# YAZILIM LABORATUVARI PROJE 3

Ferdi ELİK-140202066,Furkan AYDIN-140202034

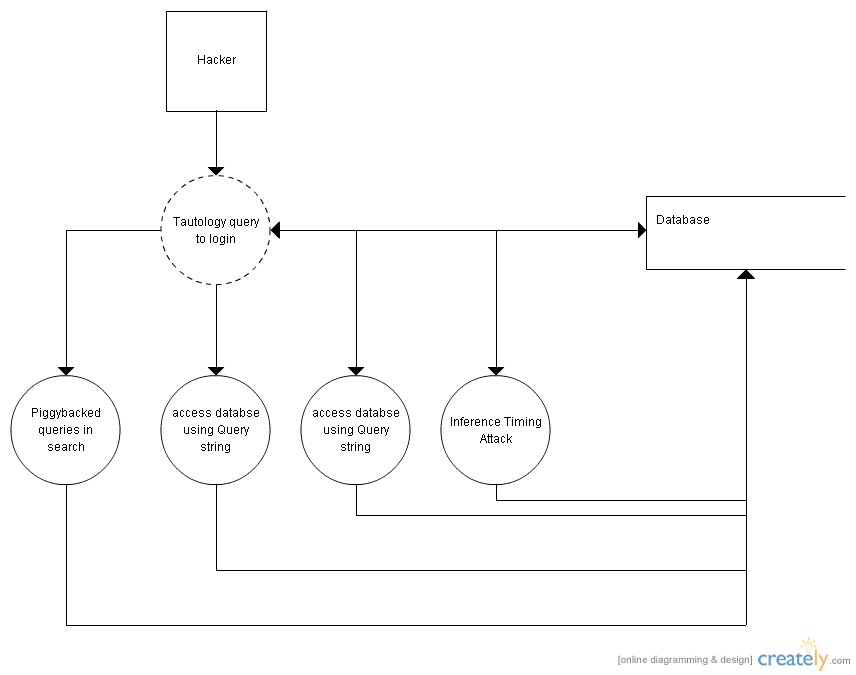
**PROJE:**ZAYIF (VULNERABLE) WEB UYGULAMALARI GELİŞTİRİLMESİ

**1. Problem Tanımı:**Projemiz de bizden bir zayıf web uygulaması oluşturmamız ve onun bazı açıklarını kullanarak bu uygulamayı daha iyi bir hale nasıl getirebiliriz bunu görmemiz istenmektedir.Kullandığımız SQL injection,Command injection,XSS-Cross site scripting gibi müdahaleler gerçekleştirerek bunları nasıl engelleyebiliriz bunu görmemiz gerekmektedir.

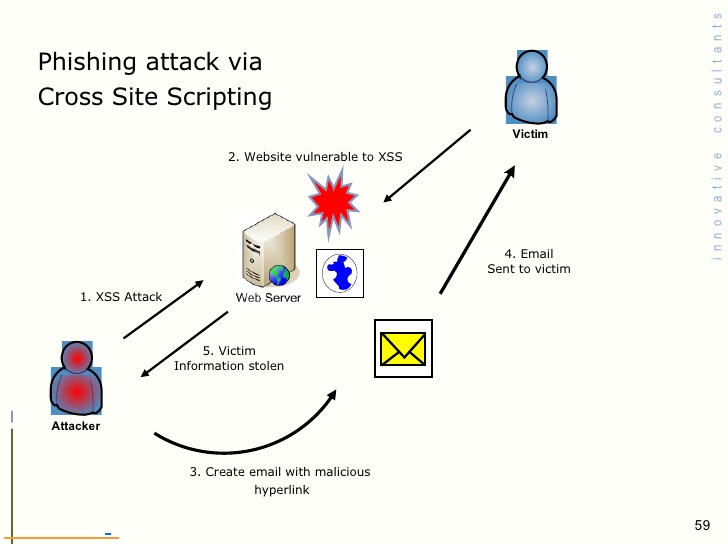
**2. Yapılan Araştırmalar:** Proje yapılma aşamasında SQL injection,Command injection ve XSS'i tek tek araştırdık.Bizim kendi kullandığımız java da nasıl bu tür müdahaleleri gerçekleştirebiliriz ve bu konu da nasıl önlemler alabiliriz bunu inceledik.Bir çok örnek üzerinde durduk.Projemiz de localhost kurmak için kullandığımız TomCat Server'ı[1] araştırdık ve bunu Intellij de nasıl kullanabiliriz bunu araştırdık.Database ile ilgili de araştırmalarımız oldu ve bunları nasıl uyum içinde kullanabileceğimiz konusunda araştırma yaptık.

**3. Tasarım**

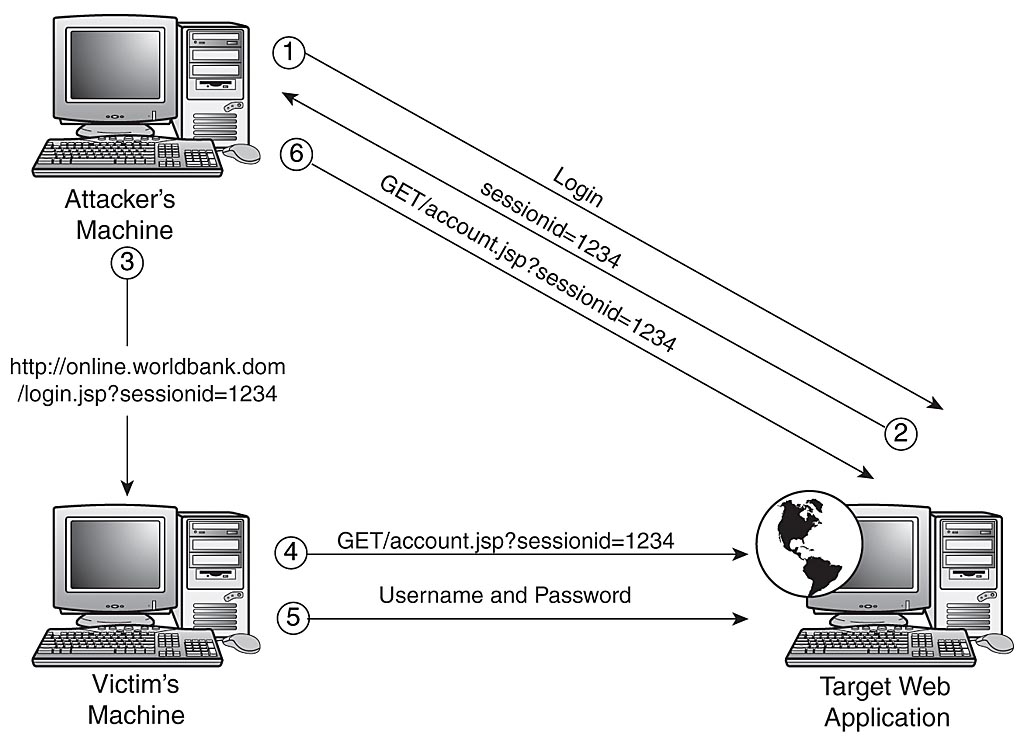
**3.1. SQL Injection**



**3.2.XSS-Cross Site Scripting[2]**



**3.3.Command Injection[3]**



**4. Yazılım mimarisi:** Projemizi Java dili ile kodladık.Web sitesini oluştururken arayüz de javascript kullandık ve css'den yararlandık.Database kısmında mysql'den yararlandık.IDe olarak ise Intellij'i kullandık.Localhost için TomCat Server'dan yararlandık.

**5. Genel Yapı:** Projemizi genel olarak açıklayacak olursak eğer bir kısım zayıf web sitelerinde işe yarayacak olan siteye erişim müdahalelerini kendi oluşturduğumuz zayıf web uygulamasına uygulayarak bu konu da bilgi sahibi olduk ve aynı zaman da bu müdahaleleri nasıl engelleyebiliriz hangi önlemler alabiliriz bunları öğrendik.

**6. Referanslar:**

**Website**

-**[1]** https://www.jetbrains.com/help/idea/2017.1/run-debug-configuration-tomcat-server.html

**-[2]** https://www.acunetix.com/websitesecurity/cross-site-scripting/

**-[3]** http://www.includekarabuk.com/kategoriler/DVWAUygulamasi/Ders-4---Command-Injection-Low-Level.php

-stackoverflow.com

**Communication**

Discord

Teamviewer

Bitbucket

**Connection**

Git Hub/Git Bash