The Hacker's Library

An easy and complete , step-by-step guide of being anonymous...

# Gather Information Using Google Hacking

3:39 PM KADAM PARIKH HACKING, PART3 NO COMMENTS

As a part of our chapter on Footprinting and Reconnaissance, this article is to make you aware about how to gather information using Google search. We have seen earlier on how to search google servers that deep to get direct download links. Ever though what was it?

We have been using Google search for a long time but none of us tried to search deep in server. Just we clicked on the website link that google showed to us but instead we can try Google search to modify results according to our needs. These all can be done using **Google Dorks - also known as google commands or filters**. So, let us start understanding what Google Dorks is and how to use them.

Google Dorks can be used as per our wish:

- For Hacking
- For Normal Uses

It depends on individual how he/she uses this function. Let us start understanding the term and its uses.

## Basics

Google hacking involves using advanced operators in the Google search engine to locate specific strings of text within search results.

## Examples

- Some of the more popular examples are finding specific versions of vulnerable Web applications.
- Devices connected to the Internet can be found. A search string such as

  ```
  inurl:"ViewerFrame?Mode="
  ```

  will find public web cameras.
- Another useful search is following

  ```
  intitle:index.of
  ```

  followed by a search keyword. This can give a list of files on the servers. For example,

  ```
  intitle:index.of mp3
  ```

  will give all the MP3 files available on various servers. We have seen this technique to get direct download links of movies, PDFs, songs and more..

## History

Everytime the history seems to us. But here, this is not the case. It is the case were a computer expert turned into a hacker.

The concept of "Google Hacking" dates back to 2002, when Johnny Long began to collect interesting Google search queries that uncovered vulnerable systems and/or sensitive information disclosures - labeling them **googleDorks.**

The list of googleDorks grew into large dictionary of queries, which were eventually organized into the original Google Hacking Database (GHDB) in 2004. In short, GHDB is an extended version of Google Dorks.

After the release of GHDB, Johnny Long wrote his own book on Google Hacking popularly known as **Google Hacking for Penetration Testers.**

## Introduction

A misconfigured server may expose several business information on Google. It is difficult to get access to files from database sites through Google. We can use as an example, the use of “cache” Google, where it stores older versions of all sites that were once indexed by their robots. This feature allows you to have access to pages that have already been taken from the air, since they already exist in the database of Google. To read more on Google cache and to know how to use it, click here..

## What kind of data can be exploited?

We all know that Google spies on us by keeping a record of what we search or what we do..! Similarly, Google keeps a spy of various servers too. It maintains the information either in its storage server or in its server cache. Hence, many a times, important data of a server gets leaked unknowingly.

You might have heard of performing **SQL injection** using Google search. Here are many other data that we can obtain from Google using GHDB.

### Advisories and Vulnerabilities

These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

### Error Messages

Really retarded error messages that provide us more of the information. When we come to know that a website is not properly configured, we can start searching for the mistake in the site which can be used as a vulnerable part to whole website. Sometimes, error message provide us this kind of information.

### Files containing juicy info

No usernames or passwords, but interesting stuff which has same value as usernames and passwords.

### Files containing passwords

Google search can also provide us passwords form its database if we use Dorks correctly.

### Files containing usernames

These files contain usernames, but no passwords...

### Footholds

Queries that can help a hacker gain a foothold into a web server

### Pages containing login portals

These are login pages for various services. Consider them the front door of a website's more sensitive functions.

### Pages containing network or vulnerability data

These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... all sorts of fun stuff!

### Sensitive Directories

Google's collection of web sites sharing sensitive directories. The files contained in here will vary from sesitive to top-secret!

### Various Online Devices

This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.

### Vulnerable Files

HUNDREDS of vulnerable files that Google can find on websites...

### Vulnerable Servers

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

## Tools which help to perform Google Hacking

There are two official websites which help us perform google hacking:

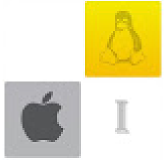
- http://www.hackersforcharity.org/
- https://www.exploit-db.com/

Also there is an app available on playstore named "Google Dorks" which can be used to learn basics of GHDB.

There are so many things to learn in GHDB and all of them cannot be mentioned in a single article. Hence, I am looking forward to open a new tab in this blog specially for GHDB. So, keep in touch..!

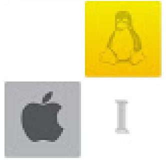
Share This: Facebook Twitter Google+

## Related Posts:



Methods to determine the OS of the target system

I have mentioned in my previous article about why determining the OS of target's system is so important when attacking. In this article, I am ... Read More

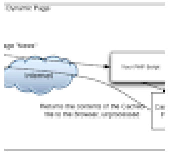


Footprinting and Reconnaissance - Determining the Operating System

Determining the Operating System on which the server runs is the most important part of Hacking. Mostly, hacking is breaking-into the target's s... Read More

Footprinting and Reconnaissance - Finding Companies' Restricted URLs

Restricted URLs provide an insight and understanding of the number of websites hosted on a particular server. Not only the number of website... Read More



Footprinting via Cached Pages

First of all, to know how to use cached data from search engines in hacking, we need to know what is cached data. Cached data is the data whi... Read More

Footprinting and Reconnaissance- Introduction

Normal 0 false false false EN-US X-NONE X-NONE ... Read More

Newer Post Home Older Post

## 0 comments:

## Post a Comment

Thanks for reading this article.

Please comment your reviews..This will help us improve.

Enter your comment...

Comment as: Google Accoun ▼

Publish Preview

## Popular Posts

-

Caller ID Spoofing - How to Call Anyone from Any Number and Unlimited Credits Trick..!

  Before going deep into which application to use for call spoofing and more, let us first understand the concept of caller id spoofing. ...

-
Email Footprinting - Trace an Email and Collect Information from it..!

  In the previous article, I wrote on Website Scraping, Website Monitoring and Website Mirroring . It contained the methodology of gather...

-

Making a simple C++ Keylogger - Download with Source Code

  Hello friends.. Today I am going to discuss here about the most awaiting post by our readers. You are going to learn about making a r...

-

  How to Cross-check your Facebook Profile Visitors..!

  Everyone loves to find out who is more interested in him and it is a human tendency. It has made this undeclared feature of facebook a...

-

  How to Unlock Pattern Lock or Password In Android Smartphone?

  Android is the most used Mobile OS in the world and Engineers from Google work so hard to make it more secure after every update. If y...

-

  Whois Lookup - Gather Information through Whois Footprinting

  Hello friends... This is out 100th article today. And we are excited to get response from all of you. Just before starting to study thi...

-

  How to get Direct Download Links

  If you are a movies lover like me then you too might be usually keep on searching for direct download links of your favorite movies. T...

-

  How I hacked GTU's Website - Admin Panel hack - Exams site - SQL Injection

  Once again, a flaw was found in GTU's website. But this time it's different as I found it :). BTW, if you don't know about l...

-

  GTU Website Hacked...!

  The Website got Hacked yesterday. It was not so late when I received a message in my group that GTU Website got Hacked..! At first I d...

- Spy on someone's facebook data in one click..!

Ever wondered how to spy on your someone's facebook account. Obviously, you would open his/her profile on facebook and look it u...

Search SEARCH

## Get FREE Articles via Email..!

Email address... SUBMIT

## Total Pageviews

6 5 8 2 9

## Trending..

### How I hacked GTU's Website - Admin Panel hack - Exams site - SQL Injection

Once again, a flaw was found in GTU's website. But this time it's different as I found it :). BTW, if you don't know about l...

## Pages

- Certified Ethical Hacking Tutorials
- Linux Tutorials

## Blog Archive

- ▶ 2018 (8)
- ▼ 2017 (100)
  - ▶ December (1)
  - ▶ October (1)
  - ▶ August (2)
  - ▶ June (3)
  - ▶ May (6)
  - ▼ April (6)
    - Rooting Android - Everything you need to know..!
    - Caller ID Spoofing - How to Call Anyone from Any N...
    - Gather Information Using Google Hacking

Latest Hacking Tools LEAKED..! - NSA Was Targettin...

Hacker Stole $800,000 From Russian ATMs Without Ev...

Anonymous hacks ISIS website and Infects them with...

- ▶ March (17)
- ▶ February (26)
- ▶ January (38)

## About Me

**Kadam Parikh**

View my complete profile

## Contact Form

Name

Email *

Message *

SEND