

## Google Hacking Database (GHDB)

Google Hacking Database sitesi yüzlerce google dork'unun hazır olarak sunulduğu ve belirli bir tasnife tabi tutulduğu sistemin adıdır. Bu sisteme aşağıdaki adresten ulaşılır.

<https://www.exploit-db.com/google-hacking-database/>

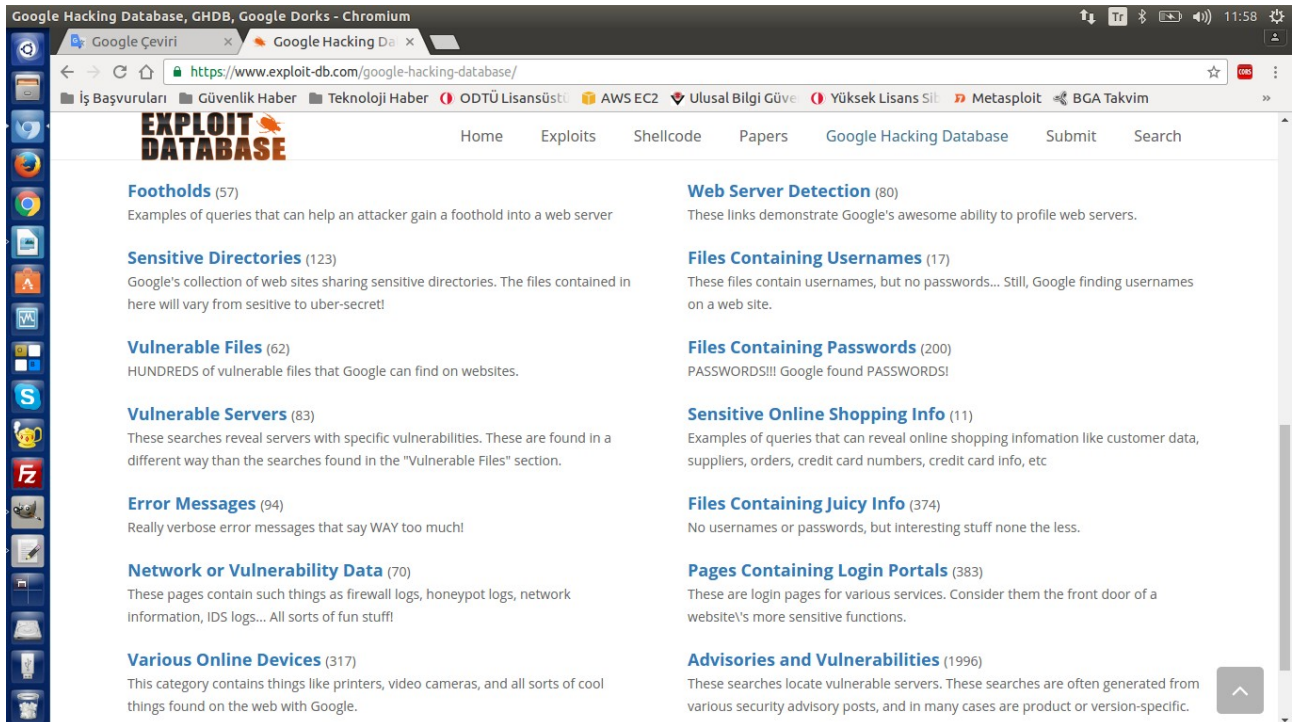
Output:



The screenshot shows the Google Hacking Database (GHDB) website. The page title is "Google Hacking Database (GHDB)" and the subtitle is "Search the Google Hacking Database or browse GHDB categories". There is a search bar with a dropdown menu set to "Any Category" and a "SEARCH" button. Below the search bar is a table with the following data:

Date	Title	Category
2016-11-29	"PHP Mailer" "priv8 Mailer" ext:php	Footholds
2016-11-29	inurl:".esy.es/default.php"	Sensitive Directories
2016-11-29	"PHP Credits" "Configuration" "PHP Core" ext:php inurl:info	Web Server Detection
2016-11-29	Hostinger © 2016. All rights reserved inurl:default.php	Sensitive Directories
2016-11-29	intitle:"Integrated Dell Remote Access Controller 6 - Enterprise"	Pages Containing Login Portals
2016-11-29	Mez4-Mail ext:php	Footholds

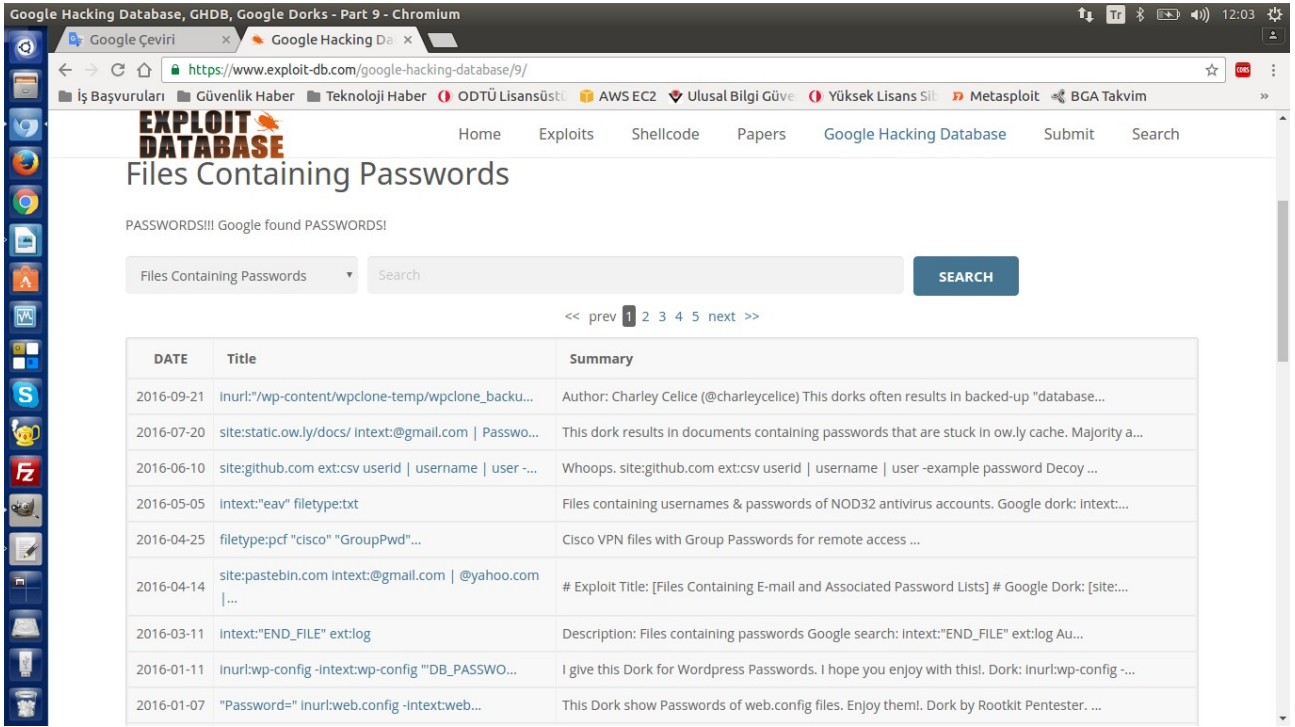
Ana sayfada sisteme en son eklenen dork'lar sıralanmaktadır. Aşağıda ise sistemde depolu dork'ların kategorileri yer almaktadır.



The screenshot shows the Google Hacking Database (GHDB) website. The page title is "Google Hacking Database (GHDB)" and the subtitle is "Search the Google Hacking Database or browse GHDB categories". There is a search bar with a dropdown menu set to "Any Category" and a "SEARCH" button. Below the search bar is a list of categories with their respective counts and descriptions:

Category	Count	Description
Footholds	57	Examples of queries that can help an attacker gain a foothold into a web server
Sensitive Directories	123	Google's collection of web sites sharing sensitive directories. The files contained in here will vary from sensitive to uber-secret!
Vulnerable Files	62	HUNDREDS of vulnerable files that Google can find on websites.
Vulnerable Servers	83	These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section.
Error Messages	94	Really verbose error messages that say WAY too much!
Network or Vulnerability Data	70	These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... All sorts of fun stuff!
Various Online Devices	317	This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.
Web Server Detection	80	These links demonstrate Google's awesome ability to profile web servers.
Files Containing Usernames	17	These files contain usernames, but no passwords... Still, Google finding usernames on a web site.
Files Containing Passwords	200	PASSWORDS!!! Google found PASSWORDS!
Sensitive Online Shopping Info	11	Examples of queries that can reveal online shopping information like customer data, suppliers, orders, credit card numbers, credit card info, etc
Files Containing Juicy Info	374	No usernames or passwords, but interesting stuff none the less.
Pages Containing Login Portals	383	These are login pages for various services. Consider them the front door of a website's more sensitive functions.
Advisories and Vulnerabilities	1996	These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

Biz "File Containing Passwords", yani *Şifre içeren Dosyalar* kategorisine girelim. Kategoriye girdiğimizde ekrana şifre içeren dosyaları verecek sistemde kayıtlı tüm dork'lar sıralanacaktır.



The screenshot shows the Exploit Database website interface. The search results are displayed in a table with columns for DATE, Title, and Summary. The first result is dated 2016-09-21 and has the title 'inurl:"/wp-content/wplclone-temp/wplclone\_backup...'. The summary for this result is 'Author: Charley Celice (@charleycelice) This dorks often results in backed-up "database...'. There are 8 results in total, with the first one being highlighted.

DATE	Title	Summary
2016-09-21	inurl:"/wp-content/wplclone-temp/wplclone_backup...	Author: Charley Celice (@charleycelice) This dorks often results in backed-up "database...
2016-07-20	site:static.ow.ly/docs/ Intext:@gmail.com   Passwo...	This dork results in documents containing passwords that are stuck in ow.ly cache. Majority a...
2016-06-10	site:github.com ext:csv userid   username   user -...	Whoops. site:github.com ext:csv userid   username   user -example password Decoy ...
2016-05-05	intext:"eav" filetype:txt	Files containing usernames & passwords of NOD32 antivirus accounts. Google dork: Intext:...
2016-04-25	filetype:pcf "cisco" "GroupPwd"...	Cisco VPN files with Group Passwords for remote access ...
2016-04-14	site:pastebin.com intext:@gmail.com   @yahoo.com   ...	# Exploit Title: [Files Containing E-mail and Associated Password Lists] # Google Dork: [site:...
2016-03-11	intext:"END_FILE" ext:log	Description: Files containing passwords Google search: Intext:"END_FILE" ext:log Au...
2016-01-11	inurl:wp-config -intext:wp-config ""DB_PASSWO...	I give this Dork for Wordpress Passwords. I hope you enjoy with this! Dork: inurl:wp-config -...
2016-01-07	"Password=" inurl:web.config -intext:web...	This Dork show Passwords of web.config files. Enjoy them! Dork by Rootkit Pentester. ...

Ekrana verilen tabloya göre dork'un sisteme eklendiği tarih, dork'un kendisi ve dork'u açıklayan metin sunulmaktadır. En baştaki

Date	Title	Summary
2016-09-21	inurl:"/wp-content/wplclone-temp/wplclone_backup/"	...

kaydına girelim.



Home Exploits Shellcode Papers Google Hacking Database Submit Search

inurl:"/wp-content/wplclone-temp/wplclone\_backup/"

Previous

Google Dork Description: inurl:"/wp-content/wplclone-temp/wplclone\_backup/"

Google Search: inurl:"/wp-content/wplclone-temp/wplclone\_backup/"

Submitted: 2016-09-21

Author: Charley Celice (@charleycelice)

This dorks often results in backed-up "database.sql" files, which contain WordPress usernames and passwords.

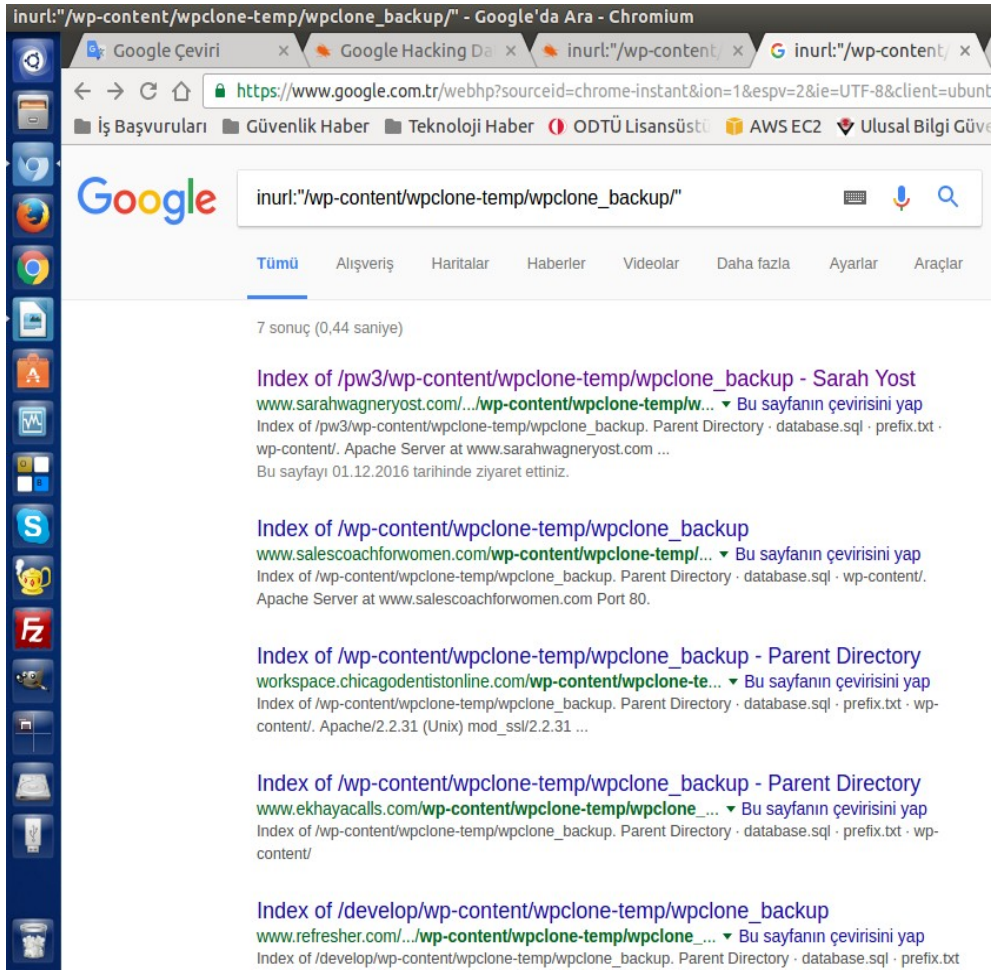
-stmerry

Görüldüğü üzere ekrana google arama kutucuğuna gireceğimiz dork ve o dorkun ne iş yaptığına dair bir açıklama verilmiştir. Açıklamaya göre dork database.sql dosyasını sunan web sitelerini ekrana verecektir. database.sql dosyası bir tür veritabanı backup dosyasıdır. database.sql wordpress uygulamalarında sıkça görünen, veritabanının herşeyini alan yedek dosyasıdır. Bu dosya ele geçerse şifreler de ele geçmiş olacaktır.

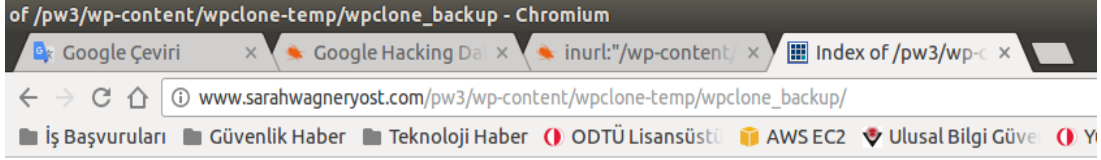
Şimdi dork'umuzu google'a girelim:

> inurl:"/wp-content/wpclone-temp/wpclone\_backup/"

Output:



Herhangi birine (örneğin ilk linke) tıklayalım:

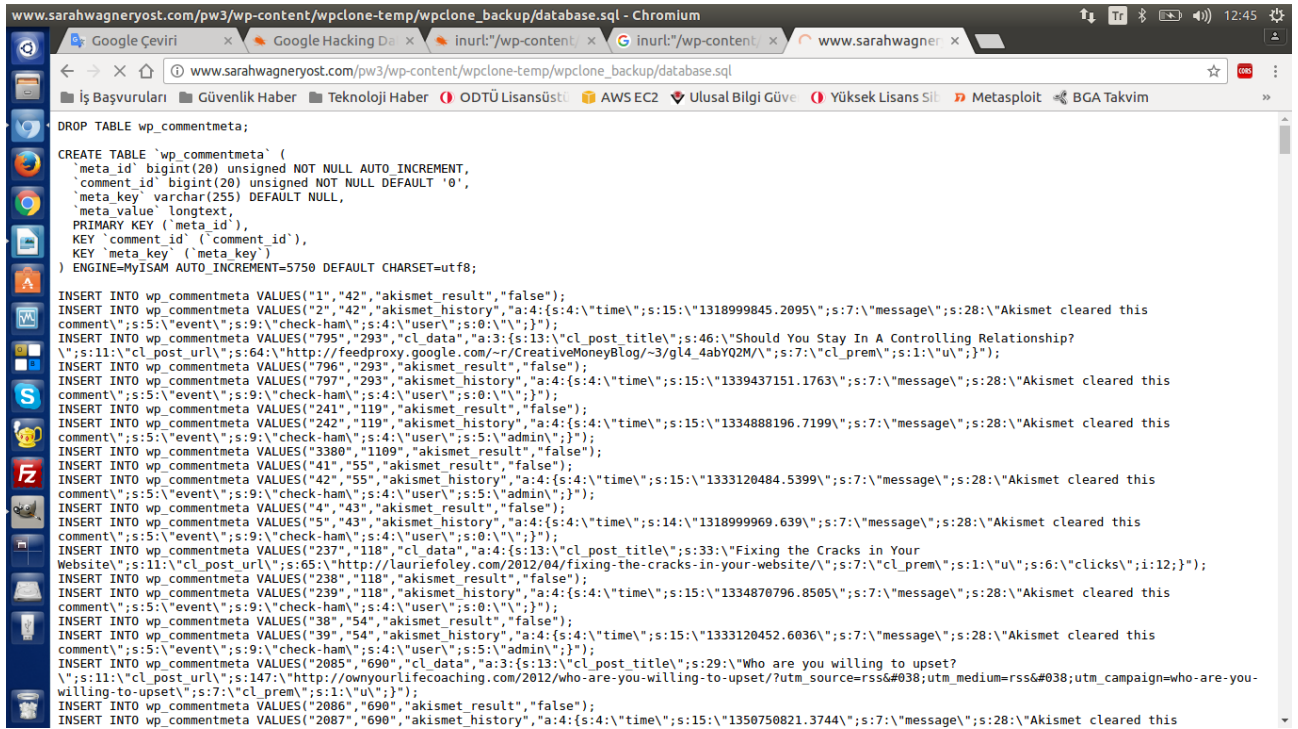


## Index of /pw3/wp-content/wpclone-temp/wpclone\_backup

- [Parent Directory](#)
- [database.sql](#)
- [prefix.txt](#)
- [wp-content/](#)

Apache Server at www.sarahwagneryost.com Port 80

Görüldüğü üzere bir wordpress uygulamasındaki izin ifşası zafiyeti sayesinde database.sql dosyasını görüntüleyebilir olduk. Şimdi database.sql dosyasını içine girelim:



Görüldüğü üzere backup dosyası önce bir tablo oluşturmakta ve sonra tabloya veriler insert etmekte. Yani bu sql dosyası bir veritabanına import edildiğinde o tablo oluşacaktır ve içine belirtilen girdiler girilecektir.

Sonuç olarak database.sql dosyası veritabanından export'lanarak oluşturulan bir backup dosyası olduğu için veritabanını komple tüm var olan içerikleriyle beraber baştan oluşturabilme yetisine sahiptir. O yüzden bu sql dosyası içerisinde illaki daha önceden girilmiş bir admin kullanıcı adı ve şifre bilgileri kayıt olarak yer alacaktır. Dolayısıyla bu sql dosyasını yerel sistemimize wget ile indirip inceleyerek kullanıcı adı ve şifre bilgilerine ulaşabiliriz. Ardından hedef wordpress uygulamasına login olup ana sayfasına "Hack'lendiniz" türü şeyler koyabiliriz. Görüldüğü üzere kullandığımız dork ile sürüyle wordpress uygulaması hack'lenebilir.

Not: database.sql dosyasındaki şifre hash formatında olabilir. O nedenle JTR'ye ihtiyaç var.

## **Makaleden Çıkan Tanımlar**

Google dork zafiyet içeren siteleri bulmamızı sağlayan kodlara denir. Daha geniş tanımlayacak olursak google dork belirlediğimiz kriterlere uygun zafiyetlere sahip siteleri bulmamızı sağlayan kodlara denir. GHDB ise yüzlerce google dork'larının yer aldığı ve kategorize edildiği veritabanına denir.

## **Yararlanılan Kaynak**

<https://www.youtube.com/watch?v=d3NzsrnVrlw>

Tez Raporu/İnternette Edinilmiş Kıymetli Bilgiler/Elden Geçirdiğim Notlar/What is Dork.docx