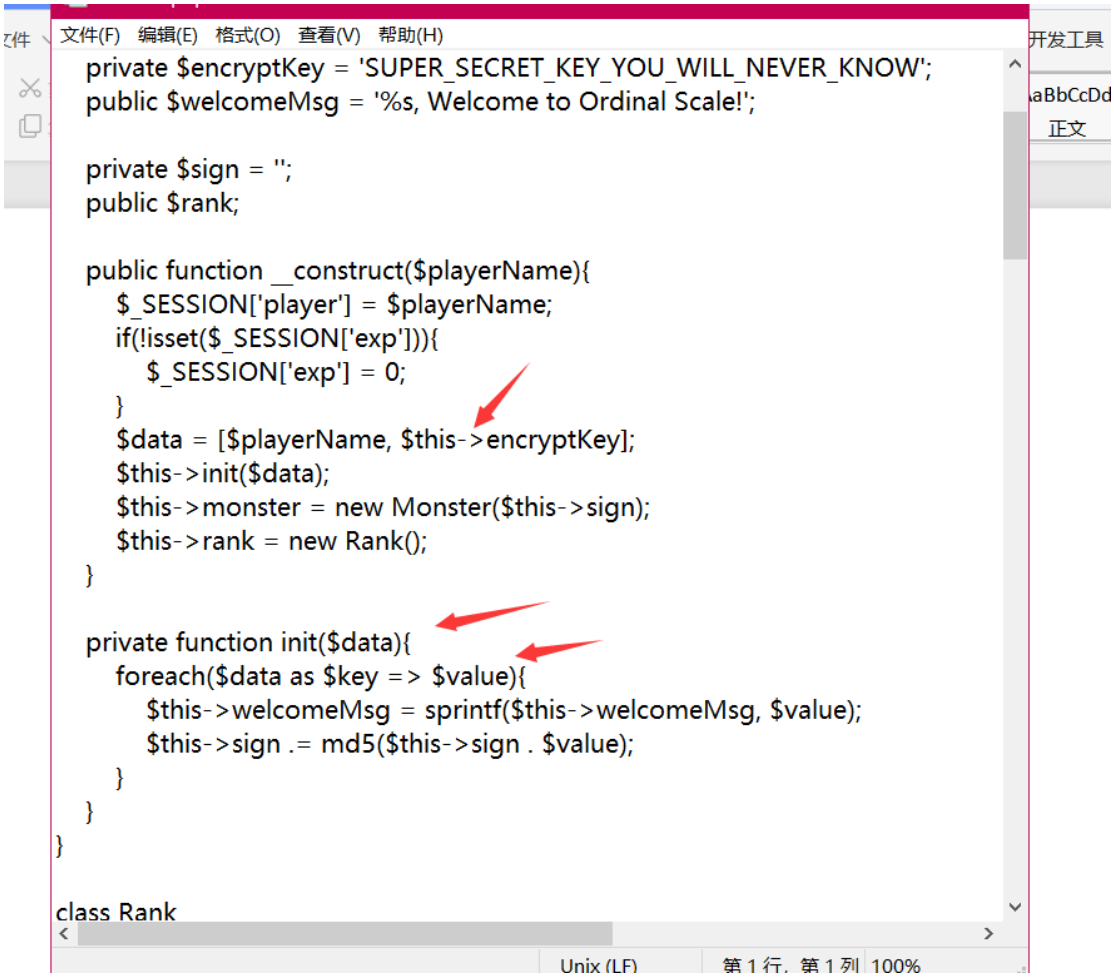
Week3 write up lupin111

Web 序列之争

F12 看到源码 路径 下载 source.zip

看代码



```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
    private $encryptKey = 'SUPER_SECRET_KEY_YOU_WILL_NEVER_KNOW';
    public $welcomeMsg = '%s, Welcome to Ordinal Scale!';

    private $sign = '';
    public $rank;

    public function __construct($playerName){
        $_SESSION['player'] = $playerName;
        if(!isset($_SESSION['exp'])){
            $_SESSION['exp'] = 0;
        }
        $data = [$playerName, $this->encryptKey];
        $this->init($data);
        $this->monster = new Monster($this->sign);
        $this->rank = new Rank();
    }

    private function init($data){
        foreach($data as $key => $value){
            $this->welcomeMsg = sprintf($this->welcomeMsg, $value);
            $this->sign .= md5($this->sign . $value);
        }
    }
}

class Rank
```

这里是一个循环 data 是一个数组 data[0] 假如为%s 时，会把 encryptKey 输出

得到密钥

gkUFUa7GfPQui3DGUTHX6XIUS3ZAmClL

后面就是 pop 链的构造 ，php 反序列化的问题 0.0 ，感谢茄子帮我看了我的 php 序列化脚本 0.0.

Web2 Cosmos 的二手市场 0.0

此题我非常规解出，后来了解到 一个 web 竞争的漏洞

服务器接受请求是并发的，所以可以多线程发很多很多请求，让服务器处理。

买东西钱还没扣东西就到了，然后又把东西卖出了，这样多次，就能达到一个亿。

我没写脚本用 bp 跑 0.0 最高只跑到 4000 万。

Misc 三重隐写

Mp3 隐写 Lsb 隐写 还有一个在音乐专辑的图片上的一个条形码

解出 flag.7z 的密码 得到 flag

MISC 日常

首先双图，盲水印很明显 运行脚本拿到一个密码 还提示了一个加密磁盘的软件

分析文件夹里的影月 发现里面藏了文件 提出来 是 一个名为 container 的加密文件 用解密文件 解密 ，输入盲水印解出的密码 ，然后拿到 3 个文件

一个用 sqlite 的 cookie 文件 一个 sid 下的保护文件 一个 mimikz 运行的文件。

从 mimikz 文件得知 ltsm，解密后为 welcome2020 （具体是什么忘记了）

然后用 cookieview 软件 高级功能那把 3 个文件一起利用 拿到 flag。