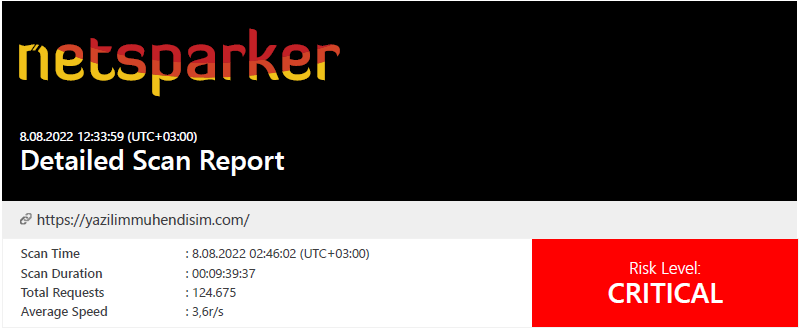
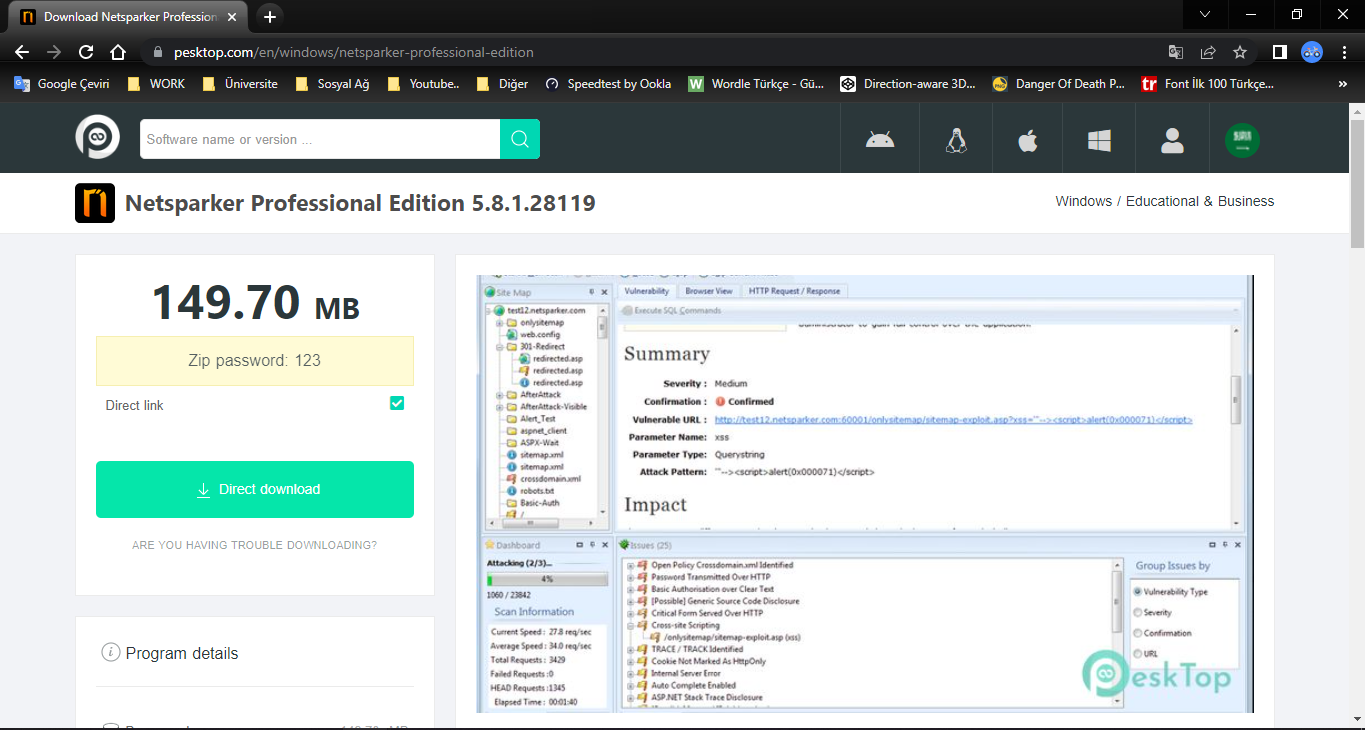
**NETSPARKER :**



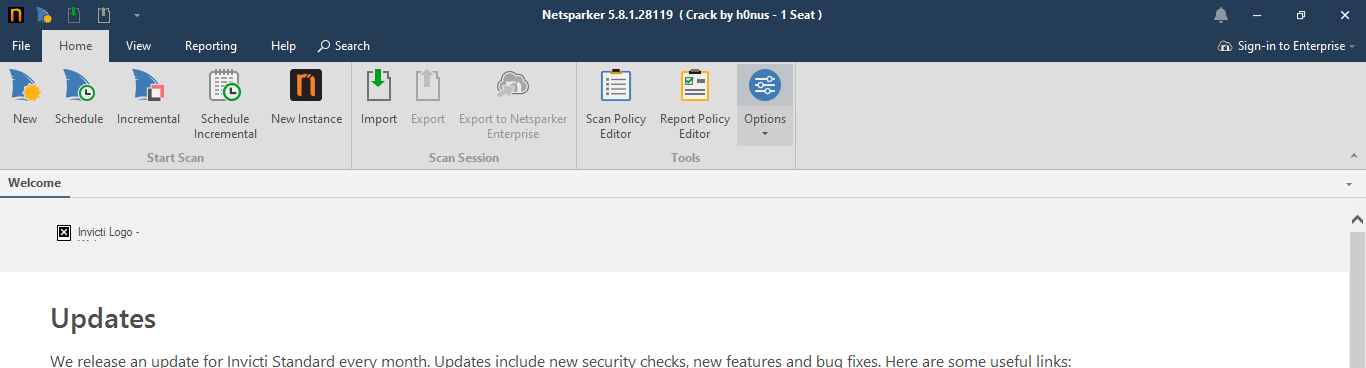
Web uygulamarınıza tıpkı kötü niyetli bir hacker gibi saldırıp web uygulamalarınızdaki zafiyetleri size toparlayan bir uygulama tarayıcısıdır.

NetSparker cross-site scripting (xss) SQL injection gibi popüler zafiyetleri hiç zorlanmadan size raporlayabilir. Hatta bunları yaparken hiçbir rakibinin yapamadığı ekstra bir şeyi de yapar size bu zafiyetlerden yola çıkarak sisteminizde dışarıya aktarılabilecek önemli bir veri varsa onları dışarı aktarıp size sunar.

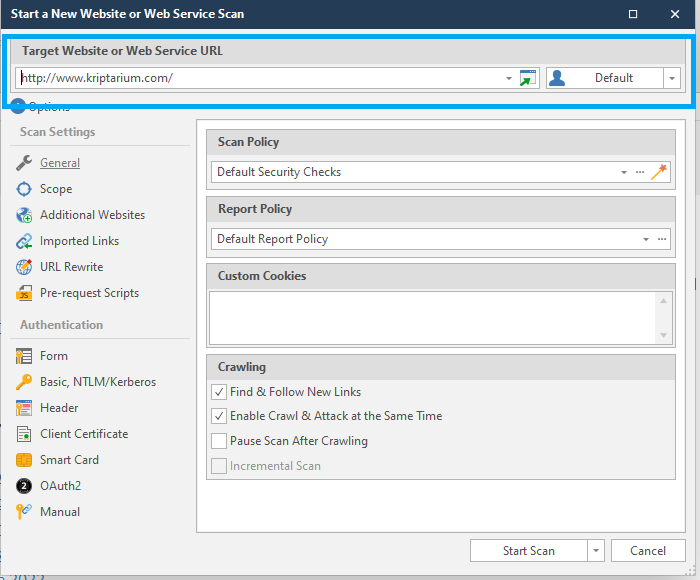
<https://pesktop.com/en/windows/netsparker-professional-edition>



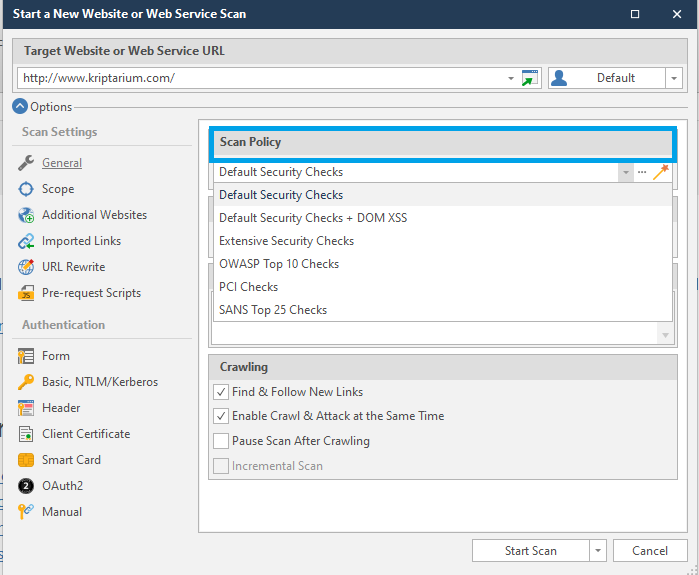
Yukardaki link e tıklayaralk NetSparker web uygulamamızı indiriyoruz. Zip dosyası içerisinde kurulu gelen uygulamayı açıyoruz.



New butonuna tıklıyoruz



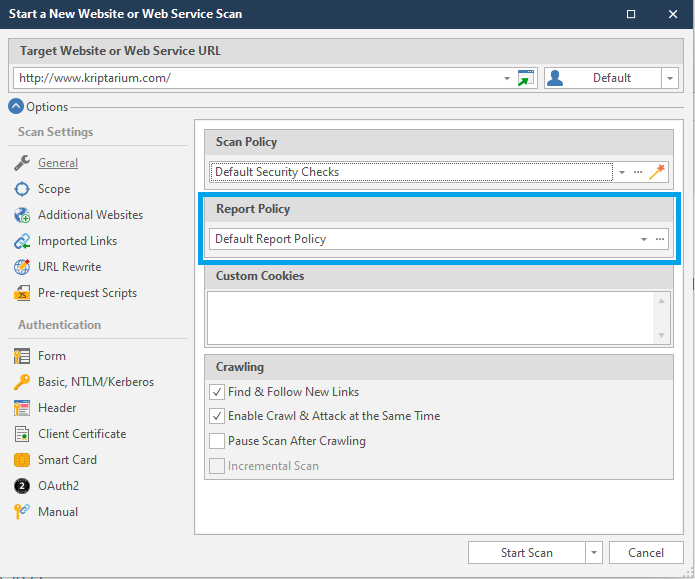
Tarama yapılacak adresi yukardaki işaretli alana yazıyoruz.



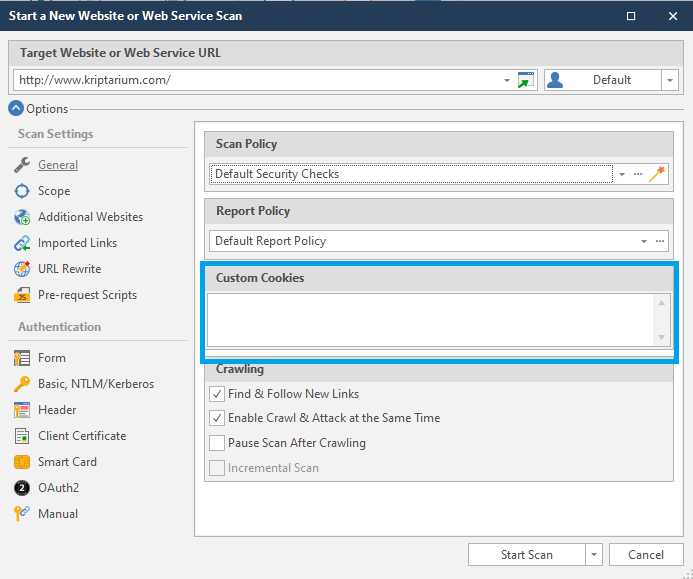
Hangi güvenlik zafiyetlerini aramasını istediğimiz ayarı seçiyoruz.

Sadece belirli zafiyet gruplarına karşı tarama yapabileceğimiz gibi kapsamlı olarak da tüm testlerin yapılmasını isteyebiliriz.

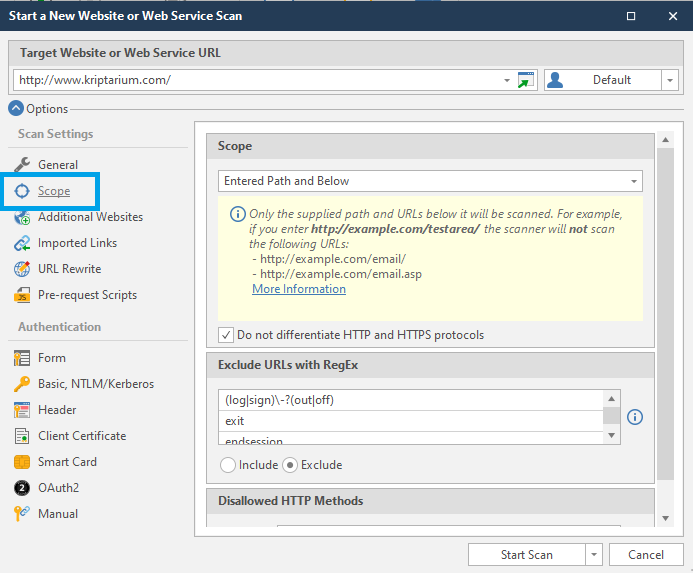
,



Özel bir raporlama formatı hazırladıysanız o formata raporlama yapması gerektiğini NetSparker a işaretli bölgeden bildiriyoruz.



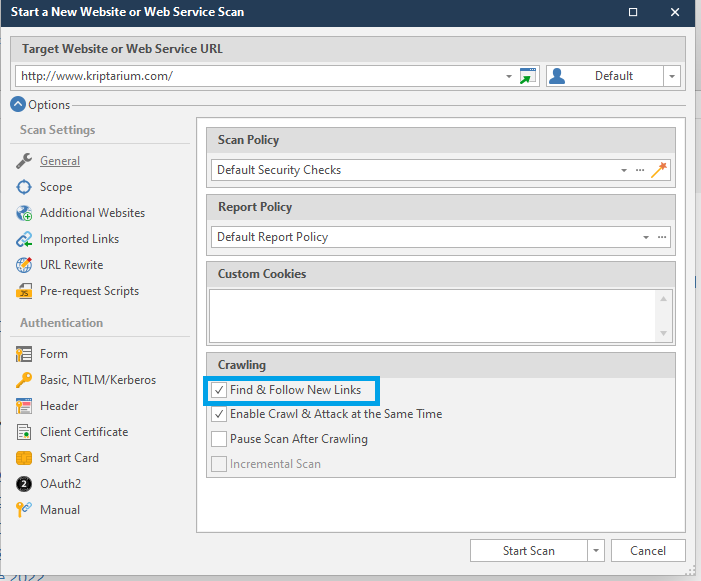
Kullanmamız gereken bir costum cookie varsa işaretli alanda da onu belirtiyoruz.



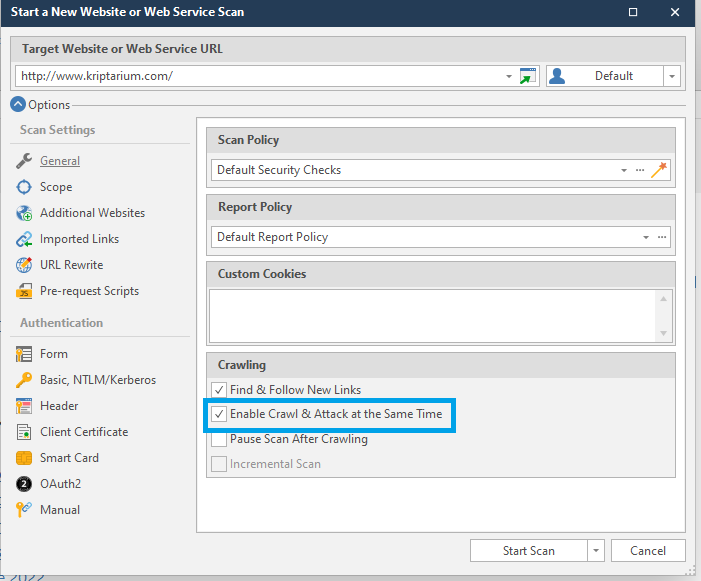
Bu kısımda tarama dışında tutmak istediğiniz veya özel olarak dahil etmek istediğimiz sayfa adreslerini varsa eğer bu kısımda belirtebiliyoruz.

NetSparker varsayılan olarak bazı oturum sonlandırma sayfalarını tarama dışında tutuyor.

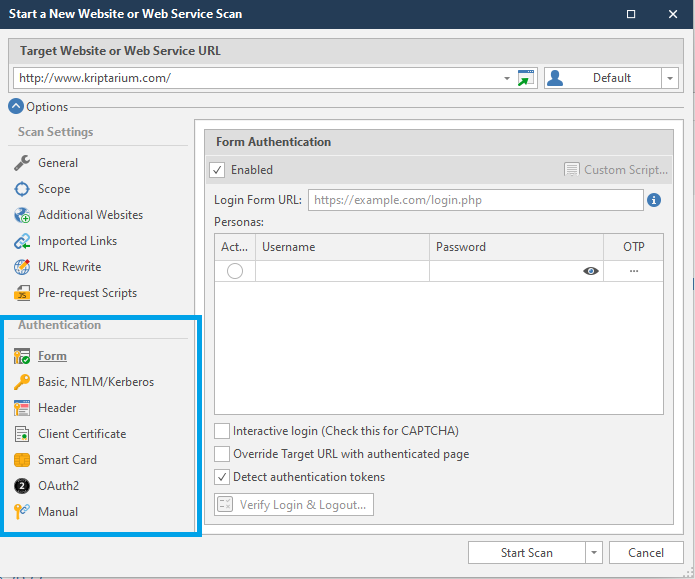
Ayrıca 404 hata sayfaları ve anti csrf korumalarında otomatik olarak tanımlıyor.



Bulunan bağlantıları ve onların alt dizinlerinin takip edilerek taranma işlemi varsayılan olarak seçilidir.



Hem dizi ve dosyaların keşfedilmesi hem de güvenlik açıkları denetimlerinin aynı anda yapılması da varsayılan olarak seçilidir.



Taramak istediğimiz web uygulamasında eğer bir kimlik doğrulama bilgisine sahip iseniz bu işaretli kısımda tanımlama yapabiliriz.

Böylece hedef web uygulamasında kimlik doğrulaması olmadan erişilmeyen sayfalarda da zafiyet taraması yapabiliriz

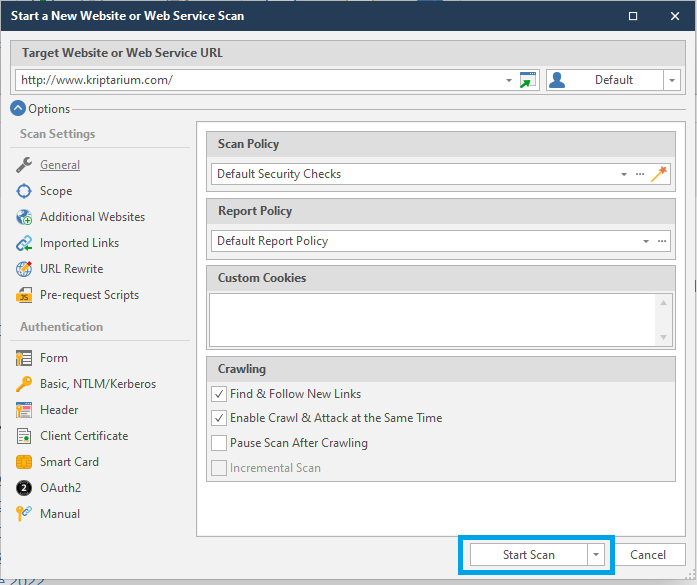
Ayrıca bazı yapılandırma ayarlarını da otomatik olarak yapmış olacağız.

Örneğin ;

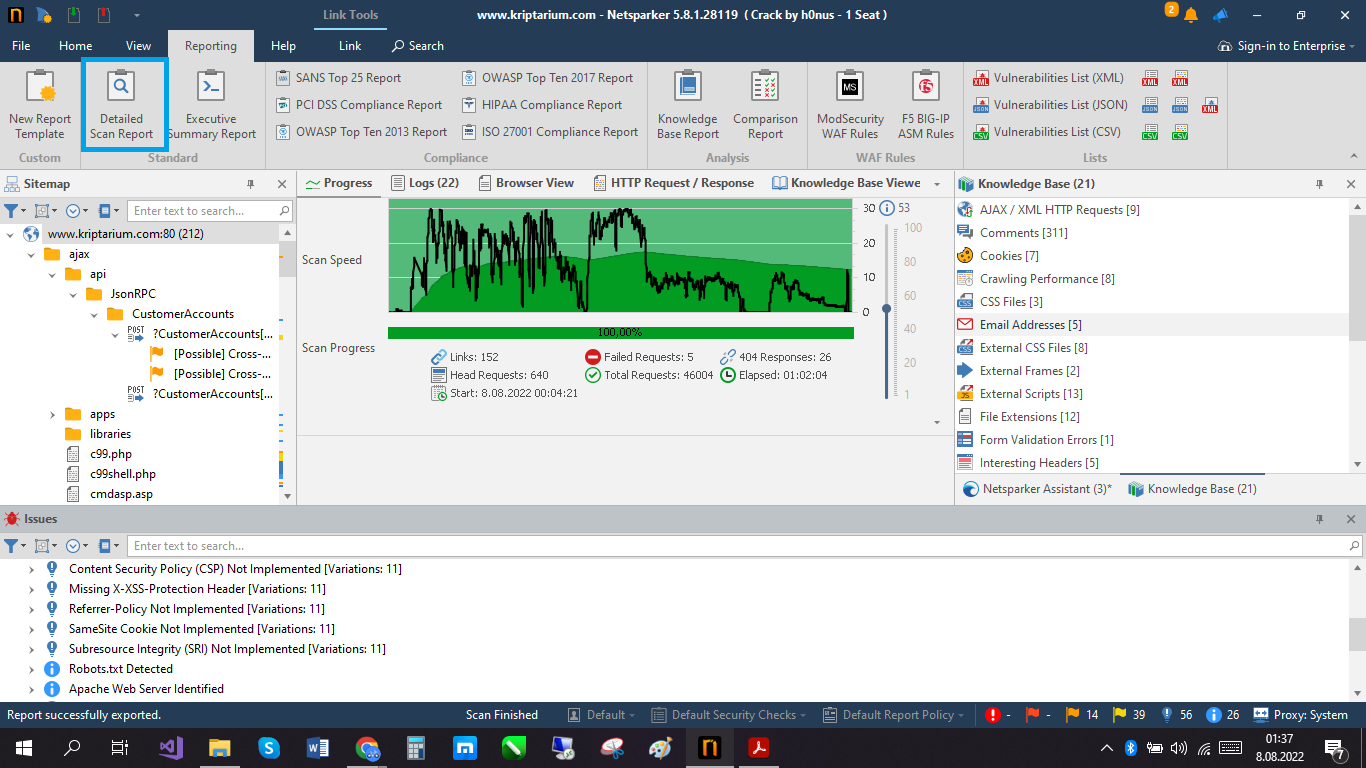
NetSparker uygulama üzerinde tarama esnasında oturumu sonlandırma sayfasına istek yaptığı anda uygulamadan çıkış yapabilir.

Yetkilendirme sayfasına giriş yaptıktan sonra bu gibi oturum sonlandırma sayfalarını tanır ve tarama profilinde de bu şekilde tanımlama yapar .

Aynı parametleri kullanan login formlarında da bu giriş bilgileri kullanılır.

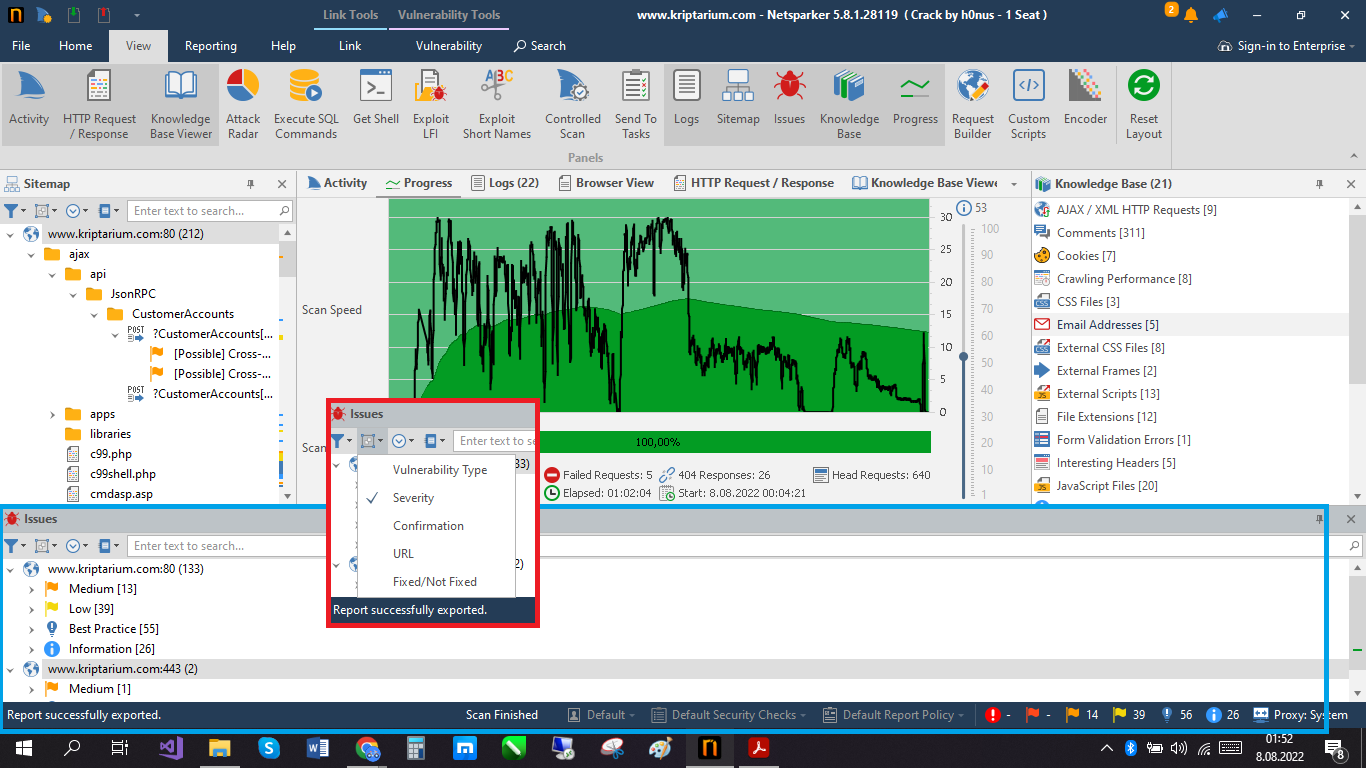


Start Scan butonuna tıklayarak taramamızı başlatıyoruz.



Sonuç çıktı ekranımız.

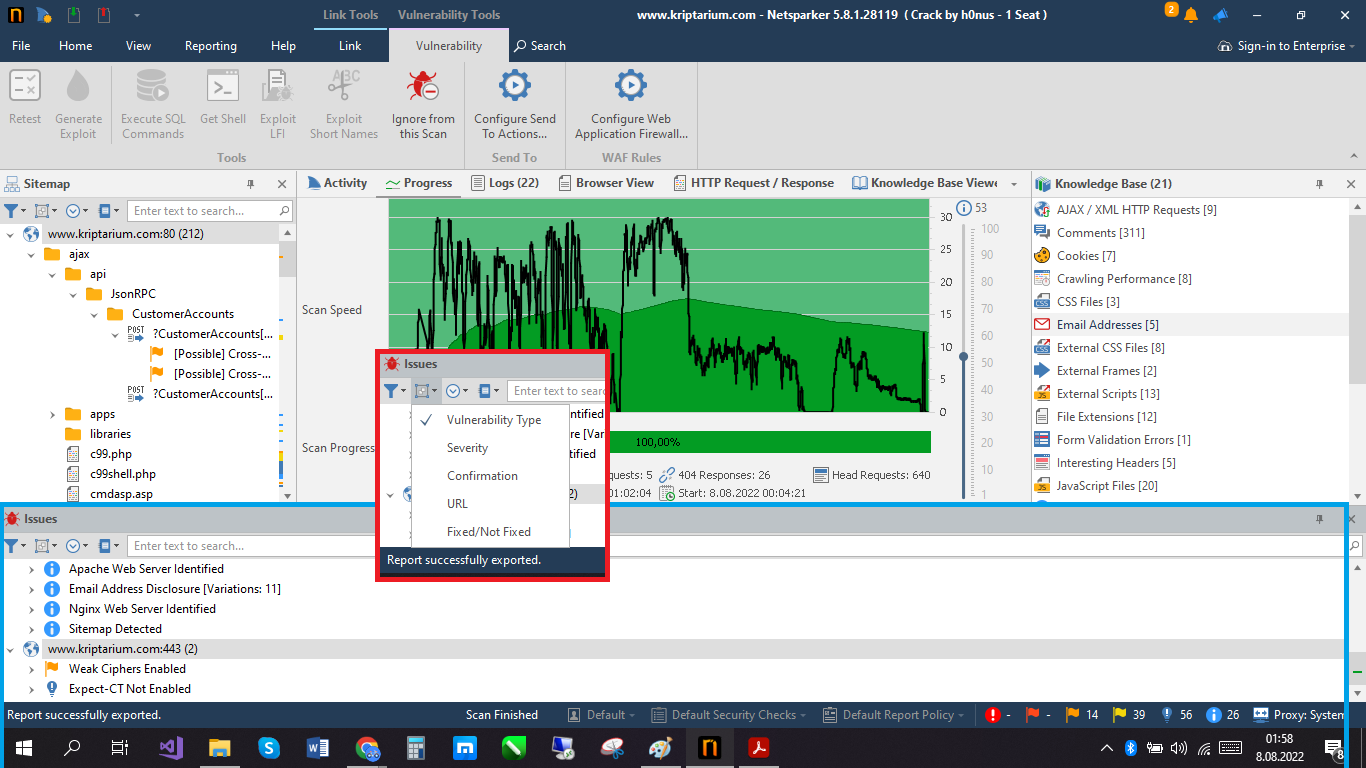
Yaklaşık olarak 1 saatte toplam 46 bin istek atarak sonuca ulaştık.



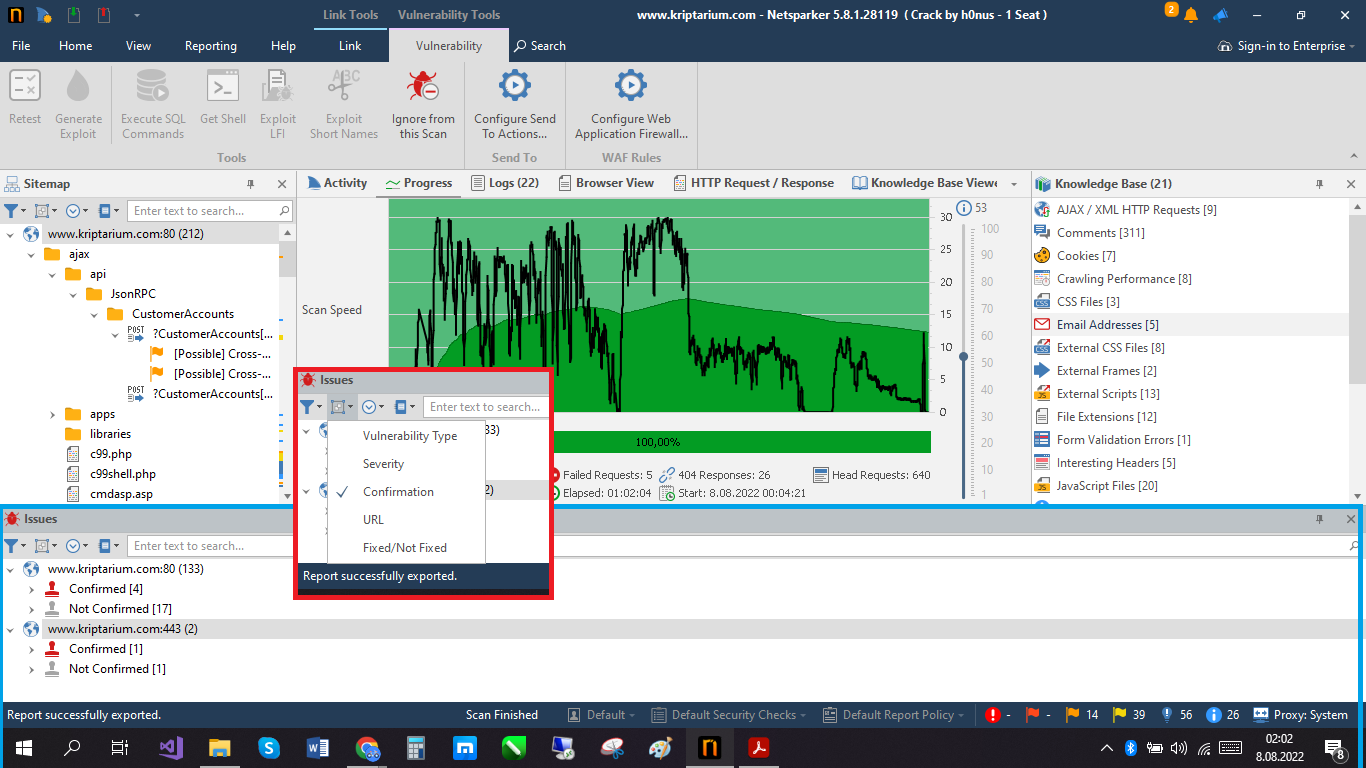
Mavi işaretli alanda bulunan bulguları görüyoruz . Bu bulguların üstüne tıklayarak içeriğine de erişebiliyoruz.

Kırmızı işaretli grup by alanında bulguları tür , önem , URL , onaylanma durumuna göre sıralayabiliyoruz.

Bu alanda önemine göre sıralı sonuçları görüyoruz.

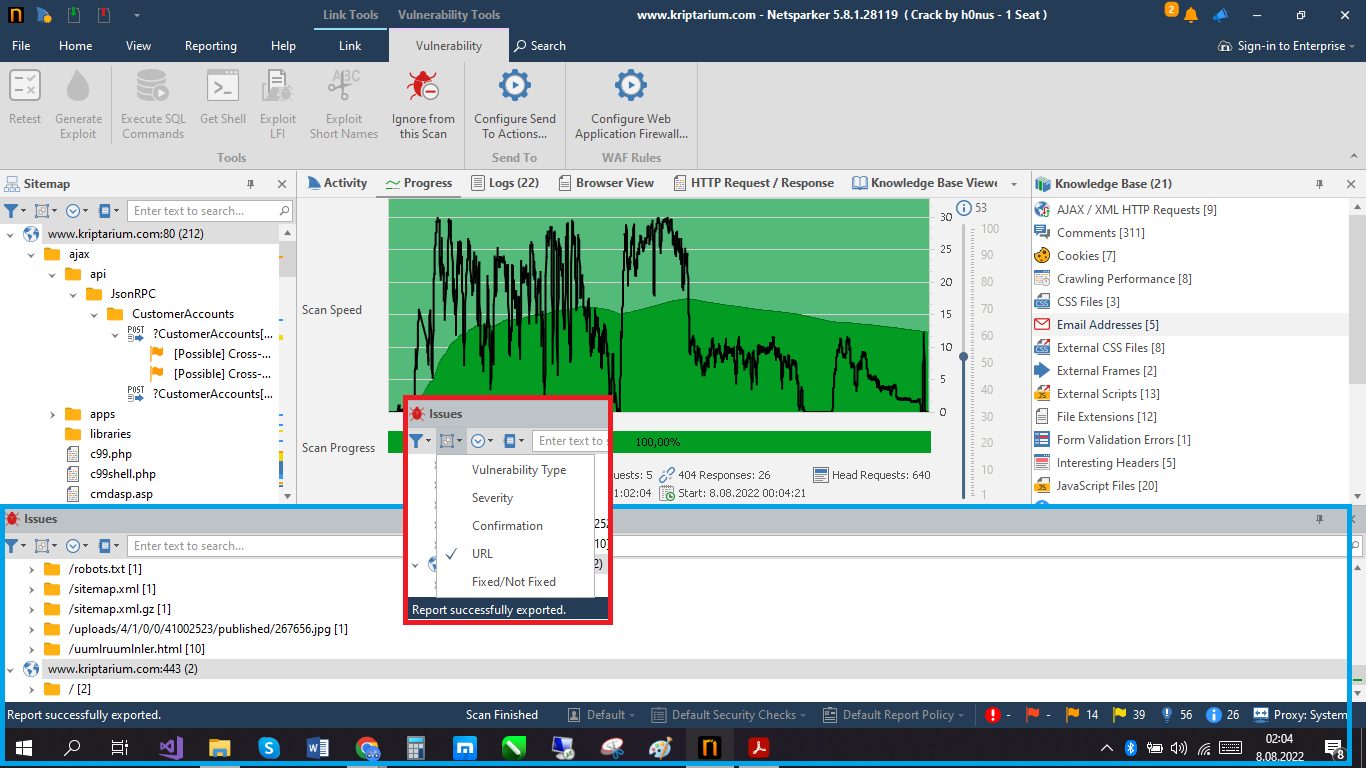


Bu alanda türlerine göre sıralı halde görüyoruz.

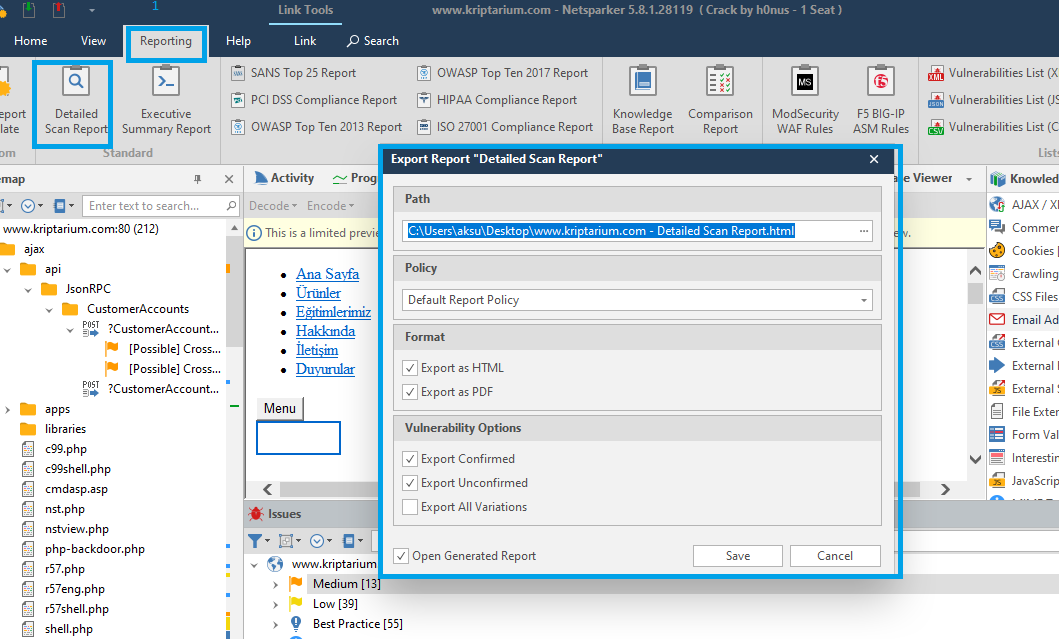
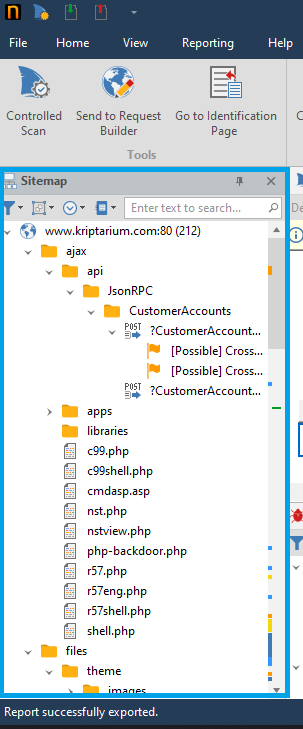


Bu alanda onaylanma durumuna göre sıralı halde görüyoruz.

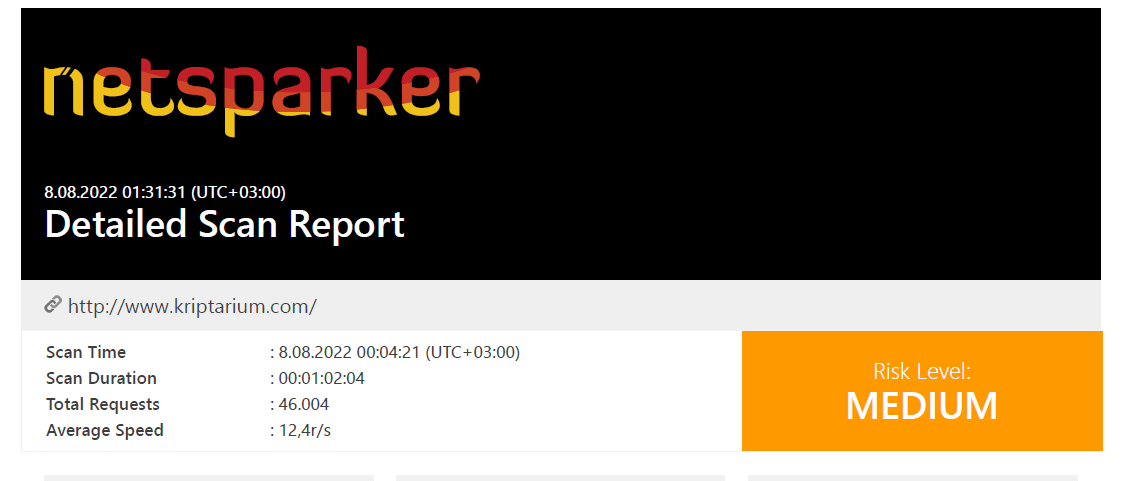
Bu alanda ise URL listesini görüyoruz.



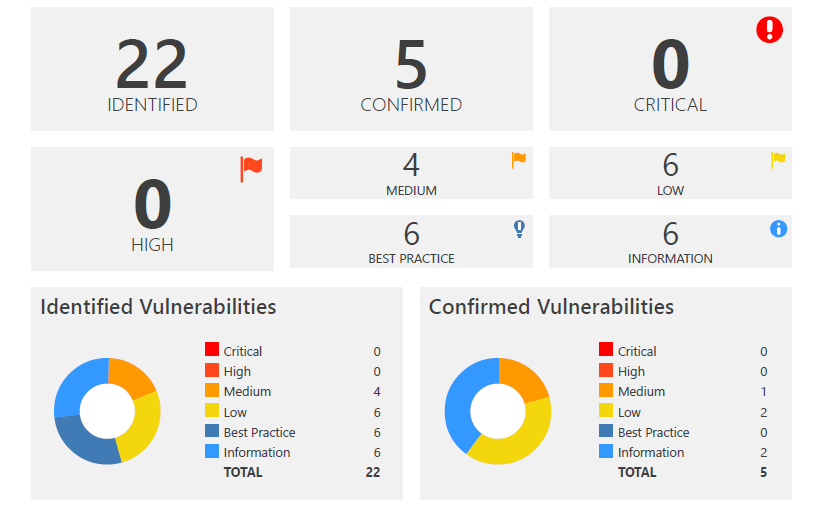
Keşfedilen dizin ve dosyalarla birlikte bunlar üzerindeki bulgular bu alanda listeleniyor.



Keşfedilen bulguları içeren zafiyet raporun bilgisayarımıza şekildeki gibi .html veya .pdf olarak kaydediyoruz.



Oluşturduğumuz rapor dosyasında hedef kaynağın risk durumu orta (medium) olarak elde ediyoruz.

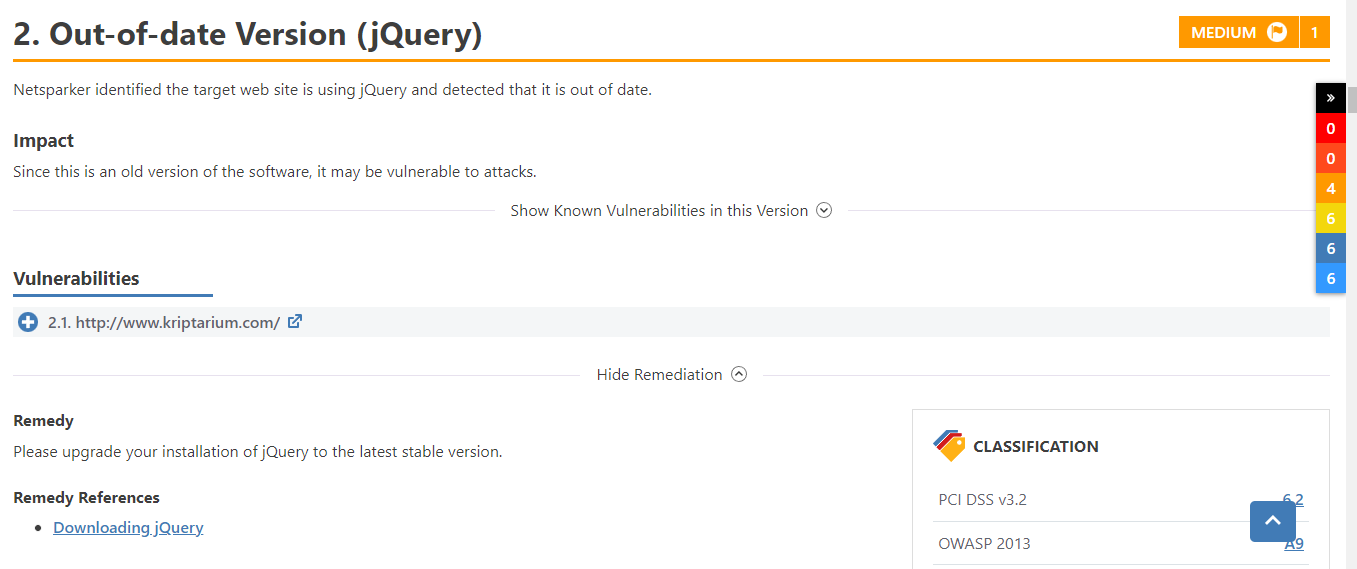


Raporumuz da tanımlanmış ve onaylanmış şeklinde ikiye ayrılmış güvenlik açıkları karşımıza çıkıyor.

Bunlardan 22 tanesi tanımlanmış (identified) 5 tanesi ise onaylamış (confirmed) bulgudur.

Identified vulnerabilities içinde 4 adet orta riskli , 6 adet adet düşük riskli , 6 adet best practice , 6 adet bilgi bulgusu bulunmaktadır.

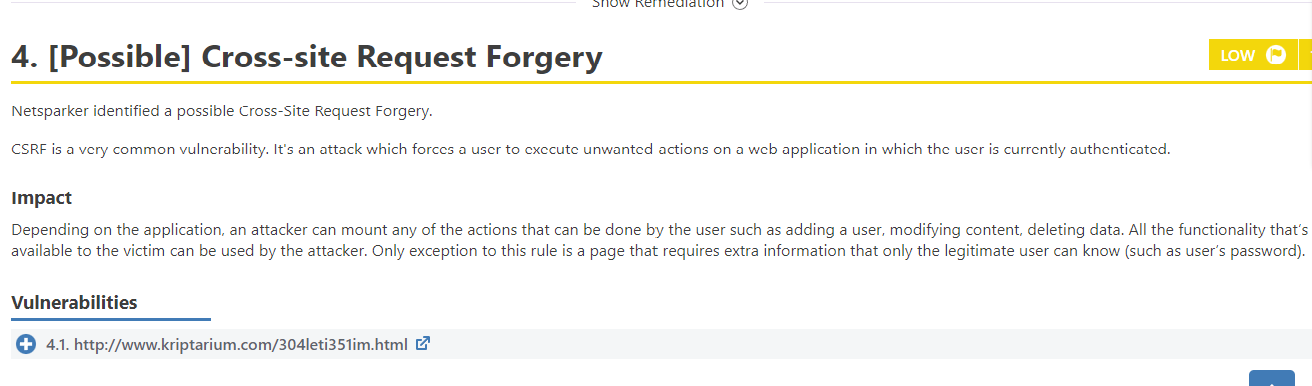
Confirmed Vulnerabilities içinde ise 1 adet orta riskli 2 adet düşük riskli 2 adet bilgi bulgularını görüyoruz .



Orta derece bir açıkta

Hedef web uygulamasının jQuery kullanıldığı tespit edilmekle beraber güncel olmadığını da bize gösteriyor

Aynı zaman bu açıkların çözümlerini de bize sunuyor. jQuery sürümünüzü son ve kararlı sürüme yükseltin.

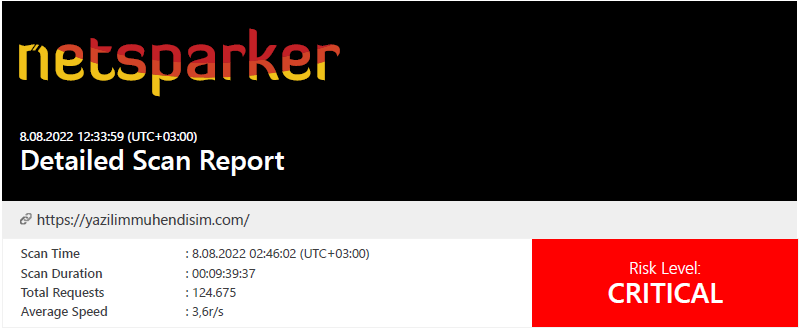


olası bir Siteler Arası İstek Sahteciliği tespit edildi.

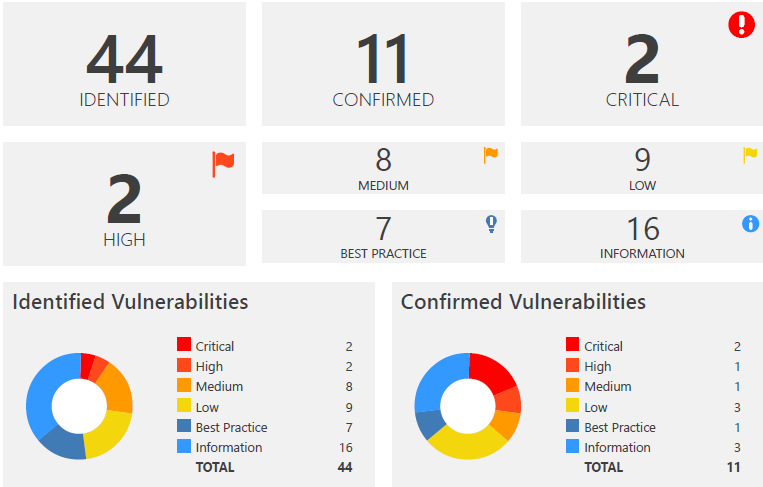
CSRF çok yaygın bir güvenlik açığıdır. Kullanıcıyı, o anda kimliğinin doğrulandığı bir web uygulamasında istenmeyen eylemler yürütmeye zorlayan bir saldırıdır.



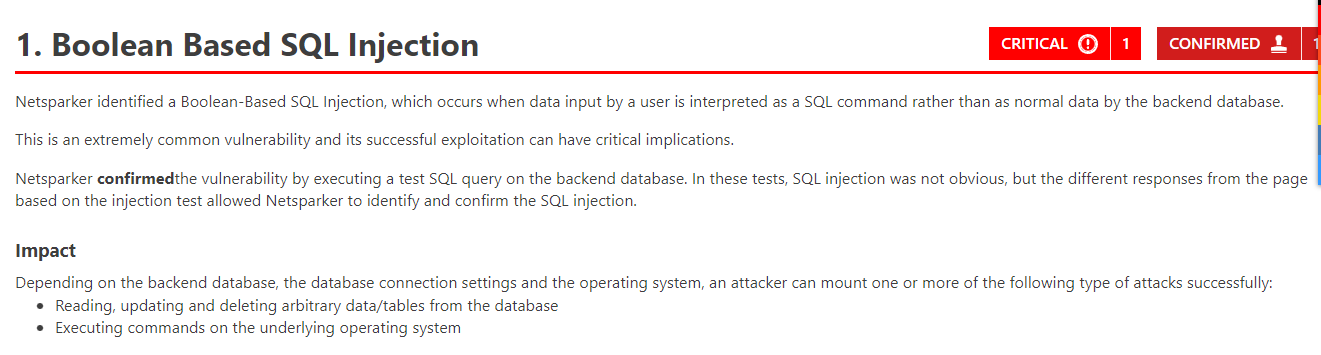
Şeklinde bize çözüm sunmaktadır.



<https://yazilimmuhendisim.com> adresine yaptıgımız tarama da risk seviyesi kritik düzeyde çıkmıştır.



Güvenlik açıkları şemaları yukardaki gibidir . Toplamda 2 kritik düzeyde , 2 yüksek düzeyde 8orta,9 düşük risk bulunmuştur.



Netsparker, bir kullanıcı tarafından veri girişi arka uç veritabanı tarafından normal veri olarak değil de bir SQL komutu olarak yorumlandığında oluşan Boole Tabanlı SQL Enjeksiyonu tanımladı.

Bu son derece yaygın bir güvenlik açığıdır ve başarılı bir şekilde kullanılmasının kritik sonuçları olabilir

Raporların tamamına ekte ulaşabilirsiniz.