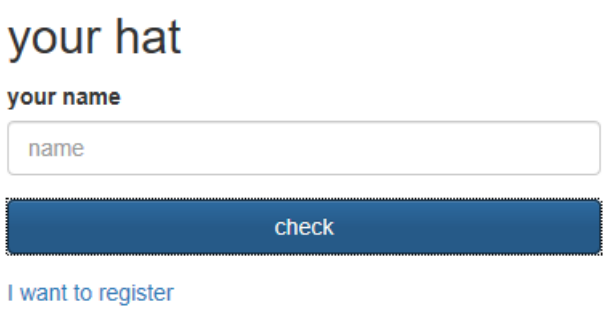
i春秋wanna to see your hat?

转载

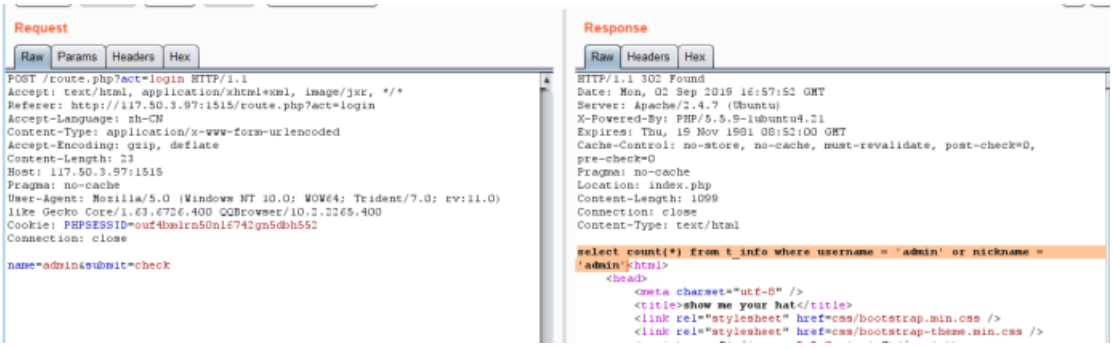
weixin_30701575 于 2019-09-04 22:59:00 发布 110 收藏 1
原文链接：http://www.cnblogs.com/wosun/p/11462167.html

打开题目网页发现是个选择帽子的网页，点击超链接进入一个网页让我们输入我们的name然后匹配帽子颜色（其实不管怎么填都是绿色的）这里也有个注册窗口

先查看源码没什么特别发现，再试试抓包吧



在这个界面抓包



Go一下发现了数据库的注入点

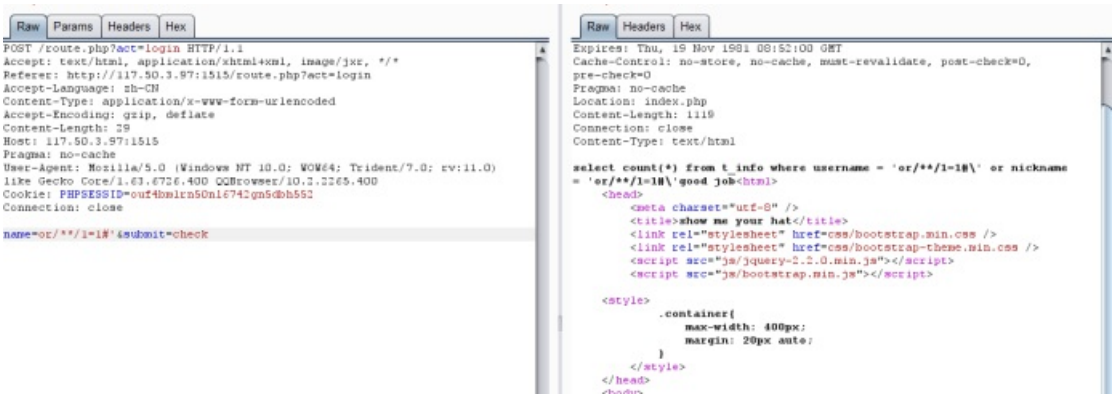
再使用admin'进行测试，发现'被转义为了\

多次测试后发现空格会被过滤，其他也就没什么了

所以这里还是可以进行注入的

我们使用#来注释name后面的内容，构造永真句来让name等于他想要的内容

使用payload：or/**/1=1#'



Go一遍发现可行

将proxy中的name修改后forward回去得到flag

flag{good_job_white_hat}

I give up!

转载于:https://www.cnblogs.com/wosun/p/11462167.html