HCTF GAME-WEEK2 @Cyris

从 0 开始之 XSS challenge0

过滤条件不多，**payload** 如下。

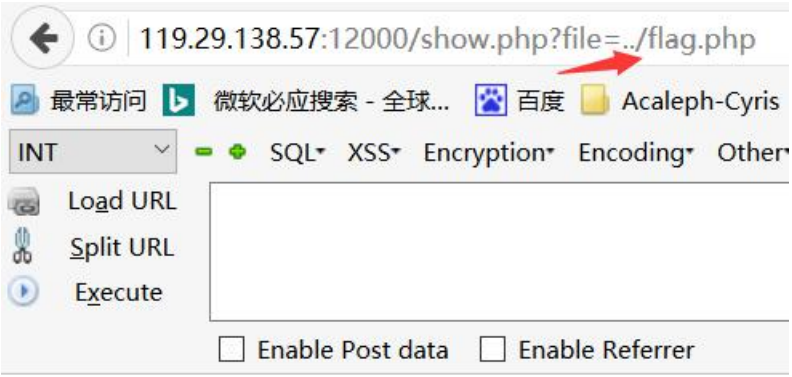
C014 13:04:34
- 好
- payload给我

hgame{Capτ_Zhe_Cy} 13:05:15
<svg/onload=alert(1)

C014 13:06:02
hctf{xss_f1rst_st3p}

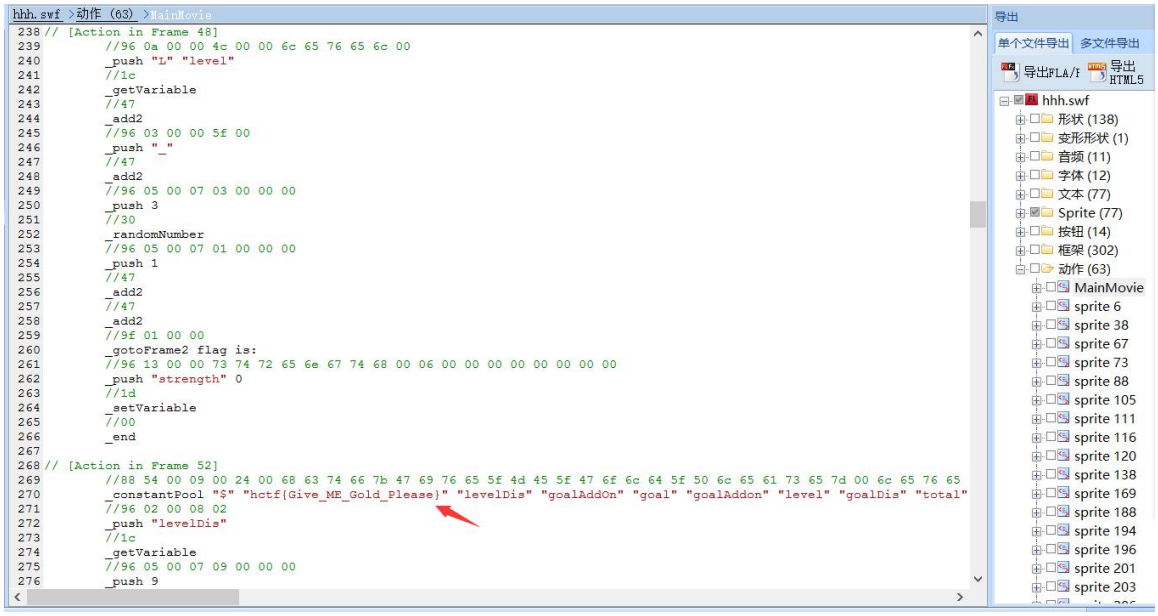
从 0 开始 LFI 之 0

送分题，题目直接给出 **flag** 在**../flag.php** 里啦。



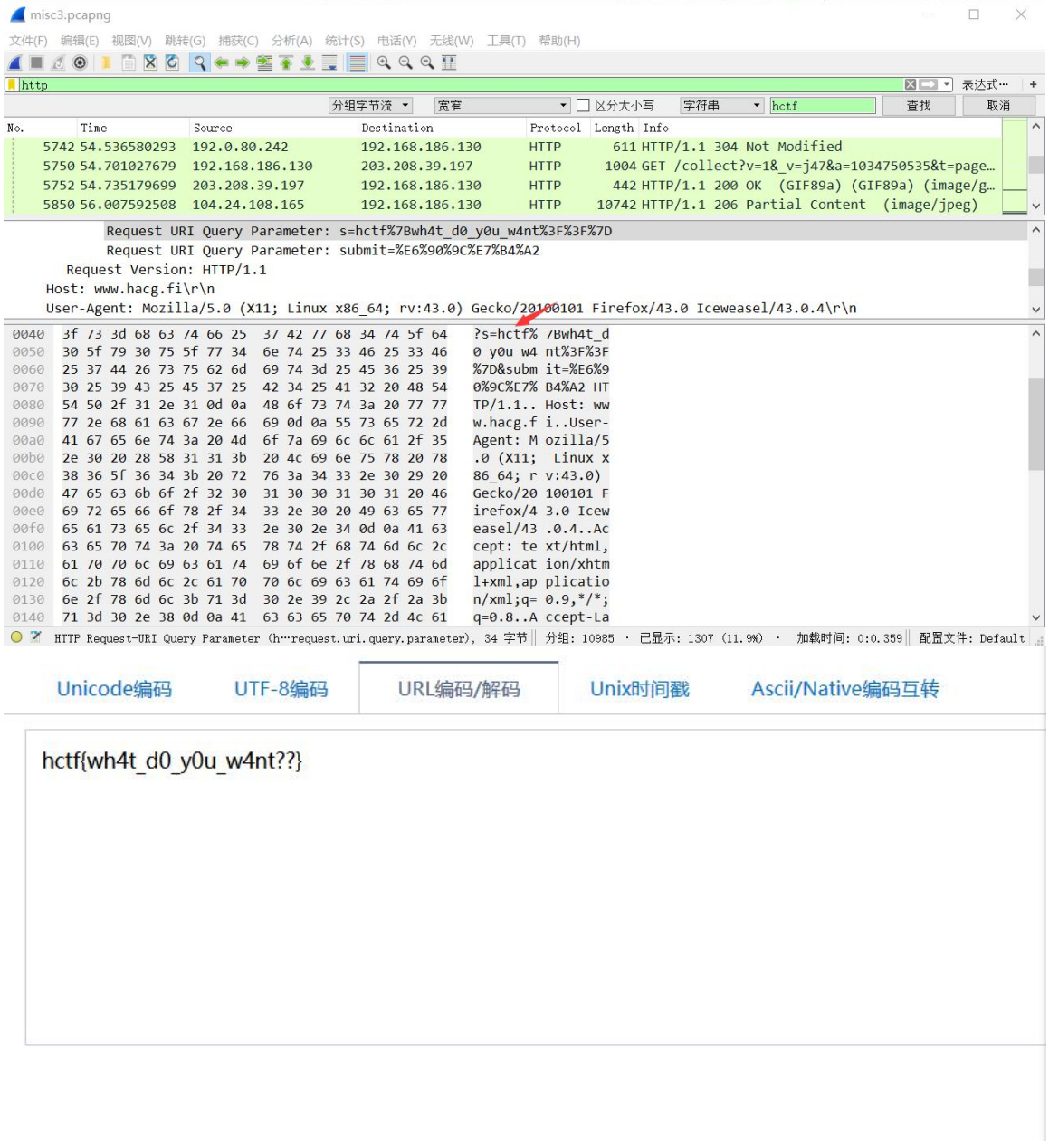
Re 从零开始的逆向之旅：Gold Miner

黄金矿工好好玩！猜想 flag 需要玩通关后才能拿到，但是既然是个 flash 文件可能可以反编译拿到源码，用朔思打开，在动作栏里的代码中找到 flag。



我是一个有格调的 misc 题目

下载得到 pcapng 格式文件，用 wireshark 打开搜索关键字 hctf，URL 解码得到 flag。

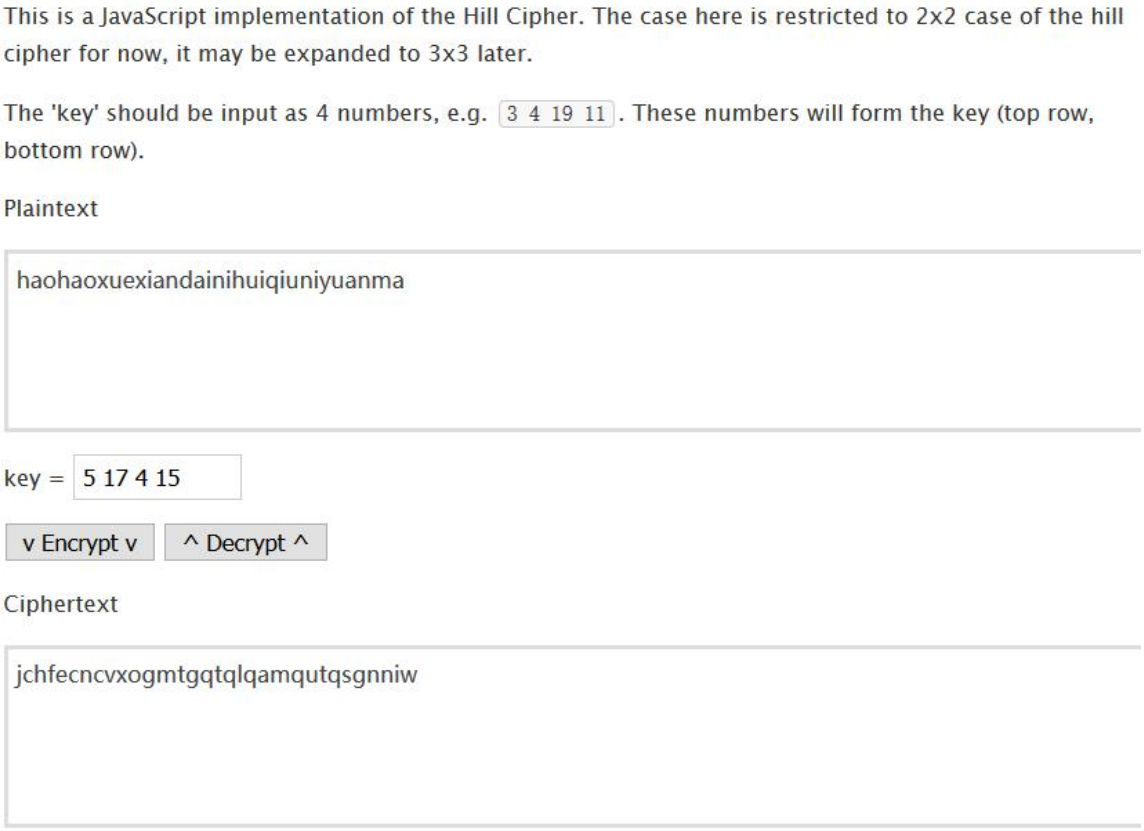


密码学教室进阶（五）

RSA 题。在博客上看到一个因数分解网站 http://factordb.com/，把 n 丢进去后利用公式解出 m，再 16 进制转文字拿到 flag。

密码学教室进阶（六）

希尔密码，开始居然在手算....脚本好像写错了没跑出正确答案，翻各种博客翻到在线工具，丢进去，payload。



进击的 Crypto [0]

RSA 题。打开后发现好几组 rsa...而且 n 还都是质数，丢 factordb 里分解不出，观察发现 e 都是 65537，用公约数的方法分解 n，再利用公式得到 flag。python 脚本如下：

In [2]:
```
def gcd(a, b):
    if a < b:
        a, b = b, a
    while b != 0:
        temp = a % b
        a = b
        b = temp
    return a
n1=28989197955870674811941817152881961892555962828020048566215146047714
n2=29703811006265969568420235185761287243393105045336995893094671661144
print(gcd(n1,n2))
```

```
174020591931642579445639482520669966832472464887563376831648240313949745
497456756209514495961820914225045161529643317531728161012587865008674424999803296228716056432443128645691909125715946229286854864870821
899631190828171757188986378429230898856002204891580815930976676783807695195461562646917675429591266528741337
```

```
共有素因子p:174020591931642579445639482520669966832472464887563376831648240313949745
675620951449596182091422504516152964331753172816101258786500867442499980329622871605643244312864569190912571594622928685486487082899631190828171757188986378429230898856002204891580815930976676783807695195461562646917675429591266528741337

q:166584871560820727096589642347689679565074855614352117551421403470172486999617714211766560053113999351102121040050712302652946259905787937498701699126275189937913458623225733035633870625681735432630656542758649284674875757423561657674667345174775248412119912423941445877761025122933990376999367161895532332413
(p-1)(q-1):28989197955870674811941817152881961892555962828020048566215146047714999804743571465320756664500939106612607504133407755470924915037883788416084924998195415611009578161228226056524027626453567996030151847302248848345942762209886902216532270655286303624781479379460319335849225128417295447574269158603952744753067929430643767654134361856077479086952596050103229260549332162283880933412256690704972272591482241504719239583553832517101002627902972766382348390234025244104758903594182154264608253064591147474926897905565268510612314967001168801828416175430667565309345429769612310894416216848938615940859975971462716982432

d:23970484252049799941009491025402847199589547608423248727463341005412569303124324904667548474998403819620120134526961863935256299049665995972596520600228996862477990297619952061111945635368498760591268424815847038172558771791750936387324721593613074747555322169954898227398345345897152106436016600911039614125051561160505003478114579601487627892656791317136031506758454906485279943582153628118362946488319791100939016315552523581094960608643819478813888972872912431195828154243745138192980848098375862075068488401978843490831010885099416595035430514482400175729547917152915260033158247594615642530348193824791506476491

m:792157350412422570162821343981744064639802965956062465847717699157247344779065111421
16:686374667B49375F31735F64346E6765723075735F325F53683472655F7072696D337D
flag:hctf{I7_1s_d4nger0us_2_Sh4re_prim3}
```

我是最简单的渗透题

试了好多万能密码都不行，可能姿势不太对 ovo，就拿 sql 扫了一下，拿到两组 username 和 password，问了土土说暴力也可以那就这么写啦，命令行及两组数据如下：