CTf_WriteUp_HTTP——302临时重定向

原创

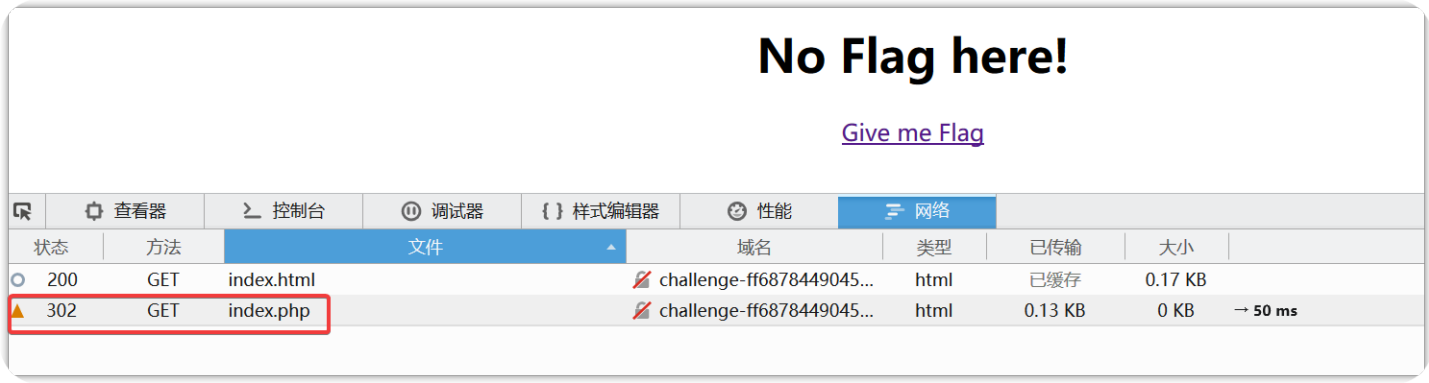
Art_Dillon 于 2020-03-26 00:07:08 发布 1343 收藏 8

分类专栏： CTF 文章标签： http

本文链接：https://blog.csdn.net/c1ata/article/details/105108309

HTTP——302临时重定向

题目描述

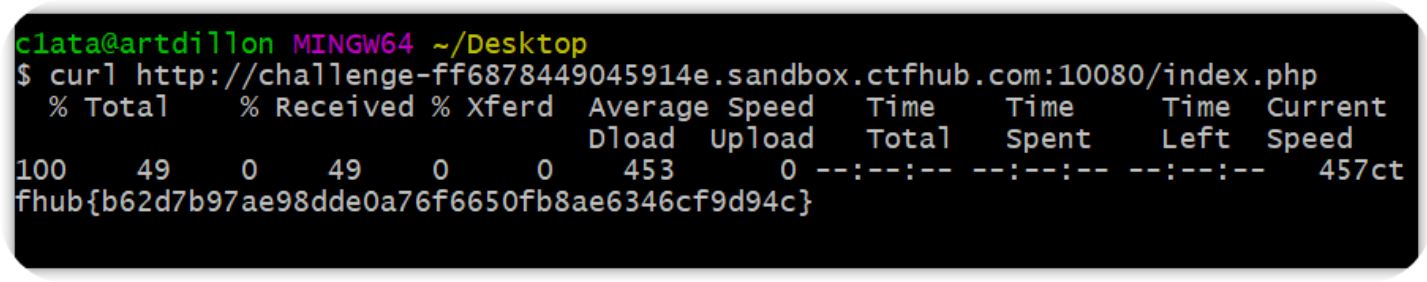


点击给出的链接后，没有发生任何变化。

解决方案

通过擦好看网络请求，可以发现发生了302临时跳转，所以我们无法通过浏览器直接访问未跳转的页面，而flag 可能藏在我们目前无法访问的页面之中。所以我们要想办法去访问未跳转的原网站。

而不强制跳转我们可以通过`curl`指令来完成。因为curl默认是不跟随重定向的。



成功在命令行中找出flag；

相关知识

什么是HTTP 302 跳转？

首先我们要知道**状态码**，状态码是HTTP请求过程**结果的描述**，由三位数字组成。这三位数字描述了请求过程中所发生的情况。状态码位于**响应的起始行**中，如在 HTTP/1.0 200 OK 中，状态码就是 200。

每个状态码的**第一位数字**都用于描述状态（“成功”、“出错”等）。如200 到 299 之间的状态码表示成功；300 到 399 之间的代码表示资源已经转移。400 到 499 之间的代码表示客户端的**请求出错**了。500 到 599 之间的代码表示**服务器出错**了。

整体范围	已定义范围	分　　类
100～199	100～101	信息提示
200～299	200～206	成功
300～399	300～305	重定向
400～499	400～415	客户端错误
500～599	500～505	服务器错误

那么302就属于重定向的状态码，它表示你要访问的资源在别的地方。

301	Moved Permanently	在请求的URL已被移除时使用。响应的Location首部中应该包含资源现在所处的URL
302	Found	与301状态码类似；但是，客户端应该使用Location首部给出的URL来临时定位资源。将来的请求仍应使用老的URL

302表示临时重定向，而301表示永久重定向；

PHP 302 跳转代码

```php
<?php
    header("HTTP/1.1 302 found");
    header("Location:https://www.baidu.com");
    exit();
?>
```

PHP 301 跳转代码

```php
<?php
    header("HTTP/1.1 301 Moved Permanently");
    header("Location: http://www.baidu.com/");
    exit();
?>
```

curl 指令

`curl`是一种命令行工具，作用是**发出网络请求**，然后**得到和提取数据**。

我们直接在`curl命令`后加上网址，就可以看到网页源码。

```
curl www.baidu.com
```

```
$ curl www.baidu.com
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2381  100  2381    0     0  20350      0 --:--:-- --:--:-- --:--:-- 20350<!DOCTYPE html>
<!--STATUS OK--><html> <head><meta http-equiv=content-type content=text/html;charset=utf-8><meta http-equiv=X-UA
-Compatible content=IE=Edge><meta content=always name=referrer>
   ......


 </html>
```

curl 默认是不进行重定向的。如果要进行重定向，我们需要加上-L参数

```
curl -L taobao.com
```

加上 `-o 参数` 可以保存网页源代码到本地

```
curl -o taobao.txt taobao.com -L
```

加上`-i参数`可以看到**响应报文**

```
curl -i baidu.com
```

```
$ curl -i baidu.com
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    81  100    81    0     0    627      0 --:--:-- --:--:-- --:--:--   627HTTP/1.1 200 OK
Server:
Date: Wed, 25 Mar 2020 16:00:02 GMT
Content-Type: text/html
Content-Length: 81
Connection: keep-alive
Last-Modified: Tue, 12 Jan 2010 13:48:00 GMT
ETag: "51-47cf7e6ee8400"
Accept-Ranges: bytes

<html>
<meta http-equiv="refresh" content="0;url=http://www.baidu.com/">
</html>
```

除此之外，curl 的功能远不止如此。以后再慢慢研究。