CSRF的本质及防御

wilsonlee1 / 2017-10-20 07:25:04 / 浏览数 3305 安全技术 技术讨论 顶(0) 踩(0)

本质：产生的原因本质上是参数可知或可预测
防御：
1、加密参数：加密加盐，不可知，不可预测
  忧虑，引入其他麻烦：一、数据分析困难
                二、正常功能会受影响，比如url收藏
2、验证码：用户在确认操作
  破解：只防止了用户不知情点击的情况，用户知情时也可以诱导点击
3、referer check：验证上一url，源检测
  破解：一、诱导合理顺序产生合理源referer
      二、有些应用可以自定义referer
  忧虑：referer check不一定可用，有些应用禁止了（处于隐私考虑或其他）
  辅助手段
4、token：增加一个随机参数 （问题：只是参数值随机、不可预测，还是参数名也有必要随机？ 名也随机不好传参？），只有服务端与客户端知道的秘密（如可在cook
  缺陷：只防护单纯的csrf，当存在xss时，token也被获取

具体应用场景、业务可使用、适用的不同，有些简单设置，有些严格设置；设想如果可以token加密怎样？ 这几种都应用怎样？
但具体业务场景中不太现实，毕竟还需要为业务做数据分析、考虑用户体验等等；
so，具体应用、场景，具体分析、设计；
有不对的地方欢迎大家指正，谢谢

点击收藏 | 0 关注 | 0

上一篇：甲方安全建设步骤 下一篇：蜜罐与内网安全从0到1（一）

1. 2 条回复


wilsonlee1 2017-10-20 07:25:32

CSRF：无法获取受害者的cookie，无法看到cookie；
      只是利用受害者是被服务器信任的（靠验证cookie），而给服务器发送请求；
xss：利用cookie只是xss的一种体现，xss还可以篡改网页、URL跳转等等；跨站脚本，脚本可以做什么，xss就可以做什么；
    单在利用cookie上来说：获取受害者的cookie，从而得到服务器的信任，进行后续攻击
    获取手段是反射、存储、dom
有不对的地方欢迎大家指正，谢谢

0 回复Ta


1530384314075416 2017-11-06 17:01:22

这个我很好奇，求分享，“有些应用可以自定义referer”？？
“利用受害者是被服务器信任的”，CSRF不是服务器信任，是浏览器信任

0 回复Ta

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板