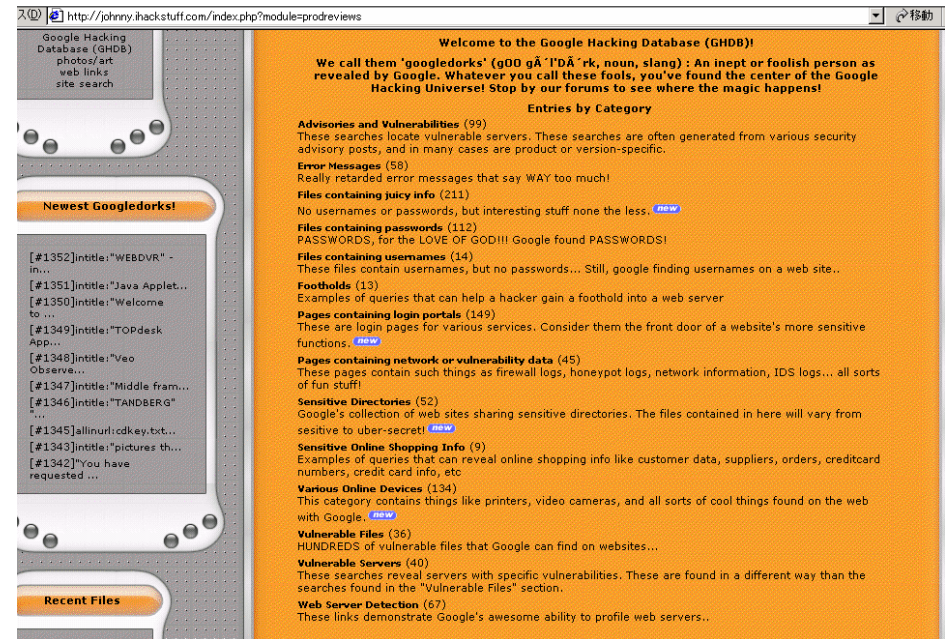
3

Google Search Engine

- Advanced Search Operators
 - site:
 - restrict search to a specific web site
 - filetype:
 - search within the content of particular file type
 - cache:
 - displays the version of a web page
 - link:
 - search word within hyperlinks
 - intext:, allintext:
 - searches words within a specific website, but ignores the URLs and page titles
 - intitle:, allintitle:
 - search words within the title of a document
 - inurl:, allinurl:
 - search words within the URL of a document

Presented by Anthony LAI & Marco
Leung, 2005

4



Different Categories of Queries

- Programmer/Developer Bad Practice(s)
- Operating System Vulnerability and Information Exposure (Configuration file, default admin access path)
- Application server security
- Database-related information exposure (Setup queries, database maintenance etc)
- Others

Example (1)

- "A syntax error has occurred" filetype:html intext:LOGIN -"[removed]"



Example (2)

- filetype:ora tnsnames

```
# TNSNAMES.ORA Network Configuration File: D:\oracle\ora92\network\admin\tnsnames.ora
# Generated by Oracle configuration tools.

EXTPROC_CONNECTION_DATA.COMPIERE.ORG =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))
  )
  (CONNECT_DATA =
    (SID = XE)
    (PRESENTATION = RO)
  )
)

INST1_HTTP.COMPIERE.ORG =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = MAIN)(PORT = 1521))
  )
  (CONNECT_DATA =
    (SERVICE = SHARED)
    (SERVICE_NAME = XE)
    (PRESENTATION = http://pdbservice)
  )
)

PROD1.COMPIERE.ORG =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = prod1)(PORT = 1521))
  )
  (CONNECT_DATA =
    (SERVICE_NAME = prod1.compiere.org)
  )
)

COMPIERE.COMPIERE.ORG =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = MAIN)(PORT = 1521))
  )
  (CONNECT_DATA =
    (SERVICE_NAME = compiere.compiere.org)
  )
)

CRAN.COMPIERE.ORG =
```

Presented by Anthony LAI & Marco Leung, 2005

9

Tools

- Using Web interface
 - Athena
 - GooScan
- Using Web Service API
 - SiteDigger

Presented by Anthony LAI & Marco Leung, 2005

10

Automated Tools - GooScan

```
Terminal — bash — 101x20
n30Computer:Applications/temp/gooscan-v0.9 n30$ ./gooscan -t www.google.com -q "allinurl: admin mdb"
-o gooscan_results.html

***!!! WARNING: You are querying a www.google.com server !!!***
This tool was designed to query Google appliances, not the google.com website.
The google.com scanning functionality is included for EDUCATIONAL PURPOSES ONLY
to help webmasters determine the potential Google exposure of their sites.

Do you acknowledge that:
- You are knowingly violating Google's terms of service found at
  http://www.google.com/terms_of_service.html
- You are using this tool to assess your own web site's exposure
- The use of this tool in this way is not condoned by the author
- You will not hold the author liable in any way for the use of this tool

Agree? (y/n) [n] y
doing lookup of www.google.com...
"allinurl: admin mdb" returned 229 results.
n30Computer:Applications/temp/gooscan-v0.9 n30$
```

Presented by Anthony LAI & Marco Leung, 2005

11

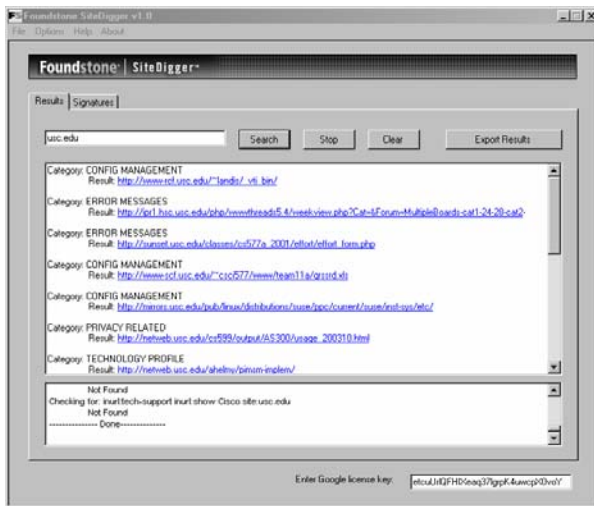
Tools - Athena



Presented by Anthony LAI & Marco Leung, 2005

12

Tools - SiteDigger



Presented by Anthony LAI & Marco Leung, 2005

13

Tools - SiteDigger

- Version 2 features (tentative release 15th July)
 - Proxy support / Google appliance support
 - XML signatures in OASIS WAS format
 - Adding signatures for OWASP top 10
 - Signature contribution option
 - Raw search tab
 - Configurable # of results

Presented by Anthony LAI & Marco Leung, 2005

14

Protection from Google Hackers (1)

- Keep your sensitive data off the web
 - Don't put any secure information on a web site
- Consider removing your site from Google's index
 - <http://www.google.com/remove.html>
- Use Meta tags
 - Prevent all robots from indexing a page
 - `<META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">`
 - Prevent only Google robots from indexing a page
 - `<META NAME="GOOGLEBOT" CONTENT="NOINDEX, NOFOLLOW">`
 - Allow robots to index the page, but don't follow the outgoing links
 - `<META NAME="ROBOTS" CONTENT="NOFOLLOW">`

Presented by Anthony LAI & Marco Leung, 2005

15

Protection from Google Hackers (2)

- Use a robots.txt file
 - <http://www.yoursite.com/robots.txt>
 - Document to indicate which parts of the server should not be accessed
 - Remove entire website
 - place the following robots.txt file:

```
User-agent: *
Disallow: /
```
 - Remove part of web site
 - Remove all pages under a particular directory

```
User-agent: Googlebot
Disallow: /lemurs
```
 - Remove all files of specific file type

```
User-agent: Googlebot
Disallow: /*.gif$
```

Presented by Anthony LAI & Marco Leung, 2005

16

Countermeasures

- Keep sensitive data off the web!!
- Perform periodic Google Assessments
 - Update robots.txt
 - Use meta-tags: NOARCHIVE
 - <http://www.google.com/remove.html>.

SUMMARY

- How Google works
- Information disclosure with Google
- Tools
- Countermeasures