基于 web 环境下 CSRF 的攻击和防御

梁桐彬 唐宾徽

四川大学锦城学院计算机与软件学院 四川 成都 610000

【摘 要】近些年互联网的迅速发展，人们的工作和生活都进入了信息化时代。而 Web 系统凭借着它动态交互以及跨平台的种种友好的特性在各种系统中脱颖而出，广泛应用在我们生活当中，成为生活中不可或缺的一部分。例如电子商务网站，资讯类门户及视频网站等等。与此同时，在当今的互联网环境下，依然存在着许多的风险因素，Web 技术的广泛运用同样也会有类似的担忧。跨站请求伪造 CSRF 是目前 Web 网站中主要且容易被忽视的安全威胁之一，攻击者可以利用 CSRF 产生一些恶意的请求，引导合法的授权用户进行一些恶意操作。整个过程中合法用户完全不知情，并且在 web 中简单的身份验证只能判断出请求是来自于某个浏览器，不能判断该请求是否是符合用户意愿，因此这类恶意操作很难被快速判断。因此，如何有效地阻止 CSRF 威胁是 Web 环境下客户端和服务器交互的一个重要的安全性问题。本文针对 CSRF 攻击，首先介绍了相关原理技术，再提出了具体的防御方式。

【关键词】CSRF; Web; 安全威胁

引言

CSRF（Cross-site request forgery）跨站请求伪造，在 2000 年被国外的安全人员提出，而在国内直到 6 年后才被真正关注。在 2008 年，纽约时报，百度，YouTube，和 Gmail 等国际上多个知名网站分别被爆出 CSRF 漏洞。许多类似的大型网站对此毫无防备，以至于在网络安全业界称 CSRF 为“沉睡的巨人”。[1]

通过 CSRF 攻击个人账户时，攻击者可以肆意访问受害者所持有账户的隐私信息，进行个人信息的修改，删除。若被攻击的账户是企业中高权限账户，还会有破坏公司正常经营和泄露商业机密的风险。攻击数字钱包时，攻击者还可以伪造用户的请求进行转账。在社交网络中，攻击者可以利用受害者的账号传播邮件及消息，达到泄露隐私，传播不良信息及诈骗他人等的目的。这一系列的个人隐私的泄露及财产的损失造成的影响十分恶劣。

CSRF 漏洞的危害性十分严重，那么当务之急是如何有效地避免。在本文中会提到业界几种常见的防御方式。

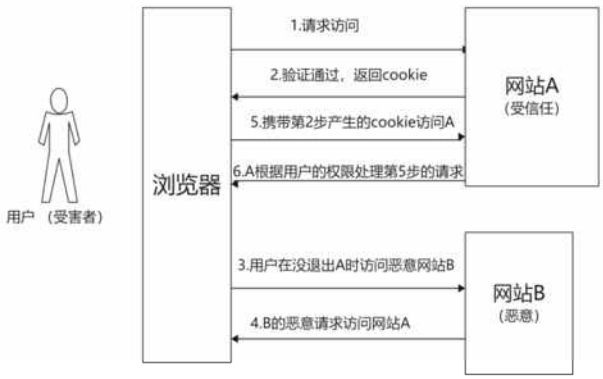
1 CSRF 简介

CSRF 攻击的全称是跨站请求伪造（Cross-site request forgery），CSRF 是通过伪装成来自合法用户的请求来访问到被攻击目标站点。该攻击可以绕过受害者，在其并不知晓的情况下以他的名义伪造请求发送给受攻击站点，从而达到非法访问网站的目的。

2 CSRF 的原理

那么为什么会存在 CSRF 呢？那么就必须提到 Cookie。因为 HTTP 协议是无状态的，服务器端并不知道客户端的身份。而在平时使用中有时又需要记录客户端状态，所以每个客户端请求一次，服务器端就颁发一个证书。而每个客户端的证书都是不相同的，当客户端需要再次访问时，就将这个证书与其他内容一起传到服务器，此时服务器再检查时就可以通过这个证书确认用户的身份了，而这个证书就是 Cookie。Cookie 实际上就是一小段的文本信息，服务器只会认有没有 cookie，而无法区分是不是用户正常访问，这就是 Cookie 的工作原理。

而 CSRF 的整个过程就用到了 Cookie. 如下图所示



图一

如图 1 所示，这是一个 CSRF 攻击的例子，第一步合法用户通过浏览器传递参数请求访问网站。第二步在相关参数通过验证后，用户成功登录，受信任网站再产生 Cookie 信息并返回。第三步攻击者伪造的含恶意请求及类似病毒代码的恶意网站诱使用户直接点开，在正常情况下这个恶意请求网站打开前用户并没有关闭已经打开的合法网站，于是会出现同一浏览器中打开一个 TAB 页访问恶意网站的情况。第四步恶意网站接收到用户操作信息后，会发出一个恶意指示，返回一些恶意性代码，要求访问合法网站。第五步浏览器在接受到这些信息后，根据恶意网站的指示，直接携带 Cookie 信息向合法网站发出请求。这个过程不需要经过用户的处理。而此时合法网站并不知道这个请求其实是由恶意网站发起的，但是凭借着合法用户的 Cookie 信息及相应的权

限，会误以为是来自于受害者用户的合法请求，进而导致来自恶意网站的恶意代码被执行。

因此，合法网站会报据用户的权限来处理非法网站所发出的恶意请求，而这个请求可能以用户的身份完成一系列看似合法，实际非法的操作，实现了非法入侵的目的。[2]

3 CSRF 的产生特点

从 CSRF 的产生原理中我们可以发现容易被 CSRF 的攻击的站点往往有以下几个特点：

①合法受信网站的服务器端在用户登录后返回一个 Cookie，在不关闭受信网站的情况下在 tab 页面下又打开了恶意网站。

②同样有的更改了 Cookie 失效时间的网站易被攻击，如果一个 Cookie 失效时间设置得越长，那么被攻击者发现甚至利用的概率也就越大。

③完全靠 Cookie 识别用户的网站。有的网站完全依靠 cookie 机制区分用户，不进行任何其他方式验证。

④本身站点信息具有一定传播性及影响力，或者含一些易被攻击者所利用的敏感信息。

4 CSRF 的攻击方式分类

结合上述 CSRF 的原理，可以知道 CSRF 的实现基于 HTTP 请求。因此可将 CSRF 攻击分为两种方式：GET 和 POST。[3]

GET 攻击方式和 POST 的最直接的区别就是 GET 请求的 URL 中就包含了参数，而 POST 通过 request body 传递参数。所以在 GET 型攻击时，一般攻击者会在自己的伪造的恶意站点上写入以下一些恶意代码 :<img src= 目标站点 url></img>。一旦用户在登陆合法网站的同时不慎访问了恶意站点上含有上述上述恶意代码的部分，攻击者便可直接 GET 请求到受信任网站，完成一系列操作。

而 POST 型 CSRF 攻击会复杂一些，POST 型通常使用表单的形式进行提交，在用户登陆受信任站点的情况下，访问了恶意站点上的表单，攻击者就可向向受信任网站发送 POST 请求，进而进行一系列修改操作。

5 CSRF 的防御方式

从 CSRF 的原理以及特点分析，可以知道跨站请求伪造攻击是通过受害者浏览器中的认证信息来欺骗受信任站点进而实现请求伪造，并不是直接窃取受害者用浏览器进行正常请求时的其他信息，如密码及其他个人资料等敏感信息。所以在受信任服务器端需要针对涉及高风险数据的增删改等操作重点防护，而查询操作返回的数据，CSRF 是无法篡改的

CSRF 的本质在于服务器端在校验时使用的是保存在 cookie 中，且容易被伪造的数据来校验，所以一旦破坏这个条件，那么攻击者就无法再实现 CSRF。

CSRF 防范主要是在服务器端进行，防范的核心就在于受信任服务器端不只依靠客户端传来的 Cookie 验证，还必须使用其他的校验信息来判断是否是合法用户的请求。主要的实现方法有下列几种：

①验证 HTTP Referer

Referer 是 HTTPheader 的一部分，当客户端向服务器发送请求的时候，带上 Referer 就可以告诉服务器该请求由何处发出。收到请求后，服务器端再通过判断请求 Referer 来决定是否接受该请求。比如一个用户的汇款操作是在 http://www.Bank.com/account 上完成的，那么正常情况下用户首先就必须登陆到该网站，再通过点击汇款或其他触发汇款事件发生，此时请求的 Referer 值就是来自于这个 URL。而使用 CSRF 的攻击者，请求的 Referer 值则是来自攻击者的站点 URL。所以每次汇款请求都可以对 Referer 进行验证，来判断是否为正常操作下的请求。而每次对请求的 Referer 进行验证，该方法虽在一定程度上可以避免 CSRF 攻击且原理简单，却也有一些缺点，很多时候用户对隐私的观念较敏感，基于隐私方面的考虑，可以设置浏览器不发送 Referer，例如当 HTTPS 跳转到 HTTP 时，浏览器就不会发送。甚至有的浏览器还可以自定义发送的 Referer 头。[4] 所以该方法也有一些局限性。

②加密 cookie 信息

因为在 CSRF 中，攻击者其实是无法得到 Cookie 的详细内容，只是一个“借用”的作用。因此可以在发送前对 Cookie 值进行 Hash 加密。服务器端接收到后对 Hash 值进行校验，校验合格的则通过请求。加密后的 Cookie 值几乎不能被破解，攻击者无法构造 Hash 后的 Cookie 值，从而避免了跨站请求攻击。[5]

③校验 token

令牌（token）作为一种身份标识，是服务端随机生成的一串字符串，在用户登陆时服务器端就会生成并返回给客户端，且有时间限制，客户端每次提交请求时都会带上 token。所以可以将 HTTP 请求中将一个随机的 token 加入到参数，如果请求的 token 值与服务器返回给用户的 token 不匹配或者请求中的 token 不存在，则该请求可能是被 CSRF 所攻击，从而拒绝。[6]

结束语

本文阐述了 CSRF 的原理，攻击方式及一些常见的防御手段。威胁虽然比较大，但其产生的根本原理较容易把握，开发和维护人员不应对此掉以轻心，应该更加注意测试相关漏洞，综合评估后选择合适的防御方案。

【参考文献】

[1] 郑新新，马兆丰，黄勤龙．跨站请求伪造 (CSRF) 分析与检测技术研究 [A]. 中国通信学会、辽宁省通信管理局 . 第十届中国通信学会学术年会论文集 [C]. 中国通信学会、辽宁省通信管理局：中国通信学会青年工作委员会，2014:7.

[2] 吕东，周童 .CSRF 攻击与防御方法研究 [J]. 电子世界，2017(12):139-140.

[3] 孙丹 . 浅析 CSRF 攻击方式及防御技术研究 [J]. 科技广场，2016(07):78-83.

[4] 徐淑芳． 服务器端 CSRF 防御研究 [D]. 江西师范大学，2014.

[5] 陈春艳 . 跨站请求伪造攻击的基本原理与防范 [J]. 电脑知识与技术，2014,10(05):902-904.

[6] 王保锦，林卉，王健如，李桂青 . 跨站请求伪造攻击技术浅析 [J]. 网络安全技术与应用，2020(05):28-29.

基金项目：2018 年教育部协同育人项目：网络空间安全课题建设项目（项目编号：201801012040 ）