《PHP 反序列化漏洞》实验报告

姓名：方有斌 学号：2012116 班级： 计科三班

实验名称：

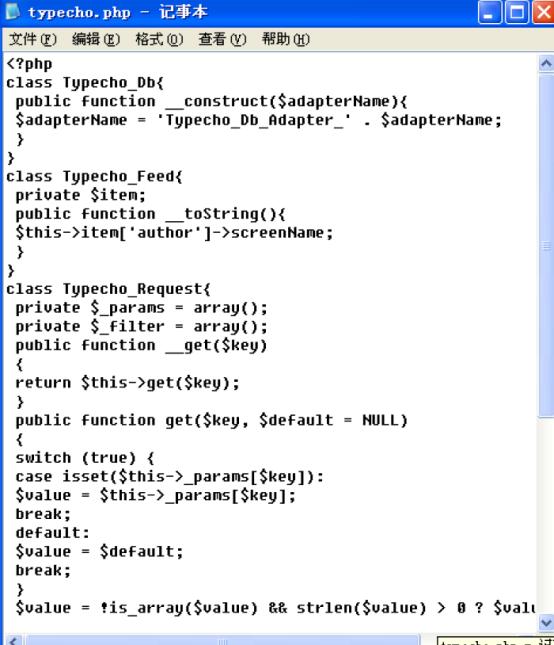
PHP 反序列化漏洞

实验要求：

复现 12.2.3 中的反序列化漏洞， 并执行其他的系统命令。

实验过程：

1. 根据示例编写 typecho.php：



由于 unserialize()的参数是可控的，利用这一点进行漏洞的设置。

Typecho\_Db 的构造函数中，包含了字符串拼接的操作，通过查询 PHP 魔术方法发

现， \_\_toString()方法将会被调用。继续观察代码发现Typecho\_Feed 中存在

\_\_toString()方法。

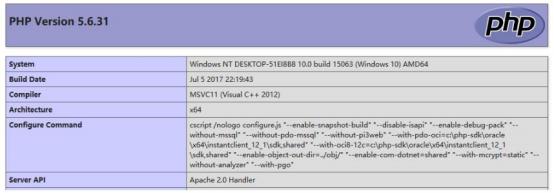
\_\_toString()方法中，若$item[‘author’]是一个对象， 并且该没有 screenName 属性， 那么这个对象中的将会调用\_\_get()方法， \_\_get()方法在Typecho\_Request 类 中。

\_\_get()方法返回 get()，get()中调用了\_applyFilter()方法， applyFilter()方 法调用 call\_user\_function()函数， 该函数中$filter，$value 可以被控制。于是构 造攻击链

2. 编写攻击代码：



3. 复现结果：



浏览器打开 exp.php，通过 get 请求的方式传递给 typecho.php，phpinfo()便可

成功执行。如果想要执行系统命令， 将 phpinfo();替换为 system(‘ls’);即可

心得体会：

通过这次实验的复现了反序列漏洞的实现，构造攻击链利用 PHP，魔法函数进行攻击， 修改 unserialize()的参数传入一个精心构造的序列化字符串， 使我对魔法函数和攻击链的构 造有了初步认识。