0x01 url任意跳转

未做任何限制，传入任何网址即可进行跳转。

漏洞示例代码：

```
<?php
    $redirect_url = $_GET['url'];
    header("Location: " . $redirect_url);
    exit;
?>
```

Payload：?url=http://www.baidu.com，即可跳转到百度首页

0x02 编码解码

黑盒测试遇到过一个案例，感觉有点意思，写个demo复现一下

漏洞示例代码：

```
<?php
    $url = base64_decode($_GET['url']);
    header("Location: " . $url);
?>
```

将url进行base64编码，参数传递到服务端解码，然后进行url跳转。

http://www.baidu.com base64编码后 aHR0cDovL3d3dy5iYWlkdS5jb20=

Paylod：?url=aHR0cDovL3d3dy5iYWlkdS5jb20=

0x03 常见的一些 绕过姿势

```
利用默认协议

?url=\\www.baidu.com
?url=\/www.baidu.com
?url=\\\\www.baidu.com      等价于：?url=http://www.baidu.com

前缀式
       利用问号?：  ?url=http://www.evil.com?www.aaa.com

       利用井号#：   http://www.aaa.com?returnUrl=http://www.evil.com#www.aaa.com

       其他形式：

           ?url=http://www.baidu.com\aaa.com

           ?url=http://www.baidu.com\\aaa.com
```

```
后缀式

      利用@符号：?url=http://www.aaa.com@www.evil.com

      其他形式：  http://www.aaa.com.evil.com


其他思路：  使用IP地址、IPv6地址、更换ftp、gopher协议
```

0x04 白名单限制绕过

白名单限制

?redirect_uri=http://www.baidu.com

尝试进行跳转到其他网站时发现做了白名单限制，非QQ域名禁止跳转，会报错说跳转链接非法

利用问号绕过限制

?redirect_uri=http://www.baidu.com

?redirect_uri=http://www.qq.com?http://www.baidu.com

?redirect_uri=http://www.baidu.com?&http://www.qq.com

?redirect_uri=http://www.baidu.com/test.html?&http://www.qq.com

?redirect_uri=http://www.baidu.com\test.html?&http://www.qq.com

在代码中判断是否为目标域名，但开发小哥哥们喜欢用字符串包含来判断

http://www.aaa.com?returnUrl=http://www.aaa.com.evil.com

http://www.aaa.com?returnUrl=http://www.evil.com/www.aaa.com

http://www.aaa.com?returnUrl=http://www.xxxaaa.com

若再配合URL的各种特性符号，绕过姿势可是多种多样。

比如，利用反斜线：

http://www.aaa.com?returnUrl=http://www.evil.comwww.aaa.com

http://www.aaa.com?returnUrl=http://www.evil.com\www.aaa.com

多次跳转,即aaa公司信任ccc公司，ccc公司同样存在漏洞或者提供跳转服务:

http://www.aaa.com?returnUrl=http://www.ccc.com?jumpto=http://www.evil.com

实际挖掘过程中还可以将上述方法混合使用，甚至使用URL编码、ip地址替代域名等手段。

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。


Bypass