**5. HTTP REQUEST SMUGGLER 📦**

**Aracın Ne İşe Yaradığı ve Amacı 🎯**

HTTP request smuggler, HTTP request smuggling adı verilen kritik güvenlik açıklarını tespit etmek ve test etmek amacıyla geliştirilmiş özel siber güvenlik araçlarıdır. Front-end ve back-end sunucular arasındaki HTTP parsing tutarsızlıklarını tespit eder.

**Kullanım Alanları 🛠**

💻 Web Proxy/Load Balancer Testing:

• Reverse proxy yapılandırma hatalarının testi

• CDN ve load balancer güvenlik kontrollerinin bypass edilmesi

• Cache poisoning saldırı vektörlerinin testi

🛡 Penetrasyon Testi Senaryoları:

• Yetki kontrollerinin bypass edilmesi

• Session hijacking testleri

• Cross-site scripting payload'larının gizlenmesi

**Ana Araçlar ve Geliştiriciler 👨‍💻**

🔹 PortSwigger HTTP Request Smuggler:

• Geliştirici: PortSwigger (James Kettle öncülüğünde)

• Platform: Burp Suite Extension

• GitHub: <https://github.com/PortSwigger/http-request-smuggler>

🔹 Smuggler (defparam):

• Geliştirici: @defparam

• Platform: Standalone Python 3 aracı

• GitHub: <https://github.com/defparam/smuggler>

**Teknik Özellikler ⚡**

📍 Detection Teknikleri:

• CL.TE Detection: Content-Length / Transfer-Encoding çakışması

• TE.CL Detection: Transfer-Encoding / Content-Length çakışması

• TE.TE Detection: Obfuscated Transfer-Encoding

**Kurulum Adımları 🖥**

💾 PortSwigger Extension:

1. Burp Suite'i açın

2. Extender → BApp Store → 'HTTP Request Smuggler' ara ve yükle

💾 Defparam Smuggler:

git clone <https://github.com/defparam/smuggler.git>



cd smuggler



python3 smuggler.py -h



**Kullanım Örnekleri 📂**

# Defparam smuggler - tek host test  
python3 smuggler.py -u [https://target.com](https://target.com/)  
  
# Çoklu host test  
cat hosts.txt | python3 smuggler.py  
  
# Gelişmiş parametreler  
python3 smuggler.py -u [https://target.com](https://target.com/) -v custom-vhost.com -m POST -t 10

**Avantajlar ve Dezavantajlar 📊**

✅ Avantajlar:

• Yüksek kritik vulnerability'leri tespit eder

• Otomatik scanning

• Burp Suite entegrasyonu

• Ücretsiz ve açık kaynak

⚠️ Dezavantajlar:

• False positive riski

• Server poisoning potansiyeli

• Teknik uzmanlık gereksinimi

• Hedef sistem üzerinde potential disruption

**GitHub Bilgileri 📎**

• PortSwigger Repository: <https://github.com/PortSwigger/http-request-smuggler>

• Defparam Repository: <https://github.com/defparam/smuggler>

• Community: 1000+ stars (PortSwigger), 800+ stars (defparam)