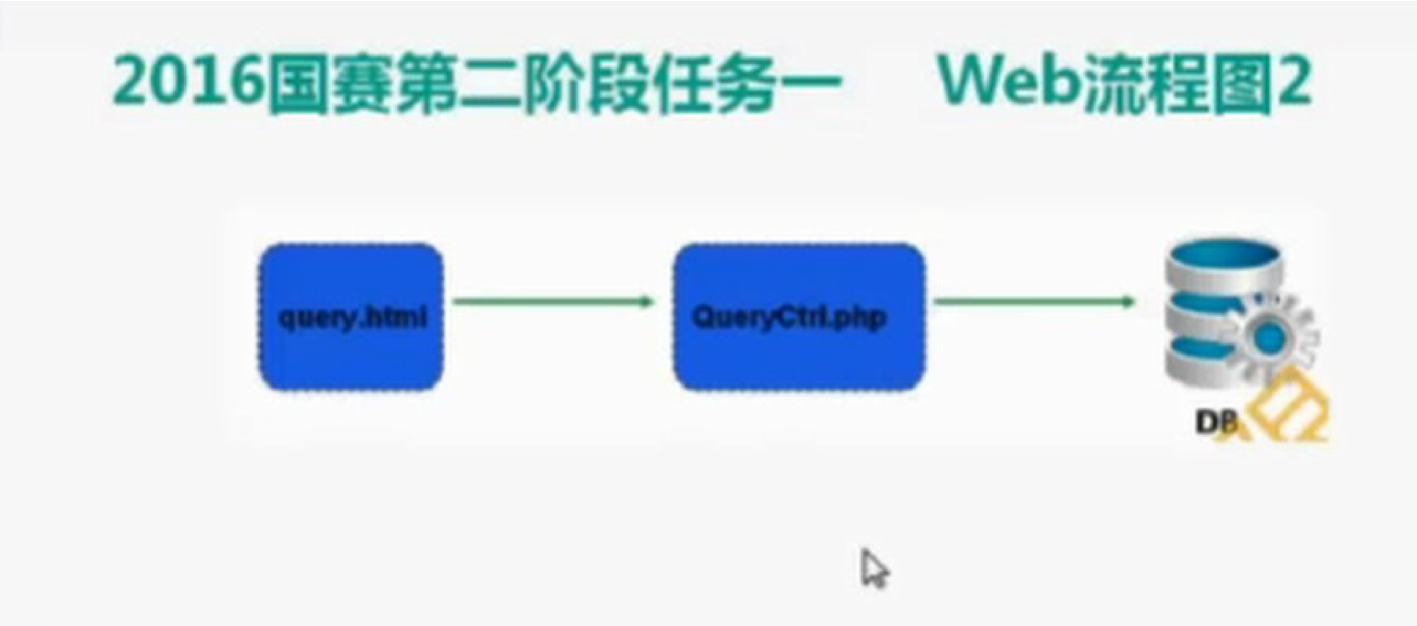
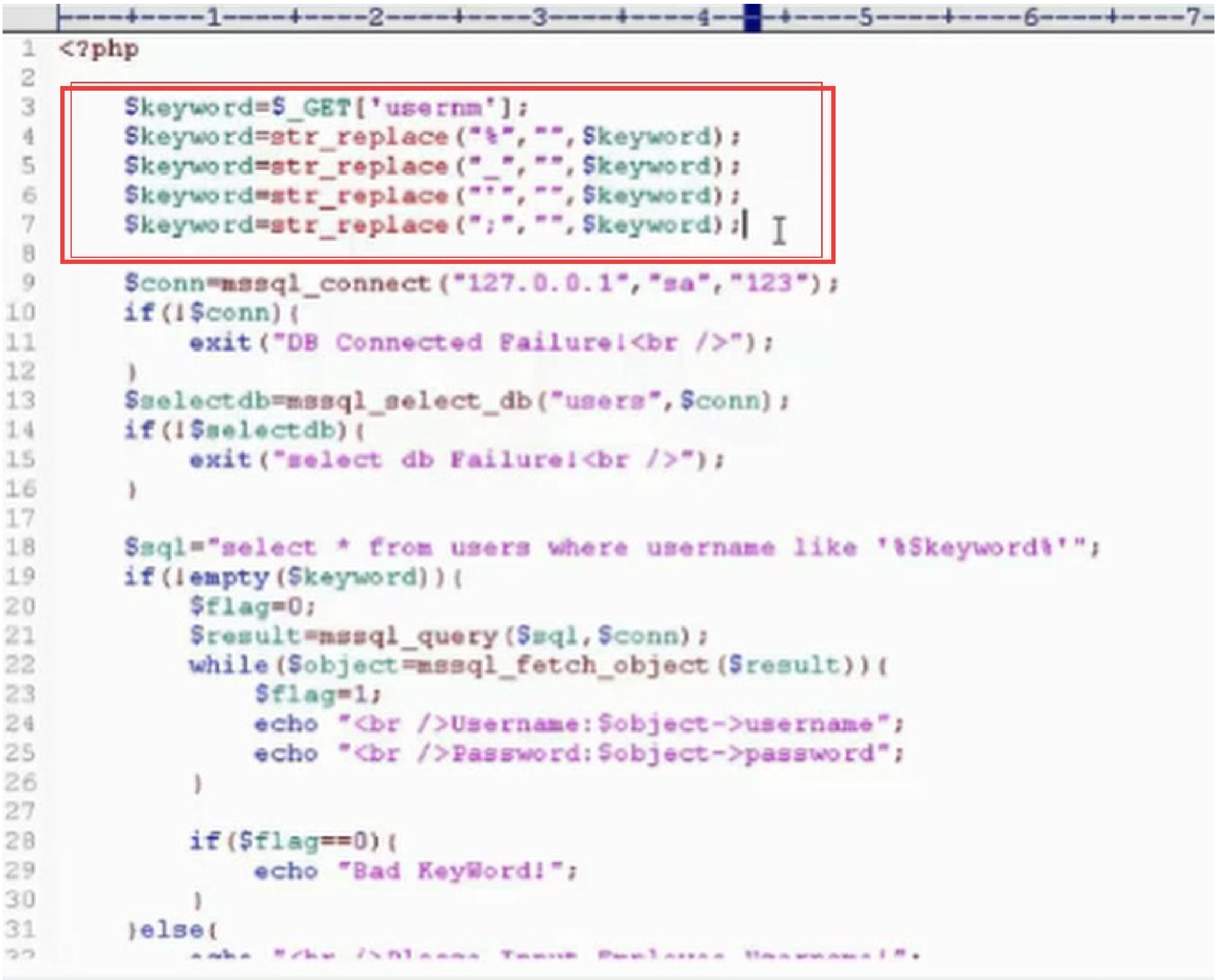


2016国赛第二阶段任务一　Web流程图2

防注入思路:

转义和过滤！！！

过滤一般用str_replace（）函数;



```
<?php

    $keyword=$_GET['usernm'];
    $keyword=str_replace("%","",$keyword);
    $keyword=str_replace("_","",$keyword);
    $keyword=str_replace("'","",$keyword);
    $keyword=str_replace(";","",$keyword);

    $conn=mssql_connect("127.0.0.1","sa","123");
    if(!$conn){
        exit("DB Connected Failure!<br />");
    }
    $selectdb=mssql_select_db("users",$conn);
    if(!$selectdb){
        exit("select db Failure!<br />");
    }

    $sql="select * from users where username like '%$keyword%'";
    if(!empty($keyword)){
        $flag=0;
        $result=mssql_query($sql,$conn);
        while($object=mssql_fetch_object($result)){
            $flag=1;
            echo "<br />Username:$object->username";
            echo "<br />Password:$object->password";
        }

        if($flag==0){
            echo "Bad KeyWord!";
        }
    }else{
        echo "<br />Please Input Replace Username!";
```

转义:一般用addslash()函数;