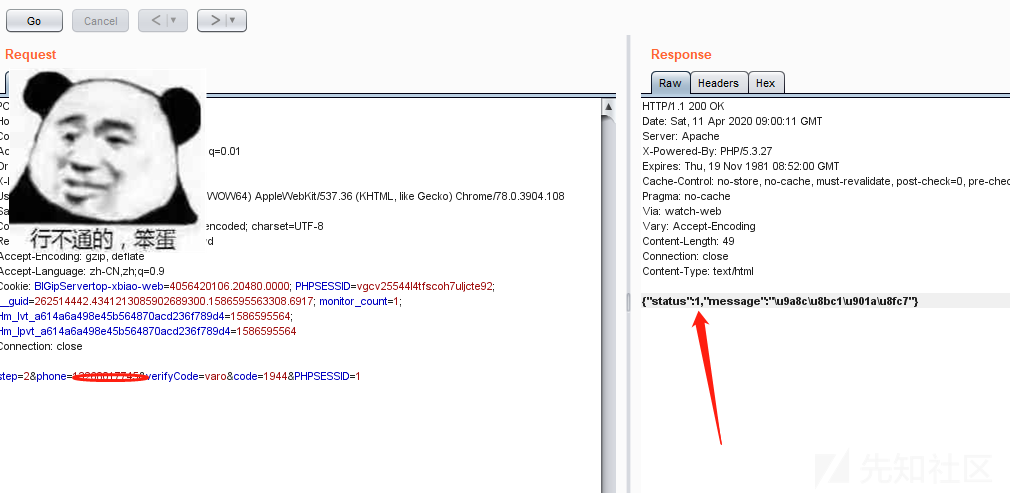
一篇文章教你如何找出找回密码漏洞。（新手推荐）

简介。  
.在测逻辑漏洞的时候，我们经常会测量找回密码处，这时，请容小弟给各位表哥谈及，四种绕过逻辑去修改其他人的密码。

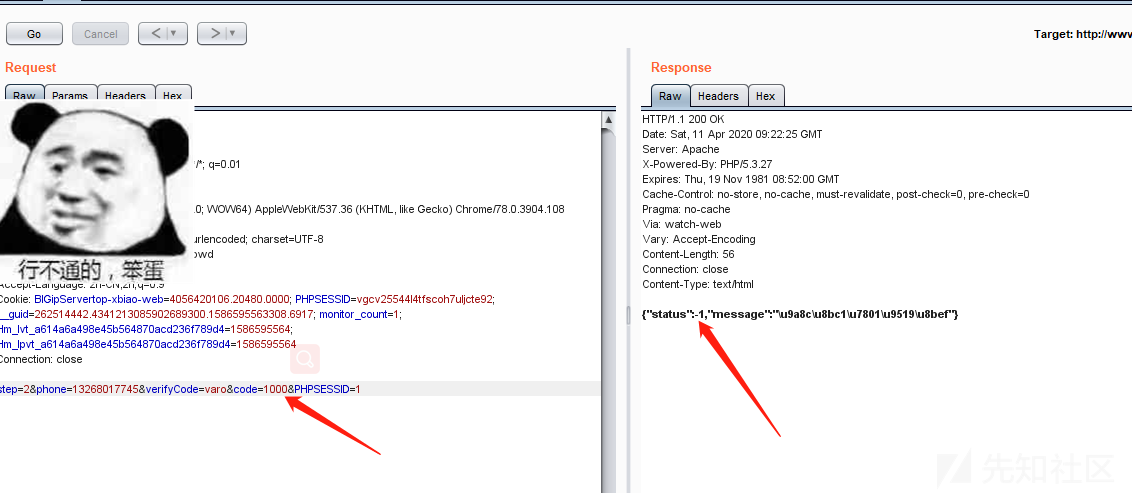
第一种，修改标志位返回标志位进行找回任意用户的密码。  
1.在一些网站上我们注册一个账号，然后我们点击找回密码这个功能。  
2.然后输入一个真实的验证码进行找回密码。再点击下一步的时候打开拦截包的功能。并点击下一步后把数据包发送到repeater 这个功能上，

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411170922-2212f328-7bd4-1.png)

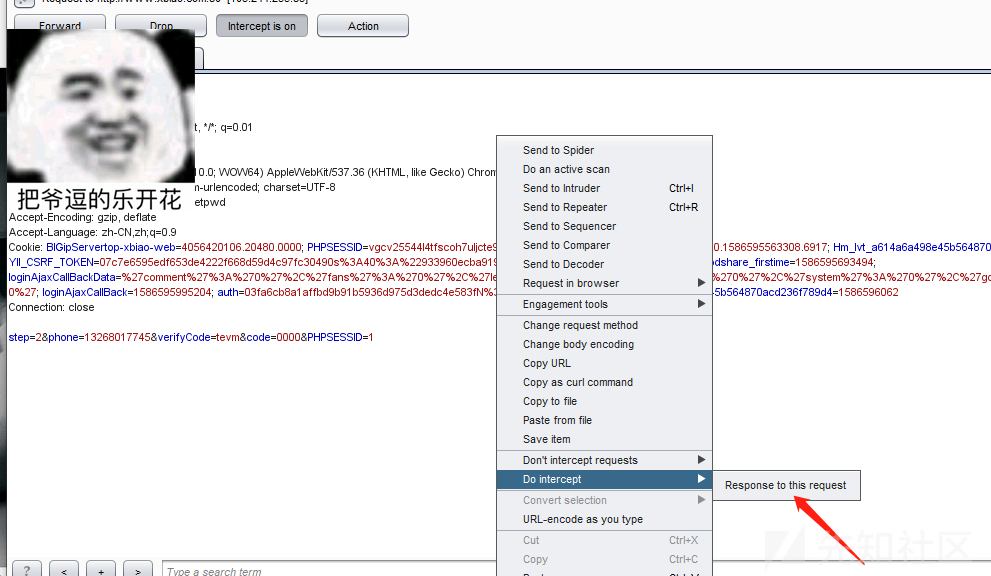
3.然后我们看我我们发包后返回的一个显示情况。这时候我们能看到我们发送正确，可以看到返回包的status（状态）的参数，为1，

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411171316-add64752-7bd4-1.png)

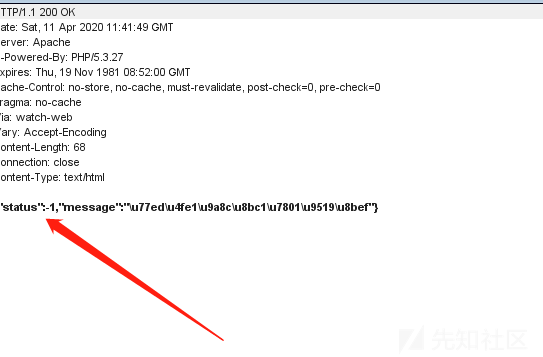
4.然后我们再修改验证码后再发送一次，这时我们可以看到我们的返回包的status（状态）的参数，为-1，所以我们考虑status是不是一个能不能过的标志位。

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411172354-2a2301fa-7bd6-1.png)

5.所以我们随便选择一个输入一个验证码，并点击下一步。然后拦截数据包  
[](https://xzfile.aliyuncs.com/media/upload/picture/20200411193340-4a8be4e0-7be8-1.png)

6.打开查看返回包的功能，然后放包  
[](https://xzfile.aliyuncs.com/media/upload/picture/20200411193634-b285f84c-7be8-1.png)

7.然后把返回包的 status 参数从 -1 改为 1.然后放包

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411194210-7aadde84-7be9-1.png)

8.这时候我们看到我们虽然没输入一个正确的验证码，但还是跳转到找回密码页面。

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411194036-42f929da-7be9-1.png)

1. 总结  
   漏洞形成原因在于，跳转页面的标志位放在前端，使用户可以轻易的修改。

第二种，修改发送验证码的手机号来修改漏洞。  
复现这个漏洞需要两个手机号，一个用来注册用户

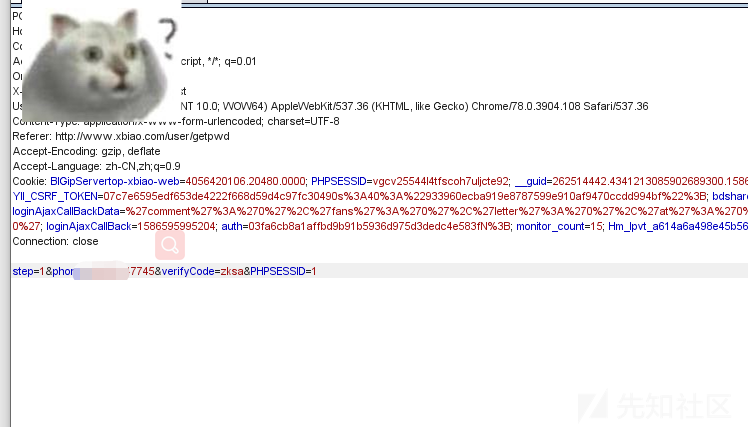
1.我们在获取短信

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411201638-4b51c3f8-7bee-1.png)

2.这时我们看到我们的短信号码为的后四位为2554，

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411202021-d01fa7d0-7bee-1.png)

3.这时候我们只需要将我们的短信号码修改为其他手机号，这时候我们就把验证码发送到其他手机上，从而达到修改任意手机号码的用户密码的效果了。

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411202237-219f48d6-7bef-1.png)

4.总结  
漏洞原因在于后台只验证了验证码，而未对手机号进行验证，从而导致了此漏洞。

第三钟 删除验证码（干货来着）

1.我们登陆莫网站后台，这个是一个莫cms的一个后台，有就是你找到这个网站的漏洞后，你就能找到很多网站的漏洞。

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411202903-07b45d3e-7bf0-1.png)

2.然后一般网站的用户名都会有一个管理员用户 ，所以我们可以尝试 admin

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411203129-5e4f9cbc-7bf0-1.png)

3.结果显示不存在

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411203147-69734b3e-7bf0-1.png)

4.这时候就要考验你们对管理员的了解怎么样了。一般这时候我会把网站的名字放进去试试看

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411203324-a2bb6a7a-7bf0-1.png)

5.没想到真的有，有趣

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411203348-b11464dc-7bf0-1.png)

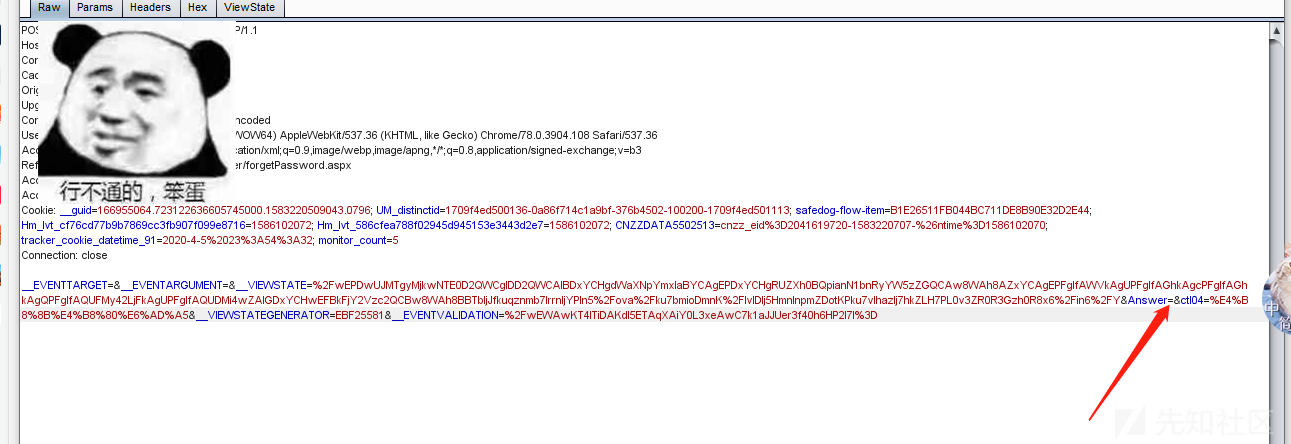
6.这时候我们可以随便输入一个值，然后打开拦截包功能，，然后点击下一步

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411203507-e01cdb88-7bf0-1.png)

7.然后我们肯定数据包中有我们输入的答案 love

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411203607-045d7d72-7bf1-1.png)

8.这时候我们只需要把love这个参数删除掉就放包。

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411203723-31979eda-7bf1-1.png)  
9.这时候，神奇的事情发生了。我们居然成功的找到了密码

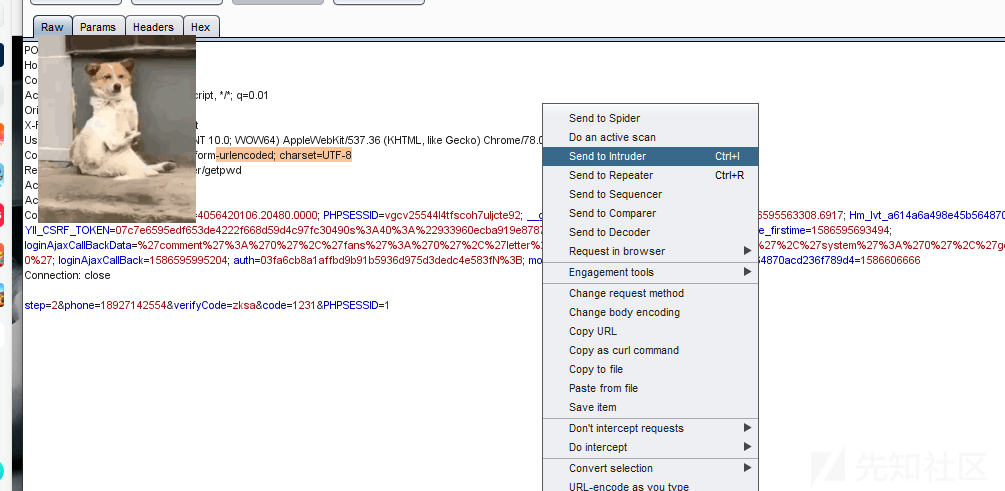
[](https://xzfile.aliyuncs.com/media/upload/picture/20200411203800-4777b316-7bf1-1.png)

1. 总结  
   ；漏洞形成的原因是他的数据传输可能类似于 sql = $admin&$password .  
   然后当 passwrod为空而admin=用户名称时。他就不会验证passwrod ，而是从数据库中直接把这个用户的账号密码给你找出来

第四种，验证码爆破。

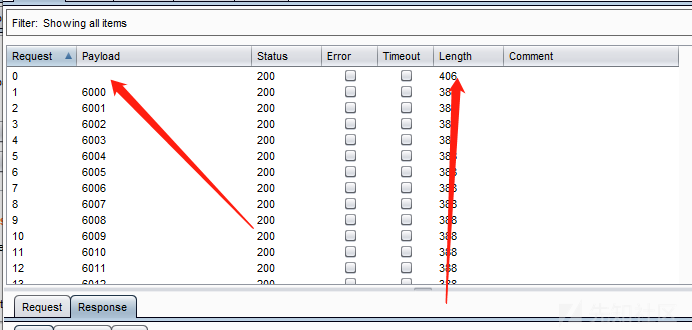
这个爆破只存在于四位验证码爆破才有危害.  
1.第一步打开一个商场网站，并在上面注册一个用户 。（然后在注册的时候我们知道验证码为四位）  
2。点击找回密码的功能点输入我们的账号并获取验证码

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411195037-a9176aa0-7bea-1.png)

3.然后我们点击一个验证码进行随机爆破。，发送到定时器进行爆破，  
[](https://xzfile.aliyuncs.com/media/upload/picture/20200411200607-d3860ab0-7bec-1.png)

4.不一会，就能看到我们香飘飘的验证码了。具体爆破方法请百度，这里不演示。

5.这时候我们找到一个返回的数据大小不同的包即可。

[](https://xzfile.aliyuncs.com/media/upload/picture/20200411201302-cab7fa32-7bed-1.png)

6.总结  
形成原因分别为对验证码的输入次数没有经过严格的样子。