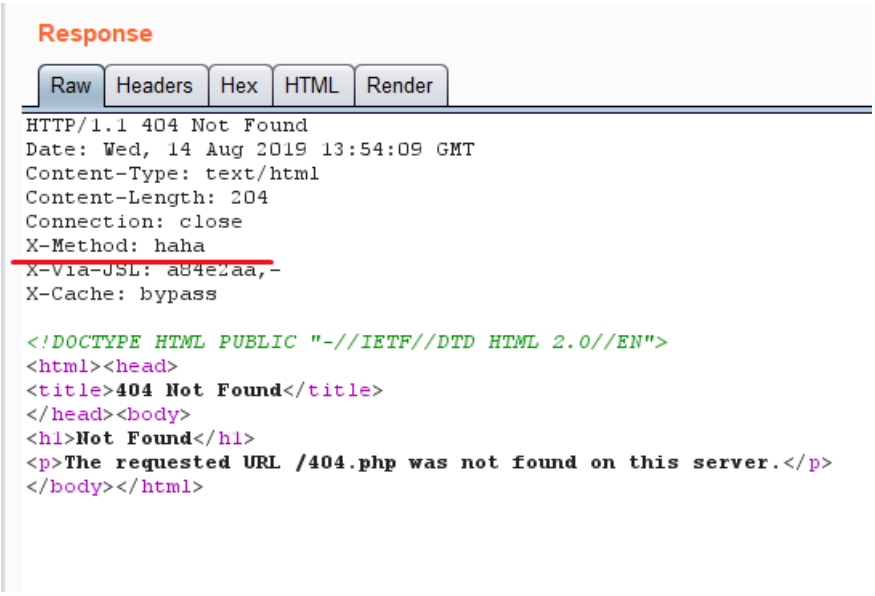
i春秋Not Found

转载

weixin_30701575 于 2019-08-14 23:51:00 发布 115 收藏
文章标签： php
原文链接：http://www.cnblogs.com/wosun/p/11355485.html

点开网页，显示404，告诉我们404.php的存在，我们先试试404.php，打开是haha四个字母，源码和抓包都没看到什么，然后其抓包，也没什么，无功，返回原网页，抓包，没发现什么的感觉，go一遍，在response中发现了刚刚看到的haha四个字母



百度一下

没搜到什么。。。。据别的wp里说的好像是提示我们要注意http的请求方法。。。（具体原因也没说）

这里就继续接着写吧

据菜鸟教程，http有9种请求方法

HTTP 请求方法

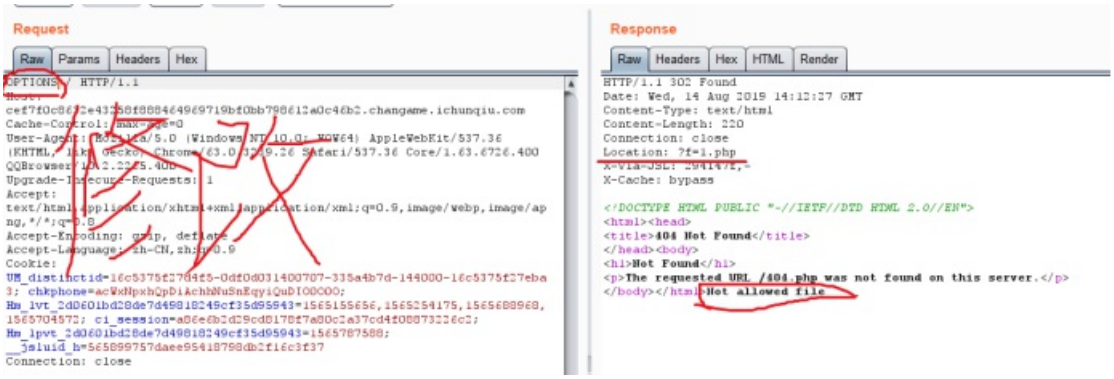
根据 HTTP 标准，HTTP 请求可以使用多种请求方法。

HTTP1.0 定义了三种请求方法： GET, POST 和 HEAD方法。

HTTP1.1 新增了六种请求方法：OPTIONS、PUT、PATCH、DELETE、TRACE 和 CONNECT 方法。

序号	方法	描述
1	GET	请求指定的页面信息，并返回实体主体。
2	HEAD	类似于 GET 请求，只不过返回的响应中没有具体的内容，用于获取报头
3	POST	向指定资源提交数据进行处理请求（例如提交表单或者上传文件），数据被包含在请求体中。POST 请求可能会导致新的资源的建立和/或已有资源的修改。
4	PUT	从客户端向服务器传送的数据取代指定的文档的内容。
5	DELETE	请求服务器删除指定的页面。
6	CONNECT	HTTP/1.1 协议中预留给能够将连接改为管道方式的代理服务器。
7	OPTIONS	允许客户端查看服务器的性能。
8	TRACE	回显服务器收到的请求，主要用于测试或诊断。
9	PATCH	是对 PUT 方法的补充，用来对已知资源进行局部更新 。

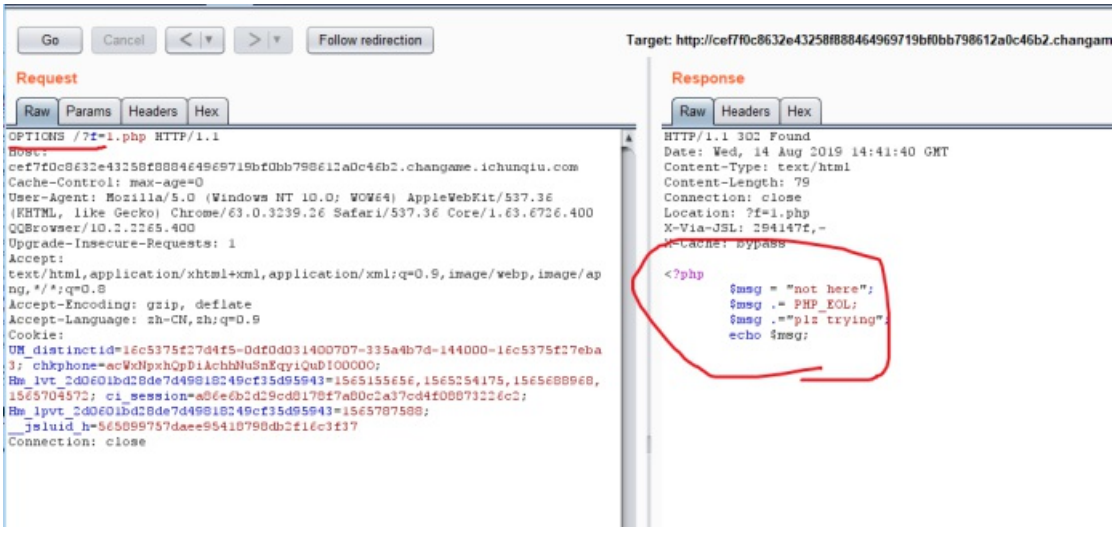
而这里就在抓到的包种逐个修改http请求类型进行尝试



发现当http以options的形式进行请求时出现了文件查询的操作

去url中试试访问/1.php，结果not here plz trying，意思是不在这里，请尝试其他方法。

。。。。无果，在url中加入/?f=1.php试试，没什么显示，查源码，没东西，抓包



正常返回了，也许这里能读取文件，就试试

将OPTIONS后面的文件改为flag.php。。。。。不行

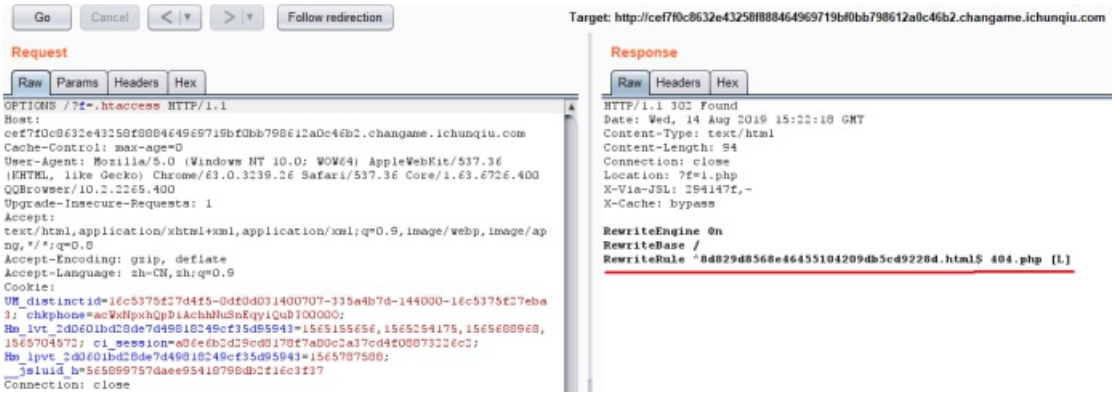
据别的wp里说这里是apache搭建的网页所以根目录里通常有.htaccess配置文件。。。

反正我是没找到哪里说的是apache搭建的。。。

百度了一下，似乎是通过HEAD来判断的，这个操作我还不会

好吧，先展示不管，继续做题

直接?f=.htaccess



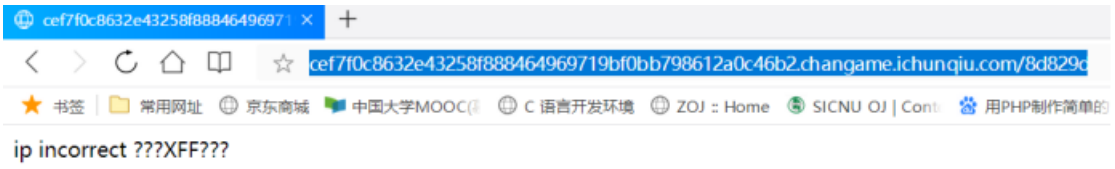
又是两个文件，访问试试。。。。。

1. php可以，不过前面那个文件不能这样读取，需要直接在url中读取就行了

直接访问

http://cef7f0c8632e43258f888464969719bf0bb798612a0c46b2.changame.ichunqiu.com/8d829d8568e464551(

提示我们



Ip不正确，然后询问我们的XFF（网页中的一个设置）

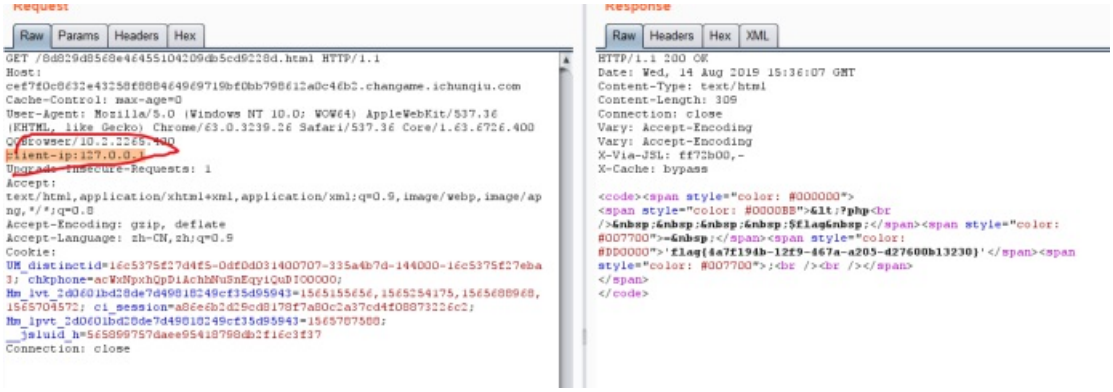
所以这里抓包进行修改

先尝试传入本地ip：X-Forwarded-For:127.0.0.1（不行），他提示了我们XFF的。。。

所以这里还有一种方法client-ip:127.0.0.1

Success！

拿到flag



转载于:https://www.cnblogs.com/wosun/p/11355485.html