

撞库攻击是场持久战—安全小课堂第十六期

2016-07-01 京东安全应急响应中心

安全小课堂第十六期

用户数据泄露一直是目前互联网行业的焦点，厂商和黑客之间在用户数据这个舞台上一直在进行着旷日持久的攻防战。而撞库攻击则是黑客获得用户数据最常用的手段。本期我们来聊一聊撞库攻击。

本期邀请了
汽车之家安全专家H5
猪八戒网安全专家齐迹
唯品会安全专家孤独雪狼
欢迎小伙伴们~

1



豌豆妹

撞库攻击是什么？



葫芦娃

撞库是黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登陆其他网站后，得到一系列可以登录的用户。很多用户在不同网站使用的是相同的帐号密码，因此黑客可以通过获取用户在A网站的账户从而尝试登录B网址，这就可以理解为撞库攻击。



小新

撞库其实分好多种，“定向的弱密码”、“其他裤子撞”、“纯爆破”都应该算撞库。

哆啦A梦



通俗来讲，我的一条裤子有四个包，分别在前后左右，你的裤子也是，所以就撞“裤”了。在小区捡到一串钥匙，不知道是谁家的，于是我就挨个家门去试。

2



豌豆妹

黑客通过何种途径得到用户数据呢？

葫芦娃



- 1、网上泄漏，利用网站漏洞、网上下载、购买、交换；
- 2、第三方漏洞平台忽略的漏洞等。

3



豌豆妹

撞库前的信息收集一般有哪些途径呢？

小丸子



邮箱、vpn这些边界点是最有效的途径，然后结合账号信息收集，密码字典进行下一

步，这些是对企业安全最有危害的。



豌豆妹

一些判断账号是否存在的接口防御没做好就会有风险，这样的接口也会是撞库踩点的对象吧？



葫芦娃

是的。撞库攻击一直是各大企业头痛的问题，验证码对于黑产、黄牛来说，被破只是时间问题。验证码虽然也增加了很大的难度，但关键是企业大了，接口那么多总有被遗忘的角落，给了黑产机会。撞库的弱点主要在一些不起眼的地方，比如登录调用的api之类的，直接post email，pass等参数，就返回true或者false。

4



豌豆妹

撞库成功的账号拿来干啥？能说下背后产业链么？



哆啦A梦

通俗来说，得到新裤子，就可以拿去和别人换更新的裤子，然后循环，裤子越来越大。



小丸子

其实销路很多，信息关联后，可以卖信息，诈骗，继续撞库关联其他的信息等。虚假营

销，也是一个产业链，用这些账号去发布虚假营销信息。另外还有很多，比如扫码后去做免登爬虫、cookie热部署做业务作弊、钓鱼等，如果有金钱的账户可以直接进去套现。电商行业最简单粗暴的就是诈骗，电商最大的风险是信息泄露，撞库是很重要的一部分。

小新



撞库成功后的账号有两种，一种是会员账号，这种就是用来诈骗、倒卖信息等，一种是企业账号，企业账号的危害直接影响到企业内网。

5



豌豆妹

如何防御撞库攻击？

哆啦A梦



自己搞一套裤子，用户登陆检查一下，发现泄漏就不让登陆，请求频率控制，人机识别。

小丸子



我们把控每个产品安全上线的流程，其中关键接口都会对接FDS风控，例如有小伙伴提到的很多企业对于判断用户名是否存在的接口不关心，但在电商行业不一样，电商行业是非常关注这些看似很弱小的接口。我们发布过安全红线要求，其中就有一条是关键接口需要做好防频调控。

小新



- 1、密码策略健壮；
- 2、OTP策略；
- 3、边界梳理加固；
- 4、黑ip库拦截；
- 5、人机识别；
- 6、验证码。



豌豆妹

请教大家的人机识别都是怎么做的呢？



小丸子

基于用户请求行为进行分析，设备唯一标识，异地判断等。



豌豆妹

异地判断一般有哪些策略呢？



葫芦娃

设备指纹、人机识别等。可通过ip换算经纬度在算距离，我们的登陆cookie就做了这个，所以xss拿了cookie也不一定好使，这也是为什么有些人xss后拿去无法登陆的一种原因。再往后，就是行为分析基于用户行为（时间段、频率、浏览器、访问路径、访问来路等），通过算法对用户的行为进行聚类，得到大部分用户的行为路径，然后通过机器学习建立模型，就能自动判断是否有异常了。



豌豆妹

鼓掌~感谢小伙伴的答疑解惑哟~咱们下期见！




安全小课堂往期回顾：

- 1、论安全响应中心的初衷；
- 2、安全应急响应中心之威胁情报探索；
- 3、论安全漏洞响应机制扩展；
- 4、企业级未授权访问漏洞防御实践；
- 5、浅谈企业SQL注入漏洞的危害与防御；
- 6、信息泄露之配置不当；
- 7、XSS之攻击与防御；
- 8、电商和O2O行业诈骗那些事儿（上）；
- 9、电商和O2O行业诈骗那些事儿（下）；
- 10、CSRF的攻击与防御；
- 11、账户体系安全管理探讨；
- 12、远程代码执行漏洞的探讨；
- 13、服务器安全管控的探讨；
- 14、畅谈端口安全配置；
- 15、谈一谈github泄露。



 jsrc_team

 京东安全应急响应中心

动动手指~关注下呗~