

Writeups de la compétition LoveCTF, 1^{ère} édition

Team : W3hunters

Catégorie du challenge : Stégano

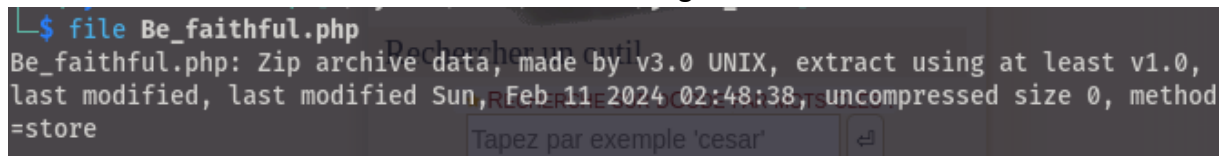
Titre du challenge : Jesus love

Un seul fichier pour ce challenge.



```
[~/.myHome/CTFs/LoveCTF/jesus_love]  
$ ls  
Be_faithful.php
```

Oui, nous avons pensé qu'il s'agissait effectivement d'un fichier php, nous avons donc perdu beaucoup de temps à essayer d'avoir une page web grâce à ce fichier mais gloire à **file**, nous sommes sortis de l'ignorance.



```
$ file Be_faithful.php  
Be_faithful.php: Zip archive data, made by v3.0 UNIX, extract using at least v1.0,  
last modified, last modified Sun, Feb 11-2024 02:48:38, uncompressed size 0, method  
=store
```

Waoh, il s'agissait en réalité d'un fichier zip. Nous sommes contents parce qu'on pense être sur la bonne voie. Essayant d'extraire les fichiers, nous avons été confrontés au problème de mot de passe. Chic !!

Nous ne l'avions pas, nous avons d'abord essayé du brute-force avec les informations que nous avons : le nom de l'auteur du chall, le nom de la compétition, le titre du chall et autres choses un peu trop évidentes pour être le mot de passe. Rien ne marchait, pourquoi ne pas donc tenter d'utiliser **john** ?

```

[~]/myHome/CTFs/LoveCTF/jesus_love]
$ zip2john Be_faithful.php > zip_hash.txt
! Did not find local file header for Jesus_love/ at 0
ver 2.0 efh 5455 efh 7875 Be_faithful.php/Jesus_love/task.txt PKZIP Encr: TS_chk, c
mplen=7176, decmplen=9572, crc=D2125765, hts=15CC, cs=15cc, type=8

[~]/myHome/CTFs/LoveCTF/jesus_love]
$ cat zip_hash.txt
Be_faithful.php/Jesus_love/task.txt:$pkzip$1*1*2*0*1c08*2564*d2125765*45*4d*8*1c08*
15cc*7fd9bdd60cb0e4584fa9ea02b0ca81779db887ca4337abc1854d821837809f51353f0262168636
29f7b9f078bc53e7d62b067df2597a1cfa1a546c0f79094e797744387c5c920a1c82debe86654217c6a
40d7be7041b15a91f6c4a255c07c3f8fb9ddb7f3b353ca040a39f2f21377ca1b0ecb511a577c37c3e6a
dbfb6847163322f33d15bfce02bf8fa9fa192855cf086a162aa9eef9fd89d87d7de1461d61638c76916
191aa83c78b432e440902407413319df86bef570b3014d8fb153412cc1131219b55a214710028c83433
a192457704ba119f70ebef1ce357b32d8175ecfaae0cb5b594fbd3f557c64d43a773edbf9fe08cd0a17
b4b393e3e2c505cd90a9a2abcbcb6530380f5b44363502fdb287c499a2f835d36200898100ab3a33a47
cc4a95ca8d885b54bfc95953f77cd4448c7a096dff6fe5857bcc637a2c8680197285bc453d5ce88bc3
ad22618f8ef9a8d42fb2fcc7aed30a6cc04e5e578154fe4746c028731f9b8ab109da23f0354d4ad029c
3ebe998445e1499e5b1cfff84a7bbc5859b5da366c7c3524a79a1f1bf1c63444a7aebba0525cd1c32e0f
771fc7999c61621cf759894eb02d899e18700d706e38c584a42db921c4957b7e4ce07600ac40a070dc9
5ed6a6a826b9f41eb3d08d08cc53d5e154ac0ef29e95d630545ea754dcb9e1590f6daab5c2a7c38b18a
3c5311e967d605ddfa019c875356e8ec833a5b011b31a07a9fbc7eb0544111e7d1a930222b2252626a2
caaf77cab38027c03d5e84a12227ac69d504d009183dbbf9ff6c711419802004994647ef5507f2da90
99e735acb2c230709f08a42757e8b6c864f59d7c75731aa78ea8f821bf083bb4e4443abc4c9662fab50
04e69d2bbe4c7dca2fbb6b5ff2cc8543486b0f06f8e8c6533658af65d21a04b454501eb3a200b55a836
8ed080c9cd8525ae97ad596e45939925ddb81681a000eadfb07472077b23efcda36b8c773191ab27411
2a32e48261d2be501fc7e6808a8d582e0eb094c7ad519ef5b6e3594179e45034bd559fd5c74f79e9881
92fa3d4dd48b03ce05796208d14d39fbec26789635780907b7369cda1d008fea18180bb91c72d9d9a6
51511d9b299fba2cfd1d532f9eb0e29c5e47f214922739d11c461e92ba6782fa1470bf2f56db93d9d7b
515a892a662b3471b15c5191e0753dc8a00e5563995785f36ef371388354a9977c85d7fb45daf9b468e
0eb197da9eb59c43b7a5db85b8548975650cdd4d206f204e603da231637d340a4fa8f03cd26a2685c4b
035932b0e4b408c92b77f460851b840493d39288becaa1f54f44bc2ba53b01e98abe4743c705662ff08
d40b519ab3415225a393a0b588f28c8952c6ff5eb853293f226547e6f1a88f3a3bda5741471f9d98cfb
d08339d46aefa6fc69e8c86343b64f7334c767621e32431d22df3e299cb12137bbc0e790143b7888afb
ddf0be9fd8a5dee3d16e3606aced997a907737af8af86222f0e4b14c236d44e27cdb392af232286effa

```

Parce qu'on avait déjà une fois cracker le hash généré, on a eu ce retour lors de la rédaction du writeup. Un autre challenge.

```

$ john -wordlist=/usr/share/wordlists/rockyou.txt zip_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
No password hashes left to crack (see FAQ)

```

Google nous a instruits sur le fonctionnement de john. Ce dernier après avoir cracké le hash d'un fichier et trouvé le mot de passe, il le stocke dans un fichier nommé **john.pot**

```

$ cat ~/.john/john.pot
$pkzip$1*1*2*0*1c08*2564*d2125765*45*4d*8*1c08*15cc*7fd9bdd60cb0e4584fa9ea02b0ca817
79db887ca4337abc1854d821837809f51353f026216863629f7b9f078bc53e7d62b067df2597a1cfa1a
546c0f79094e797744387c5c920a1c82debe86654217c6a40d7be7041b15a91f6c4a255c07c3f8fb9dd
b7f3b353ca040a39f2f21377ca1b0ecb511a577c37c3e6adbfb6847163322f33d15bfce02bf8fa9fa19
2855cf086a162aa9eef9fd89d87d7de1461d61638c76916191aa83c78b432e440902407413319df86be
f570b3014d8fb153412cc1131219b55a214710028c83433a192457704ba119f70ebef1ce357b32d8175
ecfaae0cb5b594fbd3f557c64d43a773edbf9fe08cd0a17b4b393e3e2c505cd90a9a2abcbcb6530380f5
b44363502fdb287c499a2f835d36200898100ab3a33a47cc4a95ca8d885b54bfc95953f77cd4448c7a
096dff6fe5857bcc637a2c8680197285bc453d5ce88bc3ad22618f8ef9a8d42fb2fcc7aed30a6cc04e
5e578154fe4746c028731f9b8ab109da23f0354d4ad029c3ebe998445e1499e5b1cfff84a7bbc5859b5d
a366c7c3524a79a1f1bf1$SOURCE_HASH$90907239eef6a0c5ee9ccfd0c7b31852: maxMAN1230#$

```

Nous avons le mot de passe et pouvons continuer.

```
[~/myHome/CTFs/LoveCTF/jesus_love]
$ unzip Be_faithful.php
Archive: Be_faithful.php
  creating: Jesus_love/
[Be_faithful.php] Jesus_love/task.txt password:
  inflating: Jesus_love/task.txt

[~/myHome/CTFs/LoveCTF/jesus_love]
$ ls
Be_faithful.php  Jesus_love  zip_hash.txt

[~/myHome/CTFs/LoveCTF/jesus_love]
$ tree
.
├── Be_faithful.php
├── Jesus_love
│   └── task.txt
└── zip_hash.txt

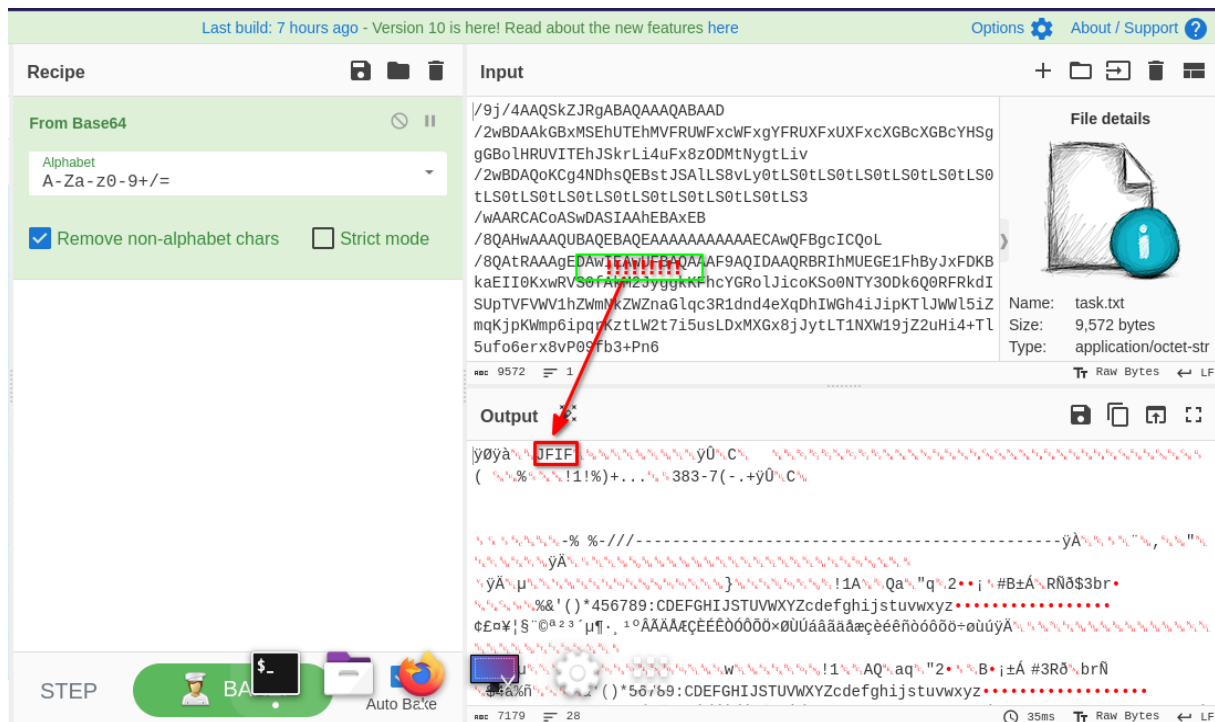
2 directories, 3 files

[~/myHome/CTFs/LoveCTF/jesus_love]
$ file Jesus_love/task.txt
Jesus_love/task.txt: ASCII text, with very long lines (9572), with no line terminators
```

Ouvrir task.txt Enregistrer

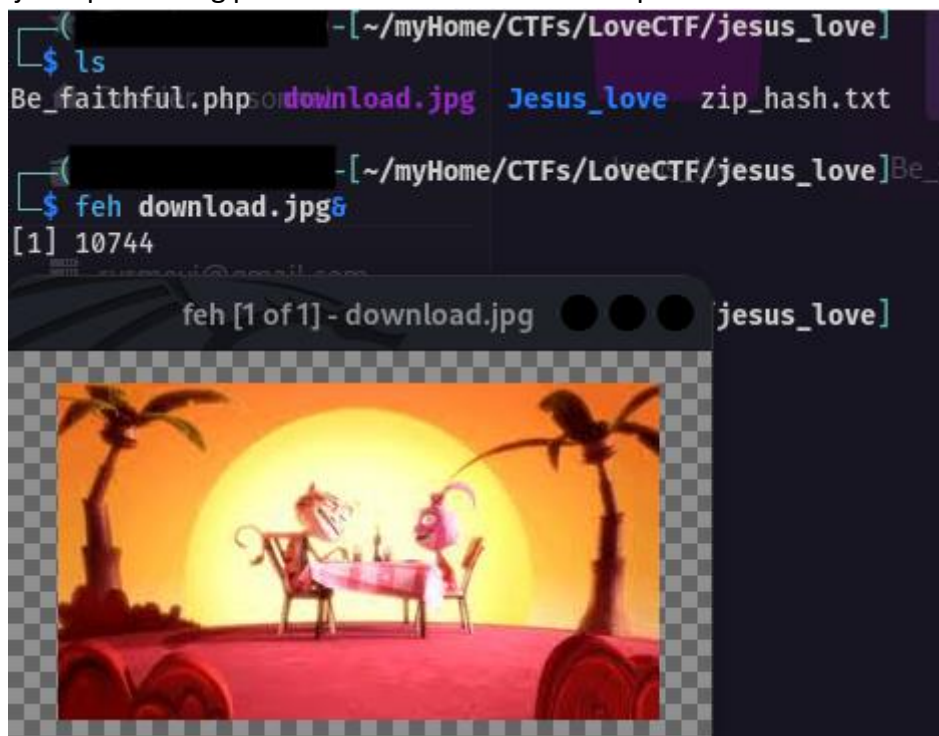
```
1 /9j/4AAQSkZJRgABAQAAQABAAZ/
2wBDAAGBxMSEhUTEhMVFRUWFxcWFxgYFRUXFxcUXFxcXGBcXGBcYHsggGBolHRUVITEhJSkrLi4uFx8zC
2wBDAQoKCG4NDhsQEBstJSA1LS8vLy0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0t
wAARCAoASwDASIAAhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAEAwQFBgcICQoL/
8QAtRAAAgEDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFh
8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNO
K+TcbJrVwJEB24Pet3TNckbaDgkheG7+v8qjmg8uMtKu9RwVwCQffP8PvWHcXUZBMAYFOSp9M4yDn1PSu
wri+qTVSz+871iYqnzXNy98Q28fGdx9qzJPGK/
woPxNcnZ6b07AeW2T7H+ddTYeDwXYD9a6ZUaFJe87syjXr1fhHL4tb+4P1q3Z+K9x+ZOPxzWz/
YcRCgr90Y44z9afHoUA/g/U1z0Prf2TfKq/zE1neLKMqfwPWRQwoorNFOQuKtqmR/
LP8q5210NoymtYlBRtqQLTgKm5XMRgUuKkApwQ1VyeYi20batx2TnopqwmkueuBU86IdWC3ZmbaNTa/
wDyzeXopDo7eop+0RH1mn3MnbRtq/
Jp3y7VXeBh1BFHOjRVYvZLffJipikQincrmISKtBUxFNK1NyuYiK0hFS4pMU7juREUwipitRyKcHHWgq5
OvTw+GpyXc8yviasZdj1HTdUjnGUPPcdxV2vJtH1QxSKwP+H0Neq2swkRXXoRn6VhisP7J+R04bEe1Wu5
wFQRJfSDOSM/h+LaujeH0hG5huf9BW1W0qsTaQXzZjGnOWS38jh7u3ku7jIHg/kK6vS9KSEcD5u5/
wq5aWaxjaox/WrAwsqtdyXKtkOFJRfM9z01UKsBf8dD7Z9vevKbvmRvL4B7Z/
T6V6rr2m+fEVH3uorzK+sHhfawIPuK7svcbPXU5cam2tNC7Z6BcSrvCCdGDj72ew00a6DSfCEmcy1gPQH
CuoVaJIAwwwzXnqg/tam86MWvd0Zm6Vqom+U/
K46itQJXL3enPBj5nJGcgjriurt33KC04pVElrHYVVKpL4ZboQJTtlShacq1kW5EQWpYbZm4UVp2emE8vv
ZB7QqFKjeIHqKvGKmG0odMcahkT6WjdODWZc6ay+49q6Yx00pU6o6qeKmutzjytNK10d3pytyODWNPbEH
U1S120iMhCKay1lXXiibfuZc+w/rWbJ4rk/gt2P1J/oK0VGo+g/
aJG7eWgkRkPQivJvE2ivA5BHHUHSRXbzeLZEBMkG3HTJYZ+nHNYV5dyXvLq4Rc7dq5And2EVSi7v4TmxP
CqWoaBLGN2wlc9dpGfzqjDaEkKTgZr1WqdWOUqP0j7SnLTQ7uXxEXgzjDHPTsP6VjaZ4h8nI2A57n0a67
ZiNVKmWopESngV0wpXPOLMYI6eFp2KXFdUaJnJjcUYp2KXFaqiibjcUmKfijFV7FDuMxSYp+KTFZSohcj
U9B7K01cso20in02rOMu4Z3+6PKU/dLD5iPp2qh/
wJER06QvIf8AaPH6V6HcQBhg1g3MBU4ahVJLbQ90jiefQx4NKiT7saj8P8an2CrJFMipcze50qRyHjuyL
nV7wvbbLWMeoJ/Mmti7tg6LGHbQ00tvLRUH8Ixw7q/
uuTzKSXNzGN4pTMDdAffPpXk7xPnoRXuckYPUVzfizTk8gsqKCpByoArpweK9n7ttyK1Pn1M/
wrpMsa7n+UHT3b698V0RFM0i682GN/Uc/
Udas0LY4icpTd+hpTsloVpYLYMrAEHsa5a+8HBnJRgAexrr9tNxU0606fwsqcIz3JAtK3CkntT65vxtcs
gsLv3Hq0ceuP8ivSYjka+ozXXjk48sFsjoJtceqgQLTUFTKteazS4KtSAUoFPVaLkNiBav6da7jk9BVeJ
oOkIruEYNadroHAZCRkYB4P4100gysokAG5Q2FK52njP3T90jvjitI3tdmdfDxTfIzfoqvb3G/
lex2sCMYqxVKzORpp2YULRScRDTVO71GKPO91BAyRnn8gnu7tYxl2Cj3ry7Wdt1enY4EbFTzkbseh7d4
aN810juYTPLL12oh+7y2SPXIqeGd0YLKODwDnIZ9av2qgIoHQAafTFMvotyEd8HH+92rK9pezlFW9PeE6
rj+tb4FZPixM2svsAf1FaUH+8j6mVT4WcB4UuCJMZ6givU9KfdEh9sflXxejSYLH1r1vwy+YfoxFenmL
NKT5ndHdhqc6C5pNcrN2yjZ1F1CP3q/LKg/5aDjP445resHd0jdSucknjCuPUjqp/
```

Le fichier task.txt ne nous fut pas facile à saisir mais l'encodage ressemblait à du base64.



La signature d'un fichier jpg. Waah. Nous téléchargeons donc cet output.

C'est une photo de M. Chat et de son amouruse [j'ai oublié le prénom de la lapine, anyway].
Ah, toujours pas de flag pour nous mais nous sommes quand même sur la bonne voie.



Nous utilisons donc nos outils habituels parmi lesquels **stegseek** le géant a fait le miracle

```
([redacted] ~) -[~/myHome/CTFs/LoveCTF/jesus_love]
$ stegseek download.jpg
StegSeek 0.6 per https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "inlove1"
[i] Original filename: "flag.txt".
[i] Extracting to "download.jpg.out".
    cyrmevi@gmail.com

([redacted] ~) -[~/myHome/CTFs/LoveCTF/jesus_love]
$ tree
.
├── Be_faithful.php
├── download.jpg
├── download.jpg.out
├── Jesus_love
│   ├── task.txt
│   └── zip_hash.txt
└── 2 directories, 5 files

([redacted] ~) -[~/myHome/CTFs/LoveCTF/jesus_love]
$ file download.jpg.out
download.jpg.out: ASCII text

([redacted] ~) -[~/myHome/CTFs/LoveCTF/jesus_love]
$ cat download.jpg.out
LoveCTF{T0d4y_1s_V4l3nt1n3_d4y_b4t_4150_45H_W3dn35d4y}
```