## 20200728信息安全实训

| | | | |
|---|---|---|---|
| **笔记本:** | 我的第一个笔记本 | | |
| **创建时间:** | 2020/7/28 18:41 | **更新时间:** | 2020/7/28 22:16 |
| **作者:** | 820410740@qq.com | | |

序列化 serialize
将对象转换成字符串

反序列化 unserialize
将字符串转换成对象
Class类 共有属性
前端给后端字符串，后端进行反序列化

序列化漏洞重要函数
class

**魔术方法**:
自动触发的函数，当满足了这个函数的条件，就会自动的触发。

_construct() 当一个对象创建时被调用
_destruct() 当一个对象销毁时被调用
_wakeup:在使用unserialize函数时会自动调用。

pikachu

```
<?php
class s{
```

**序列化**（serialize）
将**对象**的状态信息转换为可以存储或传输的形式的过程。在序列化期间，对象将其当前状态写入到临时或持久性存储区。以后，可以通过从存储区中读取或反序列化对象的状态，重新创建该对象。**【将状态信息保存为字符串】**
**反序列化**（unserialize）
序列化是将对象的状态转为字符串储存起来，那么反序列化就是再将这个状态拿出来使用**【将字符串转化为状态信息】**
（**这项技术一般来说是对一个类进行处理**
）
**魔术方法**:
自动触发的函数，当满足了这个函数的条件，就会自动的触发。
**常见魔术方法**:

```
var $test = "<script>alert(123)</script>";
}
$s = new S();
echo serialize($s);
```

序列化结果

```
O:1:"s":1:{s:4:"test";s:27:"<script>alert(123)</script>";}
```

通过代码审计对输入框输入

```
test";s:27:"<script>alert(123)</script>"
```