Web攻防之暴力破解（何足道版）

sm0nk / 2017-11-29 15:25:00 / 浏览数 4856

原文首发猎户安全实验室公众号

为啥叫"何足道版"，当然跟足道足疗没啥关系不能仁者见仁哈。
当时主要想表达区区小事何足挂齿之意（含抛砖引玉之意），何足道哉。当然据研究金庸武侠，何足道乃倚天前期人物！昆仑派前辈，外号"昆仑三圣"，以琴、棋、剑三圣著
2333

0x00 @序

攻防之初，大多为绕过既有逻辑和认证，以Getshell为节点，不管是SQL注入获得管理员数据还是XSS
获得后台cookie，大多数是为了后台的登录权限，假若我们获得一枚口令，都是柳暗花明。不管口令复杂与否，只要在构造的字典内都是爆破之结晶。
Web形态及业务之错综，我们暂可将能够自定义字典的请求归类到爆破，以便信息的提炼和知识的逻辑推理。

本文主要收集了常用的一些爆破相关的零碎点和技巧点。

0x01 账户探测

1. 探测存在与否
2. 第一梯队：Top500用户名、手机号
3. 第二梯队：邮箱、员工编号

0x02 指定口令爆破用户名

1. 指定类123456口令爆破用户名
2. 正常的top500，top10000帐号；

   单个字母、两个字母、三个字母、四个字母随机组合的帐号；
   a)小工具pydictor值得推荐
   python pydictor.py -base L --len 2 3

   b) Burp也可以

   一位数字、二位数字、三位数字、四位数字的随机组合

   ```
   for n in xrange(10000):
   print str(n).zfill(4)
   ```

5. 厂商名相关帐号
   a) 如：facebook、fb_steven ...
   b) 页面联系邮箱的规则学习及自创建

0x03 密码爆破

top500, top3000,top10000，自定义密码
a) Top 系列，几乎安全从业都有自己的弱口令字典，常规就好，太大的字典跑起来也费劲，关键是定制
b) 定制字典，pydictor值得推荐：https://github.com/LandGrey/pydictor

c) 社工库的使用，指定用户的历史密码，是一种尝试

厂商特色口令生成，如baidu@123
a) 适用于应用管理员类人员以及主机协议类密码
b) 更多定制类字典也可以pydicor
c) http://www.cnblogs.com/shellr00t/p/5316401.html

d) 加密密码暴力破解
e) 普通编码类，如base64

f) 自定义加密算法（目标系统使用了可猜测的加密算法去加密口令）
可参考浮萍写的基于RSA算法加密口令后爆破脚本：
https://github.com/fupinglee/MyPython/blob/master/web/RSADemo.py
g) Selenium 自动浏览器提交模块（可适用与不明加密算法，模拟正常操作流）

*详细代码过程参考我博客：
http://sm0nk.com/2017/11/27/%E5%9F%BA%E4%BA%8ESeleinum%E7%9A%84%E5%8F%A3%E4%BB%A4%E7%88%86%E7%A0%B4%E5%BA%94%E7%94

1. 弱文件后的后台爆破
   a) 弱文件爆破获得后台
   b) 后台密码爆破
   i. 各大中间件及CMS的口令破解，如weblogic 、tomcat
   ii. 自定义后台的密码破解
2. Webshell 密码爆破
   a) Shell 发现（弱文件以及蛛丝马迹）
   b) Shell 爆破（有专用工具，也可用burp完成）
3. 辅助信息
   a) Web 源码、JS 以及注释信息中是否包含用户名以及口令指定规则
   b) 技术运维人员的桌子上面的便签信息（若能接触到目标内部）...

0x04 登录验证码爆破

1. 验证码绕过
   a) 验证码非必须参数，可省略
   b) 验证码不失效，可多次使用
   c) 验证码问题集合答案有限，可以遍历后破解
   d) 非空逻辑校验，验证码置空 或 去掉校验参数的请求
   e.g. ecshop后台暴力破解验证码绕过
2. 简单验证码识别

   https://github.com/fupinglee/CrackCaptcahLogin/releases
   类似工具很多，看使用习惯。
3. 高模糊度验证码识别
   a) 一般的识别流程都是二值化、去干扰、区域选择、OCR识别
   b) 可用云打码平台（不打广告）

0x05 短信/邮箱验证码爆破

1. 部分登录验证码的分类也可适用于此
2. 验证码的本身绕过
   a) 返回包回显（包括返回包、输出在cookie等）
   b) JS控制
   c) 返回包控制：True&false控制（0&1），修改返回包可绕过
3. 4位数字，验证码爆破，很快
4. 6位数字，验证码爆破；可根据多线程的前提进行多进程处理，0-199999一波；200000-399999一波...（依次类推）；也可以看频率，哪块区间分布的概率较高可重点关
5. 弱token
   a) 例：奇虎360任意用户密码修改漏洞，发送给邮箱的验证链接里面的vc值为时间戳的md5加密；作为一种检验参数可被猜测。
   b) 基于密码找回的手机号、UID、邮箱等遍历，结合客户端源码可能的些蛛丝马迹
   c) 不完全属于爆破逻辑，但可互补增值，参考
   http://bobao.360.cn/learning/detail/287.html

0x06 数据信息爆破（遍历）

关键参数的的信息遍历(select)
a) 包括用户名
b) ID号
c) 手机号
d) 邮箱
e) 身份证号
f) 订单号
g) 银行卡
h) 信用卡(e.g 携程乌云漏洞)
i.PAN+信用卡到期时间（即：最小的身份验证模块）；
ii.PAN+信用卡到期时间+CVV；
iii.PAN+信用卡到期时间+CVV+持卡人地址；
iv. From http://t.cn/Rfrsdki

批量注册(insert)
a) 逻辑不严谨或校验不严格，实现多帐号的薅羊毛

一套组合拳（也可关联到爬虫）：
a) 两个常见的功能：密码找回、网站论坛

b)
切入点一：从密码找回功能分析，有相当一部分网站，提供账号检测功能，且提示存在与否，根据友情提示以及次数限定情况，可以通过返回包匹配存在的帐号，包括用
c)
切入点二：密码找回功能，输入手机号后会提示...正在找回XXX的密码信息...，这个就是用户名，（若输入用户名，有可能提示正在找回某手机号的密码信息（部分打码
d) 切入点三：网站论坛，为了交流，以及用户的活跃度，部分网站存在bbs、club等论坛信息，一般二次开发的Discuz 。
上面会存在关于个人的一些数据，比如用户名（论坛网名）、性别、粉丝情况、帖子情况、联系方式、住址（部分需要登录权限）、还有一些倾向数据，比如购物平台关
e)
从这三个切入点来讲，单独哪个可能都影响不足够大，没有达到影响的最大化。从一个数据利用者角度分析，最希望得到与平台性质相关的属性，比如交友网站的性别和
那把三个切入点的数据整合起来能得到什么呢？
i.通过用户检测 获得手机号用户个人信息；
ii.通过手机号检测，获得用户名信息；
iii.通过论坛遍历，获得ID和用户名信息；
iv. 通过关联以上数据，可以对应手机号------>用户名 ------> 论坛ID，同样也就意味着获得了某手机号的用户关注了什么的信息。Demo 说明
用户：188xxxx8888 用户名：HelloWorld 关注：某别墅
用户：138xxxx9999 用户名：52BMW 关注：宝马X6
用户：159xxxx6666 用户名：HelloKitty 就职某金融企业
用户：186xxxx5555 用户名：独孤求败 购买了大疆无人机

针对Demo数据，从一个数据威胁角度来分析，那可以实现精准营销。带来的场景就是另一片天地。

0x07 爆破关联

1. 数据重放-短信炸弹
   a)无任何限制的短信炸弹
   b)单独手机号存在短信阈值限制，有可能通过间隔符绕过，18888888888,,,与18888888888效果一样；
   c)针对单独手机号有阈值限制，但可随意轮询其他手机号，同样有危害
   d)会导致短信网关的资源浪费和流失
2. 数据重放-邮箱炸弹
   a)相对短信炸弹成本较低，但其逻辑同短信炸弹
3. 子域名爆破
   a)根据自己平台和习惯选择即可：subDomainsBrute、Layer、FuzzDomain
4. 子目录、弱文件爆破
   a)弱文件爆破，对比过老御剑、weakfilescan、dirfuzz、cansian.py 仍然觉得一款基于python3的dirsearch 值得拥有（可自定义字典）
   https://github.com/maurosoria/dirsearch
   b)也可以自己写，就是基本的web请求，以及返回包的长度或特征匹配。
5. Fuzzing 测试
   a)SQL、XSS
   b)拒绝服务漏洞，例如SPIKE对表单测试特殊字符的异常处理

0x08 协议口令爆破

1. SSH RDP FTP MySQL MSSQL ...
   a)Fenghuangscan值得推荐，Hydra（Kali自带）值得拥有；
   b)Nmap 也可完成部分破解工作，本身是一个基础工具，但script下的脚本能让你做出不基础的事情
   c)毕竟直接拿到远控权限事半功倍，可直接获取数据，对于测试来讲还可获取源码，以半审计的方法进行挖掘。
   d)且有人以此为生（全网抓鸡）
2. SMTP、VPN协议类
   a) 第一点提到的一些协议，初具成熟均不公开于互联网（当然意识和测试情况也有），但SMTP 和 VPN 类，大部分都有，也是入侵的概率很大的入口点
   i. brut3k1t（github有）
   ii. 也有自定义的PY脚本
   iii. 小技巧点：部分对同一用户有密码失败次数限制，可把循环颠倒过来，用同密码刷一遍用户，在用下一个口令刷一遍用户...
   b)翻到邮箱，根据信息检索，信息很精准，很有可能获得认证信息
   c)获得VPN认证，在内网搞事，一不小心就干掉了一个大家伙。
3. 特殊服务类未授权访问或者弱认证
   a)Redis未授权访问
   b)Jenkins未授权访问
   c)MongoDB未授权访问
   d)ZooKeeper未授权访问
   e)Elasticsearch未授权访问
   f)Memcache未授权访问
   g)Hadoop未授权访问
   h)CouchDB未授权访问
   i)Docker未授权访问
   j)毕竟这些未授权可以直接getshell或直接获得数据
   详细介绍利用及加固请参考https://www.secpulse.com/archives/61101.html

0x09 攻击防御

1. 登录界面暴力破解，哪些加固方法？
   a)阈值的设立
   i.单位时间内超过额定请求次数，封帐号&封IP段时间
   ii.支持逆向思路
   b)密码输入错误次数达到3次后增设验证码
   i.验证码自身的安全性参考下一个问题
   c)自身应用系统的健壮性
   i.强制要求用户注册时满足口令复杂度要求
   ii.定期检索数据库弱口令帐号的存在，可比对top500的密文值
2. 图形验证码自身常见的加固方法？
   1)字体扭曲
   2)字体粘连
   3)字体镂空
   4)字体混用
   5)主体干扰线
   6)背景色干扰
   7)背景字母干扰
   8)公式验证码
   9)加减法验证码
   10)逻辑验证码
3. Modsecurity类防御暴力破解类？
   a)若代码变更成本大，可以使用Modsecurity（当然直接买硬WAF也可以）
   b)https://www.trustwave.com/Resources/SpiderLabs-Blog/Defending-WordPress-Logins-from-Brute-Force-Attacks/（Freebuf有翻译）
4. 针对验证码可多次重用的加固方法？
5. 主机类暴力破解的防御方法？
   a)自身的帐号口令体系满足复杂度要求
   b)若非必须的服务，直接禁止对外的开放，包括22、3389
   c)限定指定IP访问（网络的访问控制）
   d)不使用口令方式，使用私钥类登录
   e)意识类：不在标签写密码；运维管理类也不直接统记录到一个txt

上一篇：绕过 Cisco TACACS+ ... 下一篇：浅析PHP反序列化漏洞之PHP常见...

1. 8 条回复

mr.bingo 2017-11-29 15:31:49

感觉以后写了文章，却想不到牛逼100分的名字，就不敢发文章了。{手动可怜}

0 回复Ta


sm0nk 2017-11-29 15:33:56

不仅爆破是门艺术，生活和扯淡都是艺术。

1 回复Ta


sm0nk 2017-11-29 15:35:59

@mr.bingo 名称代起服务，一顿小龙虾（手动哈哈）

0 回复Ta


hades 2017-11-29 15:44:23

@sm0nk 潘少辛苦了 (□•□□•□)□□

0 回复Ta


bigcow 2017-11-30 11:01:27

不如跳舞，爆破不如跳舞

0 回复Ta


bywalks 2017-12-19 11:33:29

厉害厉害。有收获。

0 回复Ta


mahuateng**** 2018-01-22 11:51:33

确实，收益匪浅

0 回复Ta

wir****rk93 2018-01-27 00:52:58

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板