

【WP】攻防世界新手Web&Crypto writeup

原创

[Tiumo](#) 于 2019-12-27 15:41:00 发布 108 收藏

文章标签: [php](#) [laravel](#) [thinkphp](#) [wordpress](#) [curl](#)

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/y320284/article/details/108646694>

版权

viewsource

- 直接f12, 或者chrome在url前加view-source:

getpost

- 直接加参数就行了。
- POST参数不用工具直接加个form就行了。

robots

- 查看robots文件会得到一个php的文件, 访问获得flag。

backup

- 下载文件index.php.bak获得flag。

cookie

- 查看cookie, 可以知道存在cookie.php, 访问后从http头得到flag。

disabled_button

- 直接改源码, 删掉disabled属性。

simplejs

- 写了一大堆没什么用的代码, 其实就是把fromCharCode一个一个读出来, 直接把fromCharCode解码再转char就行了。

xff_Referer

- 伪造X-Forwarded-For和Referer。

weak_auth

- 弱口令, 随便猜几个就猜到了。

webshell

- 使用蚁剑连接扫目录, 下载flag.txt获得flag。

command_execution

- 命令拼接, 先用find指令找到flag.txt, 在cat指令查看。

simple_php

- a=
- b=1235a

base64

- 直接base解码

caeser

- 凯撒密码，偏移量12

Morse

- 莫尔斯码，1换成-，0换成.

Railfence

- 手动分栏：提示词是cyberpeace，闭括号一定在最后一个

不仅仅是Morse

- 莫尔斯码加上培根加密