突破封闭Web系统的技巧之正面冲锋

作者: LANDGREY ● 创建时间 2017年12月24日 17:45 ● 更新时间 2017年12月30日 00:08
浏览: 988 次. ● 标签: #渗透测试, #思考, #Web安全备忘录
您的IP地址: 140.207.23.83

首发于：信安之路公众号

前言：

在互联网安全服务公司乙方工作的人或者进行SRC众测等相关渗透测试时，经常碰到客户只给一个"xxx信息管理系统"、"xxx平台"之类的一个Web登录界面的系统的链接地址，其它全凭自己造化，去找漏洞吧!

我将上面讲的"需要认证后才能进入系统进行操作，但是当前没有认证凭证"的web系统"统一称为"封闭的Web系统"，本文认为阅读人员有一定的渗透测试经验，并将就如何突破封闭的Web系统，进行探讨。分享自己的思路与常用技巧，欢迎同道中人一起交流思路。

注：本文有一定的攻击性操作，仅为安全从业人员渗透测试思路交流，请在法律条规允许的范围内进行安全测试。

一：文章脉络

《突破封闭Web系统的技巧》由两篇文章组成。这是第一篇文章"正面冲锋"。下面是本文的脉络：

```
正面冲锋
0x00：登录绕过
0x01：密码猜解
0x02：管理员猜解
0x03：普通用户猜解
0x04：突破加密传输的口令
0x05：突破登录IP限制
0x06：图形验证码绕过
0x07：短信验证码绕过
0x08：双因子验证绕过
```

二：正面冲锋

遇到需要登录才能进一步测试的系统，又没登录口令？没关系，我们有不少正面冲锋的小技巧，相信你看完一定有所收获。

0x00：登录绕过

如果能绕过系统认证，直接登录，那就万事大吉了！登录绕过的方法主要有：

1. SQL注入万能登录密码 a’ or ’1’=’1’ --
2. XSS获取到已登录系统的用户Cookie，替换后可进入系统
3. 通过列目录漏洞或目录文件扫描，发现存在未授权访问的管理页面，可以直接访问进行操作
4. 通过抓包，更改用户id、登录名或Cookie中的敏感认证字段值，即可越权访问
5. 通过已知的后门链接或代码中固化的后门管理口令，直接登录

0x01：密码猜解

大部分系统登录是绕不过的，最常用的还是猜解已知用户名的密码，用合法的凭证登录系统。

Web系统进行密码猜解，大部分人喜欢叫密码爆破，因为猜解一个人的密码，通常需要成千上万的密码来试。密码猜解的目的是准确、高效的获得已知用户的正确密码。

1. 用来发送HTTP/S协议爆破密码的工具主要是用Burpsuite。其它的就是用一些脚本，自己造轮子或用已经写好的较为通用的脚本，如 htpwdScan 。

2. 高效的保证就是猜解时使用的密码字典要适合，一般是先尝试TOP500、TOP1000、TOP10000系列的通用弱口令字典。

3. 还没有成功的话，就需要自己根据目标的信息构造特定字典来爆破了。可以自己写脚本生成，但是费时费力，对于比较急的任务往往不适用。推荐下自己写的一个高级字典生成工具pydictor 可以直接配置里面的规则生成字典，也支持高级玩家写自己的密码生成插件，一劳永逸。其它的一些好的字典生成工具推荐 crunch、Cewl、Cupp。

0x02：管理员猜解

在不能判断系统中存在什么样的用户名时，通常先进行管理员用户名的猜解，然后再根据存在的用户名进行密码破解。我总结了一个常见系统管理和测试用户名字典AwesomeSystemTestUsername，可以做为管理员用户名的猜解使用。

如果一个系统对存不存某用户名无任何有用提示，可以直接使用上面的字典，加上弱口令TOP1000，同时爆破用户名和密码，常有意外收获！

0x03：普通用户猜解

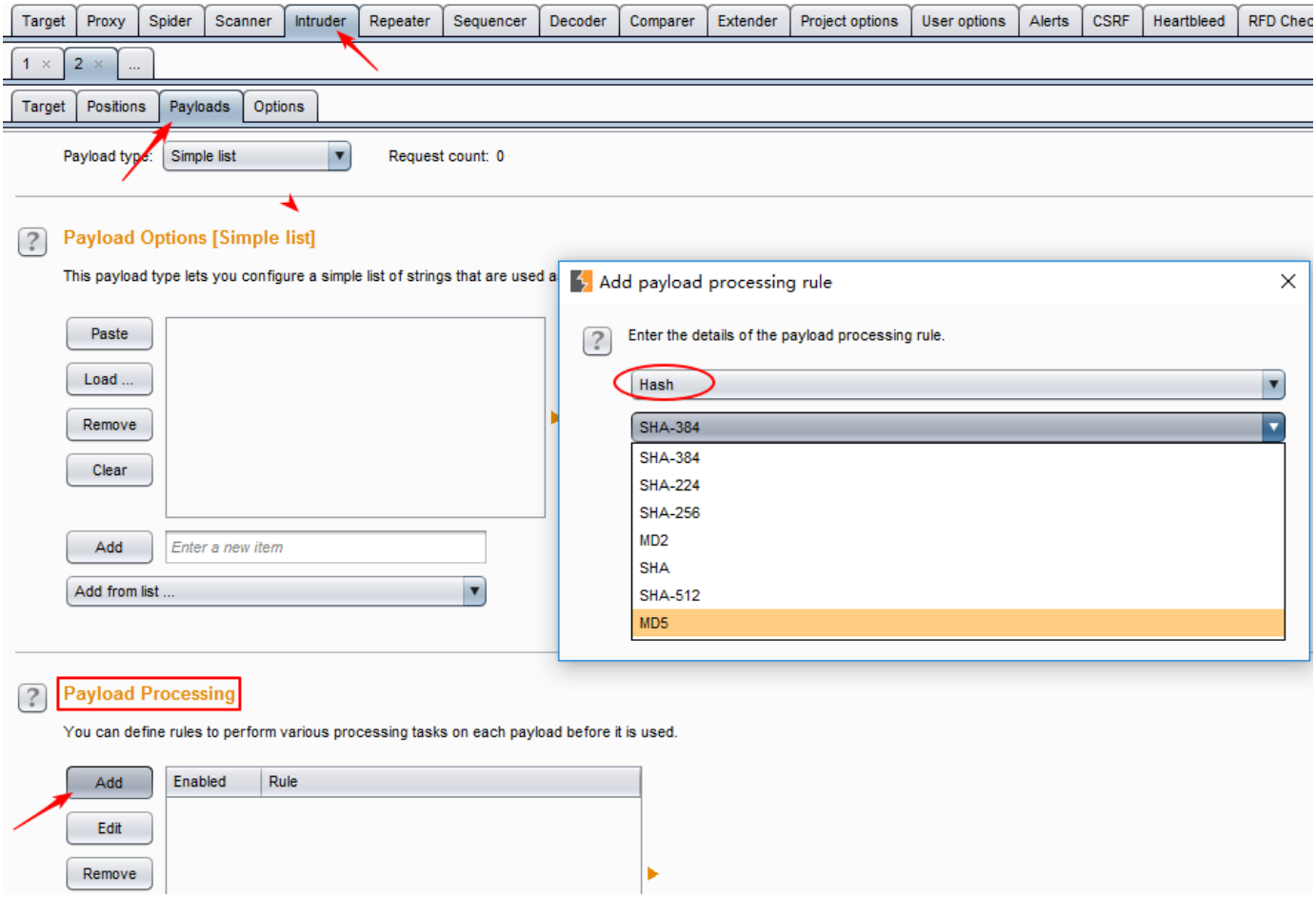
如果封闭系统是个多(几十或几百个)业务员系统，那么此时最好用一个普通用户名字典进行猜解。常见的有姓名拼音字典TOP500、TOP10w等。

同样，如果一个系统对存不存在某用户无任何有用提示，要猜解的用户名又非常多，可以选几个弱口令如"123456"，"abc123"，"1234"，"1111"，"111111"，同时爆破用户名和密码。

0x04：突破加密传输的口令

有些业务系统的口令传输到后端前，为了安全和老板的要求，通常是由前端js进行编码或加密后再传输的。常见的Web系统编码和加密方式有base64编码、md5加密、sha1加密、DES加密、AES加密、RSA加密。这时候，有三种爆破方法。

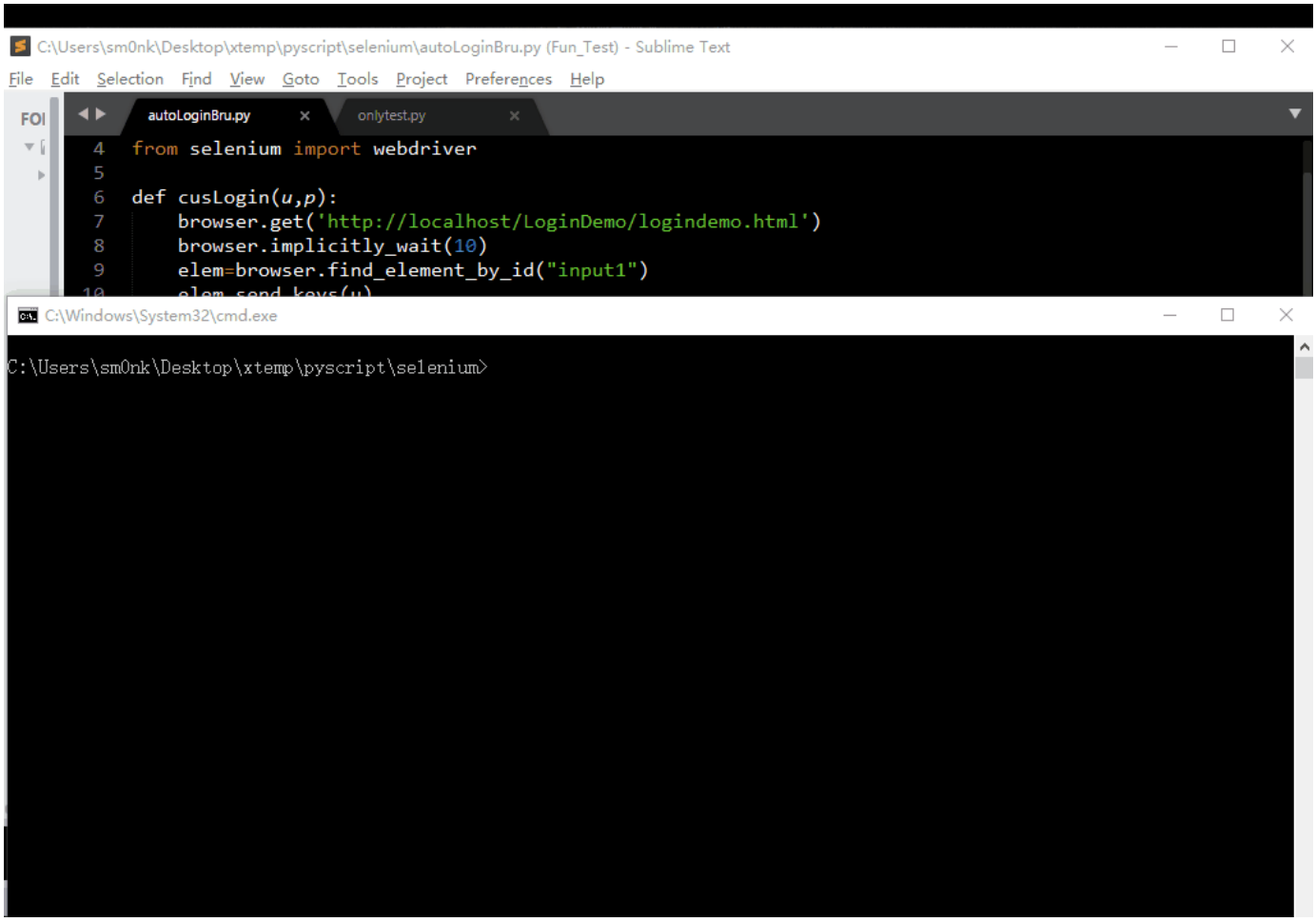
一：用爆破工具在传输前按照标准方法加密好再传输，Burpsuite的Payload Processing可以很好的工作。



二：用工具提前生成好加密好的字典，然后爆破工具直接加载字典即可。在生成加密字典方面，pydictor是不二之选。encode功能内置支持多种加密方法，并且支持自定义加密方法，直接调用js文件中的加密方法进行加密等。另外，还可以用内置工具handler，加密自己现有的字典，让字典适用本次爆破场景。

当然，也可以写轮子直接调用可以解析js语法的组件并执行，例如python的execjs模块、pyv8模块等，原理和pydictor调用js文件中的加密方法相同。

三：对于某些动态加密或难以还原加密算法的场合，可以用selenium+webdriver模拟浏览器操作，自动填写密码提交。具体可参考文章基于SELEINUM的口令爆破应用。



0x05：突破登录IP地址限制

如果对方系统设置了可以登录系统的IP地址白名单，可以尝试用下面的9个HTTP头字段，伪造下IP地址碰碰运气。运气学？天机不可泄漏。

```
Client-Ip: 127.0.0.1
X-Client-IP: 127.0.0.1
X-Real-IP: 127.0.0.1
True-Client-IP: 127.0.0.1
X-Originating-IP: 127.0.0.1
X-Forwarded-For: 127.0.0.1
X-Remote-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1
X-Forwarded-Host: 127.0.0.1
```

0x06：图形验证码绕过

对于上面的几种情况，一旦出现验证码，我们就不能愉快的爆破口令了，那么有什么方法可以绕过验证码进行密码猜解呢？

1. 图形验证码不刷新或无效

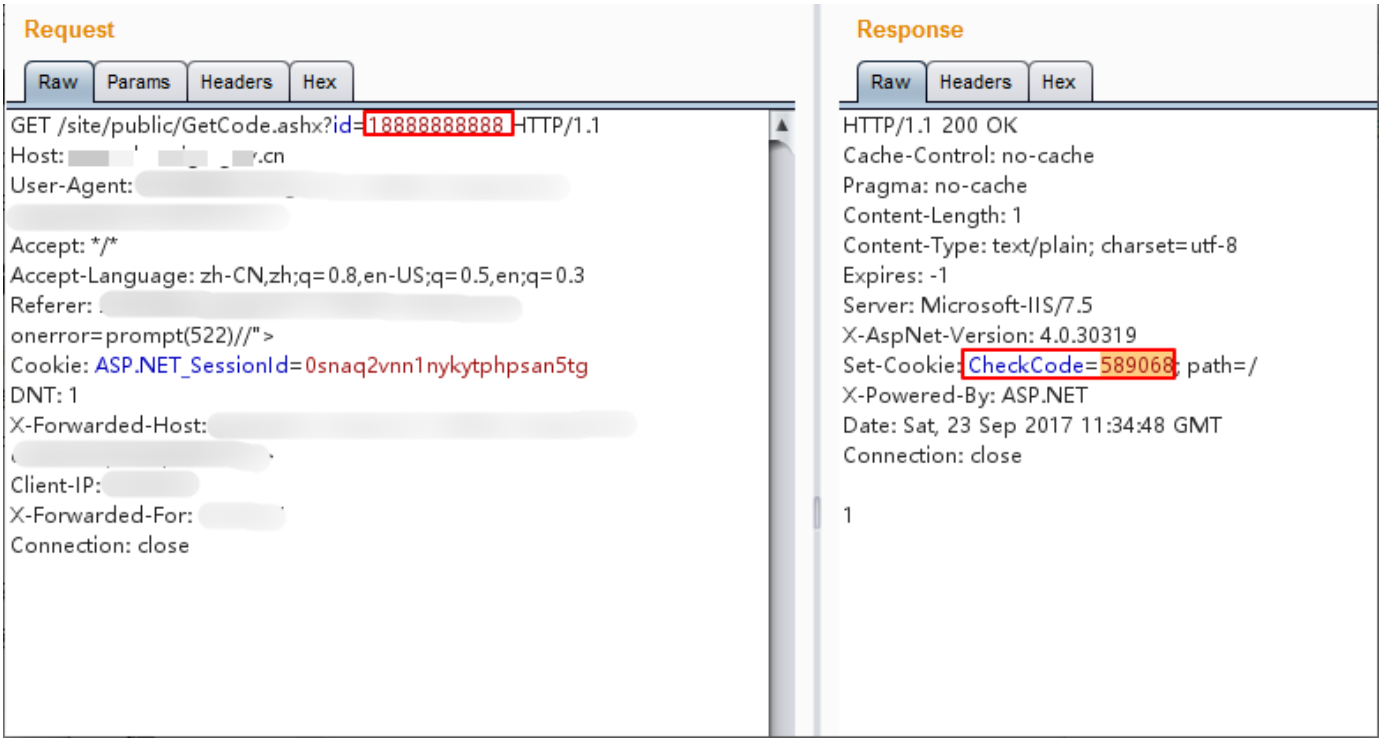
手工尝试一次登录后，在某一时间段内无论登录失败多少次，只要不刷新页面Session不过期，就可以无限次的使用同一个验证码来对一个或多个用户帐号进行暴力猜解;

登录失败之后，系统会打开一个新页面或者弹出一个新的警告窗口，提示用户登录失败，点击确定后返回登录界面且验证码刷新。这种情况下，只要我们不关闭新窗口或弹窗，验证码就不会失效;

还有就是不管输入什么数据，验证码都会判断通过的极少数情况。

2. 图形验证码值可直接获取

验证码通常会被他们隐藏在网站的源码中或者在请求的Cookie中，或在response数据包中返回，可以写脚本正则匹配也可以用Burpsuite的macros功能，来匹配返回数据包中数据。



3. 图形验证码参数绕过

对于请求数据:user=admin&pass=1234&vcode=brln，有两种绕过方法，一是验证码空值绕过，改成user=admin&pass=1234&vcode=；一是直接删除验证码参数，改成user=admin&pass=1234。另外有时修改或删除Cookie中的一些值也可以绕过，导致不需要填写验证码也可以登录。

4. 存在无验证码页面

经过测试，如果我们发现网站验证码自身并不存在缺陷，那我们接下来就可以尝试寻找一些其他的登录页面或接口来尝试暴力破解。如隐藏的页面、测试页面、老旧版本的页面

5. 万能验证码

渗透测试的过程中，有时候会出现这种情况，系统存在一个万能验证码，如000000，只要输入万能验证码，就可以无视验证码进行暴力破解。

6. 验证码数量有限

多见于计算类型的验证码，如1+2=？，这种类型的验证码严格意义上来说不能叫做验证码，多刷新几次验证码，我们可能会发现系统中的算数题目只有那么几道，这种情况下只要将验证码全部下载下来，生成一个md5库，然后将前端生成的验证码与本地文件进行对比即可。

7. 简单验证码识别

在平常的漏洞挖掘过程中，如果我们发现登录的验证码非常简单且易于识别，那我们就可以尝试使用自动化工具来进行登录破解了，如PKAV的HTTP Fuzzer、tesseract-ocr库。

8. 使用高级算法识别验证码

还没有仔细研究过，主要是对特定网站的图形验证码训练识别模型，达到一定的准确率就可以调用进行模拟提交图形验证码的值了。具体可参考以下三篇文章：

使用KNN算法识别验证码

卷积神经网络识别验证码

使用TensorFlow训练验证码

0x07：短信验证码绕过

对于网站要求输入手机号，接收手机短信，校验短信验证码进行登录的系统，正面冲锋的主要思路有：

1. 短信验证码生命期限内可暴力枚举

在验证码还未过期的时间段内，可枚举全部的纯四位数字、六位数字等较简单的短信验证码；

2. 短信验证码在数据包中返回

同图形验证码的2，可以直接获取到短信验证码。

3. 修改请求数据包参数或Cookie值绕过

比如有post数据包：mobile=18888888888&userid=00001,Cookie中有：codetype=1

在特定步骤，修改mobile=自己的手机号，自己手机就可以收到别人的验证码，后面再用别人的手机号和接收到的验证码登录；

修改Cookie中可疑的参数和值，进行绕过，比如上面修改codetype=0；

4. 修改返回包绕过

举个简单的例子：提交错误的短信验证码，返回包中有：status=false，用Burpsuite 的"Do intercept"功能修改为status=true，即可绕过前端判断，成功进入系统。具体还要结合实际的场景，灵活操作。

5. 攻破短信验证码接口

有些网站会遗留短信验证码测试页面，比如/test.html等，如果能找到并且还可以正常使用，系统真是想怎么进就怎么进了;一般系统的短信验证码功能，都会有个接口平台可以获取到手机接收到的所有短信，找到并攻破也能进入系统。

6. 默认万能密码

为了方便测试以及维护，有的系统会留有万能验证码，上线后还保留着。可能是固定的写在配置文件、js文件或代码中，也可能是随时间变化的，遇到是缘，定要珍惜。

0x08：双因子验证绕过

我碰到的双因子验证手段主要有两种：

第一种是输入了正确密码后，系统向绑定的手机号发送一条带有一定随机性的明文短信验证码，通常是6位纯数字，验证通过才能登录系统。大多数的web系统的双因子认证手段属于此类。

第二种是用已经绑定的第三方的软件上的实时动态码作为第二凭证，如Google Authenticator、手机令牌应用等，一般也是6位纯数字，验证通过后才能登录。

对于第一种短信验证码形式的双因子验证方式，完全可以套用0x06中短信验证码绕过里的姿势来绕过测试；第二种比较有难度，但是可以通过寻找第三方的软件漏洞来bypass Web系统的双因子验证。另外，还有三种通用的绕过方法：

```
1. 暴力破解
   如果Web系统实现不当，枚举所有的6位数字，有几率可以成功登录系统
2. 利用密码重置成功后的seesion
   当双因子认证保护的Web系统开放密码重置功能时，可以尝试去重置密码，重置成功后获得的Session一般可以直接登  录系统，
3. 第三方Oauth认证跳过双因子验证
   有许多Web系统可以通过第三方Oauth授权，比如QQ帐号、微博账号授权登录等，获得授权后，就直接跳转回Web系统，自动登录
```

三：总结

封闭的Web系统用登录凭证来保护自己柔弱的躯体，不让陌生人触碰。看似封闭、难以一窥的系统，但其实仔细梳理一遍思路，细心耐心的右击看过每一行网站源码，嗅探每一个参数的意义。你就会有一个强烈的想法：我就是网站管理员，我密码忘了，现在我要用我的方法进入系统！

参考：

登录加密算法破解秘籍

对登录中账号密码进行加密之后再传输的爆破的思路和方式

利用漏洞中验证码绕过的小技巧

破解拦截绕过网站手机短信验证码方式

4-methods-to-bypass-two-factor-authentication

<