

ANKARA ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ



BLM4538 - IOS İle Mobil Uygulama Geliştirme II

Proje Raporu

EMİR ŞEN

21290158

19.06.2025

GitHub Linki: <https://github.com/ertaku12/BugSheriff-ReactNative>

APK Linki: https://drive.google.com/file/d/15QEb1TR7P5mX1G58UdhbQ59xwWLweUj9/view?usp=drive_link

Video Linki: https://drive.google.com/file/d/1kIC-jr1ePG-IF4RKROBmpCcScuF0gSUK/view?usp=drive_link


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:

Giriş Yap Sayfası

 Login

Welcome Back

Enter your credentials to login

Username

Password

Login

[Forgot password?](#)

Don't have an account? [Sign Up](#)

Kayıt Ol Sayfası

≡ Signup

Sign Up

Create your account

Username

Enter username

Password

Enter password

Confirm Password

Confirm your password

Secret Question

Select a Secret Question

Secret Answer

Answer to your secret question

Create Account

or

Already have an account? Log In

Şifremi Unuttum Sayfası (gizli soru)

≡

Forgot Password

Reset Password

Please fill in the details to reset your password

Username

New Password

Confirm New Password

Secret Question

Select Your Secret Question

▼

Secret Answer

Reset Password


Remember your password?

☐

Log In

Kullanıcıların profil sayfası

- Kullanıcı profilindeki bilgileri düzenleyebilir.

 Profile

User Profile

Username: a

New Password

Confirm New Password

What is your favorite book? ▼

Devlet Ana

Tr123456778

Update Profile

Programların listelendiği sayfa

Programs

Programs

Search programs

Cloud Fortress PenTest

Scope: AWS, Azure, and Google Cloud Platforms.
Focus on Misconfigurations, Privilege Escalations, an...

Status: Open

Ends: Sat, 01 Feb 2025 00:00:00 GMT

VIEW DETAILS

IoT Device Security Crackdown test 2021 2029

Scope: Internet of Things (IoT) Devices and Their
Companion Applications. Look for Issues like Insecur...

Status: Open

Ends: Wed, 12 Dec 2029 00:00:00 GMT

VIEW DETAILS

E-commerce Bug Smash

Scope: E-commerce Platform Including Checkout
Process, User Accounts, and Payment Systems. Prior...

Status: Open

Ends: Fri, 31 Jan 2025 00:00:00 GMT

VIEW DETAILS

Program detay sayfası

- Programlara tıklandığında böyle bir sayfa açılır. Buraya kullanıcı, zafiyetini açıklayan PDF formatında bir raporu sisteme yükleyebilir.

≡ Program Details

Cloud Fortress PenTest

Description:

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

Start Date:

Sun, 01 Dec 2024 00:00:00 GMT

End Date:

Sat, 01 Feb 2025 00:00:00 GMT

Status:

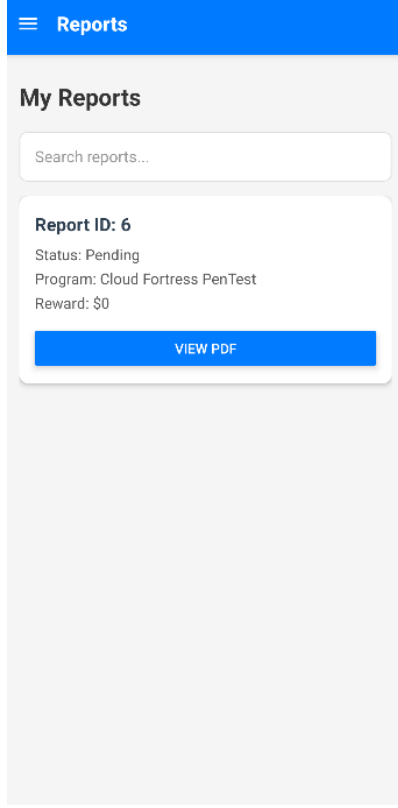
Open

UPLOAD REPORT (PDF)

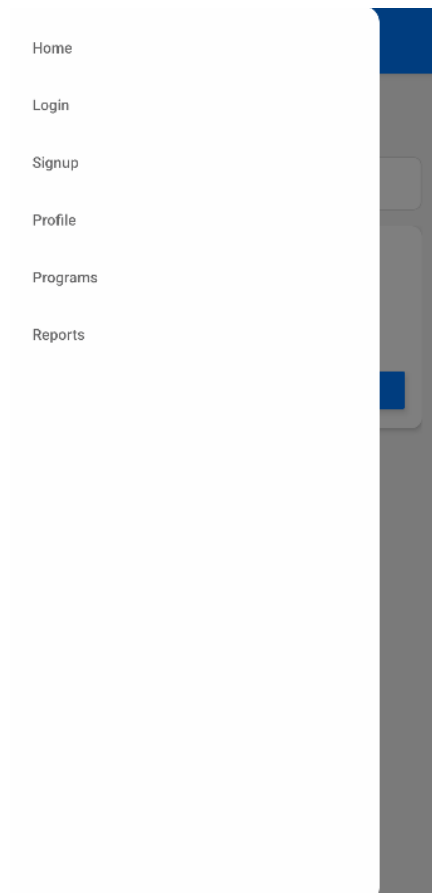
GO BACK

Raporlar sayfası

- Kişi sadece kendi gönderdiği raporları görüntüleyebilir. Başkasının raporunu görüntüleyemez.
- 'View PDF'e tıklandığında PDF formatındaki rapor görüntülenebilir.

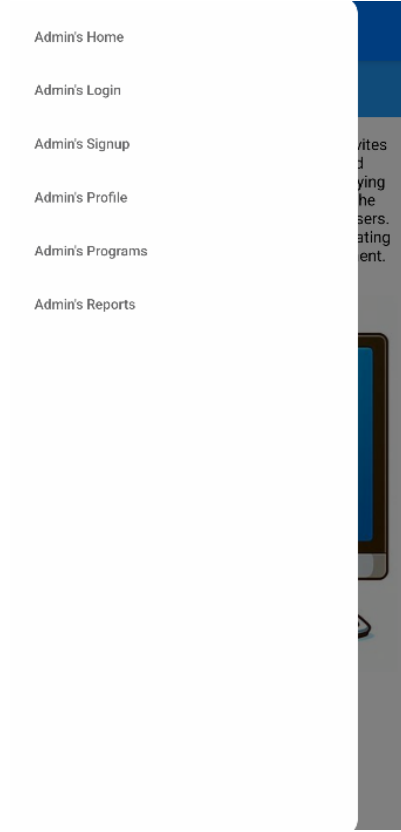


User's Sidebar




Admin's Sidebar

- Kullanıcı adı 'admin' ise başka bir sidebar kullanıcıyı karşılayacak (login ekranından sonra).
- Admin kullanıcısının fonksiyonlarına normal bir kullanıcı asla erişemez.



Admin'in program sayfası

- Admin program silebilir, yeni program ekleyebilir.

 Admin's Programs

Search Programs

Long press a program to delete it

ADD PROGRAM

Mobile Security Challenge
Scope: iOS and Android Apps. Test for Insecure Data Storage, Improper Platform Usage, and Security Misc...
Status: Closed
Ends: Fri, 15 Nov 2024 00:00:00 GMT

Cloud Fortress PenTest
Scope: AWS, Azure, and Google Cloud Platforms. Focus on Misconfigurations, Privilege Escalations, an...
Status: Open
Ends: Sat, 01 Feb 2025 00:00:00 GMT

IoT Device Security Crackdown test 2021 2029
Scope: Internet of Things (IoT) Devices and Their Companion Applications. Look for Issues like Insecur...
Status: Open
Ends: Wed, 12 Dec 2029 00:00:00 GMT

Cloud Fortress PenTest testson
Scope: AWS, Azure, and Google Cloud Platforms. Focus on Misconfigurations, Privilege Escalations, an...
Status: Closed
Ends: Sat 01 Feb 2025 00:00:00 GMT

Admin'in program detay sayfası

Programlara tıklandığında böyle bir sayfa açılır. Admin kullanıcısı, program ayrıntılarını düzenleyebilir.

Admin Program Details

Name

Mobile Security Challenge

Description

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

Start Date (MM-DD-YYYY)

09-15-2024

End Date (MM-DD-YYYY)

11-15-2024

Status

Closed

UPDATE PROGRAM

GO BACK

Admin Rapor Sayfası

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

Admin's Reports

Search by ID, Program Name, Status, or Reward

Refresh

Report ID: 4

Cloud Fortress PenTest testson

Status: Accepted

Reward: 250

IBAN: [Kopyala](#)

Save

View PDF

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 alınmıştır.
- Şifreler hashlenerek saklanmaktadır.

Dosya Yükleme ve Yönetimi:

- Yalnızca PDF dosyaları kabul edilmektedir.
- Yüklenen dosyalar için UUID tabanlı benzersiz isimlendirme kullanılmaktadır.

Veri tabanı Yönetimi:

- *SQLAlchemy* kullanılarak programlar, raporlar ve kullanıcılar arasında ilişkiler yönetilmektedir.

Hata Yönetimi:

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

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
 - o Kullanıcı
 - o Admin
- Login Page
- Signup Page
- Forgot Password (Gizli soru ile)
- Profil sayfası
 - o Kullanıcı
 - o Admin
- Programların listelendiği sayfa
 - o Program arama
- Program detayları sayfası
 - o Rapor yükleme
- Raporların listelendiği sayfa
 - o Rapor arama
 - o Rapor pdf'inin görüntülenmesi
 - o Rapor durumunun görüntülenmesi
- Admin için programlar sayfası (tüm programlar)
 - o Program arama
 - o Program ekleme
 - o Program silme
 - o Program düzenleme
- Admin için raporlar sayfası (tüm raporlar)
 - o Rapor arama
 - o Rapora ödül ve durum ataması yapma
 - o Rapor eki (pdf) görüntüleme