# Google Dorks

**FBI warning about new dangerous search tool?**

The **FBI** has sent a warning to police and other emergency personnel, about a 'deadly' new tool which 'malicious criminals' using for deadly effects against the **American government**.

The warning, reported by **Ars technica**, refers specifically to 'Google Dorking' also known as 'Google Dorks'. They use specialized syntax searches such as 'filetype:sql'.

'Google dorks' refers to search syntax which allow users to search within a specific website ( by using the term **URL** ) or for specific file types, they can also search for specific databases. These terms are widely known, and they are also legal. The warning is for organizations who don't know how to secure their databases properly.

## Is google dorks the 'weapon of the malicious'?

In October 2013, unknown attackers used 'google dorks' to search for vulnerable websites to find vulnerable versions of a so called '**internet Message Board Software**' product, according to the researchers, Says the **FBI warning**.

After they search for vulnerable software identifiers, the attackers were able to create new administrator account, on about 35,000 websites.

## Shocking searching employed web users

The warning also offers a useful link to Google's own testing Centre for preventing such attacks, the google hacking database.
Webmasters can use this to check if files are 'visible' to Google Dorks, and then hide them if they wish.

**Ars Technica** points out that the warning refers to 'malicious cyber criminals' and refers to a notorious case in which reporters were accused of 'hacking' a website by using freely available information and an automated tool, **GNU Get.**
However, as **Ars Technica** explains, the warning is not really meant to highlight a 'new' technique.

**Ars Technica** is warning webmasters for Google Dorks, urging them to keep their websites secure.

This warning from the **DHS** and the **FBI** was mostly intended to give law enforcement and other organizations a sense of urgency to take a hard look at their own website 'security' **Ars** comments.

Local police departments have increasingly become the target of the '**hacktivists**'.
Recent examples include attacks on the **Albuquerque police** department's network in March following the shooting of a homeless man and the attacks on the **St. Louis County Police** network in response to the recent events in **Ferguson, Missouri**.

The warning says; 'Ensure sensitive websites are not indexed in search engines. Google **USPER** provides webmaster tools to remove the entire site, individual **URL's**, cached copies and directories from Google's index.

## What is 'google dorks' exactly ?

Almost every website you visit has a private 'virtual notebook', also known as a database.
A database stores everything you do on their website.

If you give the website your phone number, credit card number or social security number, it stores your information in the '**virtual notebook'** of the website. When you leave the website you'd think that you are the only one that can see your information but, unfortunately, the whole world can get any information you have entered on almost every website, but only if your website doesn't hide private information from Google search. The search indexes of Google make everything public, including those '**virtual notebooks'** and everything stored in those notebooks.
If you gave your credit card number on a site, then there is a high chance that the site isn't secured and has put all the information public, Google will then automatically add the information to its search.
This information is very easy to find for anyone and especially for cyber-criminals because Google has made it so that anyone can do a google search with the word filetype: and then have access to the '**virtual notebook'**.

A person has contacted google when he found out about this 'Google Dorks' problem, he thought they would fix it. But he was wrong. Google was fully aware that people can find all your information, they felt like they could stop it, normally it's their job to 'censor or curate' their results unless they are required to do so by the law.

**From:** Google Security Team <security@google.com>;
**Date:** Tuesday, June 26, 2012 5:46 PM
**To:** princezuda@planetzuda.com <princezuda@planetzuda.com>;
**Subject:** Re: [#1052689843] Urgent privacy bug: Google indexing passwords, usernames, mysql backups, etc.

Hi Ryan,

Thank you for your report, I apologize it was not answered sooner. We do not consider these searches (commonly called "google dorks") to be a security risk that we can control. The amount and variety of information that is indexed on the internet precludes any sort of blacklisting system where certain information is removed. Additionally it is Google's long standing policy to not censor or curate our results except where required by law (such requests can be viewed at http://www.chillingeffects.com).

The best way to remove these results is for the affected website owners to remove the content from their website (or restrict access via robots.txt or another mechanism) and then submit a request for the content to be removed from the Google Cache.

Regards,
Kevin
The Google Security Team

This is the e-mail Google sent back to the person.

'Official letter from Google saying that they will not stop their search engine from exposing info from a database'.

# How do you use Google Dorks?

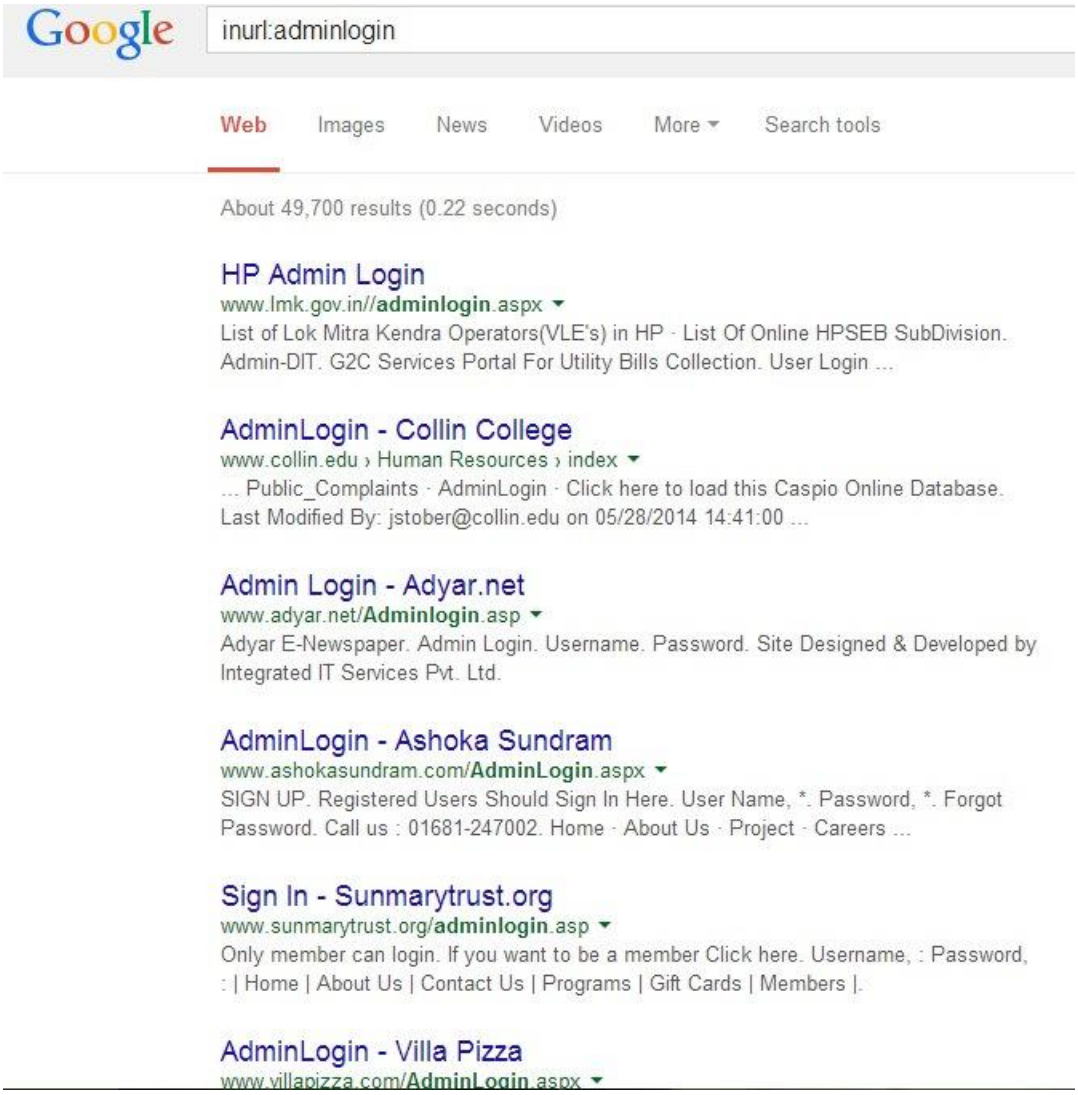
## Google hacking

I already explained what Google Dorks is.

So now I'm going to explain how hackers or cyber criminals use these Google Dorks to create complex query to Google search engine to extract the results that normal users can't.

Let's assume the hacker wants to find the admin login page of all websites; we have a Dork for this **INURL** because the hacker want to search admin login pages and generally admin login page's names look like adminlogin, login, etc.

So we write Dork - inurl:adminlogin




You can see on the screenshot that we have the admin login pages of tons of websites.

Similarly , we can now construct this Dork for any particular website.

So now we construct a Dork - **site:facebook.com inurl:login**

In the Dork above we combine two Dork sites and inurl, it will give us a Facebook login page, not an admin login page because Facebook restricts that page from google. You can try it for any website to find login or admin login pages.

let's try a more complex Google Dork now: **intext:"Hikvision" inurl:"login.asp"**

The Dork above will give us login the page of hikivision cameras that are installed like **cctv**.

**Example's**

Let's try some more complex and more interesting**: intext:phpMyAdmin SQL Dump filetype:sql intext:INSERT INTO `admin` (`id`, `user`, `password`) VALUES –github**

The above dork will find **sql** dump files which are dumped files of data from the website. So Here you can see all password and usernames and also all sensitive information that reside on the database

Another interesting example: **ext:mdb inurl:*.mdb inurl:fpdb shop.mdb**

The directory **"http:/xxx/fpdb/"** is the database folder used by some versions of FrontPage. It contains many types of Microsoft Access databases. It contains customer info like phone numbers but also plain text passwordsRemove the **shop.mdb** part to see the complete list of databases.

**ext:log "Software: Microsoft Internet Information Services *.*"**

Above Google Dork will give you the log files of the sites that have the Microsoft internet information server installed. This file includes ftp usernames, password, path information and database names.

**intitle:"WSO 2.4" [ Sec. Info ], [ Files ], [ Console ], [ Sql ], [ Php ], [ Safe mode ], [ String tools ], [ Bruteforce ], [ Network ], [ Self remove ]**

The above dork will find the ESO 2.4 shells uploaded by the hacker on any server.

**allintitle:”index.of” “backup files”**

This Dork above will give you the backup files of the server.

**intitle:”apache 1.3 documentation”**

The Dork above will show you the apache 1.3 documentation page directly.

Now you can see by yourself how easy you can use Google Dorks.
Always be sure that when you give your private information that the website is actually secured.
Because you can see how easy hackers can get all your information.