06/08/2021

Mobil Uygulamada SQL Injection

Hazırlayan

Ümmü Derya Çelik

SQL Injection Nedir?

Bir SQL Injection saldırısı, istemciden uygulamaya giriş verileri aracılığıyla bir SQL sorgusunun eklenmesinden veya enjeksiyonundan oluşur.

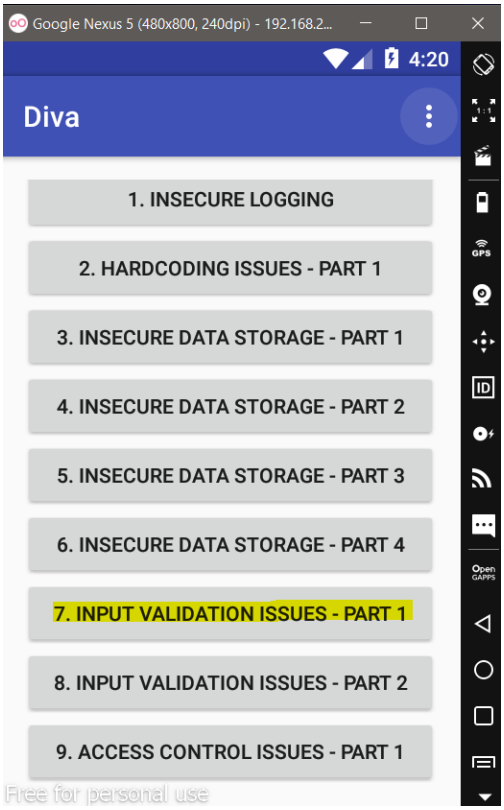
Başarılı bir SQL Injection istismarı, veritabanından hassas verileri okuyabilir, veritabanı verilerinde ekleme, güncelleme, silme gibi değişiklikler yapabilir, veritabanında Veri tabanı yönetim sistemi anlamına gelen DBMS'yi kapatmak gibi yönetim işlemlerini yürütebilir. DBMS dosyasında bulunan belirli bir dosyanın içeriğini kurtarabilir sistem ve bazı durumlarda işletim sistemine komutlar verebilir.

Çoğu mobil uygulama HTML5 teknolojisiyle çalışır. İstemci tarafı depolama, kullanıcıya özel veriler için giderek daha fazla kullanılmaktadır. Uygulama birden fazla hesaba sahip olacak şekilde tasarlanmışsa, SQL Injection saldırısının etkisi daha fazla olacaktır.

Bu saldırı türü OWASP Mobil Top 10 listesinde 7.Madde olan İstemci kod kalite sorunları kategorisine girmektedir. Buradan da anlayacağımız üzere sıklıkla rastlanılan ve sonuçları ağır olan bir zafiyettir.

Bu zafiyeti, örnek göstermek için android emülatörüme indirdiğim Diva uygulamasında bir görelim;

NOT: Emülatör ve testler için ortam kurulumundan diğer raporlarda bahsedilmiştir.



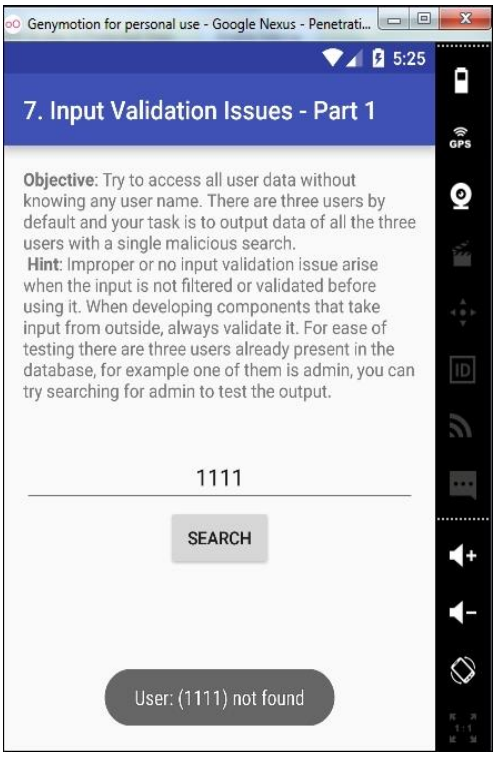
Şekil 1

ilk olarak Emülatörümüzden Diva uygulamasını açalım.

Diva, testler için bilinçli olarak zafiyetli bırakılmış bir uygulamadır.

SQL Injection, 7.Maddede bulunan giriş doğrulama sorunları kategorisine girmektedir.

7.Maddeye tıklıyoruz.

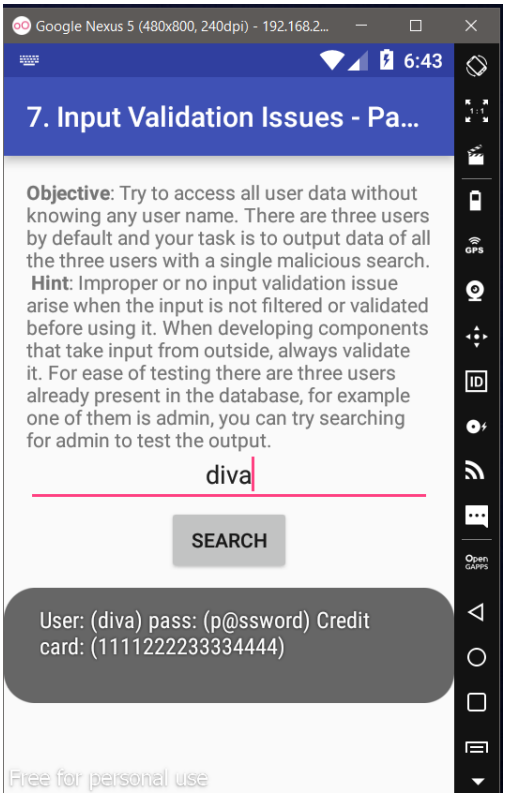


Şekil 2

Görselde görüldüğü gibi bir kullanıcı girişi ekranı gelmektedir.

Denemek adına uygulamada kayıtlı olmadığını bildiğim "1111" gibi bir değer giriyorum ve kullanıcı bulunamadı hatası vermektedir.

Şimdi uygulamada kayıtlı olduğunu bildiği "diva" kullanıcısını deneyelim.



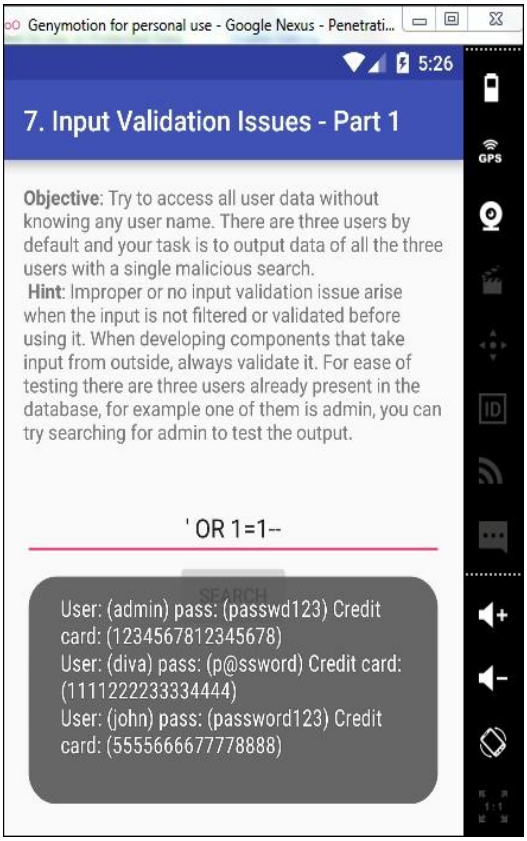
Şekil 3

Kayıtlı kullanıcı girildiğinde görselde de görüldüğü gibi kredi kartı bilgileri ve şifresi gelmektedir.

Şimdi bir de SQL Injection sorgusuyla giriş yapmayalı deneyelim.

Şekil 4

Şekilde de gördüğümüz " diva'or'1'='1 " SQL sorgusu girildiğinde her iki tarafta da 1=1 olduğundan ve koşul sağlandığından %100 doğru kabul edilip veri tabanındaki tüm kullanıcı adı ve bilgileri ele geçirilebilmektedir.



Şekil 5

Yine bu sorgu gibi " ' OR 1=1— " ifadesi yazılırsa yine veritabanı içindeki tüm verilerin görüntülendiğini görebilirsiniz.