学习周记（四）（上）

原创

極品一═☆宏 于 2019-01-30 07:14:49 发布 694 收藏

分类专栏： CTF_web

本文链接：https://blog.csdn.net/qq_43214809/article/details/86660341

CTF_Web周练习（二）

从1月13日至1月25日，差不多快两周的时间没有碰这个东西了。好在考完了期末考试，现在有时间了，也该干干正事了，提高提高自己的能力，做点题，写点自己的wp与体会吧，一定要在寒假的时间做到每天进步一点点。I'm f***ing coming! ˙▽˙

先写写自己的计划，一周的时间是七天，按照4、3分配，前四天中前两天做攻防世界的题，后两天做做其他平台的题；接下来的三天自己积累一些经验，找一些相关资料，最后形成一份周总结。

下面开始上半部分的总结。

时间:2019年1月26日至1月29日

一、攻防世界：

由于攻防世界这个机制吧，首先题目顺序不一样，做题超过两天自动换，做完后原题目的链接废掉，所以没有可提供的题目链接；其次wp中自己的体会可能多一点，毕竟初学者，一道题在我手上花费的时间可能真的比较长，从我自己一个新手的角度去分析一下。

1.unserialize3：（_wakeup()漏洞利用）

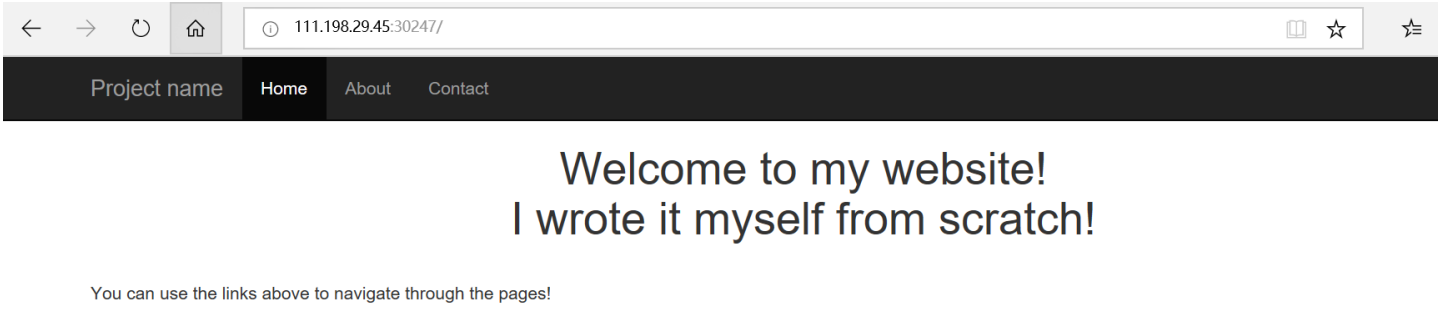
这道题其实还是很简单的，就是一个简单的_wakeup()函数利用。

打开题目环境后，很简单的几行代码，上来一个class xctf，然后就是function_wakeup()，后面再跟着一个unserialize()，不用多加考虑，一定是考unserialize()和_wakeup()函数某些知识、特性的。

查了一些资料，wakeup()这里还是有点东西的，当被反序列化的字符串其中对应的对象的属性个数发生变化时，会导致反序列化失败而同时使得_wakeup()函数失效，就是问题的关键所在。那么接下来，只要构造一个payload绕过_wakeup()即可，结合题中所给条件，其序列化应为：O:4:“xctf”:1:{s:4:“flag”;s:3:“111”;} 即一个xctf对象，属性为1，属性值flag为"111".按照漏洞表述，我们只需要改变属性个数即可，因此，将1改为2后，?code=O:4:“xctf”:2:{s:4:“flag”;s:3:“111”;} ,得到我们想要的flag。

2.mfw：（git泄露）

这道题的链接打开是一个网址，里面有三个板块，‘home’,‘project’,‘about’。



点击'About'后，出来一个页面，写着建造网站用到的方法，第一个就是Git，那么这就很明显了，八成是git泄露，工具一扫，出来了点东西，是个index.php，进去瞅一瞅。

```php
<?php

if (isset($_GET['page'])) {
    $page = $_GET['page'];
} else {
    $page = "home";
}

$file = "templates/" . $page . ".php";

// I heard '..' is dangerous!
assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");

// TODO: Make this look nice
assert("file_exists('$file')") or die("That file doesn't exist!");

?>
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1">

        <title>My PHP Website</title>

        <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/css/bootstrap.min.css" />
    </head>
    <body>
        <nav class="navbar navbar-inverse navbar-fixed-top">
            <div class="container">
                <div class="navbar-header">
                    <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false" aria-co
                        <span class="sr-only">Toggle navigation</span>
                        <span class="icon-bar"></span>
                        <span class="icon-bar"></span>
                        <span class="icon-bar"></span>
                    </button>
                    <a class="navbar-brand" href="#">Project name</a>
                </div>
                <div id="navbar" class="collapse navbar-collapse">
                    <ul class="nav navbar-nav">
                        <li <?php if ($page == "home") { ?>class="active"<?php } ?>><a href="?page=home">Home</a></li>
                        <li <?php if ($page == "about") { ?>class="active"<?php } ?>><a href="?page=about">About</a></li>
                        <li <?php if ($page == "contact") { ?>class="active"<?php } ?>><a href="?page=contact">Contact</a></li>
                        <!--<li <?php if ($page == "flag") { ?>class="active"<?php } ?>><a href="?page=flag">My secrets</a></li> -->
                    </ul>
                </div>
            </div>
        </nav>

        <div class="container" style="margin-top: 50px">
            <?php
                require_once $file;
            ?>

        </div>

        <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/1.12.4/jquery.min.js" />
        <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/js/bootstrap.min.js" />
    </body>
</html>
```


看到里面的绿色部分，在网址中输入一个?page=flag，然后发现是个空页，对我而言并没什么卵用。到这里，我的解题思路就结束了。讲真，以我现在的技术或者说是知识储备能力，我啥也干不了，出于对解题方法的好奇，花了6块金币查了一下师傅写的writeup。看完以后的直观感受还是懵逼，毕竟菜是原罪。后来自己又查了一些相关资料，大致理解了是怎么个意思。出发点是上级目录，由于page是GET得到的，那么就可以在page中添加一些相应的东西，wp中给出了system()，但是到现在我也没弄明白这到底是怎么个意思，为什么要这么去构造。所以决定这道题先放一放，我在后三天里再去问问，再看看。≡(▔﹏▔)≡

3.confusion：（SSTI注入）

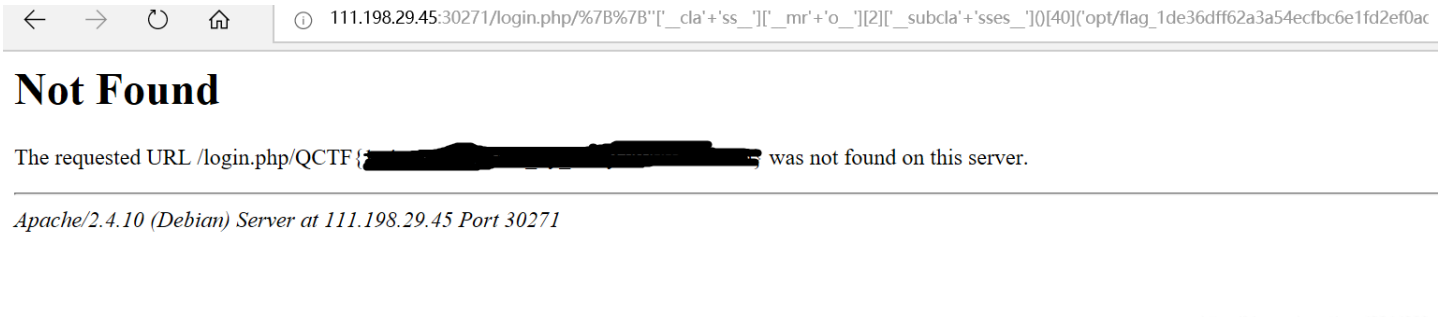
这道题相信大多数人都见到过了，我也是做完题才知道这是2018QCTF的一道web题。
不多说，打开链接后是一个网址，有一个图片。

然而，这个网页在点击'Login'和'Register'的时候，显示Not Found，既然这样，在'Login'的界面下看一下源码，出来了点东西：

貌似是给出了flag的一个有关信息，一个txt文件，但是如果直接把文件地址放到url中，看不到有用的信息。那么接下来想着是否存在漏洞或者说是注入，我当时先上了tplmap进行扫描，还是比较幸运的，查找到了注入机会；再结合之前我自己在搜查一些资料时，看到过与这类似的注入，又找了一些，最后确定是SSTI注入。
SSTI注入型题目确实是第一次见到，并没有什么经验，又查了一些资料。SSTI部分是基于 FLASK JINJA2模板的注入，FLASK是由python写的一个基于JINJA2引擎的web应用框架，我们知道python是面向对象的编程语言，所以有着类，对象和继承属性,而这种SSTI就充分利用了这些。许多师傅们给出了适用于不同python版本的payload，以python2为例，适用于读文件的payload是：

```
#读文件:
{{ ''.__class__.__mro__[2].__subclasses__()[40]('/etc/passwd').read() }}
```

对于这个题来说，我们先将绿色字体替换为本题中给出的'opt/flag'的那一部分，但是还是没有得出flag。这就有点捉急了，既然这样得不出，在方法没错的前提下那就只能试试看看能不能绕过去，至于这个怎么绕又是一个问题，其实有很多种方法，从过滤关键字的角度来看，我们可以直接利用字符串拼接，就像" cla'+'ss "、" mr'+'o "、" subcla'+'sses "这样，最后得到flag。做完题后我自己又上网查了一些关于SSTI的相关知识和题目，碰巧看到了这道题的其他解法，有个师傅给出了request.args传值绕过，还有一个是getattribute函数绕过，方法还是蛮多的。

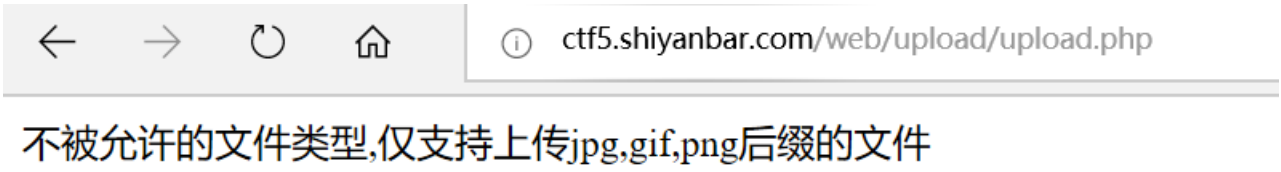


二、实验吧：

1.上传绕过：

题目链接：http://ctf5.shiyanbar.com/web/upload

打开链接后提示上传文件，先上传了一个图片，显示说必须上传文件后缀名为php的，那么好按它说的做，传个php文件，结果又显示仅支持上传jpg,png,gif后缀的文件。



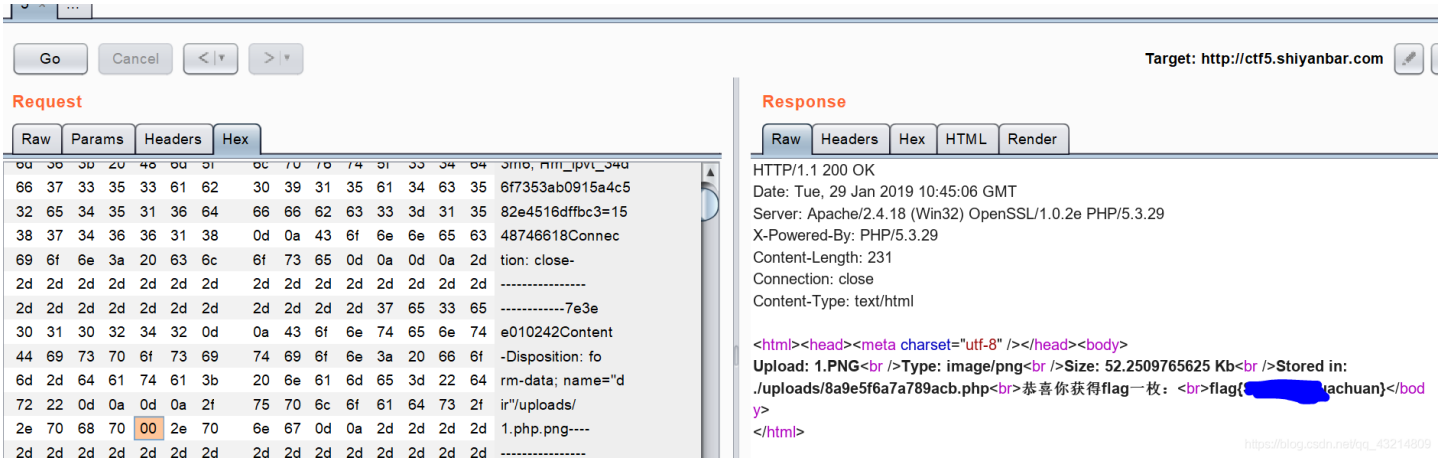
这就有些懵逼了，怎么个情况。只能打开burpsuite抓下来看一下，发到repeater。

```
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101382%2CnickName%3A%E6%A5%B5%
E5%93%81%E2%94%81%E2%95%90%E2%98%86%E5%AE%8F;
PHPSESSID=up3lqer0o8reajtvaebreqe3m6;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1548746618
Connection: close

----------------------------7e3ee010242
Content-Disposition: form-data; name="dir"

/uploads/
----------------------------7e3ee010242
Content-Disposition: form-data; name="file"; filename="1.PNG"
Content-Type: image/png
```


当时感觉，比较有用的应该是'/uploads/'这一部分，按照它的说法，我理解的是上传文件的后缀名既有php，也得有png。这样的话就涉及到了一些问题，这道题目说是上传绕过，上传文件没有问题，绕过这个怎么去理解，如何去满足这个条件。之前也做过几道与绕过有关的题目，认真的讲，理解不深。在这道题里我先想到的是00截断，而且如果真的是00截断的话，00位置应该是在php后，png前，带着这个想法去实践一下。那么现在的问题就是从哪下手，先在filename里试了一下，没成功，那么就只能从/uploads/那里动手了，但需要注意的是，00截断编码的问题，我不知道这个编码是怎样的，所以先敲了个空格，直接改成了/uploads/1.php .png；然后在hex里找到空格对应的数，直接改成00，得到flag。

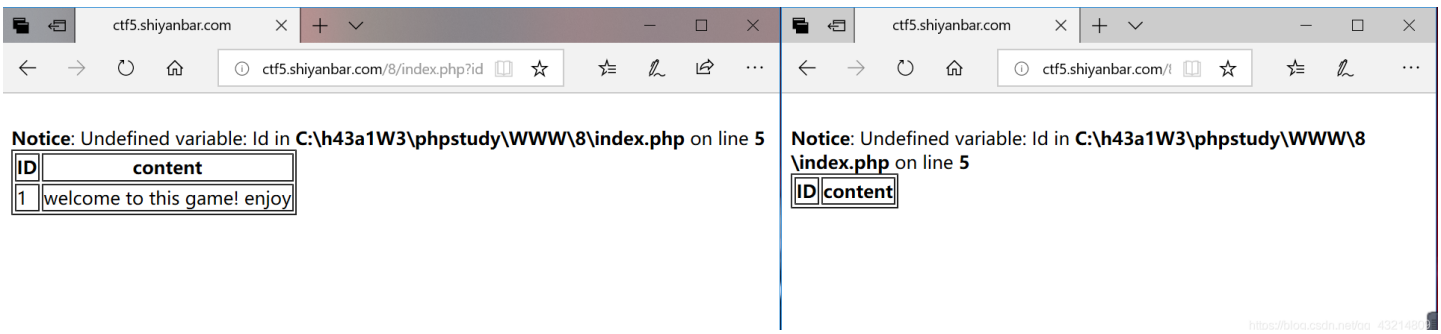


2.这个看起来有点简单（sql注入）：

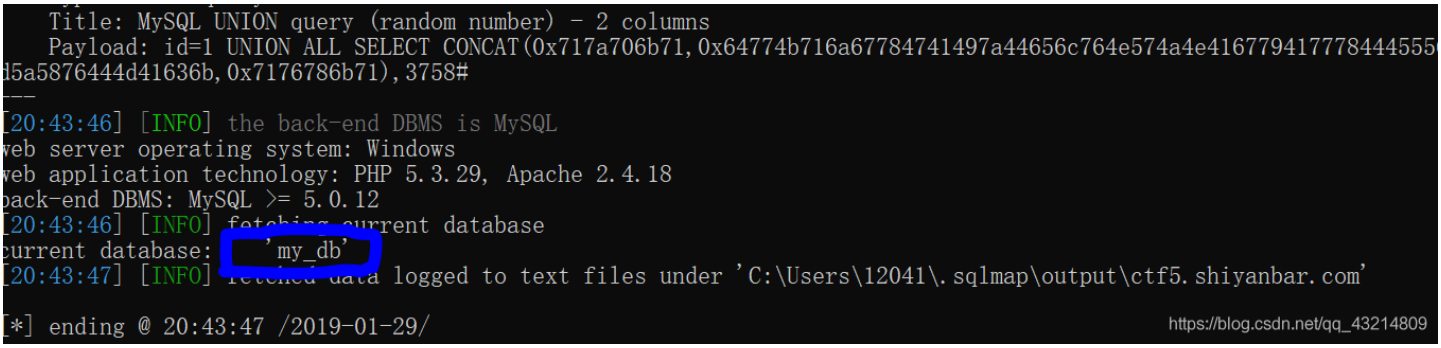
题目链接：http://ctf5.shiyanbar.com/8/index.php/?id=1

这算是我一次做sql注入的题目，我之前对这种题型都是敬而远之的，毕竟江湖传言很难。第一次接触后的感受还好，与题目表述相差无异 =_=‖ 。

题目中给出了id=1，打开网页后也是有关id的内容，所以应该是sql注入无疑了。为了证实是sql注入，先'and 1 = 1'然后'and 1 = 2'，果然两个页面显示不一样。

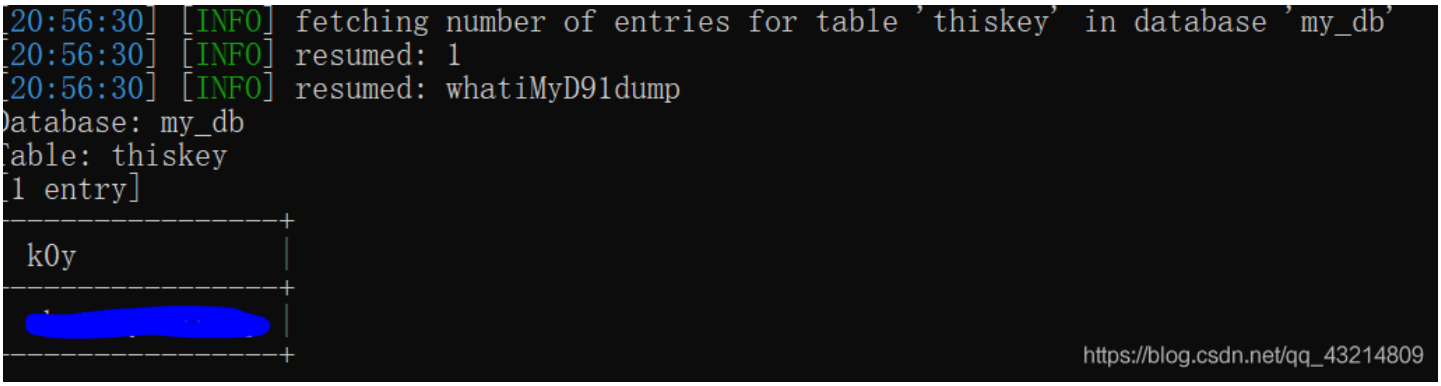


确定是注入了，直接上工具sqlmap按套路跑一下就好了。首先先查一下网站所用的数据库，发现是my_db；



紧接着我们要查一下表和列：

查出表名thiskey，列名k0y。直接dump得解。



3.感受体会：

1.首先，隔了将近两个星期又重新开始，感谢自己有这份兴趣吧。可能现在确实水平低，技术差（或者说没技术），但自己还是能够边写边学，自己找事干，每天记录自己的解题过程，虽然做一道题的时间花费很长，但是感觉真的值了，每次解完后再去看看别的师傅们的wp，再从中找一些思路，或者说其他的方法，也是一种提升吧。

2.自己涉及的题目广度和深度还是比较低，一种类型有许多种不同的考点，到目前为止我个人涉及的还是少，在这一点上以后还是要多加练习，多加查阅。通过这四天的练习，后三天的总结查阅也有了大致的计划，知道从哪些方面去拓宽视野。

3.最后还是按惯例，感谢一些师傅们的wp，一些辅助性资料，实用，真的实用。

sql：https://blog.csdn.net/qq_33530840/article/details/82144515

_wakeup()；http://www.venenof.com/index.php/archives/167/

文件上传漏洞：https://thief.one/2016/09/22/