XSStrike - XSS Tespit ve Exploit Aracı

# 📌 XSStrike Nedir?

XSStrike, gelişmiş bir XSS tespit ve exploit aracıdır. Hem Reflected hem de DOM tabanlı XSS açıklarını tespit etmek için Python ile yazılmış açık kaynaklı bir çözümdür. Zararlı script yerleştirme açıklarını düşük false-positive oranı ile yakalayabilir.

# 🚀 Temel Özellikler

- Reflected ve DOM tabanlı XSS tespiti

- Context-aware payload üretimi

- Web crawler ile URL keşfi

- Fuzzer ile parametrik testler

- Blind XSS, WAF bypass ve payload özelleştirme seçenekleri

# 🛠️ Kurulum

XSStrike aracını kurmak için aşağıdaki adımları takip edebilirsiniz:

git clone https://github.com/s0md3v/XSStrike.git  
cd XSStrike  
pip install -r requirements.txt

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

# 🔧 Kullanım Örnekleri

Yardım menüsünü görüntülemek için:

python3 xsstrike.py -h

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Temel kullanım örneği:

python3 xsstrike.py -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --crawl –fuzzer



# 💻 Örnek Terminal Çıktısı

# metin, ekran görüntüsü, yazı tipi içeren bir resim Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.📎 Sonuç

XSStrike, penetration testlerinde XSS tespiti için oldukça güçlü ve esnek bir araçtır. Yüksek doğruluk oranı, özel payload üretimi ve bypass teknikleri ile diğer geleneksel XSS araçlarından ayrılır.