另一角度看越权漏洞—安全小课堂第三十八期

京东安全应急响应中心 2016-12-16

安全小课堂第三十八期

相比与其他漏洞，越权漏洞最易被进行手工检测，简单粗暴直接有效。接着上期的越权漏洞话题，咱们今天着重说检测和修复方面~

本期邀请到硬土壳信息安全高级工程师虾米与JSRC资深白帽子rasca1。

文丨11点姑娘　图丨源自网络

> > > 1 < < <

豌豆妹

越权漏洞检测方面，咱先聊聊黑盒层面如何进行检测呗~

小新

相比与其他漏洞，越权漏洞是最容易被手工检测的，简单粗暴直接有效。
越权分为两种，一种垂直权限、水平权限，检测方式基本一样。
在挖掘越权漏洞时首先是要找到效验的用户身份的id，这个用户id有可能出现在数据包的参数里，也可能出现在cookie里，比如腾讯业务大部分都是cookie里uin参数，当然有些站点业务会生成无规则的身份验证id或者没有id只有cookie_session，这就增加了很大难度。
一个网站大概会有两种角色：用户、管理员。比如id:110和id:120，两个都是用户角色，而id:001 是管理员。当前登录的用户是id 110(用户角色)，可以在修改年龄功能提交时，抓包修改数据包id值为120，然后就会改掉id为120用户的年龄，但是修改id为001(管理员角色)后，并不能修改掉001用户的年龄，即为水平权限，如果也可以改掉001用户的年龄即是垂直权限。
垂直权限越权，是这两种角色可以用修改数据包里身份验证id的方式，达到对两种角色用户增、删、改、查的目的。
水平权限，只能越权当前用户角色。

豌豆妹

白盒检测方面呢?

哆啦A梦 

1、检查所有的功能函数是否做了权限判断;
2、判断权限的功能函数是否遵循安全编码的规范,是否依赖不可以信的数据;
3、对传入参数是否做了加密处理。

豌豆妹

开发应该怎么写呢?

葫芦娃 

1、不要依赖不可信的数据,如数据库、cookie、用户传入的数据;
2、对敏感数据进行加密,例如:
http://host/userdetail.aspx?userId=1,容易认为的进行猜测userId=2等等,
如果没有判断权限,就容易出现信息泄露的问题,但若url是
http://host/userdetail.aspx?userId=ABAWEFRA,则很难进行猜测;
3、对所有的功能函数进行权限判断。

豌豆妹

有什么规范吗?

小新 

1、遵循sdl开发流程；
2、坚持进行安全开发编码规范培训；
3、上线前做安全测试。

> > > 2 < < <

豌豆妹

挖掘越权漏洞需要注意的事项有哪些呢？

柴可夫斯基 

因为越权漏洞的危害较大，所以在挖掘增加、删除、修改功能的越权漏洞时尽量不要去遍历用户id，不要随意修改、删除其他用户资料。

> > > 3 < < <

豌豆妹

能从修复的角度用一两个实例，详细的说说修复方案吗？

哆啦A梦 

对象：某oa系统

问题描述：

由于OA系统档案查询模块没有对查询者的权限进行完整验证，导致攻击者可以利用该漏洞，在查询模块通过修改工号的方式遍历公司所有员工的个人信息。（注：editStaffInfoByCode参数值即工号）

解决方案：

1、修改网站代码，添加权限验证功能，可以划分用户组，根据用户组进行权限划分，并严格限制用户的访问;

2、复用管理范围和数据权限功能(mybatis拦截器对查询进行拦截并处理)，使数据查询控制在管理范围的范畴内;

3、前端不向后端传递参数，用于查询的工号在后端从redis服务器上直接拉取当前用户的工号;

4、前端传递的参数不使用工号，而使用档案的uuid代理主键，防止攻击者使用伪造数据遍历。

豌豆妹

好嘞~谢谢小伙伴们的分享呢！本期告一段落啦~咱们下期见哟！