**🧠 1. PPMap Nedir?**

**PPMap**, web uygulamalarında **JavaScript nesnelerinin prototiplerine izinsiz müdahale edilmesi** sonucu oluşan **Prototype Pollution** zafiyetlerini otomatik olarak tespit eden bir araçtır.

* HTTP parametreleri üzerinden prototip manipülasyonu testleri yapar
* Çeşitli payload kombinasyonlarını dener
* Potansiyel istismar yollarını gösterir

📌 Prototype Pollution, özellikle **Node.js, JavaScript tabanlı API’ler** ve istemci tarafı JS kütüphanelerinde görülür.

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🔍 Prototype Pollution taraması | Otomatik parametre testleri |
| 🛠️ Payload üretimi | Farklı prototip manipülasyon teknikleri |
| 📊 Zafiyet raporu | Etki derecesi ve istismar potansiyeli |
| 🌐 GET/POST destekleri | HTTP istekleri üzerinden test |

**⚙️ 3. Kurulum (Kali / Linux)**

**✅ 1. GitHub’dan indirme:**

metin, ekran görüntüsü, yazı tipi, grafik içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**✅ 2. Python bağımlılıklarını yükleme:**

metin, ekran görüntüsü, yazı tipi, grafik içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Python 3.x önerilir.

**🚀 4. Kullanım Komutları**

**✅ 1. Tek hedef URL taraması:**

python3 ppmap.py -u "https://example.com/api"

**✅ 2. GET parametre testi:**

python3 ppmap.py -u "https://example.com/api?param=value"

**✅ 3. POST parametre testi:**

python3 ppmap.py -u "https://example.com/api" -d "param=value"

**✅ 4. Hedef listesi ile toplu tarama:**

python3 ppmap.py -l targets.txt

**📋 5. Örnek Terminal Çıktısı**

**metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**🧠 6. Prototype Pollution Nedir?**

Prototype Pollution, JavaScript nesnelerinin **Object.prototype** gibi temel prototiplerine zararlı verilerin enjekte edilmesiyle oluşur.

* Bu, tüm nesneleri etkileyebilir
* XSS, RCE veya veri manipülasyonu gibi zincir saldırılara yol açabilir

**🧪 7. Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🔍 Web API güvenlik testi | Parametre bazlı zafiyet taraması |
| 🧠 Red Team saldırı keşfi | JS nesne manipülasyonu ile istismar hazırlığı |
| 🛡️ Blue Team güvenlik denetimi | Prototip kirliliği önleme testleri |
| 🧪 Eğitim ortamı | JS güvenlik açıklarının öğrenilmesi |

**🎯 7. Öğrenim Kazanımları**

* Prototype Pollution zafiyet mantığını kavrama
* HTTP parametreleri üzerinden JS manipülasyonu yapma tekniklerini öğrenme
* Python tabanlı güvenlik tarayıcılarının çalışma mantığını anlama
* Web uygulamalarında API güvenlik testlerini uygulamalı öğrenme