**4. WAF EVASION (SQLMAP TAMPER SCRIPT KOLEKSIYONU) 🛡**

**Aracın Ne İşe Yaradığı ve Amacı 🎯**

SQLMap Tamper Scripts, Web Application Firewall (WAF) bypass teknikleri için kullanılan SQL injection payload dönüştürme scriptleridir. SQL injection payload'larını WAF imzalarından kaçınacak şekilde modifiye eder ve çeşitli encoding/obfuscation teknikleri kullanarak güvenlik filtrelerini atlatır.

**Kullanım Alanları 🛠**

📍 Primer Kullanım Alanları:

• SQL Injection Testing

• WAF Testing ve etkinlik değerlendirmesi

• Penetration Testing

• Red Team Exercises

• Security Research

**Teknik Özellikler ⚡**

📂 Popüler Tamper Scripts:

• Encoding/Obfuscation: apostrophemask.py, base64encode.py, charencode.py

• SQL Syntax Manipulation: between.py, equaltolike.py, greatest.py

• Space Replacement: space2comment.py, space2plus.py, space2hash.py

• WAF-Specific Bypasses: bluecoat.py, securesphere.py, modsecurityversioned.py

**Kurulum Adımları 🖥**

# SQLMap kurulumu  
git clone --depth 1 <https://github.com/sqlmapproject/sqlmap.git> sqlmap-dev

cd sqlmap-dev



python sqlmap.py --help



**Kullanım Örnekleri 📂**

# Tek tamper script  
python sqlmap.py -u "<http://target.com/page.php?id=1>" --tamper=space2comment  
  
# Çoklu tamper script  
python sqlmap.py -u "<http://target.com/page.php?id=1>" --tamper=space2comment,randomcase,charencode  
  
# WAF tespit etme  
sqlmap -u "<http://target.com/page.php?id=1>" --identify-waf  
  
# Advanced bypass senaryosu  
sqlmap -u "<http://target.com/app.php?id=1>" --tamper=modsecurityversioned,space2comment,charencode --technique=B --proxy=http://127.0.0.1:8080

**Avantajlar ve Dezavantajlar 📊**

✅ Avantajlar:

• Otomatik WAF bypass

• Geniş WAF desteği

• Çoklu obfuscation teknikleri

• Açık kaynak ve ücretsiz

⚠️ Dezavantajlar:

• Yasal risk (yetki olmadan kullanımı illegal)

• Performance yavaşlığı

• Modern WAF'ların tespit etme kabiliyeti

**GitHub Bilgileri 📎**

• Repository: <https://github.com/sqlmapproject/sqlmap>

• Tamper Scripts Lokasyonu: sqlmap/tamper/

• Script Sayısı: 65+

• Lisans: GPL v2