

1、知识点

Null

2、源码

```
<?php

if($_GET[id]) {
    mysql_connect(SAE_MYSQL_HOST_M . ':' .
SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);
    mysql_select_db(SAE_MYSQL_DB);
    $id = intval($_GET[id]);
    $query = @mysql_fetch_array(mysql_query("select content from ctf2 where
id='$id'"));
    if ($_GET[id]==1024) {
        echo "<p>no! try again</p>";
    }
    else{
        echo($query[content]);
    }
}

?>
```

3、分析

1) 程序通过GET方法获取参数id的值，并拼接到数据库中进行查询，其中使用intval函数进行判断，如果id==1024，就报错。

```
if($_GET[id]) {
    mysql_connect( server: SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT, username: SAE_MYSQL_USER, password: SAE_MYSQL_PASS);
    mysql_select_db( database_name: SAE_MYSQL_DB);
    $id = intval($_GET[id]);
    $query = @mysql_fetch_array(mysql_query( query: "select content from ctf2 where id='$id'"));
    if ($_GET[id]==1024) {
        echo "<p>no! try again</p>";
    }
    else{
        echo($query[content]);
    }
}
```

2) 那么此时利用intval函数的四舍五入特性，传id的值为1024.1即可成功绕过。由于该题为CTF中的一题，Flag不在此处，只学习思路。

4、利用

?id=1024.1