WebCrack：网站后台弱口令批量检测工具

yzddmr6 / 2019-09-15 10:45:42 / 浏览数 3736 安全工具 工具 顶(1) 踩(0)

自己开发webcrack的过程，希望能跟大家分享一下。

注：本工具借鉴吸收了TideSec的web_pwd_common_crack很多优秀的思路，在此基础上增加了很多拓展功能使其更加强大，在这里给TideSec的大佬点个赞！

前言

在做安全测试的时候，随着资产的增多，经常会遇到需要快速检测大量网站后台弱口令的问题。

然而市面上并没有一个比较好的解决方案，能够支持对各种网站后台的通用检测。

所以WebCrack就应运而生。

工具简介

WebCrack是一款web后台弱口令/万能密码批量爆破、检测工具。

不仅支持如discuz，织梦，phpmyadmin等主流CMS

并且对于绝大多数小众CMS甚至个人开发网站后台都有效果。

在工具中导入后台地址即可进行自动化检测。

实现思路

大家想一下自己平常是怎么用burpsuite的intruder模块来爆破指定目标后台的

```
■■ -> send to intruder -> ■■■■■■■■■■ -> ■■payload■■ -> ■■■■■■■
```

找出返回包长度大小不同的那一个，基本上就是所需要的答案。

那么WebCrack就是模拟这个过程

但是就要解决两个问题

如何自动识别出要爆破的参数

如何自动判断是否登录成功

识别爆破参数

对于这个问题采用了web_pwd_common_crack的解决办法

就是根据提取表单中 user pass 等关键字，来判断用户名跟密码参数的位置

但是在测试中还发现，有些前端程序员用拼音甚至拼音缩写来给变量命名

什么yonghu，zhanghao，yhm(用户名), mima 等

虽然看起来很捉急，但是也只能把它们全部加进关键字判断名单里。

如何判断登录成功

这个可以说是最头疼的问题

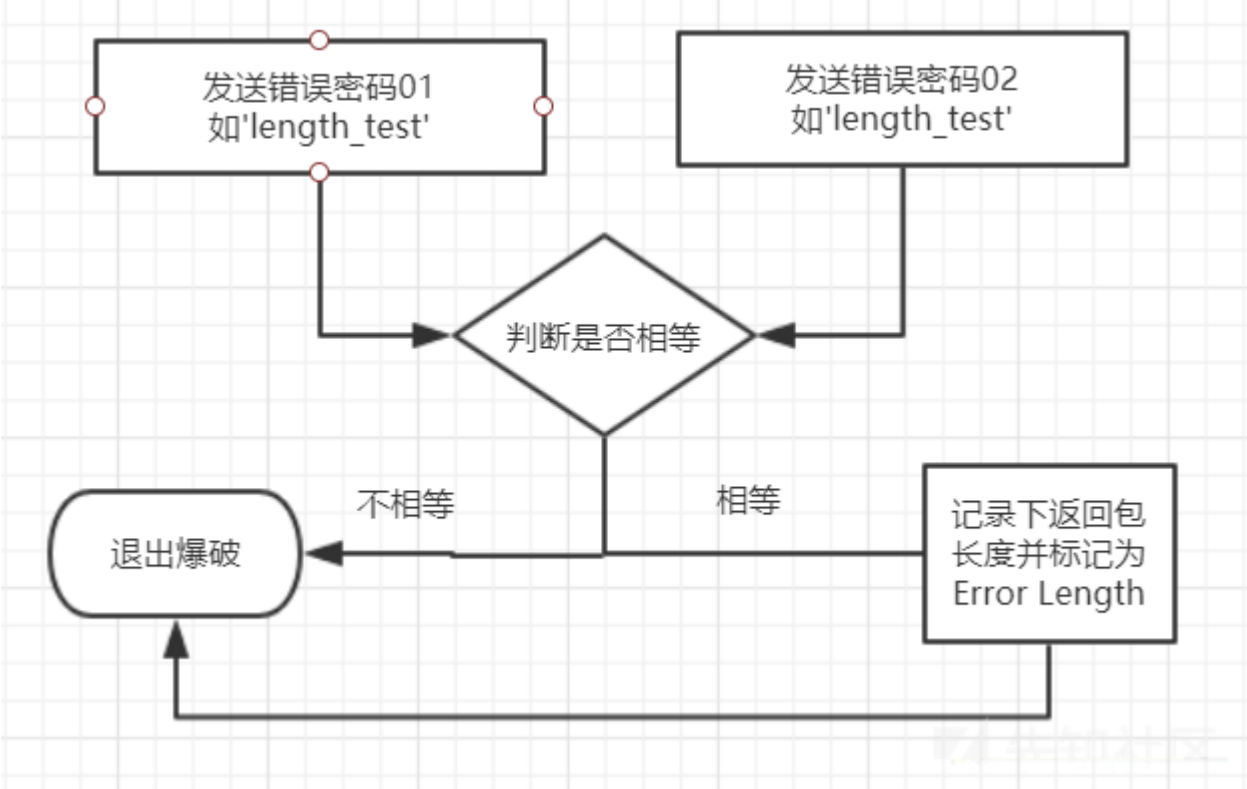
如果对于一种管理系统还好说，只要找到规律，判断是否存在登录成功的特征就可以

但是作为通用爆破脚本来说，世界上的网站各种各样，不可能去一个个找特征，也不可能一个个去正则匹配。

经过借鉴web_pwd_common_crack的思路，与大量测试

总结出来了以下一套比较有效的判断方式。

判断是否动态返回值并获取Error Length



先发送两次肯定错误的密码如`length_test`

获取两次返回值并比较

如果两次的值不同，则说明此管理系统面对相同的数据包返回却返回不同的长度，此时脚本无法判断，退出爆破。

如果相同，则记录下此值，作为判断的基准。

然而实际中会先请求一次，因为发现有些管理系统在第一次登录时会在响应头部增加标记。如果去掉此项可能会导致判断失误。

判断用户名跟密码的键名是否存在在跳转后的页面中

这个不用过多解释，如果存在的话说明没登录成功又退回到登录页面了。

有人会问为什么不直接判断两个页面是否相等呢

因为测试中发现有些CMS会给你在登录页面弹个登录失败的框，所以直接判断是否相等并不准确。

还有一种计算页面哈希的办法，然后判断两者的相似程度。

但是觉得并没有那个必要，因为有不同的系统难以用统一的阈值来判断，故舍弃。

关键字黑名单检测

本来还设置了白名单检测机制

就是如果有"登录成功"的字样出现肯定就是爆破成功

但是后来发现并没有黑名单来的必要。

因为首先不可能把所有CMS的登录成功的正则样本都放进去

其次在测试的过程中，发现在其他检测机制的加持后，白名单的判断变得尤其鸡肋，故舍弃。

并且黑名单的设置对于万能密码爆破模块很有好处，具体往下看吧。

Recheck环节

为了提高准确度，防止误报。

借鉴了web_pwd_common_crack的思路增加recheck环节。

就是再次把crack出的账号密码给发包一次，并且与重新发送的error_length作比对

如果不同则为正确密码。

在这里没有沿用上一个error_length，是因为在实际测试中发现由于waf或者其他因素会导致返回包长度值变化。

框架拓展

用上面几种办法组合起来已经可以做到基本的判断算法了

但是为了使WebCrack更加强大，我又添加了以下三个模块

动态字典

这个不用过多解释，很多爆破工具上都已经集成了。

假如没有域名，正则检测到遇到IP的话就会返回一个空列表。

假如域名是

```
test.webcrack.com
```

那么就会生成以下动态字典列表

```
test.webcrack.com
webcrack.com
webcrack
webcrack123
webcrack888
webcrack666
webcrack123456
```

后缀可以自己在脚本中定义。

万能密码检测

后台的漏洞除了弱口令还有一大部分是出在万能密码上

在WebCrack中也添加了一些常用的payload

```
admin' or 'a'='a
'or'='or'
admin' or '1'='1' or 1=1
')or('a'='a
'or 1=1--
```

可以自行在脚本里添加更多payload。

但是同时带来个问题会被各大WAF拦截

这时候黑名单就派上用场啦

可以把WAF拦截的关键字写到检测黑名单里，从而大大减少误报。

小插曲

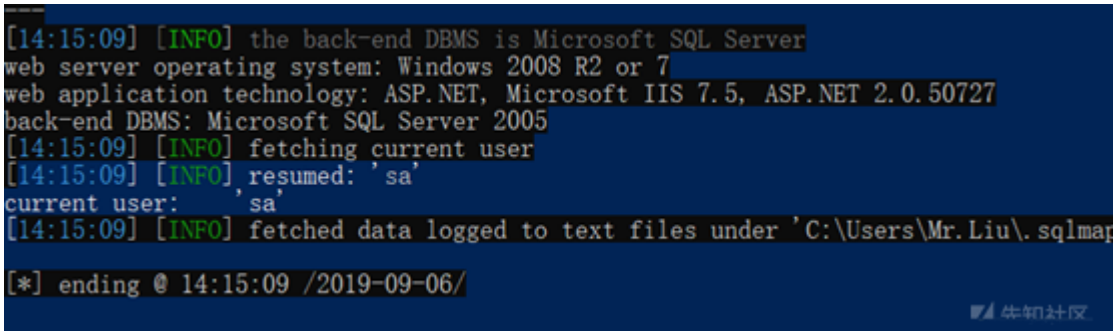
用webcrack检测目标资产进入到了recheck环节

但是webcrack却提示爆破失败。

手工测试了一下检测出的万能密码

发现出现了sql错误信息

意识到可能存在后台post注入



发现了sa注入点

这也反应了对于后台sql注入，webcrack的正则匹配还做的不够完善，下一个版本改一下。

自定义爆破规则

有了上面这些机制已经可以爆破大部分网站后台了

然而还是有一些特(sha)殊(diao)网站，并不符合上面的一套检测算法

于是webcrack就可以让大家自定义爆破规则。

自定义规则的配置文件放在同目录cms.json文件里

参数说明

```
[
   {
       "name":"■■■cms■■",
       "keywords":"■■■cms■■■■■■■■,■■■cms■■■",
       "captcha":"1■■■■■■■■■0■■■■■■■■■■■■■■■■■■■■■■■1■■■■■■",
       "exp_able":"■■■■■■■■■■■■■■",
       "success_flag":"■■■■■■■■■■■■■■",
       "fail_flag":"■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■dz■■■■■■■■■■cms",
       "alert":"■■1■■■■■■note■■■",
       "note":"■■■■■■■■UTF-8■■■■■■■■■■■■■■"
   }
]
```

举个例子

```
{
       "name":"discuz",
       "keywords":"admin_questionid",
       "captcha":0,
       "exp_able":0,
       "success_flag":"admin.php?action=logout",
       "fail_flag":"[redacted]",
       "alert":0,
       "note":"discuz[redacted]"
   }
```

其实对于dz,dedecms,phpmyadmin等框架本身的逻辑已经可以处理

添加配置文件只是因为程序默认会开启万能密码爆破模块

然而万能密码检测会引起大多数WAF封你的IP

对于dz，dedecms这种不存在万能密码的管理系统如果开启的话不仅会影响效率，并且会被封IP

所以配置文件里提供了各种自定义参数，方便用户自己设置。

关于验证码

验证码识别算是个大难题吧

自己也写过一个带有验证码的demo，但是效果并不理想

简单的验证码虽然能够识别一些，但是遇到复杂的验证码就效率极低，拖慢爆破速度

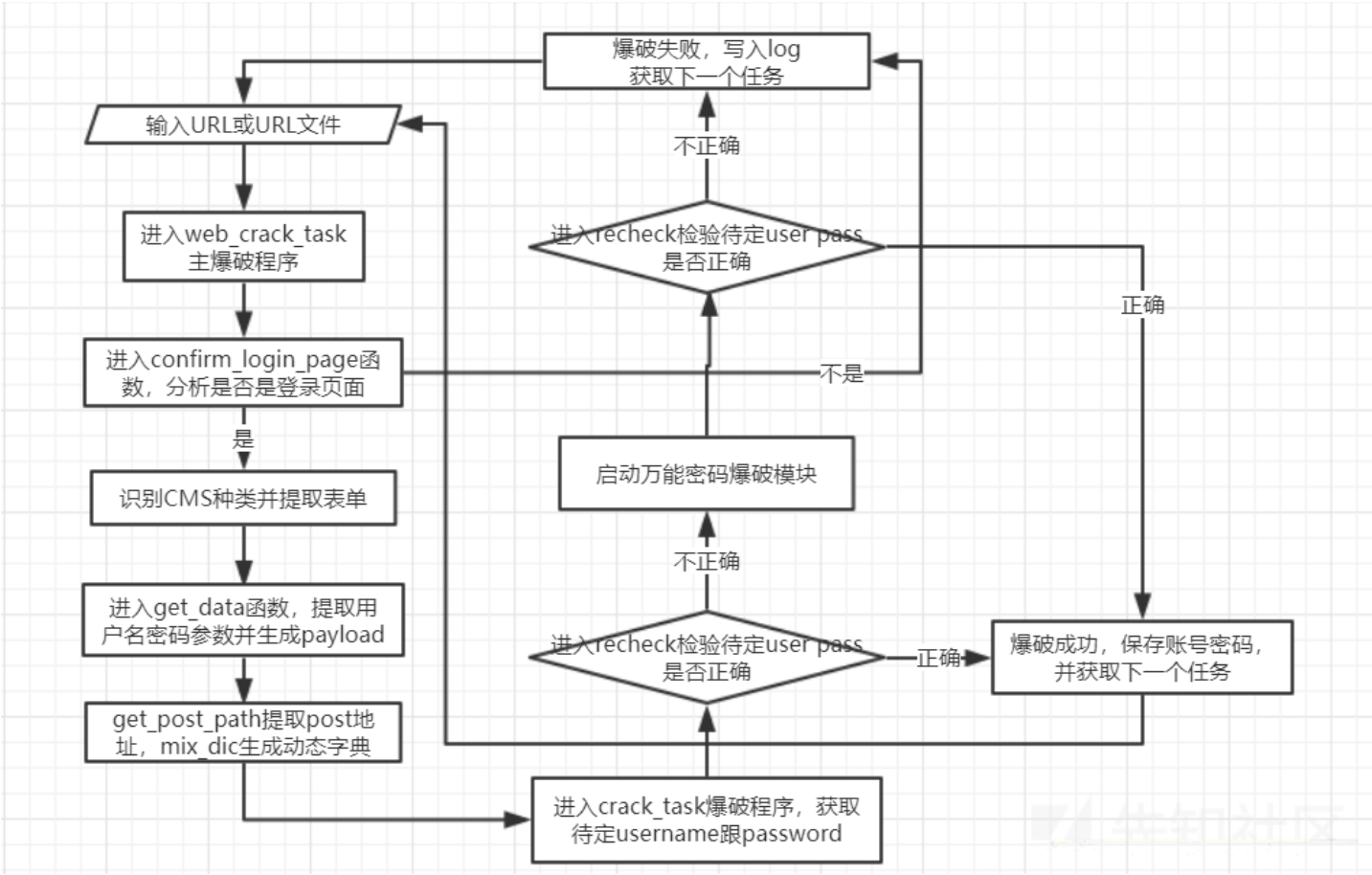
并且你识别出来也不一定就有弱口令。。。

所以就去掉了这个功能

如果有大佬对这方面有好的想法，欢迎在github上留言或者邮箱 yzddmr6@gmail 联系我。

总流程图

一套流程下来大概是长这个亚子



对比测试

找了一批样本测试，跟tidesec的版本比较了一下

web_pwd_common_crack 跑出来11个

其中7个可以登录。4个是逻辑上的误报，跟waf拦截后的误报。

webcrack 跑出来19个

其中16个可以登录。2个是ecshop的误报，1个是小众cms逻辑的误报。

webcrack比web_pwd_common_crack多探测出来的9个中

有5个是万能密码漏洞，2个是发现的web_pwd_common_crack的漏报，2个是动态字典探测出来的弱口令。

最后

这个~~辣鸡~~项目断断续续写了半年吧

主要是世界上奇奇怪怪的网站太多了，后台登录的样式五花八门。

有些是登录后给你重定向302到后台

有些是给你重定向到登录失败页面

有些是给你返回个登录成功，然后你要手动去点跳转后台

有些直接返回空数据包。。。

更神奇的是ecshop(不知道是不是所有版本都是这样)

假如说密码是yzddmr6

但是你输入admin888 与其他错误密码后的返回页面居然不一样。。。

因为加入了万能密码模块后经常有WAF拦截，需要测试各个WAF对各个系统的拦截特征以及关键字。

总的半年下来抓包抓了上万个都有了。。。。。。

因为通用型爆破，可能无法做到百分百准确，可以自己修改配置文件来让webcrack更符合你的需求。

如果有好的想法欢迎在github上给我留言。

项目地址

https://github.com/yzddmr6/WebCrack

本人代码辣鸡，文笔极差，还望大佬轻喷。

上一篇：ByteCTF一道题的分析与学习P... 下一篇：Remote Code Execu...

1. 4 条回复

小菜鸟吃菜 2019-10-11 10:48:05

手动点赞

0 回复Ta

 wooyun路人甲 2019-10-18 09:34:17

支持！

0 回复Ta

 aspxm**** 2019-10-21 22:47:11

输入网址后程序直接闪退，error.txt2019-09-09.6451234' action'

0 回复Ta

 aspxm**** 2019-10-22 10:38:38

敢问大神，需要在py哪个版本中运行？

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