BİLGİSAYAR MÜHENDİSLİĞİ WEB SAYFASI YAPIMI



YAZILIM LABORATUARI II / PROJE III

**ZAYIF (VULNERABLE) WEB UYGULAMALARI GELİŞTİRİLMESİ**

Cihan SAVAŞ (130202098)

Mehmet Samet YILDIZ (150202104)

Bilgisayar Mühendisliği Bölümü

Kocaeli Üniversitesi

[cihansavas.85@gmail.com](mailto:cihansavas.85@gmail.com), [msy3443@gmail.com](mailto:msy3443@gmail.com)

Cihan Savaş-130202098 Cihat Duyku-150202106

*Mehmet Samet Yıldız-150202104*

Bilgisayar Mühendisliği Bölümü

Kocaeli Üniversitesi

[cihansavas.85@gmail.com](mailto:cihansavas.85@gmail.com), [cihatduyku@gmail.com](mailto:cihatduyku@gmail.com)

[msy3443@gmail.com](mailto:msy3443@gmail.com)

# Özet

Bu projenin amacı ülkemizdeki siber güvenlik derslerinde kullanılabilecek bir düzeyde vulnerable web uygulamaları geliştirmektir. Bunun için sadece üzerinde zafiyetler bulunan bir web uygulaması değil bu uygulamadaki zafiyetlerin neden kaynaklandığının ve bu zafiyetlerin nasıl sömürüleceğinin (exploitation) de açık ve anlaşılır bir şekilde dokümantasyonu yapılmıştır.

# Giriş

# Projede üç temel zaafiyet üzerinde durulmuş örnekler yapılmış ve zaafiyetler giderilmiştir. SQL Injection, XSS ve Command Injection işlenmiştir. Her zaafiyet için bir Yardım butonu eklenmiştir. İlgili yönergeye, zaafiyet hakkındaki tanımlara ve bilgilere bu yardım butonu üzerinden ulaşabilirsiniz. Ayrıca her zaafiyet sömürüldükten sonra giderilmeye çalışılmıştır. Zaafiyeti olmayan güvenliği arttırılmış sayfalara ulaşmak için ilgili uygulamanın yardım butonuna bastıktan sonra gelen ekranda zaafiyeti gider butonuna tıklayıp sömürü yapmaya çalışabilir ve sonuçları karşılaştırabilirsiniz

# Temel Bilgiler ve Genel Yapı

Projeyi gerçeklerken yararlandığınız teknolojiler; Php,HTML5,CSS,Ajax,Jquery,Mysql,Bootstrap gibi web dünyasının mihenk taşı olan aynı zamanda son teknolojileri yakalayan mimarilerdir.

Projede web güvenlik için en temel üç zafiyet sömürülmeye çalışılırken. Yardım butonu ile ekrana pop-up şeklinde gelen responsive bir modal ile nasıl sömürü yapılacağı açıkça anlatılmıştır.

# Yazılım Mimarisi

1)Proje 4 temel sayfadan oluşmaktadır.Bunların alt sayfaları da mevcuttur.

2)index.php:Anasayfa olarak kullanılan sayfadır. Temel olarak projenin amacı ve yapısı anlatılmıştır.

3)kurulum.php:Kurulum dokümantasyonu site içinde de belirtilip şekillerle anlatılmıştır.

4)sql.php:Bu sayfada sql injection zafiyeti sömürülmüş olup zafiyeti giderilmiş olan sqli.php sayfasına dallandırılmıştı.

5)xss.php:Bu sayfada xss zafiyeti sömürülmüştür. Sömürü için bir login paneli örneği kullanılmıştır. Eğer sistemde bir kullanıcı yoksa direkt olarak oturum.php sayfasına yönlendirilmektedir. Varsa hoş geldiniz olarak kullanıcı adı selamlanmaktadır. Zafiyeti giderilmiş olan sayfa ise xssafe.php olarak belirlenmiştir.

6)komut.php:komut enjeksiyonu zafiyeti işlenmiştir. Zafiyeti giderilmiş sayfa ise komutsafe.php olarak belirtilmiştir.

# Yapılan Araştırmalar ve Karşılaşılan Sorunlar

Öncelikle birkaç doküman okunarak zafiyetler hakkında bilgiler toplanmıştır. Bunun için Önay Metin KIVILCIM’ın slide share daki dokümanı incelenmiştir.

Ayrıca include Karabük adlı web sayfasından yararlanılmış ve youtube üzerinden çeşitli güvenlik uygulama dersleri izlenerek kavranmaya çalışılmıştır.

Php dili hakkında araştırma yapılmış olup mysqli kullanımı detaylıca öğrenilmiştir

Projede back-end kısmında zaman zaman aksaklıklar yaşanmıştır. Bu problemler syntax hatası ve mysqli kullanımı ile alakalı olmuştur.Stackoverflow üzerinden hatalar giderilmiştir.

Xss sayfasında login ile bir örnek yapılmak istenmiştir. Session kullanımında bir takım hatalar ortaya çıkmıştır.

ob\_start();

session\_start();

Yukarıda görüldüğü üzere session\_start(); komutundan önce ob\_start(); komutu kullanılarak bu sorun çözülmüştür.

Hatalar için bakılan stackoverflow linkleri

<http://stackoverflow.com/questions/21555927/php-check-which-form-was-submitted>

<http://stackoverflow.com/questions/15836551/how-to-change-default-browser-for-wamp>

<http://stackoverflow.com/questions/28965288/how-to-display-php-code-and-html-tags-as-text-in-a-web-page>

<http://stackoverflow.com/questions/60174/how-can-i-prevent-sql-injection-in-php>

# Kaynakça

[1] Comman Injection

1. <https://youtu.be/BVI1-ikJ-xw?list=PLjIugO7mKMYxWoCVpt7qXZ5thI4d0vaHF>
2. <http://www.recepkizilarslan.com/os-command-injection-ile-sistemlere-sizma/>
3. <http://blog.btrisk.com/2015/02/isletim-Sistemi-Komutlari-Enjeksiyonu.html>
4. <https://www.exploit-db.com/papers/13597/>

[2] XSS Injection

1. [http://musana.net/xss-detayli-dokuman.html/](http://www.sinanoztop.com/css-ve-jquery-ile-modal-box-nasil-yapilir/)
2. <https://hackerolmak.wordpress.com/xss-nedir-nasil-yapilir-genis-anlatim/>
3. <https://youtu.be/D7KndoW1Tj8>
4. <https://www.mertsarica.com/xss-ve-beef/>
5. <https://www.sitepoint.com/php-security-cross-site-scripting-attacks-xss/>

[3 ]SQL Injection

1. <http://www.zskblog.com/detay.aspx?id=22>
2. <http://www.wikihow.com/Prevent-SQL-Injection-in-PHP>
3. <http://php.safakbilisim.com/tag/sql-injection/>

## Kazanımlar

Bu projede Sql Injection, Xss Injection ve Commamd Injection üzerimde durularak web programlama yaparken bıraktığımız zafiyetleri fark etmiş olduk bizim için daha sağlam kod yazmamız gerektiğini fark ettik aslında yazdığımız kodların çoğu o kadarda güvenilir olmadığını fark ettik Bunları giderilmesi ve özellikle filtreleme yöntemlerini araştırarak bunları kullanmayı öğrendik. PHP dilinde salt olarak yazmak yerine mysqli veya PDO kullanımının önemi bizim için kazanım oldu bu tarz hem nesneye yönelik hemde güvenilir methodları araştırarak öğrenmiş olduk. Ayrıca izlediğimiz tuttorialler sayesinde sniffing nasıl yapılır sunucu nasıl ele geçirilebilir veya veri tabanı nasıl görüntülenir bunları açıkları kullanarak tecrübe etmiş olduk.

## Tasarım Ekran Görüntüleri

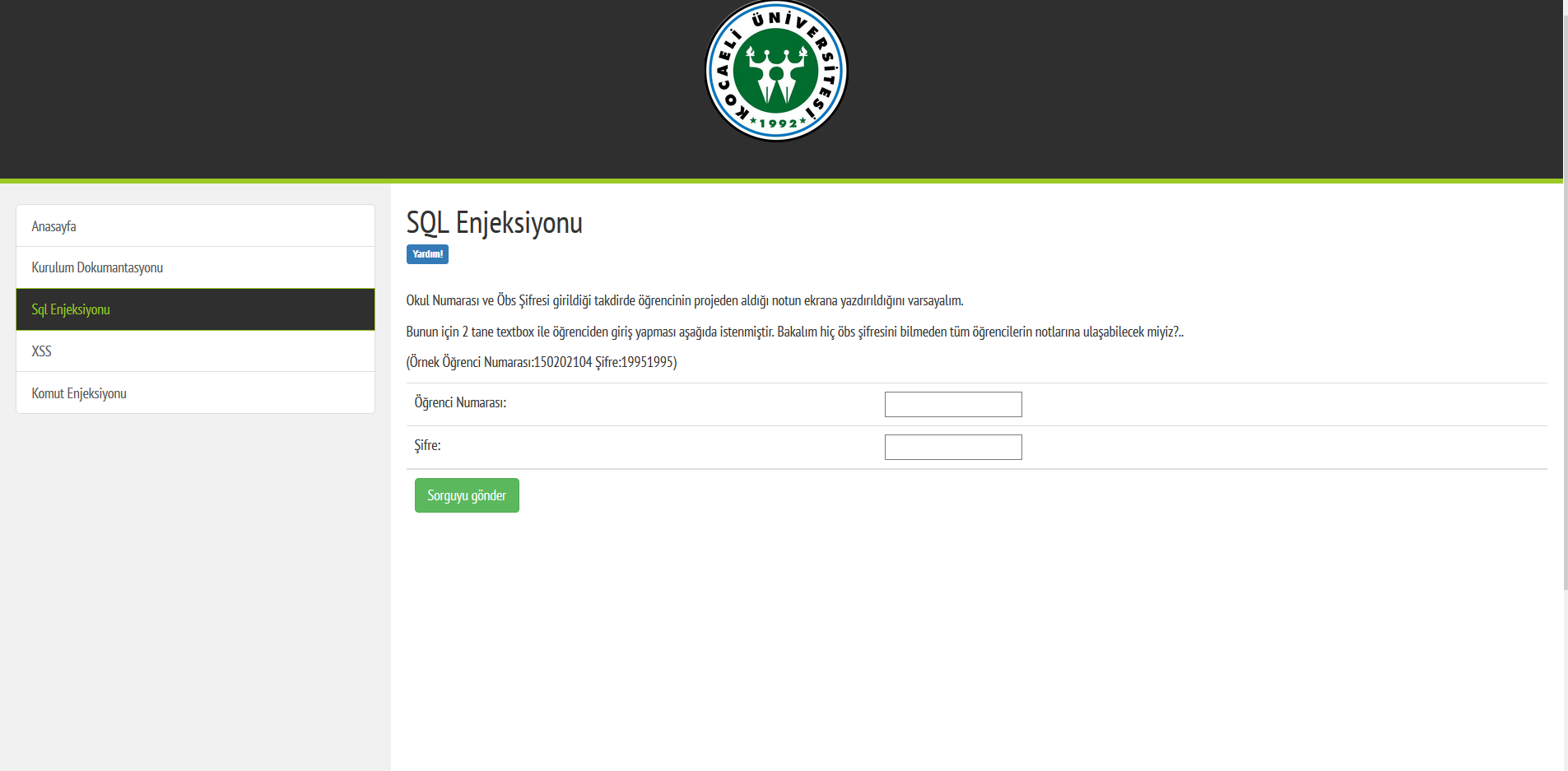
1)



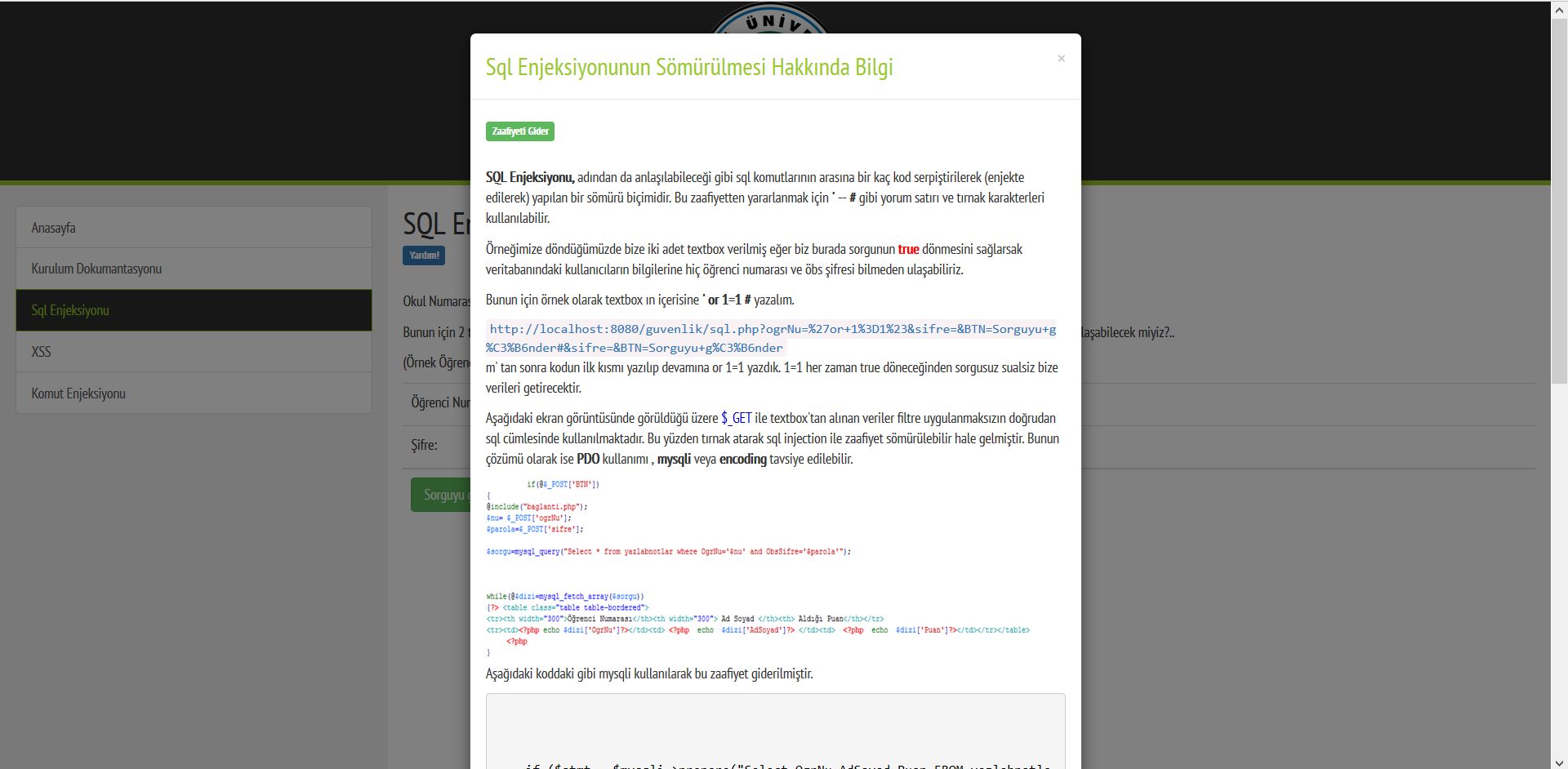
2)



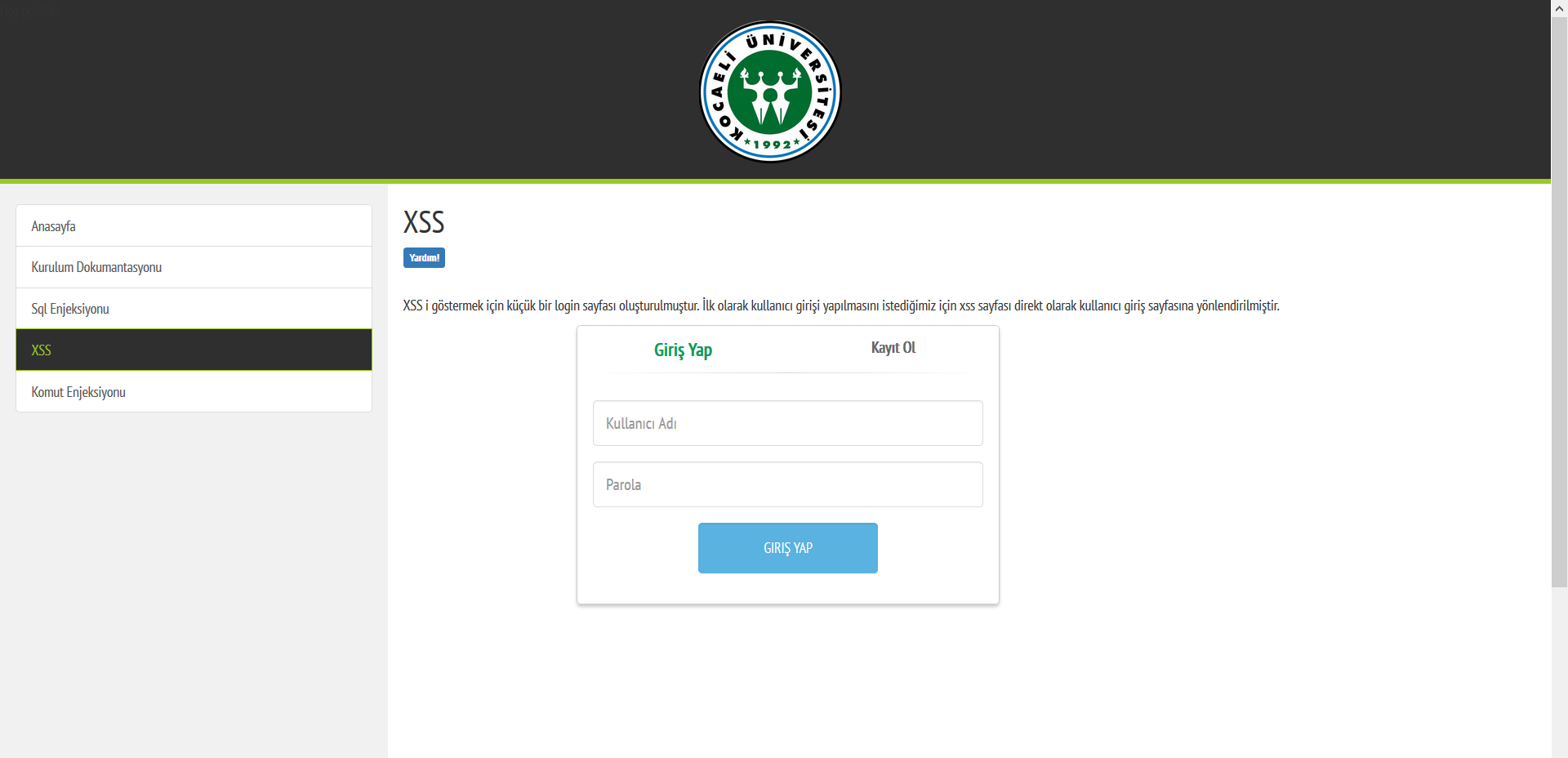
3)



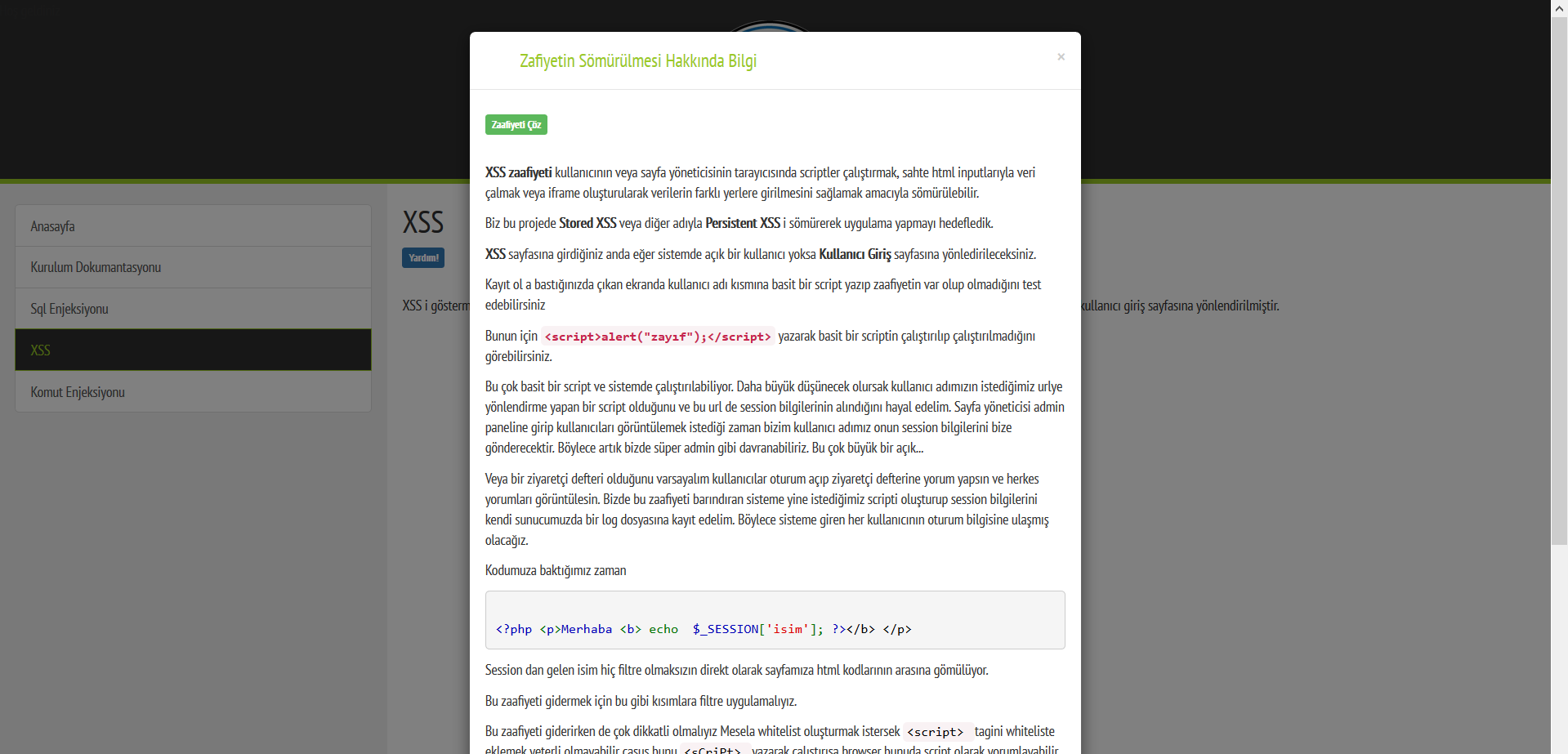
4)



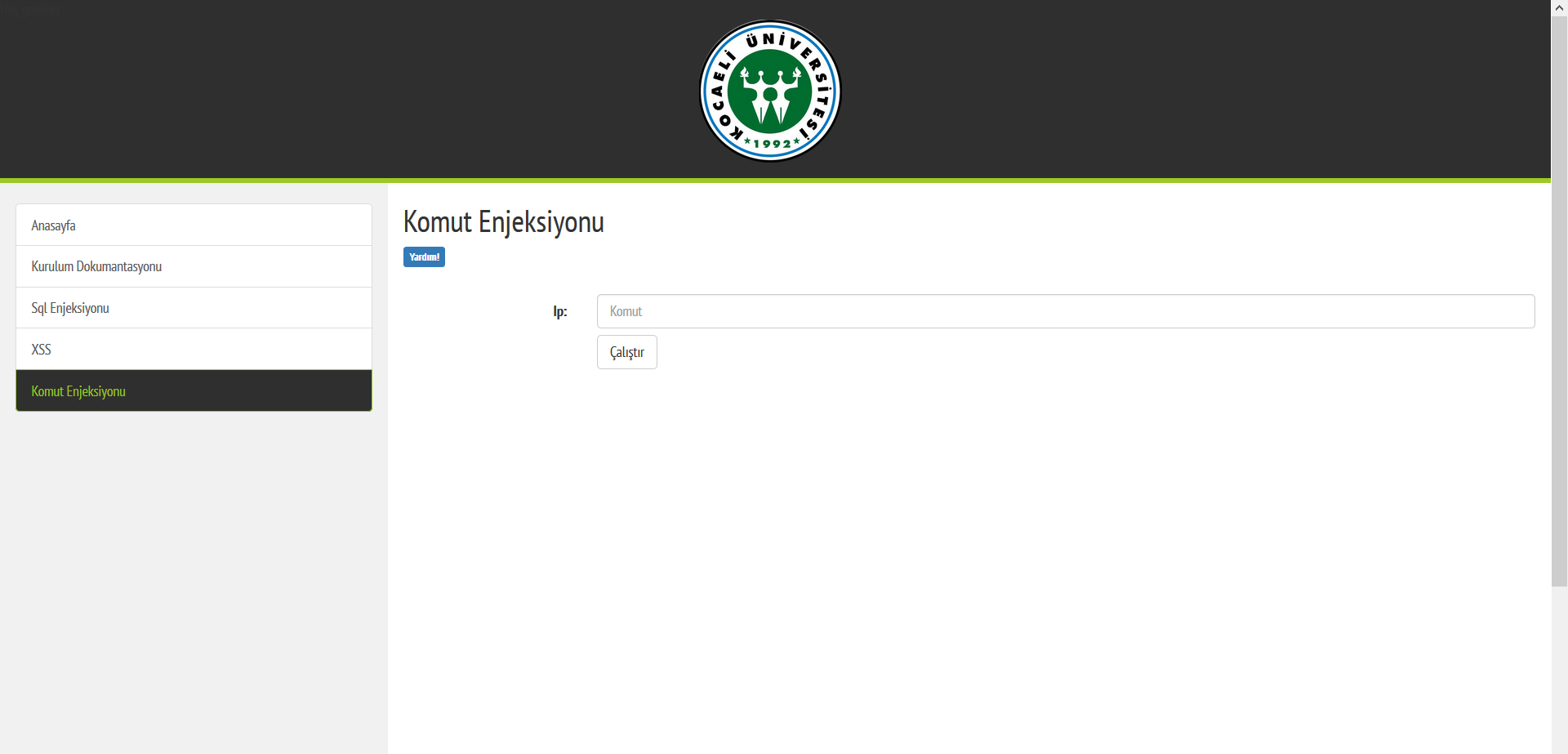
5)



6)

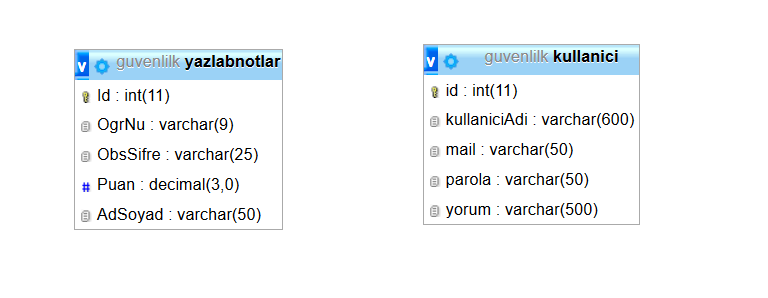


7)



## Veri Tabanı

## Mysql tablo görünümü



\*Tablolar Arasında bir ilişki kurulmamış, sadece uygulamaya yönelik veri tabanı kayıtları turtulmuştur.

## Er Diagramları

