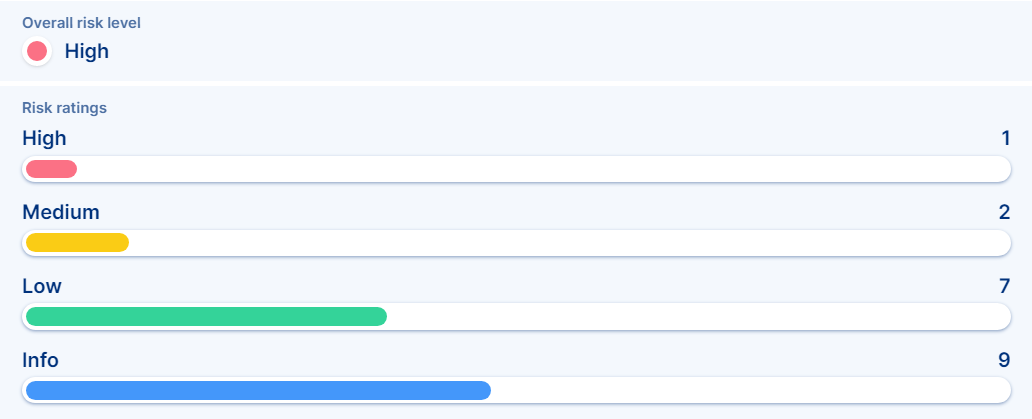
1. **YÖNETİCİ ÖZETİ:**



Taradığım çeşitli araçlarla dpu.edu.tr ve portal.dpu.edu.tr domainlerindeki en kritik sorun “Sunucu taraflı yazılım için güvenlik açığı” oldu. Buradaki sorunun temeli 3. parti yazılımların güncellemelerindeki sorunlar olarak gözüküyor. Bu güncelleme problemleri yeni versiyonlara güncellenmesiyle çoğunu çözebilir gibi duruyor.

Orta seviye risk olarak “Missing Secure Flag” ve cookie settingslerde sorun var. Bunun çözümü de çeşitli güvenlik kanalları ile çözülebilir olarak gözüküyor.

Düşük ve önemsiz olan riskler ise “Missing Security Header” başlığında çeşitli hatalar bulunmakta.

Genel olarak değerlendirirsek, site gayet güvenli duruyor. Çoğu saldırı işlerine karşı güvenli bir altyapısı olduğunu söyleyebiliriz. Çeşitli araçlarla bilgi toplama işlemi yaptığımda (pasif veya aktif) çok az veri elde edebildim bu da sitenin araştırmalara hacklenmelere saldırılara karşı daha güvenli halde olduğunu gösteriyor.

1. **GİRİŞ:**

Pentest’e katılan kişi : HAZAR HASCAN

Saat bilgileri/ Tarihler:

6.12.2022 20.30-23.30

11.12.2022 15.00-20.00

**3- METODOLOJİ:**

3-A) centralops sorgusu:

\*Server’ın ip aralığını öğrendim.

(inetnum: 194.27.43.0 – 194.27.43.255 )

\*Mnt-by altyapı olarak ULAKNET-MNT öğrendim

\*server : ns1.dpu.edu.tr

\*email: [root@ns1.dpu.edu.tr](mailto:root@ns1.dpu.edu.tr)

\*domain servers:

(ns1.dumlupinar.edu.tr , ns2.dpu.edu.tr , 194.27.43.172 , ns.ulak.net.tr)

\*expires on: 2023/1

3-B) whois sorgusu:

\*domain servers:

(ns1.dumlupinar.edu.tr , ns2.dpu.edu.tr , 194.27.43.172 , ns.ulak.net.tr)

\*expires on: 2023/1

NIC Handle: tbk1036-metu

Organization name: TRABİS KK

Adress: ANKARA

3-C) nmap sorgusu (\*dpu.edu.tr // -portal.dpu.edu.tr):

\*993 filtered tcp ports (no response), 5 filtered tcp ports (host-unreach)

PORT STATE SERVICE

80/TCP open http

443/TCP open https

-998 filtered tcp ports (no response)

PORT STATE SERVICE

80/TCP open http

443/TCP open https

3-D) theHarvester sorgusu:

portal.dpu.edu.tr için sadece 2 değer aldım

\*ASN numarası ve bir IP buldum.

( AS8517 - 194.27.43.97 )

dpu.edu.tr için bulduğum değerler çok fazlaydı

\*1 adet ASN numarası ( AS8517 )

\*5 adet interesting url’ler ( http://covid19.dpu.edu.tr )

\*39 IP adresi ( 74.125.198.121 )

\*248 host ( eysuzem.dpu.edu.tr:194.27.235.123 )

**4- BULGULAR**

Okulumuzun web sitelerinde bir çok önlemin bulunduğunu düşünüyorum. DDOS savar, antivirüsler, firewall, Saldırı önleme sistemleri, filtre uygulamaları. Burada kullanılmayan domainler güvenlik açığı olmaması için kapatılabilir 248 tane bulduğum host’un içinde kullanılmayanlar illaki vardır diye düşünüyorum. Server kısmında 3. parti yazılımlar güncellenerek son sürümlerdeki yeniliklerden daha iyi faydalanılabilir.

**5- SONUÇ**

Dpu.edu.tr ve portal.dpu.edu.tr ile ilgili son yorumlarım iki sitede de işlerin gayet iyi gözüktüğü ve bir sorun olmadığını düşünüyorum. Pentest’de pasif ve aktif bilgi toplama araçları kullandım. Amaç olarak ödev yazabilirim fakat gayet keyifliydi.

İletişime geçebileceğiniz mail adresi: [hazar.hascan@ogr.dpu.edu.tr](mailto:hazar.hascan@ogr.dpu.edu.tr)

Bu rapor ödev için verilen süre zarfında yapılmıştır.

AD SOYAD: HAZAR HASCAN OKUL NUMARASI: 201913172016