FORENSIC CTF - Verify

By rwx4m

Description:

People keep trying to trick my players with imitation flags. I want to make sure they get the real thing! I'm going to provide the SHA-256 hash and a decrypt script to help you know that my flags are legitimate.

Terdapat 3 file yang digunakan untuk menyelesaikan tantangan ini.

```
ctf-player@pico-chall$ ls
checksum.txt  decrypt.sh  files
```

File checksum berisi hash untuk menyesuaikan dengan file yang akan di decrypt nantinya untuk mengetahui file yang benar dan tentunya berisi flag yang dibutuhkan

```
ctf-player@pico-chall$ cat checksum.txt
b09c99c555e2b39a7e97849181e8996bc6a62501f0149c32447d8e65e205d6d2
```

Sedangkan isi dalam direktori "files" akan terlihat seperti digambar:

```
ctf-player@pico-chall$ cd files/
ctf-player@pico-chall$ ls
0QFPjDGl  4KcKU6Xa  9WLdePls  EwszjufH  JQE8B4Up  OYPSxPCM  SeCAw3kn  XQmQCztH  gKBJEwGs  ml8BheQF  sNGrPNW9  x5pS
IkgV
0wKPM7Vk  4S7OA4S1  9XyOtfBh  Exys8oSP  Jq1cYZ8g  OcFa3rqO  T9fmDPnm  XmhfK5Aq  gnoyjDG7  mpB3SJWA  srFcLJ99  xTT3
GfqC
10tptfxh  4l0tWwNc  9b7gQszB  EyBcl2bB  JvzvG7Vc  OhmnsfSS  TE8FU1FG  Y08kAtsE  hB16cKX4  mydpiMHQ  sx2fH87w  xkDm
Ej9c
119zBIIk  5Dpo5Lpk  9d8nFwcg  FAUDGtqU  JwS9q7vh  OkPLXtNq  TPG0sahr  YObSF7u7  hEGhq5DP  n1vcSeUf  tHu44y2r  yCAh
bvDl
19TB8pZ3  5b3OmDaM  9sJDOYFY  FC37odB0  KCldRqWv  OonPniJj  TY6AsyPx  ZLIAqMxY  hL8N2SgO  n61Ajy0l  tNRgqUFc  yNyu
2uzv
1OUKnRjk  5gbVyEtu  9wIEX6Ap  FCHv0zyb  KWhAd048  PEZRi3Qx  TaBG0B2a  ZT5qZdGA  hOTod2wC  nB8BgvEZ  tyOIINiW  yQ6g
SAs0
1P1L0ygq  5oIfd9IJ  AW7wekIn  FCJb9D8b  KYU5dJBV  PTIOjUAO  TcrKRBQh  ZvqyoPUN  hv37OPgb  nEgEYBGO  u6AnP5n8  yao0
qUIY
1WcKHuTD  60q4LDsH  AeWfGlLB  FVtBZjMA  KuP4CIgp  PdjdvRzf  Tmbnqy9u  aWo9YugC  hvIjwsas  nU1oL2aA  u8hC52SO  yokR
4dAH
1ylhS7Z6  65hhdaTN  ApzPkEpG  FomVLBE8  L06xBBN8  PerdXdmX  Tz0v6vYA  agEHnOGT  izhGFAI2  nYYUwHcx  uEMcyj1c  yqCs
XOqL
1zs9Zs50  6HSJkEvn  AxDAiV2s  FsqsVy3q  Lomzo8KF  PrXtVj8G  UB35i7KM  aoamig9W  j1UdH57T  nYqk1CS8  uPw05ctW  z28R
dHqr
295tU6Ga  6SsAocNZ  BPRXW4rK  G7Jl9HbP  LpfjpjFP  Psk7CJHK  UeppfEJC  bjT6NSbK  jHDEMmlj  ngGtZvlW  uS8ThjW5  zIiq
nki2
2TcWPeh8  6kiru4ve  BS2al2Fb  G8ZDeoVW  LrwcukXM  PuKmA1eP  UnO02Frc  bpIGPWgD  jIKe6Zfx  o5TDRZjh  uXM7xQLM  zQ8S
4zxx
2VOltutT  7JZPNEfJ  BS3exq10  GCr8IGJ3  Lwf6P5Kj  Q99Jg4Jp  UujEEh69  c7U1KrcA  jmfr71Fv  oCABmA5i  uY6oCo6R  zTra
YrZH
2p5KxTdA  7jb2Imqm  Bm8zsl99  GEcq4lun  Lz03kcSk  QDL15MCI  UzINJ2WT  cAyG03oe  k41e31GY  oLkVCEIL  ucYToezK  zVoj
uqQn
2pIUNmB1  7ndywIni  COSVSvXt  GSeAwi8t  MPLtzWsV  QHLGtwDe  V3VqDddi  cBV6POlr  kHJFs8HF  ojutsLQ9  uhL7kMRa  zeT6
ehJv
2zYguKpI  8EQoMwiP  CUpZfKDA  GYNiwrKN  MQCiGgtX  QUSFNv4Q  V63YcFAp  cLQTUGHU  kUvLqJ4G  otrltBmC  vCDimHt8
34fINKgc  8KKJnhNd  CZAKNO37  GaLnr2As  MTVTG4gg  QVvIXef5  VDQTXMlu  cWmXM172  kgbulnT1  p44Dq1SO  vIvKsEXP
3AGK4MB5  8XAFnxGx  CcSCdqM1  H61uqmwe  MjMbgBEF  QZ5JwuqX  VEPlKaaH  cakrE5Le  kqKs9dUN  p4ngbycR  vg9T5LbS
3MI3phiM  8mDcrT5i  D5EzyM4s  HBsJejHU  N7Su3TaZ  R1hA1txm  VYprzg0m  cf4lMuNt  kzYNVanR  p9czQWyi  viE4fMXT
3VvoBZaT  8vIsQrBk  D7AhYHSs  HNkAl0Wv  NP3YFw2T  R7FAFiUX  Voj9jP6c  dDawndt3  l1I9SlrE  pZmUSlts  vu8ZQzXa
3f9IBKbV  8vPNDGew  DduIkX8T  HlXjxzfY  NPoWK5Mi  R9PUBlcL  VpCCDBvS  ddo7McIO  lJ0BQ2Wq  pmvuhDPp  w17zkUuj
3uK74LSS  8wqM09n0  DhaIB5aS  Iv7SD7gz  Nc49l2EU  RMO0PzgH  W6HJyLNP  ewYxe6yI  lLGVJakI  qLRvinCQ  wBzvlLFE
451fd69b  96lBoWaU  E5Y6zplS  IvHedMU7  Nel9Qkh9  S0ZumPXR  W6injFLn  fAijPDvG  lNCXHhQD  r8rSf0xW  wIqKXeki
4AVsbijj  98tbiuSQ  EMW8xsyg  J2C3jKRR  NqHkUxDY  SC2gThOs  Wraq7ZVn  flHrhjvC  lP1vtSZx  ro6pmtK2  wRApz452
4GLVcGAT  9Lg5sIdT  EUrDQxDU  J2taODo4  NvZsOWbG  SIFatJfR  XNYpvkxx  fmPAeitt  la1Cjzyx  rprBM8iU  wlgmaCgQ
4J715L0D  9LyIv77J  EZUfAdt0  J5TeIktX  OAqU3ZEC  SVB3p5ql  XP1tFwB7  gGs1IK8o  ld5v1JVF  rrNGwJSR  wuh7Cgbl
```

Untuk percobaan, saya melakukan decrypt keseluruhan file di dalam direktori files tetapi didapatkan.

```
ctf-player@pico-chall$ decrypt.sh files/*
bad magic number
Error: Failed to decrypt 'files/0QFPjDGl'. This flag is fake! Keep looking!
```

Setelah itu dilakukan, saya menggunakan create checksum menggunakan command sha256sum terhadap keseluruhan file dan melakukan pipe (|) grep terhadap hasil checksum yang sesuai dengan isi dari file didalam checksum.txt.

Setelah didapatkan dilakukan decrypt terhadap file yang sesuai dan menemukan flag yang butuhkan. ^^

FORENSIC CTF - Verify

By rwx4m

```
ctf-player@pico-chall$ sha256sum files/* | grep "b09c99c555e2b39a7e97849181e8996bc6a62501f0149c32447d8e65e205d6d2"
b09c99c555e2b39a7e97849181e8996bc6a62501f0149c32447d8e65e205d6d2  files/451fd69b
ctf-player@pico-chall$ decrypt.sh files/451fd69b
picoCTF{trust_but_verify_451fd69b}
```

Scan Surprise