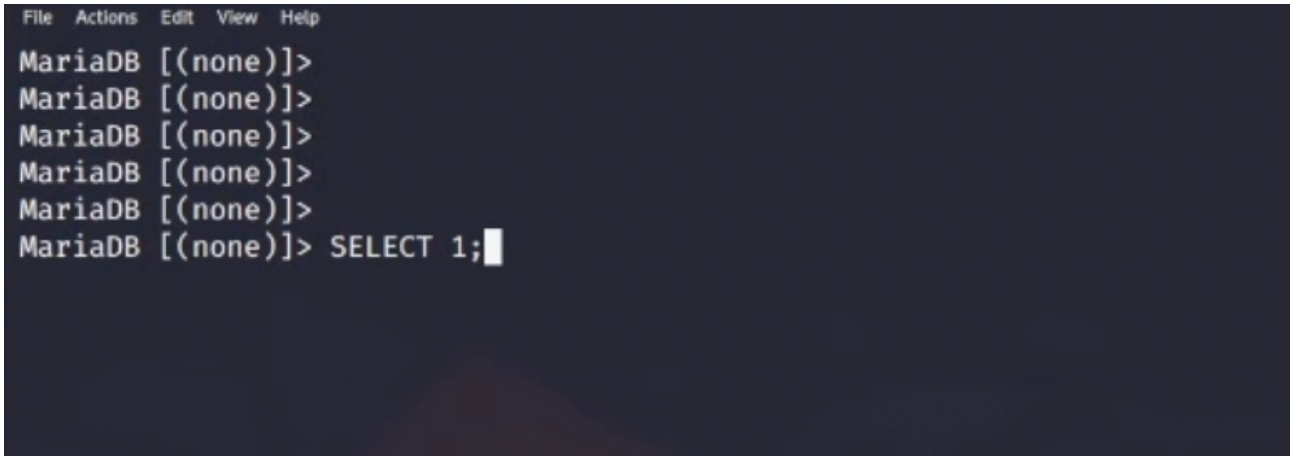
WEB SECURITY (WAS TEACHED BY MDI 🖤)

Web Security 101 0x01 | SQL Injection:

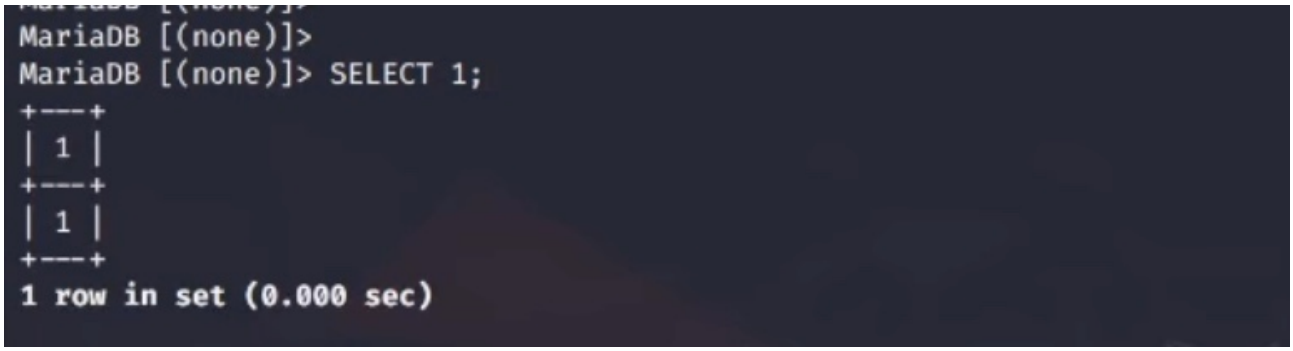
SQL Injection: Saldırganların yazılan web yazılımlarını kullanarak o web yazılımının veri tabanında kendi SQL sorgularını kullanabilme durumudur.

NOT: Kali'de veri tabanı konsoluna geçmek için super user olduktan sonra "**mysql -u root -h <IP> —skip-ssl**" komutu kullanılır.

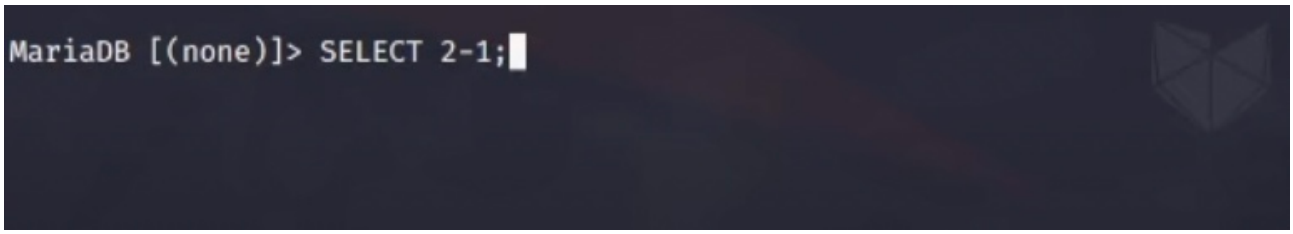
SORU-I: Veri tabanı seçilmeden atılmış olan aşağıdaki sorgunun çıktısı nedir?



CEVAP-I: Veri tabanı seçmeden ve '*FROM*' kullanmadan "*SELECT 1;*" dersek sonuç "**1**" çıkar. Üstteki 1 "*kolon adı*", alttaki ise "*verisi*"dir. Kolon kısmı değişkenlik gösterebileceği için cevap olarak alt kısımdaki veriyi söylemeliyiz.



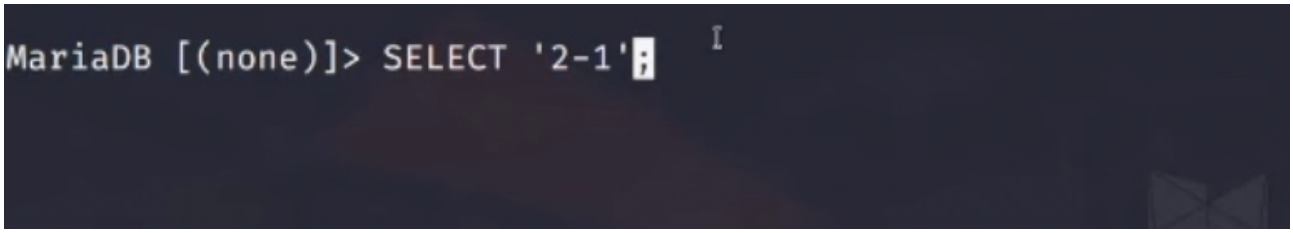
SORU-II: Veri tabanı seçilmeden atılmış olan aşağıdaki sorgunun çıktısı nedir?



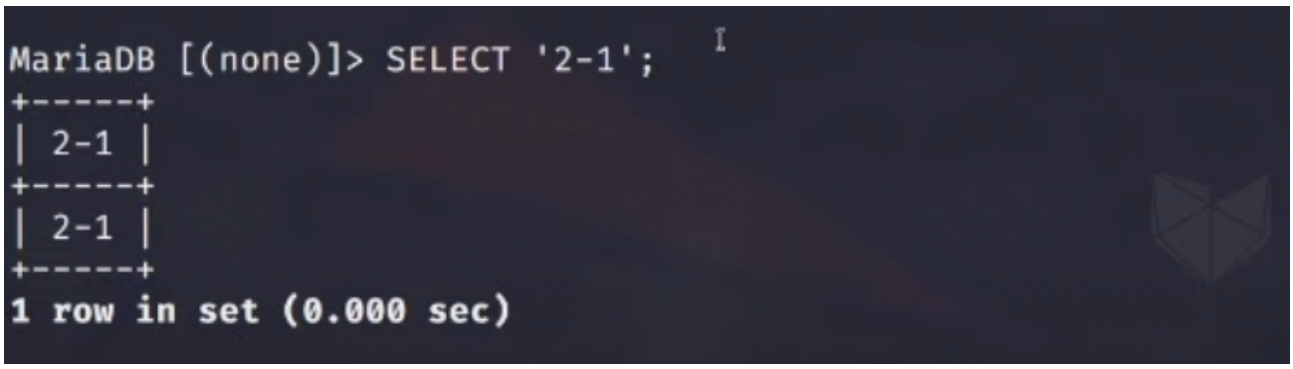
CEVAP-II: Cevap yine **1**'dir.

ANLAMAMIZ GEREKEN ŞEY: Veri tabanı, verilen toplama-çıkarma işlemini gerçekleştirebilir.

SORU-III: Veri tabanı seçilmeden atılmış olan aşağıdaki sorgunun çıktısı nedir?



CEVAP-III: Bu bir string işlemi olduğu için çıkarma işlemi yapmak yerine olduğu gibi çıktı verir.



SORU-IV: Veri tabanı seçilmeden atılmış olan aşağıdaki sorgunun çıktısı nedir?

```
MariaDB [(none)]> SELECT '2'-'1';
```

CEVAP-IV: Sonuç "**1**" çıkar. Veri tabanı burada string bir ifadeden string bir ifadeyi çıkarıp integer'a atayabildiği için sonucu 1 döndürür.

```
MariaDB [(none)]> SELECT '2'-'1';
+----------+
| '2'-'1' |
+----------+
|        1 |
+----------+
1 row in set (0.000 sec)
```

SORU-V: Veri tabanı seçilmeden atılmış olan aşağıdaki sorgunun çıktısı nedir?

```
MariaDB [(none)]> SELECT '2'+'a';
```

CEVAP-V: Sonuç "**2**" çıkar. Veri tabanı burada ilk stringi integer bir değere *cast* edebilir ancak ikinci ifadeyi edemez ve 0 gibi sayar. Dolayısıyla buna göre toplama işlemi yapar.

```
MariaDB [(none)]> SELECT '2'+'a';
+----------+
| '2'+'a' |
+----------+
|        2 |
+----------+
1 row in set, 1 warning (0.000 sec)
```

SORU-VI: Veri tabanı seçilmeden atılmış olan aşağıdaki sorgunun çıktısı nedir?

```
MariaDB [(none)]> SELECT 'b'+'a';
```

CEVAP-VI: Sonuç "**2**" çıkar. Çünkü her iki stringi de bir integer değere cast edemez.

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

SORU-VII: Veri tabanı seçilmeden atılmış olan aşağıdaki sorgunun çıktısı nedir?

```
MariaDB [(none)]> SELECT '2' '1';
```

CEVAP-VI: Sonuç "**21**" çıkar. Çünkü veri tabanı burada iki string arasındaki boşluğu '*string concatenation*' yaparak iki string ifadeyi birleştirir ve buna göre bir sonuç döndürür.

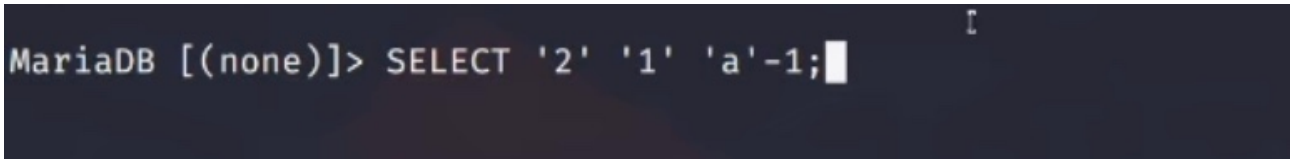
```
MariaDB [(none)]> SELECT '2' '1';
+----+
| 2  |
+----+
| 21 |
+----+
1 row in set (0.000 sec)
```

NOT: *String concatenation* yapmanın bir diğer yolu "***SELECT concat('string1','string2');***"dir. Aslında buradaki '*SELECT*' ifadesi diğer dillerdeki '*print*' ve türevleriyle benzer işlevdedir.

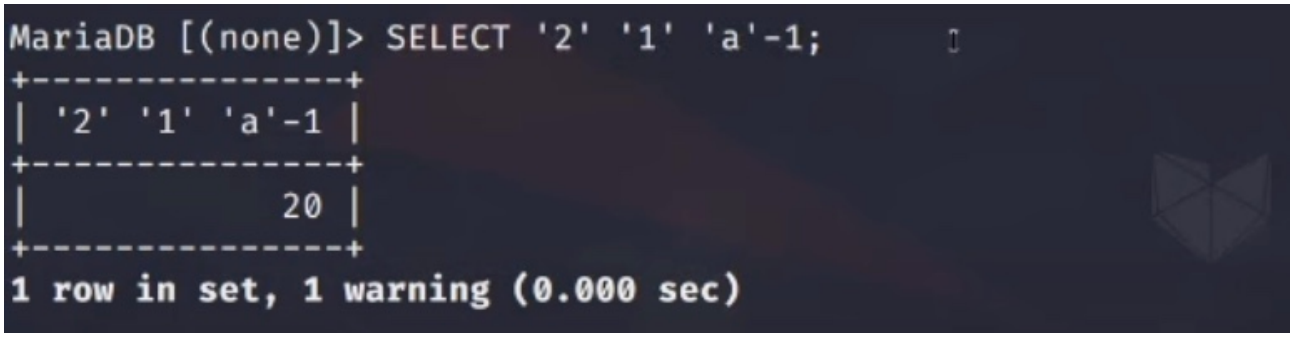
SORU-IX: "SELECT '2' '1' 'a';" girdisi ne sonuç döndürür?

CEVAP-IX: Sonuç "**21a**" olarak çıkar.

SORU-X: Veri tabanı seçilmeden atılmış olan aşağıdaki sorgunun çıktısı nedir?



CEVAP-X: Sonuç "**20**" olarak çıkar. Veri tabanı önce soldaki "***'a'-1***" kısmını hesaplayıp "*-1*" bulacaktır. Daha sonra soldaki stringleri concatena edip '*21*'i elde edecektir. En son işlem olarak ise 21 ve -1'i işleme sokup matematiksel işlem yapacak ve sonucu "**20**" olarak döndürecektir.



NOT: MySQL'de "^" işareti XOR operandıdır.