URL跳转奇葩姿势详解

JutaZ

目录

CONTENT

1

关于我

一个新手

2

URL的标准形式

scheme://user:password@domain:port/path?query_string#fragments

① 方案名
② 验证信息
③ 主机名
④ 端口号
⑤ 路径
⑥ 查询字符串
⑦ 片段字串

引自《白帽子讲浏览器安全》

3

绕过及FUZZ

实现 test.a.com 跳转到 b.com
限制：仅允许跳转至*.a.com

- a.com:80@b.com
- b.com?a.com
- b.com#a.com
- a.com.b.com
- a.comb.com
- b.coma.com

3

绕过及FUZZ

a. 个性化字典
- URLENCODE
- 字符绕过字典
- 其他可信域名
- 等等

b. 其他尝试
- CRLF漏洞
- 反射xss
- 其他猥琐姿势

4

其他跳转方式

乌云案例一

代码逻辑缺陷

详细说明：

问题URL：http://[redacted]//ce.[redacted].org
http://[redacted] com=>http://[redacted]/home
也就是说直接打开http://[redacted] com，网站会跳转到/home页面，但HOST值是从最后一个//后取的而不是第一个//
所以只要在http://[redacted].com后面加上//然后再加任意站点都可以跳转，当然正常打开的前提是跳转的站点要有/home这个页面

漏洞证明：

```
HTTP/1.1 302 Found
Connection: Keep-Alive
Content-Length: 0
Date: Wed, 23 Sep 2015 12:26:48 GMT
Location: http://ce[redacted].org/home
Server: Apache-Coyote/1.1
Set-Cookie: ses_cache__cas__st__=7dd8da7a-3c64-401a-84f0-5585ad701be5; Domain=ssp.[redacted].com; Path=/
X-Cf-Requestid: 58bb2a7a-3e68-4626-707e-45c5abc81a37
X-Prism-Spanid: 0
X-Prism-Uid: 20150923_36ED68C4-EBFD-4541-93CB-8C1DEA8D02C5
Content-Type: text/plain; charset=utf-8
```

4

其他跳转方式

乌云案例二

第三方插件缺陷

简要描述：

某功能设计不当导致URL跳转（已被攻击者利用，恶意信息活跃于各大社交平台）

详细说明：

某功能设计不当导致URL跳转（已被攻击者利用，恶意信息活跃于各大社交平台）

```
http://paypassport.[redacted].com/ids/oauth20/authorize?client_id=suning_01&response_type=code&redirect_uri=http://nWQxM.[redacted].cn&www.qq.com
```

近日，[redacted]等网络虚拟社交平台因[redacted]官方网站URL跳转导致各种恶意信息活跃流传。
攻击者利用接口http://paypassport.[redacted]com/ids/oauth20/authorize中的redirect_uri跳转漏洞，跳转到仿造[redacted]的网站，同时对账号密码进行验证与记录（成功登录会跳转至本人[redacted]，错误提示重试。）
攻击者伪造网址：http://nWQxM.[redacted].cn
这个漏洞其实要追踪到2014年05月左右爆出的OAuth2 Covert Redirect漏洞。安全研究人员发现授权协议OAuth2.0存在Covert Redirect漏洞，可能导致用户信息遭窃取。经分析，此问题原因在于第三方应用的redirect_uri存在跳转漏洞。目前有些网站采用快捷登录或者以其他方式开放了自己网站的相关API接口，基本鉴权方式都是采用了目前国际主流的Oauth2.0方式。但是很多开发者并没有意识到redirect_uri过滤的重要性。

4

其他跳转方式

乌云案例三

隐藏极深的跳转

详细说明：

http://sp1.[redacted]com.cn/dan.php?c=IZO-5HDYnWOsnWRzPWTOIgF_5y9YIZOlQzqYQhP8QdFnTy9kiYYO 这段代码掩藏了什么呢？

巧遇贴吧

衍生危害一

跳转时传递了cookie等数据 BY:呆子不开口

简要描述：

[redacted]上你点我的链接，我就可xss你，并可拿到httponly的cookie，以及些其他方面的危害

详细说明：

见如下请求，实现了一个代理访问url的功能
http://[redacted].com/p/aj/proxy?api=http%3A%2F%2Fcontentrecommend.mobile.[redacted].cn
这个请求做了些url白名单的校验
但有如下问题：
一、存在绕过漏洞，导致ssrf漏洞，可以访问内网
这个代理功能存在url绕过漏洞，api参数使用下面格式的值可以绕过
http://contentrecommend.mobile.[redacted].cn@123.[redacted].3/wb.php
攻击poc见：http://[redacted].com/p/aj/proxy?api=http%3A%2F%2Fcontentrecommend.mobile[redacted]cn%40123.[redacted].3%2F[redacted].php
服务端程序会去请求http://123.[redacted].3/[redacted].php
这样就可以ssrf访问内网了
二、xss
如果我们代理访问的是我们控制的页面，我们的页面可以输出一个存储xss了
三、httponly cookie
程序在代理访问我们的页面时，会把当前用户的cookie也带给我们。我的服务端php程序，通过$_SERVER['HTTP_COOKIE']就可以取到

5

衍生危害

衍生危害二

客户端伪协议 BY:呆子不开口

我就在想，程序员会不会在这个应用相关操作里面使用了appkey作为参数
我扶了扶镜框，发现了一个，在取消授权功能那里直接传了appkey
然后不出所料，果然也是特权的appkey，可以拿到用户的gsid
这样就很完美了，基本通杀所有的用户了，只要在私信或评论里给他发个攻击链接就可以了
我又想一想，攻击面可不可以再扩大点呢，比如当这个人没有在用[illegible]时，我在别的地方给他发个链接让他中招有没有可能呢，比如在[illegible]里打开这个链接
那我就猜，我在[illegible]里点链接可不可以加载[illegible]客户端去自动打开我们的poc链接呢
找了下，[illegible]是支持url scheme的，类似于s[illegible]o://
简单的反编译了下[illegible]客户端，进入搜了下browser，果然有这样的url
s[illegible]o://browser/
我报着试一试的心态访问了下这个，s[illegible]o://browser/?url=http://www.[illegible].com
跟前面一样顺利，成功了
所以在[illegible]里发一个链接，比如http://sdadsadasdasd.com/302.php。这个请求会302跳转到s[illegible]o://browser/?url=http://www.sh[illegible]curl.com
这种方式在我的版本的[illegible]内嵌浏览器是支持的，如果不支持，可以试试欺骗用户去点击这样的链接，s[illegible]o://browser/?url=http://www.shang[illegible]curl.com
当然不止是[illegible]里面，其他浏览器，或者其他应用的内嵌浏览器，很多也是支持这样的伪协议打开的。攻击面可以更广
到这里就差不多了，发给表妹，她中招了
但她在得知我并不知道她密码后，她还是改了密码