# GitHub: Zafiyet POC ve OSINT Araçları Açısından Önemi



## GitHub Nedir?

GitHub, geliştiricilerin yazılım projelerini depolamak, paylaşmak ve iş birliği yapmak için kullandığı en büyük açık kaynak platformlarından biridir. Microsoft tarafından satın alınan bu platform, yazılım geliştiricilerinin hem bireysel hem de ekip çalışmaları yürütebildiği bir sürüm kontrol sistemidir (Git tabanlıdır).

## Zafiyet POC (Proof of Concept) Açısından GitHub

- Güvenlik araştırmacıları bir zafiyet keşfettiklerinde bu zafiyetin çalıştığını göstermek amacıyla POC (Proof of Concept) kodlarını yayınlarlar.  
- GitHub, bu tür POC kodlarının paylaşıldığı en yaygın platformlardan biridir.  
- Yeni çıkan zafiyetlerin test edilmesi ve doğrulanması için birçok araştırmacı doğrudan GitHub aramalarını kullanır.  
- Örnek POC içerikleri:  
 • CVE bazlı zafiyet scriptleri  
 • Metasploit modülleri  
 • Python, Go veya Bash scriptleri

## OSINT (Open Source Intelligence) Araçları Açısından GitHub

- Açık kaynak istihbarat (OSINT), halka açık kaynaklardan bilgi toplama sürecidir.  
- OSINT araçlarının büyük bir bölümü GitHub üzerinde barındırılmaktadır.  
- Pentester’lar, Red Team üyeleri ve siber güvenlik meraklıları bu araçları GitHub üzerinden indirerek testler yapabilir.  
- Öne çıkan OSINT araçları:  
 • theHarvester  
 • Photon  
 • Recon-ng  
 • SpiderFoot  
 • Email2phonenumber

## GitHub’da Arama Örnekleri

- CVE-2024 exploit → Belirli bir zafiyetin PoC dosyalarını aramak için  
- OSINT tool → Yeni keşfedilen açık kaynaklı bilgi toplama araçlarını bulmak için  
- bug bounty recon → Zafiyet avcılarının kullandığı pasif ve aktif keşif araçları için

## Sonuç

GitHub, hem zafiyetlerin test edilmesi hem de açık kaynak istihbarat araçlarının keşfi ve geliştirilmesi açısından vazgeçilmez bir platformdur. Güvenlik araştırmacıları ve etik hackerlar için bilgi hazinesi niteliğindedir.