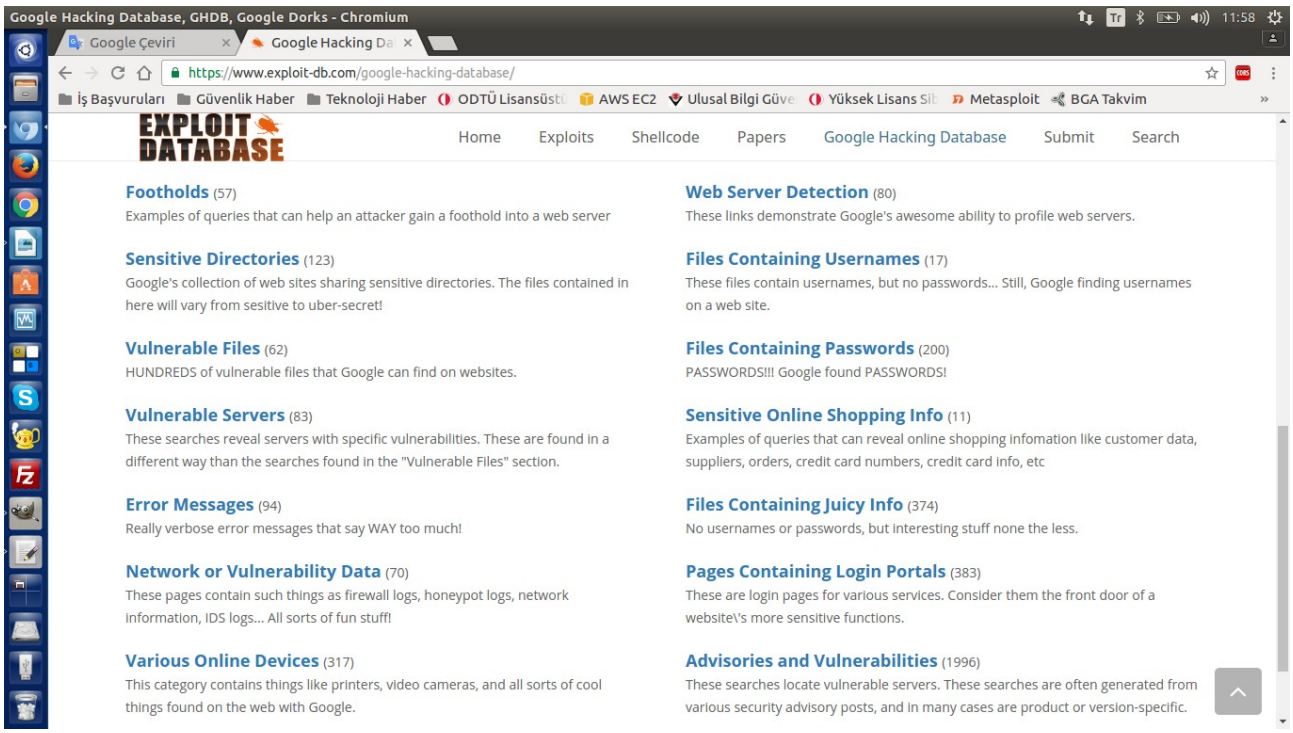
Google Hacking Database (GHDB)

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

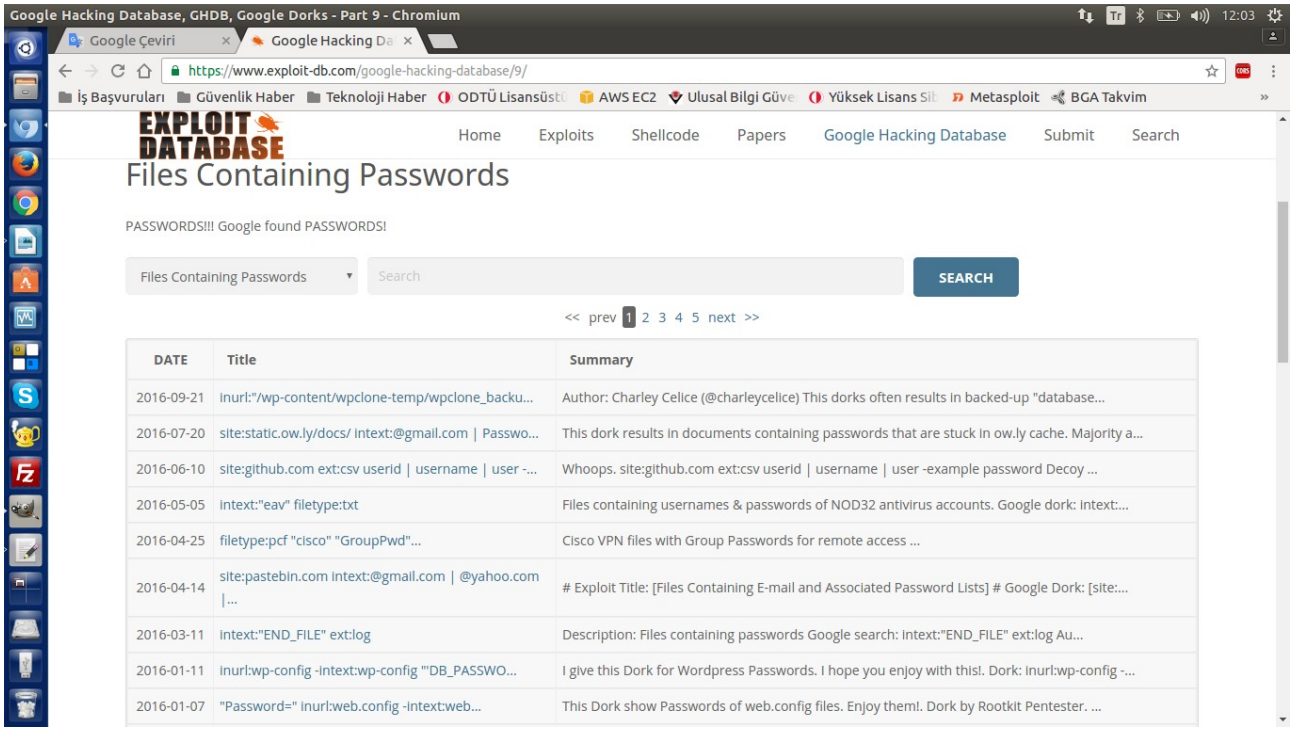
https://www.exploit-db.com/google-hacking-database/

Output:

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



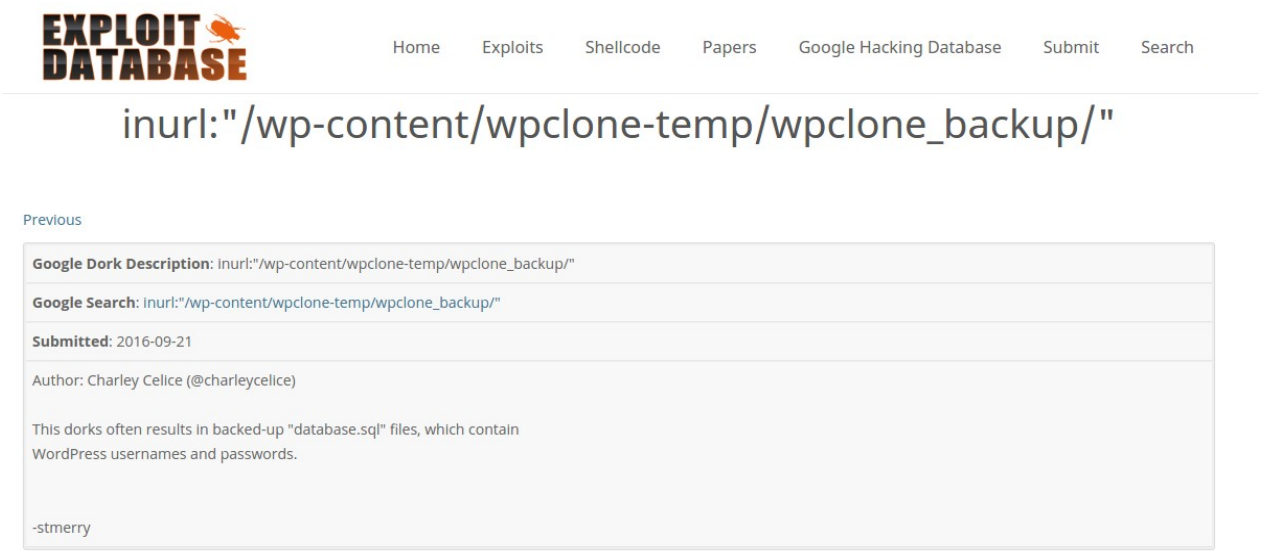
Biz “File Containing Passwords”, yani *Şifre içeren Dosyalar* kategorisine girelim. Kategoriye girdiğimizde ekrana şifre içeren dosyaları verecek sistemde kayıtlı tüm dork'lar sıralanacaktır.



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

Date	Title	Sumary
2016-09-21	inurl:"/wp-content/wpclone-temp/wpclone_backup/"	...

kaydına girelim.

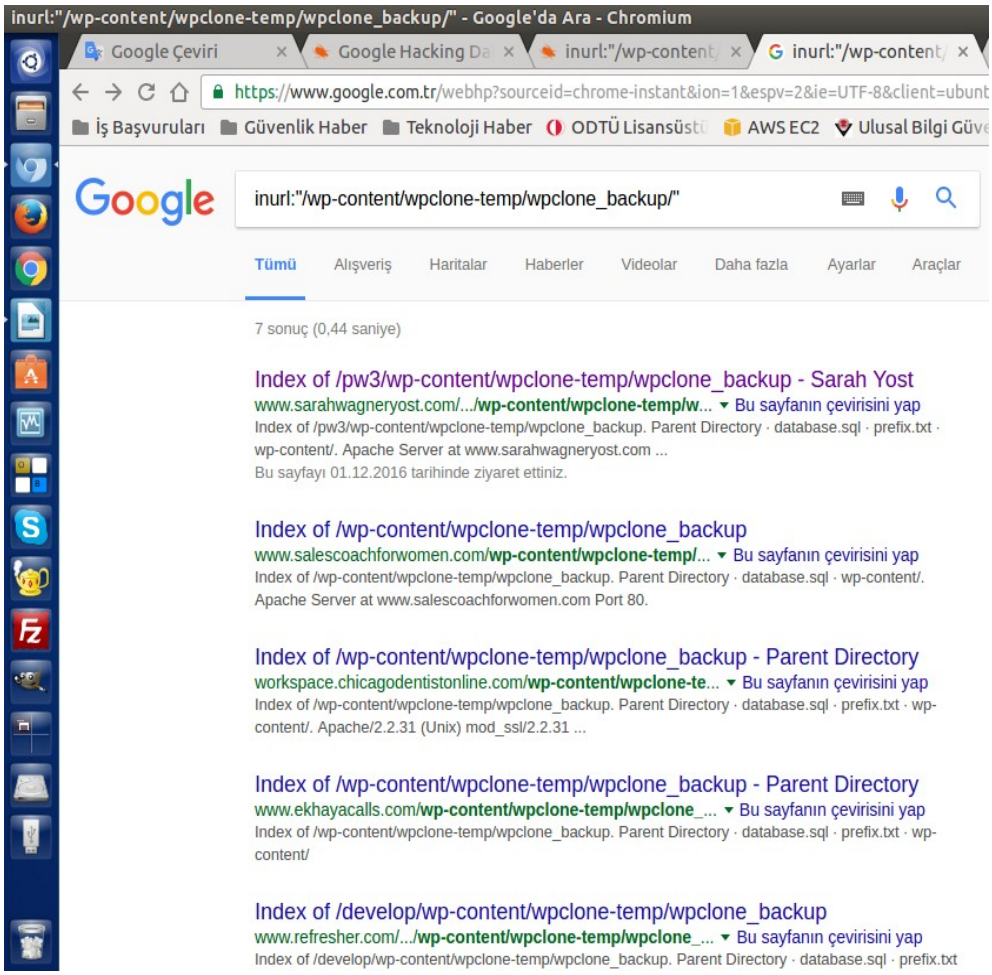


Görüldüğü üzere ekrana google arama kutucuğuna gireceğimiz dork ve o dorkun ne iş yaptığına dair bir açıklama verilmiştir. Açıklamaya göre dork database.sql dosyasını sunan web sitelerini ekrana verecektir. database.sql dosyası bir tür veritabanı backup dosyasıdır. database.sql wordpress uygulamalarında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

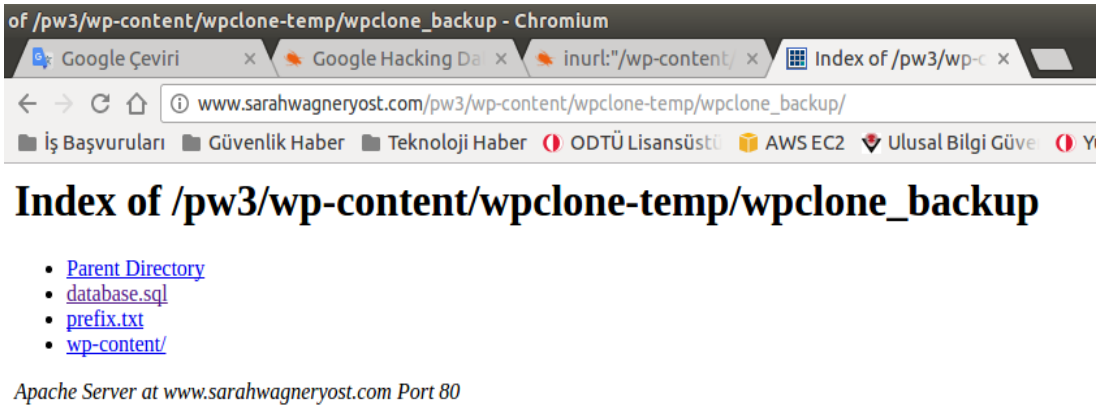
Şimdi dork'umuzu google'a girelim:

> inurl:"/wp-content/wpclone-temp/wpclone_backup/"

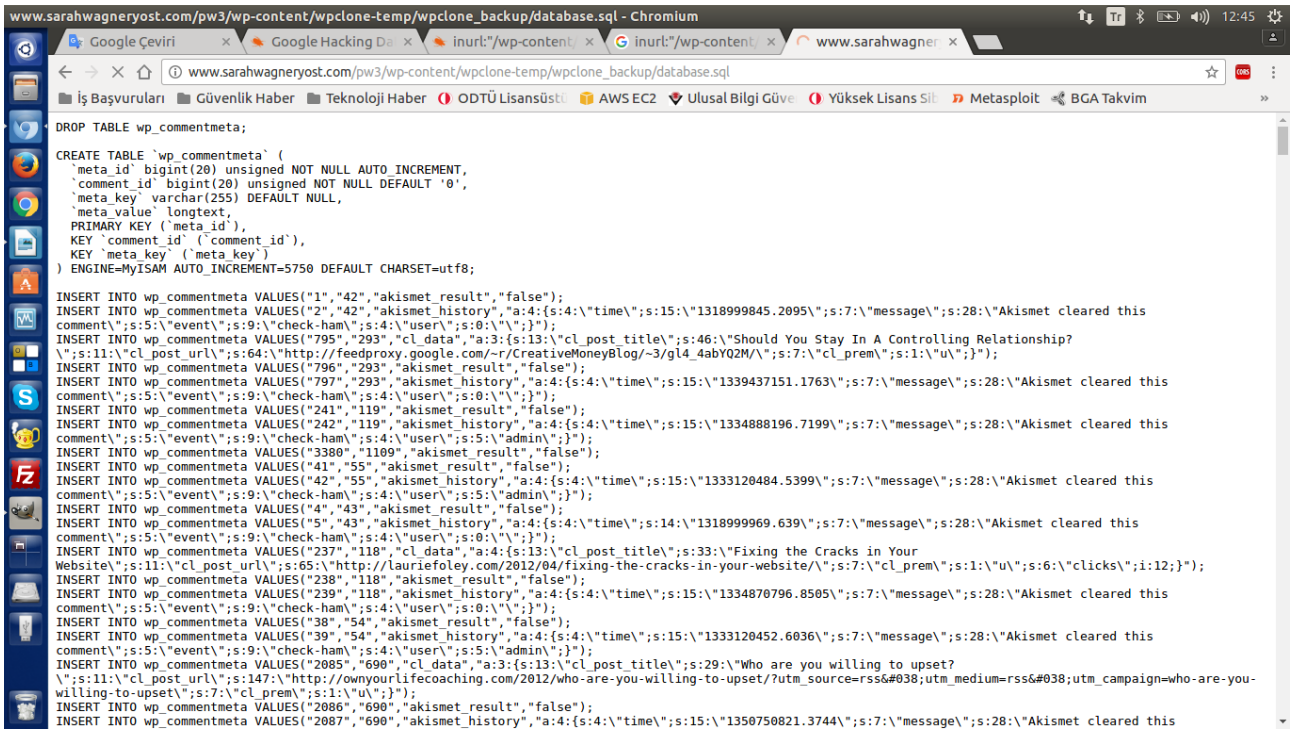
Output:



Herhangi birine (örneğin ilk linke) tıklayalım:



Görüldüğü üzere bir wordpress uygulamasındaki dizin 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=d3NzsrmVrlw

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