SQL INJECTION

Muhammed Fatih YILMAZ

mfth78@hotmail.com

İÇERİK

- SQL injection zafiyeti ve giderilmesi

Kodumuzda gördüğünüz üzere parametreleri direkt sorguya verdiğimizden şu ifade gerçekleşir

```
SELECT * FROM users WHERE username='admin' && password='topsecretpw'
```

Eğer biz sorgudaki ifadelerimiz yerine ‘ or 1=1 – ifadesini yazdığımızda

```
SELECT * FROM users WHERE username=''or 1=1 --' && password=''or 1=1--'
```

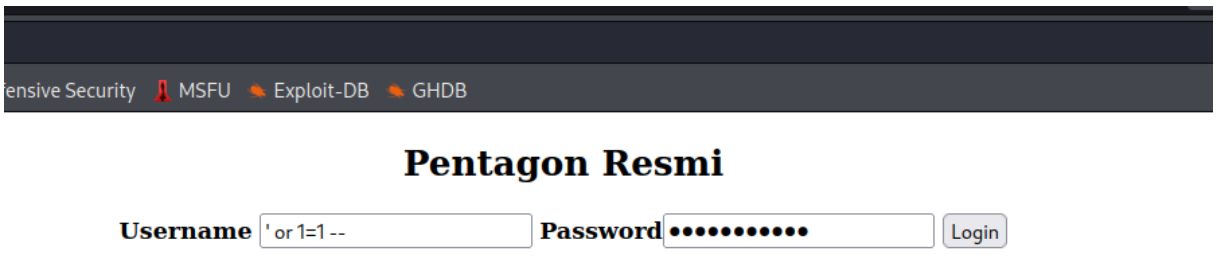
Mysql databasemizde bu ‘ (tırnak) işareti ile sql sorgusundaki ifadeden çıkıp kendi istediğimiz or 1=1 her türlü true olacağı için kendi sorgumuzu doğru kabul edilebilir hale getirdik, -- işareti ile de diğer kısımları yorum olarak mysql algıladı ve bu sayede database de istediğimiz kullanıcıya erişim sağlamış olduk.

first.php

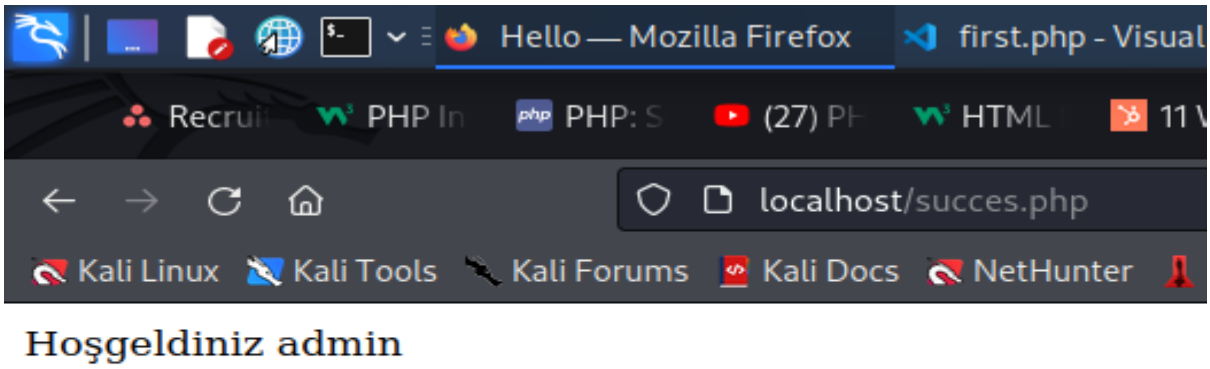
var > www > html > first.php > ...

```
22  </body>
23  </html>
24  <?php
25  try {
26
27      $db=new PDO("mysql:host=127.0.0.1;dbname=sqli","diva","diva");
28      $db->setAttribute(PDO::ATTR_ERRMODE,PDO::ERRMODE_EXCEPTION);
29
30  } catch (PDOException $e) {
31      die(" $e Hata meydana geldi.");
32  }
33  if($_POST){
34      $uname=$_POST["uname"];
35      $pass=$_POST["psw"];
36      $query=$db->query("SELECT * FROM users WHERE username='$uname' && password='$pass'",PDO::FETCH_ASSOC);
37      if($query->rowCount()){
38          foreach($query as $row){
39              $_SESSION["user"]=$row["username"];
40          }
41
42          header("Location:/succes.php");
43
44      }
45      else{
46          echo "Başarısız Giriş";
47      }
```

Zafiyetli Kod Bloğu

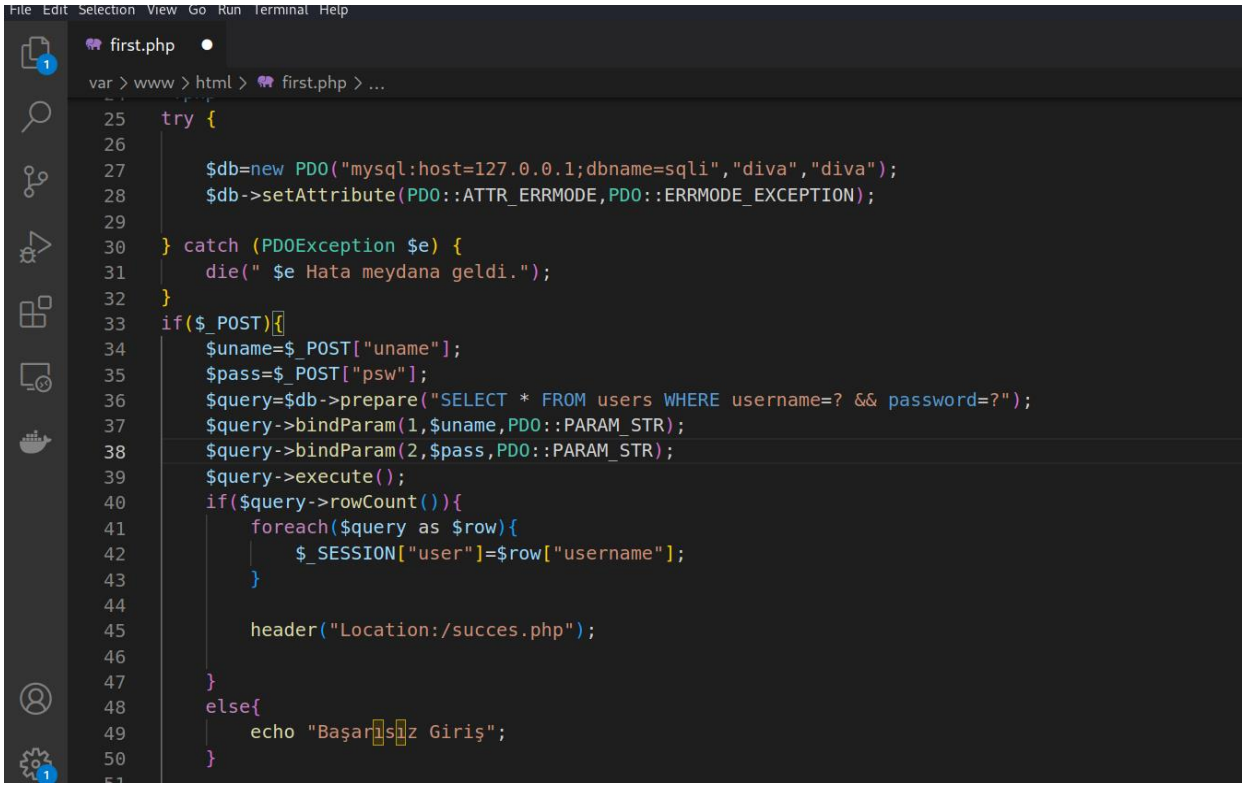


SQL İnjection Deneme

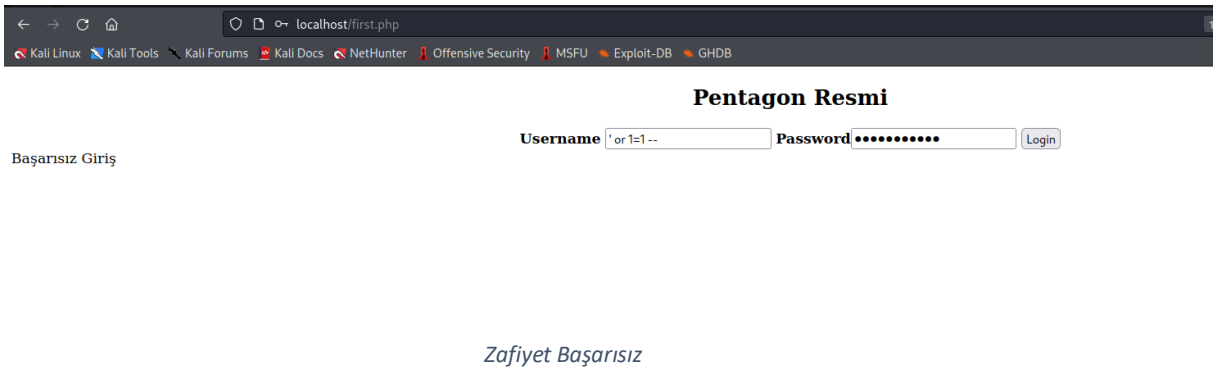


Zafiyet Gerçekleşmesi Sonucu

Bunu engellemek için PDO da aşağıdaki görselde kodda da gözüktüğü üzere prepare fonksiyonu yer almaktadır. Bu fonksiyon SQL sorgusunu oluşturur ve direkt değişkeni almak yerine ? ile değişken yerini tutup bunu databaseye gönderir. Database bu sorgumuzu ayrıştırır, ve execute etmeden saklar. Yani buna bağlı dönecek sonuçlar hazırdır. Daha sonra sorguda ? ile gösterilen parametreleri bindParam komutuyla uygulayarak sorguyu çalıştırır. bindParam da parametrelerin nereye hangi sırayla string mi integer mi olacağını belirleyerek SQL injection zaafiyetini engellemiş oluruz.



Zafiyet Engellenmiş Kod Bloğu



Zafiyet Başarısız