MEHMET İNCE && AHMET BİRKAN'den Notlar

SQL İNJECTİON ;

Mysql servisini linux'da başlatalım bunu için ;
service myqsql start
service mysql status : Bu ise çalıştığını kontrol etmemiz için gereken komut.
Mysql'e bağlanmak için ise.

Mysql -u root -p : giriş yapıp bağlanmamıza yarar.

Örnek bir site ve arkada da çalışan koda benzer bir şey yazalım.
www.x.com/?id=1
Şimdi bize bir değerinde olan içerik gelicek arkada şu çalışıyor ;

"Select * from haberler where id = 1 "
şimdi biz database i tablo adını columları kaçar tane oldukları hakkında hiçbir bilgimiz yok. Bunun için tek tek bulmak gibi amacımız var. ama öncesinde zafiyeti tespit etmek gerekiyor. İlla zararlı kod çalıştırmaya gerek yok , normal matematiksel bir sorgu da çalıştırabiliyor muyuz kontrol edelim
www.x.com/?id=2-1 veya 2^1
bunun response'u id=1'dir burada sadece 2 den 1 çıkardık böyle bir sorgu çalıştırdık.
Daha sonra sorgu çalıştırabilidiğimi öğrendikten sonra, kendi sorgumuzu yazalım.
Burada UNION ile başlicaz. UNİON'suz bu işlemi yapamayız.

Bizim yazılımcının yazdığı sorgu ile bizim sorgumuzu birleştirmemiz gerekiyor çünkü , bunuda UNION yardımı ile yapıyoruz.

Ve UNION SELECET 1'den başlayarak yaklaşık 1-10 arasına kadar yazalım. Sorguyu çalıştırdıktan sonra site 200 response veriyorsa , siteyi incelersek , bu 1-10 arasında birkaç rakam görmüş olabiliriz bunlar column sayısı. Yani diyelim ki 3 5 7 yi gördük bu alanlara sorgu yazdırabiliriz örnek verirsek ;
SELECT UNION 1,2,DATABASE(),4,VERSİON(),6,BİLGİ(),8,9,10 GİBİ.
Database adını version adını öğrendikten sonra FROM ifadesini kullanbiliriz.

From ifadesini Linux'da ki CD ifadesi gibi düşünebiliriz. Veriyi oradan getirmesini söylüyoruz. Git oradan al gel gibi.
FROM information_schema.tables Where table_schema = database;

İnformation_schema içerisinde sitenin tabloları dataları hakkında bir çok bilgi saklar bu tarz bilgileri buradan sağlicaz.

Bu sorgumuzu yazdık şimdi bu sorgumuzda select kısmından 3,5,7 çıkmıştı ya
o kısımdan birine table_name yazarsak bize tabloları getirircektir.
Diyelim ki users adında tablo bulduk. Burdan veri çekmek istiyorsak artık, columnları çekmek istiyorsak, yapacağımız şey şu

information_schema.columns bunu table olanı columns ile değiştiriyoruz.
Where ile devame edip .Ve çekmesini istediğimiz tablonun adını giriyoruz. Komutu sadeleştirirsek şu şekil

1. Hamle : UNION SELECT 1,2,(table_name)... FROM information_schema.tables WHERE column_table = ‘users’

2. Hamle : UNION SELECT 1,2,(column_name)... FROM information_schema.columns WHERE table_name = ‘users’

3. Hamle : (colmn bulduk): UNION SELECT 1,2,Columnname(),.. FROM users
bunu çalıştırısak username çekmiş oluruz.
Password colmn varsa 3 numara ile yer değiştirip deniyebiliriz.

BU SQL ÇEŞİTLERİNİN UNİON SQLİ OLANIYDI.

SQL İNJECTİON BLİND time değilllll not time

buraya koyduğum fotoğraf işlemin son fotoğrafıdır unutmamak için koyuyorum.

Sql injection açığımız burada cookie içerisinde görüyoruz. Ve burada union değil And ile blind yapıyoruz.
Öncelikle manuel olarak sitemizi kontrol ettik cookie sonunna ;
AND ‘1’=’1
payloadızımı atıp responsa baktık responsda bize hangi durum kodunu ve içerik hakkında ne döndürdüğününe baktık.
1=1 yanıtında site yüklenip bizlere “ siteye hoş geldiniz” adında alan karşılıyordu ama bunu 1=2 yaptığımızda bu yazı gidiyordu , tam da burada blind injectionumuzu tespit ettik.

Birkaç kod atıp işlevlerini inceliyelim

```
AND (SELECT 'a' FROM users LIMIT 1)='a
```

burada users tabloasundan limit 1 yazarak select ile seçtiğimiz ‘a’ ile başlicak olan veriden sadece bir tane ver diyoruz.
Ve bunun da baş harfi a mı ? Diye soruyoruz bunu bu şekilde administrator a kadar ilerlettik.

Kullanıcıyı bulduğumuza göre kaldı şifresini bulmak.

```
AND (SELECT 'a' FROM users WHERE username='administrator' AND
LENGTH(password)>2)='a
```

şimdi burada kodumuzda yeni olan kodlar lenght
bu verinin içeriğinin byte sayısını döndürür örnek vereyim burada şifre 2 den büyük mü demişiz. True döndüyse 3 e çıkarıyoruz ve bu son true döndüğü yere kadar devam etmelidir.

' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='a

şimdi substrıng ile metnin uzunluk içinde ki harf değerinine deneme yapabiliriz. Ve burada 1,1 demişiz bunun anlamı ise 1 tane getir ve 1. karakter. Biz bunu 2,1 yaparsak 1. şifrenin 2 karekteri olucaktır. Burada ki = a da ona manuel denememizdir.
Bunu intercepten yapabilriz. Bu süreçte 1,1 2,1 3,1 4,1 ... şifremiz kaç karekterli ise bu şekilde ilerleyip öğrenmek gerkeiyor.
Ve hatıralrsak true değeri girdiğimizde site bize hoş geldiniz döndürüyordu brute force yaparken buna dikkat edelim.