IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

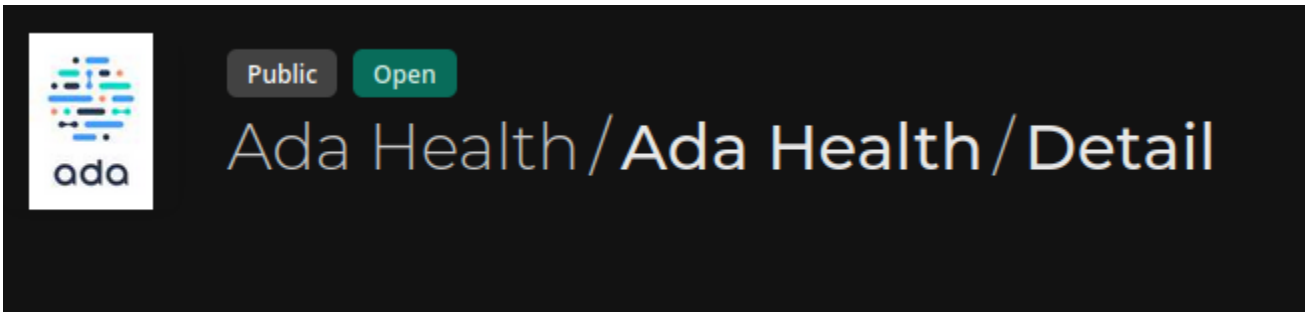
Report 03 – Ada Health

Lecturer in charge – Ms. Chethana Liyanapathirana

IT21826368 – Nanayakkara Y.D.T.D

Contents

1. Ada Health/Ada Health/Detail



1.1.Overview

Description

Hi, we're Ada. We've been working hard to improve health outcomes since 2016. Built by doctors and scientists and powered by a 10 million-strong user base, our medical AI simplifies healthcare journeys and helps people take care of themselves. We help people understand, manage, and get care for their symptoms with trusted medical expertise in minutes. Our enterprise solutions convert medical knowledge and clinical excellence into better outcomes for our partners.

Bounties

		Low 0.1 - 3.9	Medium 4.0 - 6.9	High 7.0 - 8.9	Critical 9.0 - 9.4	Exceptional 9.5 - 10.0
Tier 1	€	100	500	1,000	3,000	5,000
Tier 2	€	50	250	750	2,500	4,500
Tier 3	€	50	150	500	1,500	3,500

View changes

1.2.Scope

In scope

We Are Specifically Looking For

- Accessing any user, customer, or partner sensitive information
- PHI (Protected Health Information) and PII (Personally Identifiable Information)
- Remote Code Execution vulnerabilities are also on our target

OpenAPI Documents

- Assessment BFF Open Api documentation is added as attachment.

Extra Information

- For FHIR and Smart Auth flows, please check the related repositories https://github.com/adahealth
- Some endpoints can host OpenApi and GraphQL documentation
- We have stage endpoints without real data corresponding to prod environment. 20 reqs/sec are accepted on stage environments. Reconnaissance techniques can be applied for discovering. Found vulnerabilities for listed assets will be accepted.

SLA Internally

We will validate all submissions within the below timelines, once your submission has been verified by Intigriti. Submissions validated outside of this may be awarded a €25 bonus. This remains at the discretion of Ada Health to award.

Vulnerability Severity	Time to validate
Exceptional	2 Working days
Critical	3 Working days
High	7 Working days
Medium	15 Working days
Low	30 Working days

Working hours = Mon - Fri 9 AM - 5 PM CET

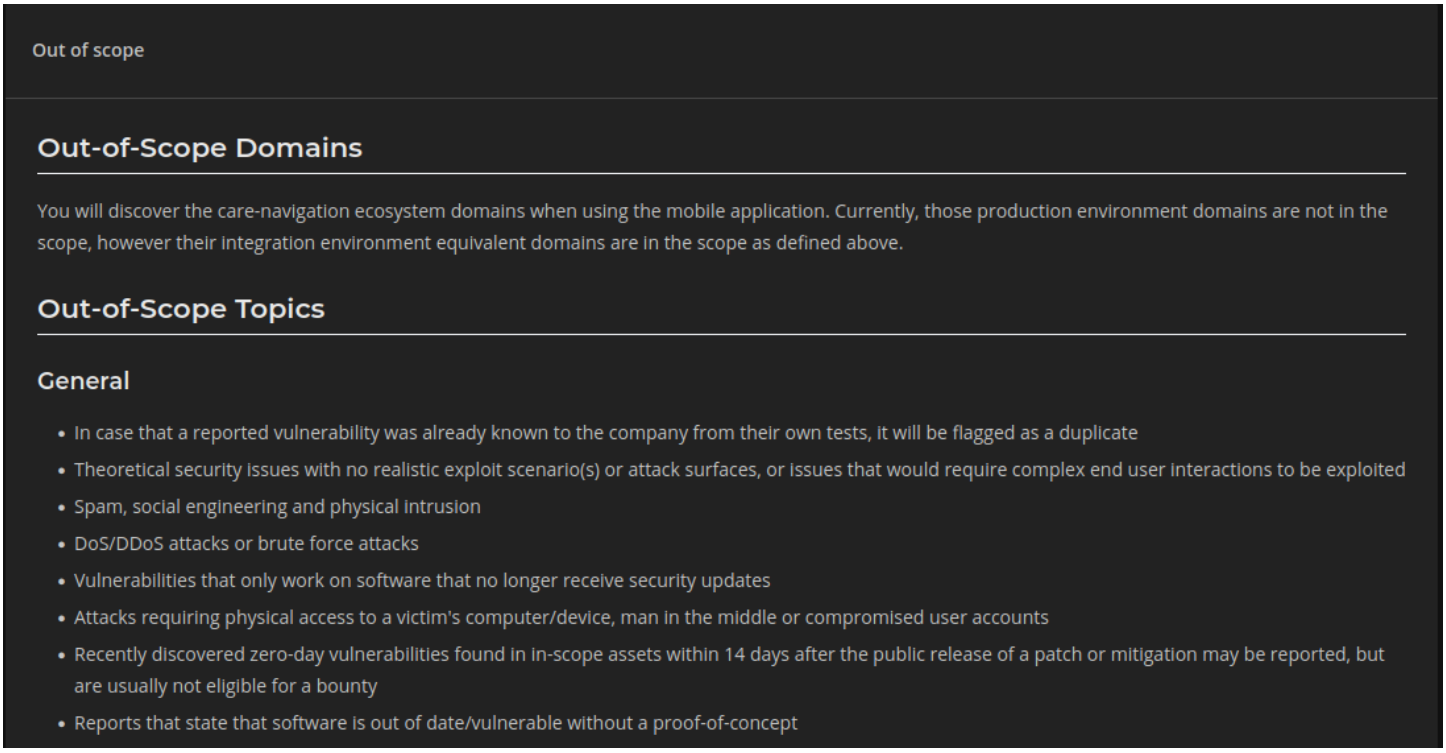
Check Our Fix

We may offer up to €50 bonus to verify a resolved High, Critical, or Exceptional issue. This remains at the discretion of Ada Health to award.

Feedback

Would you like to help us improve our program or have some feedback to share, please send your anonymous feedback here: Program Feedback Link Please note this form will be checked periodically and **should not** be used for submission or support queries.

1.3. Out of Scope



Out of scope

Out-of-Scope Domains

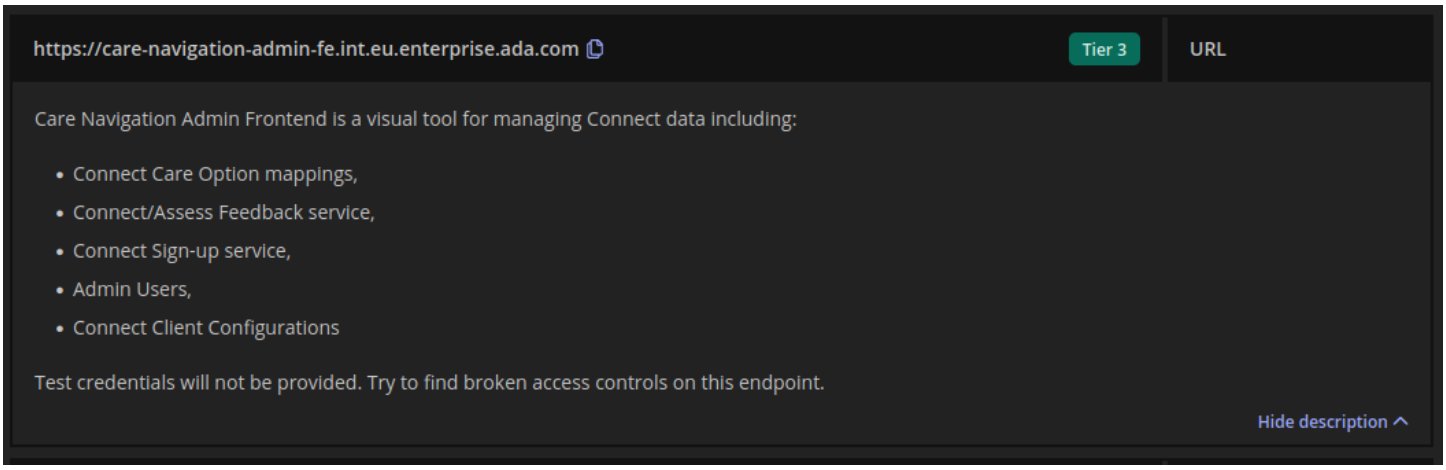
You will discover the care-navigation ecosystem domains when using the mobile application. Currently, those production environment domains are not in the scope, however their integration environment equivalent domains are in the scope as defined above.

Out-of-Scope Topics

General

- In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited
- Spam, social engineering and physical intrusion
- DoS/DDoS attacks or brute force attacks
- Vulnerabilities that only work on software that no longer receive security updates
- Attacks requiring physical access to a victim's computer/device, man in the middle or compromised user accounts
- Recently discovered zero-day vulnerabilities found in in-scope assets within 14 days after the public release of a patch or mitigation may be reported, but are usually not eligible for a bounty
- Reports that state that software is out of date/vulnerable without a proof-of-concept

1.4. Selected Domain



https://care-navigation-admin-fe.int.eu.enterprise.ada.com

Tier 3

URL

Care Navigation Admin Frontend is a visual tool for managing Connect data including:

- Connect Care Option mappings,
- Connect/Assess Feedback service,
- Connect Sign-up service,
- Admin Users,
- Connect Client Configurations

Test credentials will not be provided. Try to find broken access controls on this endpoint.

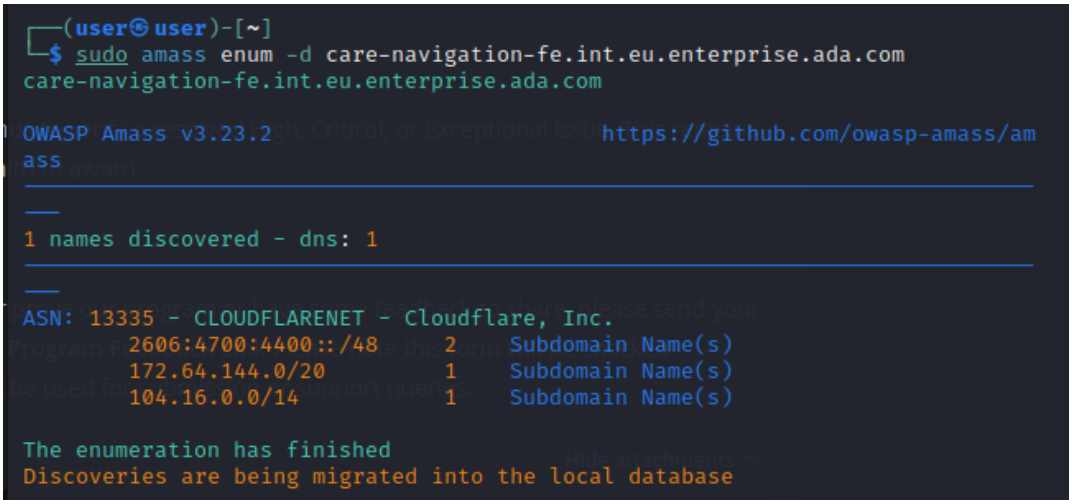
Hide description

In this report I used the above https://care-navigation-admin-fe.int.eu.enterprise.ada.com URL to do the scan.

2. Information Gathering

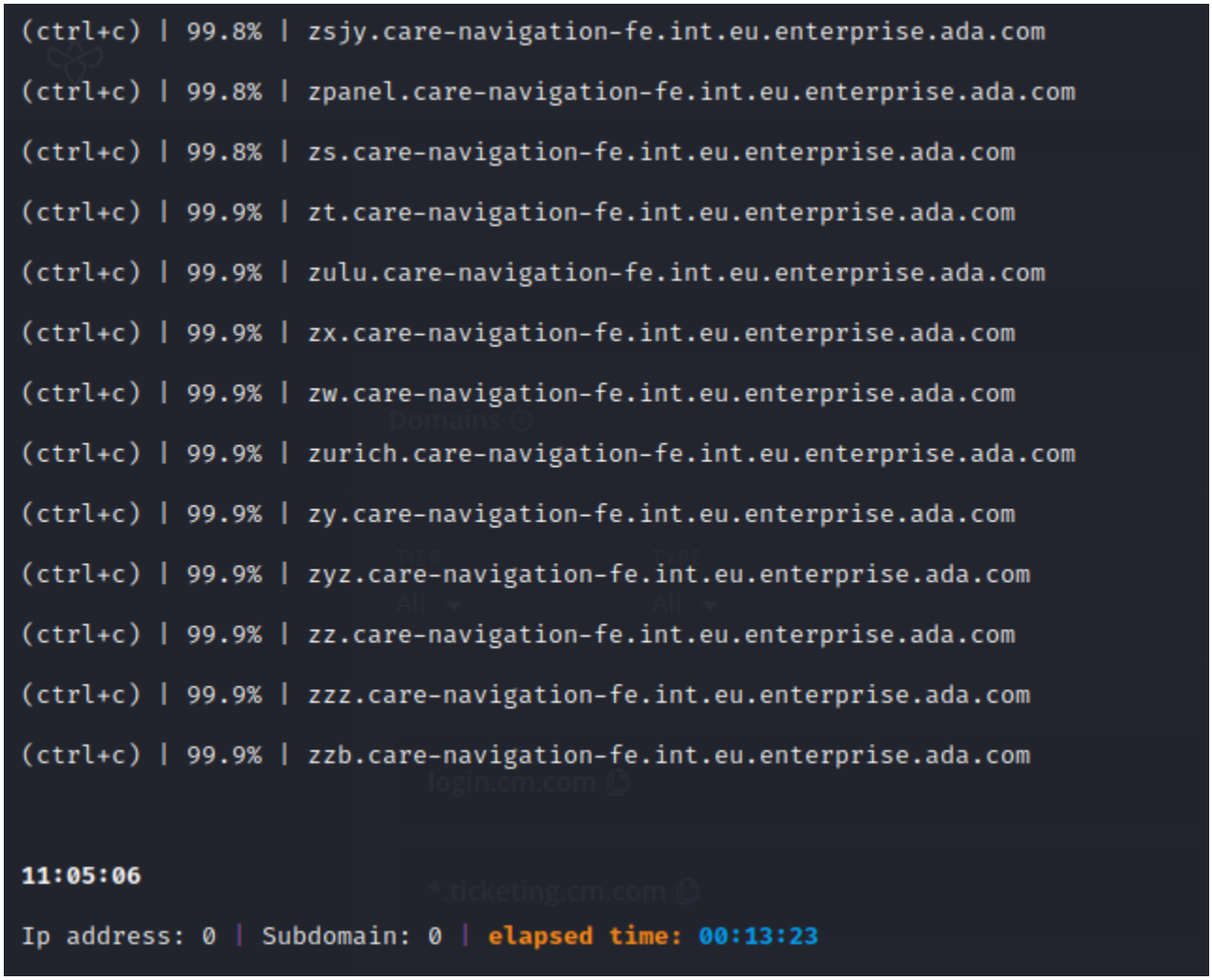
2.1. Amass

- Scan Using Amass



2.2. Knockpy

- Using Knockpy


(ctrl+c) | 99.8% | zsjy.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.8% | zpanel.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.8% | zs.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zt.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zulu.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zx.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zw.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zurich.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zy.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zyz.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zz.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zzz.care-navigation-fe.int.eu.enterprise.ada.com
(ctrl+c) | 99.9% | zzb.care-navigation-fe.int.eu.enterprise.ada.com
11:05:06
Ip address: 0 | Subdomain: 0 | elapsed time: 00:13:23

2.3. Dmitry

```
┌──(user㉿user)-[~/Documents/Programs/rapidscan-master]
└─$ sudo dmitry care-navigation-admin-fe.int.eu.enterprise.ada.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:172.64.146.211
HostName:care-navigation-admin-fe.int.eu.enterprise.ada.com

Gathered Inet-whois information for 172.64.146.211
---------------------------------


inetnum:        171.34.0.0 - 172.80.127.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ------------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2019-01-07T10:48:46Z
last-modified:  2019-01-07T10:48:46Z
source:         RIPE

role:           Internet Assigned Numbers Authority
```

```
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.108 (BUSA)


Gathered Inic-whois information for care-navigation-admin-fe.int.eu.enterprise.ada.com
---------------------------------
ERROR: Unable to locate Name Whois data on care-navigation-admin-fe.int.eu.enterprise.ada.com

Gathered Netcraft information for care-navigation-admin-fe.int.eu.enterprise.ada.com
---------------------------------

Retrieving Netcraft.com information for care-navigation-admin-fe.int.eu.enterprise.ada.com
Netcraft.com Information gathered

Gathered Subdomain information for care-navigation-admin-fe.int.eu.enterprise.ada.com
---------------------------------
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host care-navigation-admin-fe.int.eu.enterprise.ada.com, Searched 0 pages containing 0 result
Gathered E-Mail information for care-navigation-admin-fe.int.eu.enterprise.ada.com
---------------------------------
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host care-navigation-admin-fe.int.eu.enterprise.ada.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 172.64.146.211
---------------------------------
 Port           State

25/tcp          open
80/tcp          open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting
```

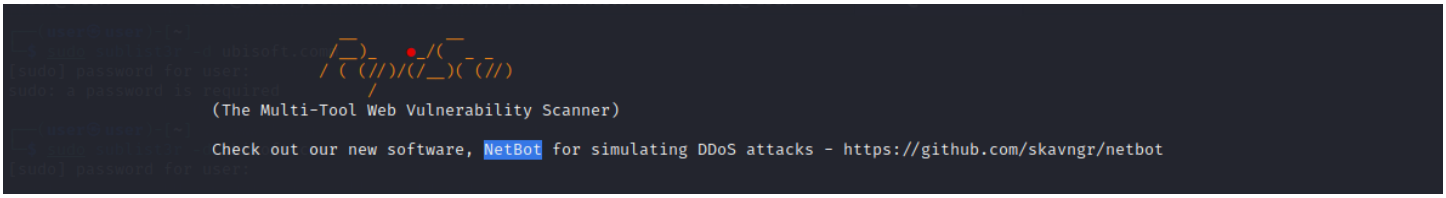
3. Scanning Vulnerability

3.1. Scanning ports using Nmap

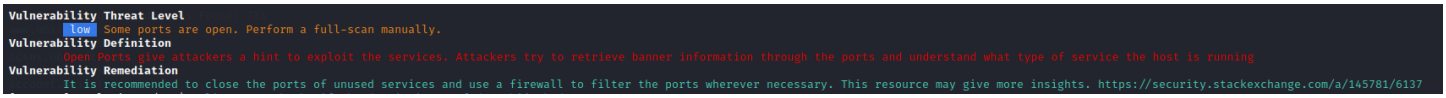
```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 172.64.144.0
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 03:59 PDT
Nmap scan report for 172.64.144.0
Host is up (0.068s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 71.65 seconds
```

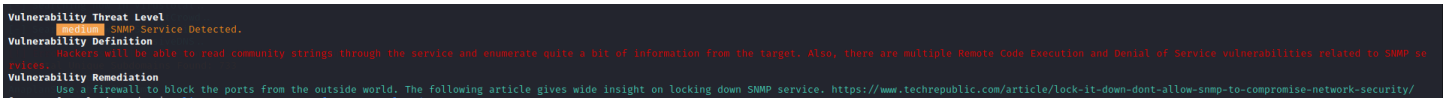
3.2. Scan with rapid scan.



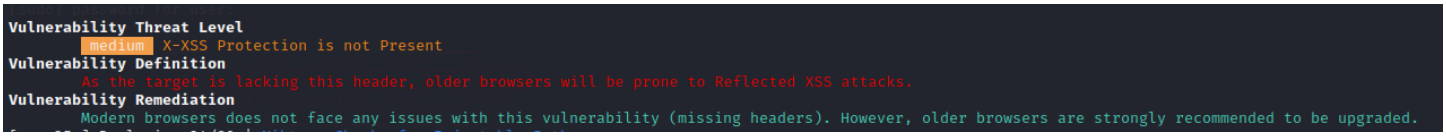
- Some ports are open.



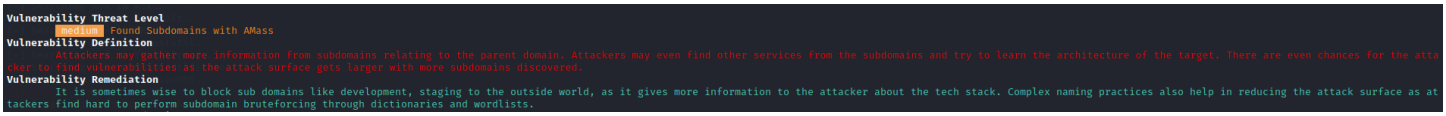
- SNMP service Detected.



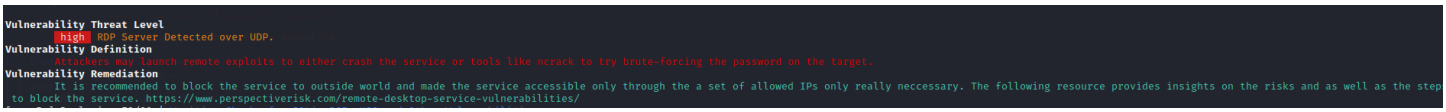
- X-XSS Protection is not Present.



- Found Subdomains with Amass



- RDP Server Detected over UDP.



4. Vulnerability description.

- SNMP Service Detected: An SNMP service has been identified, which could potentially pose a security risk due to its exposure and could lead to unauthorized access or information disclosure.
- X-XSS Protection is not Present: The absence of XSS protection in a web application or website means that it may be vulnerable to cross-site scripting attacks, potentially allowing attackers to inject malicious scripts into web pages.
- Found Subdomains with Amass: Subdomains have been discovered using the Amass tool, which may indicate a potential attack surface expansion or information exposure risk.
- RDP Server Detected over UDP: The presence of an RDP server running over the UDP protocol can pose security risks and may result in vulnerabilities in remote desktop access.

5. Affected components.

- Network devices and services using SNMP.
- Web application or website without XSS protection.
- Domain and its subdomains.
- RDP server and remote access services.

6. Impact assessment.

- SNMP Service Detected: Potential unauthorized access to network devices and potential data leaks.
- X-XSS Protection is not Present: Risk of cross-site scripting attacks, potentially leading to data theft or unauthorized actions on the web application.
- Found Subdomains with Amass: Information exposure, potential for subdomain-related vulnerabilities.
- RDP Server Detected over UDP: Vulnerabilities in the RDP service and possible compromise of remote access.

7. Steps to reproduce.

None.

8. Proof of concept (if applicable)

None.

9. Proposed mitigation or fix

- SNMP Service: Restrict SNMP access and use strong community strings. Update and patch SNMP configurations.
- X-XSS Protection: Implement proper input validation and output encoding to protect against cross-site scripting.
- Subdomains: Carefully manage and secure discovered subdomains to prevent information exposure.
- RDP Server: Review and secure RDP server configurations. Consider avoiding UDP for sensitive environments.

10. Summary

Multiple vulnerabilities have been identified, including potential SNMP service risks, the absence of XSS protection in a web application, expanded attack surface with discovered subdomains, and RDP server vulnerabilities. Mitigation measures and thorough security assessments are necessary to protect the affected components and ensure system security.