

java代码审计 深度解析

第一课 CSRF漏洞成因

PART 01

CSRF漏洞原理

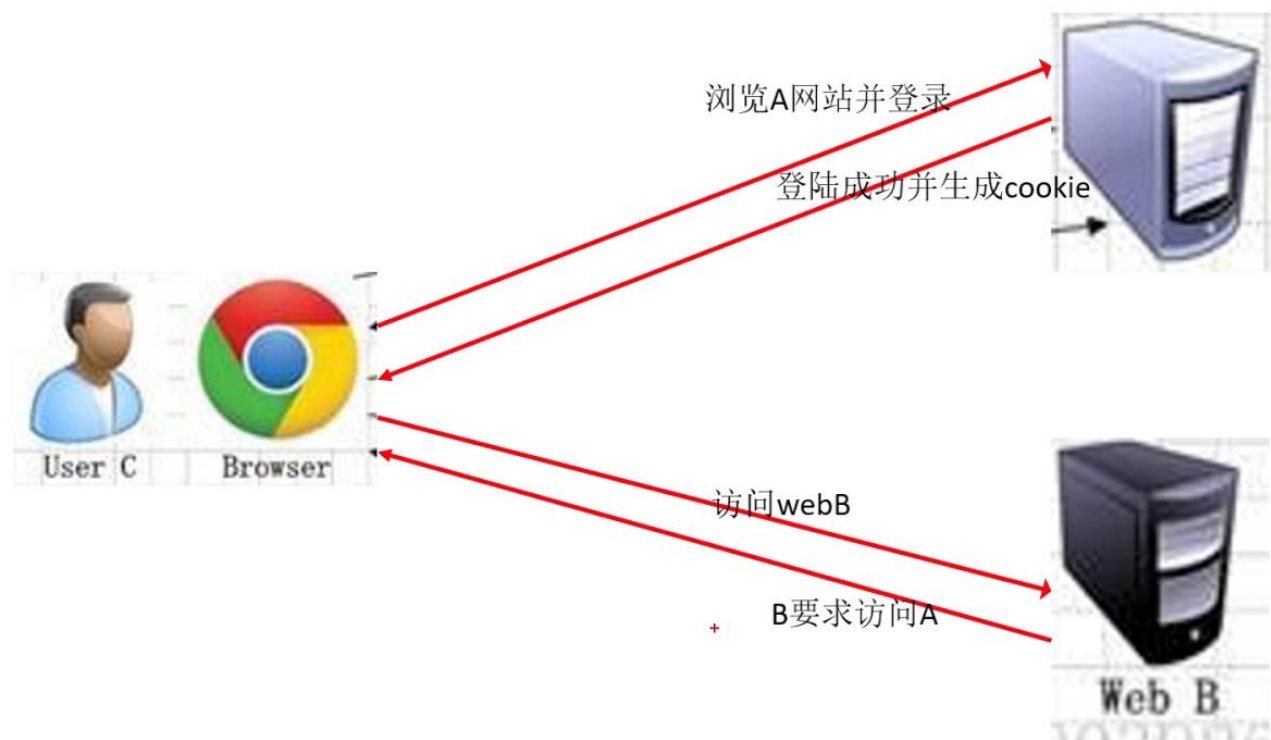


CSRF漏洞简介

CSRF (Cross-Site Request Forgery , 跨站点伪造请求) 是一种网络攻击方式 , 该攻击可以在**受害者毫不知情**的情况下以**受害者名义**伪造请求发送给受攻击站点 , 从而在**未授权**的情况下执行在权限保护之下的操作 , 具有很大的危害性。具体来讲 , 可以这样理解CSRF攻击 : 攻击者盗用了你的身份 , 以你的名义发送恶意请求 , 对**服务器**来说这个请求是完全合法的 , 但是却完成了攻击者所期望的一个操作 , 比如以你的名义发送邮件、发消息 , 盗取你的账号 , 添加系统管理员 , 甚至于购买商品、虚拟货币转账等。



CSRF漏洞简介



CSRF漏洞代码

showReportEquipment.jsp

```
"detail">
openWin('showReportRepairRevamp.action?reportRepairNO=${reportRepair.maintainnumber}','修改',700,500,0);">修改</a>

"detail">
openWin('showReportRepairDeleve.action?reportRepairNO=${reportRepair.maintainnumber}','删除',0,0,0);">删除</a>

"detail">
" onClick="openWin('showReportRepairNew.action?reportRepairNO=${reportRepair.maintainnumber}','新建维修档案',1200,
```

```
435 <!-- 删除 -->
436 <action name="showReportRepairDeleve" class="ckupFixAction" method="showReportRepairDeleve">
437 <result name="success">/jsp/common/add_success.jsp</result>
438 </action>
```



CSRF漏洞代码

```
1255 //设备报修中的详情（维修管理->设备报修->删除->提交）
1256 public String showReportRepairDeleve()
1257 {
1258     faultDetail=ckupFixService.findDetailByid(reportRepairNO);
1259     ckupFixService.deleteFaultDetail(faultDetail);
1260     return SUCCESS;
1261 }
```

```
455 public Tfequipmentfaultdetails findDetailByid(String reportRepairNO) {
456     Tfequipmentfaultdetails details=ckupFixDao.findDetailByid(reportRepairNO);
457     return details;
458 }
```



CSRF漏洞代码

```
1218 public Tfequipmentfaultdetails findDetailById(String reportRepairNO) {  
1219     Session session=this.getSession();  
1220     String hql="select f from Tfequipmentfaultdetails f where f.maintainnumber=?";  
1221     Query query=session.createQuery(hql);  
1222     query.setString(0, reportRepairNO);  
1223     query.setCacheable(true);  
1224     if(query.list().size()>0)  
1225     {  
1226         Tfequipmentfaultdetails ckupFix=(Tfequipmentfaultdetails)query.list().get(0);  
1227         releaseSession(session);  
1228         return ckupFix;  
1229     }  
1230     releaseSession(session);  
1231     return null;  
1232 }
```



CSRF漏洞代码

```
1255 //设备报修中的详情（维修管理->设备报修->删除->提交）
1256 public String showReportRepairDeleve()
1257 {
1258     faultDetail=ckupFixService.findDetailByid(reportRepairNO);
1259     ckupFixService.deleteFaultDetail(faultDetail);
1260     return SUCCESS;
1261 }

470 public void deleteFaultDetail(Tfequipmentfaultdetails faultDetail) {
471     ckupFixDao.deleteFaultDetail(faultDetail);
472 }
473 }

1237 public void deleteFaultDetail(Tfequipmentfaultdetails faultDetail) {
1238     this.getHibernateTemplate().delete(faultDetail);
1239 }
1240 }
```





谢谢观赏