Pentest——ez game

首先根据 hint，构造

http://115.28.78.16:13333/3a94a786f2f3af094a461b295bc4e2f6/.login.php.swp

和

http://115.28.78.16:13333/3a94a786f2f3af094a461b295bc4e2f6/.register.php.swp

获得 login.php 和 register.php 的 vim 泄露文件，通过 vim -r login.php 和 vim -r

register.php 恢复文件。

好吧，讲真由于涉及到 mysql 所以看的云里雾里。然后在 register 中尝试注册 admin，

发现已被注册，接着注册一个 abc 用户，在 login 中尝试登陆，显示

you are just guest, you can't touch flag!

Ok，看来需要获得 admin 权限，接着我就尝试在 login 中使用 admin 的

超长用户名，然后发现登陆成功获得 flag

Hello, admin This is your flag: hctf{mmp_you_yi_xie_wenti}

好吧，虽然 admin 不是我竞争注册到的，土爷说我的 flag 不行，然后就想到，这届 HCTF 中同样有一题条件竞争的题，想着能不能参考一下思路,然后接着发现基本上是原题，改下脚本中 post 的 url，和不同的 you are just guest, you can't touch flag! 就可以了 ok

CRYPTO——密码学进阶教室（五）

用 rsa 的分解工具将 n 分解为 p，q，然后用 d=e^(-1)mod((p-1)(q-1))算出 d 的值。

算出 d 的值后，直接使用 m=c^d mod n 算出 m 的值即明文，带入 16 进制转 ascii 工具中得 flag：

hgame{1f_u_kn0w_p_q_1n_RSA_1t_is_easy___}

CRYPTO——密码学教室进阶（六）

使用 2*2 矩阵的解码工具，经过尝试得到 flag，

hgame{xuexiandainihuiqiuniyuanma}

2*2hill 解密工具源码地址 https://www.douban.com/note/272501002/

Web——从 0 开始 LFI 之 0

一开始拿到题目尝试的时候由于查找的资料不完整，直接在原来的 url 上添加?file= 来读取文件，结果失败了。

之后发现错误后，构造 payload:

http://119.29.138.57:12000/show.php?file=../flag.php

获得 flag: hctf{Inc1ude_i5_s0_d4ngerous}

Web——从 0 开始 LFI 之 1

直接仿照上题的 payload 直接构造，http://119.29.138.57:12001/show.php?file=../flag.php QAQ 获得一个假的 flag。

然后根据查找到的资料猜测出题人把某些内容注释掉了，所以构造 payload：

http://119.29.138.57:12001/show.php?file=php://filter/read=convert.base64-encode/resource=../flag.php

获得一串base64，解码得到

```
hctf{flag_i5_n0t_here}
<!-- hhh,maybe it is in Comments.Have a try! -->
<?php
// f1ag_is_heeeeeeere/flag.html
?>
```

根据提示，构造payload http://119.29.138.57:12001/show.php?file=php://filter/read=convert.base64-encode/resource=f1ag_is_heeeeeeere/flag.html 再次获得一串base64

解码base64得到flag：hctf{Do_y0u_kn0w_php_fi1ter?}

WEB——从0开始之XSS challenge0

根据所给源码可以知道会过滤script

构造payload: <sScriptcript>alert(1)</sScriptcript>

WEB——从0开始之XSS challenge1

由于是在input中构建XSS，首先我想到的是payload是："onfocus=alert(1) value="

但是由于需要交互，所以需要修改，再然后构造的payload:

"type=image src=1.jpg onerror="alert(1)"

WEB——从 0 开始之 XSS challenge2

在 svg 中构建 xss 攻击，构造 payload:

";<script>alert(1); var sdda="

MISC——我是一个有格调的 misc 题目

下载下来发现是 pcapng 文件，用 wireshark 打开，发现不愧是老司机，然后就想从中提取出 flag，思来想去还是用 winhex 打开，然后搜索文本 hctf，获得

hctf%7Bwh4t_d0_y0u_w4nt%3F%3F%7D

一眼看出是 url 编码的 丢进去解码，得到 flag

hctf{wh4t_d0_y0u_w4nt??}