

**ParamSpider**, web uygulamalarındaki **URL parametrelerini** keşfetmeye yarayan açık kaynaklı bir bilgi toplama (OSINT) aracıdır. Amacı, hedef domain üzerindeki çeşitli URL’lerde kullanılan parametre isimlerini otomatik olarak toplamak ve güvenlik testlerinde (örneğin, web güvenlik testleri, penetrasyon testleri) kullanılacak parametre listeleri oluşturmaktır.

Bu parametreler, web uygulamalarında form verileri, sorgu dizileri (query strings) veya dinamik sayfalarda kullanılan değişkenler olabilir. ParamSpider, URL parametrelerini bulmak için hem çeşitli **arama motorları** (Google, Bing, Baidu, DuckDuckGo vb.) hem de **CT (Certificate Transparency) logları** gibi farklı kaynakları kullanarak hedef domain üzerinde parametre örnekleri toplar.

**ParamSpider'ın Özellikleri**

* Çok sayıda arama motorundan parametre keşfi yapabilir.
* Hedef domain üzerindeki URL parametrelerini hızlıca listeleyebilir.
* Parametre listesi oluşturup, güvenlik testlerinde (örneğin SQL Injection, XSS testi) kullanılacak parametreleri sağlar.
* Basit, komut satırı (CLI) aracı, kolay kullanım.
* Python ile yazılmış, açık kaynak.

## ParamSpider Nasıl Çalışır?

1. Hedef domain ismi verilir.
2. Araç, arama motorları ve CT loglarından URL örnekleri toplar.
3. Bu URL'lerdeki parametre isimlerini ayrıştırır.
4. Sonuç olarak parametrelerin eşsiz listesini verir.

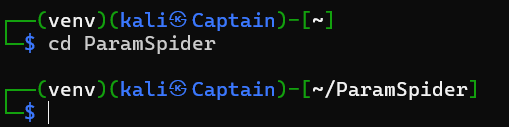
## Kurulum ve Basit Kullanım Örneği

**Kurulum (Linux / Kali gibi sistemlerde):**

*git clone* [*https://github.com/devanshbatham/ParamSpider.git*](https://github.com/devanshbatham/ParamSpider.git)

****

*cd ParamSpider*

**

*pip3 install -r requirements.txt*

*paramspider -d example.com -e '127.0.0.1:8080' -p php,aspx –proxy*

### Açıklama:

* -d example.com : Hedef domain.
* -e '127.0.0.1:8080' : Proxy adresi (örneğin lokal proxy).
* -p php,aspx : Sadece .php ve .aspx uzantılı URL’leri filtrele.
* -proxy : Proxy kullanarak istek gönder.

