WEB安全：聊聊“密码找回”

WEB安全用户密码找回多案例安全攻防实战

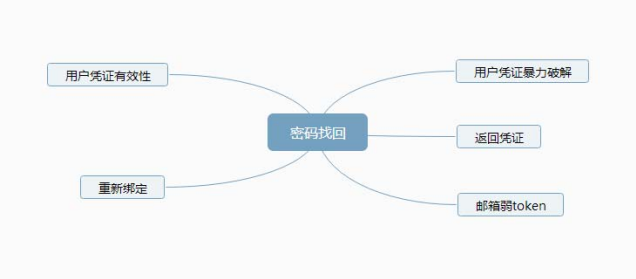
这次文章以wooyun的密码找回代表性漏洞作为案例来讲解,漏洞的描述会通过提交漏洞的原描述加上我的理解——列出，通过密码找回的过程描述，得出从漏洞的发现到漏洞的分析。

密码找回逻辑测试一般流程，首先尝试正常密码找回流程，选择不同找回方式，记录所有数据包，分析数据包，找到敏感部分，分析后台找回机制所采用的验证手段，修改数据包验证推测

内容主要是逻辑漏洞，技术性质的内容并不多，以发散思维为目标;所以web开发和安全同学都可以来看看

分享内容目录

1. 用户凭证暴力破解
2. 返回凭证
3. 邮箱弱token
4. 用户凭证有效性
5. 重新绑定



一、用户凭证暴力破解

四位或者六位的纯数字例子。

微信任意用户密码修改漏洞

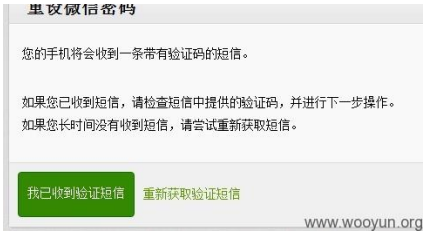
漏洞描述

在微信官方的首页上发现了找回密码功能。

点击链接之后看到这个功能.来了兴趣。

在这个页面输入一个已经注册了微信的手机号。

看到了下面的提示信息



点击“我已收到验证码”按钮，就跳转到一个修改密码的页面,如下

在这一步抓包,得到如下包文

code 区 域

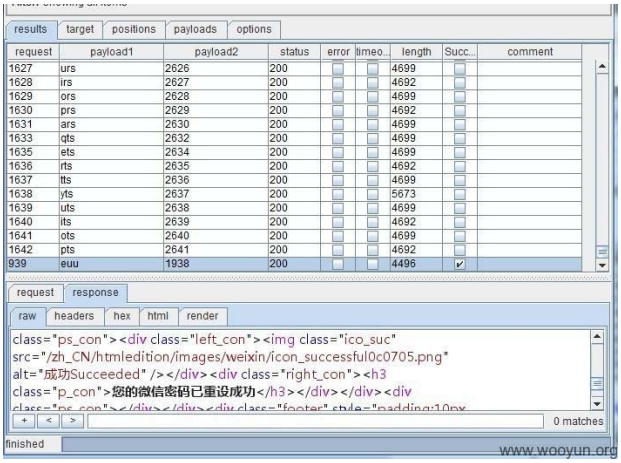
```
check=false&phone=18666666666&t=w_password_phone&isemail=0&value=18666666666&method=reset&country=A86&getmethod=web&password=zzzzzz&password2=zzzzzz&verifycode=1234
```

将包文中的verifycode进行重复提交后，发现会提示下图的信息

```
<!--method:reset<br/>retcode:7<br/>--><div class="ps_con"><d
<h3 class="p_con">您的提交请求过于频繁，请稍后再试</h3></div>
```

这样的话.就要想办法去突破.

经过多次尝试后，发现如果在phone=18666666666的号码后面，添加不为数字的字符时,可以绕过这个重复提交的限制.于是我推理出了一个验证逻辑。
如果phone=18666666666的尝试次数大于阀值,则提示请求过于频繁
但在这一步之前没有对phone进行提纯.所以可以将特殊字符带入
但在下一步的时候进行了提纯.只取了phone中的数字部分.
然后在取出此号码的verifycode进行比对.
比对成功则修改密码



修改密码成功.
这个地方的薄弱环节在于微信重置密码的验证码为4-5位纯数字.
且数字范围在1000-20000之间
也就是说.我只要尝试19000次.我用50个线程发包.3分钟即可成功修改一个密码.

原因：

虽然设置了请求阀值，但被猜解除了验证方式，并且找到了绕过方式，验证码为4-5位的数字容易爆破

三、返回乱码

一、逻辑漏洞

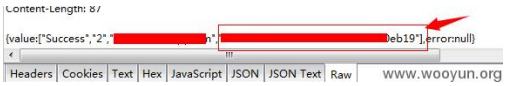
天天网任意账户密码重置（二）

描述

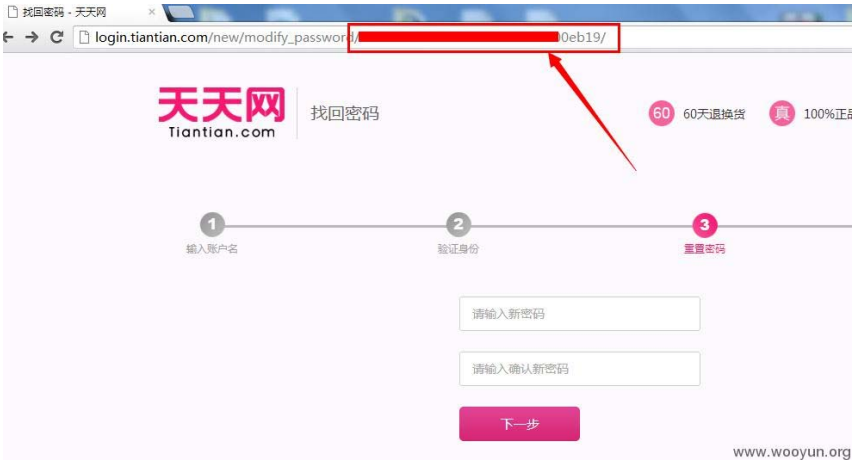
之前看到天天网有爆出漏洞的案例，这次我看看还有没有，果然发现了一枚。

和之前的漏洞一样,打开了找回密码页面，按照了正常流程来找回密码，填好邮箱和验证码，点击下一步，然后抓包。

在抓取到的数据包中发现，返回数据中会返回一个加密字符串，这让我有点好奇心起来了,我把它记录下来。



还是按照了正常流程，打开了我的邮箱，看到了一封找回密码的邮件，我点击了里面的链接地址，进入如下的设置新密码的页面。



这个时候，我把之前记录到的可疑字符串和URL做了一下对比，发现之前的字符串就是当前页面URL最后的部分，竟然是同一个！那我推测，天天网的这个找回密码设计是有问题的，那个邮箱验证码就可以直接绕过了。

设置新密码的的URL为 http://login.tiantian.com/new/modify_password/加密字符串/

为了要验证我的猜测，我在这里用天天网客服 service@tiantian.com 做了一次测试。还是用上面的正常找回密码流程，然后抓包获取到加密字符串，然后组合到上面的设置新密码的url中，就成功重置了这个客服账号的密码了。给大家截个图看看。

原因

找回密码问题的答案在页面源码中可以看到。

三、邮箱弱token

奇虎360任意用户密码修改漏洞

描述

360是一个大厂，又是做安全业务的，很好奇它的网站安全性怎么样？

好奇的我做了一个测试，我首先按照正常流程走一次找回密码，打开邮箱，查看给我来的邮件内容：

> 360个人中心找回密码（重要）！
>
> 重设密码地址：
> http://i.360.cn/findpwd/setpwdfromemail?vc=c4ce4dd3d566ef83f9xxxxxx&u=xxxx@gmail.com,
> 马上重设密码！
> 如果您没有进行过找回密码的操作，请不要点击上述链接，并删除此邮件。

参数vc可以看出是一串32位字符的md5，通过cmd5.com网站解密后发现是个数字，类似1339744000，第一反应猜测是个用户id。我脑袋里马上出来了一个思路，遍历id并且修改u变量是不是可以修改任意用户密码呢？试了一下不可以。 再仔细看了看这个数字，感觉比一般的用户ID大，反复看了几次，突然发现怎么像是个时间戳？

通过时间戳格式化发现，还真是一个时间戳！ 再次大胆的猜测了一下这里的流程，用户取回密码时，会产生一个精确的时间戳，和帐号绑定，记录在某个密码重置库内。

修改这个用户密码必须要知道绑定的时间戳才可以，从表面的逻辑来看，好像没问题。不过开发同学忽略了一个细节，什么细节呢？如果这个时间戳是新生成的，我在一定得时间段内进行暴力猜解，很快就可以获取到这个有效得链接。
写了个利用工具测试一下。

打开之后果然验证了我的猜测。

修改密码成功后，后跳到了登陆页面，用刚刚修改得密码登陆后看到了个人资料页面。

原因

使用了特定值的加密作为token，被猜解到使用了时间戳的MD5值。在实际过程中我们也可以尝试用户名，手机，邮箱，等等的不同加密方式。

四、用户凭证有效性

短信验证码例子。

OPPO手机重置任意账户密码（3）

描述

oppo在wooyun上暴露了好几次，这次我也来试试。

先逛逛网站，发现主站的帐号跟nearme开发者社区的帐号是通用的，所以如果只要重置了nearme社区帐号主站帐号也被修改。问题出现在www.nearme.com.cn

依然按照正常找回密码流程来，首先我用自己的手机号186****8188找回密码，点击获取一下验证码，于是这时我手机收到了一个4位的数字验证码。

然后到这步暂停，我不去使用验证码重置。

接下来我要做安全测试了，用18688888888这个帐号进行测试。

我们点击登录处的忘记密码,输入要找回的帐号18688888888。

选择通过手机号码找回密码。

关键的地方在3.身份认证这一步，我把18688888888替换成我自己的手机号186****8188
输入刚才自己手机获取到的验证码：0198，直接确认下一步。

提交成功，输入新密码:oppoceshi1。

确认一下，重置成功。

那么我们接下来就是要用18688888888：oppoceshi1。

登录一下，测试是否成功以我自己的手机号跟验证码修改了此账户的密码。

登陆成功

也就是说我已经成功用自己的手机号186****8188重置了18688888888的账户密码。

原因

只验证了验证码的有效性，却没有对验证码和手机号码做绑定验证。

五、重新绑定

手机绑定例子。

网易邮箱可直接修改其他用户密码

描述

这次我们看一个126邮箱的找回密码漏洞，这个还真和上面的方式有点不一样。

我先来注册一个126邮箱测试帐号。

点击“立即注册”，后会跳转到一个手机绑定得安全提示页面来。

注意看下这个链接的参数，有个uid，把uid修改成想要黑掉的网易邮箱帐户的uid。

填入一个自己的手机号码，再把验证码发回来。

那我们点击确定并进入邮箱，这个时候这个目标网易邮箱已经被越权绑定了密保手机。

现在我们要改密码就比较简单了，走正常的密码取回流程，发现这个邮箱多了一个通过手机的取回方式，这个手机尾号就是我刚刚绑定的手机！

網易通行证 易证在手 网易任君游

密码重置成功！！

存在权限判断不当，越权操作的接口是：

http://security.mail.126.com/mobileserv/mbp.do?uid=xxxx&backurl=http://xxx.xx.xx/x

原因：

注册过程的绑定手机页面用过参数修改，将任意账号绑定至可控手机，再来通过密码找回流程找回

最后

通过这篇文章相信你对于密码找回已经有一定的了解,我们发现上面的密码找回思路基本都是通过逻辑推理加技术验证来实现。这种类似的方法还有很多，希望这篇文章对大家的思维能有一点点帮助。