SQL İNJECTİON İLE VERİ TABANI BİLGİLERİNİ ÇEKMEK

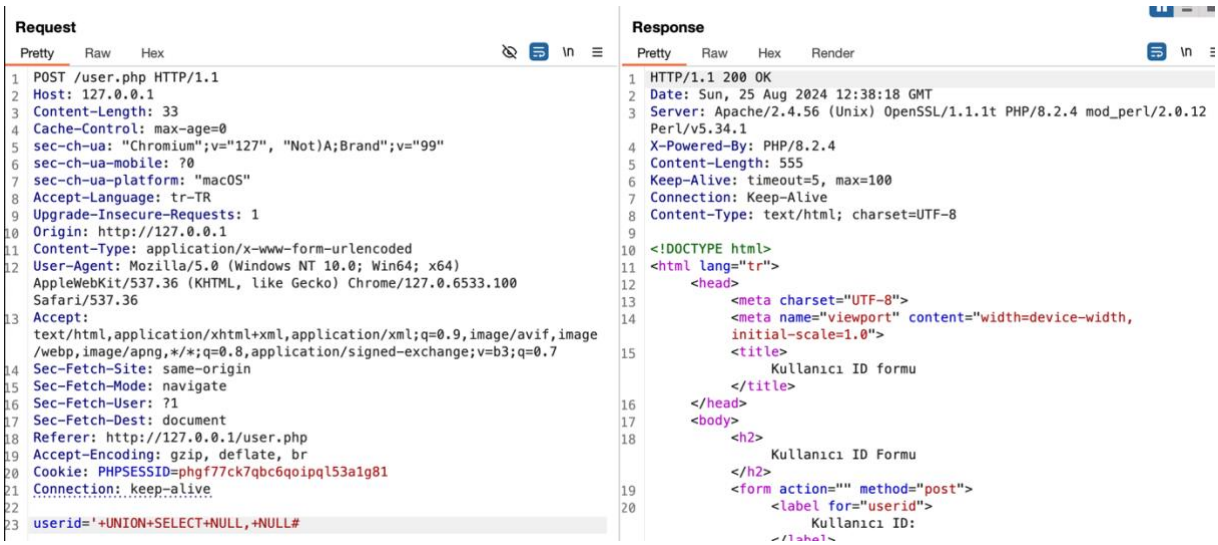
Bu raporda veri tabanı kullanıcısını, adını çekmeyi ve time delay verdirerek sunucuyu geciktirmeyi işleyeceğiz.

1.Veri tabanı kullanıcısını çekmek:

Öncelikle user.php web sitemizin veri tabanından kaç sütun döndürdüğünü öğrenmemiz gerek. Bunu yapmak için union sorgularını kullanacağız. UNION sorguları birden fazla SELECT sorgusunun çalıştırılmasını sağlar ve asıl sorgumuz şu olur. 'UNION+SELECT+NULL# bu ifadeyi detaylandıralım:

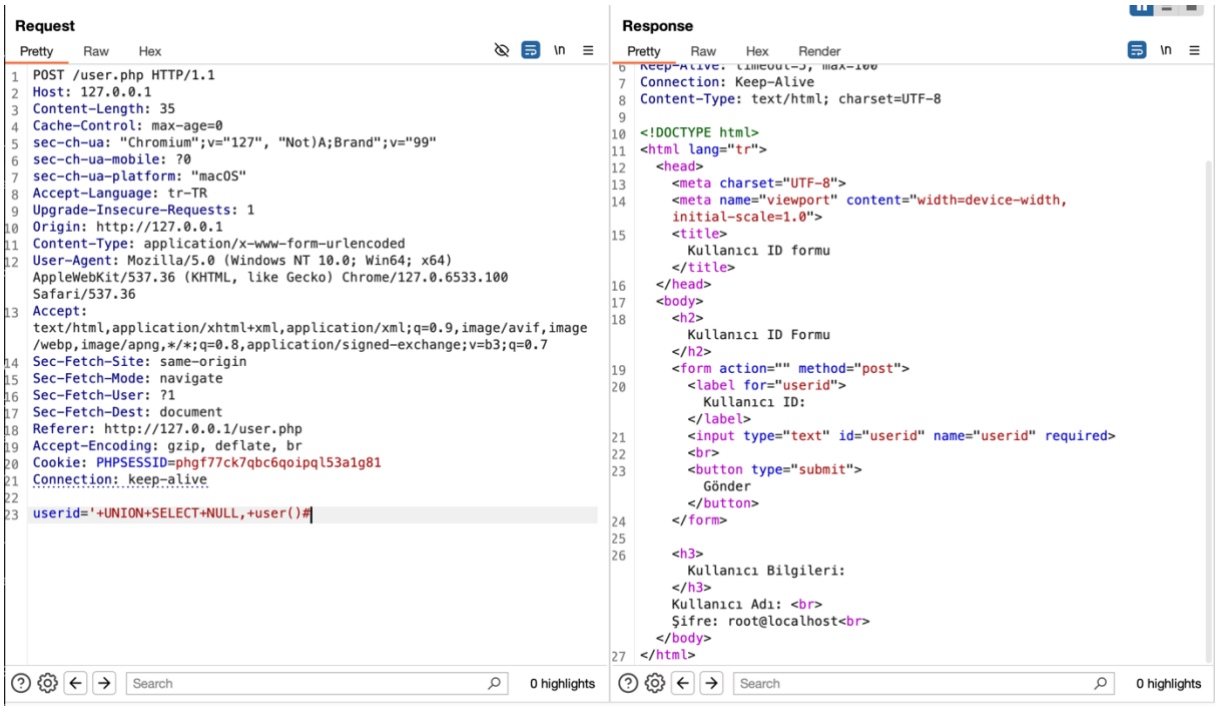
NULL ifadesi sql sorgularında boşluk/boş değer olarak adlandırılır. Bu sayede kaç sütun olduğunu, kaç kez null döndürdüğünü kontrol ederek anlayabiliriz. Sonuçta bu sorgu sütun sayısı kadar null döndürmeli çünkü union sorguları sütun sayısıyla orantılı olmalıdır yoksa hata verebilir. Aralardaki + operatörü url encoding yaparken boşluk ifadesinin geçersizliğinden kaynaklanır bunun yerine + veya %20 ifadeleri kullanılır.

Şimdi user.php için BurpSuite repeater kısmını açıyoruz.Buradaki id kısmına hata vermeyene kadar NULL ekleyerek bu payloadı yükleyeceğiz.



Göründüğü üzere web sitemiz 2 sütun içeriyor. Bunu öğrendiğimize göre 1. veya 2. sütuna (NULL yerine) istediğimiz komutları yazarak veri tabanı bilgilerini çekebiliriz. Öncelikle kullanıcıdan başlayalım:

Veri tabanı kullanıcısını çekmek için mysql,postgresql,mssql gibi farklı veri tabanı yönetici sistemlerinin farklı payloadları olabilir, bunu deneyerek öğreneceğiz. Ben önce mysql olduğunu varsayarak kullanıcıyı çekmek istiyorum, bunun için şunu kullanacağım: '+UNION+SELECT+NULL,+user()

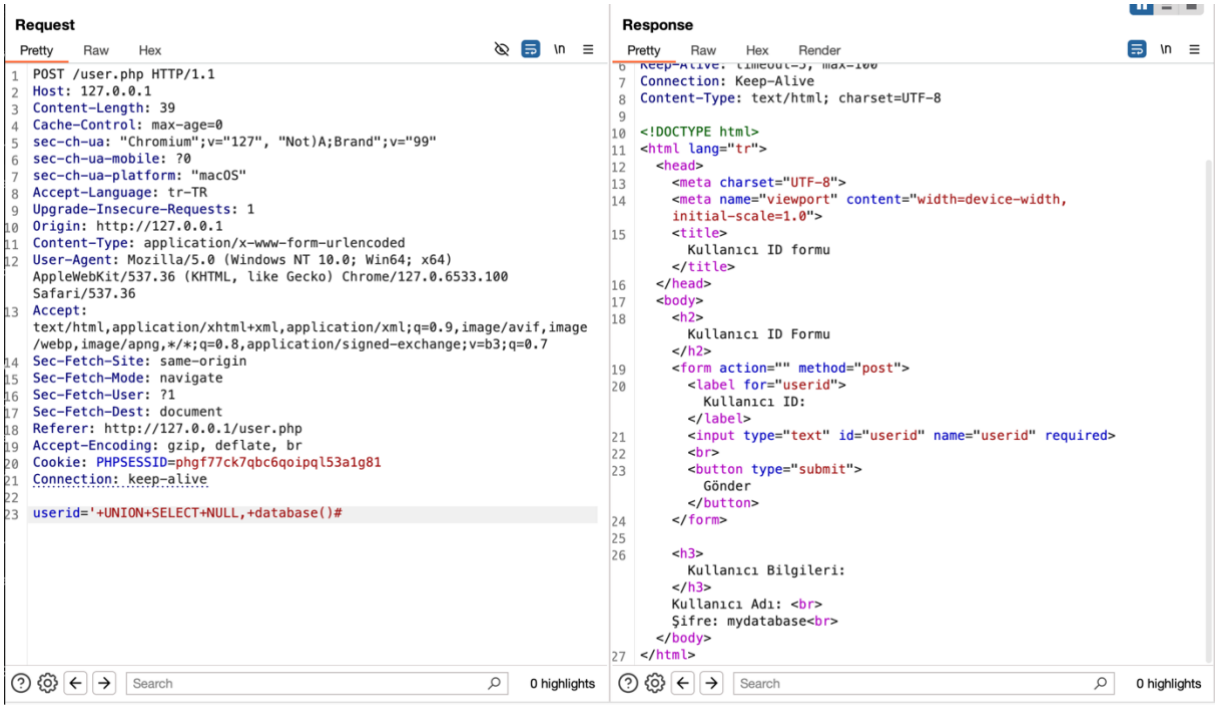


Şekilde görüldüğü gibi sorguyu kullandık, sonundaki # operatörü yüklenen payloaddan sonrasının yoruma alınmasını sağlar. Bunun yerine diğer veri tabanı sunucu sistemlerinde " -- " da kullanılabilir.
Gelen cevabı incelediğimizde bu, veri tabanının root kullanıcısı ile çalıştığını ve bu kullanıcının yerel (localhost) bağlantı üzerinden eriştiğini gösterir.

2. Veri tabanı adını çekmek:

Veri tabanı adını çekmek için asıl sorgumuzaun herhangi bir NULL kısmına database() girebiliriz ve sorgu şuna dönüşür:
'UNION+SELECT+NULL,+database()# bu sorguyu kullanırken yrouma alma operatörünün ve database() kısmının mysql için kullanıldığını unutmamalıyız. Diğer veri tabanı sistemleri için değişkenlik gösterebilir.

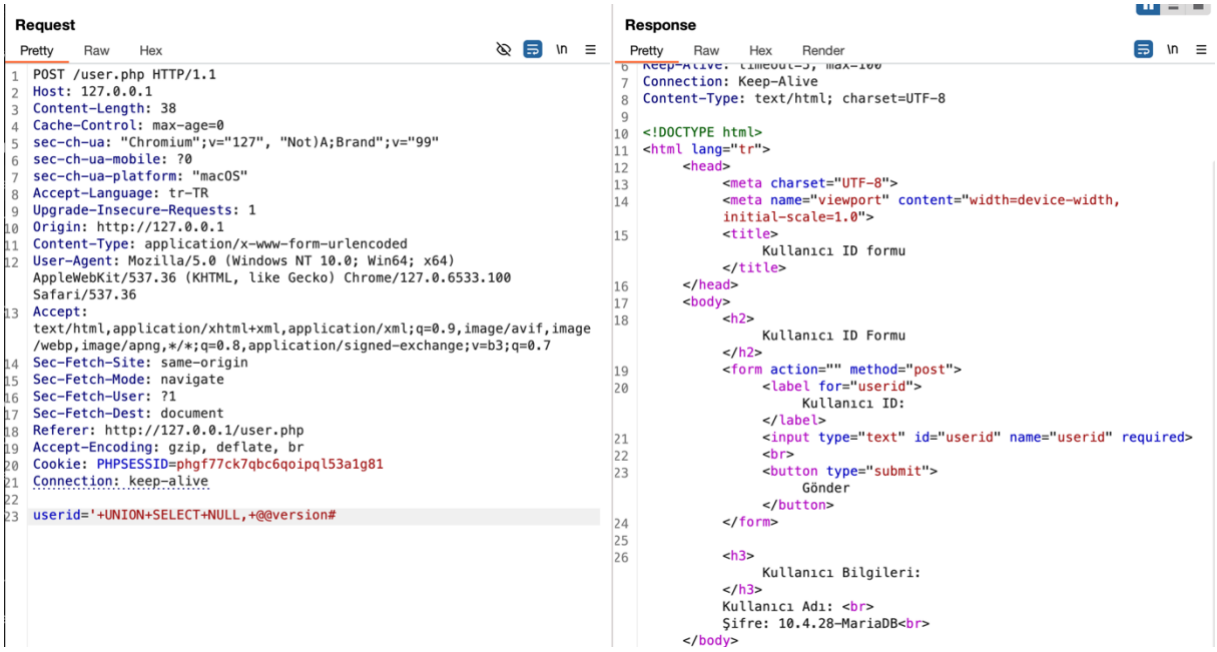
Şimdi sorgumuzu enjekte edelim:



Şekilde görüldüğü gibi gelen cevapta “mydatabase” isimli bir veri tabanı adı görüyoruz.

3. Veri tabanı versiyonunu çekmek:

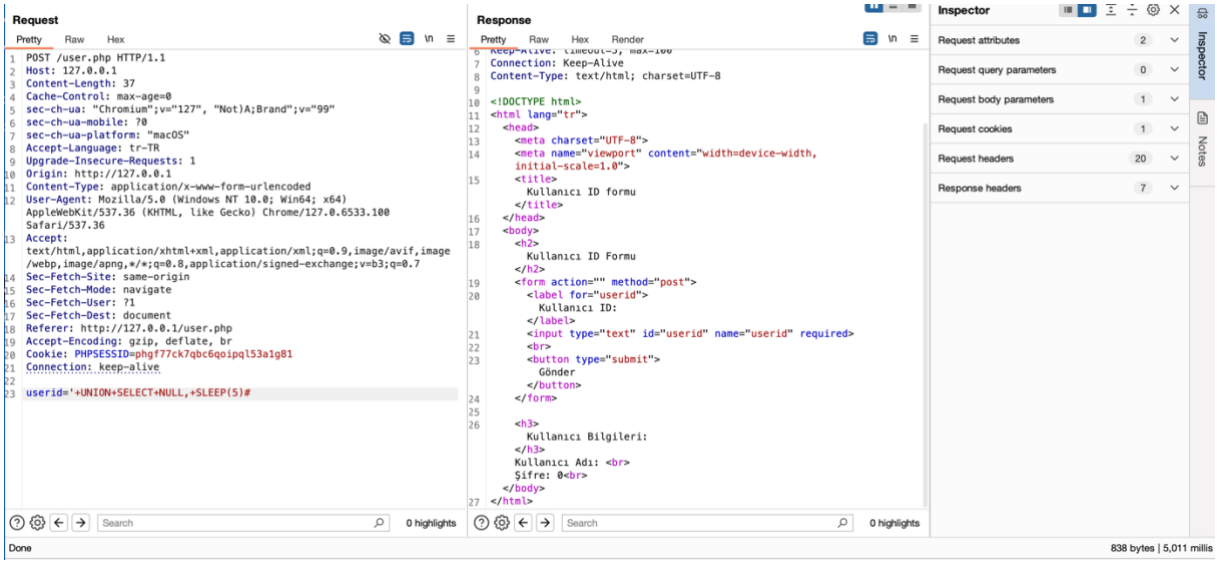
Bunun için yine asıl sorguyu değiştirmeden mysql için uygun olan payloadı yükleyeceğiz. Port Swigger sql injection cheat sheet bölümünde postgresql, mysql, oracle gibi diğer sistemler için payloadlar bulunmaktadır. Biz mysql için kullanacağız. Yani şu sorguyu kullanacağız:
‘UNION+SELECT+NULL,+@@version#



Gelen cevabı incelediğimizde 10.4.28-MariaDB görüyoruz. MariaDB, MySQL'in bir çatallı versiyonudur ve aynı SQL dilini ve birçok aynı arka plan yapılandırmasını paylaşır. 10.4.28-MariaDB çıktısı, kullanmakta olduğunuz MariaDB veritabanı sunucusunun sürüm numarasını ifade eder.

4. Veri tabanı sunucusunu geciktirme:

Veri tabanının mysql sistemli olduğunu anlamıştık. Şimdi sleep fonksiyonunu kullanarak sunucuyu geciktireceğiz.
Bunun için yine sqli cheat sheet kısmından yardım alacağız. İncelediğimiz sayfada mysql için kullanacak olduğumuz payloadı şu şekilde düzenleyebiliriz: '+UNION+SELECT+NULL,+SLEEP(5)#



Şekilde görüldüğü gibi sleep fonksiyonunu kullanarak 5 saniye geciktirmeyi amaçladık ve gelen cevabı sağ alt köşede görüldüğü üzere 5 saniyede aldık.

5. Payloadların etki ettiği kod kısmı:

Yüklediğimiz bu sorguların kaynak kodda nereye etki ettiklerini inceleyelim.

```
32      $id = $_POST['userid'];
33
34      // Burada userid'yi kullaniyoruz. Tablo yapiniza gore uygun sutun adini guncelleyebilirsinz.
35      $query = "SELECT username, password FROM web2 WHERE id = '$id';";
36      $result = $conn->query($query);
```

Bu bölümde, kullanıcının girdiği userID değeri doğrudan SQL sorgusuna dahil ediliyor ve sorgularımız şu hale dönüşüyor : SELECT username, password FROM web2 WHERE id = ''; UNION SELECT NULL, user() #';