学习周记（七）

原创

極品一═☆宏 于 2019-02-13 14:46:49 发布 689 收藏

分类专栏： 基础内容学习

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_43214809/article/details/86999700

版权

基础内容学习 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

信安星火web学习周记（三）

时间：2019年2月9日至2019年2月12日

1.学习内容：

学习http协议，熟练使用burpsuit，了解webshell的基础知识，熟练使用中国菜刀，使用phpstudy搭建文件上传靶场完成前五课。

2.完成情况：

（1）http协议：

作为访问万维网使用的核心通信协议，也是今天所有web应用程序使用的通信协议，http/https广泛地被人们使用。可能我们在生活中接触最多的就是带有HTTP/HTTPS协议的URL，因为URL的请求协议几乎都是HTTP。

事实上，HTTP使用普通的非加密TCP作为其传输机制，HTTPS在本质上与HTTP一样，都属于应用层协议。只不过HTTPS通过安全传输机制（SSL）传送数据，保护了数据的隐秘性与完整性。

HTTP消息分为请求和响应两种，一般情况下打开代理后用burpsuit可以看到请求与响应的相关内容。

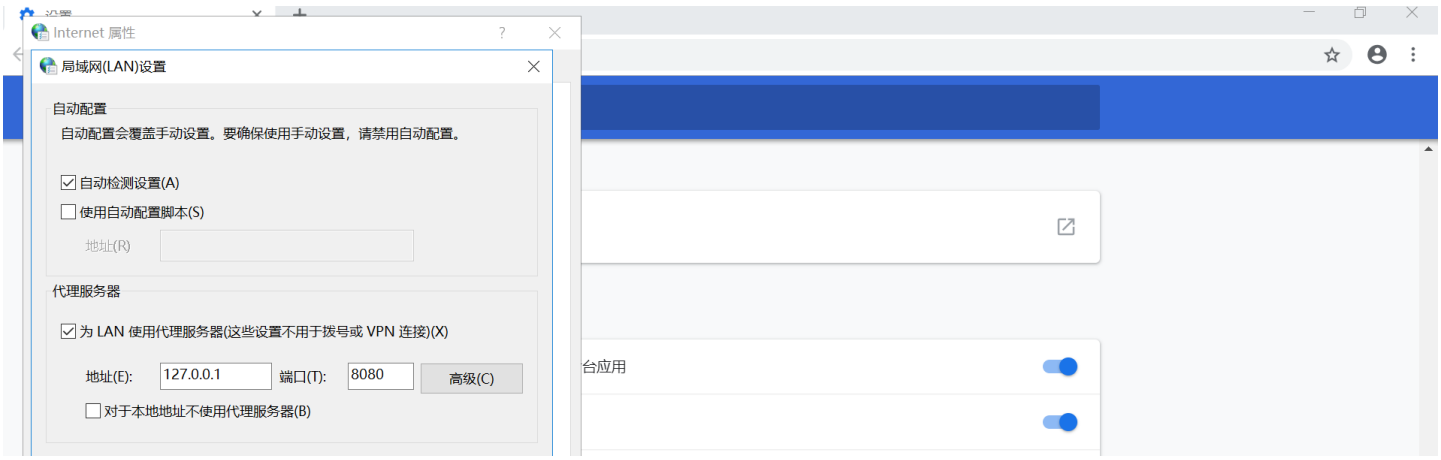
具体的内容我不在这里赘述，因为一方面里面的内容有些繁琐，下面这个链接里给出的解释非常详细，另一方面HTTP协议是一个比较大的方面，单凭几篇文章和几段表述是不太可能完全搞明白的，真正搞明白还是需要一定的知识储备与时间的。

详解链接：http://blog.csdn.net/gueter/article/details/1524447

（2）burpsuite：

当攻击Web应用程序时，除了基本的Web浏览器外，工具包中最有用的工具就是拦截代理服务器。在现在，许多拦截代理服务器已经发展成了许多工具套件，具备各样的功能，就像Burpsuite、Fiddler等等。而Burpsuite的功能最为全面，当然选择什么样的工具是个人喜好，因人而异。就我个人而言，通过之前的做题练习，我还是比较适应Burpsuite，毕竟用的次数也算比较多了。

在启动Burpsuite前，我们需要一些操作，简单来说就是设置代理，打开代理服务器。对Chrome而言，“设置”→“高级”→“打开代理设置”→“局域网设置”→“代理服务器”；设置地址：127.0.0.1，端口：8080



然后打开Burpsuite，虽然是英文，但是通过手册也可以进行熟练的操作，具体的含义网上都可以搜索到，在这里不赘述，还是附上链接，里面给得很详细了。

Burpsuite链接：https://www.cnblogs.com/nieliangcai/p/6692296.html

接下来，我主要针对我自己前期做题时运用Burpsuite的经历来谈谈我自己的感受。

第一次用Burpsuite解题是在GXNNCTF里，第二道买帽子的Web题目。当时是不会做的，赛后看过一些其他人写的writeup，方法不止一种，可以用burpsuite做，也可以不用burpsuite做。如果用burpsuite做的话，是要用到Intruder板块的。在条件竞争的情况下，开两个浏览器，同时发包购买，取cookie作为有效载荷，设置好payload后。点击attack，最后得到flag。因为我做的题里不是很常见Intruder，所以Intruder板块里payloads的一些内容并到现在也不是很清楚，比较模糊。

后来的话，再用burpsuite时就像刚才说的，Intruder就用的比较少了，一种情况下是直接Send to repeater，先看Response；另一种就是先按照题意或自己找到的相关信息在HTTP请求里查找或修改一些内容，最后再Send to repeater。例如有的时候可能在Response里直接给出".txt"或是".php"的相关文件，可以放到url里打开，也有可能是需要修改一些内容，比如说"GET"变成"POST"，在"POST"下添加"Body"变量，或是更改自己输入的内容，在请求里添加一些内容。

总的来说，基本情况就是这样，使用burpsuite的感觉还好。——(￣ー￣*|||——我暂时还没有用过其他的板块，可能以后做题的时候会遇到，到时候再总结吧。

（3）webshell与中国菜刀：

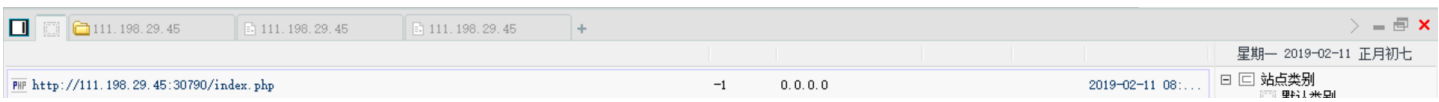
webshell通俗的来讲是网页的后门，通常情况下以asp、php、jsp等网页形式存在的一种命令执行环境。webshell的作用主要体现在站长的网站管理、服务器管理等等。至于其他的作用就是可以被利用，入侵者可以达到长期控制网站的目的。常见的脚本木马有asp、php，也有基于.NET和JSP的脚本木马。

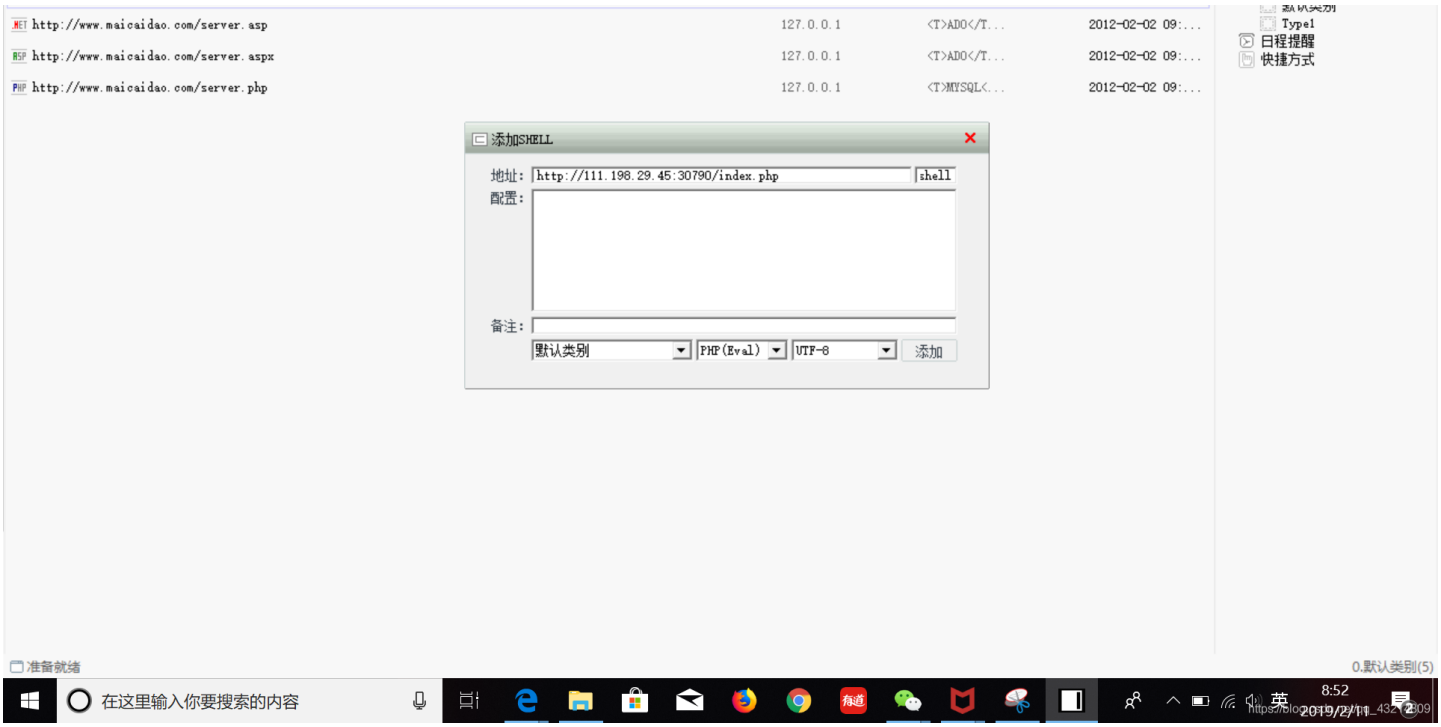
通常情况下都是以一句话木马和菜刀联合使用，一般情况下以php的一句话木马为主。通过上传木马文件，再配合菜刀进行连接，就可以看到一些内容。注意一点就是才到容易被杀毒软件杀掉，安装使用的时候注意一下。下面举个例子：

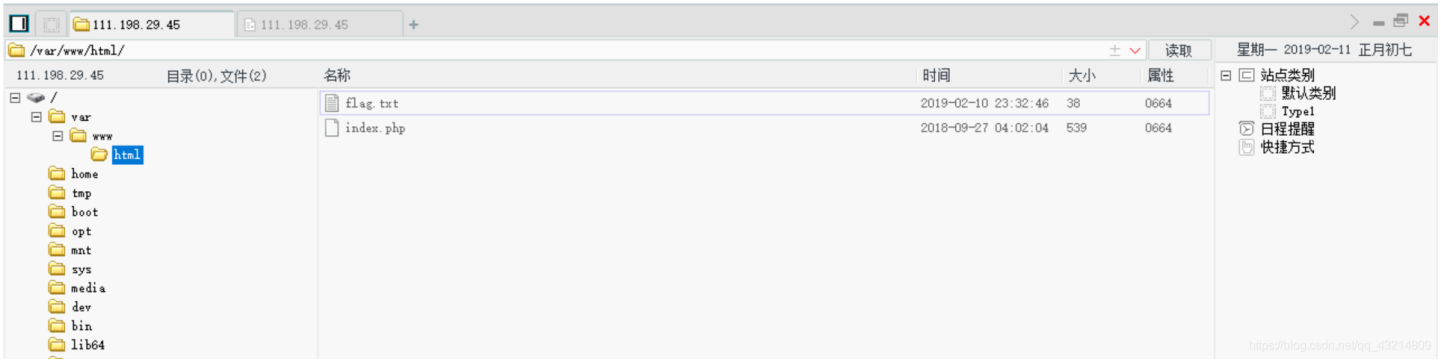
这个非常简单，就是菜刀的简单应用，菜刀直接连接，得到文件目录后，看到falg.txt，直接获取flag：

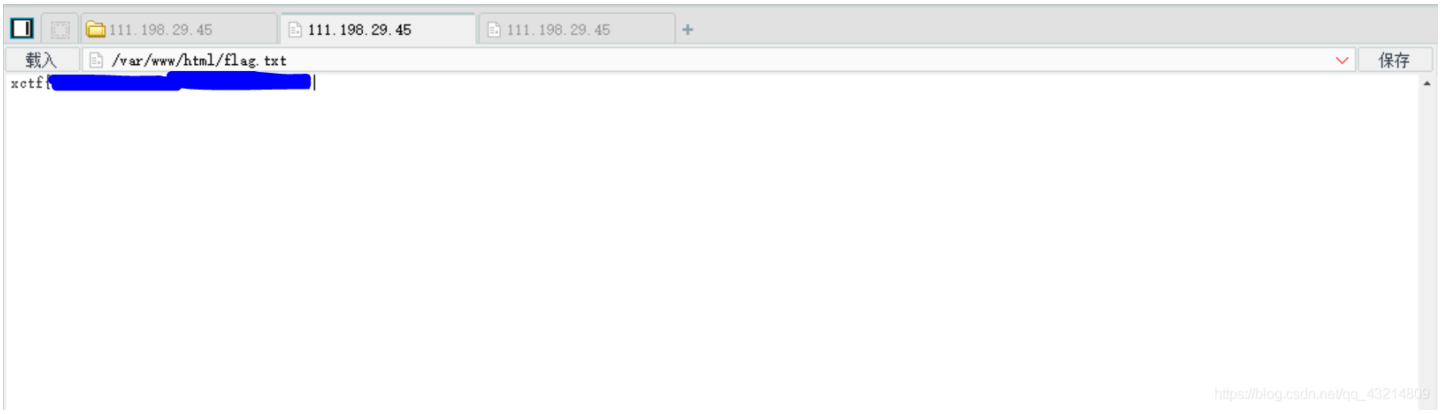
你会使用webshell吗?

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





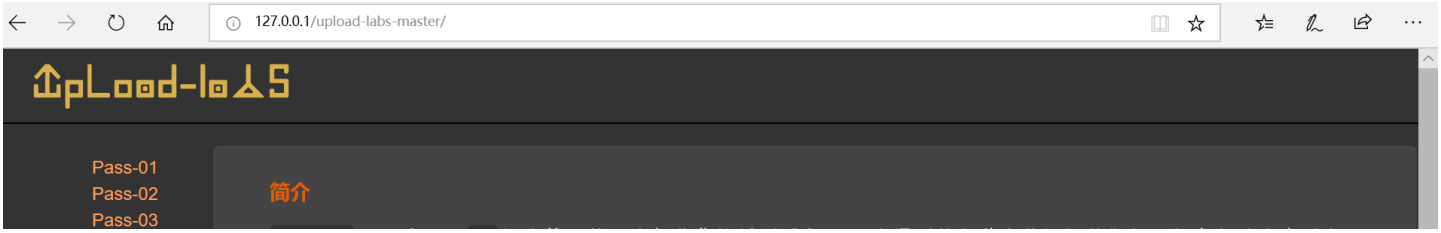


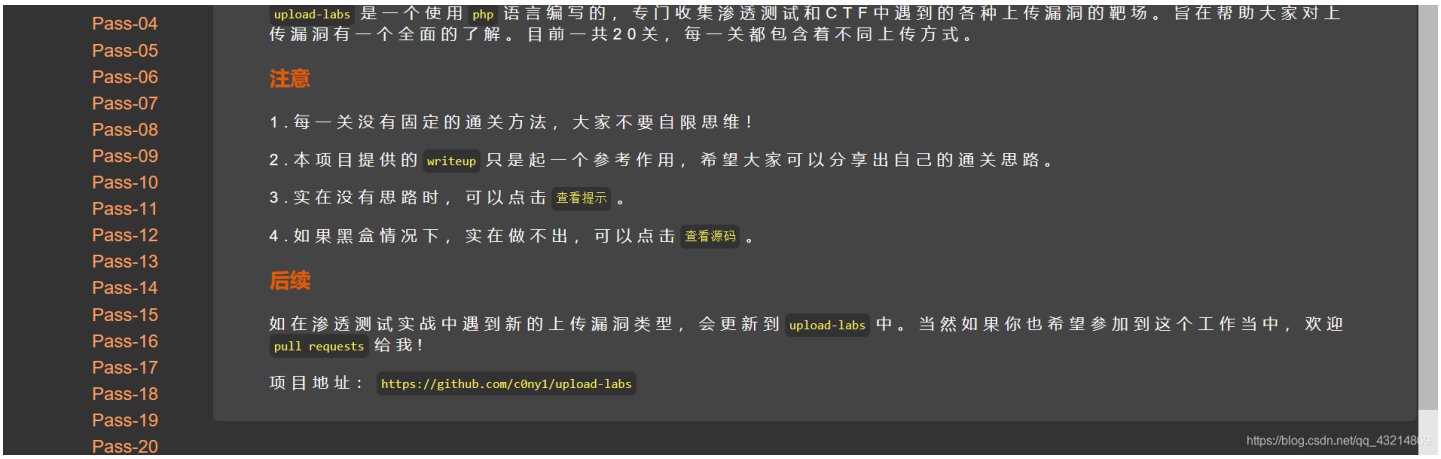


附webshell相关链接：https://www.freebuf.com/articles/web/183520.html

（4）文件上传靶场：

这个靶场直接从github上面下载就可以，解压到phpstudy/www文件夹下就可以开始做题了：





我的burpsuite没有办法在这个环境下截包，一个也截不了。所以就目前情况来看还做不了 ┬┬﹏┬┬ 。