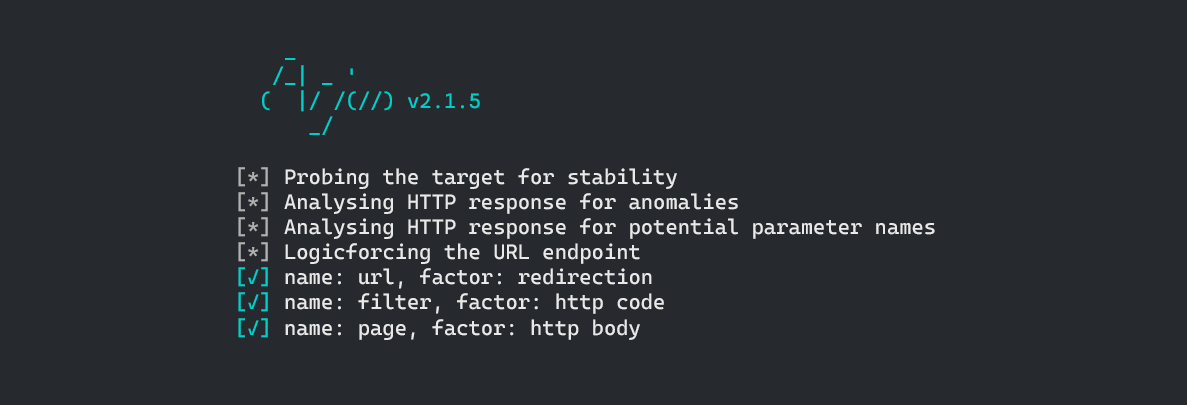
**Arjun Nedir?**

**Arjun**, bir web uygulamasında kullanılan HTTP GET ve POST parametrelerini tespit etmek için kullanılan açık kaynaklı bir araçtır. Web sayfalarının istemci tarafında görünmeyen, ancak sunucuya gönderildiğinde belirli işlemleri tetikleyebilecek parametreleri keşfetmek için kullanılır.

Bu parametreler bazen geliştiriciler tarafından bırakılmış olup, kötüye kullanıldığında XSS, SQL Injection, IDOR gibi zafiyetlere kapı aralayabilir.



**Arjun Ne İşe Yarar?**

* Hedef URL üzerinde parametre taraması yapar.
* HTTP GET ve POST isteklerine odaklanır.
* JSON, XML ve multipart içerik tiplerini analiz edebilir.
* 10.000’den fazla olası parametreyi sistematik olarak dener.
* Basit, hızlı ve düşük kaynak kullanımıyla öne çıkar.

Kurulum:

***git clone https://github.com/s0md3v/Arjun.git***

***cd Arjun***

***python3 arjun.py -h***

Ya da pip üzerinden: ***pip install arjun***

**Temel Kullanım**

1. Basit tarama (GET parametreleri):

***python3 arjun.py -u*** [***https://hedefsite.com/index.php***](https://hedefsite.com/index.php)

1. POST istekleriyle tarama:

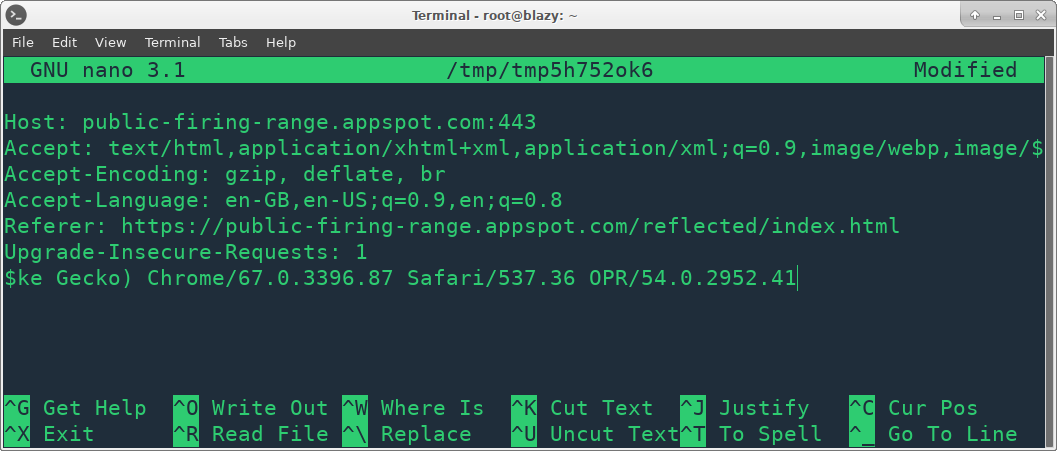
***python3 arjun.py -u https://hedefsite.com/api/login -m POST***

1. Çıktıyı bir dosyaya kaydetme:

***python3 arjun.py -u https://hedef.com -o output.txt***

1. JSON tipi içeriği kontrol etme:

***python3 arjun.py -u https://hedef.com/api -m POST --headers "Content-Type: application/json"***

******

Arjun, özellikle web uygulaması sızma testlerinde, gizlenmiş ya da belgelenmemiş API parametrelerini bulmak için büyük avantaj sağlar. Sıkça kullanılan parametreleri sistematik olarak deneyerek web sunucusunun verdiği yanıtları analiz eder ve potansiyel olarak etkileşimli parametreleri belirler.

Birçok pentester, Arjun’u Burp Suite, FFUF veya ParamSpider gibi araçlarla birlikte kullanarak zafiyet zinciri kurar. Örneğin; Arjun ile bulunan bir parametre, SQLmap ile test edilerek SQL Injection var mı diye kontrol edilebilir.

* Arjun, öğrencilerin gizli saldırı yüzeylerini keşfetmesini öğretmek için ideal bir araçtır.
* Web sitelerinde sadece görünen değil, görünmeyen yapılarla da etkileşim kurulabileceğini gösterir.
* Düşük kaynak kullanımıyla her seviyeden kullanıcıya hitap eder.
* CTF yarışmalarında sıkça kullanılır.