安全小课堂第九十二期【web漏洞之CSRF漏洞挖掘】

京东安全应急响应中心 4月24日

CSRF全称Cross-site request forgery（跨站请求伪造）是指恶意用户将某些需要他人权限的接口埋藏在自己的脚本中，将脚本利用XSS相同的注入方式或诱导用户点击执行等方式令拥有权限者执行，从而达到自己的目的。

JSRC **安全小课堂第九十二期**，邀请到**0h1in9e**作为讲师就**web漏洞之CSRF**为大家进行分享。感谢白帽子盆友的精彩提问与互动~

CSRF是什么?

京安小妹

0h1in9e:

CSRF(Cross-site request forgery),跨站请求伪造。和XSS比较相似，但又不尽相同，XSS利用站点内的信任用户，而CSRF则通过伪装来自受信任用户的请求来利用受信任的网站。说白了，就是攻击者恶意构造了网站的某些操作，引诱用户去点击，从而在用户不知情的情况下做一些操作（攻击者盗用了你的身份，以你的名义发送恶意请求）。比如严重的有修改用户密码，管理员密码、添加管理员，甚至是转账等重要操作，一般的就很多了，比如修改用户信息、更改购物车、不知不觉改了你的收货地址……

讲师

CSRF漏洞产生的成因及攻击原理是什么?

京安小妹

0h1in9e:

先说说攻击原理吧，首先用户访问了Web A之后在本地储存了Cookie认证信息；其次，用户被攻击者诱导访问了Web B上的恶意链接，这个恶意链接在Web A 上执行了恶意代码。

也就是说要完成CSRF的攻击，有两个条件（即成因）：用户本地含有正常网站的认证信息；用户访问了恶意链接。

讲师

CSRF漏洞挖掘实例举例?

京安小妹

0h1in9e：

网站上很多操作都有可能出现CSRF，这个时候需要人为地分析操作的重要程度；下面列举几种挖洞中遇到的实例：

1.某站后台CSRF添加管理员账号，直接CSRF修改密码的情况已经很难遇到了，但后台添加管理员还是可以遇到几个

2.某购物网站CSRF修改收货地址。

3.某企业招聘网站CSRF修改简历信息。

4.某社区CSRF蠕虫威胁情报分析等。

讲师

CSRF漏洞的分类及发现手法?

京安小妹

0h1in9e:
分类：从数据包的角度可以分为Get型和POST型；
从利用的角度也可以分为：
1. 对后台管理员进行攻击，比如诱骗管理员点击的修改管理密码、添加管理员等；
2. 修改普通用户账户和数据，比如修改个人资料、手机绑定、收货地址等；
3. 账户劫持，比如修改密码等；
4. 结合其他类型漏洞进行利用，比如selfxss+CSRF可成功攻击他人；
5. CSRF蠕虫，比如很多点我链接发微博、点我链接改信息等；
发现方法：
1. 首先就是对目标敏感部位进行抓包分析，比如修改信息、转账、添加信息等等。通常一个数据包HTTP请求头里边都会有一个Referer，这个需要特别去验证。比如放到Burpsuit Repeater里边去测试：去掉Referer，看结果是否有变化。如果没有变化意味着这里的Referer服务器端并未验证，那就继续看下一步。
2. 紧接着就是查看数据包是否存在类似CSRF token的字段、常见的有参数有CSRF、token、sid……（一般这些字段的值都是随机字符串），如果没有的话就排除CSRF Token的验证了。转到下一步。
3. 很多时候走完了上边两个流程其实就已经可以断定这里是存在CSRF的，不过还有一个隐蔽的地方。在某些操作对数据包的提交采用Ajax的情况，存在一种情况，就是数据包HTTP请求头会自定义一个字段，这个时候就像存在Referer的情况一样，没办法CSRF了。

讲师

CSRF漏洞有哪些高级应用场景?

京安小妹

0h1in9e:
除了2中所说的几种案例，现在更多的是需要绕过的，比如在测试某站点存在的两处敏感操作的时候，发现其存在Referer验证，需要通过绕过"判断Referer是否有某域名"才可以触发。
这里就介绍几种CSRF中Referer验证的绕过方法：
Referer为空的情况：利用ftp://,http://,https://,file://,javascript:,data:这个时候浏览器地址栏是file://开头的，如果这个HTML页面向任何http站点提交请求的话，这些请求的Referer都是空的。
判断Referer是某域情况下绕过：比如你找的CSRF是xxx.com 验证的Referer是验证的*.xx.com 可以找个二级域名 之后<img "CSRF地址"> 之后在把文章地址发出去 就可以伪造。
判断Referer是否存在某关键词：Referer判断存在不存在google.com这个关键词，在网站新建一个google.com目录 把CSRF存放在google.com目录,即可绕过
判断Referer是否有某域名：判断了Referer开头是否以126.com以及126子域名 不验证根域名为126.com 那么我这里可以构造子域名x.126.com.xxx.com作为蠕虫传播的载体服务器，即可绕过。
CSRF结合其他漏洞利用： 一个严格验证Referer的敏感操作+同域下的一个URL跳转+一台vps=一个完整的CSRF蠕虫。 在后台存在Getshell的情况下，利用CSRF可Getshell。比如Catfish—缓存漏洞&&配合CSRF到Getshell
多步CSRF利用：利用form标签的target=_black或结合frame标签进行多步CSRF利用。

：
讲师

CSRF漏洞防御手段?

京安小妹

0h1in9e:

1、在敏感操作步骤中检测HTTP头部Referer信息。Server端收到请求后，先检测Referer是否为本域的请求；

2、也可以在请求表单中加入anti CSRF token字段；

3、某些操作也可以采用验证码的形式。

讲师

白帽子提问：

伪装来自受信任用户的请求来利用受信任的网站请问这能解释下吗？

0h1in9e:

就是攻击者构造了poc,正常的用户点击之后触发，也就相当于是受信任的用户发出的请求，利用用户的凭证让用户神不知鬼不觉的操作。

白帽子提问：

这个和xss区别在哪，xss也是获取用户凭证？

0h1in9e:

Xss可以获取用户凭证，而CSRF只是利用用户凭证在用户不知情的情况下执行某些重要操作。通俗的说xss可以执行任意js，CSRF只是请求伪造而已。

白帽子提问：

请教下，如果csrf需要发送post包，要怎么操作呢？

0h1in9e:

一般用form表单就可以呢，有的时候为了防止跳转可以令其跳转到同页面frame,测试漏洞的时候也可以直接用burp生成。

白帽子提问：

好多网站验证的content-type咋办？

0h1in9e:

用js fetch（）。

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心