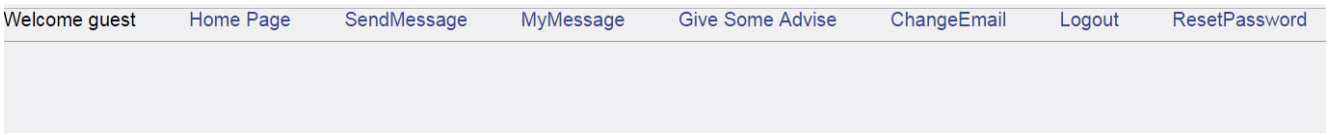
Web1:套路，不要乱打，我不叫 admin

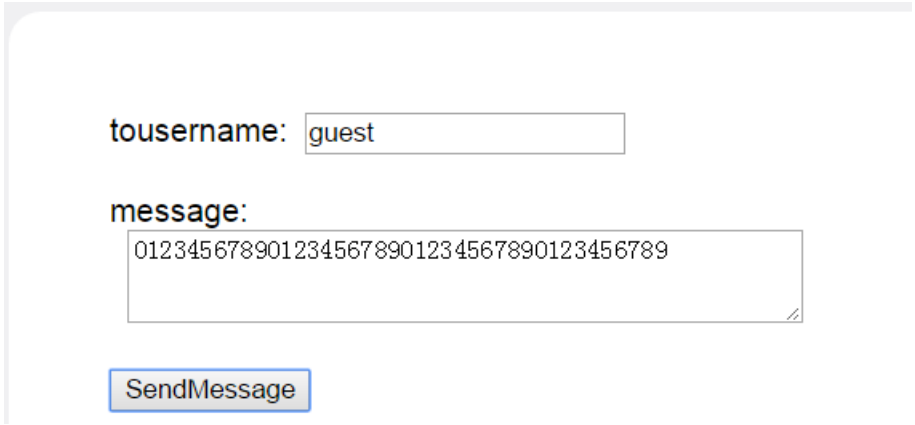
Flag: BlueCTF{This_Is_Quite_Similar_To_ROP_And_You_Make_It!}

根据题目可能需要先得到具有管理员权限的用户的名字。登录进去后，发现 http://127.0.0.1:8080/yuesai/2017-03/check.php?callback=ss&_=1489747277826
是一个可以获取用户名的 jsonp。
通过导航条可以知道



SendMessage 是给其他用户发送消息
MyMessage 是显示别的用户发过来的消息
Give Some Advise 是给管理员发送消息
ChangeEmail 是修改登录邮箱
Logout 是注销登录
ResetPassword 是重置密码

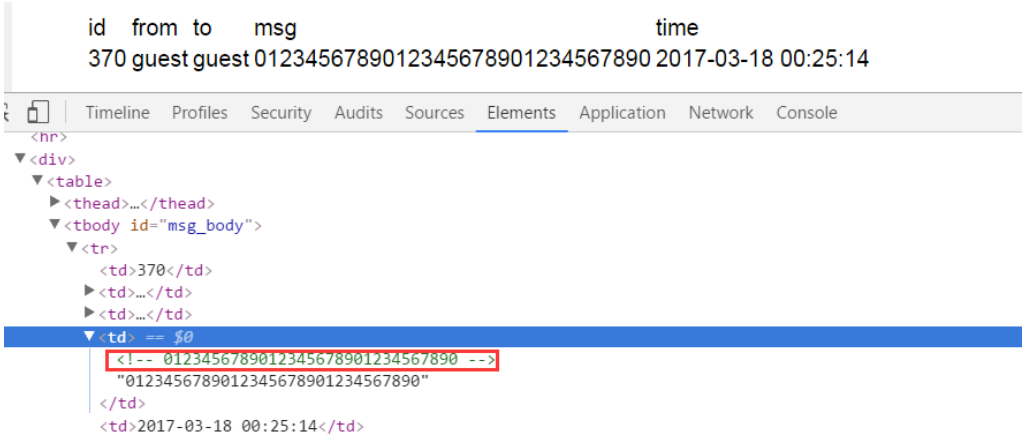
所以，套路应该是先给自己发消息，构造 xss，发送给管理员，获取管理员的名字，并且修改登录邮箱，重置管理员密码，从修改后的登录邮箱拿到修改密码的链接，登录管理员账号拿 flag。



可以看收到的消息，对字符长度做了限制为 31 个字符。

id	from	to	msg	time
370	guest	guest	0123456789012345678901234567890	2017-03-18 00:25:14

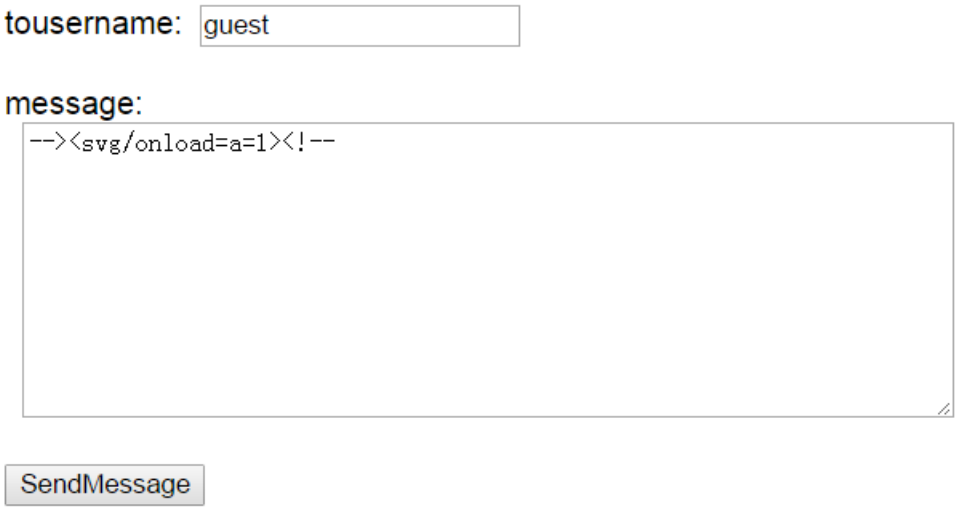
尝试构造 xss 语句，虽然都被过滤了。但是输出页出现在了 html 注释里



这里有两个问题需要解决：

1. **xss**
2. **绕过长度限制**

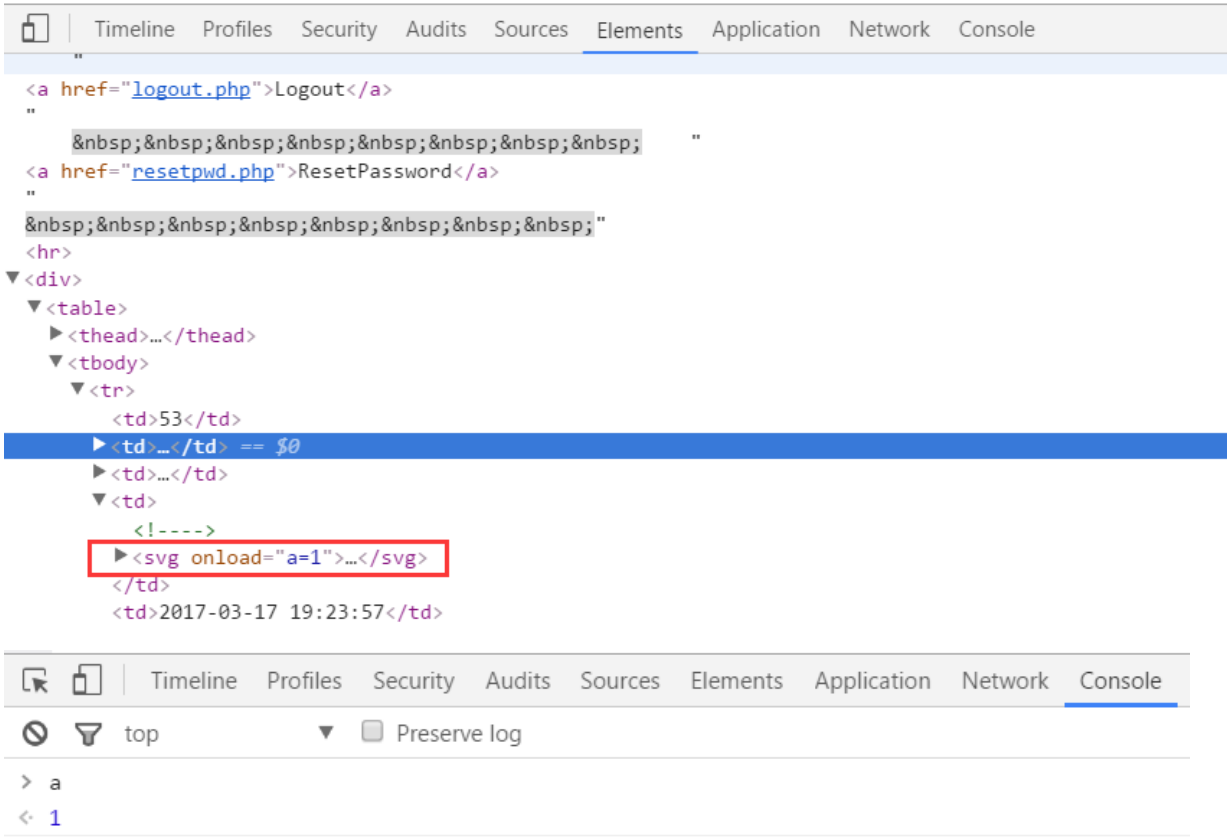
比较容易想到通过闭合注释来 xss。例如：



发送上述代码给自己后，可以看到 js 代码已经执行了。

id from to msg time

53 guest guest 2017-03-17 19:23:57



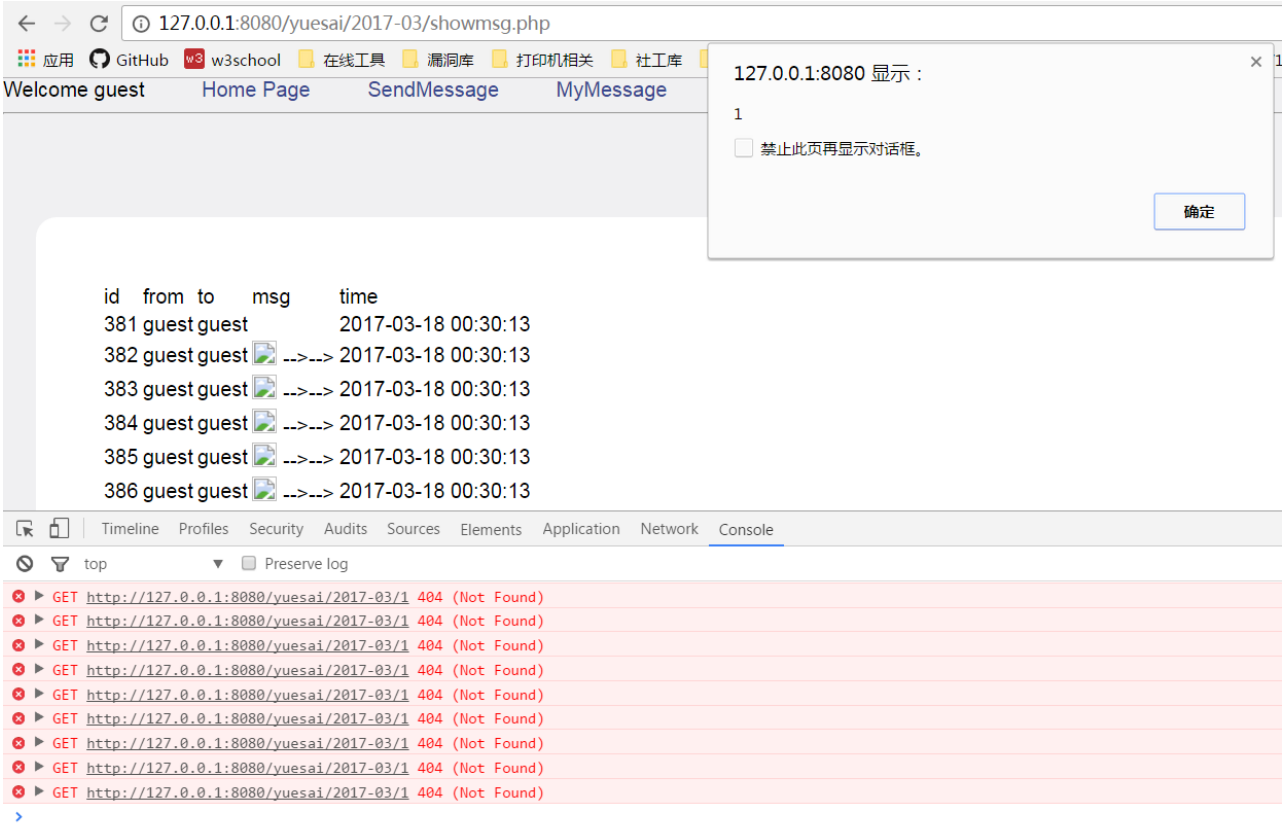
Xss 就到此为止了。如何绕过长度限制呢？

其实这里可以发送很多个消息，批量显示的时候可以一起起作用。于是构造一个 payload 依次发送组合执行。

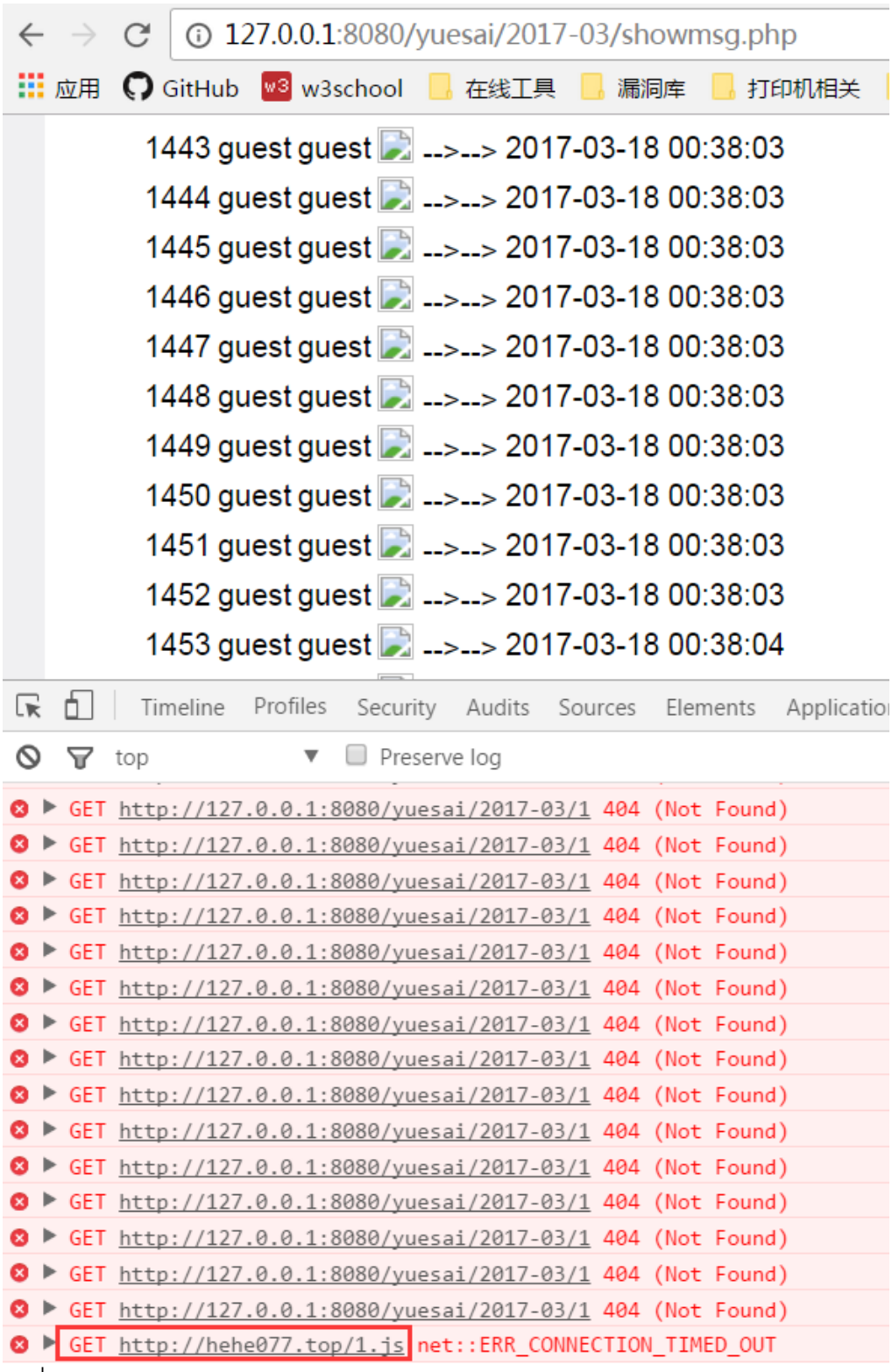
比如依次发送：

```
1 -->&lt;img/src=1 onerror=a='a'>
2 -->&lt;img/src=1 onerror=a+='l'>
3 -->&lt;img/src=1 onerror=a+='e'>
4 -->&lt;img/src=1 onerror=a+='r'>
5 -->&lt;img/src=1 onerror=a+='t'>
6 -->&lt;img/src=1 onerror=a+='('>
7 -->&lt;img/src=1 onerror=a+='1'>
8 -->&lt;img/src=1 onerror=a+=')'>
9 -->&lt;img/src=1 onerror=eval(a)>
```

会成功的弹框。



通过引入外部 js 文件，执行任意 js 代码。



最后成功向远程服务器发起加载 js 的请求。我们只需要在 js 里面获取管理员权限的用户的用户名即可。

同时我们可以利用这个 xss 修改管理员的邮箱，接收重置密码的链接。

在重置完密码后，会跳转到 index.php，跳转的时候会带上 flag。