企业级未授权访问漏洞防御实践

京东安全应急响应中心 2016-04-01

未授权访问可以理解为需要安全配置或权限认证的授权页面可以直接访问，导致重要权限可被操作、企业级重要信息泄露。据不完全统计，有2000余家企业出现过未授权访问漏洞，出现越权访问漏洞的比例约在8%，因此我们本期和各位聊一聊未授权访问的防御与落地。

本期安全小课堂非常荣幸的邀请到了来自新浪安全高级安全研究员小川、银联安全高级安全研究员苏黎士，列队撒花😼欢迎👋~

1

豌豆妹

未授权访问漏洞大多由哪几类组成呢？

葫芦娃 

越权一般分为两种：垂直越权和水平越权。垂直越权的基本思路是低权限用户越权高权限用户的功能，比如会员用户能够操作管理员的功能，这就不合理了。这种漏洞产生原因是，开发只验证了登陆状态，而没有验证用户权限。

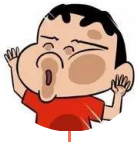
哆啦A梦 

垂直越权的测试有以下两个方法：1、盲测。盲测必须要有自己的测试规则。这一般就要使用大家平时积累的后台地址规则尝试能否越权访问了，需要不断积累，这里常出现的就是后台地址越权访问。2、开两个浏览器。各自登入高低权限账户开两个浏览器：高低权限测试，即复制低权限用户的cookie，覆盖到高权限用户的关键功请求能上，模拟发送，能改变高权限用户数据就存在越权。

2

豌豆妹

未授权访问漏洞容易在哪块业务或系统出现呢？

小新 

常出现的位置在后台功能的所有功能展示中。后台对数据的插入、浏览，删除，编辑，均可存在越权。

3

豌豆妹

导致未授权访问漏洞出现的原因有哪些呢？

小丸子

导致原因主要是后台越权。开发认为前台用户展示页没有后台的功能选项，就不会发出后台功能请求。但是一旦后台的请求规则泄露，即可模拟请求，水平越权就好测了，因为水平越权的功能是对外开放的。

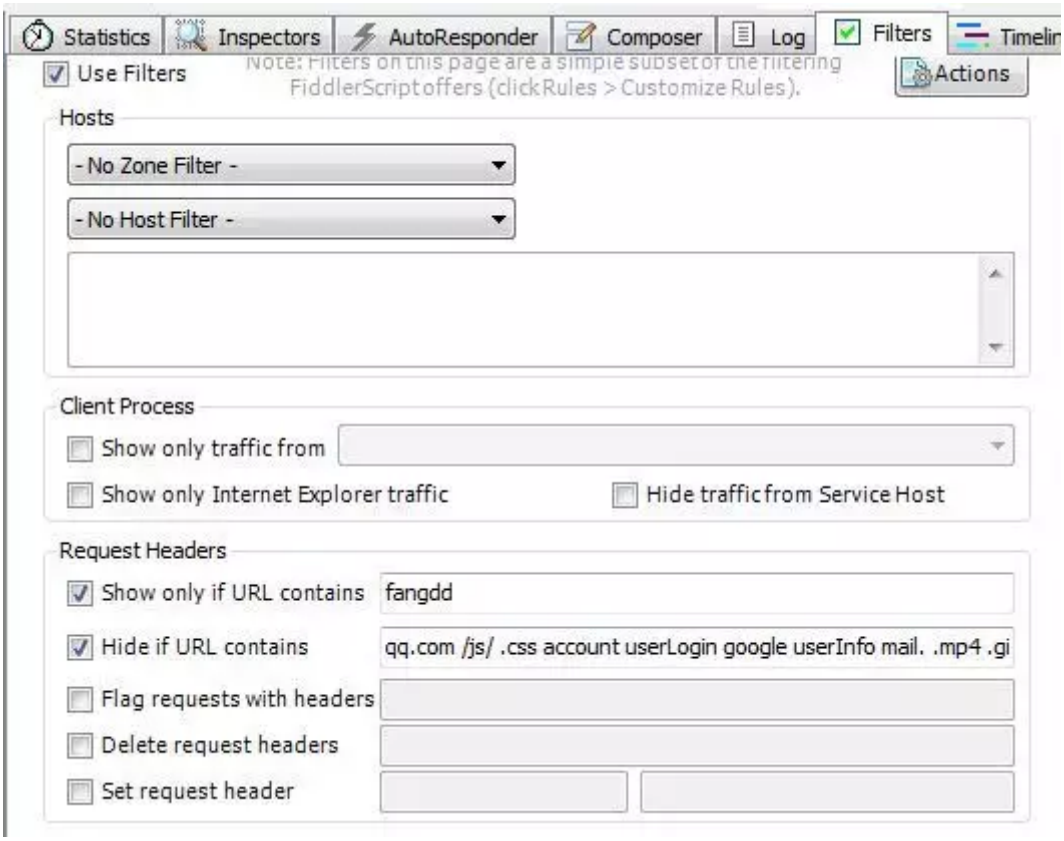
4

豌豆妹

未授权访问漏洞的测试方法有推荐的么？

哆啦A梦

测试方法我建议使用fiddler。fiddler里有一个。



filter功能里show url hidder url规则可以让你更方便的找出关键请求。开两个浏览器，复制其中一个账户的cookie，到另外一个账户的关键求上测试。

5

豌豆妹

研发层面、监控层面的防护策略，是否有好的思路？

小新

任何人都知道请求规则，cookie替换法效率就会很高，同样对数据的增删改，查询都可能造成越权。防御方面，常见的有两种。一是关键参数，二是逻辑思维严谨，加强了越权的判断，关键参数的加密。比如订单id，不采用数字，而采用加密值，那么就无法遍历。

葫芦娃

同程的订单跟用户id就是这样的经过hash的，可以验证出存在越权，但是无法遍历，风险就小的多了。加密的id一旦泄露就麻烦了。但是有一点，现在大部分公司有安装流量监控，请求都能够捕获到，被捕获后，信息也就泄露了。如果使用明文多因素方式，利用难度虽大，万一有一个参数可以判定出确认存在，遍历另外一个参数就很容易了。 比如存在订单越权访问漏洞，但是订单id加密了，越权者就不知道订单id，那么他就无法遍历获取他人订单了。在公司，我们都用的一个流量出口，公司为了内部安全，其实有监控所有人发出的请求。也就是说这个加密id会被流量监控软件捕获到，管理员是可以看到的。加密订单号只是缓解措施，一旦加密的订单号泄露，还是会造成越权漏洞出现。

小丸子

总结一下各位的思路：1、控制参数，加密或者多因素，防止遍历。但参数加密仅仅只能防止的是遍历，并不能真正解决越权，还只是缓解的方式；2、流量监控。现在有一种防范越权和自动化扫描的方法。这个方法，在开发上不用做任何的越权防范，而且扫描器也无法进行正常网站爬行，目前也有产品推出。通过做nginx代理，获取所有的通讯web流量，并且对http传输的请求、内容进行重写、js混淆加密，对返回所有的连接、参数进行重写，到客户端后，流量能正常解析，浏览器能正常接卸，依赖于浏览器的特性，但是扫描器却不知道具体的连接、参数是什么，人工查看源代码时也是混淆过的，发出来的请求也是加密过的，但是到了nginx代理后，会根据加密算法进行解密，也就是web端请求数据也全加密了是吧，明文丢给后端的应用进行处理。

豌豆妹

😈哈哈~“三人行必有我师”。听完各位的一番讨论，我是茅塞顿开啊！非常谢谢本次的特邀嘉宾和各位核心白帽子的大力支持呢~☺下期再见！

JSRC http://security.jd.com/

长按识别左侧二维码，关注我们