Furkan BAŞAN – 16541044

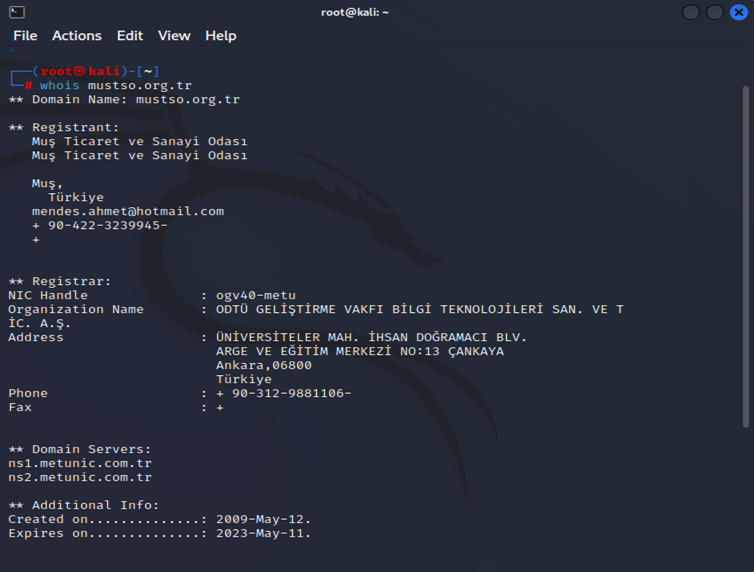
**Kişisel Rapor**  
  
Muş ticaret sanayi odasının sızma testi için grup1 de görev aldım.

Vize sunumlarında Wireshark tanıttığımdan dolayı Muş TSO da çalışırken farklı güvenlik tespit araçları kullandım (WireShark aynı ağda olmayı gerektirdiğinden grup olarak WireShark kullanmaktan vazgeçmiştik).

Taramaya WHO IS Sorgusu ile başladım

Whois sorgulama,  Bu sorgulama sonucunda domain kayıt operatöründe tutulan alan adına ait iletişim bilgileri açık olarak sergilenir.

Elde Ettiğim Sonuçlar :



Burada kayıtlı bir telefon numarası, adres ve mail hesabı görüyoruz; fakat adres olarak Ankara Çankaya verilmiş durumda telefon numarası ise 0312 alan kodu ile başlıyor buda Ankara’nın alan kodu olduğundan doğrudan Muş TSO ile alakalı değiller.

Dmitry:

Who is sorgusundan bir sonuç alamayınca daha detaylı bilgiler edinebileceğimi düşündüğüm Dmitry üzerinden bir tarama yaptım. Dmitry basitçe içerisinde who is sorgusu, açık port sorgusu vs. yapabilen bir araç. Açılımı ise “Deepmagic Information Gathering Tool”.

Elde ettiğim sonuçların özeti aşağıdaki gibidir:

HostIP:151.80.40.80

HostName:mustso.org.tr

0 Subdomain

0 Email Adresses

---------------------------------

Port State

53/tcp open

80/tcp open

(Dmitry çıktısı normalde oldukça uzun fakat zaten halihazırda yaptığım who is sorgusu ve diğer önemsiz şeyleri sildiğimde yeni ulaştığım bilgileri yazdım)

Sonuç olarak Dmitry üzerinden yaptığım taramada da bir sonuca ulaşamadım.

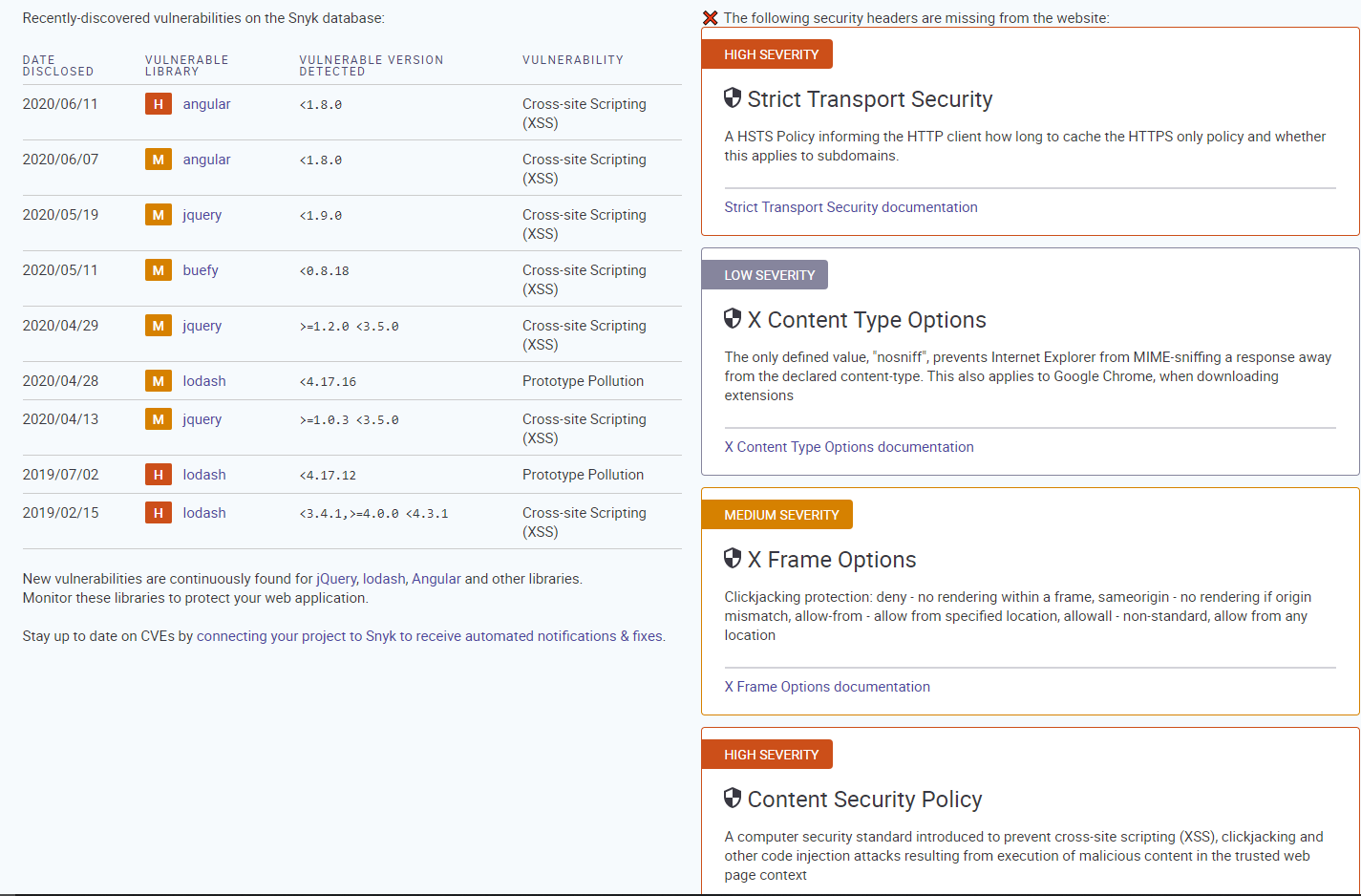
Snyk:

Snyk geliştiriciler için koddaki güvenlik sorunlarını gösteren bir online uygulama

Snyk.io ise web siteleri için domain üzerinden güvenlik taraması yapan kısmıdır.

Basitçe kendi veritabanlarında güncel güvenlik zafiyeti analizlerini site üzerinde uygulayarak sitenin analizini çıkartır.

Ücretsiz ve popüler tercihler arasında yer aldığından bu aracada başvurdum

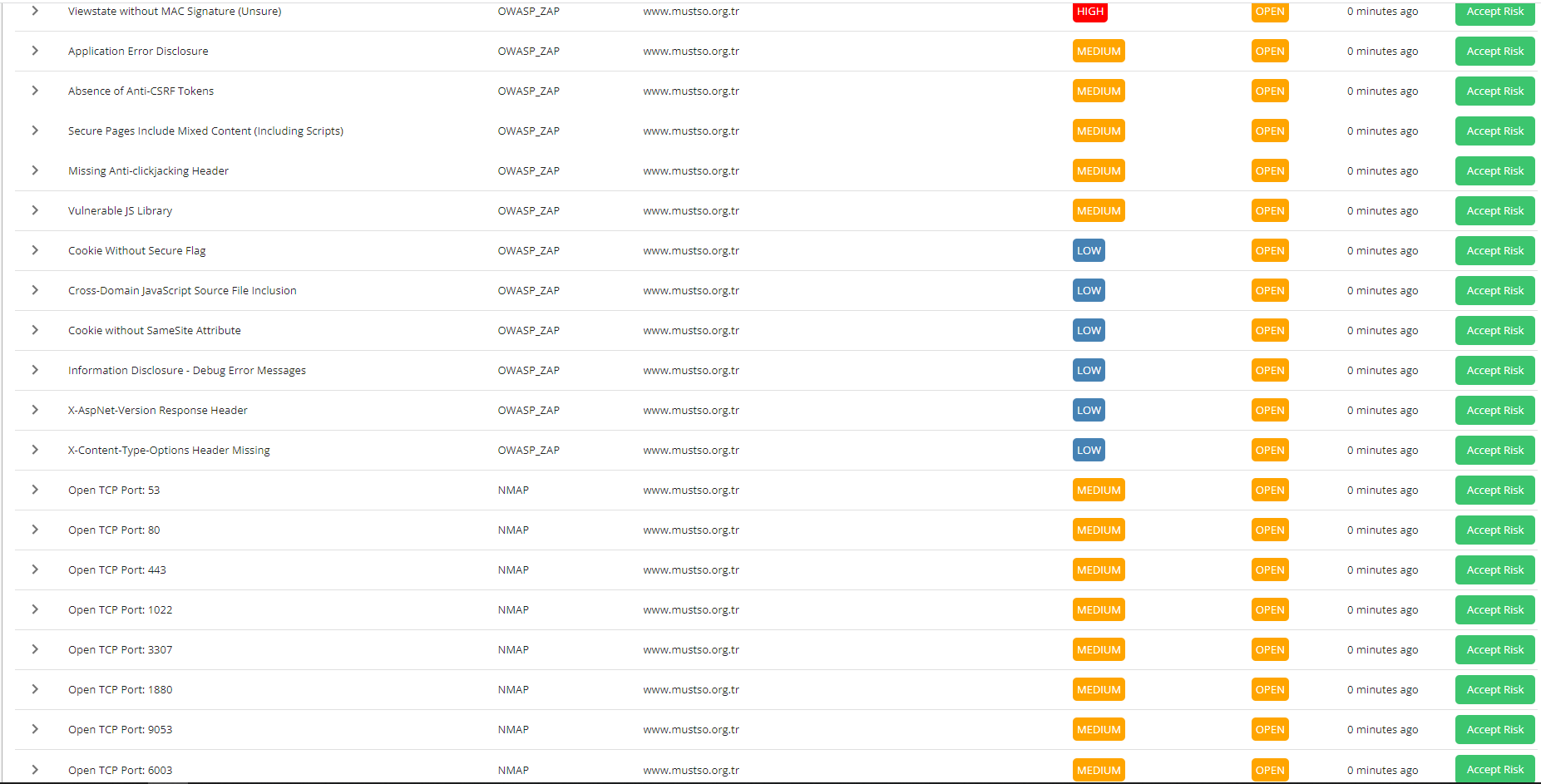


XSS Açıkları kritik tehdit olarak gösteriliyor, Fakat daha detaylı araştırdığımızda bu tehdidin XSS korumasının güncel olmadığı ve Muş TSO nun eski sürüm bir koruma kullandığını gösteriyor.

HostedScan

Yine açık kaynak kodlu bir web güvenlik taraması aracı, taramalarında aşağıdaki araçları kullanır:

* OpenVAS
* Nmap TCP & UDP,
* OWASP ZAP,
* SSLyze



Burada nmap üzerindne açık port taraması ve OWAS\_ZAP üzerindende diğer zafiyetleri taramış olduk,

Sistemde suistimal edilebilecek bir açık bulamadım.