

Guv yaz hafta 12 lab 2 Bandit Statik Kod Analizi

1. YARIŞMA METNİ

Kod: https://github.com/doganalci/gtu_sgmyo_Sgm207_hafta12_lab2.git

1.1. Senaryo – “Gizli Zafiyet Avı”

Bu projede, hayali bir firmanın geliştirdiği ileri seviye bir Python uygulamasını inceleyeceksiniz. Uygulama:

- Dinamik modül yükleme,
- Eklenti (plugin) çalışma mantığı,
- Serileştirme (serialization),
- Kriptografik fonksiyonlar,
- Komut satırı çağrılar

içeriyor. Kodlar **bilinçli olarak karmaşık** ve **obfuske** edilmiştir.

Göreviniz, **sadece Bandit aracı kullanarak** bu kodlardaki **en az 10 güvenlik zafiyetini** tespit etmektir.

1.2. Proje yapısı (öğrenciye verilecek)

```
advanced_static_analysis/  
├── core/  
│   ├── loader.py  
│   ├── engine.py  
│   ├── hidden_ops.py  
│   └── crypto_tool.py  
├── data/  
│   └── _secrets_internal.dat    # İçeriği öğrenciler için önemli değil,  
sadece pickle test verisi  
├── plugins/  
│   └── plugin_exec.py  
└── main.py
```

1.3. Görevler

1. Bandit'i çalıştırın.

Proje kök dizininde:

2. Bandit raporunu inceleyin.

- En kritik gördüğünüz **10 zafiyeti** seçin.
- Her zafiyet için:
 - Dosya adı ve yaklaşık satır numarası
 - Bandit kural kodu (ör. B301, B602, B307...)
 - Zafiyetin türü (ör. “pickle ile güvensiz deserialize”, “shell=True ile komut enjeksiyonu”, “zayıf hash (MD5)”)
 - Kısa açıklama: “Bu neden tehlikeli?”

3. Rapor oluşturun (PDF veya .md).

Her bir zafiyet için aşağıdaki formatı kullanın:

Zafiyet #1

- Dosya: ...
 - Bandit Kodu: B...
 - Tür: ...
 - Açıklama: ...
 - Örnek saldırı senaryosu (kısa): ...
4. (İsteğe bağlı) **Ek puan – Manuel analiz**
- Bandit’e ek olarak, kendi manuel incelemenizle **ek bir güvenlik riski** fark ederseniz, bunu da rapora ekleyebilirsiniz (örneğin tasarım seviyesinde riskler).

1.4. Değerlendirme Önerisi (puanlama)

- Bandit çıktısını doğru kullanma: **20 puan**
- En az 10 zafiyeti doğru tespit etme: **50 puan**
- Açıklamaların doğruluğu ve teknik derinlik: **20 puan**
- Raporun düzeni ve okunabilirliği: **10 puan**

Toplam: **100 puan**