# [HCTF 2018]WarmUp1

原创

我小皮超勇的 于 2021-09-11 11:20:40 发布 577 收藏
文章标签： php web安全

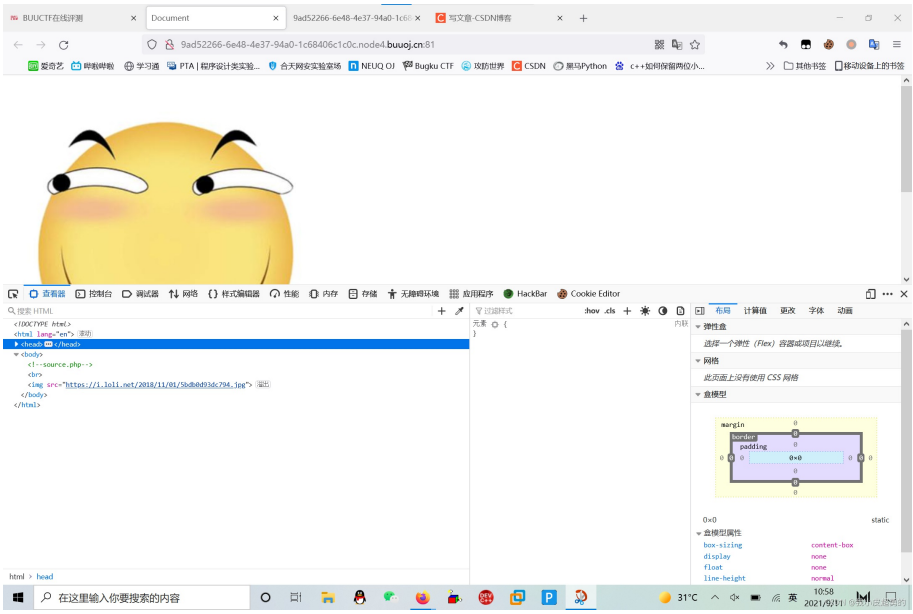
更：如果代码在csdn里看着不方便，建议复制到自己vscode里观看

本来今天想在宿舍躺捏，后来想想还是来gxg把这篇writeup补完吧

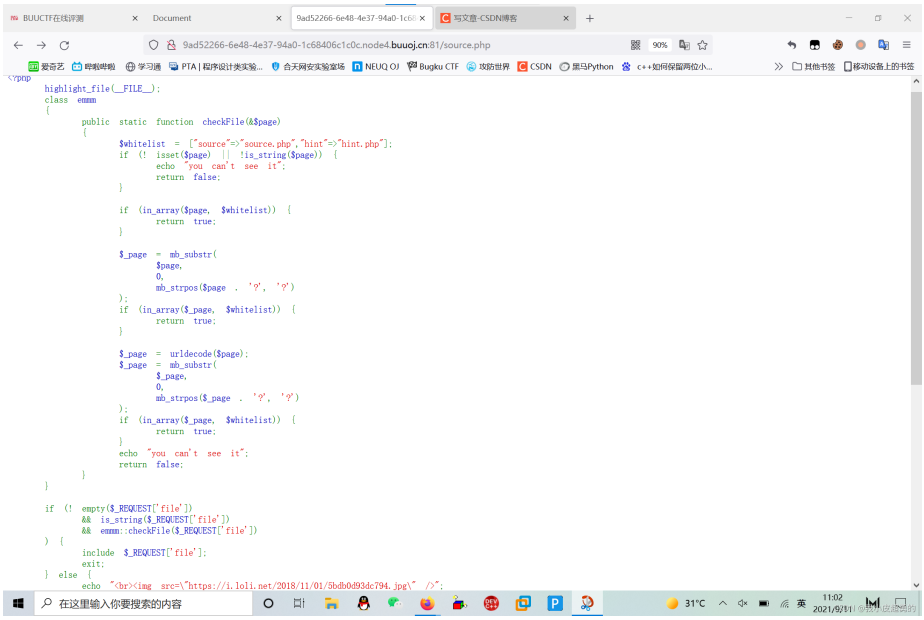
---

这是buuctf上的一道题，我认为难度不小哎，但离谱的是web题里解出人数是最多的，后面的题明明有简单一万倍的.....

首先f12看到提示：source.php

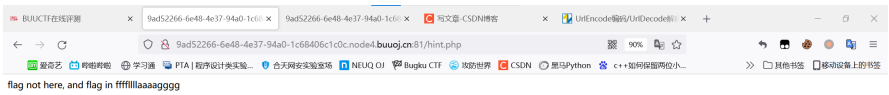


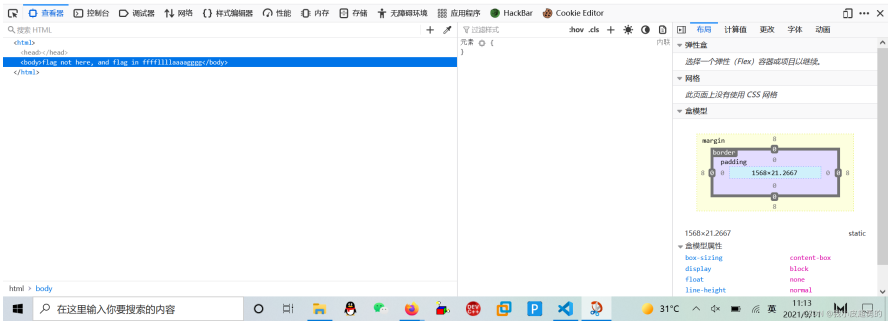
进入，可以看到里面的代码


BUUCTF在线评测
Document
9ad52266-6e48-4e37-94a0-1c68406c1c0c.node4.buuoj.cn:81/source.php
写文章-CSDN博客
爱奇艺
哔哩哔哩
学习通
PTA | 程序设计类实验...
合天网安实验室场
NEUQ OJ
Bugku CTF
攻防世界
CSDN
黑马Python
c++如何保留两位小...
其他书签
移动设备上的书签
<?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\" />";
在这里输入你要搜索的内容
31°C
英
11:02
2021/9/11

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

又发现了hint.php，进入，发现flag在ffffllllaaaagggg里



返回sourc.php看代码吧

这题应该是代码审计，折腾了我快俩小时，总算是把里面各种php函数给搞清楚有啥用。

我是一点点Google然后放vscode里一点点加注释的，下面相当于是我对php代码的翻译

```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];      //=>是对应数组的键(key)和值(value)
            if (! isset($page) || !is_string($page)) {              //issert查看$page是否已经被设置并为空，已经
                echo "you can't see it";                            //$page为字符串则返回true
                return false;
            }

            if (in_array($page, $whitelist)) {                      //搜索$page是否在$whitelist里存在，若存在则
                return true;
            }

            $_page = mb_substr(                                 //截取$page里第0个字符到第x个字符，即截取$page第一个
                $page,
                0,
                mb_strpos($page . '?', '?')                     //返回$page.?里第一个出现?的位置，设为x
            );
            if (in_array($_page, $whitelist)) {             //如果$_page也在$whitelist里，返回true
                return true;
            }

            $_page = urldecode($page);                      //对$_page重新赋值为$page的url解码
            $_page = mb_substr(                             //同上，返回$_page的第一个问号前的字符串，并赋值给$_
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {             //如果$_page还在$whitelist里，返回true
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    if (! empty($_REQUEST['file'])              //不为空
        && is_string($_REQUEST['file'])         //是字符串类型
        && emmm::checkFile($_REQUEST['file'])       //传到emmm类里的checkfile函数里查看true还是false
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

可以看出代码一直在做过滤，要求不同过滤情况下，剩余部分均在白名单(whitelist)里

这道题做了两次了，第一次卡在对代码理解上

第二次卡在urldecode上，后来看writeup里的payload，发现payload进行url解码后还是之前的payload，目前没太搞懂原理，待我马上去看看urldecode的原理。

根据过滤情况，payload首先要等与?file=hint.php?，确保了问号前的hint.php在whitelist里

然后cat ../ffffllllaaaagggg,cat ../../ffffllllaaaagggg一个个试，最后cat ../../../../../时发现了flag