



密码暴力破解漏洞

无涯老师

课程大纲

- 1、密码安全概述
- 2、不安全的密码
- 3、密码猜解思路
- 4、Python暴力破解
- 5、Burp Suite暴力破解
- 6、BP其他攻击模式
- 7、DVWA其他关卡
- 8、如何防御暴力破解
- 9、其他暴力破解工具



01

密码安全概述

密码 (password) 的作用

- 1、加密
- 2、完整性
- 3、身份认证 (口令)

《智取虎威山》片段

座山雕 （突然地）天王盖地虎！

杨子荣 宝塔镇河妖！

众金刚 么哈？么哈？

杨子荣 正晌午时说话，谁也没有家！

座山雕 脸红什么？

杨子荣 精神焕发！

座山雕 怎么又黄啦？

〔众匪持刀枪逼近杨子荣。

杨子荣 （镇静地）哈哈哈哈哈！防冷涂的蜡！

密码安全的分类

- 1、存储安全
- 2、传输安全
- 3、输入安全（登录界面）

权限管理

- 1、认证：你是谁
- 2、授权：你能做什么

漏洞利用

- 1、从数据库获取密码，解密
- 2、窃听通信数据数据，解密
- 3、直接从登录框猜测密码



02

不安全的密码

默认密码

000000

123456

空密码

身份证号后六位

手机号后六位

.....

弱口令

<https://nordpass.com/most-common-passwords-list/>

裤子

CSDN-中文 IT 社区-600 万.rar 104MB

多玩网_800W.rar 216MB

人人网 500W_16610.rar 49.5MB

猫 1000W_8228.rar 91.9MB

嘟嘟牛_66277.rar 205MB

7k7k2000 万_2047.rar 194MB

178(1000w)_3087.rar 103MB



03

密码猜解思路

猜测范围

- 1、密码长度
- 2、密码内容 0-9 a-z A-Z !@#\$%^&*

APP密码范围

返回 注册个人账户

手机号 请输入手机号码

图形码 请输入图形码 

验证码 请输入验证码 [获取验证码](#)

公证处 请选择公证处 >

密码 **6-16位字母和数字组合**

确认密码 请再次输入密码

推荐码 请输入推荐码 (非必填)

如何获取推荐码,请联系客服: [400-8780020](tel:400-8780020)

[注册完成](#)

点击注册即表示您已同意 **《公证云平台用户服务协议》**

< 注册

手机号码 [获取验证码](#)

短信验证码

用户名,4-18位数字或字母

登录密码 **6-16位数字字母或符号**

确认登录密码

真实姓名

身份证号码

☒ 我已阅读并同意《服务协议》、《隐私政策》

[立即注册](#)

温馨提示:

1.为了便于记忆,建议您使用手机号码或身份证作为用户名.

2.如您已有湖南省以上政务和社会保险账号,请

< 用户注册

请输入您的手机号码

图片的验证码 

请输入验证码: [获取验证码](#)


请输入新密码(8-16位)

请确认密码(8-16位)

☐ 我同意《用户协议》和《隐私政策》

[注册](#)

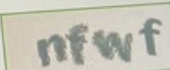
注册

 掌上12333

手机号码 请输入本人常用手机号

登录密码: 请设置登录密码
* 8-20位同时包含大写、小写及数字

确认密码: 请再次确认登录密码
* 8-20位同时包含大写、小写及数字

验证码: 请输入图中的文字 

请输入您收到的数字验证码 [获取验证码](#)

[立即注册](#)

已有账号, 现在登录



04 字典wordlist

字典从哪里来？

通用字典 (word list、dict) :

- 1、Kali自带
- 2、网络下载 (百度、github)

注意使用场合：比如Web网站密码字典、WiFi密码字典、操作系统用户密码字典、数据库密码字典.....

： 专用字典

1、指定格式字典，比如生日、手机号、QQ号

`crunch -h`

2、社工字典

`cupp`、`ccupp`

3、文章内容字典

`cewl https://sqlmap.org -w dict.txt`

kali crunch

参数	说明
-b	指定文件输出的大小，避免字典文件过大
-c	指定文件输出的行数，即包含密码的个数
-d	限制相同元素出现的次数
-e	定义停止字符，即到该字符串就停止生成
-f	调用库文件（/usr/share/crunch/charset.lst）
-i	改变输出格式，即 aaa, aab -> aaa, baa
-l	通常与-t 联合使用，表明该字符为实义字符
-m	通常与-p 搭配。用-p 替代
-o	将密码保存到指定文件
-p	生成不重复的字符串 必须放在最后 不能和-s 一起使用 会忽略最小长度和最大长度
-q	读取密码文件，即读取 pass.txt
-r	定义从某一字符串重新开始
-s	指定一个开始的字符，即从自己定义的密码 xxxx 开始
-t	指定密码输出的格式 @ 小写字母 , 大写字母 % 数字 ^ 字符
-u	禁止打印百分比（必须为最后一个选项）
-z	压缩生成的字典文件，支持 gzip, bzip2, lzma, 7z gzip 压缩最快但是最慢，7z 压缩最慢但是体积最小

crunch 案例 1-7

命令	解释
<code>crunch 1 8</code>	第一个是a，最后一个为zzzzzzzz
<code>crunch 1 6 abcdefg</code>	第一个是a，最后一个为gggggg
<code>crunch 1 6 abcdefg\</code>	第一个是a，最后一个为6个空格也可以写成 "abcdefg "
<code>crunch 1 8 -f charset.lst mixalpha-numeric-all-space -o wordlist.txt</code>	第一个是a，最后一个为8个空格 /usr/share/crunch/charset.lst
<code>crunch 8 8 -f charset.lst mixalpha-numeric-all-space -o wordlist.txt -t @@dog@@@ -s cbdogaaa</code>	从cbdogaaa开始，到" dog "结束
<code>crunch 2 3 -f charset.lst ualpha -s BB</code>	BB开始，ZZZ结束
<code>crunch 4 5 -p abc</code>	(排列组合)生成abc, acb, bac, bca, cab, cba这个时候数字无用

crunch 案例 8-14

命令	解释
<code>crunch 4 5 -p dog cat bird</code>	(排列组合) 生成birdcatdog, birddogcat, catbirddog, catdogbird, dogbirdcat, dogcatbird
<code>crunch 1 5 -o START -c 6000 -z bzip2</code>	每个txt文件包含6000个单词, 用bzip2压缩文件名: first_word-last_word.txt.bz2bzip2 -d解压
<code>crunch 4 5 -b 20mib -o START</code>	生成aaaa-gvfed.txt, gvfee-ombqy.txt, ombqz-wcydt.txt, wcydu-zzzzz.txt每个文件呢20M, 最后一个是实际大小
<code>crunch 3 3 abc + 123 !@# -t %@^</code>	3位长度, 格式: 小写、数字、字符内容顺序: 小写、大写、数字、符号大写在格式中不包括, 用+占位小写包含: abc数字包含: 123符号包含: !@#从a1!开始, c3#结束
<code>crunch 3 3 abc + 123 !@# -t ^%@</code>	格式: 字符、数字、小写字母
<code>crunch 4 4 + + 123 + -t %%@^</code>	4位, 格式: 数字、数字、小写字母、字符内容顺序: 小写、大写、数字、符号除了数字只有123以外, 其他的都不限制从11a!开始到"33z "结束
<code>crunch 5 5 -t ddd@@ -o j -p dog cat bird</code>	从birdcatdogaa开始到dogcatbirdzz结束

crunch 案例 8-14

命令	解释
<code>crunch 7 7 -t p@ss,%^ -l a@aaaaa</code>	格式：p@ss大写数字符号@ 小写字母，大写字母% 数字^ 字符-1 表明该字符为实义字符 从p@ssA0!开始到p@ssZ9 结束
<code>crunch 5 5 -s @4#S2 -t @%,2 -e @8 Q2 -l @dddd -b 10KB -o START</code> 有空格要加双引号	-s起始字符-e结束字符格式：@数字符号大写2从@4#S2开始，到@8 Q2结束
<code>crunch 5 5 -d 2@ -t @@@%</code>	从aab00到zzy99-d 限制相同元素出现的次数
<code>crunch 10 10 -t @@@^%^^ -d 2@ -d 3% -b 20mb -o START 11 -h</code>	从aab!0001!!开始到zzy 9998 结束每个文件20M
<code>crunch 8 8 -d 2@</code>	从aabaabaa到zzyzzyzz
<code>crunch 4 4 -f /usr/share/crunch/unicode_test.lst japanese -t @%% -l @xdd</code> 下载： https://github.com/jaalto/external-sf--crunch-wordlist	从@日00开始，到@語99结束



05

python实现暴力破解

python爆破

- 1、从字典读取值，生成密码
- 2、HTTP连接到需要爆破的地址
- 3、获得HTTP响应，分析响应结果，看看有没有错误提示
“Username and/or password incorrect.”
- 4、如果有提示，就继续下一次循环
- 5、如果没有，就代表爆破成功



06

Burp Suite实现暴力破解

⋮ Intruder 攻击模式

Sniper

狙击手

Battering ram

攻城锤

Pitchfork

草叉

Cluster bomb

榴霰[xiàn]弹





07

密码暴力破解的防御

暴力破解防御

- 1、sleep
- 2、Token
- 3、限制尝试次数，锁定账户

限制次数

×

该账户不存在或登录密码出错已达上限，请更换账户。









登录

忘记登录密码?

立即注册

登录

淘宝会员登录 账户激活 免费注册

二次验证

✓ 验证码发送成功

手机150*****07

请输入验证码

发送验证码

确定



reCAPTCHA (IP验证)

Confirm Humanity

Before we subscribe you, we need to confirm you are a human.



进行人机身份验证



Captcha failed. Please try again.

<https://mvnrepository.com>

One more step




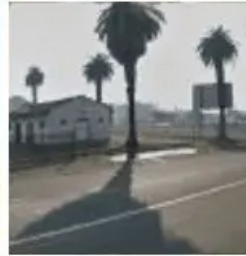





Please complete the security check






我是人类



Select all images with
a fire hydrant
Click verify once there are none left.





VERIFY

行为识别



[GitHub] Please verify your device

GitHub

[详情](#)

Hey [REDACTED]!

A sign in attempt requires further verification because we did not recognize your device. To complete the sign in, enter the verification code on the unrecognized device.

Device: Microsoft Edge on Windows

Verification code: [165316](#)

If you did not attempt to sign in to your account, your password may be compromised. Visit <https://github.com/settings/security> to create a new, strong password for your GitHub account.

 翻译邮件

LastPass...|

LOG IN

OR [CREATE AN ACCOUNT](#)

Email address

Master Password

LOG IN

[FORGOT PASSWORD?](#)

Advanced options ▾



Try again OR look for an email from LastPass to verify it's you. [Dismiss](#)

入侵防御

互联网防护

VPC防护

防护数据

攻击总数

2220

攻击次数

2181

已拦截

39

仅告警



攻击类型分布



- 异常连接 2
- 命令执行 9
- 暴力破解 2105
- 扫描 48
- 其他 21
- web攻击 35

强制修改密码

修改密码

由于你长时间未登录，确保账号安全，请修改密码重新登录

* 原密码

.....

* 新密码

.....

* 确认密码

.....|

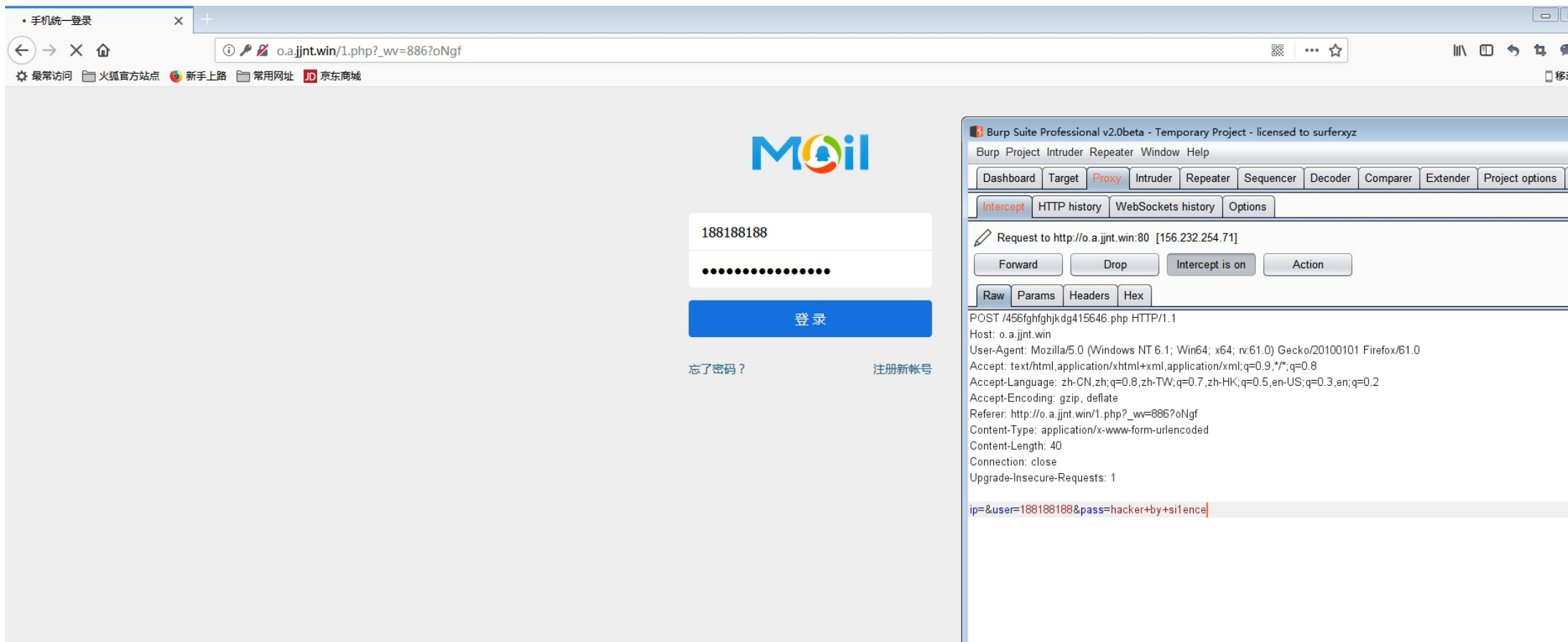
取消密码登录

segmentfault、知乎

个人用户安全建议

- 1、使用复杂密码
- 2、不同网站使用不同密码
- 3、定期修改密码
- 4、防止被钓鱼

钓鱼





08

其他暴力破解工具

wfuzz

- 1、猜参数
 - 2、爆破密码
 - 3、找出网站过滤的参数，比如SQL注入和XSS
 - 4、目录扫描
 - 5、压力测试
-

```
wfuzz -z file,user -z file,password -d  
"username=FUZZ&password=FUZZ2Z&submit=login"  
http://192.168.142.1/pikachu/vul/burteforce/bf_form.php
```



<https://github.com/vanhauser-thc/thc-hydra>
支持:

Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MEMCACHED, MONGODB, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, Radmin, RDP, Rexec, Rlogin, Rsh, RTSP, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP

Hydra

参数	解释
-R	恢复上次中断的会话
-I	忽略之前的会话文件
-S	SSL连接
-s	指定端口
-l	用户名字典, -L 来自文件
-p	密码字典, -P 来自文件
-x	密码生成
-y	禁用字符

Hydra

参数	解释
-r	rainy mode
-e	循环测试用户名而不是密码
-C	当用户名和密码存储到一个文件时使用此参数。注意，文件(字典)存储的格式必须为“用户名:密码”的格式。
-M	批量爆破
-o	输出的文件名
-b	输出格式
-f	一旦爆破成功一个就停止爆破
-t	指定爆破时的任务数量(可以理解为线程数)，默认为16

Hydra

参数	解释
-T	总并发数
-w	每个线程的连接之间的响应等待时间
-c	所有线程单次登录等待时间
-4/-6	使用IPv4 / IPv6地址
-v	显示爆破的详细信息
-O	使用旧的SSL v2或v3版本
-q	不打印有关连接错误的消息
-U	服务模块使用详细信息

Hydra-Examples

```
hydra -l user -P passlist.txt ftp://192.168.0.1
```

```
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
```

```
hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
```

```
hydra -l admin -p password ftp://[192.168.0.0/24]/
```

```
hydra -L logins.txt -P pws.txt -M targets.txt ssh
```



Medusa

<http://foofus.net/goons/jmk/medusa/medusa.html>

支持AFP, CVS, FTP, HTTP, IMAP, MS-SQL, MySQL, NCP (NetWare), NNTP, PcAnywhere, POP3, PostgreSQL, rexec, rlogin, rsh, SMB, SMTP(AUTH/VRFY), SNMP, SSHv2, SVN, Telnet, VmAuthd, VNC

medusa

参数	解释
-h	主机名或者IP名
-H	主机名或者IP名（文件）
-u	用户名
-U	用户名(文件)
-p	密码
-P	密码(文件)
-C	指定测试格式为"user:password"的字典
-O	将输出结果保存在指定文件

medusa

参数	解释
-e	额外的密码检测 (n: 空密码 s: 用户名=密码)
-M	指定执行的模块(不带.mod扩展名)
-m	指定传递给模块的参数
-d	查看支持破解的模块
-n	指定非默认的TCP端口
-s	启动SSL
-g	设置连接超时时间(默认值3)
-r	设置重试的次数(默认值3)



参数	解释
-R	重试次数
-c	验证socket连接是否可用的等待时间
-t	设置同时测试的登录总数
-T	设置同时测试的主机总数
-L	一个线程使用一个用户名
-f	在破解得到第一个用户名或密码后停止扫描主机
-F	当在任何主机上破解得到第一个用户名或密码后停止扫描
-b	不显示软件启动时的版本信息

medusa

参数	解释
-q	显示模块的使用信息
-v	详细等级 (0-6)
-w	错误调试等级 (0-10)
-V	显示版本信息
-Z	恢复中止的扫描

msf辅助模块

msfconsole

use auxiliary/scanner/ssh/ssh_login

set RHOSTS 192.168.142.66

set PASS_FILE /root/vuln/pass

set USER_FILE /root/vuln/user

exploit



Thank you for watching

无涯老师