CTF-攻防世界-MISC-高手进阶区(001-018 持续更新中...)



<u>CTF 专栏收录该内容</u> 14 篇文章 4 订阅

订阅专栏 马上就要进军CTF了,准备把MISC,CRYPTO,WEB的题目好好刷一下...

目录

MISC 高手进阶区

base64÷4

embarrass

神奇的Modbus

wireshark-1

pure_color

Aesop_secret

a_good_idea

Training-Stegano-1

can_has_stdio?

János-the-Ripper

Test-flag-please-ignore

快乐游戏题

Banmabanma

reverseMe

stage1

Hear-with-your-Eyes

What-is-this

MISCall

base64÷4

下载题目附件, 文本中只有一串字符串

666C61677B45333342374644384133423834314341393639394544444241323442363041417D

题目提示base64÷4=base16, 尝试使用base16解码

法一:编写python脚本

import base64

test="666C61677B45333342374644384133423834314341393639394544444241323442363041417D"

flag=base64.b16decode(test)

print(flag)

法二: 使用在线解码平台

https://www.qqxiuzi.cn/bianma/base.php?type=16

flag:

flag{E33B7FD8A3B841CA9699EDDBA24B60AA}

Base16编码是一个标准的十六进制字符串,它并不包含任何控制字符,以及Base64和Base32中的"="符号。

embarrass

下载zip附件,解压之后打开文件夹,发现文件misc_02.pcapng

法一: 使用linux系统下的string搜索命令 查找文件中flag

strings 文件名 | grep flag

;~/Desktop\$ strings misc_02.pcapng | grep flag GET /flag.doc HTTP/1.1 GET /flag.doc HTTP/1.1 flag{Good_b0y_W3ll_Done} flag{Good_b0y_W3ll_Done} flag{Good_b0y_W3ll_Done} flag{Good_b0y_W3ll_Done}

文件类型: Wireshark capture file (.pcapng)

法二:使用Wireshark 打开该文件,使用搜索功能搜索字符串flag

misc_02.pcapng		_ 0 X
文件(E) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分	/析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)	
▲ ■ ⊴ ◎ 👃 🖹 🗙 🖸 🔍 🖛 ⇒ 🖀 🤇	¥ 👤 🔲 @, Q, Q, II	
■ 应用显示过滤器 … 〈Ctrl-/〉		* 表达式… +
	▲ 分組字节流 ▼	取消
No. Time Source	Wireshark·分组 2766 · misc 02	1-2621
2761 182.214559 192.168.197.1 2762 182.214559 192.168.197.1 2763 182.215143 192.168.197.1 2764 182.215689 192.168.197.1 2765 182.216267 192.168.197.1 2766 182.216449 192.168.197.1 2768 182.216839 192.168.197.1 2768 182.216839 192.168.197.1 2769 182.218950 192.168.197.1 2770 182.218596 192.168.197.1	<pre>> Frame 2766: 32822 bytes on wire (262576 bits), 32822 bytes captured (26 > Ethernet II, Src: Vmware_b2:75:e0 (00:0c:29:b2:75:e0), Dst: Vmware_c0:0 > Internet Protocol Version 4, Src: 192.168.197.128, Dst: 192.168.197.1 > Transmission Control Protocol, Src Port: 52176, Dst Port: 3360, Seq: 45 FTP Data (32768 bytes data) </pre>	= 2621 = 2621
2772 182.219172 192.168.197.1 > Frame 2766: 32822 bytes on wire > Ethernet II, Src: Vmware_b2:75: > Internet Protocol Version 4, Sr > Transmission Control Protocol, FTP Data (32768 bytes data)	0830 00 01 00 <	=2621 •
● ℤ FTP Data (ftp-data), 32768 字节	III A A A A A A A A A A A A A A A A A A	置文件: Default

flag{Good_b0y_W3ll_Done}

神奇的Modbus

题目描述:寻找flag,提交格式为sctf{xxx}

发现还是.pcapng的文件,继续使用Wireshark打开,搜索 sctf字符串

文件(F) 编辑(E) 视图(V) 跳技(G) 捕获(C) 分析(A) 统计(S) 电活(Y) 无线(W) 工具(T) 帮助(H)	
📶 🗐 🖉 🔍 🖹 🛪 🗖 🔽 📥 🛥 🐔 👱 🖵 🥅 🔍 🔍 🤉 🏦	
■ cmm===================================	表达式… ↓
分組字节流 マ	查找 取消
No. Time Source Destination Protocol Length Info	
4954 2480.214 192.168.130.130 192.168.130.1 Modbus 103 Response: Trans:	1; Unit: 1,
4955 2480.255 192.168.130.1 192.168.130.130 TCP 54 62234→502 [ACK] Seq=1	1353 Ack=1610
4956 2480.966 192.168.130.1 239.255.250 SSDP 216 M-SEARCH * HTTP/1.1	
4957 2484.583 192.168.130.1 192.168.130.130 Modbus 66 Query: Trans:	1; Unit: 1,
4958 2484.583 192.168.130.130 192.168.130.1 Modbus 65 Response: Trans:	1; Unit: 1,
4959 2484.624 192.168.130.1 192.168.130.130 TCP 54 62234→502 [ACK] Seq=1	1365 Ack=1611
4960 2484.924 192.168.130.1 192.168.130.130 SSH 106 Client: Encrypted pac	ket (len=52)
4961 2484.924 192.168.130.130 192.168.130.1 TCP 60 22→61957 [ACK] Seq=1	Ack=2185 Win=
4962 2486.496 192.168.130.1 192.168.130.130 Modbus 66 Query: Trans:	1; Unit: 1, 🔻
[Request Frame: 4953]	
Byte Count: 40	
Register 0 (UINT16): 115	1
Register 1 (UINT16): 99	
Register 2 (UINT16): 116	
Register 3 (UINT16): 102	
Builder & Dimited . and	-
0020 82 01 01 f6 f3 1a ab 23 23 f9 fd ff 70 66 50 18# #pfP.	^
0030 00 e5 39 18 00 00 00 01 00 00 02 b01 03 28 009	
0040 73 00 63 00 74 00 66 00 7b 00 45 00 61 00 73 00 s.c.t.t. { [.E.a.s.	=
0050 /9 00 5T 00 40 00 64 00 62 00 /5 00 /3 00 /d 00 yM.d. D.U.S.}	

得到flag: sctf{Easy_Mdbus}

失败了!!!

发现题目名称是"神奇的Modbus",加上字母o,sctf{Easy_Modbus},尽然过了,不懂,应该是题目本身的问题

flag:

wireshark-1

题目描述:黑客通过wireshark抓到管理员登陆网站的一段流量包(管理员的密码即是答案)。flag提交形式为 flag{XXXX}

继续用Wireshark打开该文件,题目给出提示管理员密码,尝试搜索字符串password



flag:

flag{ffb7567a1d4f4abdffdb54e022f8facd}

pure_color

下载附件,得到一张图片,空白,可能使用了图片隐写

这里需要用到StegSolve工具,将隐写在图片中的内容显示出来

下载地址:

http://www.caesum.com/handbook/Stegsolve.jar(需要java环境)



flag{true_steganographers_doesnt_need_any_tools}

Aesop_secret

下载附件,得到一张gif图片,考虑对该gif图片进行帧拆分

用gif分解网站分解

http://ezgif.com/split

い「火」正式品	(拆分器)			
作物 调整大小 1				
-16				
文件大小: 6.35KiB ,到	宽度:124px, 高度: 70px, 帧数: 9	, 类型: gif 兑换 ●		
拆分选项: 以PNG格式输出图像	~			
拆分为前门				
אארפל בלאני:				
分割图像:				
分割图像:	realization	H HINNA HANNA Salahan Hanna Salahan Hanna	27.000-14 8.00014	
分割图像:	Salara Sector	E canada compositiva Manda compositiva Securitoria Securitoria	NTA GENERA Status Status Status Status Status Status	
分割图像: ゴロ 旧職		i antoni na posta de la compositiva de la compo	Provinces States Provinces Provinces	
		Stream and a second	nor, dan ne Secondaria Secondaria Researching	

得到8张图片,明显可以拼接成一张图



使用截图和画图板进行图片拼接,得到以下图像



https://blog.csdn.net/weixin 43252204

是四个字母**ISCC**,貌似也没有关于flag的相关信息,使用winhex或者记事本打开该gif图片,分析其源码,发现 在文本的结尾有一串类似编码的字符串



U2FsdGVkX19QwGkcgD0fTjZxgijRzQOGbCWALh4sRDec2w6xsY/ux53Vuj/AMZBDJ87qyZL5kAf1fmAH4Oe13lu435bfRE

尝试对其进行base-64解码,得到的结果乱码

看题目名称"Aesop_secret"猜测可能是

aes解密: https://www.sojson.com/encrypt_aes.html

密钥前面得到的ISCC,两次解密之后得到flag

flag:

a_good_idea

下载附件,解压之后发现是一张图片



使用winhex分析该图片,发现存在压缩文件,更改后缀名为.zip

Aesop.gif a_ve	ery_	goo	d_id	ea.jp	og 📋												
Offset	0	1	2	3	4	- 5	6	7	8	9	Α	В	С	D	Е	F	ANSI ASCII
00007D80	BC	\mathbf{FC}	\mathbf{FB}	\mathbf{FD}	CE	Α7	A2	\mathbf{FD}	0D	68	\mathbf{FC}	80	F9	6F	E1	8F	¼üûýΧ¢ý hü ùoá
00007D90	\mathbf{FC}	81	EC	FE	Α7	FF	00	41	15	D1	27	FA	BF	\mathbf{FB}	63	17	ü ìþ§ÿ A Ñ'ú;ûc
00007DA0	F3	6A	28	AF	CE	9F	C2	68	35	3E	FA	$\mathbf{F}\mathbf{D}$	17	F9	54	97	ój([−] ΟÂh5>úý ùT−
00007DB0	5F	F1	EB	FF	00	00	FE	86	8A	29	47	74	03	AE	7F	E3	_ñëÿ þ†Š)Gt & ã
00007DC0	F3	F1	6F	E5	4E	6E	A7	\mathbf{FD}	EF	Ε9	45	15	75	в7	01	D6	óñoåNn§ýïéE u• Ö
00007DD0	FF	00	F1	EE	FF	00	56	A 0	FF	00	C7	AC	7F	F5	CA	8A	ÿ ñîÿ V ÿ Ǭ õÊŠ
00007DE0	2в	5A	9F	02	F9	19	C7	E2	22	8F	EF	0F	F7	05	36	7F	+ZŸ ù Çâ" ï ÷ 6
00007DF0	F5	Α9	F4	3F	CA	8A	2в	94	D0	8B	5A	FF	00	90	4D	C7	õ©ô?ÊŠ+″Ð <zÿ mç<="" td=""></zÿ>
00007E00	\mathbf{FD}	74	4F	E4	D5	C5	DC	7F	0F	D7	FA	0A	28	A0	52	D8	ýtOäÕÅÜ ×ú (RØ
00007E10	E8	21	$\mathbf{F}\mathbf{F}$	00	54	BF	41	45	14	57	41	07	$\mathbf{F}\mathbf{F}$	D9	50	4B	è! <u>ÿ</u> T;AE WA ÿÙPK
00007E20	03	04	0A	00	00	00	00	00	FC	03	72	4F	00	00	00	00	ürO
00007E30	00	00	00	00	00	00	00	00	05	00	00	00	6D	69	73	63	misc
00007E40	2F	50	4B	03	04	14	00	00	00	80	00	C4	03	72	4F	90	/PK ÄrO
00007E50	FE	42	22	22	00	00	00	20	00	00	00	0D	00	00	00	6D	þB "" m
00007E60	69	73	63	2F	68	69	6E	74	2E	74	78	74	2в	29	AA	54	isc/hint.txt+) ^a T
00007E70	28	C9	57	48	СВ	CC	4B	51	28	C9	48	55	28	4E	4D	2E	(ÉWHËÌKQ(ÉHU(NM.
00007E80	4A	2D	51	C8	4F	53	28	C8	AC	48	CD	29	06	00	50	4B	J-QÈOS(ȬHÍ) PK
00007E90	03	04	14	00	00	00	08	00	A7	01	72	4F	CC	E7	29	D5	§ rOÌç)Õ
00007EA0	D2	F4	01	00	C8	F4	01	00	0B	00	00	00	6D	69	73	63	Òô Èô misc
00007EB0	2F	74	6F	2E	70	6E	67	00	52	80	AD	7F	89	50	4E	47	/to.png R€- %PNG
00007EC0	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	00	00	01	22	IHDR "
00007ED0	00	00	01	21	08	02	00	00	00	54	48	ЗA	4F	00	01	00	! TH:0
00007EE0	00	49	44	41	54	78	9C	7C	FD	D9	в6	DC	4A	8E	2D	0A	IDATxœ ýÙ¶ÜJŽ−
00007EF0	4E	00	66	24	BD	5B	BD	Α4	DD	44	44	66	9E	7в	C7	AD	N f\$¼[¼¤ÝDDfž{Ç-
00007F00	7A	AA	в7	\mathbf{FB}	FF	5F	51	2F	35	C6	A9	13	99	11	В1	3в	zª ûÿ_Q/5Æ© ™ ±;
00007F10	49	AB	F1	96	Α4	19	80	7A	00	C9	E5	D2	CE	53	3E	14	I≪ñ-¤ €z ÉåÒÎS>
00007F20	0A	\mathbf{DF}	4B	BE	E8	Α4	99	A1	9B	98	00	88	D6	FF	F7	FF	ßK¾è¤™;≻~^Öÿ÷ÿ
00007F30	F8	7F	FD	DF	DD	DD	FF	79	D6	8E	4A	0в	4F	39	35	EA	<u>φ γριιλόλο 0956</u>
Dage 73 of 756					Offe	ot.			7522	2				- 10		nck.	8E8 - 8E8 (

解压之后,得到以下文件,其中有一个暗时的文本文件



提示: try to find the secret of pixels(试着找出像素的秘密)

使用Stegsolve的combin功能分析这两张图片

打开第二张to_do.png图片,之后点击image Combiner,选择第一张图片to.png





连续更换,得到两图相减的图像,之后得到一张二维码,手机扫码即可得到flag



UT.NUT.NUT.NUT.NU

flag:

NCTF{m1sc_1s_very_funny!!!}

Training-Stegano-1

下载附件,得到一张图片,查看图片源码

steganol

有点坑,看到题目的提示还以为是图片隐写术的,用stegsolve工具跑了什么都没有,查看源码提示: Look what the hexedit revealed:(看看十六进制编辑揭示了什么)考虑到进制转换方面的,也失败了,最后看了wp,发现flag直接是steganol,而且flag的格式也和之前的不一样

can_has_stdio?

下载附件,解压之后用文本打开文件



wp得知是brainfuck语言,使用在线语言转换得到flag

http://esoteric.sange.fi/brainfuck/impl/interp/i.html



flag{esolangs_for_fun_and_profit}

János-the-Ripper

使用winhex打开,发现明显是一个压缩文件,修改后缀名,加压需要密码,使用ziperello工具破解

Offset	0	1	2	3	4	- 5	6	7	8	9	Α	в	C	D	E	F	ANSI ASCII
00000000	50	4B	03	04	14	00	03	00	08	00	0E	A2	77	44	44	D4	PK ¢wDDÔ
00000010	88	77	27	00	00	00	19	00	00	00	08	00	00	00	66	6C	^w' fl
00000020	61	67	2E	74	78	74	00	10	01	4B	93	\mathbf{FF}	03	EE	9C	FA	ag.txt K"ÿ îœú
00000030	D3	12	83	A1	57	88	57	8C	BF	41	AA	41	87	16	F6	85	ó f;W^WŒ;AªA‡ ö…
00000040	FE	40	02	DA	73	CA	1F	AC	16	97	89	44	ЗA	50	4B	01	þ@ ÚsÊ ¬ −‰D:PK
00000050	02	14	00	14	00	03	00	80	00	0E	A2	77	44	44	D4	88	¢wDDÔ^
00000060	77	27	00	00	00	19	00	00	00	80	00	00	00	00	00	00	w'
00000070	00	01	00	20	00	00	00	00	00	00	00	66	6C	61	67	2E	flag.
0800000	74	78	74	50	4B	05	06	00	00	00	00	01	00	01	00	36	txtPK 6
00000090	00	00	00	4D	00	00	00	00	00								MULTINE WEIXIN_45252204

ziperello下载:

链接: https://pan.baidu.com/s/1KW6UIUgIDqKG-e5zu162Xg

提取码: oqyy



flag{ev3n::y0u::bru7us?!}

Test-flag-please-ignore

常规操作之后,得到misc10文件,打开发现字符串

666c61677b68656c6c6f5f776f726c647d

看到字符串没有f以后的,应该就是16进制了,使用base16解码得到flag

flag:

flag{hello_world}

快乐游戏题

常规操作之后是一个, 通关游戏即可



UNCTF{c783910550de39816d1de0f103b0ae32}

Banmabanma

常规操作之后,得到一张斑马的图片



https://blog.csdn.net/weixin_43252204

查看wp说斑马的纹路是条形码,直接手机扫码得到flag

flag:

flag{TENSHINE}

reverseMe

常规操作之后,得到一张图片

$f1ag\,\{4f7548f93c7bef1dc6a0542cf04e796e\}$

https://blog.csdn.net/weixin_43252204

使用3D编辑,对图片进行垂直翻转,得到flag(或者拿一面镜子,更省事)



flag{4f7548f93c7bef1dc6a0542cf04e796e}

stage1

常规操作之后



手机扫描二维码得到



将前面得到的字符串复制,ctrl+v 弹框选择



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		A	NSI	AS	CII
0	03	F3	0D	0A	в6	26	6A	57	63	00	00	00	00	00	00	00	ó	¶&j	Wc		
16	00	01	00	00	00	40	00	00	00	73	0D	00	00	00	64	00		0	s		d
32	00	84	00	00	5A	00	00	64	01	00	53	28	02	00	00	00		Z	d :	s (
48	63	00	00	00	00	03	00	00	00	08	00	00	00	43	00	00	С			0	3
64	00	73	4E	00	00	00	64	01	00	64	02	00	64	03	00	64	sN	d	d	d	d
80	04	00	64	05	00	64	06	00	64	05	00	64	07	00	67	08	d	d	d	d	g
96	00	7D	00	00	64	08	00	7D	01	00	78	1E	00	7C	00	00	}	d	} :	х	1
112	44	5D	16	00	7D	02	00	7C	01	00	74	00	00	7C	02	00	D]	}	1 1	t	1
128	83	01	00	37	7D	01	00	71	2B	00	57	7C	01	00	47	48	f	7}	d+ 1	W	GH
144	64	00	00	53	28	09	00	00	00	4E	69	41	00	00	00	69	d	S (N:	iA	i
160	6C	00	00	00	69	70	00	00	00	69	68	00	00	00	69	61	1	ip	il	h	ia
176	00	00	00	69	4C	00	00	00	69	62	00	00	00	74	00	00		iL	ib	1	5
192	00	00	28	01	00	00	00	74	03	00	00	00	63	68	72	28	(t	cł	ır(
208	03	00	00	00	74	03	00	00	00	73	74	72	74	04	00	00		t	S	trt	
224	00	66	6C	61	67	74	01	00	00	00	69	28	00	00	00	00	fl	agt		i(
240	28	00	00	00	00	73	07	00	00	00	74	65	73	74	2E	70	(S	1	test	:.p
256	79	52	03	00	00	00	01	00	00	00	73	0A	00	00	00	00	уR			s	
272	01	1E	01	06	01	0D	01	14	01	4E	28	01	00	00	00	52			N	(R
288	03	00	00	00	28	00	00	00	00	28	00	00	00	00	28	00		(((
304	00	00	00	73	07	00	00	00	74	65	73	74	2E	70	79	74		S	te	st.	oyt
320	08	00	00	00	3C	6D	6F	64	75	6C	65	3E	01	00	00	00		<mo< td=""><td>dul</td><td>e></td><td></td></mo<>	dul	e>	
336	73	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	S				
352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					

观察发现为python编译之后的代码,保存为.pyc文件,反编译

python反编译在线工具: https://tool.lu/pyc/

反编译之后得到python源码,修饰之后运行

def flag():

```
str = [65,108,112,104,97,76,97,98]
flag = ''
for i in str:
    flag += chr(i)
print(flag)
```

flag()

flag:

AlphaLab

Hear-with-your-Eyes

常规操作之后得到的文件

bf87ed29ac5a46...

bf87ed29ac5a46...

使用Audacity(https://www.onlinedown.net/soft/46359.htm)软件打开该sound.wav文件,查看频谱图,即可得到 flag





flag:

e5353bb7b57578bd4da1c898a8e2d767

What-is-this

常规操作之后,得到文件

🗋 e66ea8344f034964ba0b3cb9879996... 2014/9/8 21:57 文件

150 KB

修改后缀名.zip,继续解压

Offset	0	1	2	3	4	- 5	6	7	8	9	10	11	12	13	14	15		1	ANSI	AS	CII
0	03	F3	0D	0A	в6	26	6A	57	63	00	00	00	00	00	00	00	ó	3 P	jWc		
16	00	01	00	00	00	40	00	00	00	73	0D	00	00	00	64	00		0	S		d
32	00	84	00	00	5A	00	00	64	01	00	53	28	02	00	00	00	"	Z	d	S (
48	63	00	00	00	00	03	00	00	00	80	00	00	00	43	00	00	с				С
64	00	73	4E	00	00	00	64	01	00	64	02	00	64	03	00	64	sN	I (d d	d	d
80	04	00	64	05	00	64	06	00	64	05	00	64	07	00	67	08	d	d	d	d	g
96	00	7D	00	00	64	80	00	7D	01	00	78	1E	00	7C	00	00	}	d	}	х	1
112	44	5D	16	00	7D	02	00	7C	01	00	74	00	00	7C	02	00	D]	}		t	1
128	83	01	00	37	7D	01	00	71	2B	00	57	7C	01	00	47	48	f	7}	q+	W	GH
144	64	00	00	53	28	09	00	00	00	4E	69	41	00	00	00	69	d	S (N	iA	i
160	6C	00	00	00	69	70	00	00	00	69	68	00	00	00	69	61	1	ip	i	h	ia
176	00	00	00	69	4C	00	00	00	69	62	00	00	00	74	00	00		iL	ib		t
192	00	00	28	01	00	00	00	74	03	00	00	00	63	68	72	28	(t	c	hr(
208	03	00	00	00	74	03	00	00	00	73	74	72	74	04	00	00		t	S	trt	
224	00	66	6C	61	67	74	01	00	00	00	69	28	00	00	00	00	fl	agt		i(
240	28	00	00	00	00	73	07	00	00	00	74	65	73	74	2E	70	(S		tes	t.p
256	79	52	03	00	00	00	01	00	00	00	73	0A	00	00	00	00	уR			s	
272	01	1E	01	06	01	0D	01	14	01	4E	28	01	00	00	00	52			N	(R
288	03	00	00	00	28	00	00	00	00	28	00	00	00	00	28	00		(((
304	00	00	00	73	07	00	00	00	74	65	73	74	2E	70	79	74		s	te	st.j	pyt
320	08	00	00	00	3C	6D	6F	64	75	6C	65	3E	01	00	00	00		<m< td=""><td>odul</td><td>e></td><td></td></m<>	odul	e>	
336	73	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	s				
352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
1 400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					

使用stegsolve工具的combiner功能将两张图片组合,即可得到flag



flag;

AZADI TOWER

MISCall

常规操作得到文件,对其加.zip后缀连续两次进行解压,得到文件ctf

flag.txt文件中提示我们: Nothing to see here, moving along...(继续向前走)

发现有.git文件,接下里就要用到git的相关知识了

在linux下打开该ctf文件夹

~/Desktop/ctf\$ ll
total 16
drwxrwxrwx 3 gcd gcd 4096 7月 25 2014 //
drwxr-xr-x 5 gcd gcd 4096 8月 22 19:18 ../
-rwxrw-rw- 1 gcd gcd 37 7月 25 2014 flag.txt*
drwxrwxrwx 8 gcd gcd 4096 7月 25 2014 glt/

git log 查看git记录

```
~/Desktop/ctf$ git log
commit bea99b953bef6cc2f98ab59b10822bc42afe5abc
Author: Linus Torvalds <torvalds@klaava.Helsinki.Fi>
Date: Thu Jul 24 21:16:59 2014 +0200
Initial commit
```

git stash show 校验列表中存储的文件

~/Desktop/ctf\$ git stash show
flag.txt 25 ++++++++++++++++++++++++++++++++++
s.py 4 ++++
<pre>2 files changed, 28 insertions(+), 1 deletion(-)</pre>

rm flag.txt 为避免冲突, 删除flag.txt文件

git stash apply 重新进行存储,复原文件



查看新的flag.txt文件,没有发现flag

查看s.py文件,发现是对 flag.txt 文件内容的读取并进行sha1 加密,同时在开头加上几个字母,怀疑与 flag 有关

```
//Desktop/ctf$ cat s.py
#!/usr/bin/env python
from hashlib import sha1
with open("flag.txt", "rb") as fd:
    print "NCN" + sha1(fd.read()).hexdigest()
```

运行s.py,得到flag

/Desktop/ctf\$ python s.py NCN4dd992213ae6b76f27d7340f0dde1222888df4d3

flag: