

密码学教室入门（二）

易知mlfrj{Hfjxfw_hnumjw_8x_ozxy_ktw_kzs}是加密后的flag
与hgame{}对比得知所有字母后移了五位
处理后得hgame{Caesar_cipher_3s_just_for_fun}

lightless的渗透教室入门篇（一）

同时发送get和post请求，如下图所示

INT

Load URL

Split URL

Execute

SQL• XSS• Encryption• Encoding• Other•

http://115.28.78.16:13333/pentest/01/?hacker=HelloGet

☒ Enable Post data

☐ Enable Referrer

Post data

hacker=HelloPost

禁用• Cookies• CSS• 表单• 图片• 网页信息• 其他功能• 标记• 缩放• 工具• 查看源代码• 选项•

想要学习渗透，第一步是先要明白我们是通过什么样的方法获取到网页的。下面有几篇学习资料，仔细阅读后完成本题。

• W3School - 简单易懂，深度不够

• RFC2616-sec5-request - 晦涩复杂，选择阅读

• RFC2616-sec9-method - 晦涩复杂，选择阅读

• 扩展阅读：《HTTP权威指南》，经典必读书目，drops曾经有提到过。

• 扩展阅读：《图解HTTP》，多了几张图，小书，也可以参考看看。

题目内容：

• 向本页面同时发送GET和POST请求；

• GET请求内容为hacker=HelloGet

• POST请求内容为hacker=HelloPost

• 如果你不知道如何发送POST请求，方法一：学习curl命令。方法二：学习burp工具。方法三：学习Chrome/Firefox上的开发者工具或各种浏览器插件。

hctf{PostAndGetIsSoEasy_comeon!}

可得flag：hctf{PostAndGetIsSoEasy_comeon!}