

SQL INJECTION

SQL Injection Nedir; kullanıcı girdilerinin SQL sorgularına dahil edilmesiyle oluşan ve saldırının veritabanına zararlı sorgular göndermesine olanak tanıyan bir güvenlik açığıdır.

Nasıl Önlenir; SQL ifadeleri ve sorgu parametrelerini kullanarak kullanıcı girdilerini güvenli hale getirip filtrelememiz lazım.

2.1 SQL Login Bypass ;

ÇÖZÜM

Login

Username

Password

Karşımıza gelen **SQL** zafiyetli web sayfamız burası ancak kullanıcı girişi verilmemiş galiba giriş olmamızı istiyor. Ve eğer kullanıcı vermediyse bu **SQL** zafiyeti genelde **Login Bypass** adı ile geçer , anlaşılmadı için öncelikle arkada dönen sorguya bakalım.

SORGU:

SELECT * FROM users WHERE username = 'kullanici_adi' AND password = 'sifre';

SQL Injection konusunda bazı **SQL** komutlarını bilmemiz gerekiyor.

Öncelikle sorguyu yorumlayalım.

Select komutu veriyi çeker , yıldız ile kullanıldığında Linux'da ki mantık ile tüm veriyi seçmeye yarar. **From** komutu ise veriyi nereden getireceğini belirtir. Biz burada users veritabanından verileri çekiyoruz.

Ve bu veritabanında değişkenler fonksiyonlar var mesela username gibi ve password gibi bunlar veritabanında tutulur.

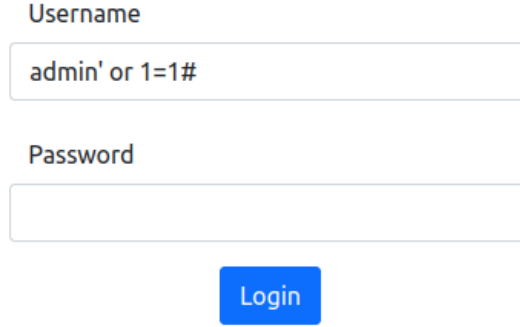
Biz atıyorum **test:test** adıyla giriş yapmaya çalıştığımızda 1. değişken çalışır yani **username=**, test kullanıcısı users veritabanında olup olmadığını kontrol eder burada **SELECT *** ile verileri getirip yazılım kontrol ediyor.

Daha sonra test adında bir kullanıcı varsa veritabanından bulup eşleştiriyor.

Eğer kullanıcı yoksa direkt hata verir giriş başarısız olur. Eğer **true** değeri dönerse yani test kullanıcısı eğer veritabanında varsa sorun yok demektir.

Bu sefer 2. değişkene gidicek bu sefer verdiğimiz parolanın test kullanıcısına ait olmadığını sorguluyacak böyle bir parola varmı diyerek, burada tabi users veritabanından verileri çekerek yapıcak. Uyuşmazsa giriş başarısız olucak.

Bunun da sebebine gelelim **username** değişkeni ve parola değişkeni arasında bir **SQL** komutumuz var bu “**AND**” bu İngilizcede olduğu gibi karşılığı **VE** demek. Burada ki mantığı kullanıcı adı **VE** parola doğruysa giriş yap. Demek istiyor, ancak biz bunu **OR** ile değiştirecez, ve bu anlamı **VEYA** ile değiştirecez, yani **OR=VEYA** demek. Bunun işleyiş mantığı ise 2 değişken’den sadece enaz 1 tanesi doğruysa benim için problem yoktur diyor. Yani her sayfanın bir admin kullanıcısı vardır galiba :) 1. Değişkenimizi bulduk bile , hadi bakalım.



Username

Password

Login

Hiç parola girme gereksiniminde bulunmuyorum. Şimdi’de bizim yazdığımız payloadı açıklayayım. Biz sorguya şu şekilde müdahale ettik.

Admin kullanıcıasını yazdık ve hemen yanına bir tek tırnak attık’ aslında sorguda bu işlem **username=’admin’** şeklinde oluyor yani admin kullanıcıasını username olarak verdik tırnağı kapattık ve sorgumuzu yazabiliriz artık, eğer ‘ tırnak koymasak tüm yazacağımız bilgiyi **username** değişkeni içine atıcaktı.

Yani şöyle olucaktı;

username=’admin or 1=1#’ böyle bir kullanıcı bilgisi arıcaktı ama biz tek tırnak atarak geri kalan veriyi string kod olarak içeriye sızdırdık.

Or ifadesini anlatmıştım , burada ki **1=1#** ifadeside bir koşul, diğer programlama dillerinde ki “**IF**” blogu gibi düşünebiliriz. 1=1e eşitse.

Ancak yanında bir adet hastag var bu da geri kalan sorguyu ve tüm değişkenleri yorum satırına çeviriyor yani **password=** değişkeni artık bir yorum satırı oldu ve onu sorguya dahil etmicek, yorum satırları ve bazı kodlar kullanılan SQL diline göre değişiklik olabilir.

Ya admin kullanıcısı doğru bir bilgi veya **1=1** ‘e eşittir bilgisi doğru. Değişik **OR** sayesinde **ADMIN** kullanıcıasının hesabına giriş yapcaz. Burada ki **1=1** eşittir ifadesi sadece matematikten ibarettir, **2=2** de yapsanız mantık aynı işlicecektir.

Ve giriş yapalım;

Soru ; E-posta adresi nedir ? | Cevap : sraincin0@moonfruit.hv



Gökyüzü Raincin
sraincin0@moonfruit.hv

Oturumu kapat

Profil Ayarları

İsim	Soyadı
Sky	Raincin
Cep numarası	
172-496-3430	
Adres	
33887 Raven Terrace	
Posta kodu	
57990	
E-posta	
sraincin0@moonfruit.hv	
Ülke	Eyalet/Bölge
Malaysia	Coventry