Xspear Nedir?

Xspear, Ruby dili ile yazılmış, web uygulamalarında XSS (Cross Site Scripting) açıklarını tespit etmeye yarayan bir güvenlik aracıdır.

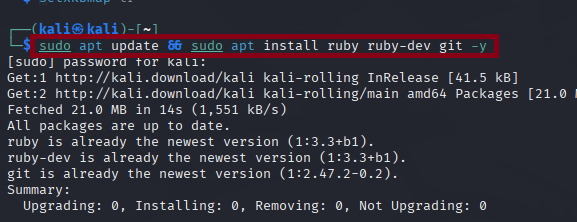
Gelişmiş filtre bypass, parametre analizi, JSON ve Header taraması gibi birçok özelliği destekler.

XSpear’in Temel Özellikleri

* Otomatik XSS taraması: GET ve POST parametrelerini analiz eder.
* Akıllı payload üretimi: Farklı filtreleme mekanizmalarını aşmak için özel payload’lar oluşturur.
* Raporlama: JSON formatında çıktı verir, eğitimde analiz için kullanılabilir.
* Proxy desteği: Burp Suite gibi araçlarla birlikte çalışabilir.
* Reflected ve Stored XSS testleri: Hem yansıyan hem de kalıcı XSS açıklarını test edebilir.

Adım 1: Ruby ve Git'i Kur

sudo apt update && sudo apt install ruby ruby-dev git -y

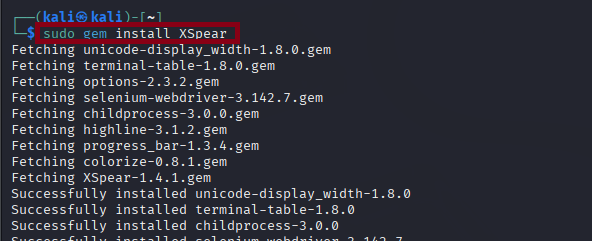


Şekil - Ruby ve Git’in apt ile kurulumu

Bu komut sistemi günceller ve Xspear için gerekli Ruby ortamını kurar.

Adım 2: Xspear Aracını Kur

sudo gem install XSpear



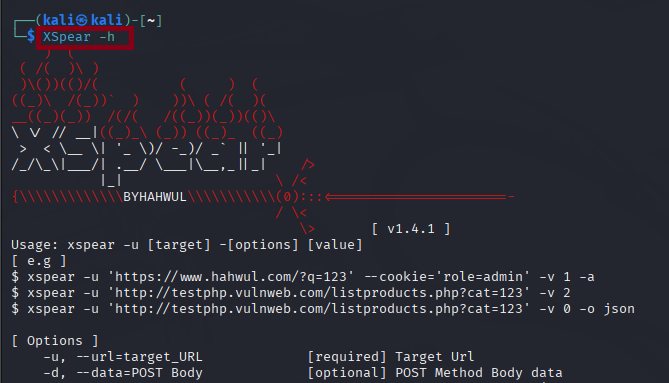
Şekil -sudo gem install xspear komutuyla Xspear’in kurulması

Bu komut Xspear’i Ruby gem deposundan indirir ve sistem geneline kurar.

İşlem tamamlandığında XSpear komutu her yerden erişilebilir olur.

Adım 3: Kurulumu Doğrula

XSpear -h

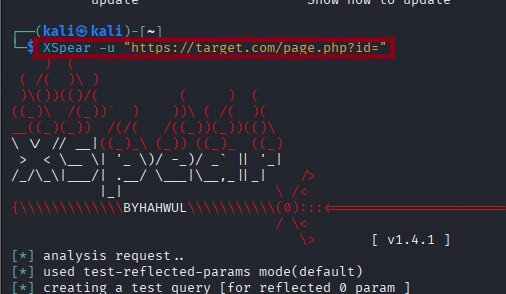


Şekil - XSpear -h komutuyla kurulumun doğrulanması

KULLANIMI

Tek URL ile Temel Tarama

XSpear -u "https://target.com/page.php?id=1"



Şekil - Tek URL taraması komutu

ETİK KULLANIM UYARISI

Xspear aracı yalnızca:

* Size ait sistemlerde
* Eğitim, CTF ve laboratuvar ortamlarında
* Yazılı izin alınmış hedeflerde

kullanılmalıdır. Aksi takdirde yasal sonuçlar doğurabilir.