CSRF的攻击与防御——安全小课堂第十期

2016-05-13 京东安全应急响应中心

安全小课堂第十期

“攻击者盗用了你的身份，以你的名义发送恶意请求”——你可以这么理解CSRF攻击。CSRF是一种依赖web浏览器的、被混淆过的代理人攻击，往往涉及到个人隐私泄露以及财产安全。

本期我们邀请到唯品会高级安全研究员haoren、知名白帽子呆子不开口，来和我们科普下CSRF那些事儿~

1

豌豆妹

CSRF的原理能给大家科普下么？

哆啦A梦

由于浏览器的特性，会自动携带同一域名下的cookie到服务器，服务器端的某些功能验

证了cookie有效性后，就执行了该功能。

豌豆妹

CSRF分为哪几种场景呢？

小丸子 

修改个人数据（横向越权），添加用户（纵向越权）等。

2

豌豆妹

CSRF容易出现在哪些业务上呢？

小新 

CSRF一般用于操作用户的资源，或者使用用户的权限进行操作，或者窃取用户的相关信息。

小丸子 

其实可以这么理解CSRF攻击：攻击者盗用了你的身份，以你的名义发送恶意请求。

豌豆妹

CSRF被认为比XSS更具危险性，大家如何看？

葫芦娃 

个人认为，CSRF不比XSS更有危险性。CSRF能完成的事，XSS更能够完成；XSS能完成的事，CSRF不一定能做到。

3

豌豆妹

能说说CSRF的最佳利用方式么？

哆啦A梦 

CSRF给电商用户新增默认收货地址、发微博、添加管理员等等，所有的敏感操作都可以是我们的攻击目标，也就是说，所有的敏感操作都需要进行CSRF的防护。

小新 

我以前发现的用户账号授权相关的操作、二维码登陆、绑定第三方账号等，这些功能有CSRF的话，就直接被盗号了。

4

豌豆妹

请教下CSRF的防护方案。

葫芦娃

CSRF的防护，主要是referer限制、token、或验证码。甚至非常敏感的操作应该要使用短信验证这种。另外，防护手段可以加上一条：多使用post方式获取参数，进行敏感功能。

小丸子

如果你的请求仅仅是ajax请求，那么还有些别的防护手段。比如校验X-Requested-With头。跨域的form表单提交是伪造不了这个ajax请求头。甚至你可以在ajax中使用冷门的put请求，这个也是form表单的请求没能力做到的。referer的防护要严格校验host，而不是简单的使用一个字符包含的检查。

哆啦A梦

安全需要打组合拳，各个部分都需要兼顾到。比如严格的日志系统，这个在企业防护CSRF中，算是事后防护了，能甄别一定的CSRF攻击。

5

豌豆妹

考虑前期开发规避、中期安全检测、后期安全有效监控，企业级CSRF的最佳实践有哪些呢？

葫芦娃

开发的话，所有的敏感请求都不要用get。对敏感功能进行来源和token的验证，最好都验证，一般只验证一个，有很多被突破的可能。如果post是ajax功能的post，那就检验ajax的header头就行了，拒绝所有form表单的post。监控的话，可部署监控日志。

豌豆妹

尽管CSRF是web应用的基本问题，而不是用户的问题，但是用户如何才能避免踩入陷阱呢？

小新

用户可通过在浏览其它站点前登出站点或者在浏览器会话结束后清理浏览器的cookie。

豌豆妹

谢谢耐心解读~下期再见哟~另外，5月20日，2016年JSRC安全乌托邦——杭州站启动，携手途牛同行，干货多多~感兴趣的小伙伴可通过活动行报名。5.20，杭州见。□□□

安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当；
7、XSS之攻击与防御；
8、电商和O2O行业诈骗那些事儿（上）；
9、电商和O2O行业诈骗那些事儿（下）。

JSRC http://security.jd.com/

长按识别左侧二维码，关注我们