越权漏洞泄露你的隐私—安全小课堂第三十七期

京东安全应急响应中心 2016-12-09

安全小课堂第三十七期

越权漏洞正在泄露你的隐私。作为一种很常见的逻辑安全漏洞，越权漏洞的危害和影响与对应业务的重要性成正相关。如果存在平行越权的话，就可以查看所有用户的敏感信息，而这些敏感信息在黑产眼中简直就是珍宝。

本期邀请到河图安全专家Vern参与讨论。

/ 1 /

豌豆妹

能说说对越权漏洞的理解么？

哆啦A梦 

越权漏洞是一种很常见的逻辑安全漏洞。可以这样理解：服务器端对客户提出的数据操作请求过分信任，忽略了对该用户操作权限的判定，导致攻击账号拥有了其他账户的增删改查功能。

/ 2 /

豌豆妹

越权漏洞的分类呢？

柴可夫斯基 

个人一般习惯根据数据库操作对象来分，基本上有以下几类： 越权查询、越权删除、越权修改、越权添加等。当然也可以根据其他特征进行分类总结，没有一定之规。

葫芦娃

宝宝补充下，可分为以下几类：
平行越权：权限类型不变，权限ID改变；
垂直越权：权限ID不变，权限类型改变；
交叉越权：即改变ID，也改变权限。

/ 3 /

豌豆妹

越权漏洞的危害能分享下么？

小新

它的危害和影响与对应业务的重要性成正相关的，越权漏洞有时候严重起来我自己都害怕。比如说某一页面是返回用户个人的身份证、手机号等userinfo。如果存在平行越权的话，就可以查看所有用户的敏感信息，而这些敏感信息在黑产眼中简直就是珍宝。在测试过程中不只一次遇到过这种情况：开发为了图省事，把用户基础信息通过一个接口查询，信息里面甚至包含用户密码信息，然而这个接口是可以越权的，通过对用户id参数的遍历，即可获取所有用户的各种信息，这就是一种变相的脱裤，而且很难被防火墙发现，因为这和正常的访问请求没有什么区别，也不会包含特殊字符，具有十足的隐秘性。

/ 4 /

豌豆妹

那如何发现越权漏洞呢？

哆啦A梦

替换鉴权参数，定位出鉴权参数，然后替换为其他账户鉴权参数的方法来发现越权漏洞。

豌豆妹

有具体的越权案例分享么？

哆啦A梦

接下来分享一个相关案例：越权查看修改任意志愿者资料，包括密码、姓名、地址、身份号等。

（1）http://i.test.com/ysf/index.do

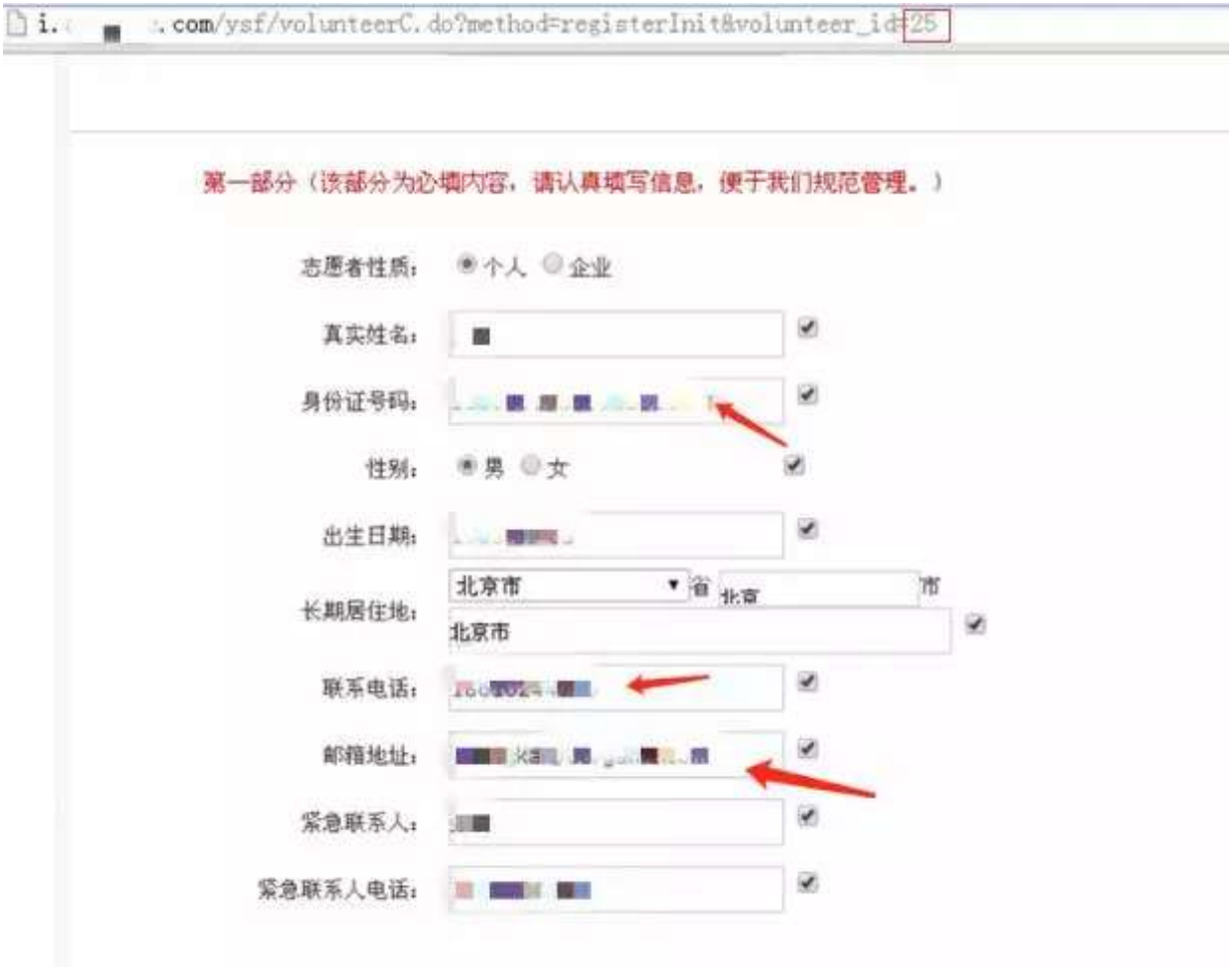
首先找到一个弱口令账号：

zzzkkktiancai 123456qq

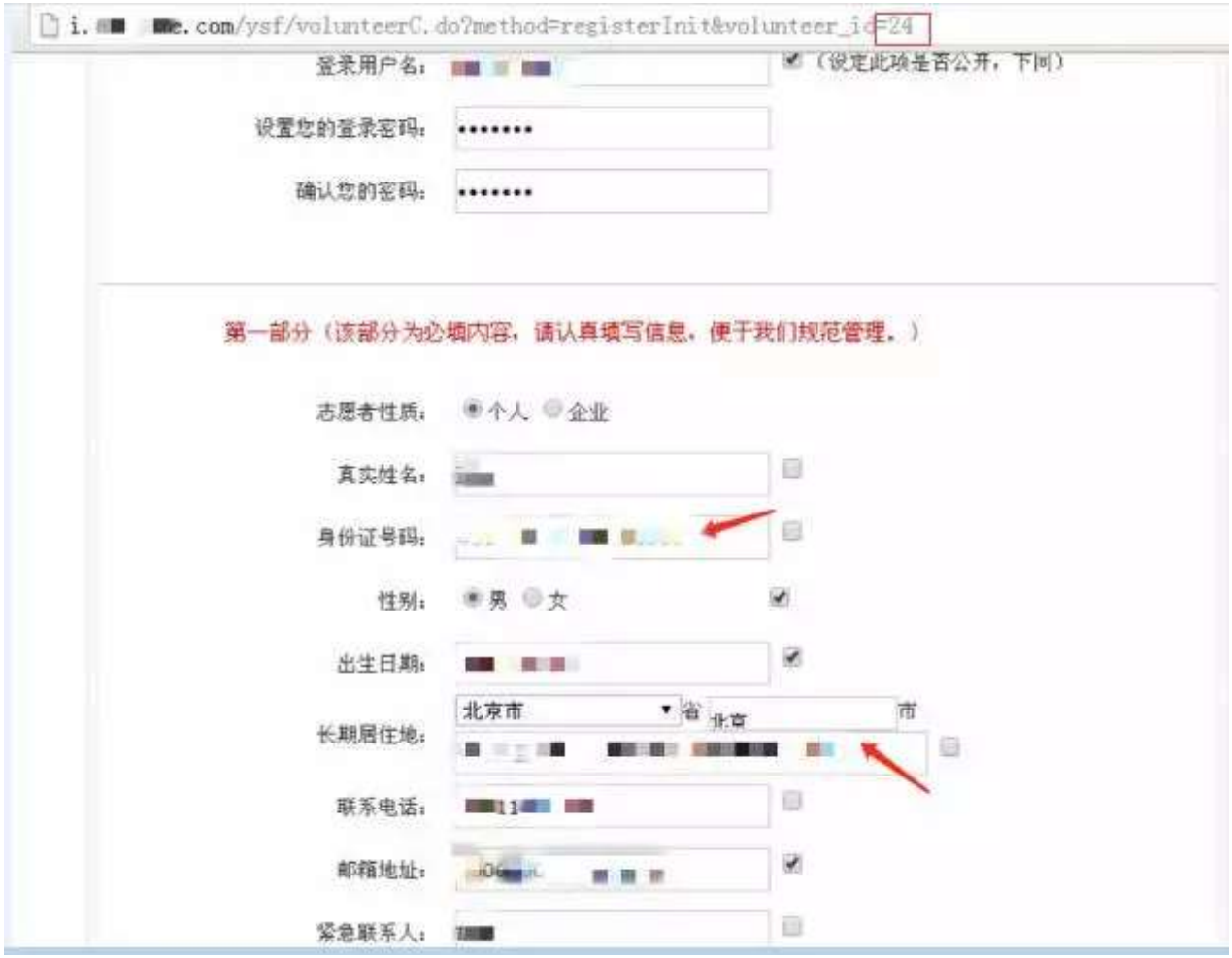
（2）登陆后发现修改个人信息的链接

http://i. test.com/ysf/volunteerC.do?method=registerInit&volunteer_id=25

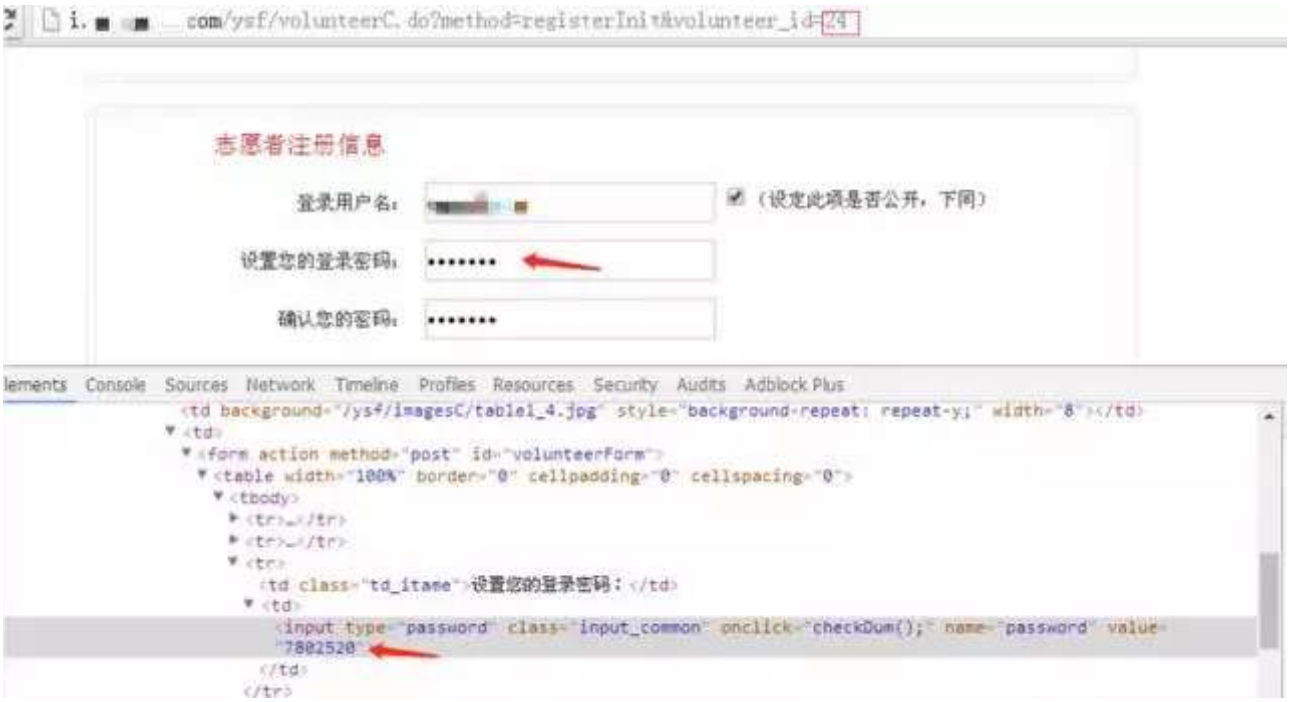
包含了很多敏感信息（因涉及到个人隐私，此处打码）：



（3）然后该处存在越权，id可以任意修改，再用几个其他用户的资料进行证明。
http://i.test.com/ysf/volunteerC.do?method=registerInit&volunteer_id=24



可以直接**F12**查看到密码：



豌豆妹

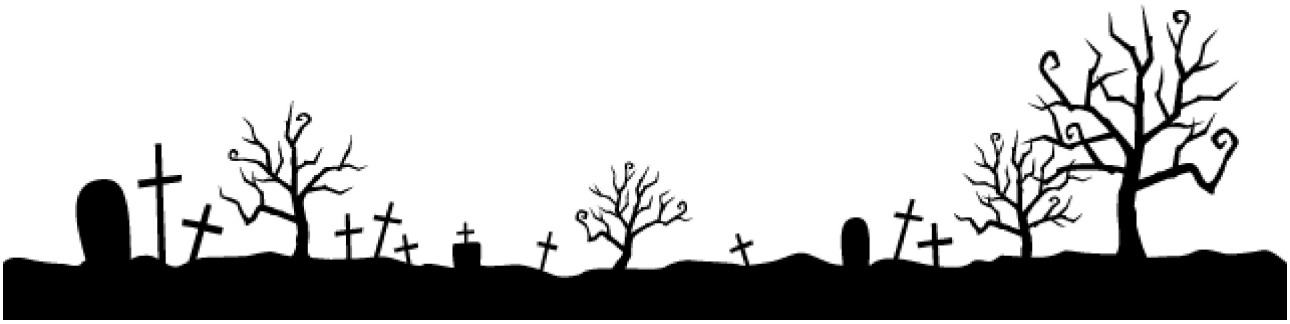
那说说越权漏洞的修复办法吧。

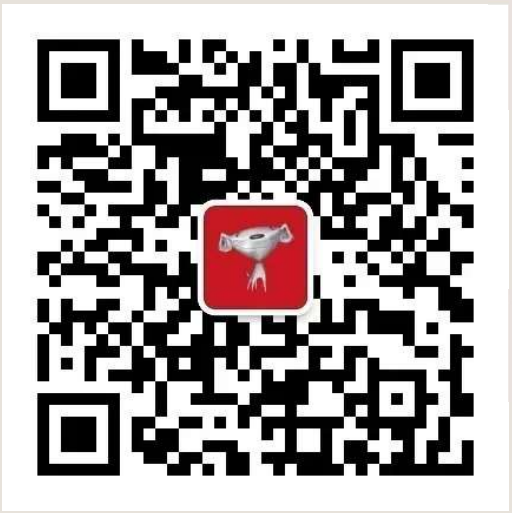
葫芦娃

1、基础安全架构，完善用户权限体系。要知道哪些数据对于哪些用户，哪些数据不应该由哪些用户操作；
2、鉴权，服务端对请求的数据和当前用户身份做校验；
3、不要直接使用对象的实名或关键字。例如订单ID使用随机数。参考OWASP TOP10的A4。

豌豆妹

谢谢分享哟~咱们下期见。





微信公众号：jsrc_team
新浪官方微博：
京东安全应急响应中心

固定栏目

技术分享 | 安全意识 | 安全小课堂