## url重定向漏洞

## 0x01漏洞原理

 原理一

1. Url重定向是程序员误信了攻击者的输入而将网站重定向到另一个站点，这通常通过url参数、HTML<meta>刷新标签、DOM中的window对象的location属性来实现的

 很多Web 网站都是通过在原始 URL 的参数中设置目标 URL 来有意实现用户访问的重定向的。应用程序通过使用这个参数来告诉浏览器向目标 URL 发送一个GET请求，，例如，假定百度网站具有重定向到 Email 的功能，就可以通过访问如下URL 实现：

[https://www.baidu.com/?redirect\_to=https://www.Email.com](https://www.baidu.com/?redirect_to=https:/www.Email.com)

在这种情况下，当我们访问上面的 URL时，百度网站会接收到一个HTTP 的GET 请求，然后依据 redirect\_to 参数中指定的值来确定将你的浏览器重定向到哪里。在这之后，百度 网站服务器会返回一个用于指示浏览器重定向用户的 HTTP响应状态码。通常，这个状态码是302，但有时也可能是 301、303、307 或 308。这些 HTTP 响应状态码告诉浏览器请求的网页找到了，但是需要浏览器发起一个 GET请求到redirect\_to 参数值，https://www.email.com/这个参数值也在HTTP 响应Location 头中。**Location 头表示了向哪里重定向 CET 请求**。现在，假设攻击者修改了原始的 URL，如下所示：https://www.baidu.com/?redirect\_to=https://www.diaoyuwangzhan.com如果百度没有验证 redirect\_ to参数是否为其将访问者重定向到一个自有合法站点，攻击者就可以将该参数的值换成它们自己的 URL。结果是，HTTP 响应可能会引导浏览器向 https://www.diaoyuwangzhan.com发起 GET 请求。一旦攻击者已经引导用户到他们的恶意网站，就可以发起进一步的攻击

 原理二

二：

HTML<meta>标签和 JavaScript 都可以重定向浏览器。HTML<meta>标签可以告知浏览器刷新网页，并向标签中的content属性定义的URL发起GET请求。

下面是一一个例子:

**<meta http-equiv=' 'refresh" content="0; ur1=https://www. Baidu. com/">**

content属性定义了浏览器发起HTTP请求的两个步骤。首先，content 属性定义了浏览器在向URL发起HTTP请求前需要等待的时间，在本例中，这个时间是0秒。其次,content属性确定了浏览器向其发起GET请求的网站中URL的参数，在 本例中，这个参数是https :/ /wWW. Baidu.com.当我们具有控制<meta>标签的content属性的能力时,或者通过其他漏洞能够注人他们自己的标签时，就可以利用这种重定向行为。

 原理三

三：

 JavaScript修改文档对象模型(DOM)中window对象的location属性来实现重定向用户。DOM是用于HTML和XML文档的API.它允许开发者修改网页的结构、风格和内容。因为location属性表示了请求将被重定向到哪里，浏览器将立刻解释JavaScript脚本并重定向到指定的URL.我们可以通过如下形式的JavaScript脚本修改window的location属性:

**window. location = https://www.baidu. com/**

**window.location.href = htts:/www.baidu.com**

**window. location.replace(htts://ww. baidu.com)**

**使用条件：我们必须要拥有执行js的权限才行（获取js权限的方法大家应该知道把）**

## 0x02 测试方法与出现位置

 方法1：直接观看get请求注意参数

Url= redirect= next= r= u=

 方法2：使用Burp查看包含url跳转的get历史请求。

出现地方：登录框的时候抓数据包 直接参加get参数

## 0x03案例

某里的src案例：

 这是一个购物商城的卖家后台的漏洞，我们在浏览时突然发现一个get参数是跳转到货物供应链的：

 [www.xxx.xxx.com/oauta/authurl/?targeturl=www.gongyinglian.xxx.xxx.cn](http://www.xxx.xxx.com/oauta/authurl/?targeturl=www.gongyinglian)

我们可以看见参数targeturl?=后面跟着跳转的参数,然后我们将参数修改为www.baidu.com 即可跳转到百度 而百度bai.du的域和某购物商城的域完全不同了，及收获一枚url跳转漏洞，提交平台获取奖励100r

****

**案列2是某企鹅src的：**

 **场景是对一个视频分享它会生成一个二维码跳转到我们要分享的视频，可我们可以在生成二维码的时候进行抓包导致ur跳转漏洞：**

分享视频地址生成的二维码



3、修改该地址为<https://www.baidu.com>,修改完成后，刷新该界面



4、使用手机扫码，直接跳转到修改的地址。



此漏洞也是获取100r