聊聊暴力破解

京东安全应急响应中心 2016-08-10

安全小课堂滴二十一期

暴力破解简单说就是猜测用户名和密码，其危害不容小觑，比如获取了管理平台的帐号，即可控制整个应用。本期，我们来聊一聊暴力破解。

本期邀请到
唯品会安全专家tony
知名安全白帽子ziwen
大家欢迎~

豌豆妹

快来普及下~什么是暴力破解呗？

小丸子 

在你已经知道一个帐号的用户名，但是还不知道密码的情况下，用暴力破解的软件去不断尝试各种密码，以试图获得正确密码的手段。简单说就是猜测用户名和密码。

哆啦A梦 

如果算上文件路径和IP等，范围还是挺广的，很多时候找不到后台等文件，也会用暴力的方式，还有一些存在规律的文件名，穷举，查看里面敏感信息，也算暴力破解吧。另外，盲注有时候也是暴力破解。

豌豆妹

恩呢~中国的词汇衍生意挺广的，所以本期只谈狭义上的暴力破解。咱们回到最开始口令帐号猜解吧。

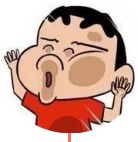
小丸子

木问题~

豌豆妹

弱弱问句它跟撞库有啥不同？

小新



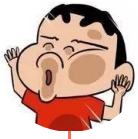
撞库一般是用已经收集到的数据库去暴力破解，这样可以提高成功率和效率嘛。

豌豆妹

那能说说造成暴力破解的原因么？

葫芦娃 

造成暴力破解的原因是因为应用没有防暴力破解的机制。

小新 

恩，一般都是验证码可以绕过，或根本不存在暴利验证机制的地方。比如验证码、限制错误次数等。

哆啦A梦 

验证码有时候加了也会存在问题，比如简单的验证码可以用很简单的开源图形识别去破解，所以最好是动态生成验证码。现在的拖动条，也存在破解概率比较高。用一些模拟鼠标操作搭配图形识别的方法，就可以破解拖动条。

豌豆妹

那能说说暴力破解的危害吗？

小丸子 

危害肯定是不容小觑的，之前12306等很多网站都遭遇过暴力破解导致的大量账户数

据泄露。

哆啦A梦

比如获取了管理平台的帐号，就可以控制整个应用了。

豌豆妹

造成暴力猜解的小工具最主要有哪些呢？

小新

最常用的burpsuite有这个功能，hydra、medusa等。一般面向服务器方面的安全，hydra最好用。web就是burp或者owasp的zap。或者Python自己开发的小工具都挺容易实现的。还有一些基于彩虹表的，类似RainbowCrack。

豌豆妹

那如何防范暴力破解呢？

葫芦娃

加验证码，设置错误次数。在每一个登陆环节都采用验证机制。

哆啦A梦

之前遇到过某网站后台就出现过类似问题，两个分站后台，有一个加了验证码，另一个就干脆没有验证。虽然验证码不是100%有效，但是给登录增加挑战是比较有效的防暴力破解方法。

小丸子

做一个统一的风控平台，甚至可以使用机器学习去识别风险ip，防范的效率就会很高了。

豌豆妹

哈~听完大家的讨论，受益匪浅啦~咱们下期再见。小伙伴们想和哪些大牛沟通，想了解哪些话题，都可发给我哟~

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；
16、撞库攻击是场持久战；
17、url重定向攻击的探讨；
18、聊聊弱口令的危害（一）；
19、聊聊弱口令的危害（二）；
20、聊聊XML注入攻击

jsrc_team

京东安全应急响应中心

动动手指~关注下呗~