




9、XCTF get_post

原创

山兔1  于 2021-09-16 23:34:16 发布  20  收藏

分类专栏: [CTF](#) 文章标签: [http java](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_53008479/article/details/120339930

版权



[CTF 专栏收录该内容](#)

50 篇文章 1 订阅

订阅专栏

X 老师告诉小宁同学 HTTP 通常使用两种请求方法, 你知道是哪两种吗?

打开网站, 看到下面

请用 GET 方式提交一个名为 a, 值为 1 的变量。

构造 payload,

```
http://111.200.241.244:50152/?a=1
```

得到,

请再以 POST 方式随便提交一个名为 b, 值为 2 的变量

在构造一个

```
http://111.200.241.244:50152/?a=1
```

```
Poat data
```

```
b=2
```

得到 flag。

基础知识:

HTTP 协议中共定义了八种方法或者叫“动作”来表明对 Request-URI 指定的资源的不同操作方式, 具体介绍如下:

GET: 向特定的资源发出请求。

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创建和/或已有资源的修改。

OPTIONS: 返回服务器针对特定资源所支持的 HTTP 请求方法。也可以利用向 Web 服务器发送 '*' 的请求来测试服务器的功能性。

HEAD: 向服务器索要 GET 请求相一致的响应, 只不过响应体将不会被返回。这一方法可以在不必传输整个响应内容的情况下, 就可以获取包含在响应消息头中的元信息。

PUT: 向指定资源位置上传其最新内容。

DELETE: 请求服务器删除 Request-URI 所标识的资源。

TRACE: 回显服务器收到的请求, 主要用于测试或诊断。

CONNECT: HTTP/1.1 协议中预留能够将连接改为管道方式的代理服务器。