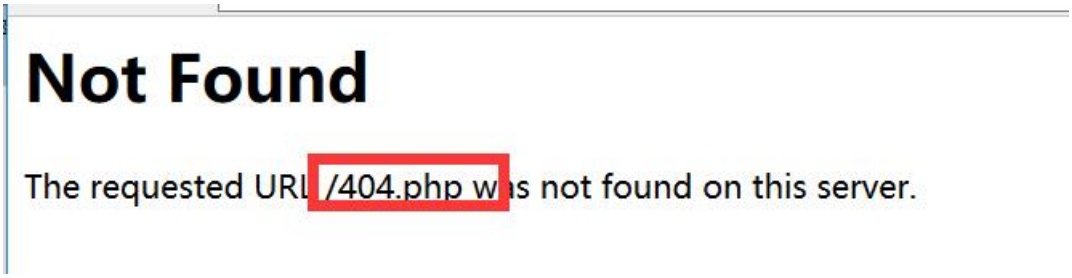
i春秋——“百度杯”CTF比赛 十月场——Not Found（http请求方法，client-ip伪造ip）...

转载

weixin_30426957 于 2018-10-14 11:24:00 发布 187 收藏
文章标签： php
原文链接：http://www.cnblogs.com/leixiao-/p/9785710.html

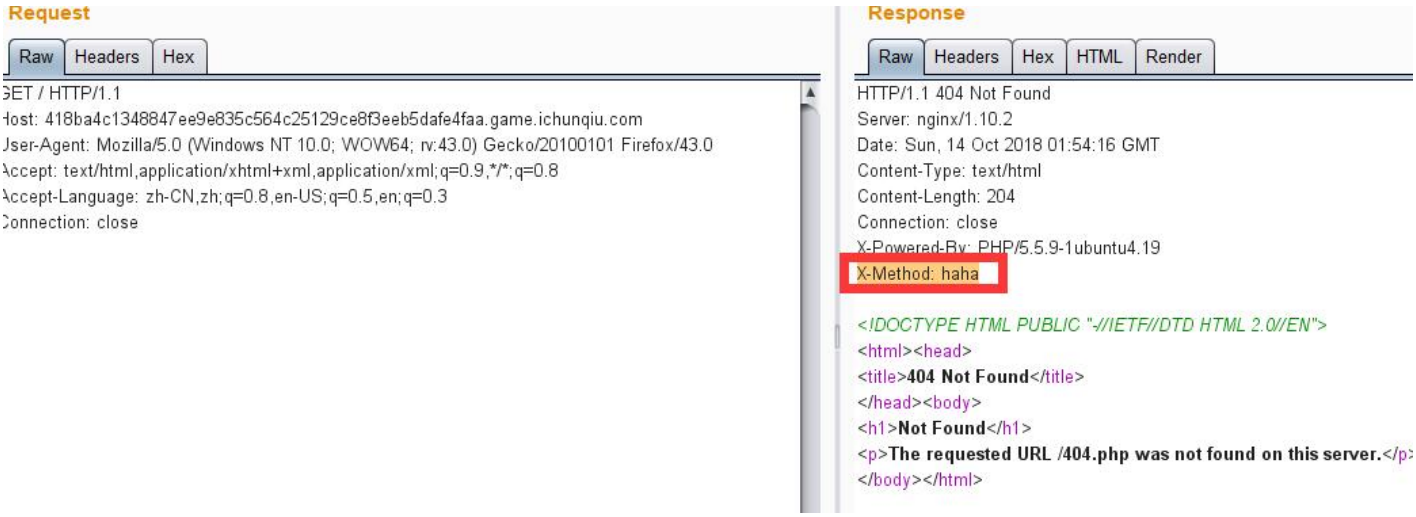
这道题也是让我很迷。。。

打开就是not found，让我一度以为是服务器挂了，细看发现有个404.php

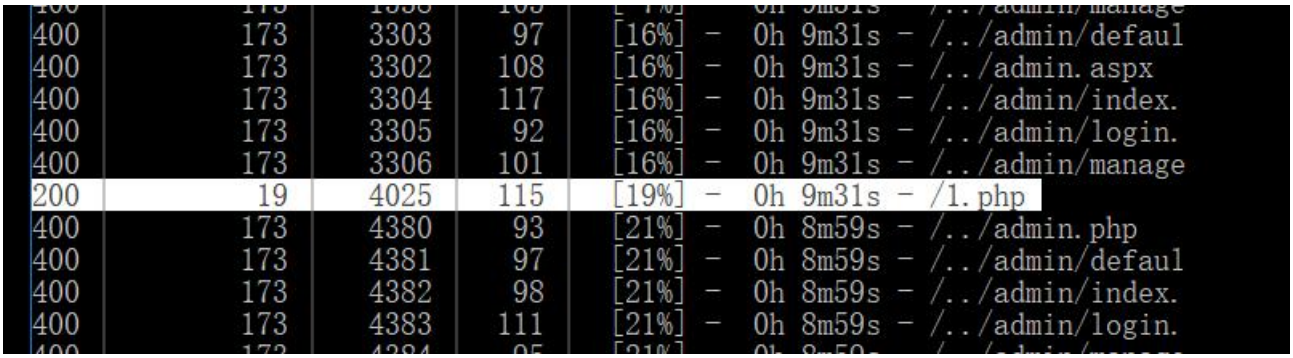


访问也没发现什么东西，只有来自出题人的嘲讽 haha~

不过在首页的header中发现个奇怪的东西，X-Method:haha，先记着，继续找线索



用cansina扫描发现一个文件 1.php，不过访问也没发现什么有用的东西，只提示 not here，plese trying

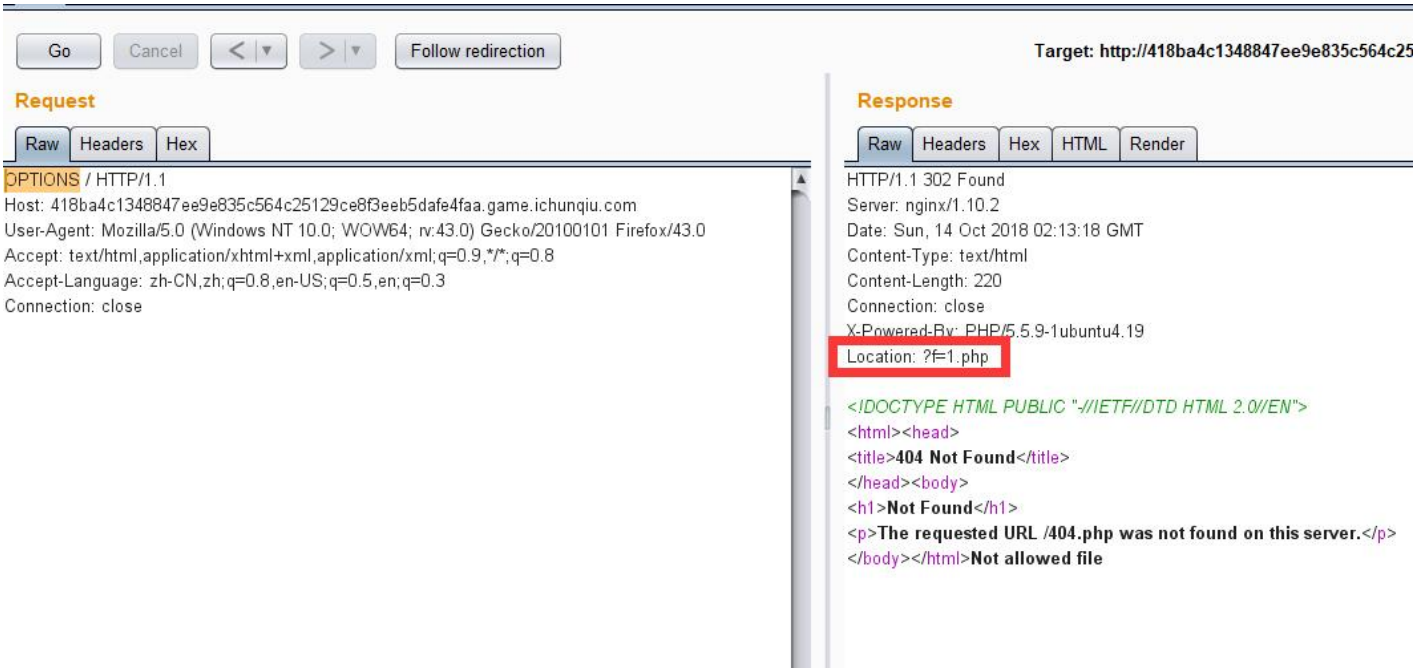


接着我是一顿各种尝试，无果。。。

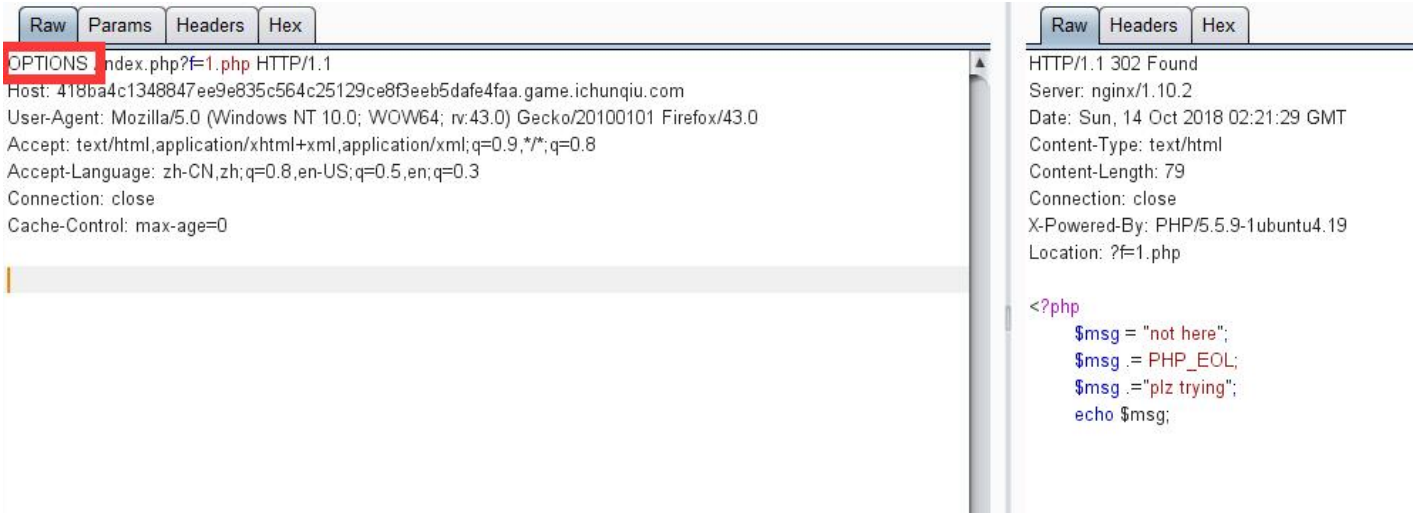
最后看过提示，才知道X-Method:haha是在告诉我们要注意http的请求方法，http共有8种请求方法，如下

> 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。

逐个测试，当到了OPTIONS时，发现

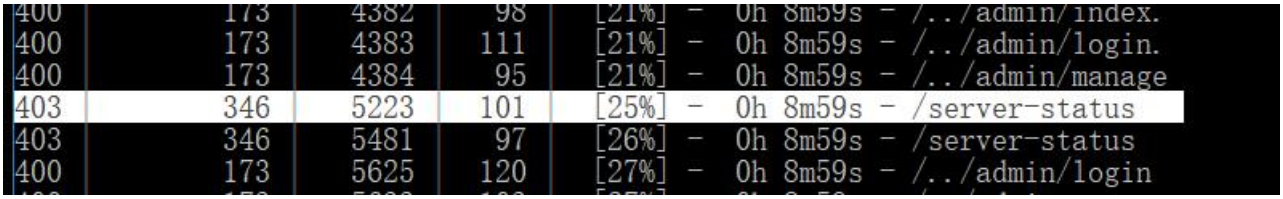


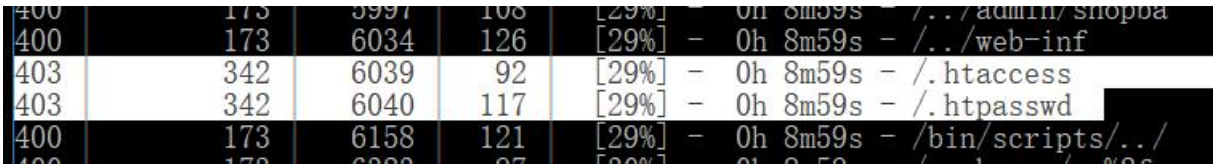
经测试直接访问这个url的话，页面不变，所以想到应该还是依旧用OPTIONS方法，于是在访问该url的时候抓包，然后在burp中修改请求方法，得到



然而这个文件并没有什么用，但是访问index.php 和 404.php 又不被允许

折腾了很久，才想起来之前cansina扫描到几个403无权访问的文件





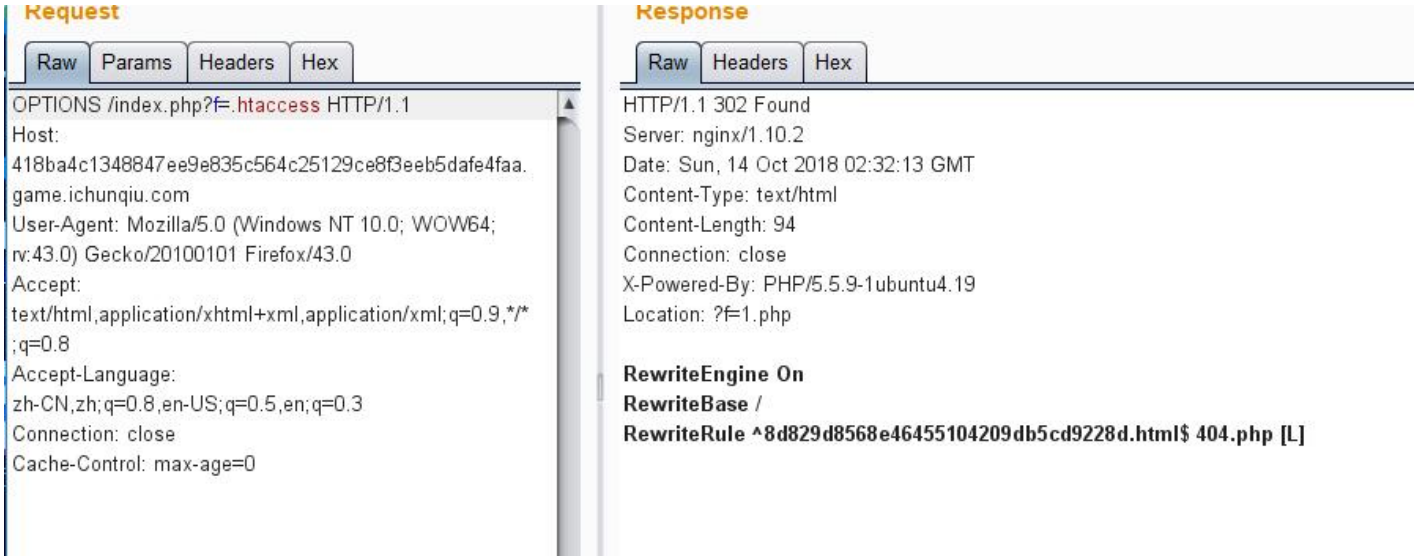
> .htaccess文件(或者"分布式配置文件"）,全称是Hypertext Access(超文本入口)。提供了针对目录改变配置的方法， 即，在一个特定的文档目录中放置一个包含一个或多个指令的文件， 以作用于此目录及其所有子目录。作为用户，所能使用的命令受到限制。管理员可以通过Apache的AllowOverride指令来设置。概述来说，htaccess文件是Apache服务器中的一个配置文件，它负责相关目录下的网页配置。通过htaccess文件，可以帮我们实现：网页301重定向、自定义404错误页面、改变文件扩展名、允许/阻止特定的用户或者目录的访问、禁止目录列表、配置默认文档等功能。

简单说，就是一个只对该文件所在的目录起作用的配置文件，里面的配置也会覆盖php.ini。扯个题外话，这种分布式配置文件大有用途，详见：

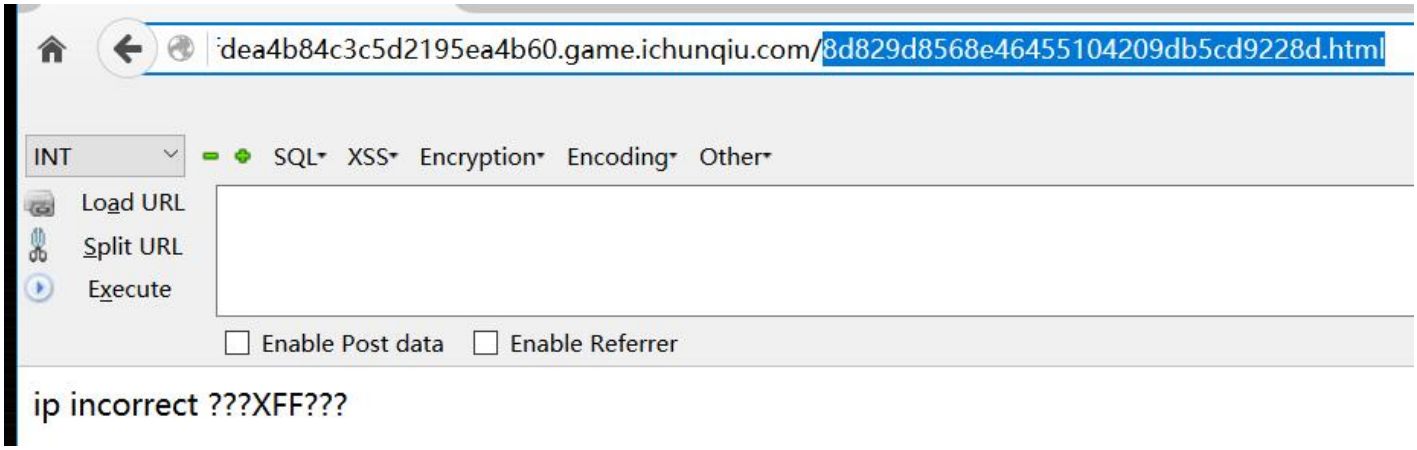
.user.ini文件构成的PHP后门： http://www.vuln.cn/6001

利用.htaccess来执行你的webshell： https://bbs.2cto.com/read.php?tid=204685

回到正题，访问该文件，得到一个html的地址



看到如下，自然想到是利用X-Forwarded-For伪造ip



尝试了多次 X-Forwarded-For:127.0.0.1 都不行，实在没办法，又看了下提示，发现除了X-Forwarded-For，还有client-ip。没系统学过http协议，对这些也不甚了解真的吃亏啊。。。

详见：https://segmentfault.com/q/1010000000686700/a-1020000000687155

转载于:https://www.cnblogs.com/leixiao-/p/9785710.html