SQL ENJEKSİYON

Öğretim Görevlisi A. Berika VAROL MALKOÇOĞLU

BEYKOZ ÜNİVERSİTESİ

İçindekiler

- Metasploitable Yükleme
- SQL Enjeksiyon

SQL Enjeksiyon

- Veritabanını tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir.
- SQL Enjeksiyon sayesinde saldırganlar web sitesindeki;
  - Kullanıcı bilgilerini çalabilir,
  - Gizlenmiş bilgilere ulaşabilir,
  - Mevcut verilere müdahale edebilir,
  - Bazı işlemleri değiştirebilir,
  - Yetkisini yükseltebilir,
  - Veritabanını komple silebilir.

SQL Enjeksiyon için Açık Bulmak

- SQL Injection bir sitede aranıp bulunurken arama kutularına ‘(tırnak) işareti koymak gerekir.
- Bu tür özel karakterler form girdilerine denenerek sayfada veritabanı hatası almayı çalışılır.
- Böylelikle SQL açığı olup olmadığı manuel bir şekilde aranmış olur.

SQL Enjeksiyon için Açık Bulmak

- Otomatik algılama için **SQLMap** gibi özel araçlar mevcuttur.
- SQLMap veritabanın kullanıcılarını, parolalarını, hash değerlerini, rolleri, tabloları, sütunları gibi bilgileri tespit edebilen bir araçtır.
- Açık kaynaklı bir yazılımdır.
- Kali Linux işletim sistemine kurulu olarak gelir.
- Bunun yanında Acunetix, Netsparker, Vega gibi bilgi toplama araçları SQL açığı aranırken kullanılabilir.

SQL Enjeksiyon İçin

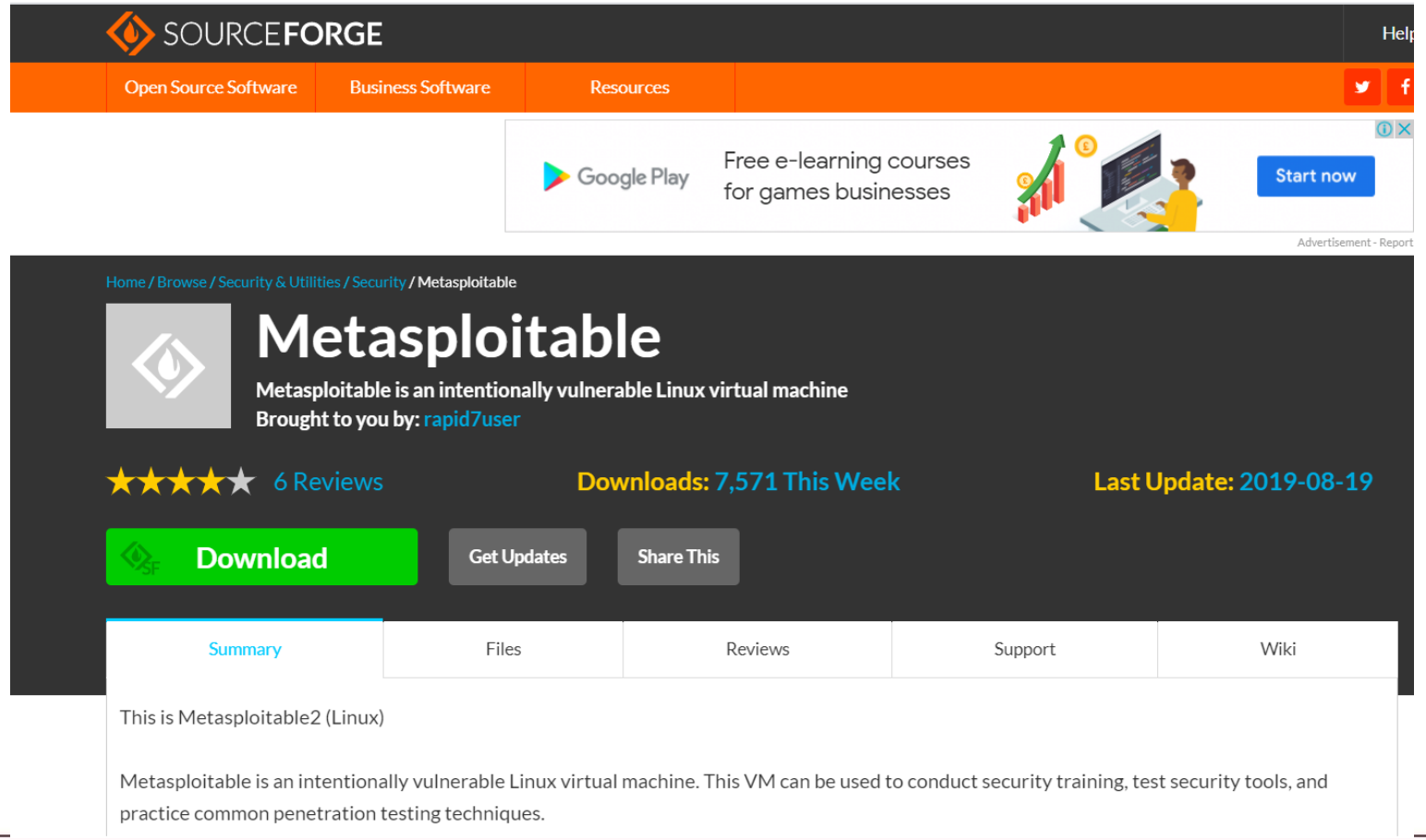
- Mutillidea web sitesini kullanıcağız.
- Mutillidea , Web uygulama güvenliği alanında kendini geliştirmek isteyen pentesterlar ve güvenlik ile uğraşanlar için PHP ile oluşturulmuş içinde belli web zafiyetlerini barındıran bir eğitim sistemidir.
- Bunu için Metasploitable yükleyeceğiz.
- Mutillidea içinde manuel açık arama gerçekleştireceğiz.

Metasploitable Yükleme

- Hacklenmesi içi yapılmış bir sanal makinedir.
- Metasploit aracının test edilebilmesi için geliştirilmiştir.
- Sızma testleri için olanak sağlayan bir sistem.
- Amacımız içindeki açıkları kullanarak saldırmak.

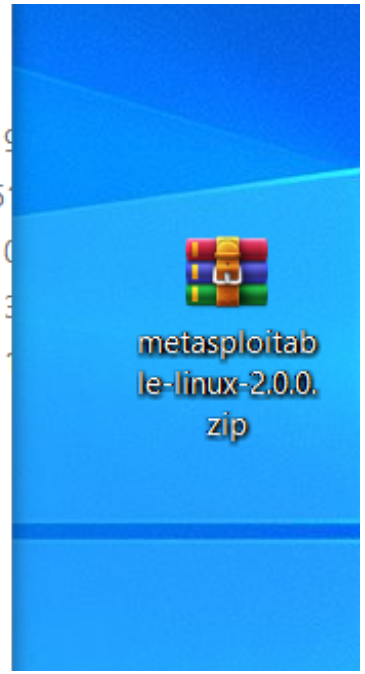
- Kurulumu: https://sourceforge.net/projects/metasploitable/

Metasploitable Yükleme

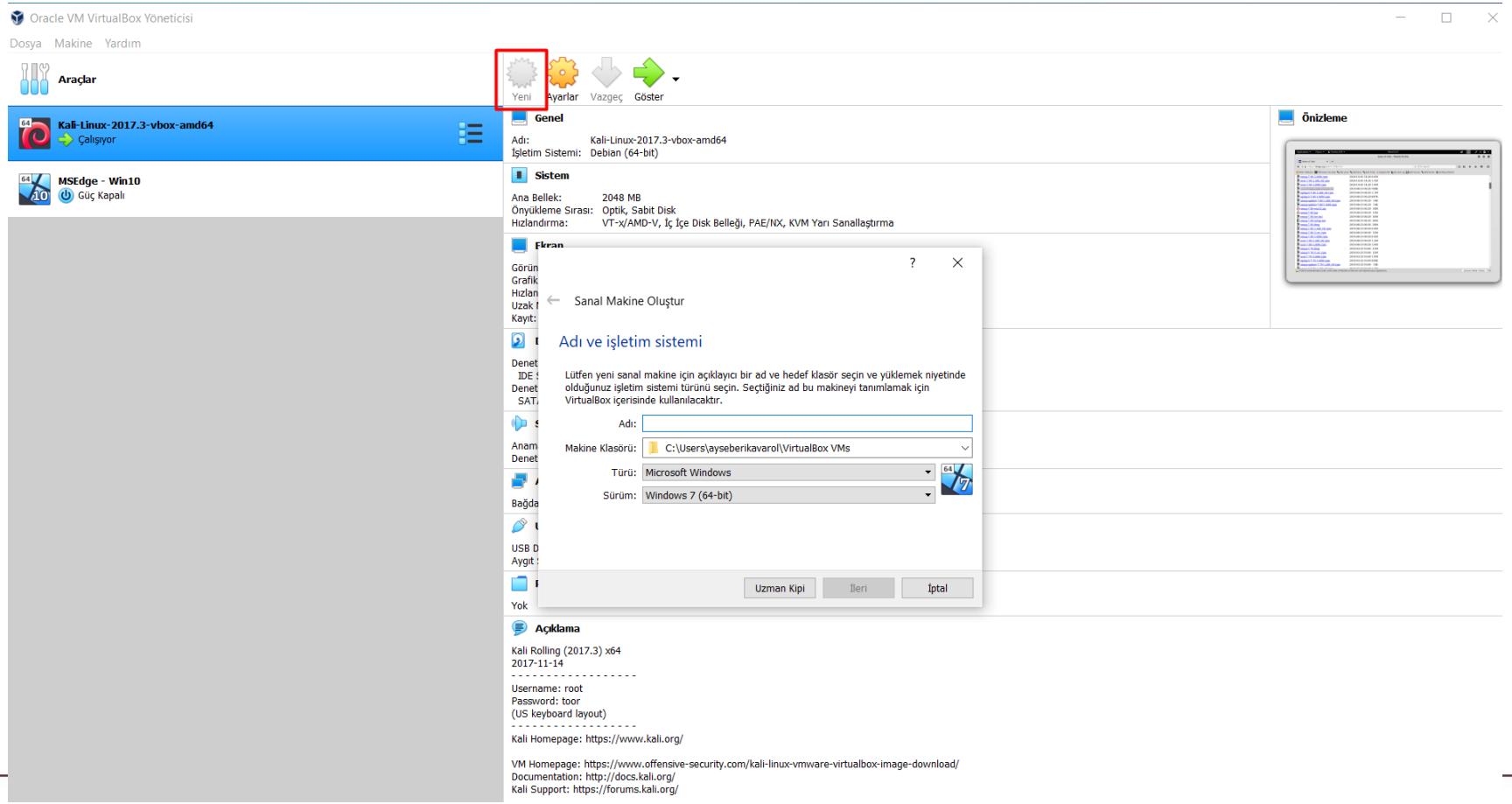


Metasploitable Yükleme

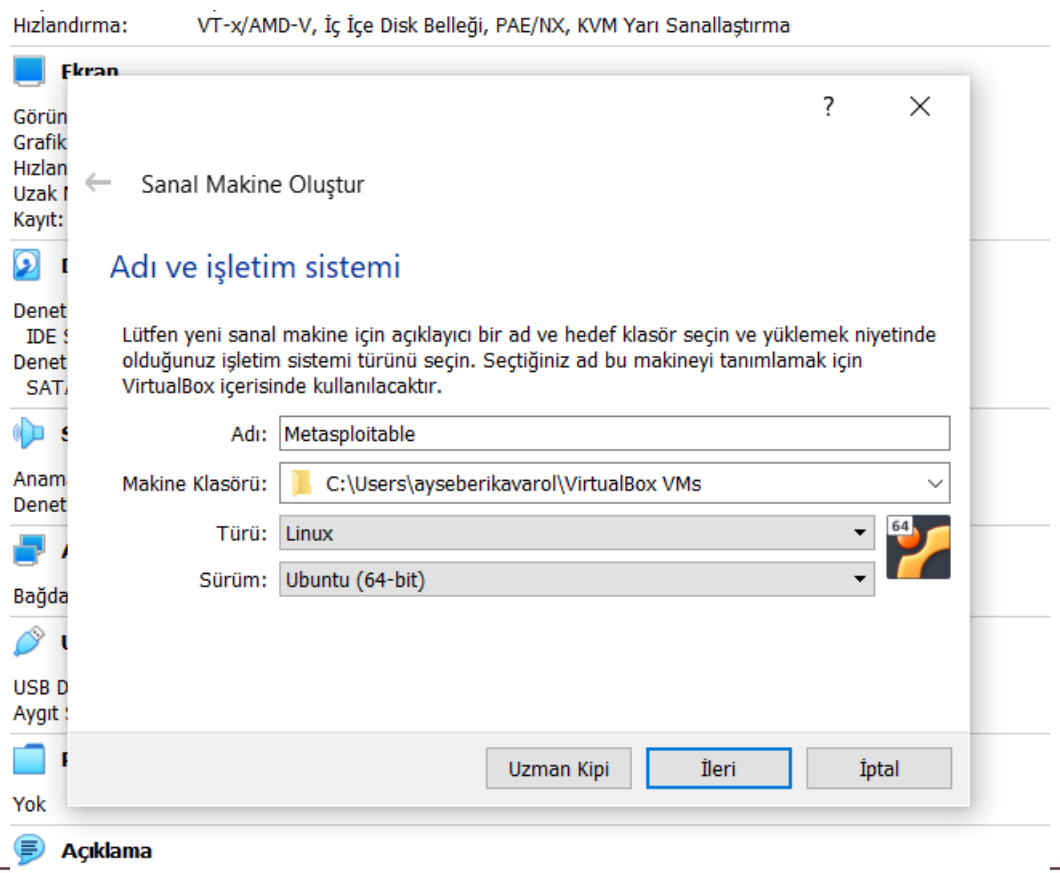
Ad	Değiştirme tarihi	Tür	Boyut
Metasploitable.nvram	20.05.2012 14:56	NVRAM Dosyası	9
Metasploitable.vmdk	20.05.2012 15:01	Virtual Machine Di...	1.880.5
Metasploitable.vmsd	7.05.2010 14:46	VMSD Dosyası	0
Metasploitable.vmx	20.05.2012 15:00	VMX Dosyası	3
Metasploitable.vmxf	7.05.2010 14:46	VMXF Dosyası	1



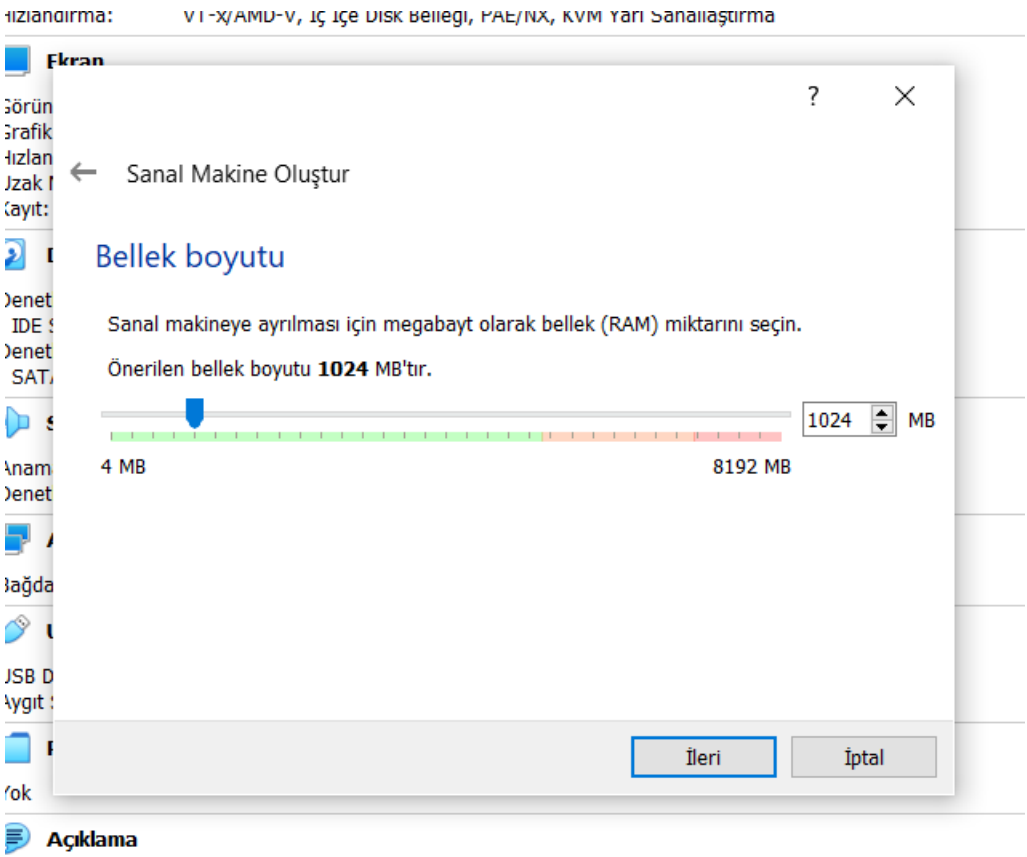
Metasploitable Yükleme



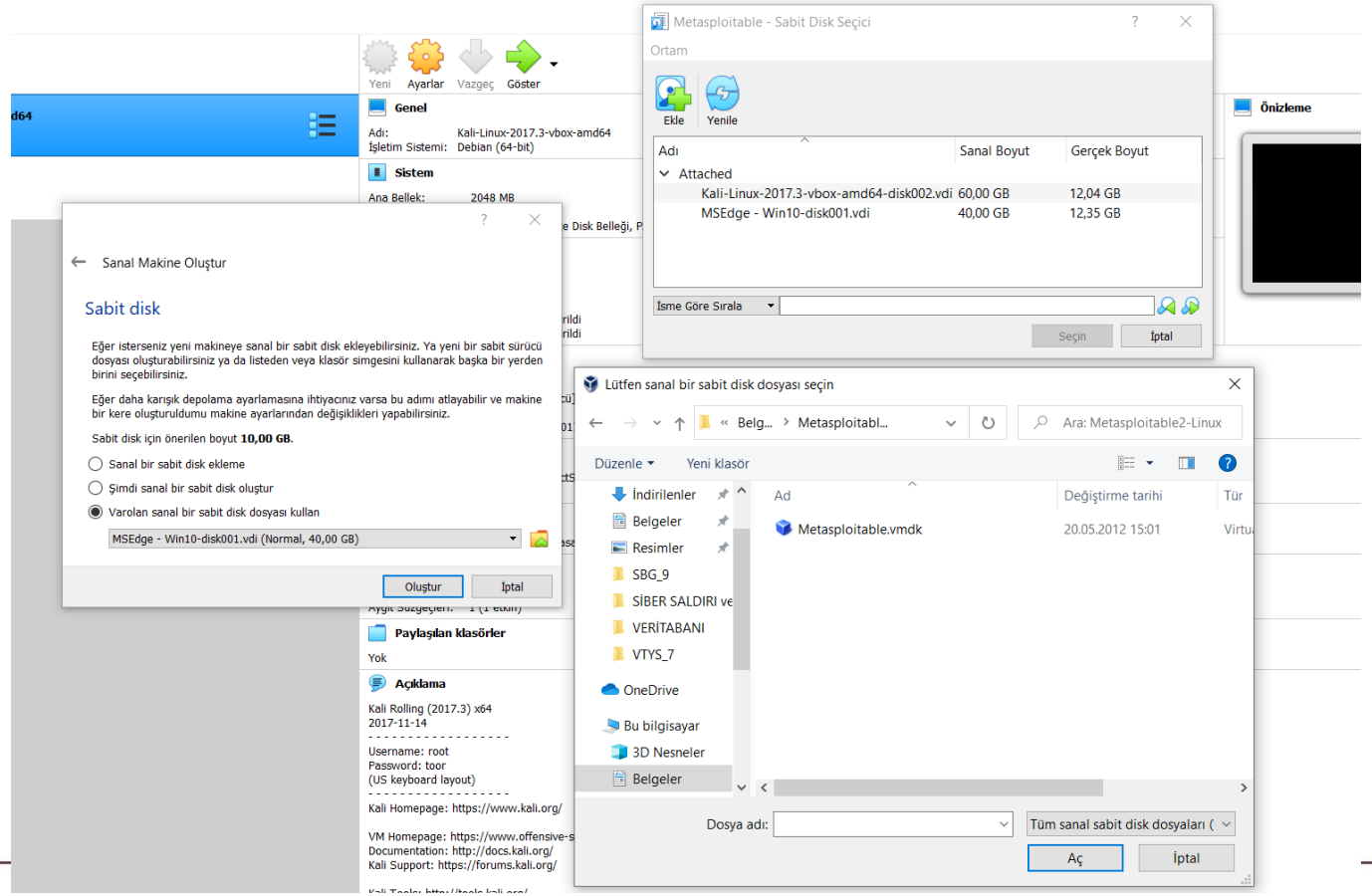
Metasploitable Yükleme



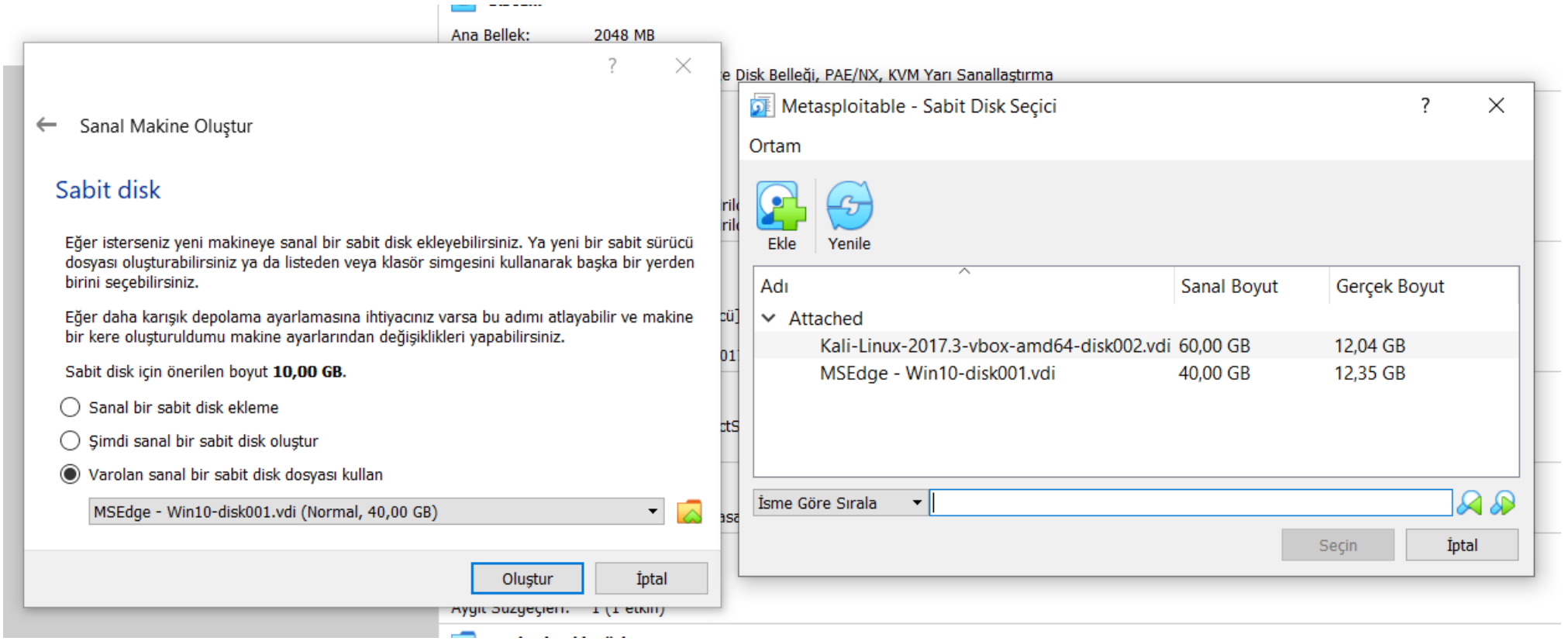
Metasploitable Yükleme



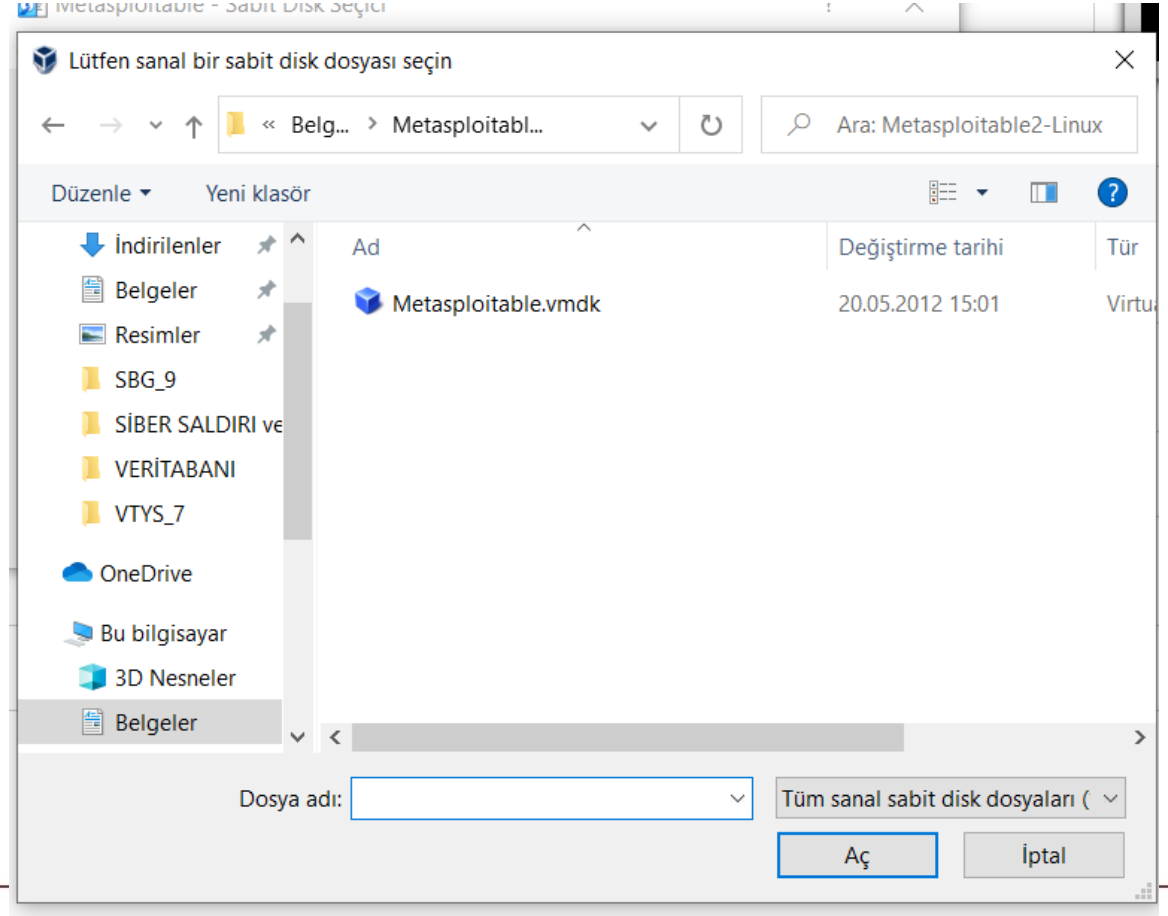
Metasploitable Yükleme



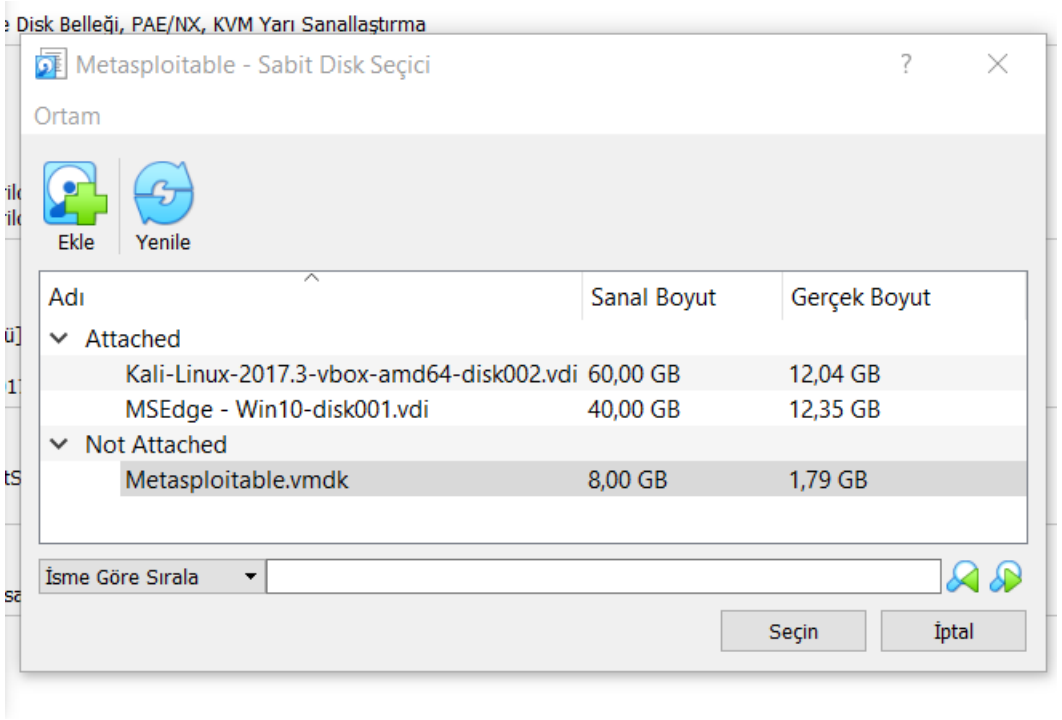
Metasploitable Yükleme



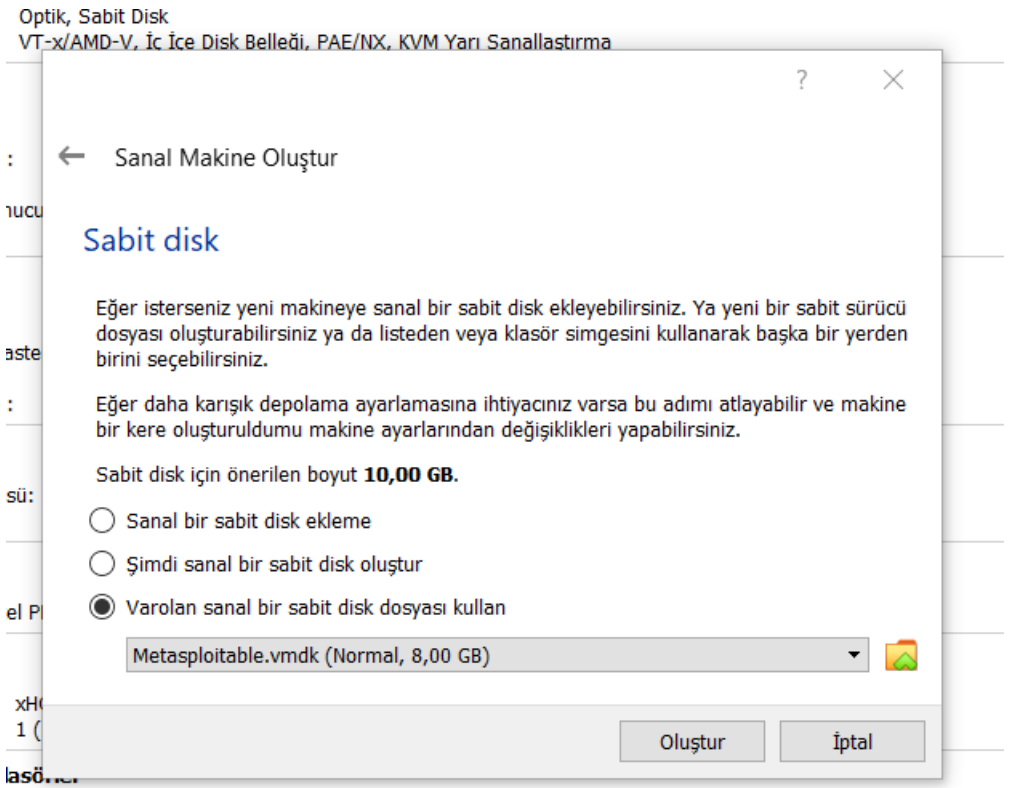
Metasploitable Yükleme



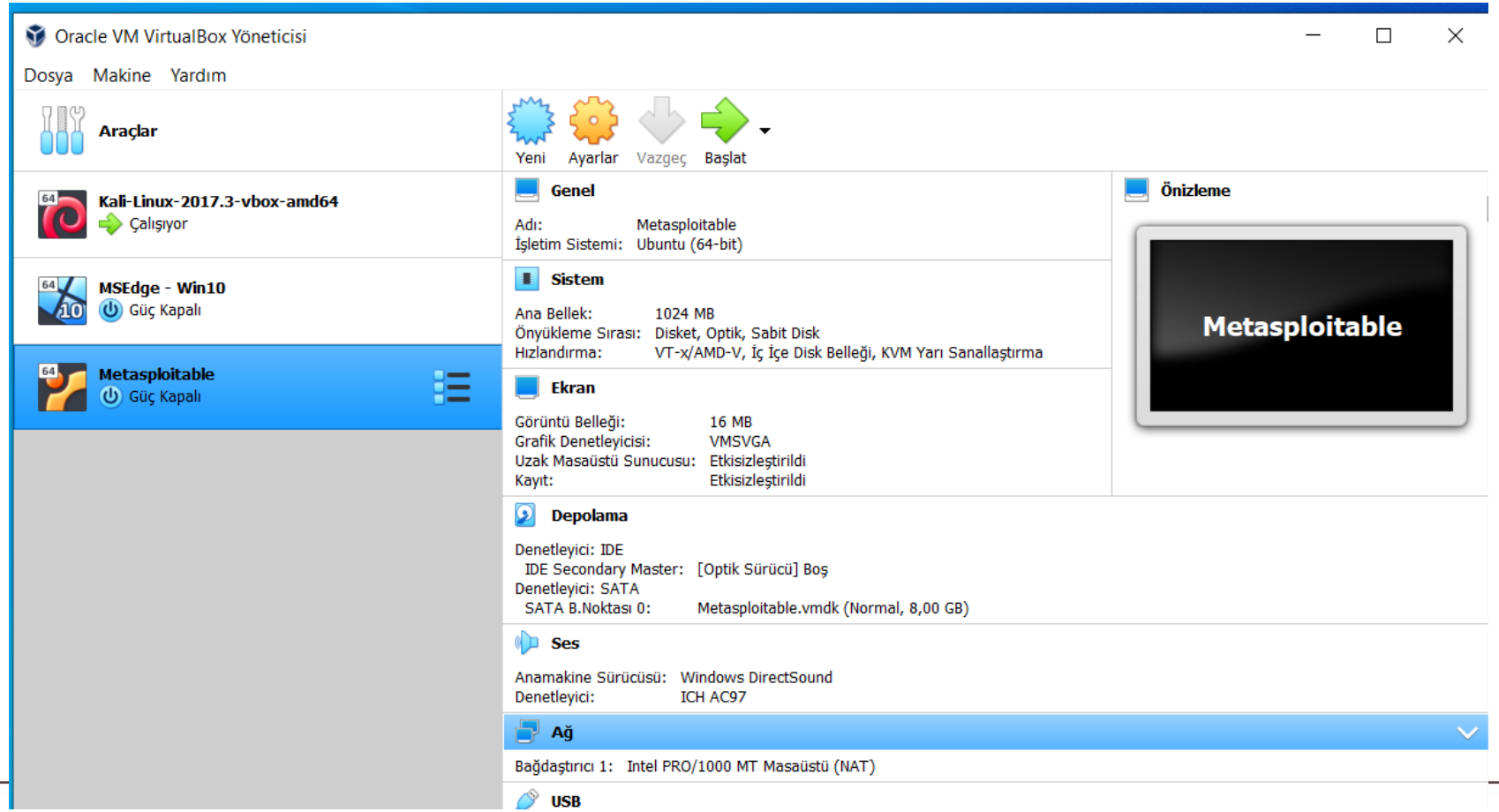
Metasploitable Yükleme



Metasploitable Yükleme

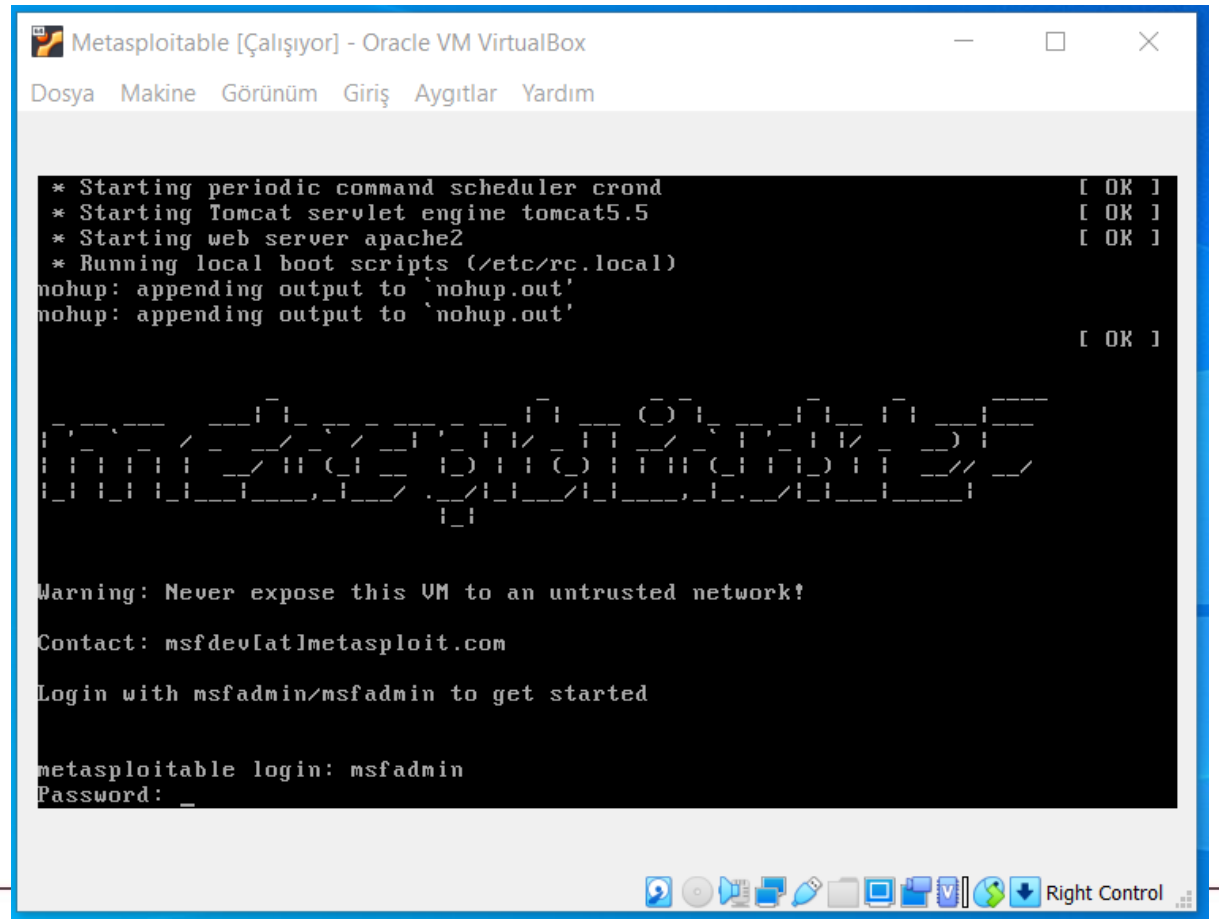


Metasploitable Yükleme

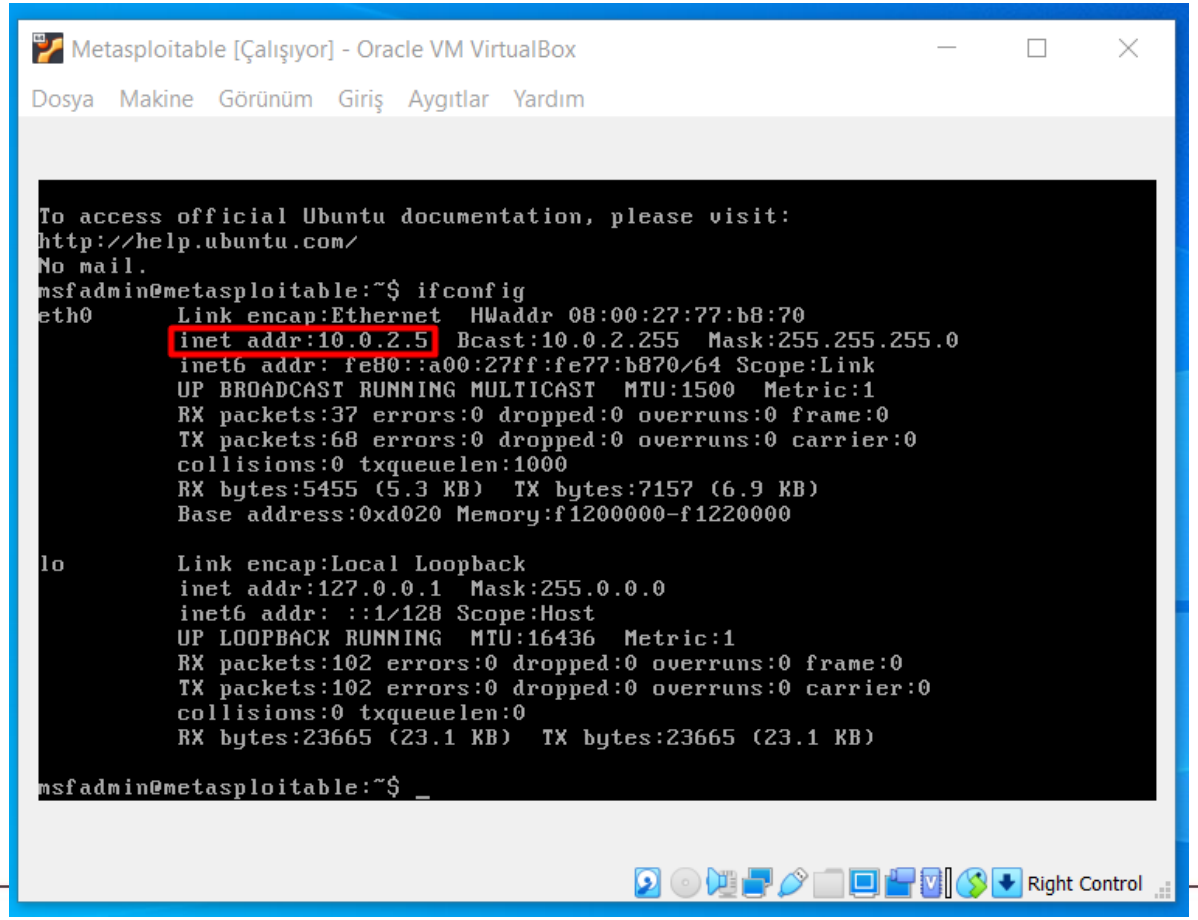


BEYKOZ ÜNİVERSİTESİ

Metasploitable Yükleme

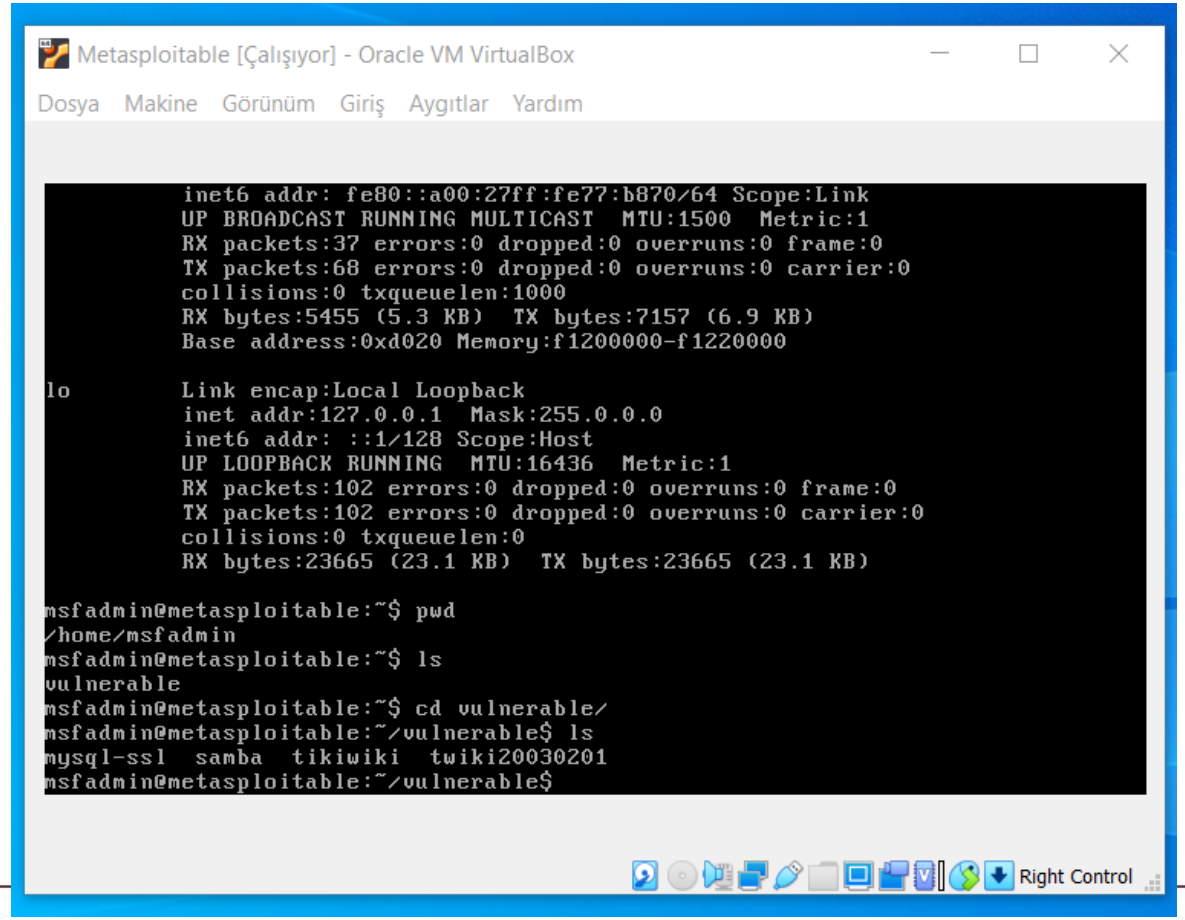


Metasploitable Yükleme

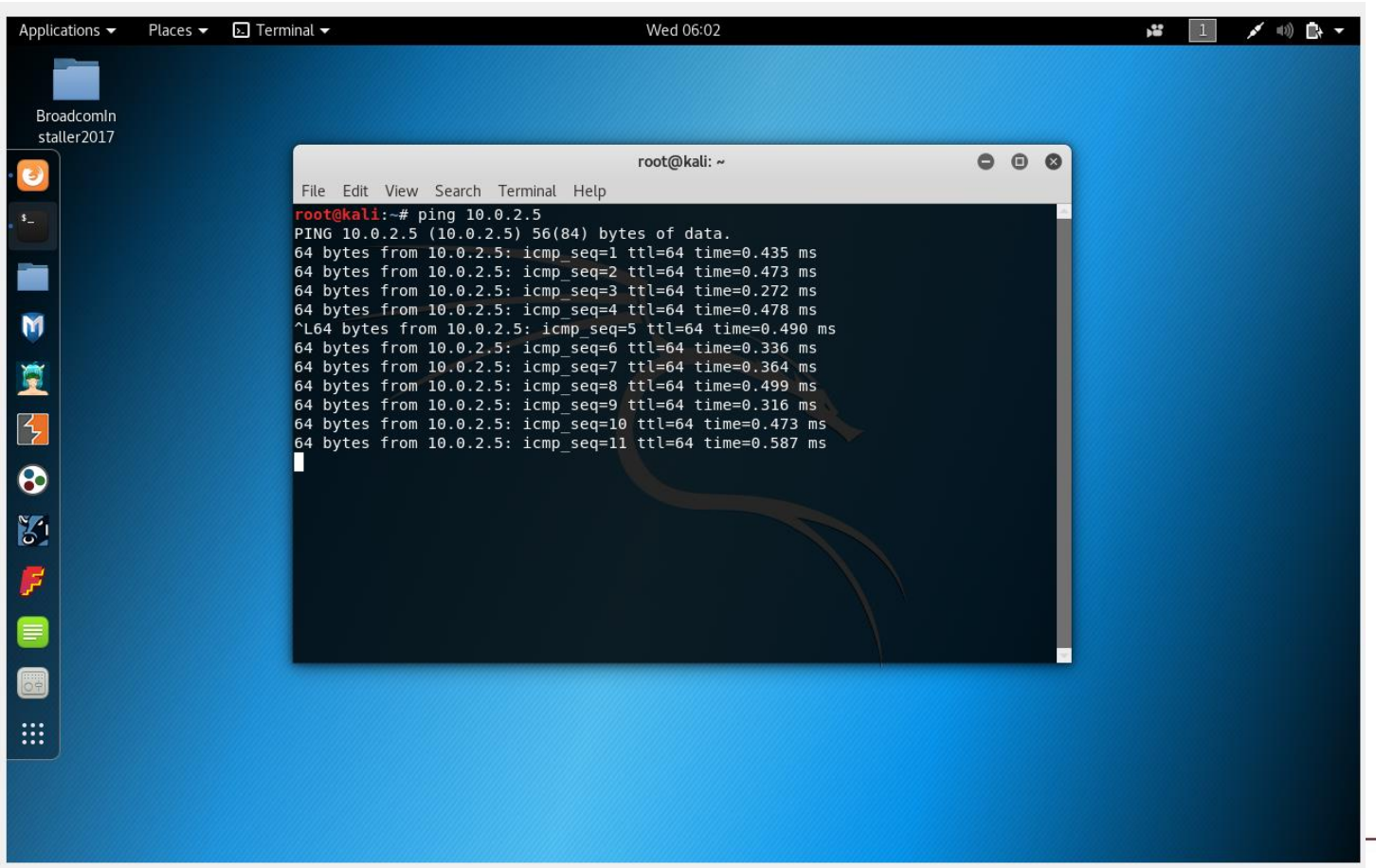


BEYKOZ ÜNİVERSİTESİ

Metasploitable Yükleme



Metasploitable Yükleme



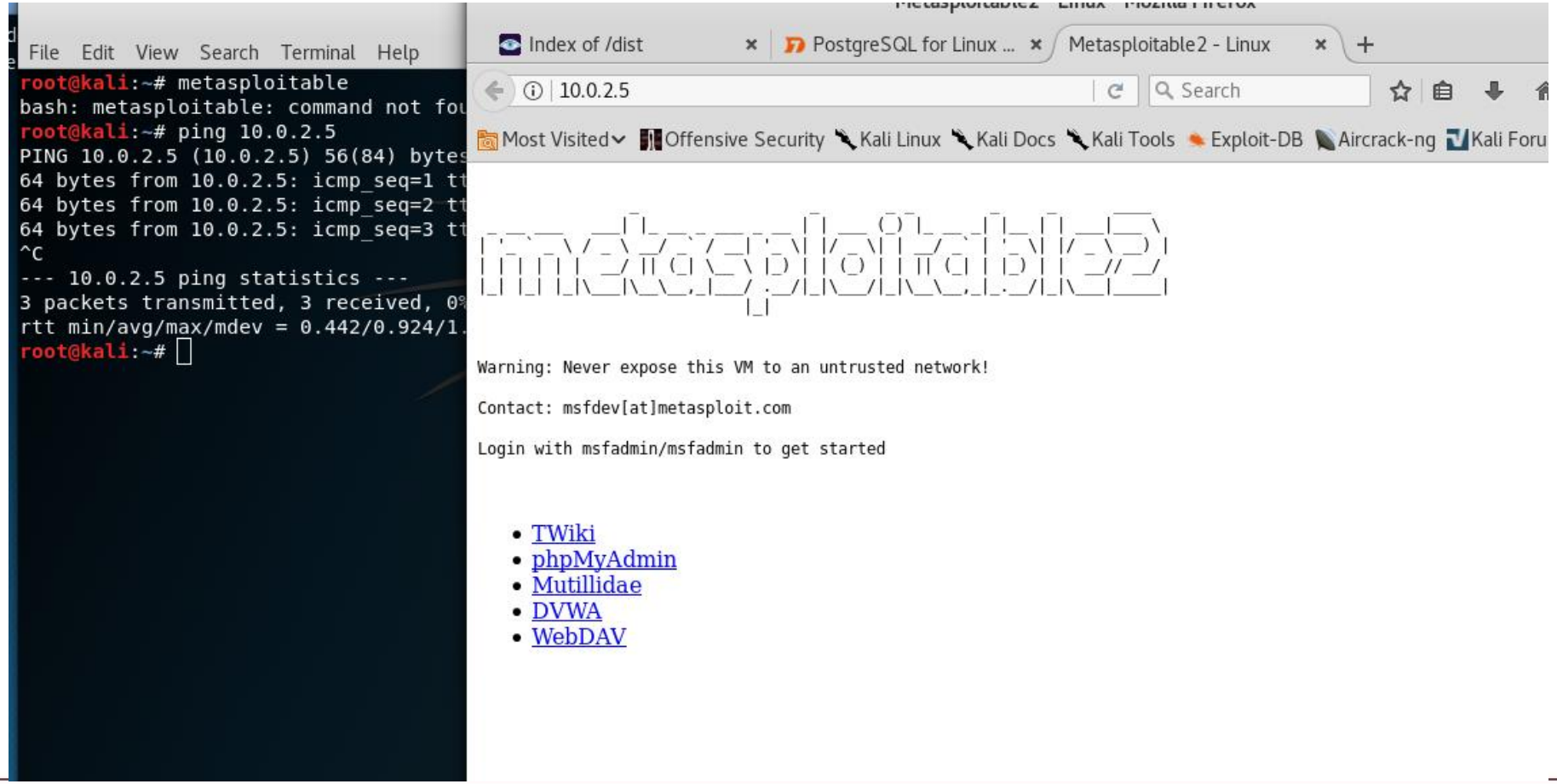
Metasploitable İçeriği (Veritabanları)

```
root@kali:~# mysql -u root -h 10.0.2.5
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)
```

```
MySQL [(none)]> use owasp10;
Reading table information for completio
You can turn off this feature to get a

Database changed
MySQL [owasp10]> show tables;
+-------------------+
| Tables_in_owasp10 |
+-------------------+
| accounts          |
| blogs_table       |
| captured_data     |
| credit_cards      |
| hitlog            |
| pen_test_tools    |
+-------------------+
6 rows in set (0.00 sec)
```

```
MySQL [owasp10]> select * from credit_cards;
+------+------------------+------+------------+
| ccid | ccnumber         | ccv  | expiration |
+------+------------------+------+------------+
|    1 | 4444111122223333 | 745  | 2012-03-01 |
|    2 | 7746536337776330 | 722  | 2015-04-01 |
|    3 | 8242325748474749 | 461  | 2016-03-01 |
|    4 | 7725653200487633 | 230  | 2017-06-01 |
|    5 | 1234567812345678 | 627  | 2018-11-01 |
+------+------------------+------+------------+
5 rows in set (0.01 sec)
```

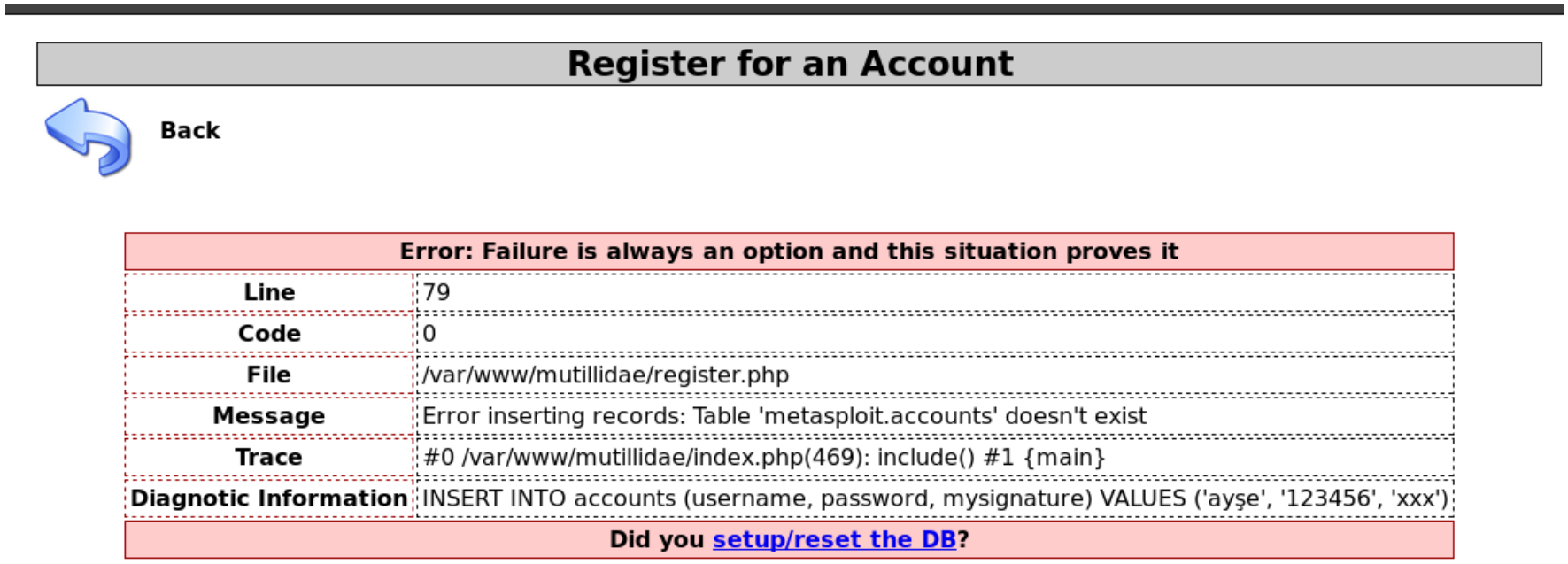
Metasploitable İçeriği (Web Siteleri)



BEYKOZ ÜNİVERSİTESİ

Mutillidae Veritabanında Düzeltme

Mutillidae Veritabanında Düzeltme



Register for an Account

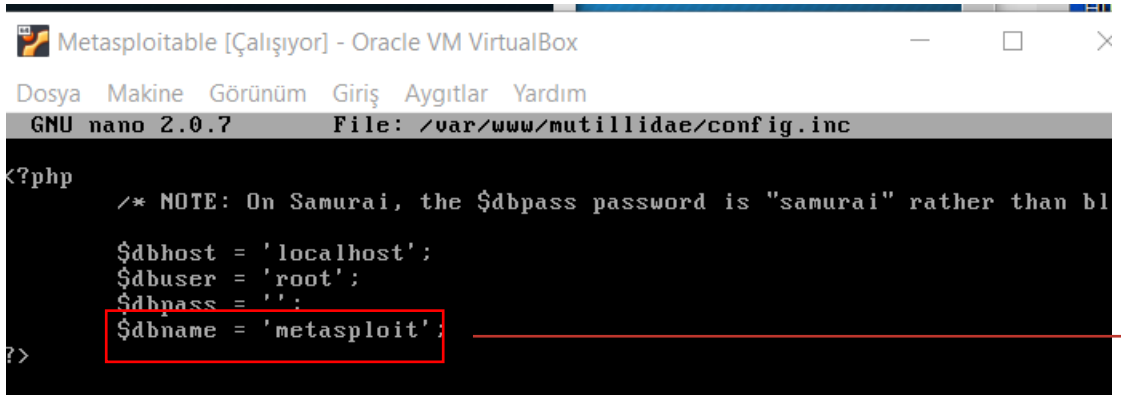
Back

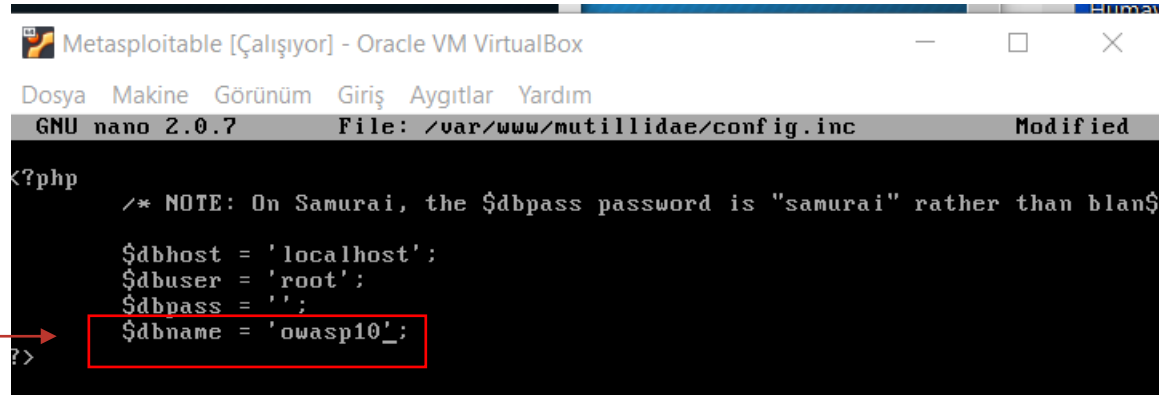
Error: Failure is always an option and this situation proves it	
Line	79
Code	0
File	/var/www/mutillidae/register.php
Message	Error inserting records: Table 'metasploit.accounts' doesn't exist
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	INSERT INTO accounts (username, password, mysignature) VALUES ('ayşe', '123456', 'xxx')
Did you setup/reset the DB?	

BEYKOZ ÜNİVERSİTESİ

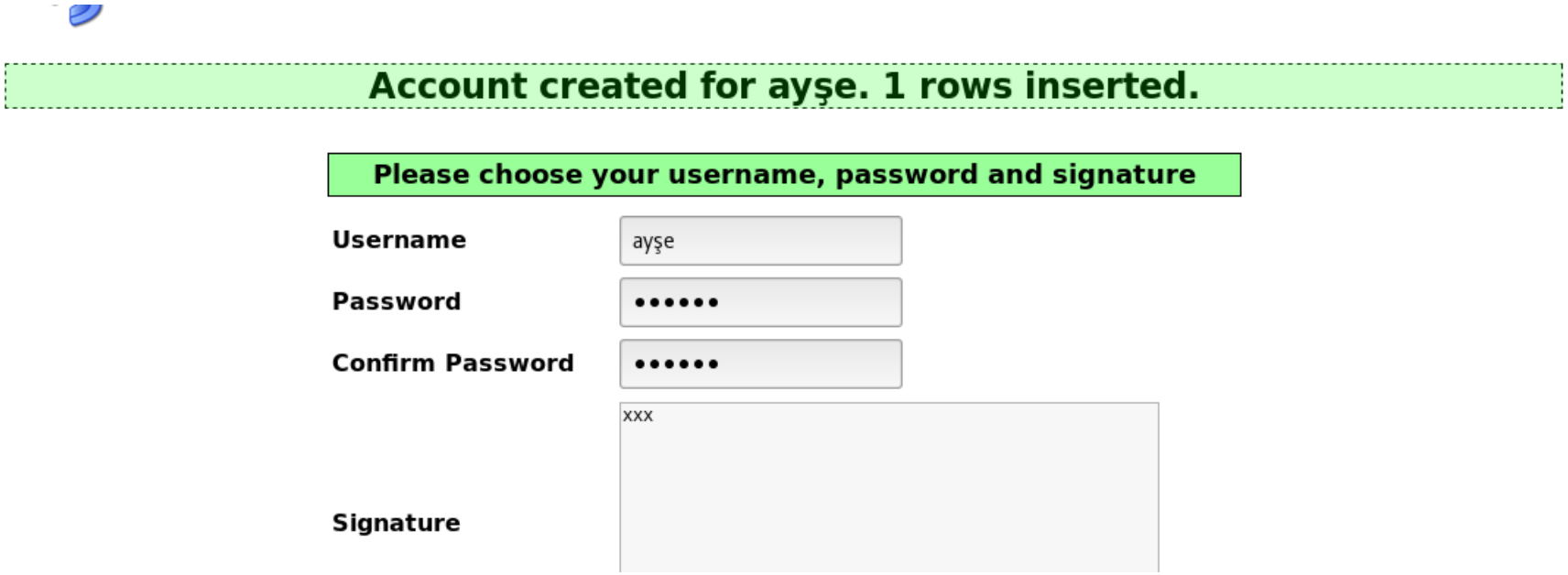
Metasploitable da Düzeltme

```
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc
[sudo] password for msfadmin:
```





Mutillidae Kullanıcı Kaydı



Mutillidae Yanlış Parola Girilmesi

Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '''' at line 1
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='ayşe ' AND password='''
Did you setup/reset the DB?	

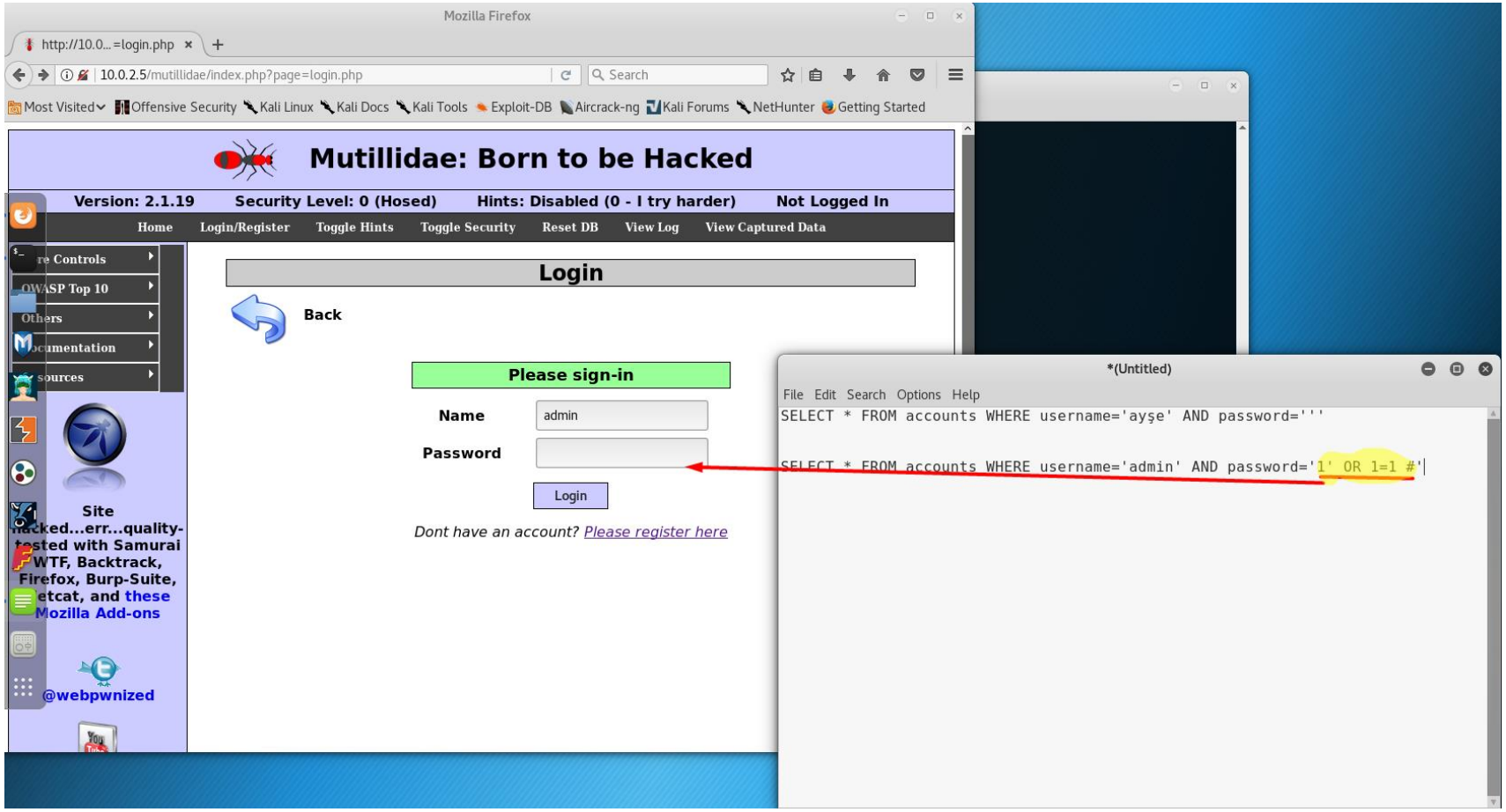
Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **148**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **254**

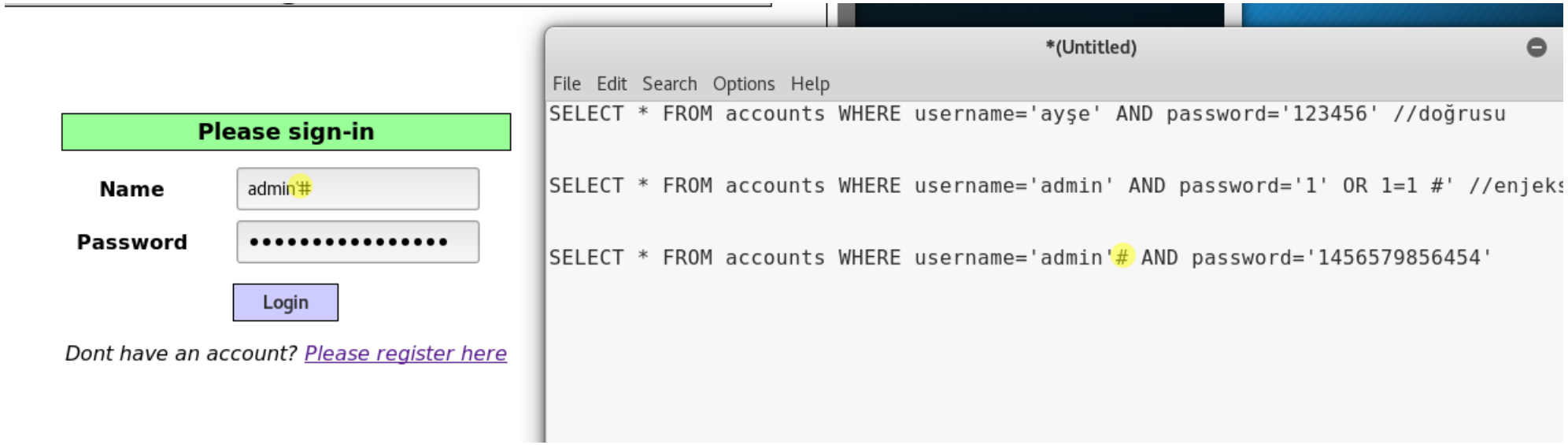
Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **255**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **256**

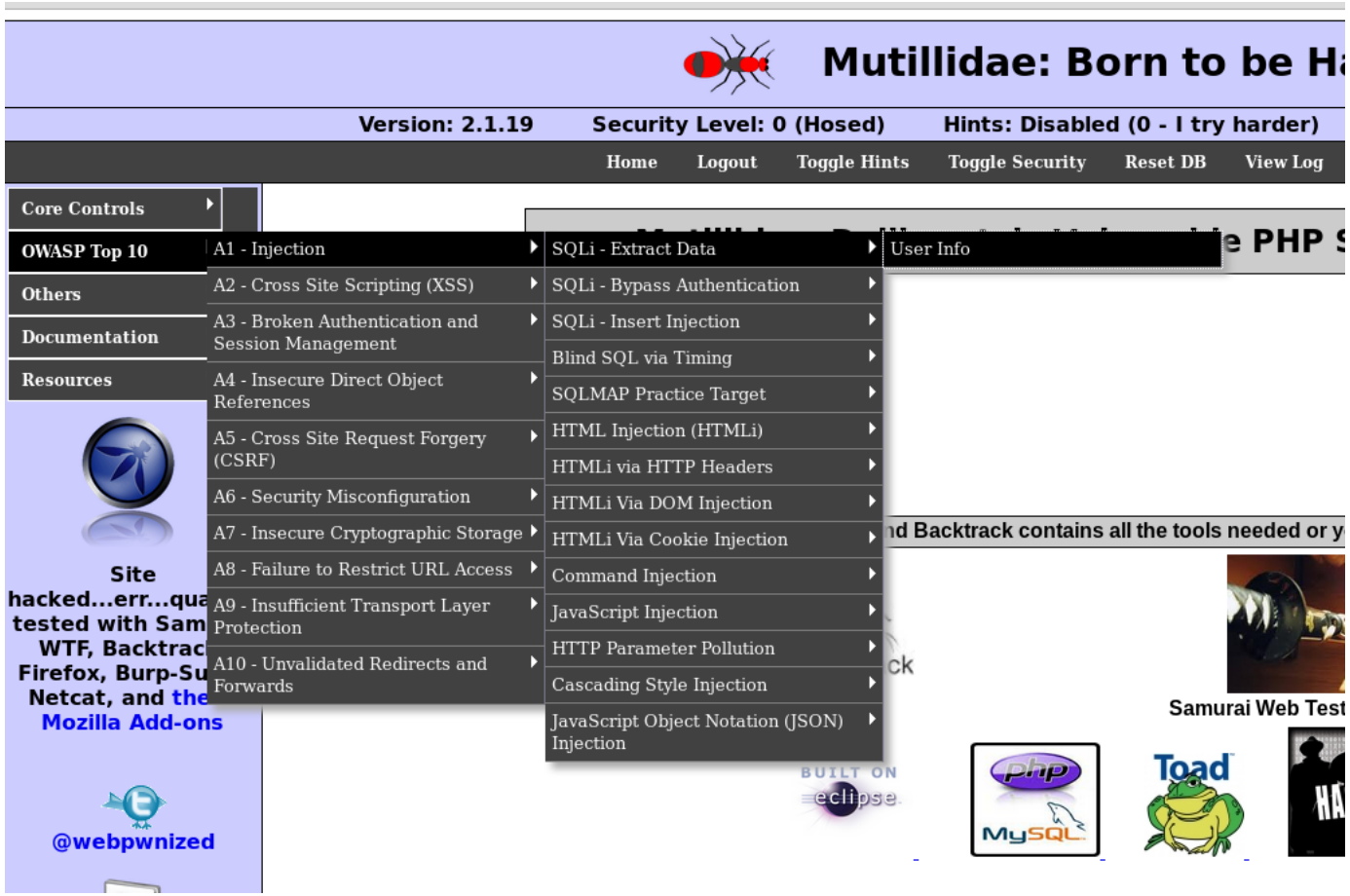
SQL Enjeksiyon Post Metodu



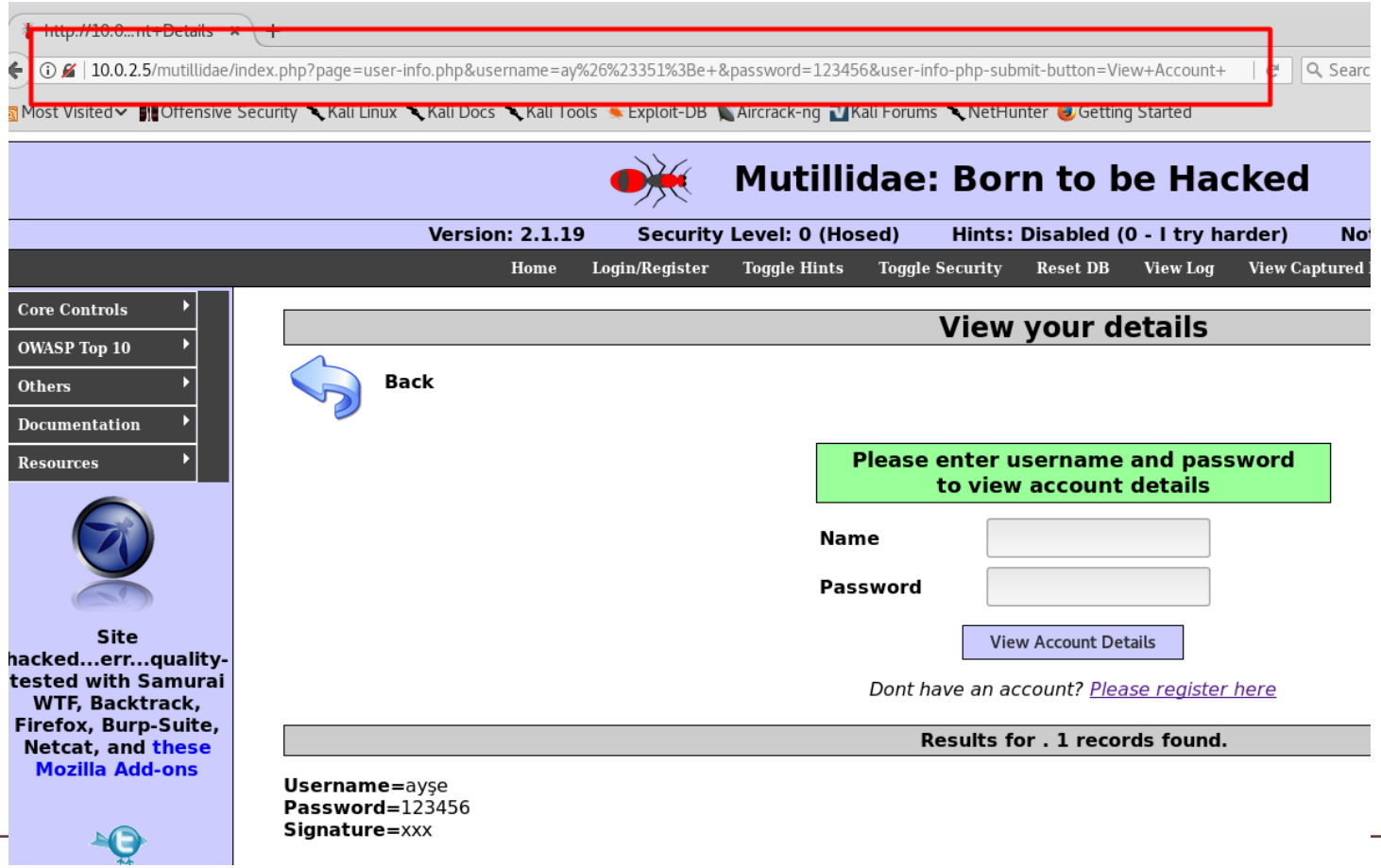
SQL Enjeksiyon Post Metodu



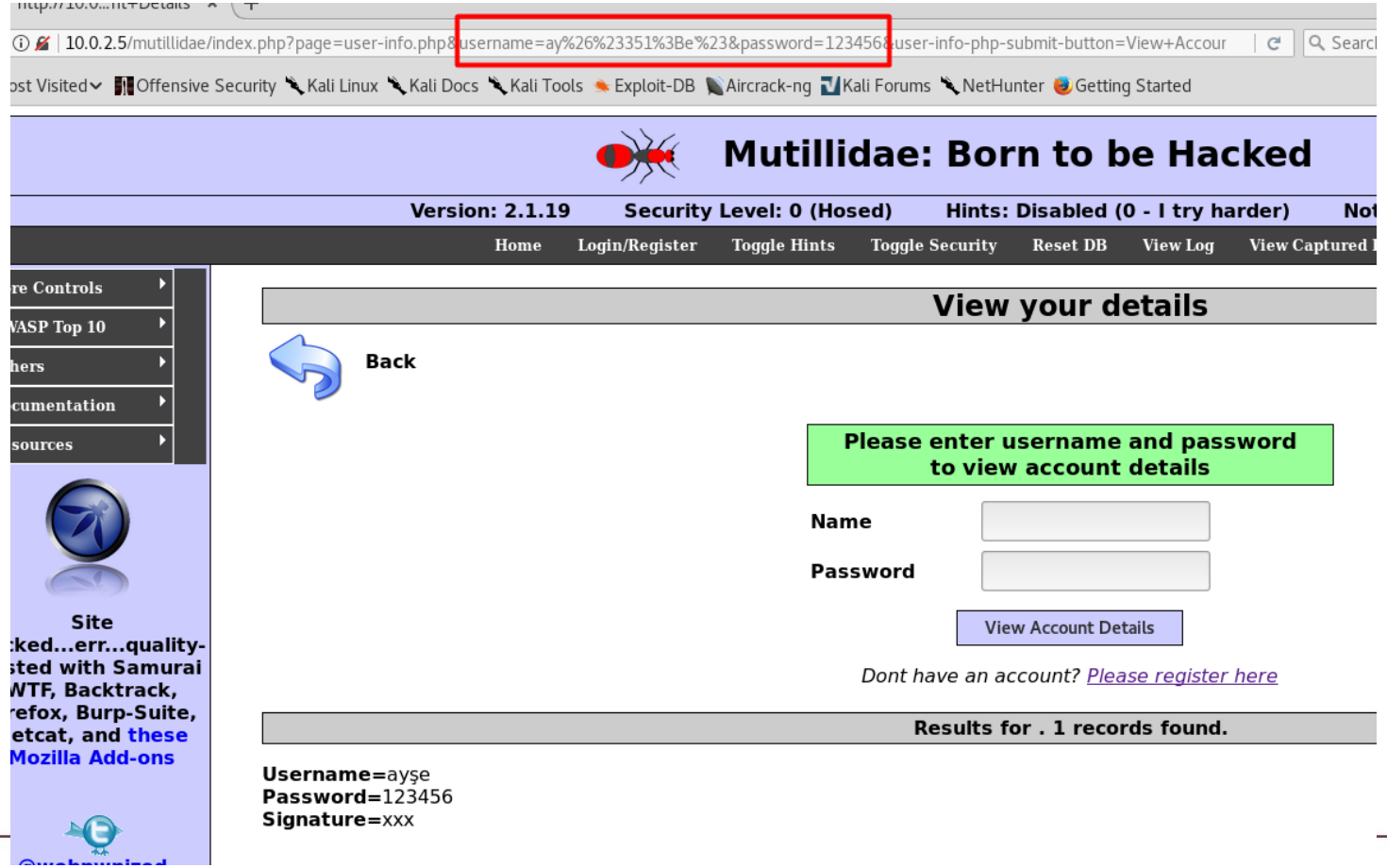
SQL Enjeksiyon Get Metodu



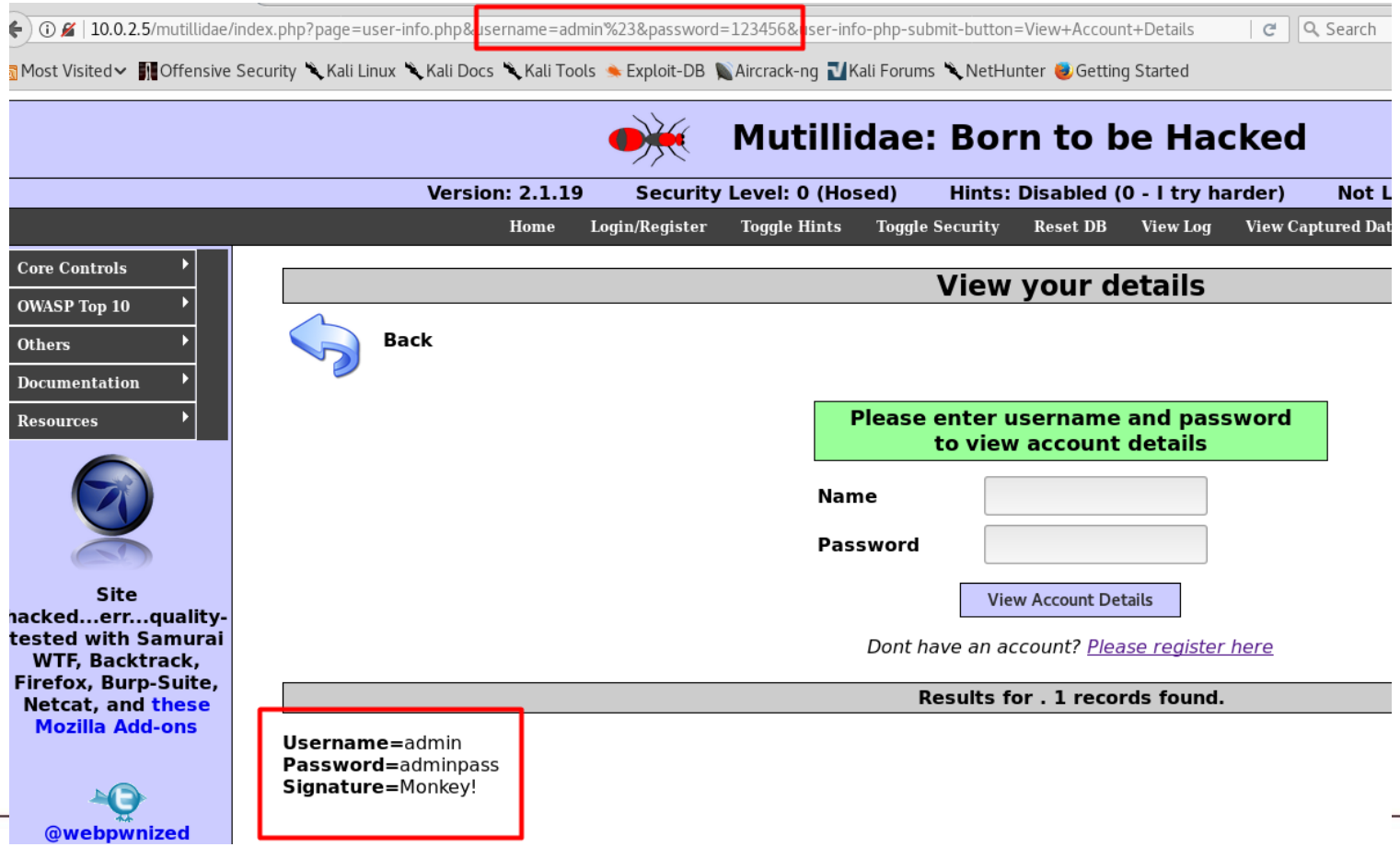
SQL Enjeksiyon Get Metodu



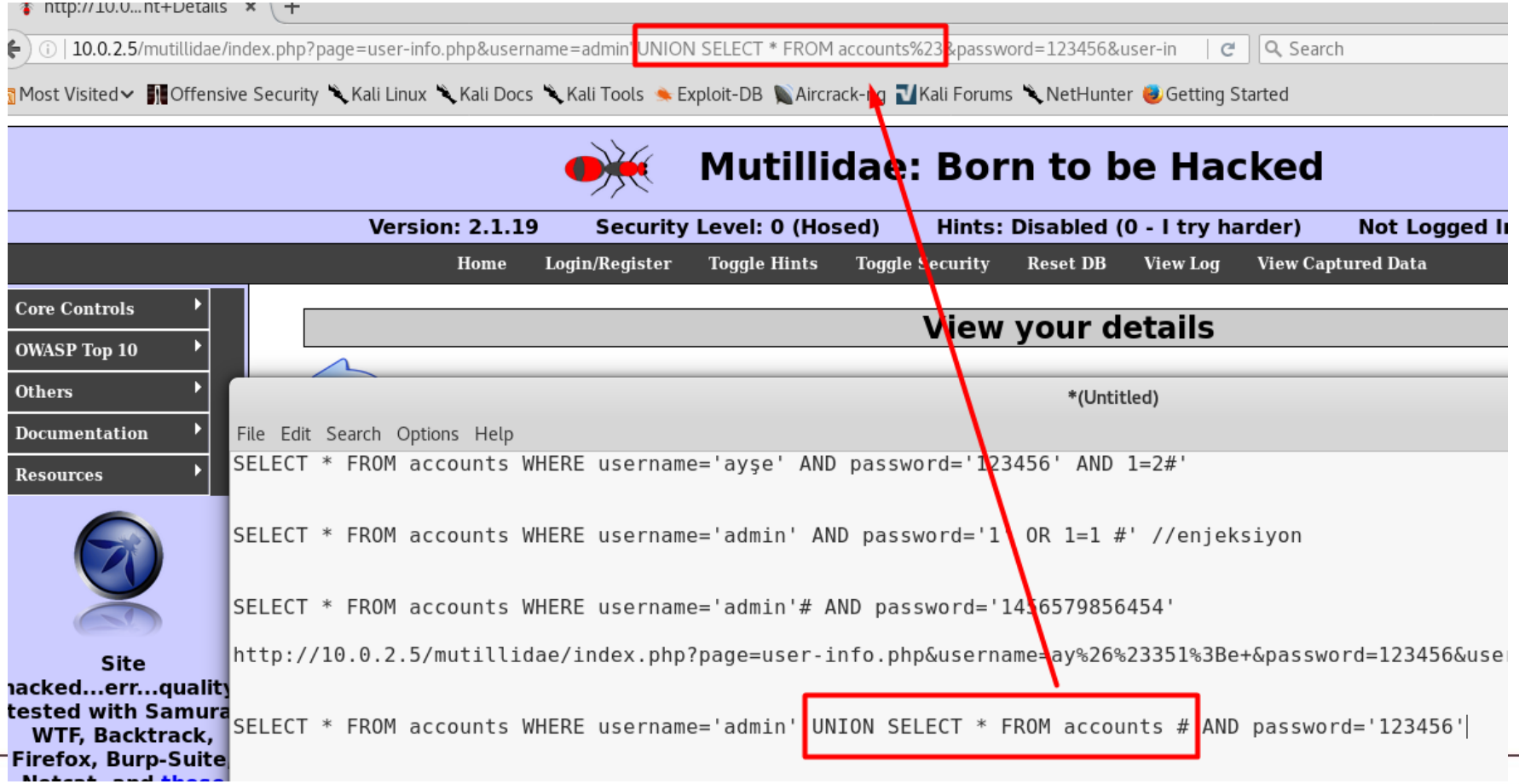
SQL Enjeksiyon Get Metodu



SQL Enjeksiyon Get Metodu



Veritabanındaki Tüm Verileri Çalmak



Veritabanındaki Tüm Verileri Çalmak

Username=admin
Password=adminpass
Signature=Monkey!

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving Fools

Username=jim
Password=password
Signature=Jim Rome is Burning

Username=bobby
Password=password
Signature=Hank is my dad

Username=simba
Password=password
Signature=I am a cat

Username=dreveil
Password=password
Signature=Preparation H

Signature=Go Wildcats

Username=john
Password=password
Signature=Do the Duggie!

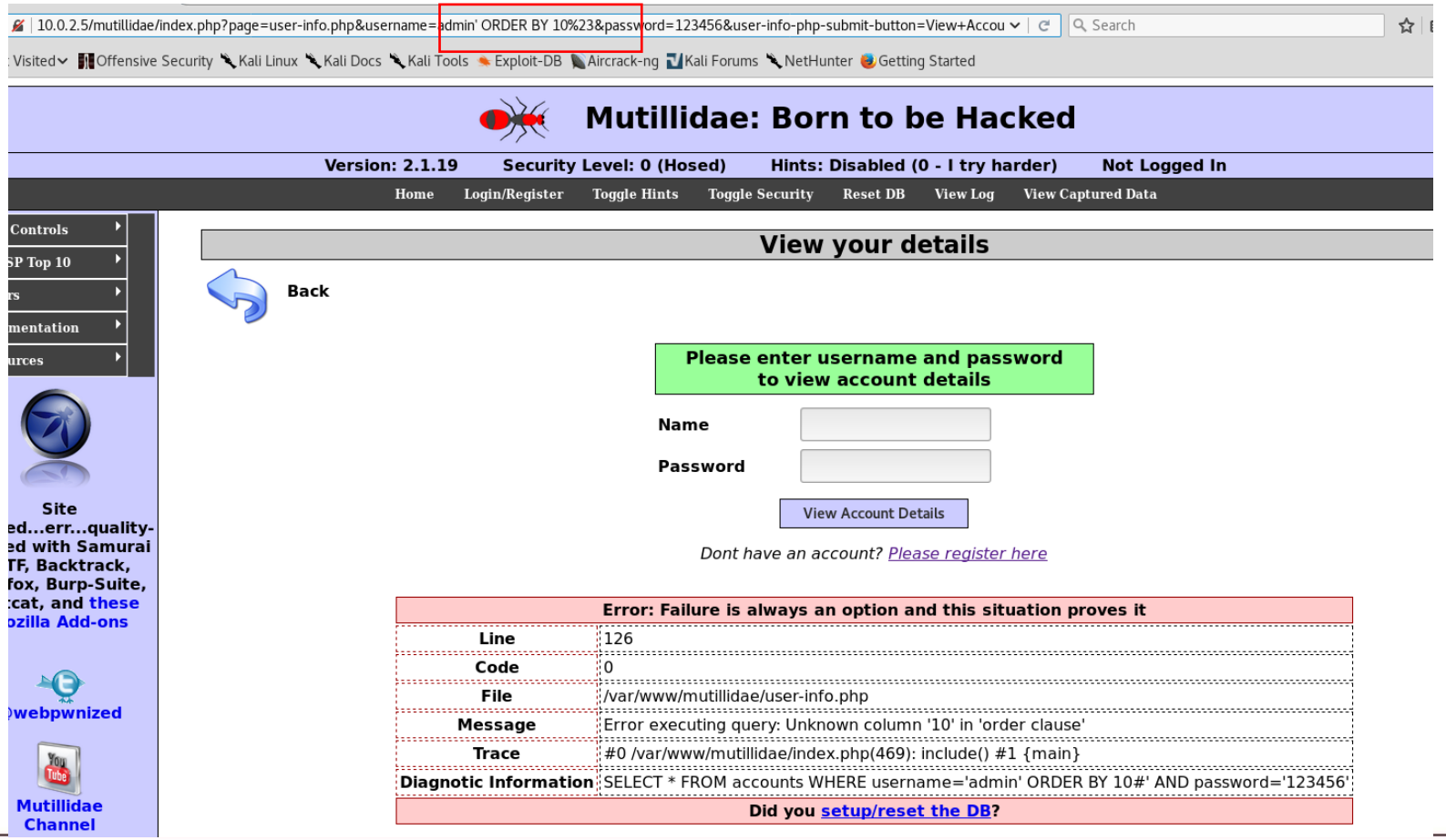
Username=kevin
Password=42
Signature=Doug Adams rocks

Username=dave
Password=set
Signature=Bet on S.E.T. FTW

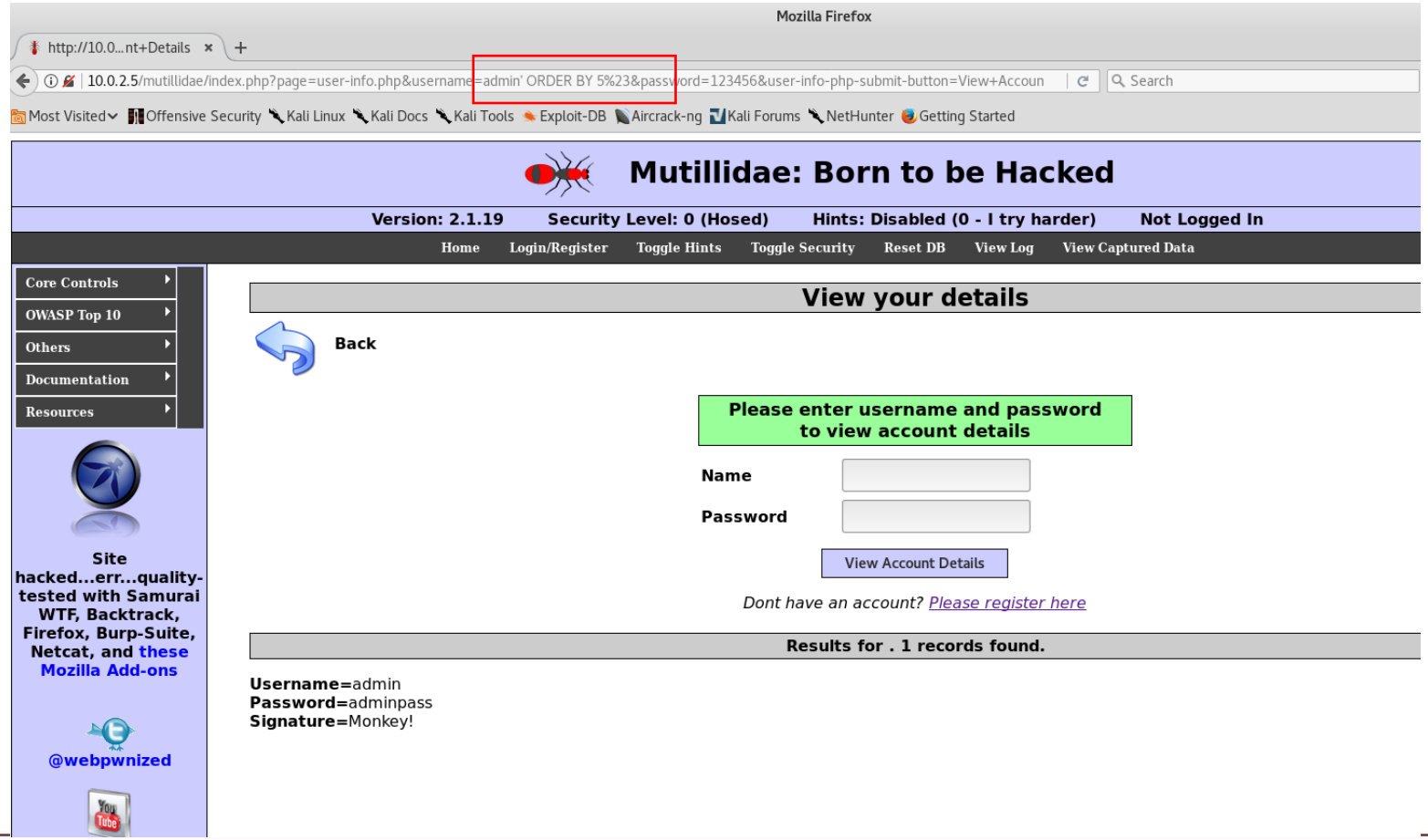
Username=ed
Password=pentest
Signature=Commandline KungFu anyone?

Username=ayşe
Password=123456
Signature=xxx

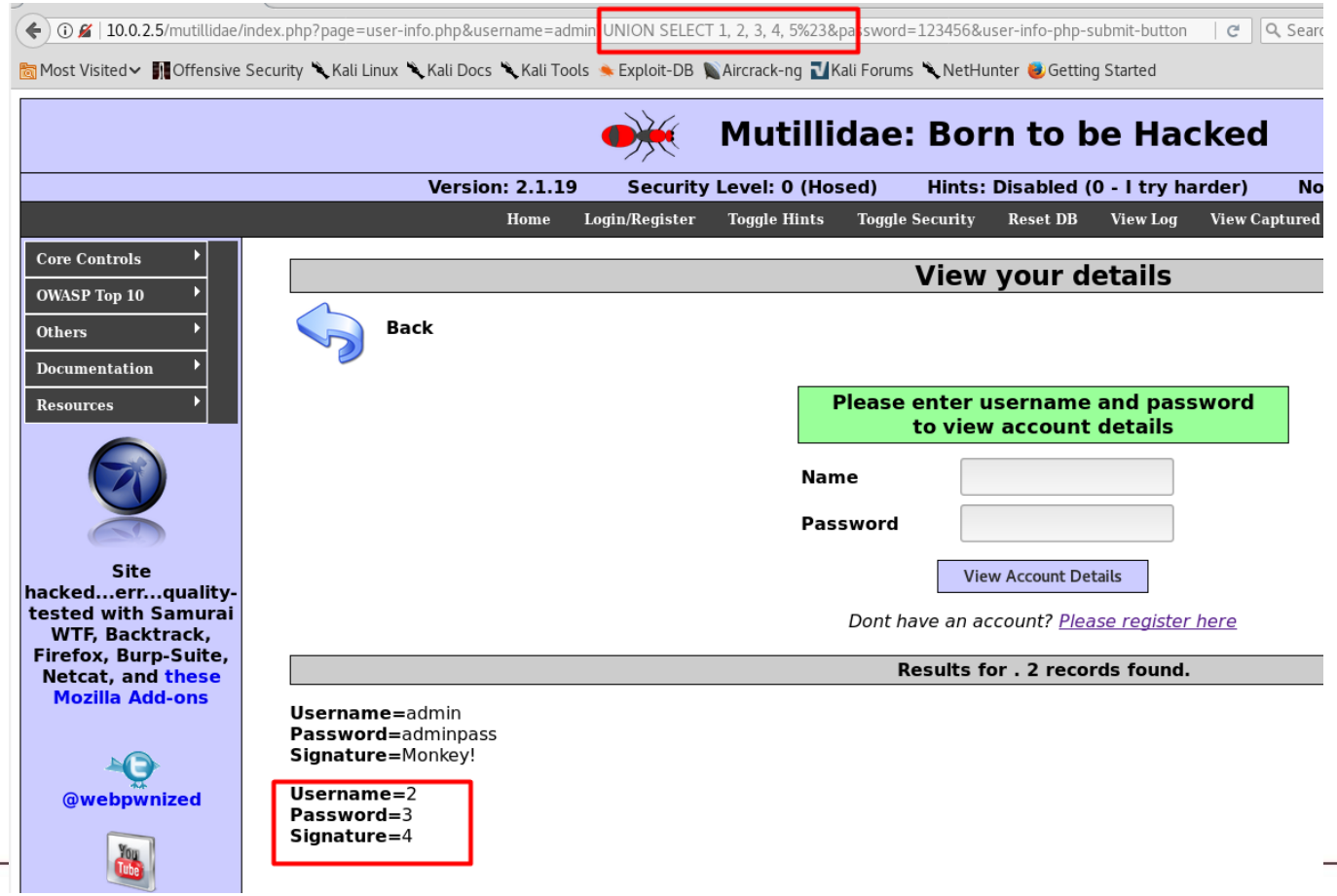
Manuel olarak Veritabanının İsmini Öğrenmek



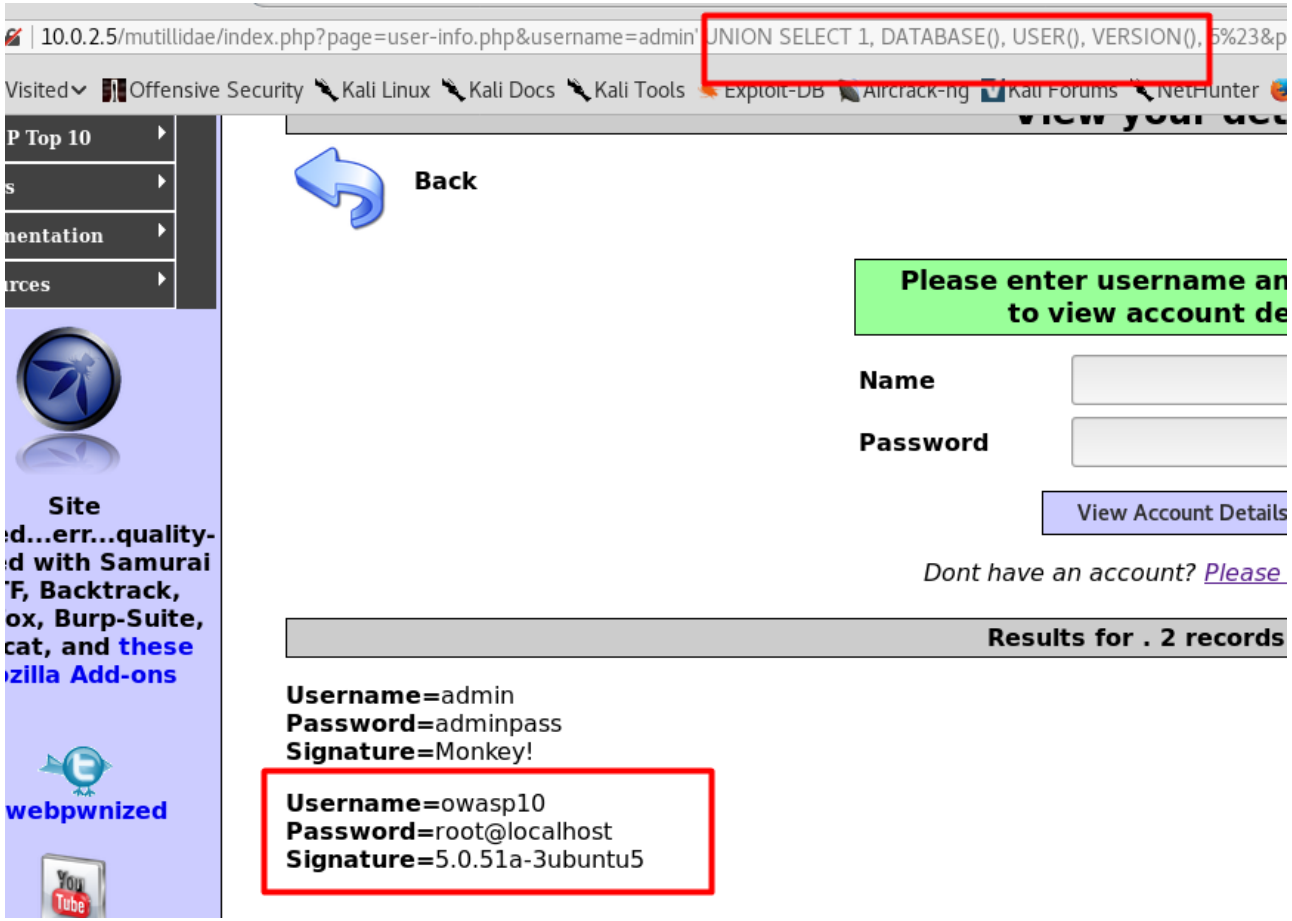
Manuel olarak Veritabanının İsmini Öğrenmek



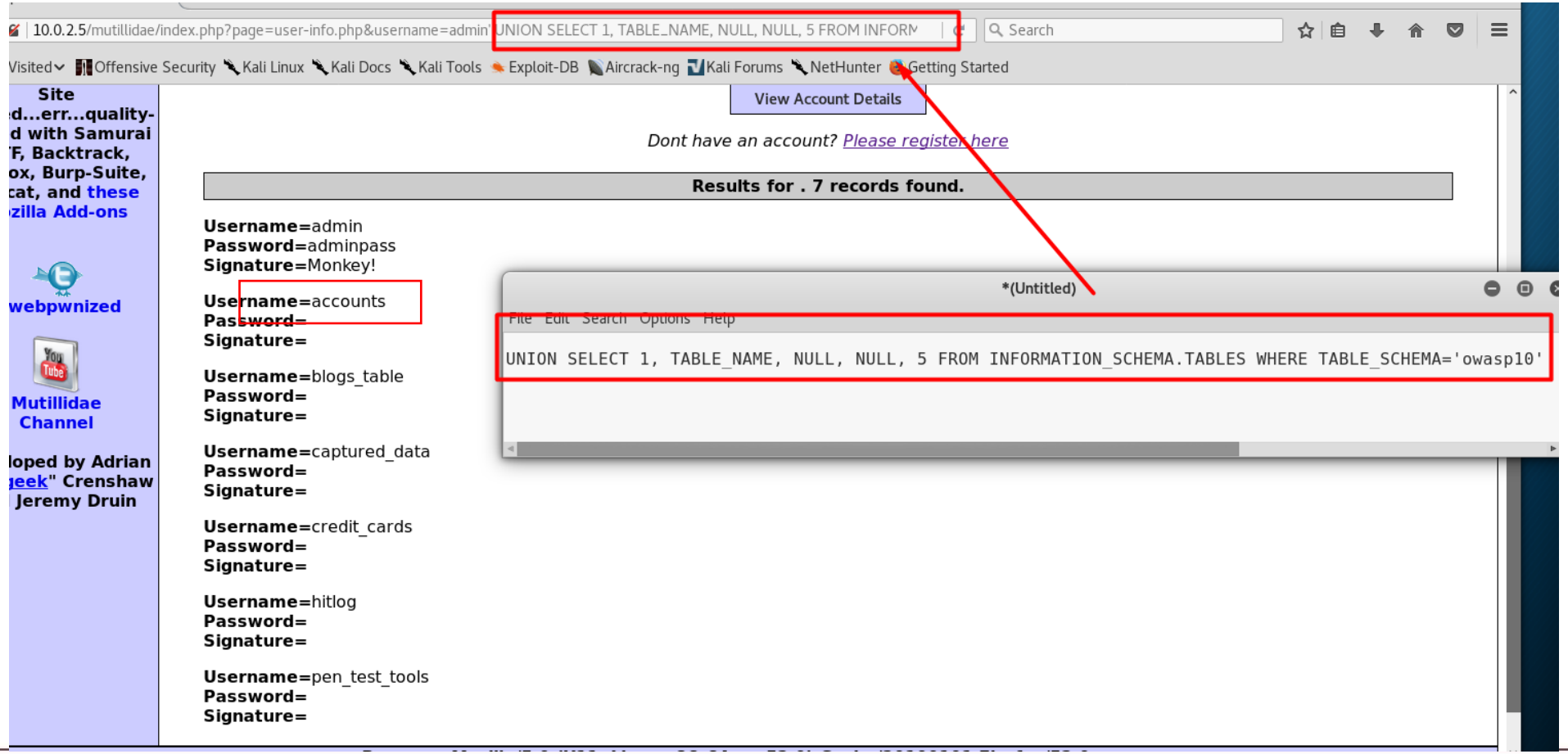
Manuel olarak Veritabanının İsmini Öğrenmek



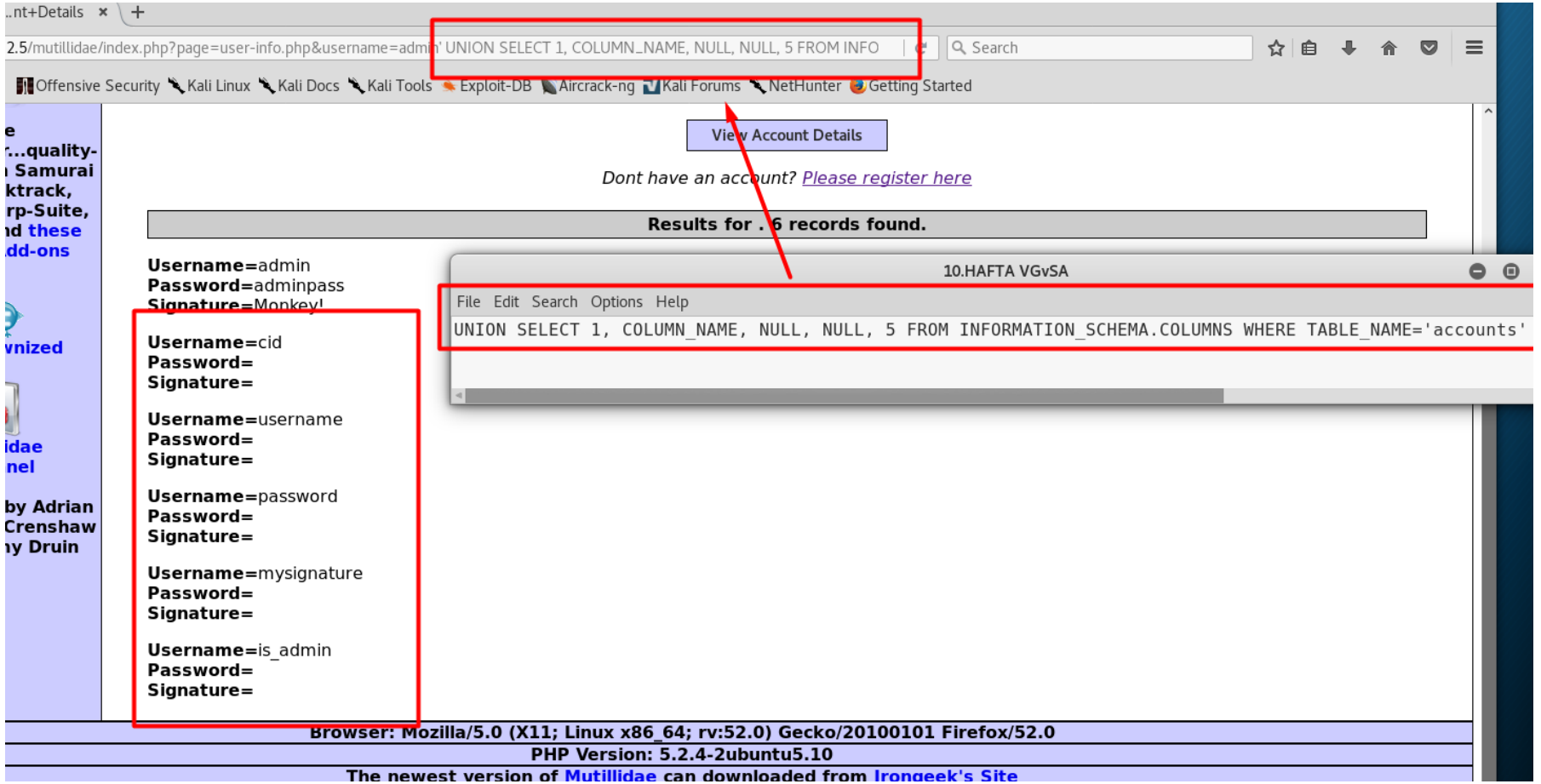
Manuel olarak Veritabanının İsmini Öğrenmek



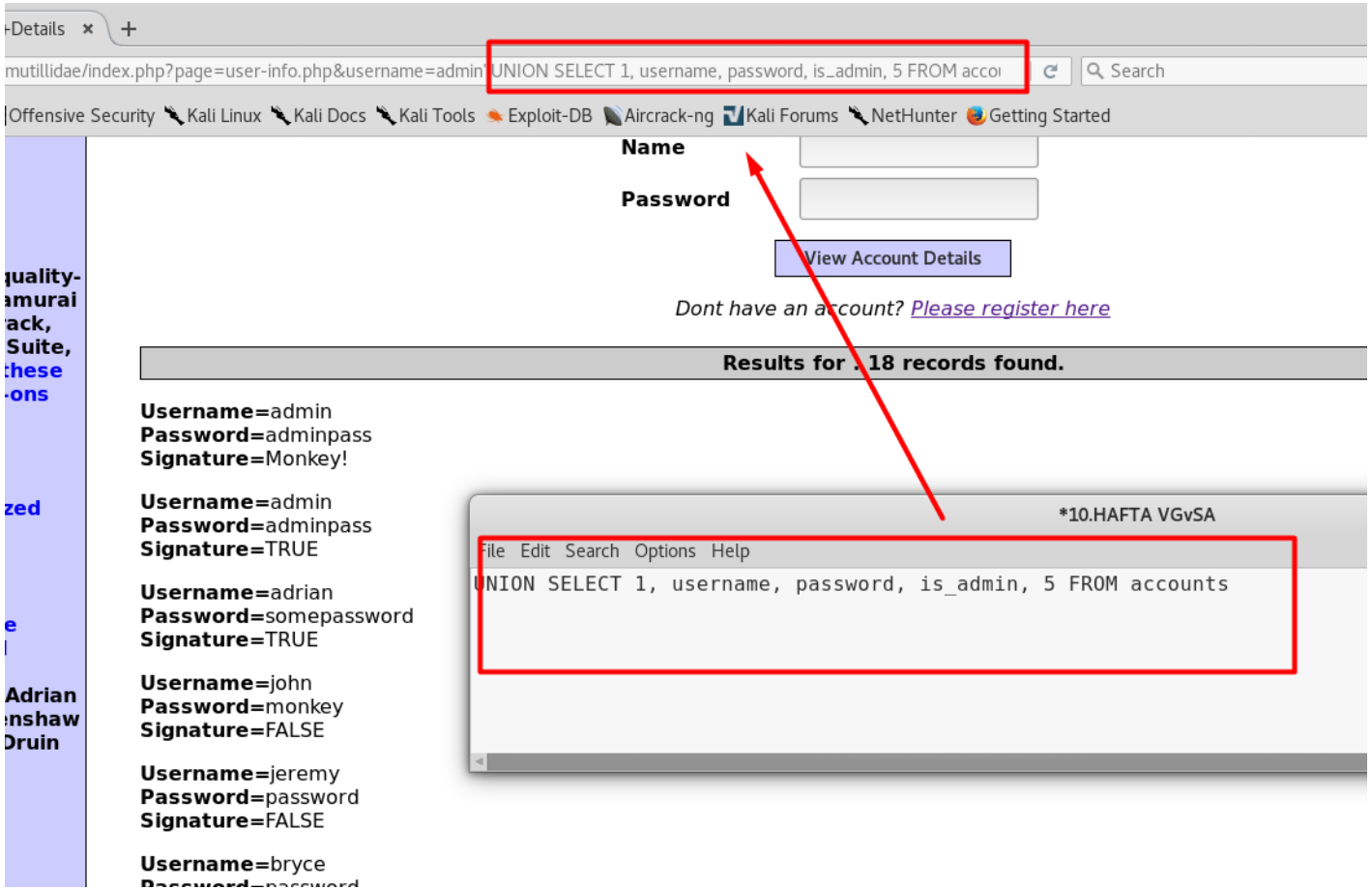
Manuel olarak Veritabanındaki Tabloları Öğrenmek



Manuel olarak Veritabanındaki Sütunları Öğrenmek



Manuel olarak Veritabanındaki Tüm Verileri Çalmak



Manuel olarak Veritabanındaki Tüm Verileri Çalmak

Username=admin
Password=adminpass
Signature=Monkey!

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving Fools

Username=jim
Password=password
Signature=Jim Rome is Burning

Username=bobby
Password=password
Signature=Hank is my dad

Username=simba
Password=password
Signature=I am a cat

Username=dreveil
Password=password
Signature=Preparation H

Signature=Go Wildcats

Username=john
Password=password
Signature=Do the Duggie!

Username=kevin
Password=42
Signature=Doug Adams rocks

Username=dave
Password=set
Signature=Bet on S.E.T. FTW

Username=ed
Password=pentest
Signature=Commandline KungFu anyone?

Username=ayşe
Password=123456
Signature=xxx