GOT HAPPENS {Writeup}

Title: Got happens Writeup - Medium

Author: // Paul Jeremiah

Category : Forensics

Description:

> Got Is EveryWhere!

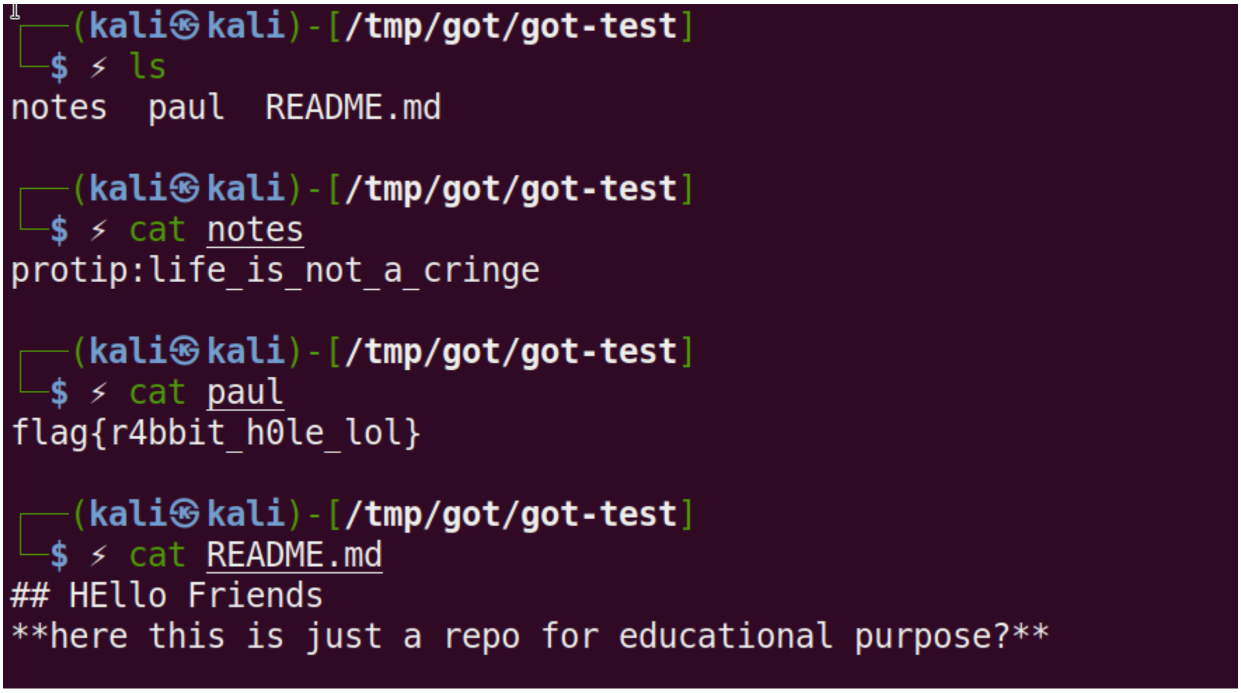
> please checkit out my cool repo which contains nothing to be useful :) and star it !
>
> > 1.clone the repo
> > 2.please do time travel
> > `#enummore` `#tryharder`

Given : https://github.com/0xcyberpj/got-test

Walkthrough:

btw got is nothing but git Right!

- Clone the given link
- `sudo git clone https://github.com/0xcyberpj/got-test`



```
┌──(kali㉿kali)-[/tmp/got/got-test]
└─$ ⚡ ls
notes  paul  README.md

┌──(kali㉿kali)-[/tmp/got/got-test]
└─$ ⚡ cat notes
protip:life_is_not_a_cringe

┌──(kali㉿kali)-[/tmp/got/got-test]
└─$ ⚡ cat paul
flag{r4bbit_h0le_lol}

┌──(kali㉿kali)-[/tmp/got/got-test]
└─$ ⚡ cat README.md
## HEllo Friends
**here this is just a repo for educational purpose?**
```

- *just some fake flags and so*

as Description says lets check logs

```
┌──(kali㉿kali)-[/tmp/got/got-test]
└─$ ⚡git log                                                                                    130 ×
commit dd1ad56d0bddb4578e2a5d17b73f0ef196a873ec (HEAD -> main, origin/main, origin/HEAD)
Author: Kali <kali@kali>
Date:   Sun Aug 1 11:07:39 2021 -0400

    none

commit 5a3ef2dc2bf036d147cb70694bee96029ff70096
Author: Kali <kali@kali>
Date:   Sun Aug 1 11:03:41 2021 -0400

    none

commit 17ae13123d760c69b2d71ed12934094c0640c4c9
Author: root <root@kali>
Date:   Sun Aug 1 10:59:33 2021 -0400


etc................
```

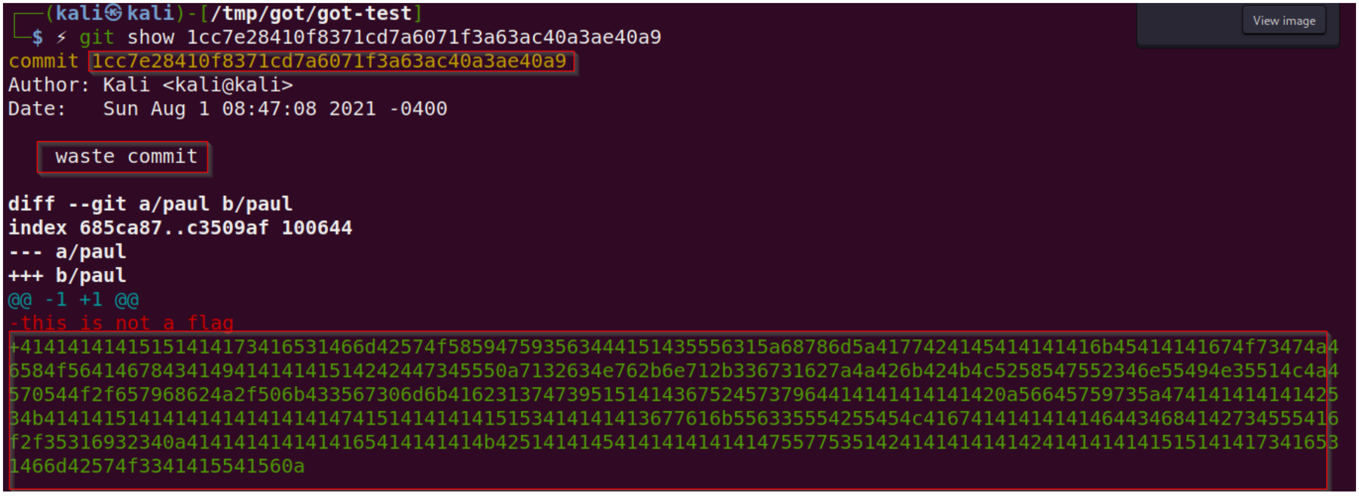
check every log

```
 ┌──(kali㉿kali)-[/tmp/got/got-test]
└─$ ⚡git show 17ae13123d760c69b2d71ed12934094c0640c4c9
commit 17ae13123d760c69b2d71ed12934094c0640c4c9
Author: root <root@kali>
Date:   Sun Aug 1 10:59:33 2021 -0400

    hello world
diff --git a/notes b/notes
index 9635f44..94f01f2 100644
--- a/notes
+++ b/notes
@@ -1,2 +1 @@
-protip:life_is_not_a_cringe
-
+}g4lf_3k4f{FTClimaT

┌──(kali㉿kali)-[/tmp/got/got-test]
└─$ ⚡echo "+}g4lf_3k4f{FTClimaT"|rev
TamilCTF{f4k3_fl4g}+
lol
```

fake flag alert



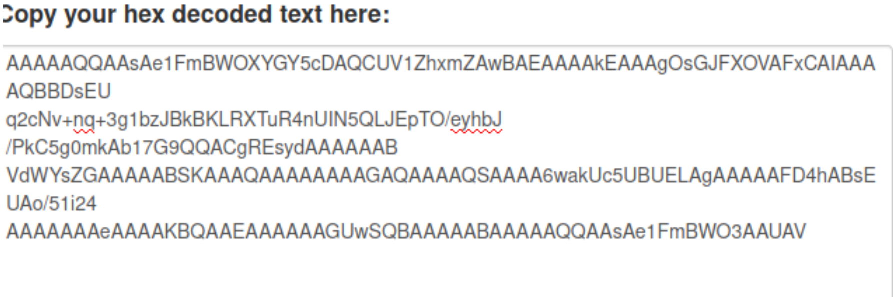
```
┌──(kali㉿kali)-[/tmp/got/got-test]
└─$ ⚡ git show 1cc7e28410f8371cd7a6071f3a63ac40a3ae40a9
commit 1cc7e28410f8371cd7a6071f3a63ac40a3ae40a9
Author: Kali <kali@kali>
Date:   Sun Aug 1 08:47:08 2021 -0400

    waste commit

diff --git a/paul b/paul
index 685ca87..c3509af 100644
--- a/paul
+++ b/paul
@@ -1 +1 @@
-this is not a flag
+41414141415151414173416531466d42574f585947593563444151435556315a68786d5a4177424145414141416b45414141674f73474a4
6584f5641467843414941414141514242447345550a7132634e762b6e712b336731627a4a426b424b4c5258547552346e55494e35514c4a4
570544f2f657968624a2f506b433567306d6b41623137473951514143675245737964414141414141420a56645759735a474141414141425
34b41414151414141414141414141474151414141415153414141413677616b5563355542554 54c41674141414141464434684142734555416
f2f35316932340a414141414141416541414141 4b425141414541414141414141475577535142414141414142414141414141515141417341653
1466d42574f3341415541560a
```

Interesting , lets start →

1.hex→ decode



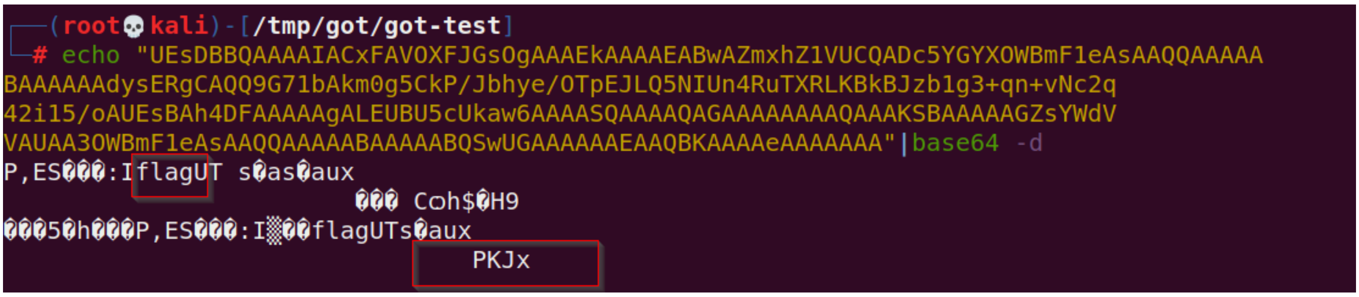
Copy your hex decoded text here:

```
AAAAAQQAAsAe1FmBWOXYGY5cDAQCUV1ZhxmZAwBAEAAAAkEAAAgOsGJFXOVAFxCAIAAA
AQBBDsEU
q2cNv+nq+3g1bzJBkBKLRXTuR4nUIN5QLJEpTO/eyhbJ
/PkC5g0mkAb17G9QQACgREsydAAAAAAB
VdWYsZGAAAAABSKAAAQAAAAAAAAGAQAAAAQSAAAA6wakUc5UBUELAgAAAAAFD4hABsE
UAo/51i24
AAAAAAAeAAAAKBQAAEAAAAAAGUwSQBAAAAABAAAAAQQAAsAe1FmBWO3AAUAV
```

seems base64 ?

- But the things here is , its just *reversed* you can see
- so what ? , → **again rev it**

```
┌──(root💀kali)-[/tmp/got/got-test]
└─# echo "AAAAAQQAAsAe1FmBWOXYGY5cDAQCUV1ZhxmZAwBAEAAAAkEAAAgOsGJFXOVAFxCAIAAAAQBBDsEU
q2cNv+nq+3g1bzJBkBKLRXTuR4nUIN5QLJEpTO/eyhbJ/PkC5g0mkAb17G9QQACgREsydAAAAAAB
VdWYsZGAAAAABSKAAAQAAAAAAAAGAQAAAAQSAAAA6wakUc5UBUELAgAAAAAFD4hABsEUAo/51i24
AAAAAAAeAAAAKBQAAEAAAAAAGUwSQBAAAAABAAAAAQQAAsAe1FmBWO3AAUAV
"|rev
UEsDBBQAAAAIACxFAVOXFJGsOgAAAEkAAAAEABwAZmxhZ1VUCQADc5YGYXOWBmF1eAsAAQQAAAAA
BAAAAAAdysERgCAQQ9G71bAkm0g5CkP/Jbhye/OTpEJLQ5NIUn4RuTXRLKBkBJzb1g3+qn+vNc2q
42i15/oAUEsBAh4DFAAAAAgALEUBU5cUkaw6AAAASQAAAAQAGAAAAAAAAAQAAAKSBAAAAAGZsYWdV
VAUAA3OWBmF1eAsAAQQAAAAABAAAAABQSwUGAAAAAAEAAQBKAAAAeAAAAAAA
```



```
┌──(root💀kali)-[/tmp/got/got-test]
└─# echo "UEsDBBQAAAAIACxFAVOXFJGsOgAAAEkAAAAEABwAZmxhZ1VUCQADc5YGYXOWBmF1eAsAAQQAAAAA
BAAAAAAdysERgCAQQ9G71bAkm0g5CkP/Jbhye/OTpEJLQ5NIUn4RuTXRLKBkBJzb1g3+qn+vNc2q
42i15/oAUEsBAh4DFAAAAAgALEUBU5cUkaw6AAAASQAAAAQAGAAAAAAAAAQAAAKSBAAAAAGZsYWdV
VAUAA3OWBmF1eAsAAQQAAAAABAAAAABQSwUGAAAAAAEAAQBKAAAAeAAAAAAA"|base64 -d
P,ES���:IflagUT s�as�aux
                            ��� Coh$�H9
���5�h���P,ES���:I▒��flagUTs�aux
                       PKJx
```

Yeah ——→ Go ahead

```
┌──(root💀kali)-[/tmp/got/got-test]
└─# echo "UEsDBBQAAAAIACxFAVOXFJGsOgAAAEkAAAAEABwAZmxhZ1VUCQADc5YGYXOWBmF1eAsAAQQAAAAA        1 ×
BAAAAAAdysERgCAQQ9G71bAkm0g5CkP/Jbhye/OTpEJLQ5NIUn4RuTXRLKBkBJzb1g3+qn+vNc2q
42i15/oAUEsBAh4DFAAAAAgALEUBU5cUkaw6AAAASQAAAAQAGAAAAAAAAAQAAAKSBAAAAAGZsYWdV
VAUAA3OWBmF1eAsAAQQAAAAABAAAAABQSwUGAAAAAAEAAQBKAAAAeAAAAAAA"|base64 -d > from_base.zip
```

```
┌──(root💀kali)-[/tmp/got/got-test]
└─# file from_base.zip
from_base.zip: Zip archive data, at least v2.0 to extract
```

- unzip & cat the flag

```
cat flag
54616d696c4354467b315f6c3076335f6731375f776834375f61623075745f7930757d0a
```

```
>>>flag="54616d696c4354467b315f6c3076335f6731375f776834375f61623075745f7930757d0a"
>>>bytearray.fromhex(flag).decode()
>>>'TamilCTF{1_l0v3_g17_wh47_ab0ut_y0u}'
```

Done
Flag:TamilCTF{1_l0v3_g17_wh47_ab0ut_y0u}

Thats all