**ANKARA ÜNİVERSİTESİ**

**MÜHENDİSLİK FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

****

**BLM4538 - IOS İle Mobil Uygulama Geliştirme II**

**Proje Raporu**

**EMİR ŞEN**

**21290158**

**17.03.2025**

**GitHub Linki:** [https://github.com/ertaku12/BugSheriff-React-Native](https://github.com/ertaku12/BugSheriff-React-Native%20)

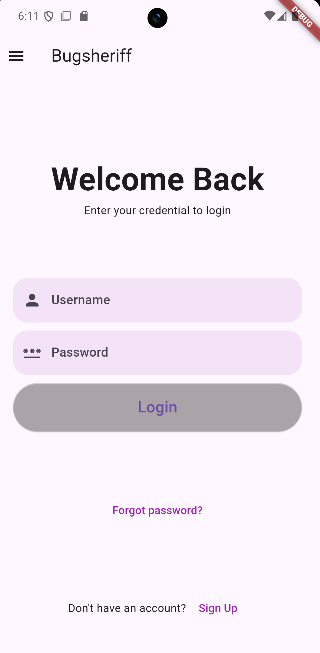
**Proje Adı:** Bug Bounty Platformu

**Amaç:**

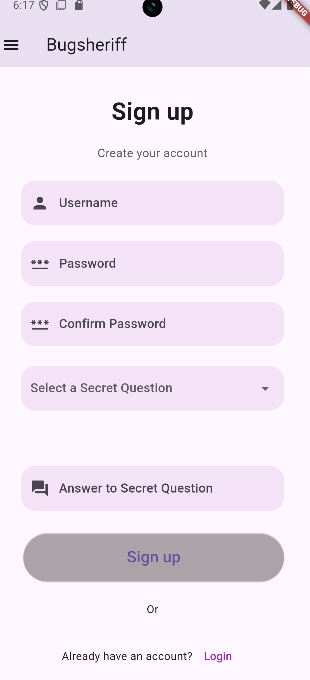
Bu proje; kullanıcıların sistemde güvenlik açıklarını rapor edebilecekleri, ödüller kazanabilecekleri ve rapor geçmişlerini takip edebilecekleri bir bug bounty platformunu içermektedir. Platformda kullanıcılar, güvenlik açıklarını tespit edip bununla ilgili rapor gönderecekler. Eğer bu raporlar onaylanırsa ödülleri verilecektir.

**Front end – React Native:**

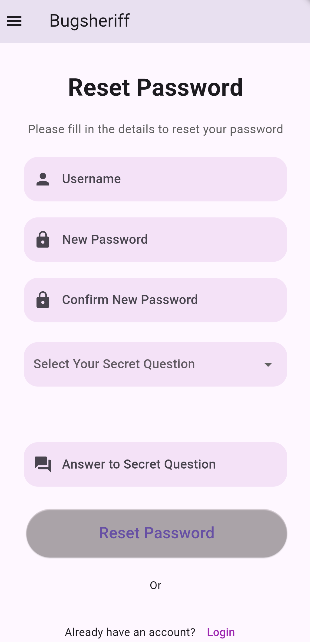
**Login Page**



**Register Page**

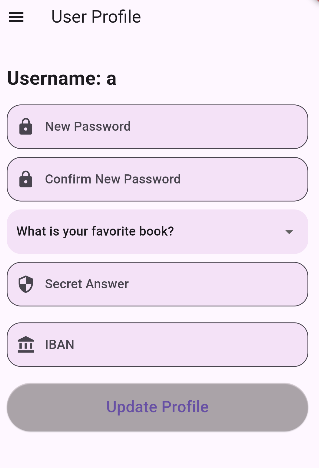


**Forgot Password (gizli soru)**

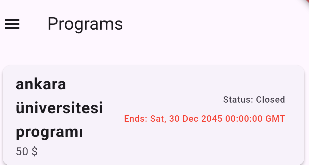


**Kullanıcıların profil sayfası**

* Kullanıcı profilindeki bilgileri düzenleyebilir.



**Programların listelendiği sayfa**



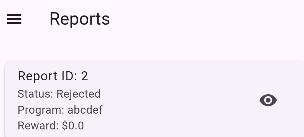
**Program detayları sayfası**

* Programlara tıklandığında böyle bir sayfa açılacak. Buraya kullanıcı, zafiyetini açıklayan PDF formatında bir raporu sisteme yükleyebilecek.

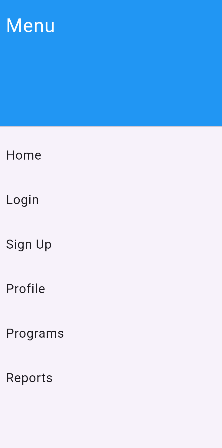


**Raporlar sayfası**

* Kişi sadece kendi gönderdiği raporları görüntüleyebilir. Başkasının raporunu göremez.
* Sağdaki göze tıklandığında PDF formatındaki rapor görüntülenebilecek.

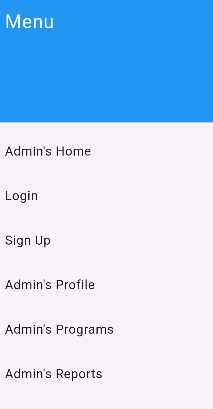


**User’s Sidebar**



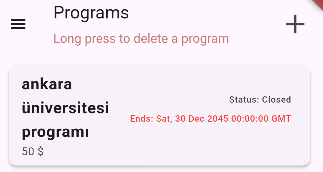
**Admin’s Sidebar**

* Kullanıcı adı ‘admin’ ise başka bir sidebar kullanıcıyı karşılayacak (login ekranından sonra).
* Admin kullanıcısının fonksiyonlarına normal bir kullanıcı asla erişemeyecek.



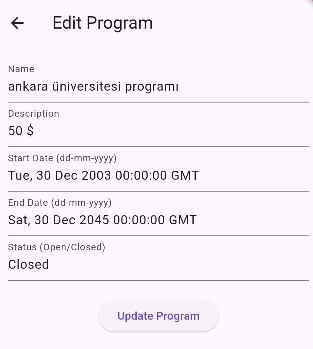
**Admin’in program sayfası**

* Admin program silebilecek, yeni program ekleyebilecek.



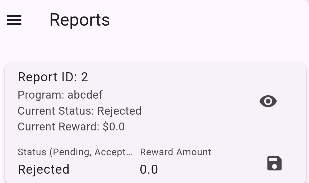
**Admin’in program detay sayfası**

Programlara tıklandığında böyle bir sayfa açılacak. Admin kullanıcısı programın ayrıntılarını düzenleyebilecek.



**Admin rapor sayfası**

* Admin adlı kullanıcı tüm raporları görüntüleyebilmektedir.
* **Fonksiyonlar:** Raporların görüntülenmesi, ödül belirlenmesi, raporların durumlarının belirlenmesi (Pending, Accepted, Rejected)
* Rapor eklerinin (pdf) görüntülenmesi



**Backend / Python – Flask:**

* Authentication ve Authorization mekanizmalarının ayarlanması (JWT)
* PostgreSQL veri tabanının kullanılması
* API fonksiyonlarının yazılması
* Dockerize edilmesi

Backend için örnek bir veri tabanı girdisi aşağıda verilmiştir.

Aynı komut ‘Docker-psql-flask/README.md’ adlı dizininde mevcuttur.

**Veritabanı terminaline erişim:**

docker exec -it postgresql bash

psql -U admin -d bugsheriff

**Veritabanı girdi komutu:**

INSERT INTO programs (name, description, application\_start\_date, application\_end\_date, status) VALUES

('Cyber Defenders Bug Hunt',

'Scope: Web Applications, APIs, and Cloud Infrastructure. Look for Vulnerabilities such as XSS, SQL Injection, and Authentication Bypass. Rewards are Categorized as Low ($50-$150), Medium ($151-$500), and High ($501-$1000).',

'10-01-2024',

'12-31-2024',

'Open'),

('Mobile Security Challenge',

'Scope: iOS and Android Apps. Test for Insecure Data Storage, Improper Platform Usage, and Security Misconfigurations. Rewards: Low ($100), Medium ($300), High ($700).',

'09-15-2024',

'11-15-2024',

'Closed'),

('E-commerce Bug Smash',

'Scope: E-commerce Platform Including Checkout Process, User Accounts, and Payment Systems. Prioritize Finding Flaws like CSRF, IDOR, and Logic Flaws. Rewards: Low ($200), Medium ($500), High ($1200).',

'11-01-2024',

'01-31-2025',

'Open'),

('Cloud Fortress PenTest',

'Scope: AWS, Azure, and Google Cloud Platforms. Focus on Misconfigurations, Privilege Escalations, and Insecure API Gateways. Rewards: Low ($250), Medium ($750), High ($1500).',

'12-01-2024',

'02-01-2025',

'Open'),

('IoT Device Security Crackdown',

'Scope: Internet of Things (IoT) Devices and Their Companion Applications. Look for Issues like Insecure Firmware Updates, Weak Authentication, and Privacy Vulnerabilities. Rewards: Low ($100), Medium ($400), High ($900).',

'10-15-2024',

'12-15-2024',

'Closed');

**Genel Kaynak Kod Yapısı**

**Endpointler**

1. GET /admin/getreports

**Amaç:** Tüm raporları listeleme (sadece adminler için).

**İşleyiş:** Report tablosundaki tüm kayıtlar sorgulanır ve program adı, rapor yolu, durumu gibi bilgiler JSON olarak döndürülür.

2. PUT /admin/report/<int:report\_id>

**Amaç:** Raporun durumunu veya ödül miktarını güncellemek.

**İşleyiş:**

* ID’ye göre rapor bulunur.
* status ve reward\_amount değerleri güncellenir.

3. POST /admin/newprogram

**Amaç:** Yeni bir bug bounty programı eklemek.

**İşleyiş:**

* Gerekli alanların (name, description, application\_start\_date, application\_end\_date, status) boş olup olmadığı kontrol edilir.
* Yeni bir Program oluşturulur ve veritabanına eklenir.

4. DELETE /admin/program/<int:program\_id>

**Amaç:** Program ve ilişkili raporları silmek.

**İşleyiş:**

* ID’ye göre program bulunur ve silinir.
* Program ile ilişkili raporların dosyaları ve kayıtları silinir.

5. PUT /admin/program/<int:program\_id>

**Amaç:** Mevcut bir programın detaylarını güncellemek.

**İşleyiş:**

* Yeni bilgilerle mevcut alanlar güncellenir.

5. POST /register

**Amaç:** Yeni bir kullanıcı oluşturmak.

**İşleyiş:**

* Kullanıcı adı, şifre, gizli soru/cevap kontrol edilir ve kaydedilir.
* Şifre *generate\_password\_hash* ile güvenli şekilde saklanır.
* Kullanıcı tipi atanır (user, admin).

6. POST /login

**Amaç:** Kullanıcı girişi yapmak ve JWT token oluşturmak.

**İşleyiş:**

* Kullanıcı adı ve şifre kontrol edilir.
* Geçerli bilgilerle giriş yapılırsa, *create\_access\_token* ile bir JWT token üretilir.

7. POST /reset-password

**Amaç:** Şifre sıfırlama işlemi yapmak.

**İşleyiş:**

* Kullanıcı adı ve gizli soru/cevap eşleşmesi kontrol edilir.
* Eski şifreyle aynı olmama kontrolü yapılır.
* Yeni şifre hashlenerek kaydedilir.

8. PUT /update-user

**Amaç:** Kullanıcı bilgilerini güncellemek.

**İşleyiş:**

* Şifre, gizli soru/cevap ve IBAN gibi bilgiler güncellenir.
* IBAN’ın 34 karakter sınırına uyup uymadığı kontrol edilir.

9. GET /user-details

**Amaç:** Kullanıcı bilgilerini görüntüleme.

**İşleyiş:**

* JWT'den alınan kullanıcı kimliğiyle, veritabanından kullanıcı bilgileri çekilir.

10. GET /programs

**Amaç:** Programları listeleme.

**İşleyiş:**

* Admin kullanıcılara tüm programlar, normal kullanıcılara ise sadece açık (Open) programlar gösterilir.

11. POST /upload

**Amaç:** Kullanıcıların raporlarını PDF olarak yüklemesi.

**İşleyiş:**

* Programın durumu (Open veya Closed) kontrol edilir. Yalnızca Open programlar için yükleme kabul edilir.
* Dosyanın PDF formatında olduğu doğrulanır.
* Benzersiz bir isimle “uploads” klasörüne kaydedilir.
* Yeni bir Report kaydı oluşturulur.

12. GET /reports

**Amaç:** Kullanıcının raporlarını listeleme.

**İşleyiş:**

* JWT kimliği ile kullanıcının raporları sorgulanır.
* Program adı, durum ve ödül bilgileri JSON formatında döndürülür.

13. GET /uploads/<path:filename>

**Amaç:** Kullanıcının kendi rapor dosyalarını indirmesi.

**İşleyiş:**

* Kullanıcının rapor üzerinde yetkisi olup olmadığı kontrol edilir.
* Dosya, "uploads" klasöründen sunulur.

14. GET /admin/uploads/<path:filename>

*/uploads/<path:filename>* yoluna benzer bir işlev adminler için sağlanır. Bu yola sadece ***user\_type=admin*** olanlar erişebilir.

Genel Notlar

Güvenlik:

* jwt\_required ve admin\_required dekoratörleri sayesinde endpoint'ler koruma altına alınmış.
* Şifreler hashlenerek saklanıyor.

Dosya Yükleme ve Yönetimi:

* Yalnızca PDF dosyaları kabul ediliyor.
* Yüklenen dosyalar için UUID tabanlı benzersiz isimlendirme kullanılıyor.

Veri tabanı Yönetimi:

* *SQLAlchemy* kullanılarak programlar, raporlar ve kullanıcılar arasında ilişkiler yönetiliyor.

Hata Yönetimi:

* Hatalı işlemler için uygun HTTP durum kodları (400, 403, 404) ve mesajlar döndürülüyor.

**Kontrol listesi:**

* User Sidebar (Home, Login, Signup, Profile, Programs, Reports)
* Admin Sidebar (Admin’s Home, Login, Signup, Admin’s Profile, Admin’s Programs, Admin’s Reports)
* Home Page
  + Kullanıcı
  + Admin
* Login Page
* Signup Page
* Forgot Password (Gizli soru ile)
* Profil sayfası
  + Kullanıcı
  + Admin
* Programların listelendiği sayfa
  + Program arama
* Program detayları sayfası
  + Rapor yükleme
* Raporların listelendiği sayfa
  + Rapor arama
  + Rapor pdf’inin görüntülenmesi
  + Rapor durumunun görüntülenmesi
* Admin için programlar sayfası (tüm programlar)
  + Program arama
  + Program ekleme
  + Program silme
  + Program düzenleme
* Admin için raporlar sayfası (tüm raporlar)
  + Rapor arama
  + Rapora ödül ve durum ataması yapma
  + Rapor eki (pdf) görüntüleme