# 

**T.C.**

**SAKARYA ÜNİVERSİTESİ**

**BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ**

BSM 498 BİTİRME ÇALIŞMASI

**WEB SECURİTY PENTEST TOOL**

**UYGULAMASI**

**RAPOR-3**

**B181210030 – VEDAT ARSLAN**

**Fakülte Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ**

**Tez Danışmanı : Prof.(Doç.) Dr. İbrahim Özçelik**

**2023-2024 Bahar Dönemi**

BÖLÜM 3.

PROJE TASARIMI

|  |  |
| --- | --- |
| 3.1. Injectıon Ekranı Tasarımı………………………………………………. | 2 |
| 3.1.1 XSS Injection Ekran Tasarımı .....………………………………………………… | 2 |
| 3.1.2 SQL Injection Ekran Tasarımı ......................................................... | 2 |
| 3.1.3 Command Injection Ekran Tasarımı ……………………………… | 3 |
| 3.2. Brute Force Ekran Tasarımı …………………………………………….. | 3 |
| 3.3. DoS(Denial of Service) Attack Ekran Tasarımı..……………………… | 4 |
| 3.4. OWASP TOP 10 Ekran Tasarımı ………………………………………... | 4 |
| 3.5. Usom(Ulusal Siber Olay Müdahale) Ekran Tasarımı …………………… | 5 |
| 3.6 Nessus Report Ekran Tasarımı... ................................................................. | 5 |
| 3.7 Fuzzing Ekran Tasarımı...………………...………………………………. | 6 |
| 3.8 Bot Net Ekran Tasarımı…………………………………………………... | 6 |

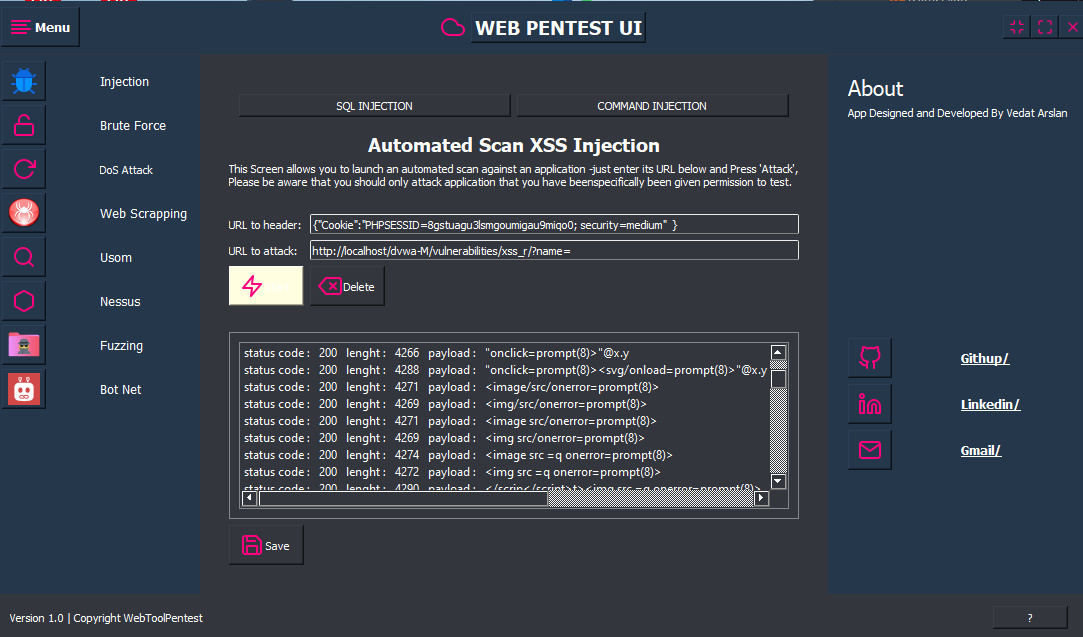
**BOLÜM 2.PROJE TASARIMI.**

**3.1 Injection Ekran Tasarımı**

Injection Ekran Tasarımı 3 sayfadan oluşmaktadır. Bunlar XSS, Sql ve Command Injectıon sayfalarıdır.

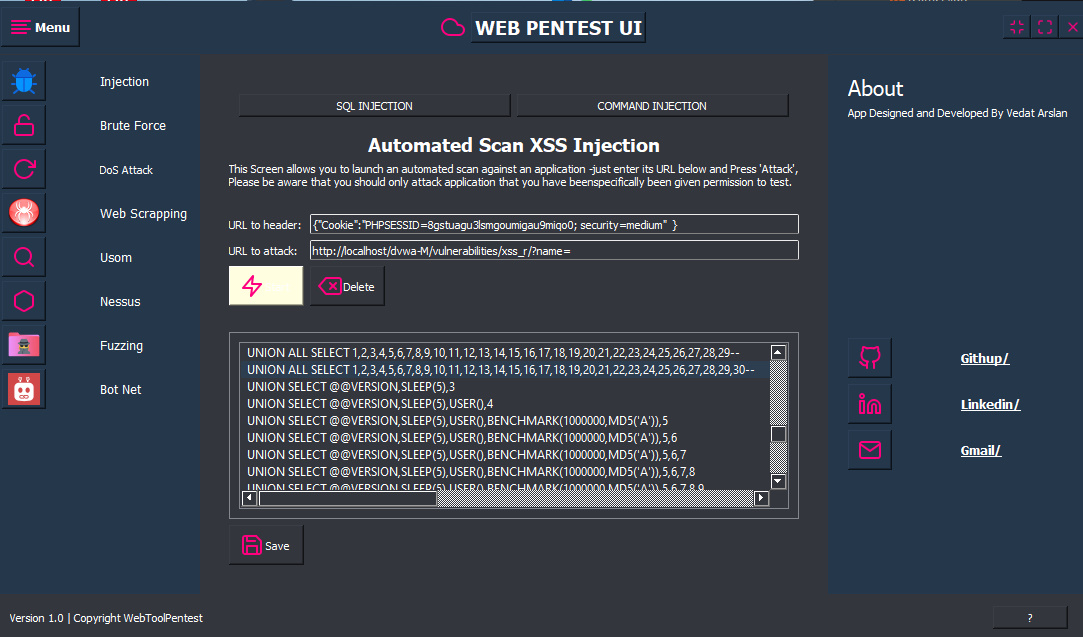
**3.1.1 XSS Injection Ekran Tasarımı**

Bu ekran DVWA uygulamasında verilen url ve cookie ile xss reflected zafiyetlerini bulur ve dosyaya kaydeder



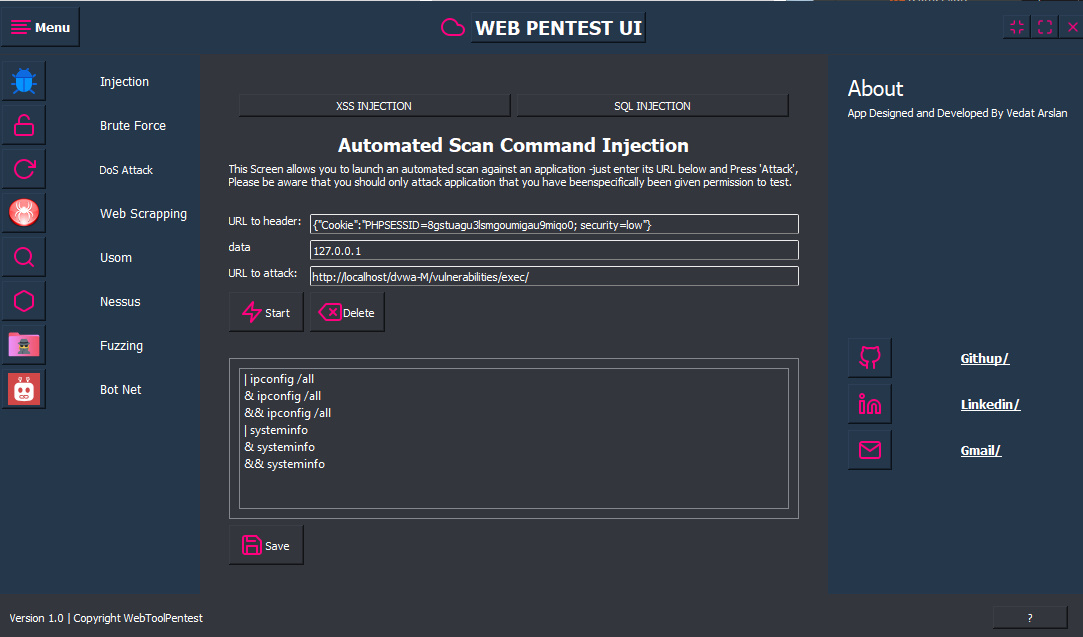
**3.2.1 Sql Injection Ekran Tasarımı**

Bu ekran DVWA uygulamasında verilen url ve cookie ile Sql injection zafiyetlerini bulur ve dosyaya kaydeder



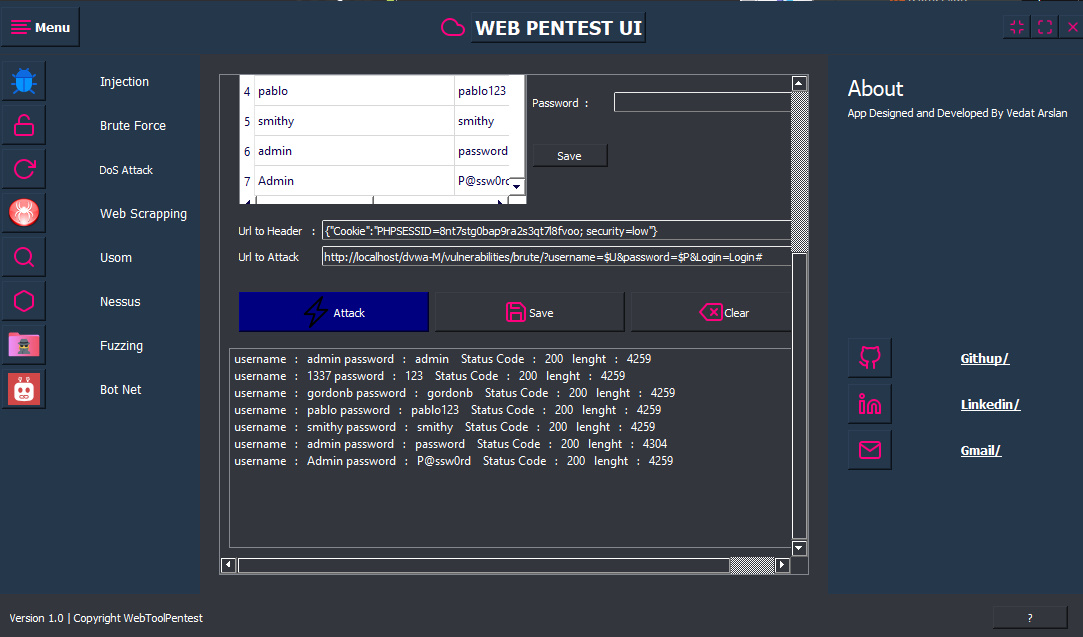
**3.2.1 Command Injection Ekran Tasarımı**

Bu ekran DVWA uygulamasında verilen url ve cookie ile command injection zafiyetlerini bulur ve dosyaya kaydeder



**3.2. Brute Force Ekran Tasarımı**

URL içinde $U ve $P öğeleri varsa, bunlar kullanıcı adı ve parola ile değiştirilir. Sonra, requests kütüphanesi kullanılarak bir HTTP isteği yapılır dönen değerin uzunluğuna bakarak kullanıcın parolası ve şifresi brute force saldırı yöntemi ile kırılır.

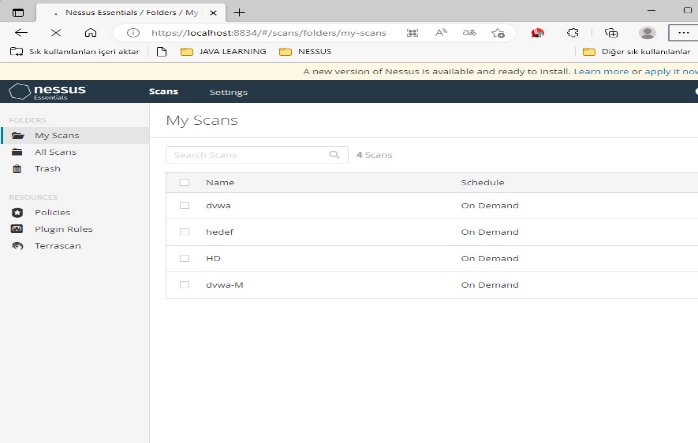
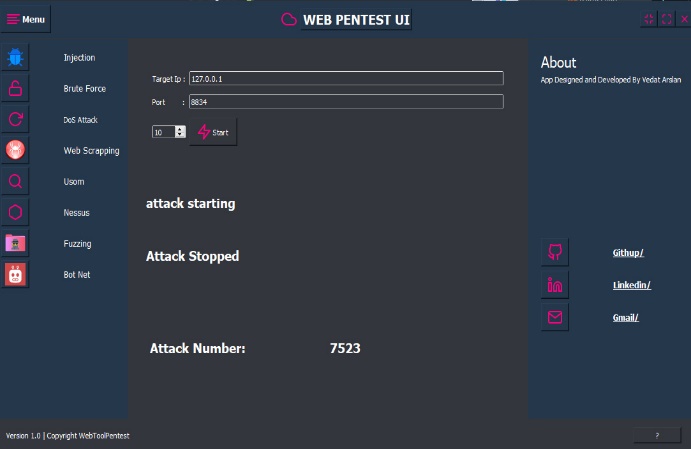
****

**3.3. DoS(Denial of Service) Attack Ekran Tasarımı**

Tek bir cihaz kullanılarak ,hedef sunucuya çok sayıda bağlantı talebi gönderilerek kaynakların tüketilmesi sağlanmıştır. Ayrıca isteği bekletip yollaması sunucunun yükünü hafifletir ve DoS attack saldırısını daha performanslı hale getirir.

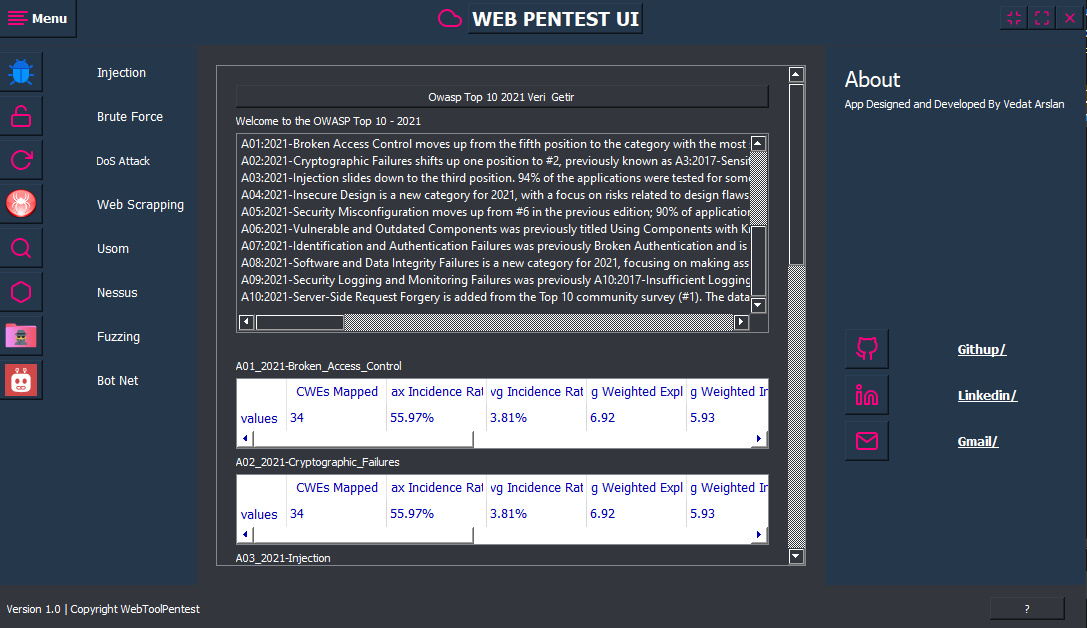
DoS saldırısını belirli zaman aralıklarında gerçekleştirecek şekilde ayarladım.

127.0.0.1 localhost ip adresim 8834 açık olan portum amaç Nessus belirli bir süre boyunca ağ dışı bırakmak.

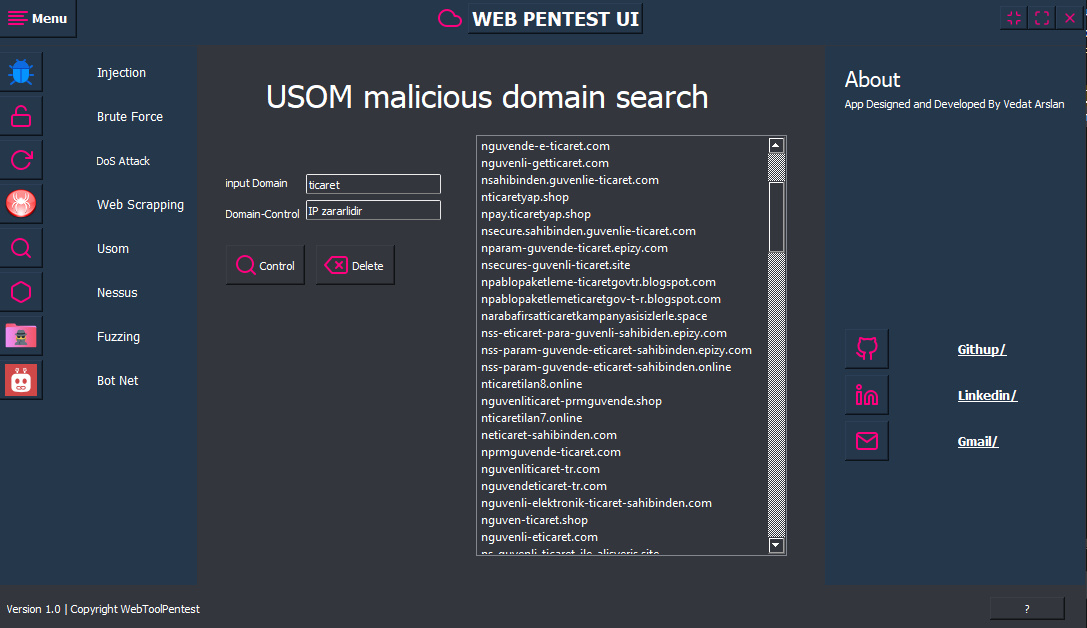


**3.4. OWASP TOP 10 Ekran Tasarımı**

OWASP TOP 10 internet sayfasından en son güncel olan,en çok yaşananan 10 zafiyeti ve bu zafiyetlerin factorlerini listeyen sayfa.

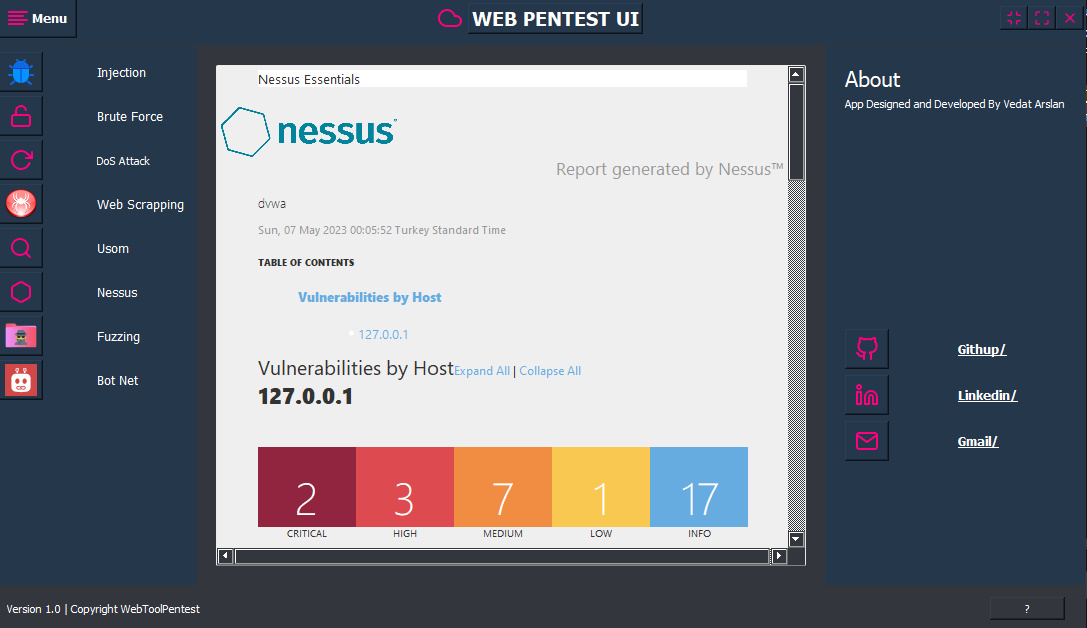
****

**3.5 Usom(Ulusal Siber Olay Müdahale) Ekran Tasarımı**

Eposta yoluyla veya farklı yollarda şüpheli domainlerin usom’un apisinden yararlanarak girilen domain ile ilgili zararlı bir domain varsa göster.

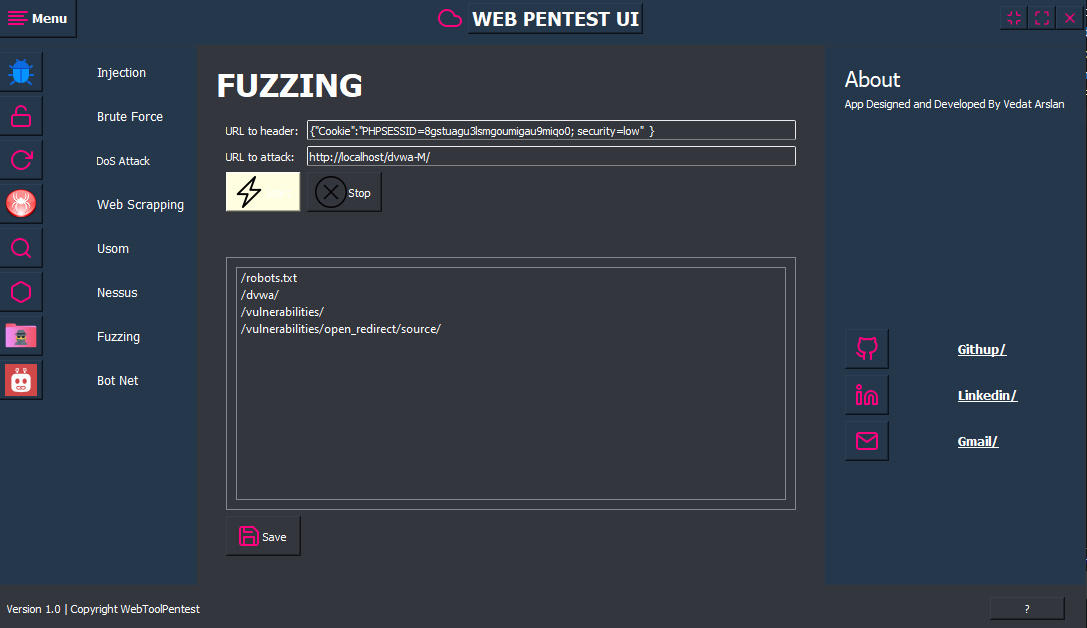
**3.6 Nessus Report Ekran Tasarımı**

Nessus taradığım zararlı web sitesinin raporunu gösteren sayfa



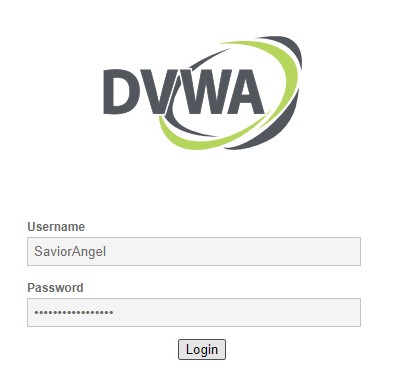
**3.7 Fuzzing Ekran Tasarımı**

Bir web sitesinin veya uygulamanın bir web dizindeki zayıf veya hatalı yapılandırılmalarından kaynaklanan güvenlik açığını tespit ve dizinleri kaydet.



**3.8 Bot Net Ekran Tasarımı**

Selenium WebDriver kütüphanesini kullanarak bir web tarayıcısını otomatikleştirerek verilen kullanıcı adı ve paroları okuyarak brute force saldırısıyla giriş yapmaya çalışır.

**metin içeren bir resim

Açıklama otomatik olarak oluşturuldu**