Week2 write up　　-Yuahwg

CRYPTO

1. Vigener~

Emmm 我觉得这道题应该是出题人友情送分的。。。。百度了维吉尼亚密码大概是什么也顺便找到了在线工具。。。然后输入题目里的那一段话解密后在最后得

> in the nineth century and so acquired its present name.
> flag is gfyuytukxariyydfjlplwsxdbzwvqt

到这句话

得到 flag=hgame{gfyuytukxariyydfjlplwsxdbzwvqt}

MISC

2. Are You Familiar with DNS Records?

成功签到了 oyeye 说的送分题。。点开题目发现打不开，又有了

well, you know, this is a song-ten-ti, have fun! XD

然并卵的hint: DNS 有很多种不一样的记录类型，其中一种类型如果没有正确设置就可能被其他邮件服务器拒收，flag 就在此域名的第二条此类型记录里

oyeye 的 hint，于是去搜索了一下 dns 的记录类型，应该是 txt 记录，开始寻找 dns 解析工具开始查询，但我找的第一个工具 emmmm

记录类型	主机记录	记录值	TTL
TXT 记录	project-a11.club		600
TXT 记录	project-a11.club		600

于是去找其他的

project-a11.club　查询

A MX CNAME TXT

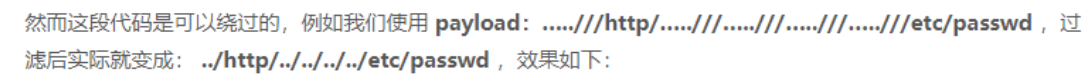
响应类型	响应IP	TTL值
TXT	v=spf1 include:spf.mail.qq.com ~all	349
TXT	flag=hgame{seems_like_you_are_familiar_with_dns}	349

得到这个结果，于是得到 flag=hgame{seems_like_you_are_familiar_with_dns}

WEB

1. easy_php

第二周的审计题。。。愣了好久。去搜 str_replace 函数时找到了这个函数的这个漏洞




```
include_once($img.".php");
```

再看这句话说明后缀已给出不用添加。

然后去搜索如何读取文件时了解到可以用 php://filter 伪协议来读取

然后又用...././/这样的操作来绕过过滤来读取上一个目录即最后的语句是这样

?img=php://filter/read=convert.base64-encode/resource=...././/flag

然后得到了一段 base64 编码，解码后得到

```
<?php
  //$flag = 'hgame{You_4re_So_g0od}';
  echo "maybe_you_should_think_think";
```

于是 flag = hgame{You_4re_So_g0od}

Ps：这周过年学习好慢。。下周需要加紧学习（先等一波 wp 复现一下再努力肝 week3