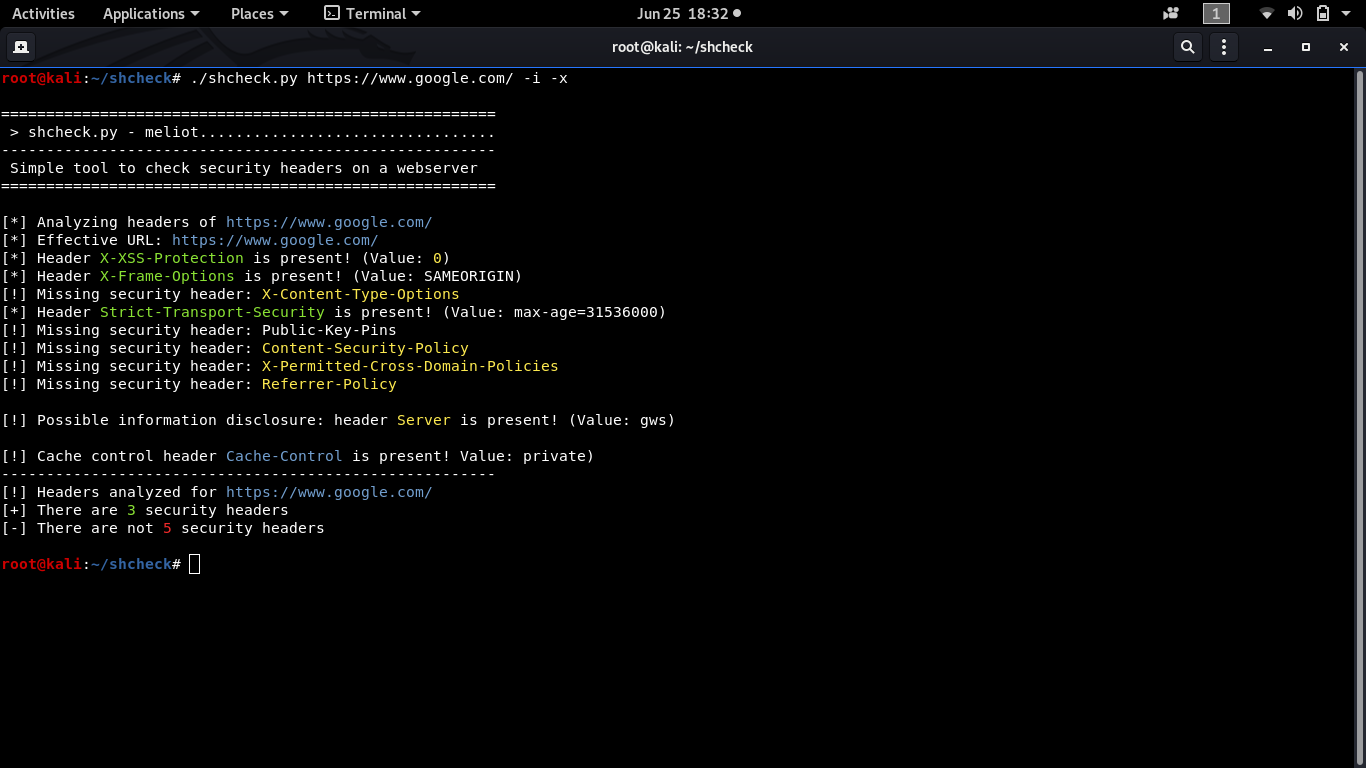
**Shcheck Nedir?**

Shcheck, Linux ve Unix tabanlı sistemlerde güvenlik açıkları ve yanlış yapılandırmaları otomatik olarak tespit etmek için kullanılan bir güvenlik kontrol aracıdır. Sistem üzerinde temel zafiyetleri, kötü izinleri ve potansiyel güvenlik risklerini hızlıca bulmak için tasarlanmıştır.

Özellikle sistem yöneticileri ve güvenlik uzmanları için, hızlı ve kolay bir şekilde sistem sağlığını kontrol etmek adına çok faydalıdır.



**Shcheck Ne İşe Yarar?**

* Dosya ve dizin izinlerini kontrol eder.
* SSH konfigürasyon dosyalarını inceleyerek riskli ayarları bulur.
* Sistem kullanıcılarını analiz eder.
* Potansiyel güvenlik açıklarını ve uyumsuzlukları raporlar.
* Rootkit ya da kötü amaçlı yazılım varlığına dair ön bilgiler sunabilir.

**Kurulum ve Kullanım:**

Genellikle Python ile çalışır ve kurulumu oldukça basittir.

***git clone https://github.com/RafalWilinski/shcheck.git***

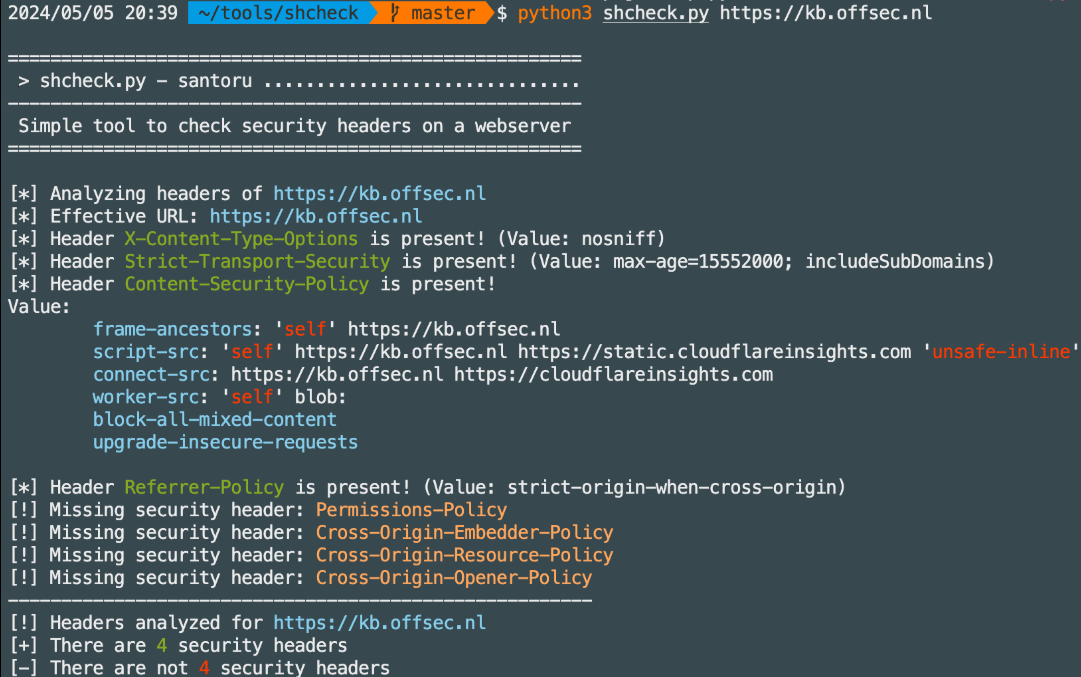
***cd shcheck***

***python3 shcheck.py***

**Kullanımı:**

Çalıştırdığınızda sistem üzerinde otomatik kontroller başlar ve tespit edilen güvenlik sorunları raporlanır.  
Örneğin:

* SSH izinlerinin açık olup olmadığı
* Sistem dosyalarının sahiplik ve izin sorunları
* Riskli kullanıcı hesapları

******

**Eğitim Notları**

Shcheck, öğrencilerin sistem güvenliği temel bilgilerini öğrenirken, gerçek zamanlı olarak sistemlerini kontrol edebilecekleri pratik bir araçtır. Linux sunucularında sık yapılan hatalar ve yanlış yapılandırmalar bu araç sayesinde kolayca tespit edilir. Böylece sistemlerin daha güvenli hale getirilmesi için gerekli adımlar atılabilir.

Shcheck, sistem üzerinde sadece yüzeysel bir kontrol yapmakla kalmaz, aynı zamanda özelleştirilebilir bir yapı sunar. İstenirse sadece belirli alanlara odaklanarak tarama yapılabilir (örneğin sadece SSH ayarlarını kontrol etmek gibi). Bu özelliği sayesinde hızlı güvenlik denetimleri yapmak isteyen sistem yöneticileri için idealdir.

Ayrıca Shcheck'in sunduğu çıktılar oldukça anlaşılır ve renkli olduğu için, öğrenciler hataları ve uyarıları kolayca fark edebilir. Bu, siber güvenlik eğitimi sırasında öğrencilerin sistem yapılandırmalarını analiz etmeyi öğrenmeleri açısından önemli bir avantaj sağlar.

Shcheck'in kontrolleri şunları da kapsar:

* /etc/passwd ve /etc/shadow gibi kritik dosyaların izinleri
* Yetkisiz kullanıcı hesaplarının tespiti
* Root kullanıcısı dışındaki hesapların UID 0 sahibi olup olmadığının kontrolü
* SSH root login gibi zayıf yapılandırmaların uyarılması

Ek olarak;

* **Renkli çıktılar**, öğrencilerin zayıf yapılandırmaları hızlı fark etmesini sağlar.
* “Kırmızı” olarak işaretlenen eksik güvenlik başlıkları, örneğin X-Frame-Options yoksa → **clickjacking**, Content-Security-Policy eksikse → **XSS** gibi zafiyetlere işaret eder.
* Shcheck’in düşük bağımlılıkla çalışması, onu Kali gibi ortamlarda basit ve hızlı bir araç haline getirir.