# BUUCTF web WarmUp writeup

原创

wow小华 于 2020-12-19 10:36:27 发布 101 收藏 3

分类专栏： ctf buuctf 刷题日记 文章标签： php



本文链接：https://blog.csdn.net/weixin_45642610/article/details/111386031



ctf 同时被 3 个专栏收录

28 篇文章 2 订阅

订阅专栏

buuctf

27 篇文章 1 订阅

订阅专栏

刷题日记

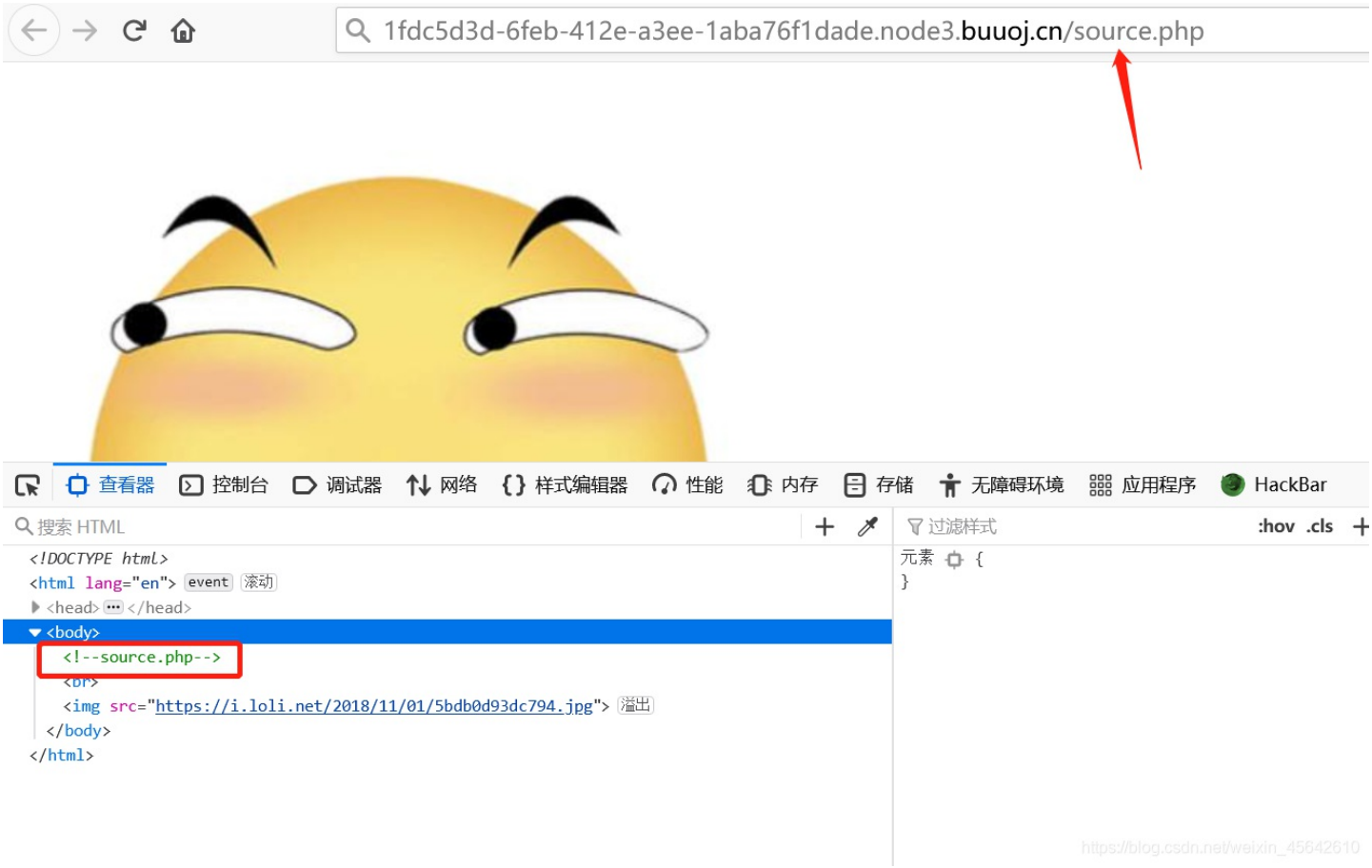
25 篇文章 1 订阅

订阅专栏

## BUUCTF web WarmUp-刷题个人日记

小白一个，写给自己看。


[打开后是这样]






按F12后发现一个文件，输入后：

```php
<?php
    highlight_file(__FILE__);
    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(
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_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\" />";
    }
?>
```

有一个类，先不管看下面，

```
if (! empty($_REQUEST['file'])
    && is_string($_REQUEST['file'])
    && emmm::checkFile($_REQUEST['file'])
) {
```

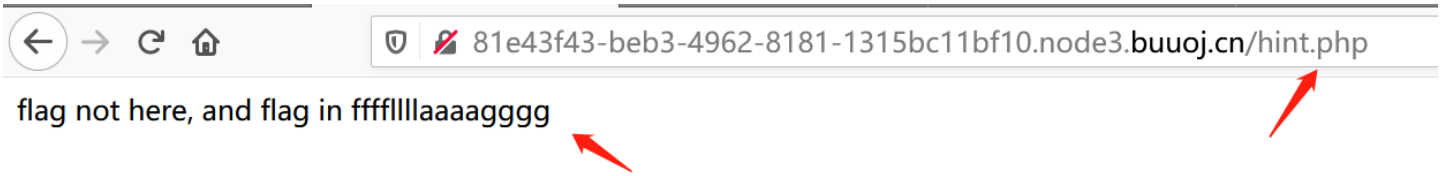
输入的参数file不能为空，要字符串，通过类里的checkFile方法，才能include $_REQUEST['file']，也就是答案flag。
方法里有4个if。第一个和进入方法前的一样，过。第二个看page变量在whitelist（白名单）数组里有没有，in_array就是看第一个参数（字符串）在第二个参数（数组）里有没有。有则true。

```
$_page  =  mb_substr(
        $page,
        0,
        mb_strpos($page . '?', '?')
```

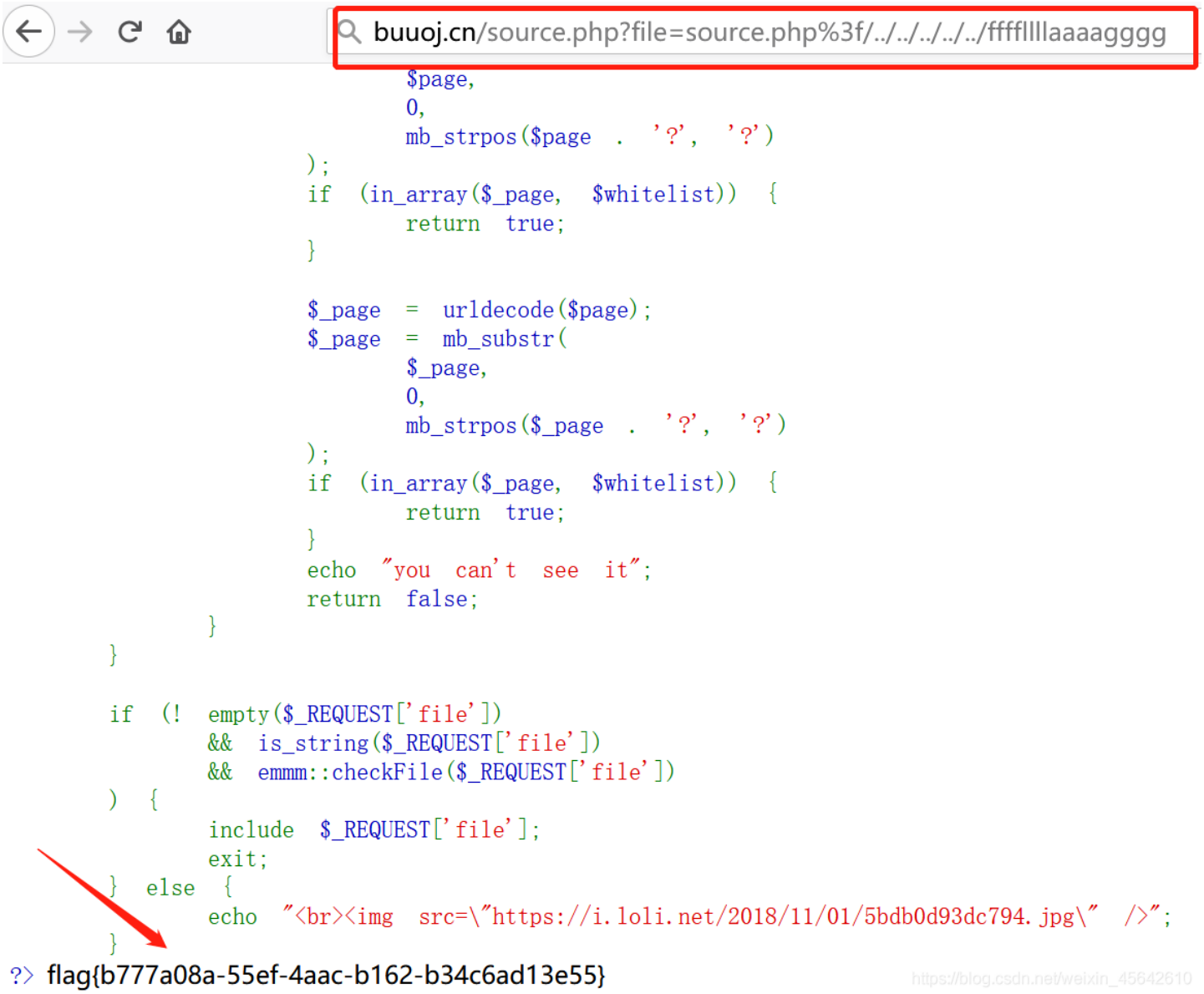
mb_substr（a,0,3）就是在a字符串里的第一位开始数3位，返回这3个字符形成的字符串。mb_strpos(a,b) 就是返回b在a中的第一个位置，没则false。
简单来说就是过滤了问号'？'。为什么要过滤这个呢？因为到时要访问的是source.php后的目录的文件，所以形式为file=source.php?..(文件名),这个问号会过滤掉，所以可以用url编码。？=%3f。用url是因为后面有url解码函数urldecode（）。
后面就重复了。
构造payload:

```
file=source.php%3f/../../../../../fffflllaaaagggg
```

%3f就是？，/.../.../.../.../（两个点），是目录穿越。啥叫目录穿越呢？我也不太明白，我是小白嘛。简单意思就是能直接到达文件，中间目录可以不用知道。
ffffllllaaaagggg哪里来的？是在hint.php里




hint.php在第一个if的上面提到，就是数组whitelist里的。
输入进去，得到flag




`flag{b777a08a-55ef-4aac-b162-b34c6ad13e55}`

参考
BUUCTF web WarmUp

这是篇写给自己的日记，因为只有自己写得出来而且能让读者看懂才能是真的明白了。写之前我以为我是明白的，写完后才算是真正明白了，写这就是个融会贯通的过程。

参考里的问号经过了二次url编码，变成了%253f，这个我不太明白，我只看到一次url解码（urldecode）。参考里说双重编码的话，经过包含时你包含的文件会被当成一个目录（具体看参考）。是说更能保证包含ffffllllaaaagggg文件吗？

再就是这个问号“？”的问题。有些输入法的问号不同，url编码后的也不同，我的搜狗输入法要英文+半角才能编码成%3f（我的url编码网站），不然会变成%ef%bc%9f，这样构造payload flag出不来。我也是醉了。（是因为传参只能用英文+半角的问号才有效吗？）