

Writeup: What is File Hash Value

HACK THE PODS CTF 第2回
作問者：嶋田壮志

1. 説明文

最近のアニメのタイトルを集めたフォルダを作ったぜ！

flagはわかりやすく、最も面白いアニメだ！

正解した諸君はぜひ見てくれよな！

FLAG's hash (MD5) = "3be411253acc83115f8f5397c445947f"

FLAG's hash (SHA1) = "fad15df0dac516d888652cd494926a82be0a582d"

2. 共有されるファイル

- flags.zip
 - 多くのフラグが格納されているフォルダの圧縮ファイル

2. 共有されるファイル

286個あるみたいですね(絶望)

```
% ls
flag000.txt flag032.txt flag064.txt flag096.txt flag128.txt flag160.txt flag192.txt flag224.txt flag256.txt
flag001.txt flag033.txt flag065.txt flag097.txt flag129.txt flag161.txt flag193.txt flag225.txt flag257.txt
flag002.txt flag034.txt flag066.txt flag098.txt flag130.txt flag162.txt flag194.txt flag226.txt flag258.txt
flag003.txt flag035.txt flag067.txt flag099.txt flag131.txt flag163.txt flag195.txt flag227.txt flag259.txt
flag004.txt flag036.txt flag068.txt flag100.txt flag132.txt flag164.txt flag196.txt flag228.txt flag260.txt
flag005.txt flag037.txt flag069.txt flag101.txt flag133.txt flag165.txt flag197.txt flag229.txt flag261.txt
flag006.txt flag038.txt flag070.txt flag102.txt flag134.txt flag166.txt flag198.txt flag230.txt flag262.txt
flag007.txt flag039.txt flag071.txt flag103.txt flag135.txt flag167.txt flag199.txt flag231.txt flag263.txt
flag008.txt flag040.txt flag072.txt flag104.txt flag136.txt flag168.txt flag200.txt flag232.txt flag264.txt
flag009.txt flag041.txt flag073.txt flag105.txt flag137.txt flag169.txt flag201.txt flag233.txt flag265.txt
flag010.txt flag042.txt flag074.txt flag106.txt flag138.txt flag170.txt flag202.txt flag234.txt flag266.txt
flag011.txt flag043.txt flag075.txt flag107.txt flag139.txt flag171.txt flag203.txt flag235.txt flag267.txt
flag012.txt flag044.txt flag076.txt flag108.txt flag140.txt flag172.txt flag204.txt flag236.txt flag268.txt
flag013.txt flag045.txt flag077.txt flag109.txt flag141.txt flag173.txt flag205.txt flag237.txt flag269.txt
flag014.txt flag046.txt flag078.txt flag110.txt flag142.txt flag174.txt flag206.txt flag238.txt flag270.txt
flag015.txt flag047.txt flag079.txt flag111.txt flag143.txt flag175.txt flag207.txt flag239.txt flag271.txt
flag016.txt flag048.txt flag080.txt flag112.txt flag144.txt flag176.txt flag208.txt flag240.txt flag272.txt
flag017.txt flag049.txt flag081.txt flag113.txt flag145.txt flag177.txt flag209.txt flag241.txt flag273.txt
flag018.txt flag050.txt flag082.txt flag114.txt flag146.txt flag178.txt flag210.txt flag242.txt flag274.txt
flag019.txt flag051.txt flag083.txt flag115.txt flag147.txt flag179.txt flag211.txt flag243.txt flag275.txt
flag020.txt flag052.txt flag084.txt flag116.txt flag148.txt flag180.txt flag212.txt flag244.txt flag276.txt
flag021.txt flag053.txt flag085.txt flag117.txt flag149.txt flag181.txt flag213.txt flag245.txt flag277.txt
flag022.txt flag054.txt flag086.txt flag118.txt flag150.txt flag182.txt flag214.txt flag246.txt flag278.txt
flag023.txt flag055.txt flag087.txt flag119.txt flag151.txt flag183.txt flag215.txt flag247.txt flag279.txt
flag024.txt flag056.txt flag088.txt flag120.txt flag152.txt flag184.txt flag216.txt flag248.txt flag280.txt
flag025.txt flag057.txt flag089.txt flag121.txt flag153.txt flag185.txt flag217.txt flag249.txt flag281.txt
flag026.txt flag058.txt flag090.txt flag122.txt flag154.txt flag186.txt flag218.txt flag250.txt flag282.txt
flag027.txt flag059.txt flag091.txt flag123.txt flag155.txt flag187.txt flag219.txt flag251.txt flag283.txt
flag028.txt flag060.txt flag092.txt flag124.txt flag156.txt flag188.txt flag220.txt flag252.txt flag284.txt
flag029.txt flag061.txt flag093.txt flag125.txt flag157.txt flag189.txt flag221.txt flag253.txt flag285.txt
flag030.txt flag062.txt flag094.txt flag126.txt flag158.txt flag190.txt flag222.txt flag254.txt
flag031.txt flag063.txt flag095.txt flag127.txt flag159.txt flag191.txt flag223.txt flag255.txt
```

2. 共有されるファイル

一つ一つがflagファイルとなっているが、全て中身が違うもの(全部アニメタイトル)

```
babyblue0@babyblue0-ctf ~/Desktop/htpctf/What_is_File_Hash_Value/flags
% cat flag001.txt
http-ctf{Diary_of_Our_Days_at_the_Breakwater}%
babyblue0@babyblue0-ctf ~/Desktop/htpctf/What_is_File_Hash_Value/flags
% cat flag002.txt
http-ctf{Major_2nd}%
babyblue0@babyblue0-ctf ~/Desktop/htpctf/What_is_File_Hash_Value/flags
% cat flag003.txt
http-ctf{Non_Non_Biyori_Nonstop}%
babyblue0@babyblue0-ctf ~/Desktop/htpctf/What_is_File_Hash_Value/flags
% cat flag004.txt
http-ctf{Shikizakura}%
babyblue0@babyblue0-ctf ~/Desktop/htpctf/What_is_File_Hash_Value/flags
% cat flag005.txt
http-ctf{The_Day_I_Became_a_God}%
```

3. Writeup

問題文には、md5とsha1のハッシュ値がそれぞれあるようです。

そもそもFile Hashとは？

ファイルの改ざんを検知するための仕組み。

ハッシュ値は、オリジナルが1Bitでも変わったら全く違うHash値を生成するという特徴がある。

データ提供者は、データとそのハッシュを提示し、

受給者は、ダウンロードしたデータからハッシュを生成し提供者のものと比較することで完全性を確保する。

3. Writeup

データ提供者



hash: aaa

データとハッシュ値を提供

データ受給者



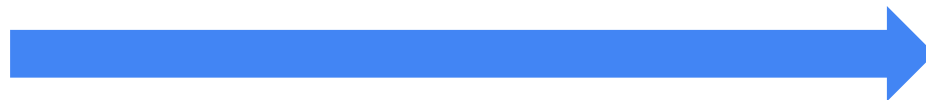
3. Writeup

データ提供者

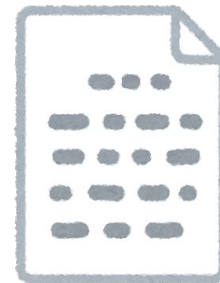


hash: aaa

データとハッシュ値を提供

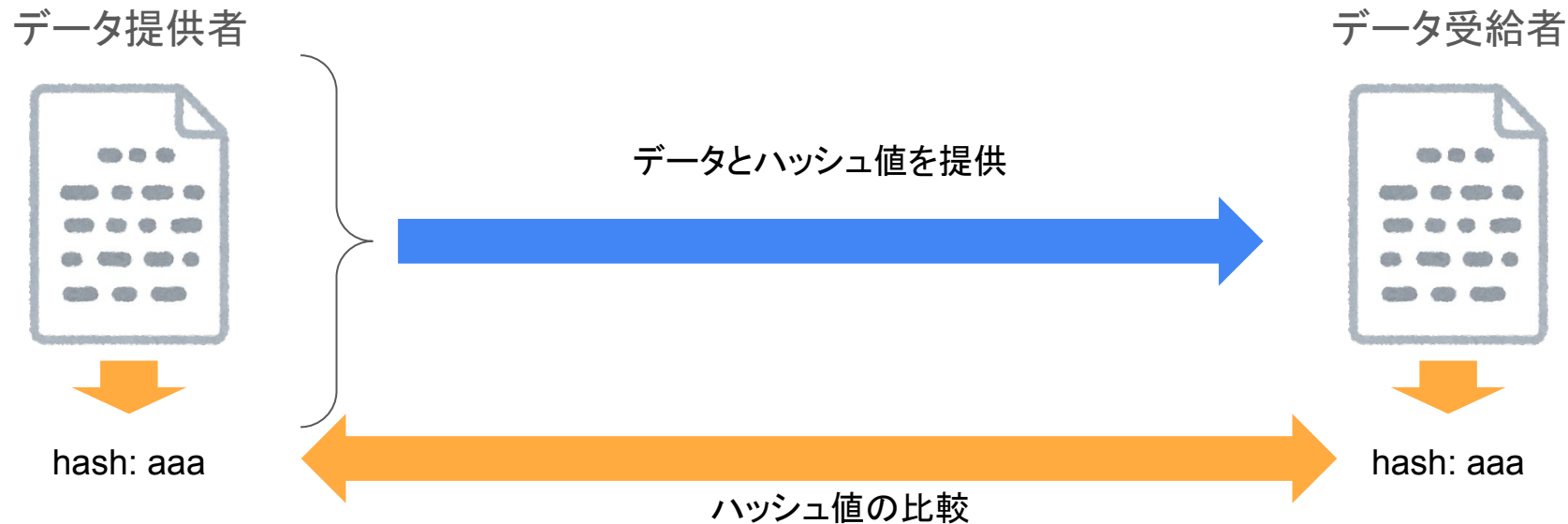


データ受給者



hash: aaa

3. Writeup



3. Writeup

つまり、

提供されたHashからflagを特定するのがこの問題の趣旨！

File Hashを計算するツールはlinuxでプリインストールされているので、それを使うだけでこの問題は解けます。

- md5sum
- sha1sum

Windowsでは、「HashMyFiles」ってツールもありますね。

3. Writeup

両方のHashを確認してみると、、

```
babyblue0@babyblue0-ctf ~/Desktop/httpctf/What_is_File_Hash_Value/flags
% md5sum * | grep 3be411253acc83115f8f5397c445947f
3be411253acc83115f8f5397c445947f  flag061.txt
babyblue0@babyblue0-ctf ~/Desktop/httpctf/What_is_File_Hash_Value/flags
% sha1sum * | grep fad15df0dac516d888652cd494926a82be0a582d
fad15df0dac516d888652cd494926a82be0a582d  flag061.txt
```

「**flag061.txt**」というファイルがヒットする。

内容を見てみると、、

```
% cat flag061.txt
http-ctf{Kaguya-sama: _Love_Is_War}%
```

3. Writeup

flag: **http-ctf{Kaguya-sama:_Love_Is_War}**

flag元ネタ:「かぐや様は告らせたい
～天才たちの恋愛頭脳戦～」

恋愛モノに見せかけた、ギャグアニメ。

OP神、ED神、キャラソン神。

今世紀最高の神アニメ。**異論は認めん。**



4. おまけ

flagファイルの286個、
全部手作業、、ではなく、スクリプトで出力している。

参考にしたのは、海外wikiのアニメリスト(2020、2021年)

https://en.wikipedia.org/wiki/2020_in_anime#Television_series

https://en.wikipedia.org/wiki/2021_in_anime#Television_series

4. おまけ

画面表示上はこのようになっている

Television series [\[edit \]](#)

A list of [anime television series](#) that debuted between January 1 and December 31, 2020.

First run start and end dates ↕	Title ↕	Episodes ↕	Studio ↕	Director(s) ↕	Original title ↕	Ref
January 3 – March 27	<i>Asteroid in Love</i>	12	Doga Kobo	Daisuke Hiramaki	<i>Koisuru Asteroid</i>	[38]
January 3 – March 20	<i>Darwin's Game</i>	11	Nexus	Yoshinobu Tokumoto		[39]
January 4 – March 28	<i>Magia Record: Puella Magi Madoka Magica</i>	13	Shaft	Gekidan Inu Curry	<i>Magia Record: Mahō Shōjo Madoka Magika</i>	[40]

4. おまけ

ここのEdit画面を見てみると、


フォーマットが決まっているみたい！


アニメのタイトルは、







"[[TITLE]]"

という形式で表される。

Editing 2020 in anime (section)


















 **You are not logged in.** Your IP address will be publicly visible if you make any edits. If you [log in](#) or [create an account](#), your edits will be attributed to a user name, among [other benefits](#).

 Content that *violates any copyrights* will be deleted. Encyclopedic content must be *verifiable*. Any work submitted to Wikipedia can be edited, used, and redistributed—by anyone—subject to *certain terms and conditions*.

B *I*      > [Advanced](#) > [Special characters](#) > [Help](#) > [Cite](#) 

===Television series===
A list of anime television series that debuted between January 1 and December 31, 2020.

{| class="wikitable sortable" border="1"
|-
! data-sort-type="text" width="150px" | First run start and end dates
! width="450px" | Title
! data-sort-type="text" width="10px" | Episodes
! data-sort-type="text" width="130px" | Studio
! data-sort-type="text" width="180px" | Director(s)
! Original title
! class="unsortable" width="5px" | Ref
|-
<!-- use the following template for new entries
|-
| AIRDATES
| ''[[TITLE]]''
| EPISODECOUNT
| [[STUDIO]]
| [[DIRECTOR]]
| ALT
| REFS
-->
|-
|{{dts|January 3}} - {{dts|March 27}}

Insert                 

Cite your sources:

Edit summary (Briefly describe your changes)

/* Television series */

By publishing changes, you agree to the [Terms of Use](#), and you irrevocably agree to release your contribution under the [CC BY-SA 3.0 License](#) and the [GFDL](#). You agree that a hyperlink or URL is sufficient attribution under the Creative Commons license.

Publish changes

Show preview

Show changes

Cancel

4. おまけ

なので、正規表現でアニメのタイトルだけを抜き出して、
出力するスクリプトをpythonで記述した。

```
1  #!python3
2  import re
3  import sys
4
5  anims = sys.argv[1]
6  with open( anims, mode="r") as f:
7      lines = f.readlines()
8
9      for line in lines:
10         res = re.findall("'\\[\\[ (? : . * \\ ) ? ( . * ) \\ ] ]'", line )
11         if len(res):
12             print( res[0] )
```

```
babyblue0@babyblue0-ctf ~/Desktop/httpctf/What_is_File_Hash_Value/create
% ./pull_anime.py ./animes2020.txt >> anime_list.txt
babyblue0@babyblue0-ctf ~/Desktop/httpctf/What_is_File_Hash_Value/create
% ./pull_anime.py ./animes2021.txt >> anime_list.txt
```


4. おまけ

あとはflagの形に変換して、
個々のファイルを生成する。

```
5 #!python3
4
3 flags = []
2
1 flag_str = "Kaguya-sama:_Love_Is_War"
6 flag_file = ""
1
2 with open( "./anime_list.txt", mode="r" ) as f:
3     lines = f.readlines()
4     for line in lines:
5         flags.append( line.replace(' ', '_').replace('\n', '') )
6
7 #重複削除
8 flags = list(set(flags))
9
10 for i,flag in enumerate( flags ):
11     full_flag = "http-ctf{" + flag + "}"
12     filename = "flag{:03}.txt".format( i )
13
14     if flag == flag_str:
15         flag_file = filename
16
17     with open( "./flags/"+filename, mode="w" ) as f:
18         f.write( full_flag )
19         print("Write flag: %s ( flags/%s )" % ( full_flag, filename ) )
20
21 print( "*****\
22         flagfile is: %s"%flag_file )
23
```

4. おまけ

```
babyblue0@babyblue0-ctf ~/Desktop/httpctf/What_is_File_Hash_Value/
% mkdir flags
babyblue0@babyblue0-ctf ~/Desktop/httpctf/What_is_File_Hash_Value/
% ./create.py
Write flag: http-ctf{Oda_Cinnamon_Nobunaga} ( flags/flag000.txt )
Write flag: http-ctf{BNA:_Brand_New_Animal} ( flags/flag001.txt )
Write flag: http-ctf{Ōsama_Ranking} ( flags/flag002.txt )
Write flag: http-ctf{The_World's_Finest_Assassin_Gets_Reincarnated}
Write flag: http-ctf{Magatsu_Wahrheit_-Zuerst-} ( flags/flag004.tx
write flag: http-ctf{The_World_Ends_with_You:_The_Animation} ( flags/flag
Write flag: http-ctf{Gleipnir} ( flags/flag283.txt )
Write flag: http-ctf{Tomica_Kizuna_Mode_Combine_Earth_Granner} ( flags/fl
Write flag: http-ctf{Adachi_and_Shimamura} ( flags/flag285.txt )
*****
flagfile is: flag195.txt
babyblue0@babyblue0-ctf ~/Desktop/httpctf/What_is_File_Hash_Value/create
% cat flags/flag195.txt
http-ctf{Kaguya-sama:_Love_Is_War}%
```

結論:Pythonすげー