初试ctf wp

原创

Tangthr 于 2019-02-21 18:40:27 发布 1515 收藏 5

分类专栏： ctf 文章标签： ctf

本文链接：https://blog.csdn.net/c1042503039/article/details/87866455

ctf 专栏收录该内容

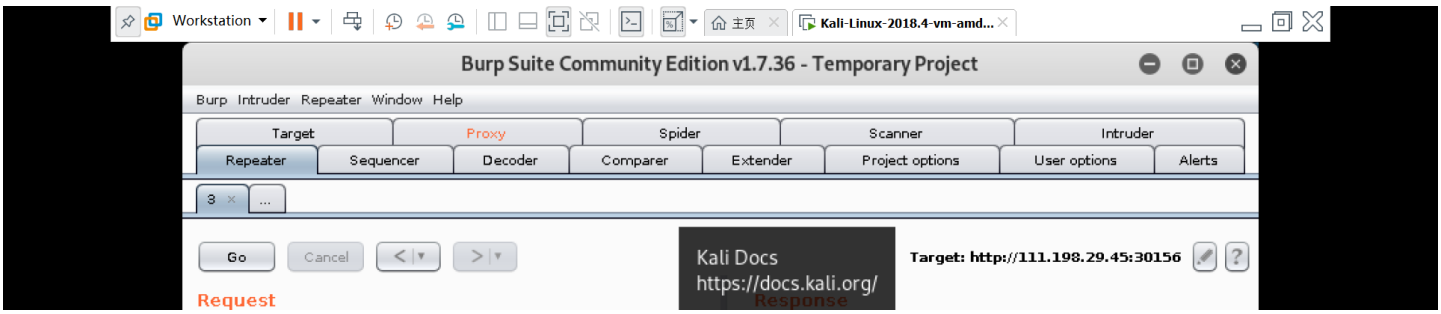
2 篇文章 0 订阅

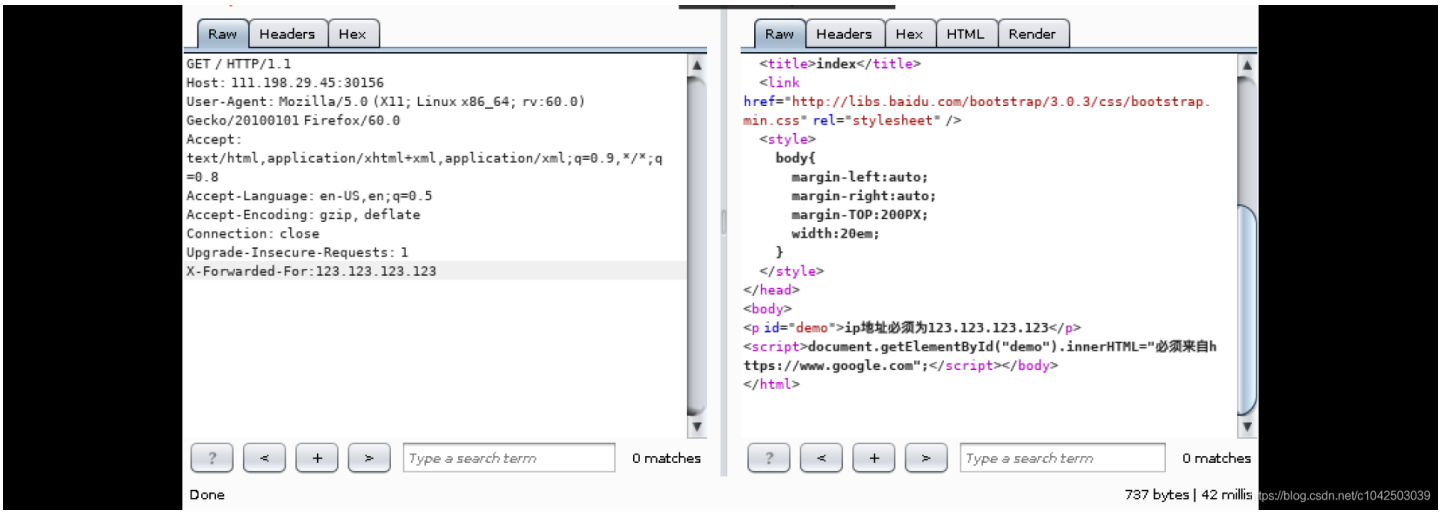
订阅专栏

初试ctf wp

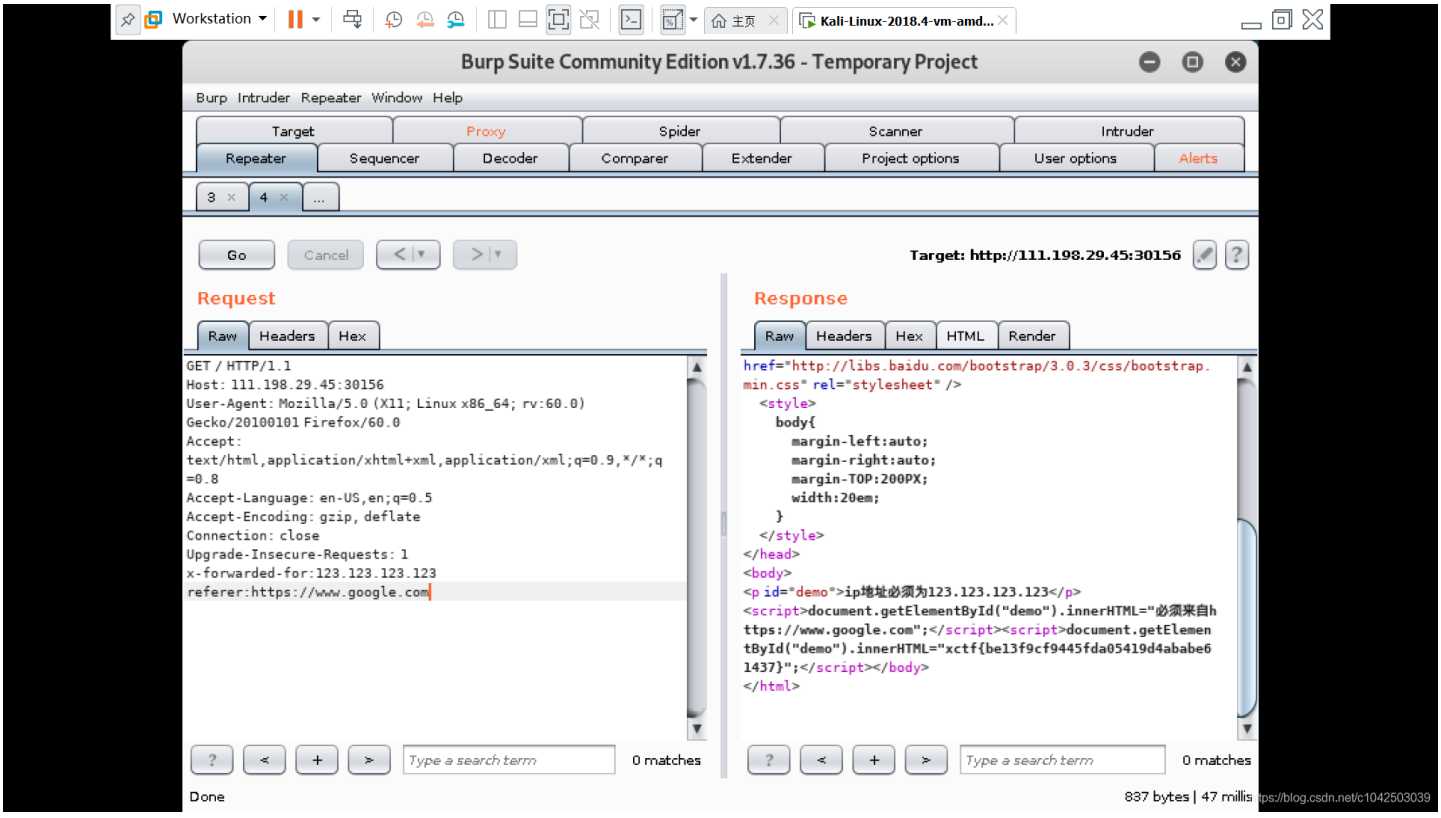
X-forwarded -for和reffer

根据提示，想到要请求真是的ip，于是我用burpsuite，拦截后到repeater，添加xff，这里遇到些问题，到r后，必须先go，再去添加xff才能有正确的提示，经验吧积累。后面又试了又不是这样，纳闷。





看到“必须来自www.google.com”所以想到还要加referer

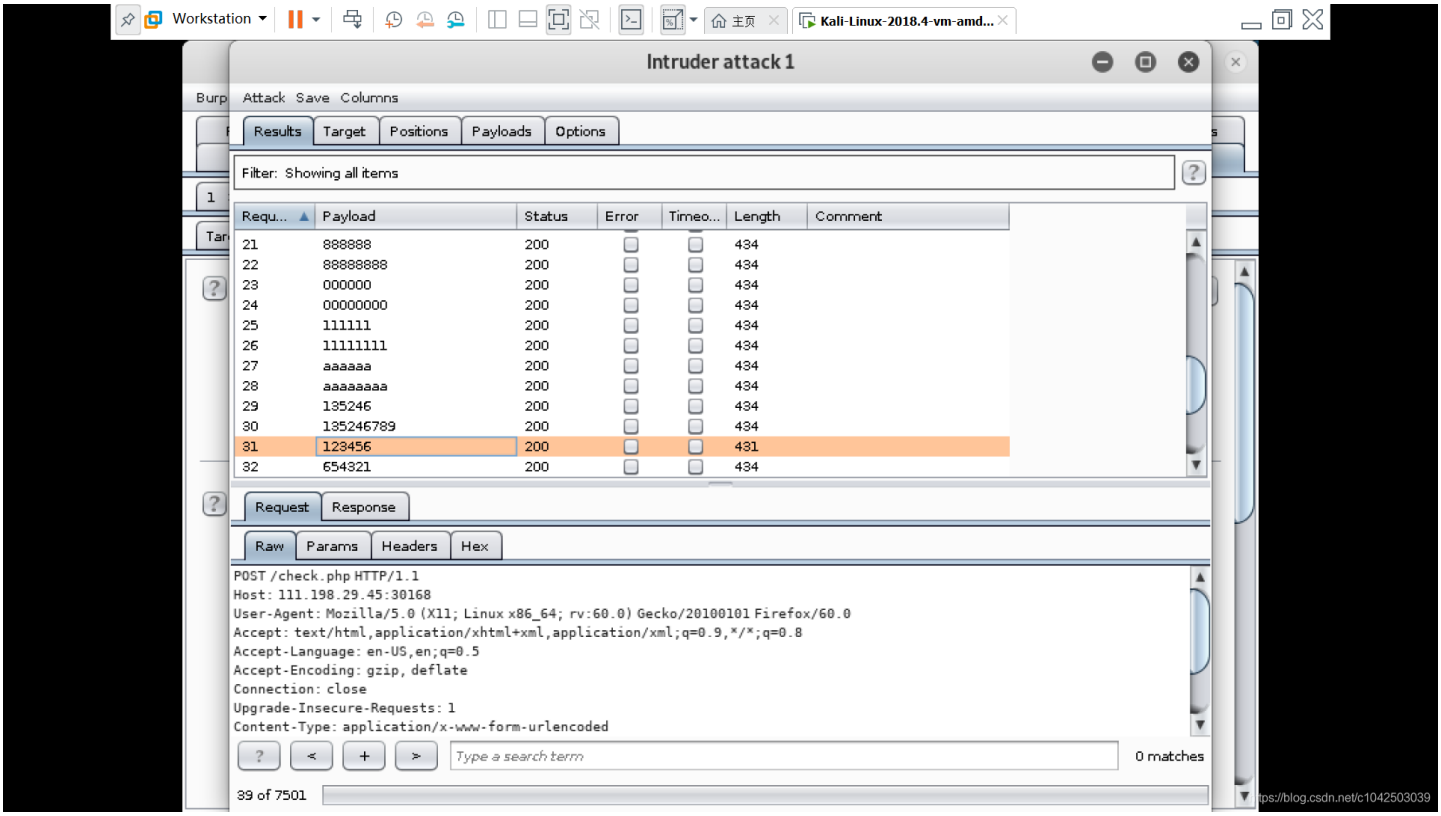


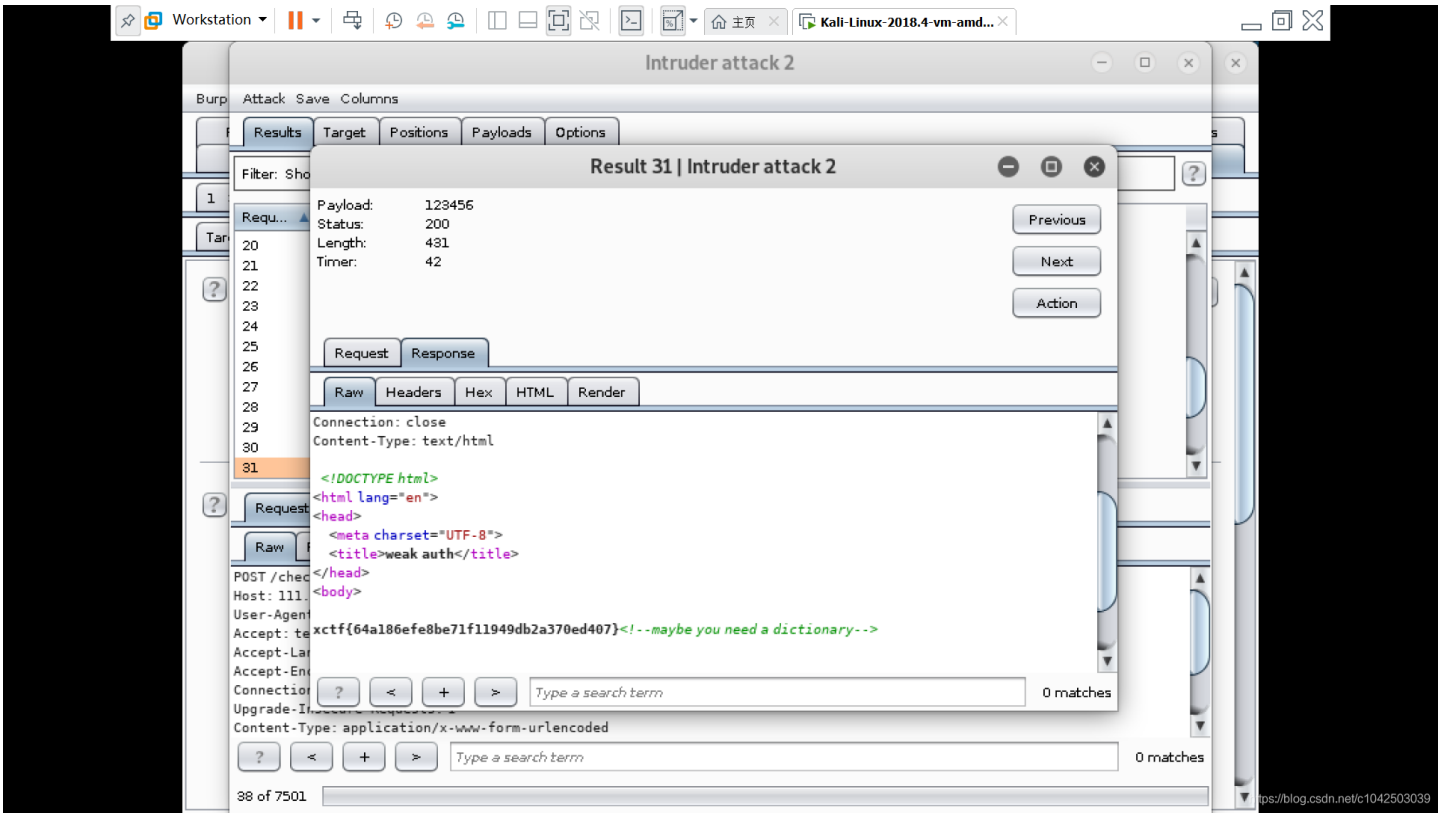
flag就出现了

实验证明，xff可以不用大写，小写也行

密码破解题

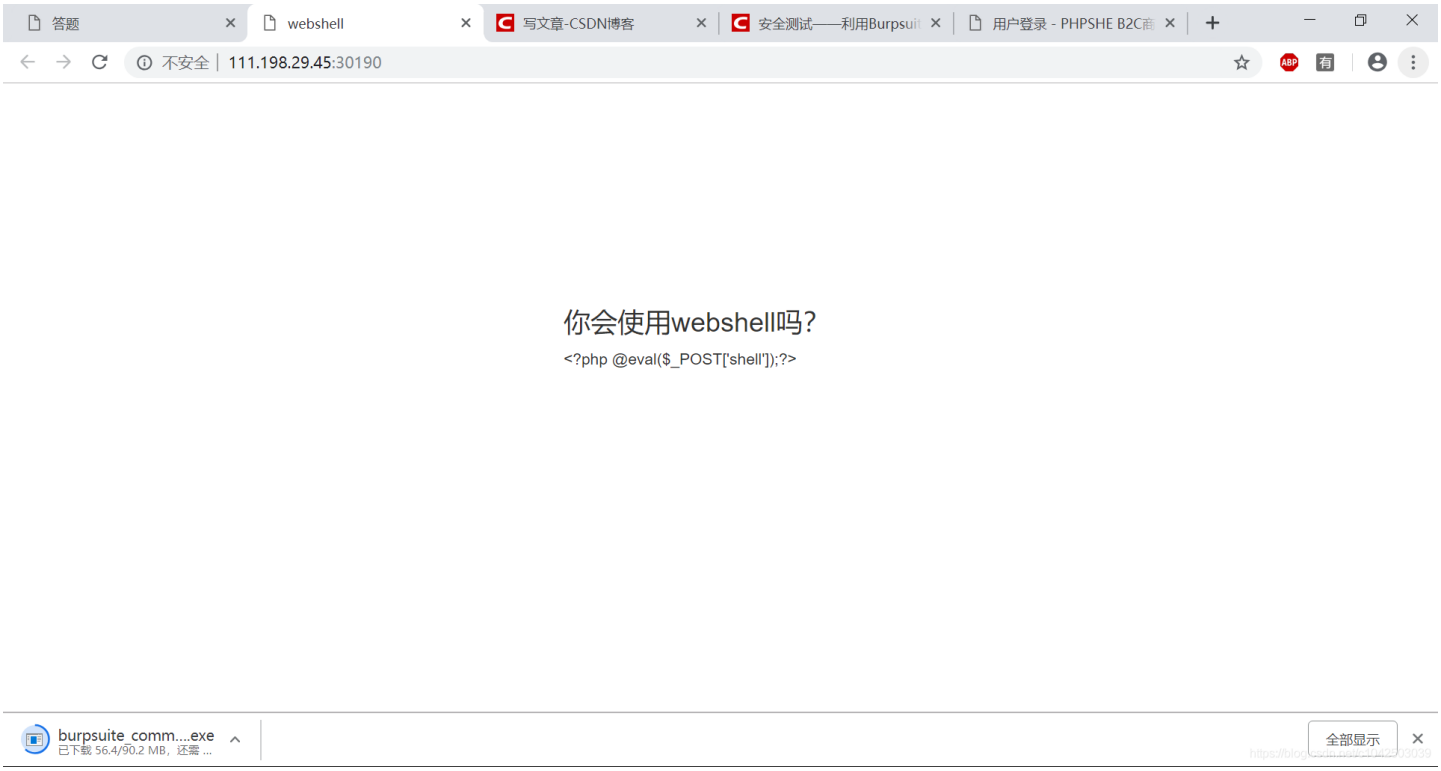
首先随便输入，它会提示要我们用admin作为用户名登陆，照做。之后显示密码错误，然后打开这时的源代码，看见注释“dictionary”，所以需要用字典爆破。在github上下载好字典到文档中（其实就是密码集合），用burpsuite拦截，到intruder,即使再做一遍，依然出现很多问题，郁闷。拦截后要在proxy界面就把username和password写上，不能到intruder写，我也不知道why。到intruder后，设置爆破点，load字典，开始attack。发现123456那一行的后面数字与其他不同，点出来，在点到response，就发现flag了。





在拦截的时候最好是跳回登陆界面，在输入用户名和密码的时候在拦截，这时候很多格式上的东西就会自动帮你写好，避免出现问题。

webshell



这题用的蚁剑，还有另一个方法，是用hackbar post一些命令，但好像是关于php的，我还不懂。
对于蚁剑，下载好加速器和代码后，添加数据，打开，就看到了flag.txt，但我不太明白为什么用dirsearch扫不出来flag.txt。而且不明白密码为啥是shell，是因为题目提示中的post shell呢？还是啥？