28 由“忘记密码”拓展开来 - 揭开安全的神秘面纱

更新时间：2020-07-24 10:52:18

不想当将军的士兵，不是好士兵。——拿破仑

上一次呢，我们跟大家从整体上聊了聊 Web 安全，认识了这门测试技术对于我们的重大意义，也大体上知道了对于 Web 应用来说，都会有哪些漏洞。但是就像老北京天桥上卖艺的常用的口头禅：光说不练假把式。我们一起来拿一些真实的“案例”来看一看最简单的安全漏洞，揭开安全测试的神秘面纱。

我们就用一个非常常见，但是大家又非常容易忽视的点，验证机制下的“忘记密码”来谈起。

当前互联网网站大多提供“忘记密码”功能，但是呢，这里面往往会存在一些典型的安全问题。核心问题就是忘记密码的流程跳过了身份验证。

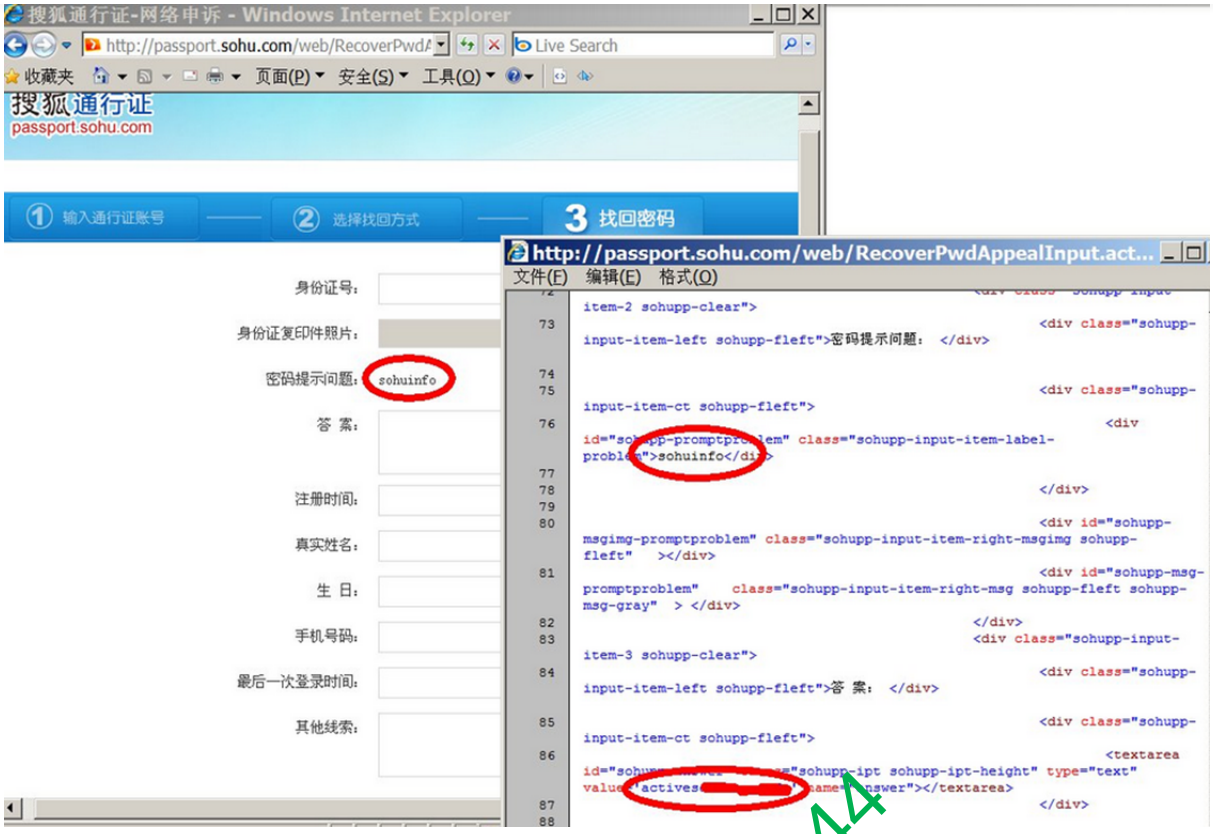
如果不考虑通过客服找回密码的话，通常网站设计有三种方式来认证用户：

2. 用户注册时留下的安全邮箱。
3. 给预留手机号发送验证码短信。

基于这几种，我们来找些例子看看互联网公司都会犯哪些傻。

第一类：记得我们上次说过，安全问题本质上还是信任问题。而有些网站过于“信任”用户，过分鄙视用户智商，以为用户都不抓包都不分析表单参数，想写什么就写什么。

第一个小例子是很多年前搜狐邮箱，现在业务已经下线了 O(∩_∩)O ，在它的登录页中有一个找回密码功能，再点击下面的“网上申诉”，在申诉页面的源代码里，不但有密码提示问题，Hiden 表单里竟然泄露问题答案，可获得任意用户修改密码问题答案，从而轻松修改任意用户邮箱密码。



除了这样的质询问题漏洞，对于忘记密码邮件，也有可能存所漏洞。某网站贴心地实现了“重新发送找回密码邮件”功能，结果一起来看一下。

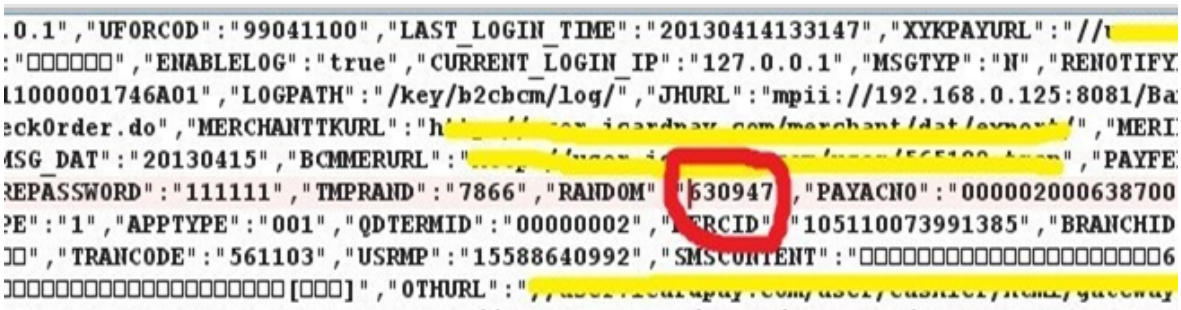
以往进行到这步，我们都会很乖的马上登录邮箱查看密码重置链接，这次在“重发发送”时使用BURP或其他工具把请求拦截下来：

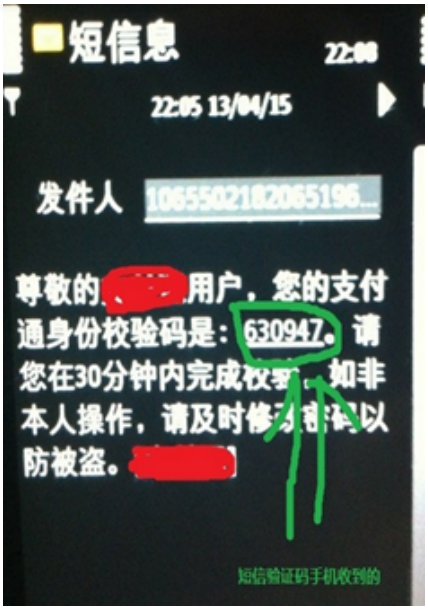
```
GET /retrieve_passwd.php?act=send_mail&email=[redacted]@163.com&uid=1033806458 HTTP/1.1
Host: i.pps.tv
Proxy-Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
DNT: 1
Referer: http://i.pps.tv/passwd_mail_veri.php?email=webid@web02.ppstream.com&uid=1033806458
```

发现传递了email参数，尝试进行篡改，将 email 改成自己的邮箱地址；没想到居然发送成功，登录邮箱，收到了重置其他用户密码的邮件。

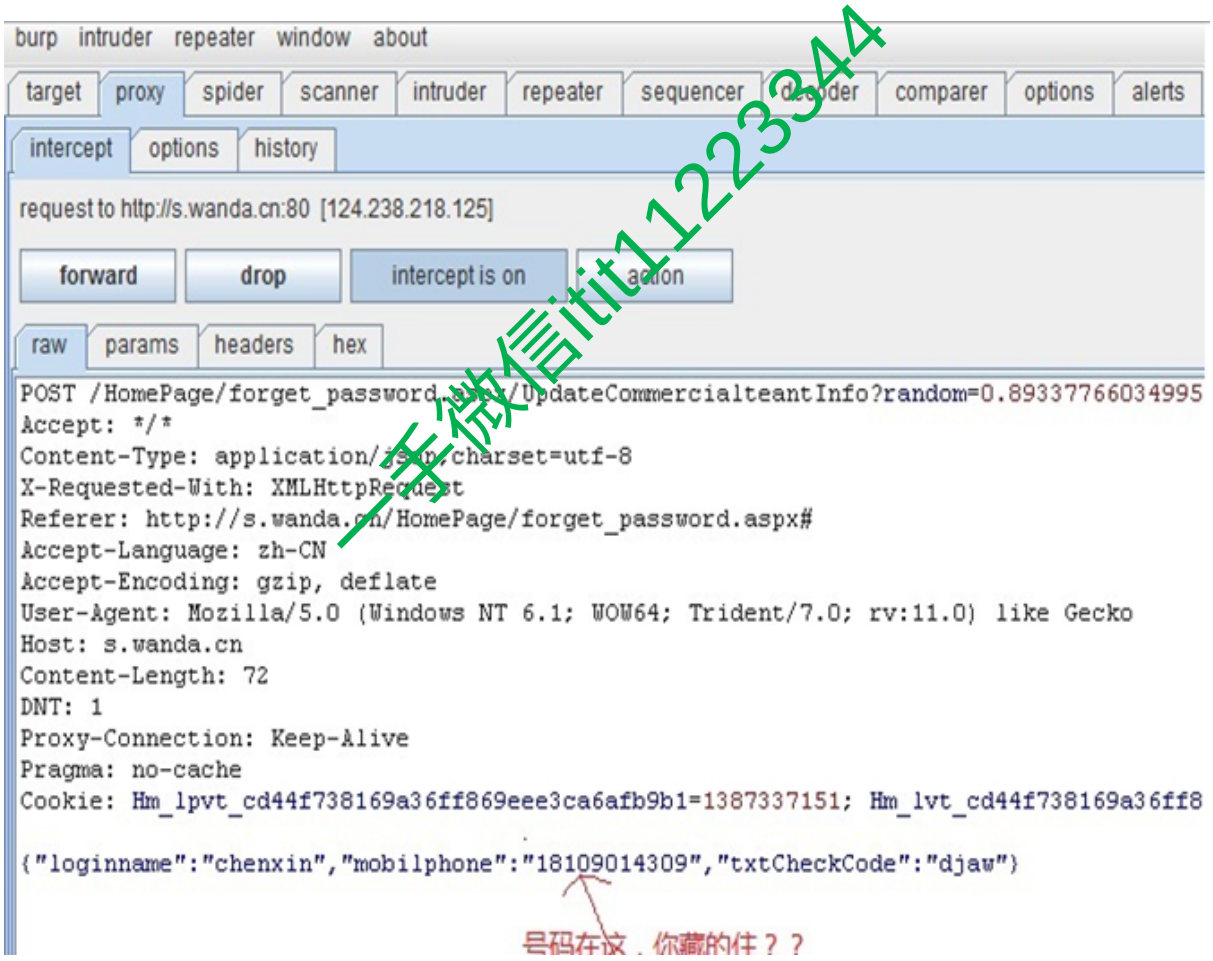
当然，还有我们现在最流行的发送手机短信，也是跑不掉的：

将请求拦截下来，注意观察拦截短信效验码；经过多次试验。发现红色的部分 是拦截到的手机验证码。





除了这样简单就拿到了验证码的，也可以像之前邮箱一样，去修改发送的手机号码，扭转乾坤：



上边的几个小例子是用一些绕过的手段来破坏了验证机制的防守。

我们再来看看另外一种类型： 知道这种明文的不太安全，所以考虑了加密，但是太过依赖 MD5

虽然 MD5 是个非常牛叉的非对称加密算法，只能 Encode 没办法 Decode。但是千万不要忘记了劳动人民的智慧，于是网络上搞出了 MD5 的彩虹表，可以破解很多的 MD5 加密，所以曾经的途牛也中招了。。。

初看这个链接感觉没有太大问题，毕竟还是将关键字符进行了加密，不太容易破解，然而现实总是打脸的：

我们发现居然是 ID 的简单加密，那如果有人想要恶意利用这个漏洞，只需要遍历 id 和 id 对应的 MD5 就可以轻松破译很多的用户了。

这样的例子也不在少数：

除了上面两类，常用的手段还包括：

- **暴力破解**，如手机四位验证码的暴力破解，密码提示问题的相关穷举破解等。
- **组合破解**，包括表单参数分析、MD5 decode、暴破综合运用等。

OK，我们简单总结一下在忘记密码，这样一个很容易被忽视的小功能上可能存在的问题：

1. 需要确认应用程序，中是否有隐含的忘记密码功能，或不通过用户名查询即可访问的情况。
2. 如果恢复机制使用质询方式，则确定用户能否枚举用户名来得到质询信息，与猜测密码相比，响应质询更容易。
3. 如果在忘记密码的请求响应中，生成一封包含恢复 URL 的电子邮件，大量此类 URL 并试图分析和预测其发送 URL 的模式，是否可以得到其他未知用户的恢复 URL。
4. 无论是使用邮件，还是发送手机验证码，查看是否可以拦截请求以修改目标邮箱或手机号，从而达到绕过的目的。

我们通过一些简单的例子，就算一个抛砖引玉的作用吧，当然，前文中这些例子呢，都是现实中已经修复并公布的安全漏洞，今天拿出来仅仅让大家引以为戒，更好的认识安全测试，也让“安全漏洞”与大家不再陌生。我们也能看到，即便是很小的一个点，也可能有如此的安全威胁，足以见得安全测试的重要性了。

对于安全测试，可能要完整的说下去还有很多，如果想要真的搞清楚安全测试，首先第一步要了

多只是发现问题、定位问题，而在安全测试里，我们还要掌握安全漏洞的防范措施，真正做到“教开发人员写代码”，毕竟，目前很多的开发还不太注重代码的安全性。

← 27 世界那么大，我想去看看 - Web安全简介

29 到底什么才算测试开发? →

精选留言 0

欢迎在这里发表留言，作者筛选后可公开显示

目前暂无任何讨论

千学不如一看，千看不如一练