

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>

版权

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

Not Found

The requested URL **/404.php** was not found on this server.

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

The screenshot shows the browser's developer tools with the 'Response' tab selected. The response is an HTTP 404 Not Found. The headers section is expanded, showing 'X-Method: haha' highlighted with a red box. The HTML body contains the text 'The requested URL /404.php was not found on this server.'

```
Request
Raw Headers Hex
GET / HTTP/1.1
Host: 418ba4c1348847ee9e835c564c25129ce8f3eeb5dafa4faa.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Connection: close

Response
Raw Headers HTML Render
HTTP/1.1 404 Not Found
Server: nginx/1.10.2
Date: Sun, 14 Oct 2018 01:54:16 GMT
Content-Type: text/html
Content-Length: 204
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
X-Method: haha

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /404.php was not found on this server.</p>
</body></html>
```

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, please trying

400	173	3303	97	[16%]	-	0h 9m31s	-	././admin/manage
400	173	3302	108	[16%]	-	0h 9m31s	-	././admin/default
400	173	3304	117	[16%]	-	0h 9m31s	-	././admin.aspx
400	173	3305	92	[16%]	-	0h 9m31s	-	././admin/index.
400	173	3306	101	[16%]	-	0h 9m31s	-	././admin/login.
200	19	4025	115	[19%]	-	0h 9m31s	-	././1.php
400	173	4380	93	[21%]	-	0h 8m59s	-	././admin.php
400	173	4381	97	[21%]	-	0h 8m59s	-	././admin/default
400	173	4382	98	[21%]	-	0h 8m59s	-	././admin/index.
400	173	4383	111	[21%]	-	0h 8m59s	-	././admin/login.
400	173	4384	95	[21%]	-	0h 8m59s	-	././admin/manage

接着我是一顿各种尝试，无果。。。

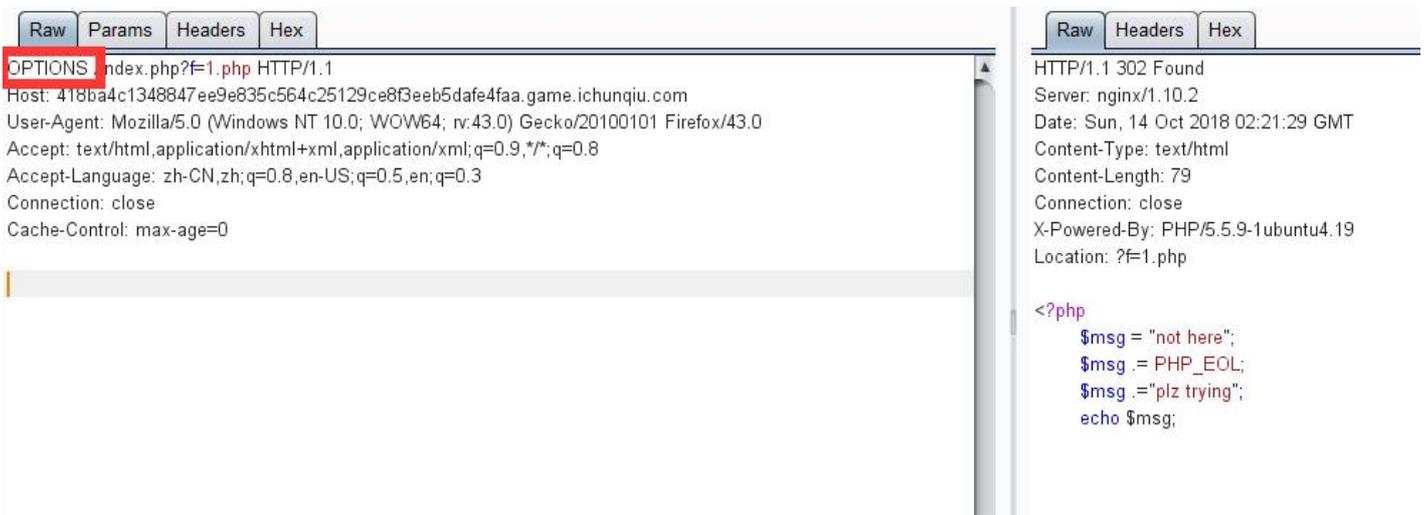
最后看过提示，才知道X-Method:haha是在告诉我们要注意http的请求方法，http共有8种请求方法，如下

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

The screenshot shows the Burp Suite interface. On the left, the 'Request' tab is active, displaying an OPTIONS request for the URL http://418ba4c1348847ee9e835c564c25129ce8f3eeb5dafa4faa.game.ichunqiu.com. The request headers include Host, User-Agent, Accept, and Accept-Language. On the right, the 'Response' tab is active, showing an HTTP/1.1 302 Found response. The response headers include Server, Date, Content-Type, Content-Length, Connection, X-Powered-By, and Location: ?f=1.php. The response body contains HTML code indicating a 404 Not Found error: <title>404 Not Found</title>, <h1>Not Found</h1>, and <p>The requested URL /404.php was not found on this server.</p>. The Location header in the response is highlighted with a red box.

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

400	173	4382	98	[21%]	-	0h 8m59s	-	../admin/index.
400	173	4383	111	[21%]	-	0h 8m59s	-	../admin/login.
400	173	4384	95	[21%]	-	0h 8m59s	-	../admin/manage
403	346	5223	101	[25%]	-	0h 8m59s	-	/server-status
403	346	5481	97	[26%]	-	0h 8m59s	-	/server-status
400	173	5625	120	[27%]	-	0h 8m59s	-	../admin/login
400	173	5997	108	[29%]	-	0h 8m59s	-	../admin/shopba
400	173	6034	126	[29%]	-	0h 8m59s	-	../web-inf
403	342	6039	92	[29%]	-	0h 8m59s	-	/.htaccess
403	342	6040	117	[29%]	-	0h 8m59s	-	/.htpasswd
400	173	6158	121	[29%]	-	0h 8m59s	-	/bin/scripts/..

.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

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
<pre>OPTIONS /index.php?f=.htaccess HTTP/1.1 Host: 418ba4c1348847ee9e835c564c25129ce8f3eeb5dafa4faa. game.ichunqiu.com User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/* ;q=0.8 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Connection: close Cache-Control: max-age=0</pre>				<pre>HTTP/1.1 302 Found Server: nginx/1.10.2 Date: Sun, 14 Oct 2018 02:32:13 GMT Content-Type: text/html Content-Length: 94 Connection: close X-Powered-By: PHP/5.5.9-1ubuntu4.19 Location: ?f=1.php RewriteEngine On RewriteBase / RewriteRule ^8d829d8568e46455104209db5cd9228d.html\$ 404.php [L]</pre>		

看到如下，自然想到是利用X-Forwarded-For伪造ip

The screenshot shows a web browser address bar with the URL: `dea4b84c3c5d2195ea4b60.game.ichunqiu.com/8d829d8568e46455104209db5cd9228d.html`. Below the address bar is a tool interface with a dropdown menu set to 'INT' and several buttons: 'Load URL', 'Split URL', and 'Execute'. There are also checkboxes for 'Enable Post data' and 'Enable Referrer'. The page content below the tool shows the text: 'ip incorrect ???XFF???'.

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>

