fakebook writeup sql注入思路

原创

Garybr0 于 2021-01-20 18:37:40 发布 136 收藏 1

分类专栏： CTF writeup SQL注入 文章标签： sql注入 网鼎杯2018

本文链接：https://blog.csdn.net/weixin_45253216/article/details/112901176

2021.1.20

网鼎杯的一道题。

习惯性拿到题目先扫目录

```
zhangyu@kali:~/dirsearch$ sudo python3 dirsearch.py -u http://220.249.52.134:32448/ -e php
[sudo] zhangyu 的密码 :

                               v0.4.1

Extensions: php | HTTP method: GET | Threads: 30 | Wordlist size: 8853

Error Log: /home/zhangyu/dirsearch/logs/errors-21-01-20_17-16-51.log

Target: http://220.249.52.134:32448/

Output File: /home/zhangyu/dirsearch/reports/220.249.52.134/_21-01-20_17-16-51.txt

[17:16:51] Starting:
[17:16:53] 200 -    1KB - /php
[17:17:10] 200 -    1KB - /adminphp
[17:17:21] 301 -  185B  - /css  →  http://220.249.52.134/css/
[17:17:21] 200 -    0B  - /db.php
[17:17:23] 200 -    0B  - /error.php
[17:17:27] 200 -    1KB - /index.php
[17:17:29] 301 -  185B  - /js  →  http://220.249.52.134/js/
[17:17:29] 403 -  571B  - /js/
[17:17:31] 200 -    1KB - /login.php
[17:17:34] 200 -    1KB - /myadminphp
[17:17:39] 200 -   37B  - /robots.txt
[17:17:45] 200 -    0B  - /user.php
[17:17:46] 200 - 1019B  - /view.php

Task Completed                                  https://blog.csdn.net/weixin_45253216
```

发现了robots.txt。

看到了/user.php.bak这个，应该是源码泄漏。
bak文件可以下载到本地，bak是back-up 备份文件，需要改为对应文件名才能打开，这里就把user.php.bak，改为user.php即可。

```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();

        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        $output = curl_exec($ch);
        $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
        if($httpCode == 404) {
            return 404;
        }
        curl_close($ch);

        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
);
    }

}
```

最主要的部分就是中间的function get（），但是我一开始看不懂。。

```php
function get($url)
{
    $ch = curl_init();//初始化一个cURL会话

    curl_setopt($ch, CURLOPT_URL, $url);//设置需要抓取的URl
    //设置cURL 参数，要求结果保存到字符串中或者输出到屏幕上
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    $output = curl_exec($ch); //运行cURL，请求网页
    $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
    if($httpCode == 404) {
        return 404;
    }
    //关闭一个curl会话，唯一的参数是curl_init()函数返回的句柄
    curl_close($ch);

    return $output;
}
```

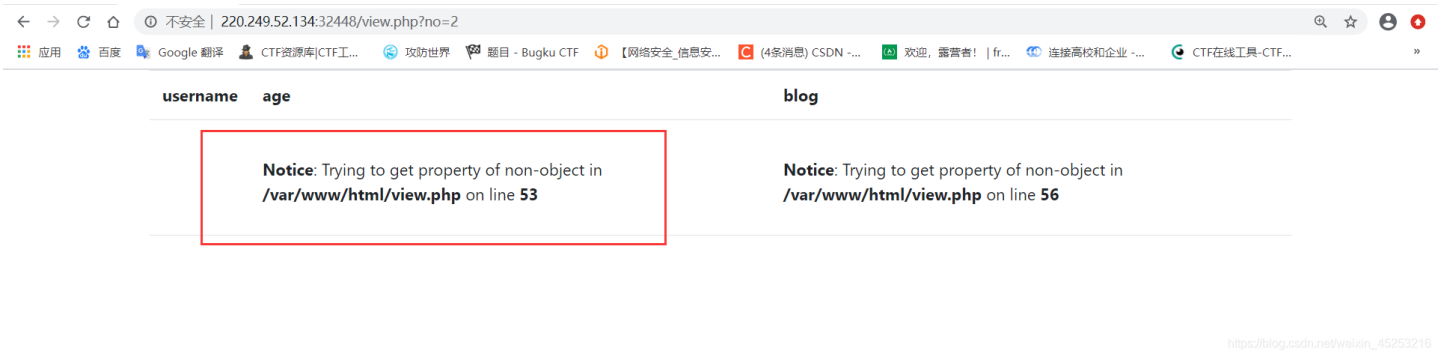

~~通过代码审计发现存在SSRF漏洞，别问我怎么知道的，知不道【狗头】~~
马上就会提到SSRF的正规解法，先记一下sql注入怎么搞。

WP

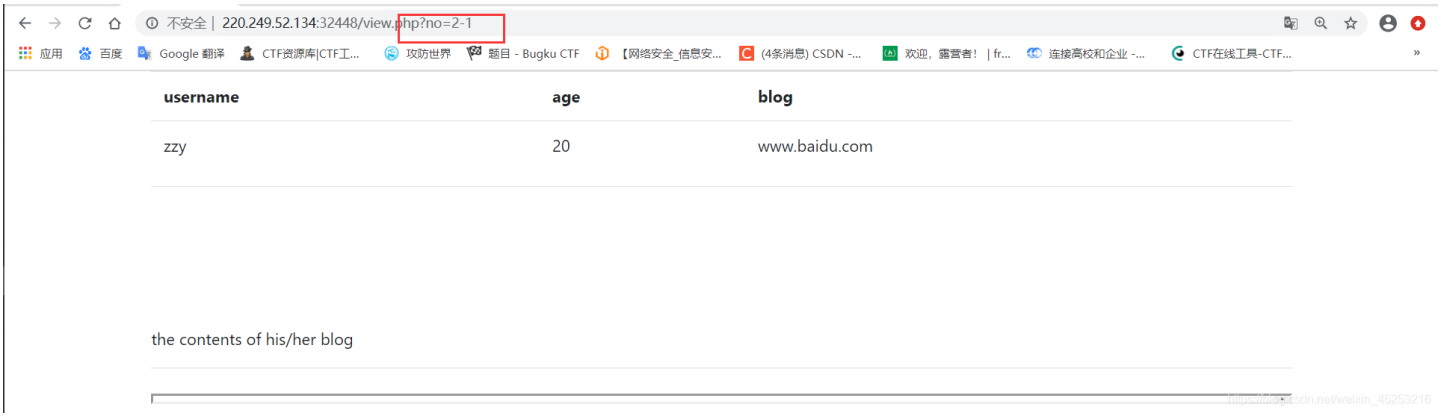
以下是本题的sql注入解法：
按格式先注册一波，然后显示以下页面：

发现只有用户名，也就是上图中的红字zzy能点击

进来之后，就是熟悉的页面了，熟悉的注入点？no=1
先简单测一波



等于2之后爆错，意思应该是只有一个用户信息，没有第二个，所以没找到。



发现2-1可以，应该是数字型注入，并且`?no=1 and 1=1`与`?no=1 and 1=2`会返回不同页面，确定存在注入无疑了，现在测试一下有几个字段。

这里 order by 1,2,3,4正常显示，直到达到5以后爆错，意思没有5个字段，最多四个。

直接上union注入：

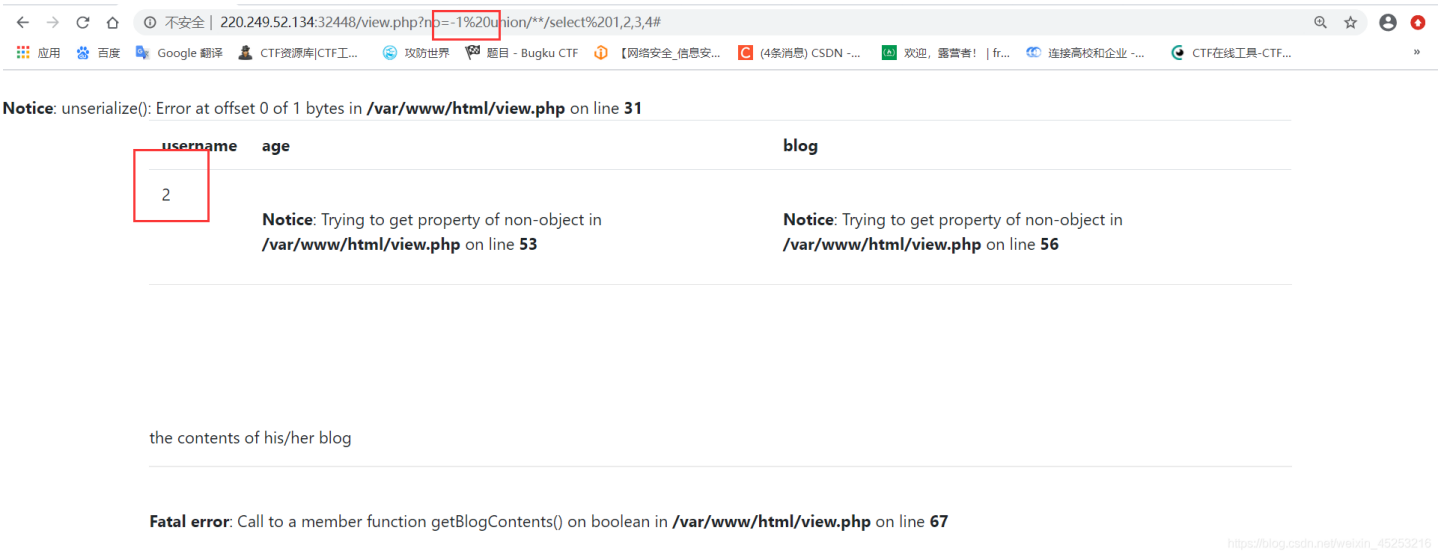
这波应该是检测到要注入了，所以回显个no hack【无奈眼神】

测试看看是不是union select本身被过滤了什么：

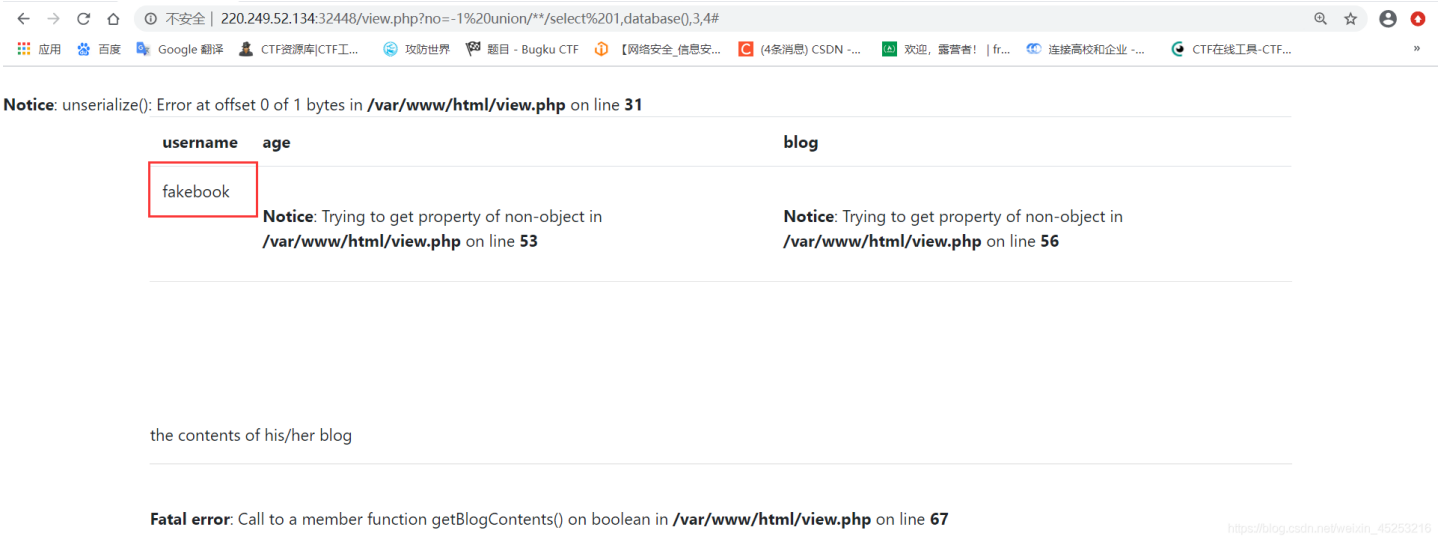
```
/view.php?no=1 union select 1,2,3,4#
/view.php?no=1 uNiOn select 1,2,3,4#
/view.php?no=1 union SeLeCt 1,2,3,4#
/view.php?no=1 UnIoN SELECt 1,2,3,4#
/view.php?no=1 union/**/select 1,2,3,4#
/view.php?no=1 ununionion select 1,2,3,4#
/view.php?no=1 union++select 1,2,3,4#
```

双写绕过有语法错误

只有用加号连字符和内联注释可以绕过。这里需要注意的是，当参数no=1时，会一直显示正常页面，我们需要让no等于一个不存在的id号才能把union联合查询的内容显示出来！！这里让no=-1。



页面除了报错信息还显示了2，证明2这里可以构造payload获得回显。
正常肌肉记忆看一下数据库和用户：



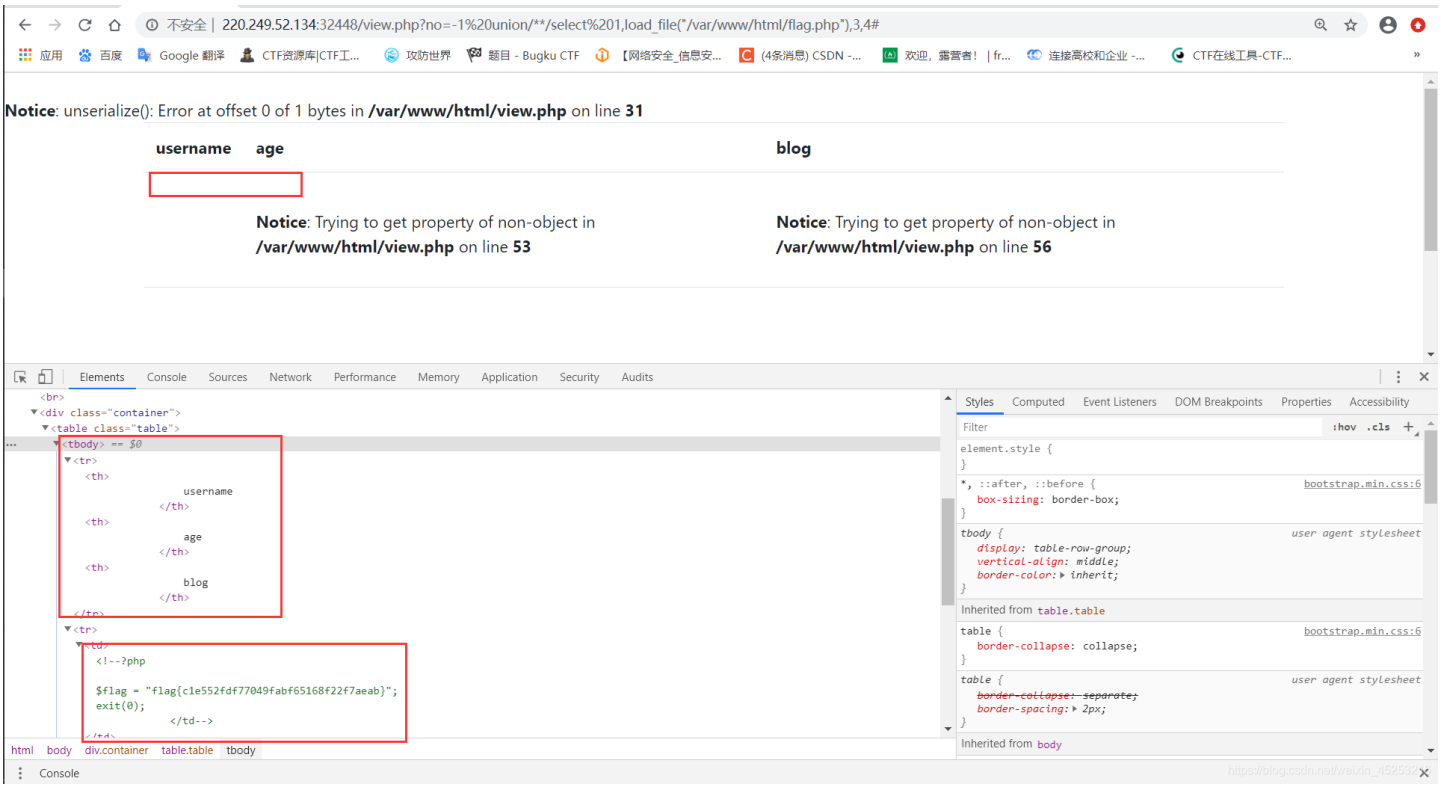
woc，用户直接就是root！！！天神权限【狗头】

mysql中的load_file函数，允许访问系统文件，并将内容以字符串形式返回，不过需要的权限很高，且函数参数要求文件的绝对路径。

emmm，本题目的这种解法唯一不足就是没有亲手在当前目录下找到flag.php这个文件，应该是只有系统管理员才有权限查看，所以我们目录扫描扫不到=.=

这里我们已经在上面看到了很多绝对路径了，非常的常规：/var/www/html/猜测一波flag的文件名flag.php

好家伙，有戏！



这里爆一样的错误，但是正常显示的地方没有东西了，因为是php文件，所以应该被解析执行了。直接F12看一波**正常回显位置隐藏的返回数据**，好家伙，我™直接好家伙，拿到flag。

知识点总结

load_file

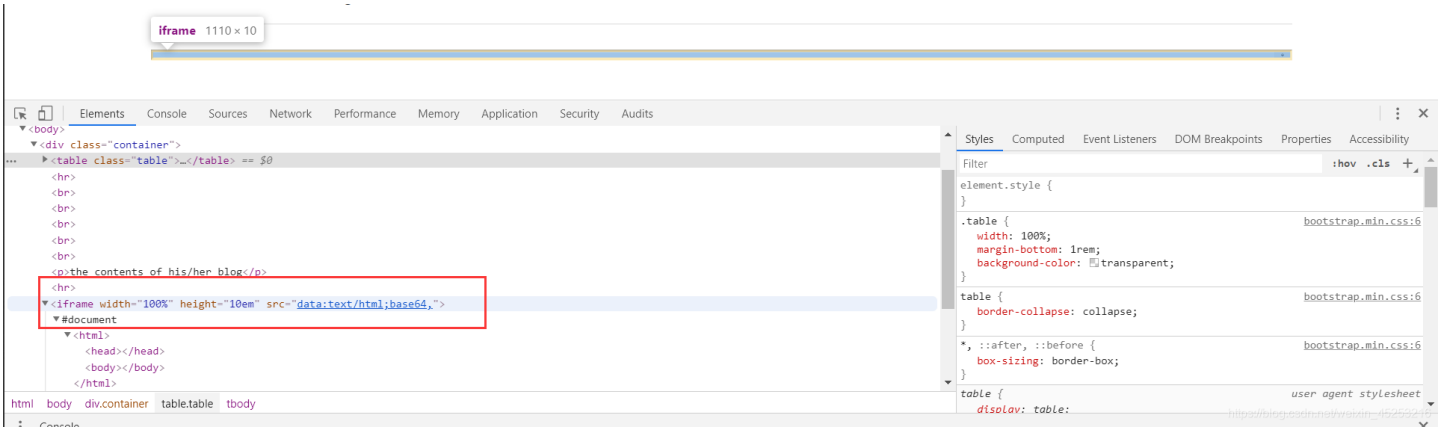
```
load_file("/var/www/html/fiag.php")
```

Mysql中的load_file函数，允许访问系统文件，并将内容以字符串形式返回。
两个注意点：
1就是需要的权限很高，必须是root;
2是文件路径必须是绝对路径。

flag是php文件格式时

当FLAG为php文件格式时，不一定在网页页面上有回显，需要F12查看页面的源代码，在对应位置查看！

通过iframe标签的联想



frame的内容大概意思是：通过data伪协议获取，此处data协议的使用格式为：data:text/html;base64,<base64编码的HTML代码>
所以应该有思路，可以通过这个点，我们想办法让data协议后面接上flag.php的内容，就能达到显示目的了。同时也来了两个问题：一，flag文件的路径并不清楚，通过扫描，我们啥都没扫出来，只能推测在同一目录下，并且具体flag文件名是什么格式，有没有变形，这些都是不知道的。二、如何将内容添加到data协议后面，这个真的不知道，希望以后能遇到要这么做的题目，看看如何利用【狗头】
具体SSRF解法，日后占链接，练习最好还是面面俱到，要不白瞎了人家网鼎杯的一道题。
不过既然有简便解法，何乐而不为呢，毕竟邓小平爷爷说过黑猫白猫，能抓住耗子就是好猫。
【狗头】