# 安全小课堂第九十九期【web漏洞挖掘之未授权访问漏洞】

京东安全应急响应中心 6月11日

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。JSRC **安全小课堂第九十九期**，邀请到**倚笑趁风凉**作为讲师就**web漏洞之未授权访问漏洞**为大家进行分享。感谢白帽子盆友的精彩提问与互动~

常见未授权访问漏洞的挖崛思路和心得?

**京安小妹**

**倚笑趁风凉：**

总体上来说分为系统服务的未授权访问以及 web系统的未授权访问。

粗略的看常见的系统服务的未授权访问有:

1、Redis未授权访问

2、Jenkins 未授权访问

3、MongoDB未授权访问

4、ZooKeeper 未授权访问

5、Elasticsearch 未授权访问

6、Memcache 未授权访问

7、Hadoop 未授权访问

8、 CouchDB 未授权访问

9、 Docker 未授权访问

10、Varnish未授权访问

11、proxool 未授权访问

12、 nfs未授权访问

13、samba 未授权访问

14、influxdb未授权访问

15、Rsync未授权访问

16、Cassandra未授权访问

17、Resin未授权访问

这些在互联网上已经有很详细的总结和分享了。

比如这两个帖子（其中没提及的google一下就有啦）：

https://paper.seebug.org/409/

https://xz.aliyun.com/t/2320/

值得注意的是，其中很多未授权访问的exp都会对系统造成不可逆的影响。所以建议测试人员对于端口类的漏洞 只要模拟未授权登陆的数据包（可以通过wireshak抓取）发往测试服务器即可，Web类的建议通过未授权访问response证明漏洞存在即可。

Web系统的未授权访问分类可能没有那么细致。但是从测试的角度可以大致分为两种。

1、 某些特定的web系统的未授权访问漏洞。如上面的jenkins未授权访问、proxool未授权访问、influxdb未授权访问，其实就是web系统的后台未授权访问。

2、 restful风格的站点，以及前后端分离使得的一些api接口产生未授权访问的情况。

3、websevice未授权访问。

从测试的角度来看，第一类需要对漏洞的积累，以及对新漏洞产生的敏感性，如果具有较强的审计能力，在有源代码的情况下，也可以进行代码审计来审查是否存在未授权访问的情况。

第二类其实技巧就相对比较多了。

我大概枚举了一下可能会用到的一些思路和技巧。

1、因为前后端分离，通过分析静态文件找到接口，其中可能会涉及到的一些技巧包括抓包+爬虫（单页应用还好，多页应用不见得能那么容易的找到静态文件），js解密解混淆（门路也比较多，对前端了解比较深入的会有优势），以及在快速迭代的过程中，可能会存在多个版本的api，其后端逻辑可能不同，所以在已有的基础上，可以通过猜解去爆破一些旧版本的不再维护的api。

2、逆向app找到接口。

3、通过开放平台获取接口信息，并且结合其他方法猜api路径

4、搜索引擎 使用 比如 site，inurl之类的使用。

5、github 源代码泄漏

5、github 源代码泄漏。

6、robot.txt爬虫协议泄漏路径

7、不安全的配置。（比如django的debug模式可以获取url信息）

其实以上每一点都有大量的技巧和经验，都是需要实际应用才能积累下来的。

第三类的websevice测试可以使用SOAP UI Pro进行自动化的安全测试。
也可以手动进行一些xxe，sql注入，ssrf等漏洞测试。

**讲师**

未授权访问漏洞给企业带来的风险问题有哪些？

**京安小妹**

**倚笑趁风凉：**
对于企业来说，最重要的是数据安全，接口的未授权访问最主要的风险是数据泄漏和滥用。像有统一安全网关的企业，端口类的漏洞一般不会直接暴露在互联网上，你只有入侵到了内网端口类的漏洞才有用武之地。
数据安全是互联网公司的基石，所以对企业来说尤为重要。我认为，未授权访问漏洞主要威胁到了企业的数据安全。

**讲师**

未授权漏洞常见的防御方案有哪些？

**京安小妹**

**倚笑趁风凉：**

系统服务的未授权访问防御方案需要注意的有两点：

1、严格按照官方的安全配置配置系统，大部分此类漏洞都是因为不安全配置导致的。

2、持续关注使用系统的cve漏洞，当出现新漏洞时及时预警及修复。

3、避免弱密码。

接口类的防御方案：

1、　　建立统一安全网关，白名单对互联网开放的端口。将流量存入数据库中。通过分析流量来判断端口是否存在未授权访问的情况（知道系统正在发生什么）。

2、　　建立统一安全接口规范，开发的接口必须按照规范设计，编码（在业务快速迭代的情况下，需要安全人员有很强的话语权才能做到。其作用是防范于未然）。

3、　　建立接口分析平台，根据策略对接口进行监控，通过埋点的方式对接口使用者信息进行收集，及用户画像（其数据维度越多，分析的精准性越高）。

**讲师**

未授权访问漏洞案例分享

**京安小妹**

**倚笑趁风凉：**
这里分享一个团队的xfk牛分析的通过ssrf打mysql未授权访问导致rce的案例。
案例链接：
https://blog.formsec.cn/2018/01/22/SSRF-To-RCE-in-MySQL/
注：pgsql和mysql其实可以达到类似的效果
以本案例来说明的原因在于，漏洞相关的研究，不要着眼于某一类漏洞。要全面了解应用或者系统的特性，再结合多种思路去最大化攻击面。

**讲师**

未授权访问漏洞有哪些高级的利用技巧？

**京安小妹**

**倚笑趁风凉：**

未授权访问的利用需要结合具体的漏洞场景进行利用 一般简单的利用方式就是数据查询或获取 高级利用一般分为两类 一种是未授权和其他漏洞的组合拳利用 比如ssrf+内网数据库的未授权访问 未授权接口+xxe等 第二种就是未授权访问服务的功能或特性的恶意利用 比如redis的未授权访问不仅可以查看数据库内容还可以通过写文件等操作获取系统权限 还有rsh未授权访问后通过Restricted Shell Bypass获得权限等

除了上面的ssrf打mysql未授权访问导致rce，举例的话，最近觉得比较高级的利用技巧就是基于Memcache未授权访问的Ddos放大器

其主要思路为利用互联网上的未授权memcahe服务，使用伪造ip来源的udp数据包进行简单查询，使得memcahe返回包远大于请求数据包实现放大器的功能。

详细分析链接：

https://blog.csdn.net/microzone/article/details/79262549

所以所谓的高级利用技巧，就是在你充分了解系统特性的情况下，使用这些特性去构造一些意想不到的攻击。

**讲师**

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

**简历请发送：cv-security@jd.com**

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心