**EK 1: Tasarla ve Üret Laboratuvar Etkinliği**

(Çevrimiçi form https://forms.gle/viCFdwqnAccSdrqx9 adresinde mevcuttur. İlgili linki tarayıcı programın adres çubuğuna kopyala-yapıştır yaparak formu açabilirsiniz.)

1. *http://testphp.vulnweb.com/index.php* web adresine bağlanın.
2. Önce *categories* linkine, onun altında ise *posters* linkine tıklayın. İnternet tarayıcı programın adres çubuğunda gördüğünüz adresi tam olarak yazın:

   ……..
3. Adres çubuğunun devamına *OR 1=1* yazıp Enter tuşuna basın. Sayfada ne gibi bir değişiklik olduğunu ve ekranda ne gördüğünüzü aşağıya yazınız.

   ……..
4. Şimdi ise adres çubuğunda *OR 1=1* devamına *bir tek tırnak işareti* ekleyerek Enter tuşuna basın. Sayfada ne gibi bir değişiklik olduğunu yazınız. Bu değişikliği nasıl yorumlarsınız?

   ……..

   ……..

   ……..

   ……..

   ……..
5. 3.maddede belirtilen *OR 1=1* adres satırına *order by 12* ekleyerek Enter tuşuna basınız. Sayfada ne gibi bir değişiklik olduğunu yazınız. Bu değişikliği nasıl yorumlarsınız?

   ……..

   ……..

   ……..

   ……..
6. *Order by 12* yazıp Enter tuşuna basınız.
7. *Order by 11* yazıp Enter tuşuna basınız. Sayfada ne gibi bir değişiklik olduğunu yazınız. Bu değişikliği nasıl yorumlarsınız?

   ……..

   ……..

   ……..

   ……..
8. 3.maddede belirtilen *OR 1=1* adres satırına *union select 1,2,3,4,5,6,7,8,9,10,11* yazıp Enter tuşuna basınız. Bu şekilde 11 sütun olduğunu tekrar doğrulamış oldunuz.

9. Karşınıza gelen sayfada en alta geliniz. En alttaki satırda 7, 2 ve 9 gibi rakamlar göreceksiniz. Bunun anlamı adres çubuğundan yapılan sorguda 2, 7 ve 9 numaralı sütunları kullanabilirsiniz. Aşağıda 2 numaralı sütun kullanılarak devam edilecektir.
10. İnternet tarayıcı program adres satırında en sonda yer alan *union select 1,2,3,4,5,6,7,8,9,10,11* kısmı içerisinde *2* yazan yeri silip yerine *@@version* yazıp Enter tuşuna basınız. Sayfada en alta inerek bu sayfayı çalıştıran işletim sisteminin adını ve versiyon bilgilerinin ne olduğunu yazınız.

    ……..
11. İnternet tarayıcı adresinde *1, @@version,3,4,5,6,7,8,9,10,11* adresinde *@@version* yazan yeri değiştirerek uygulamaya devam edelim. Kodu şu şekilde manipüle ederek Enter tuşuna basınız:

    *1,group_concat(table_name),3,4,5,6,7,8,9,10,11 from information_schema.tables where table_schema=database()*

    Bu kodu yazdıktan sonra sayfanın en altına gidip kontrolleri yapınız. Gördüğünüz tablo isimleri nelerdir? Yazınız.

    ……..

    ……..
12. Users tablosu içerisinden kullanıcı bilgilerine ulaşmaya çalışalım, hatta admin şifresini elde etmeye çalışalım.
13. *1,group_concat(column_name),3,4,5,6,7,8,9,10,11 from information_schema.columns where table_name=0x7573657273* yazarak Enter tuşuna basınız.

> BİLGİ NOTU
>
> Bir metnin hexadecimal kodunu öğrenmek için Google arama motoruna “text to hext” yazınız. Açılan sitelerden herhangi birinde giriş metni olarak users yazıp çevir diyerek users metninin hexadecimal kodunun 7573657273 olduğunu görebilirsiniz.

14. Sayfanın en altına inerek users tablosundaki sütun isimlerinin neler olduğunu yazınız.

    ……..

    ……..
15. Şimdi ise tablodan kullanıcı adı ve şifrelerini elde edelim. İnternet tarayıcı adres satırından sorguyu değiştirmeye devam edelim.

*1,group_concat(uname,0x3a,pass),3,4,5,6,7,8,9,10,11 from users* yazarak Enter tuşuna basınız.

Sayfanın en altına inerek sayfadaki kullanıcı adı ve kullanıcı şifresinin ne olduğunu yazınız.

……..

16. Bu bilgileri denemek için İnternet tarayıcı programı adres satırına *http://testphp.vulnweb.com/login.php* yazıp Enter tuşuna basınız. Elde ettiğiniz kullanıcı adı ve şifresini yazarak sisteme giriş yapınız. Başarılı bir giriş yaptıysanız ekranda ne gördüğünüzü not ediniz.

……..

……..

……..

……..

17. 11 ile 16 numaralı işlem adımlarını users tablosu dışında başka bir tablo için deneyiniz. Sonuçları not ederek adım adım hangi bilgilere ulaştığınızı yazınız.

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

Not: Bu etkinlikle ilgili daha detaylı teorik açıklamalara bilgeis.net adresinden ulaşılabilir (Bilge İş, 2022).