

Forum:[Hack Forums](#)

Thread: [USING GOOGLE TO FIND INTERESTING FILES AND DIRECTORIES](#)

Master in Online Business - December 20, 2016, 2:28 am

Using Google to find interesting files and directories

Using Google to find vulnerable targets can be very rewarding. However, it is often more rewarding to find not only vulnerabilities but to find sensitive data that is not meant for public viewing. People and organizations leave this type of data on web servers all the time (trust me, I've found quite a bit of it). Now remember, Google is only crawling a small percentage of the pages that contain this type of data, but the tradeoff is that Google's data can be retrieved from Google quickly, quietly and without much fuss.

It is not uncommon to find sensitive data such as financial information, social security numbers, medical information, and the like.

How this technique can be used

Of all the techniques examined this far, this technique is the hardest to describe because it takes a bit of imagination and sometimes just a bit of luck. Often the best way to find sensitive files and directories is to find them in the context of other "important" words and phrases.

Example: Consider the fact that many people store an entire hodgepodge of data inside backup directories. Often times, the entire content of a web server or personal computer can be found in a directory called backup. Using a simple query like "inurl:backup" can yield potential backup directories, yet refining the search to something like

"inurl:backup intitle:index.of inurl:admin" can reveal even more relevant results.

A query like "inurl:admin" can often reveal administrative directories. Several combinations of this query are often fruitful. For example:

"inurl:admin intitle:login" can reveal admin login pages

"inurl:admin filetype:xls" can reveal interesting Excel spreadsheets either named "admin" or stored in a directory named "admin". Educational institutions are notorious for falling victim to this search.

"inurl:admin inurl:userlist" is a generic catch-all query which finds many different types of administrative userlist pages. These results may take some sorting through, but the benefits are certainly worth it, as results range from usernames, passwords, phone numbers, addresses, etc.

"inurl:admin filetype:asp inurl:userlist" will find more specific examples of an administrator's user list function, this time written in an ASP page. In most cases, these types of pages do not require authentication

Have fun when Using Google to find interesting files and directories ?

Mr.Peanut - December 20, 2016, 2:30 am

Just posting here to be first on this shit. I read 1/2 of this and know this is going to be interesting. Cheers for the share op.

SIM-1534439 - December 20, 2016, 2:30 am

You are on fire my son! Posting like a maniac.

Kisame? - December 20, 2016, 2:31 am

Looks nice, however I wonder how much important stuff there could be stored on an open server without authentication. You wont find for example a persons dropbox backup since those arent public.

Also I think that everything you view like this has been viewed a lot of times before you. However, still an interesting idea. Nice post.

Master in Online Business - December 20, 2016, 3:10 am

(Dec 20, 2016 03:30 AM)Mr.Peanut Wrote: [\[CITE\]](#) Just posting here to be first on this shit. I read 1/2 of this and know this is going to be interesting. Cheers for the share op.
LOL you very funny bro?

Warxz - December 20, 2016, 3:40 am

Thanks a lot for sharing OP. Didn't knew you were able to do this!

SchwererGustav - December 20, 2016, 4:45 pm

nice tut dude ,keep up the good work

cb3rob - December 22, 2016, 12:37 pm

Just what I needed. Thx for sharing