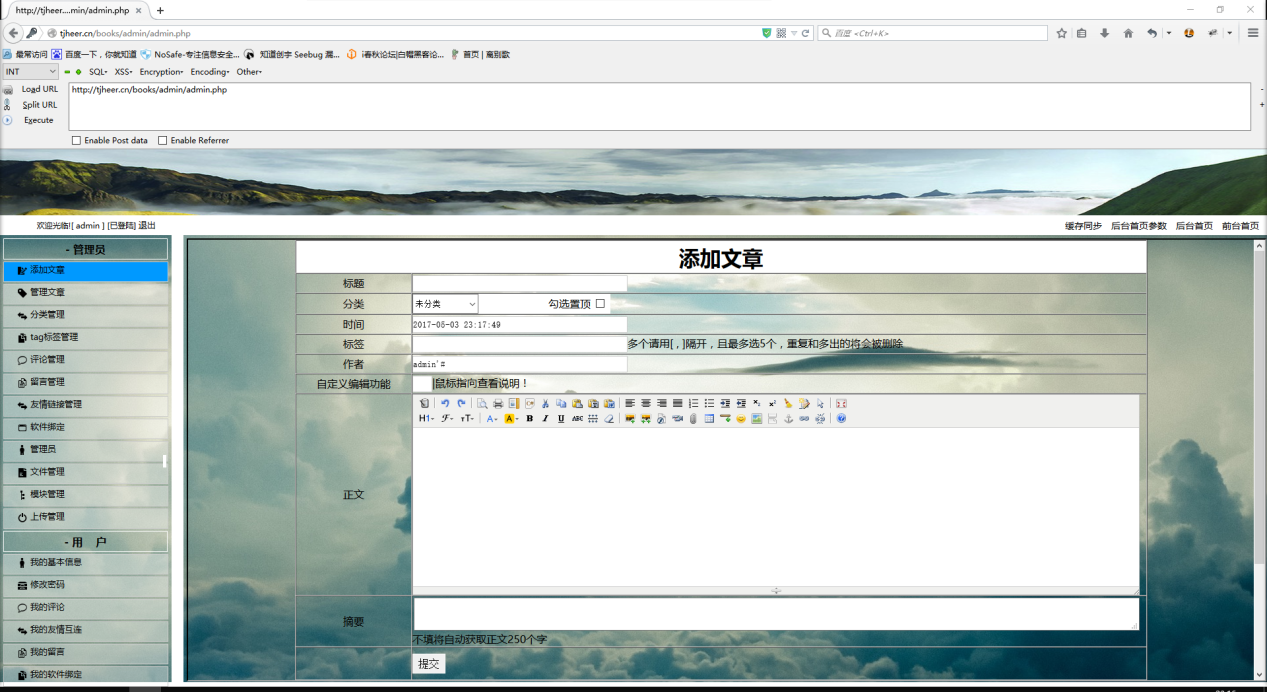
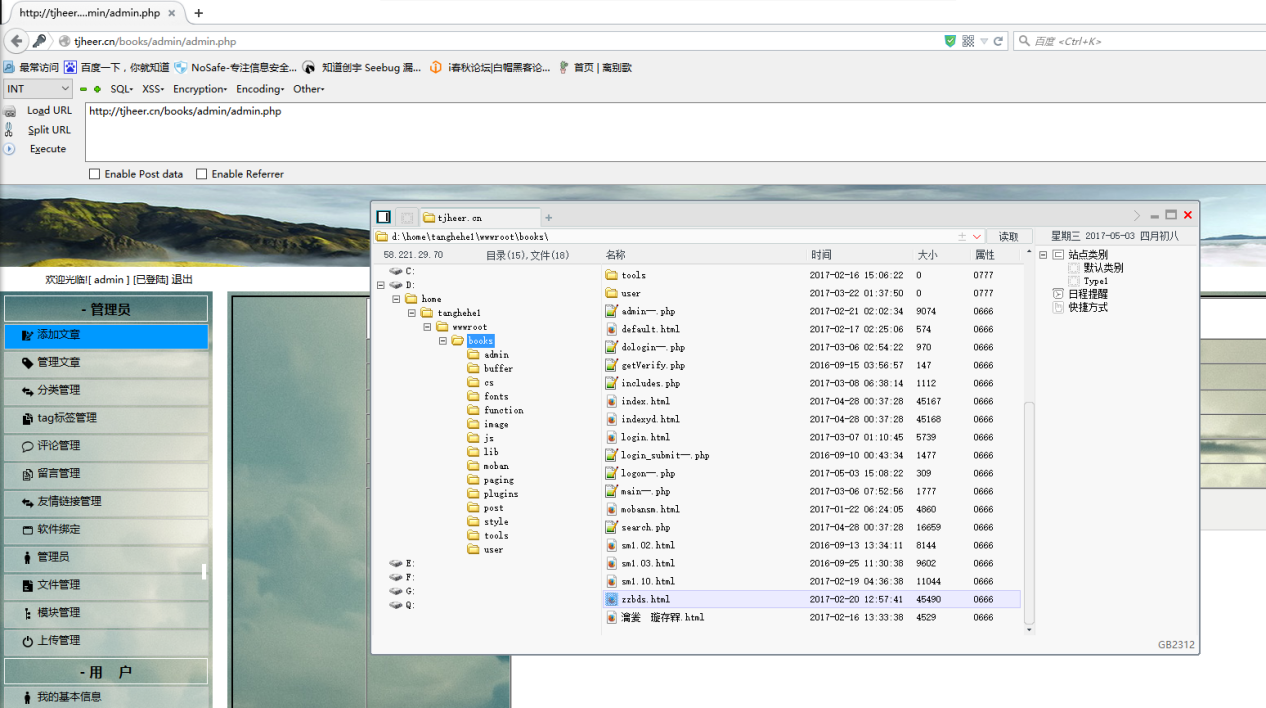
2017年5月3日

-----代码审计笔记实战官网

漏洞的组合拳成功拿下官网

验证:



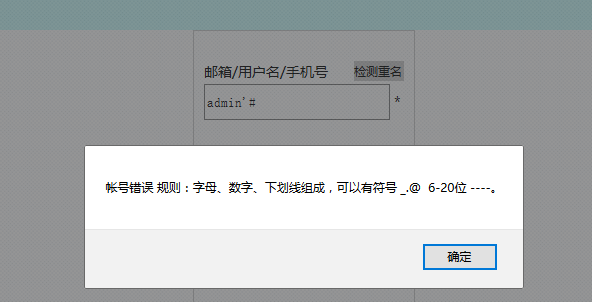


成功拿下

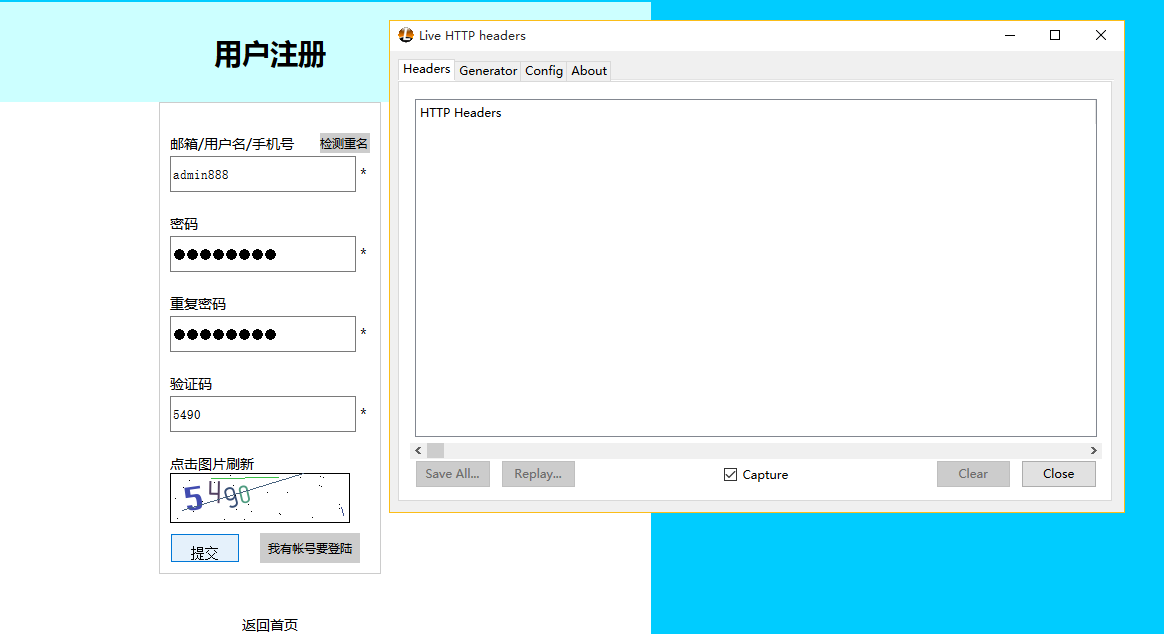
过程:

血泪辛酸史,在本地挖到的很多漏洞在官网上基本上都没法利用,比如说任意登陆漏洞,留言Xss,Sql注入等都无法正常利用,因为有一个注册漏洞没利用上,我也懒得写报告,但是今天我无意间想到我注册一个名为admin’#的用户然后登陆,岂不是可以登陆Admin的账号,说干就干,开始吧!

有前端验证,不过我们可以后面改包



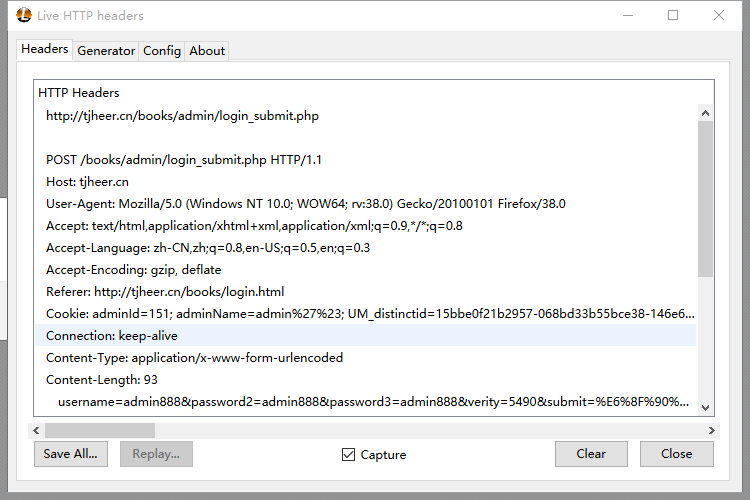
填好数据



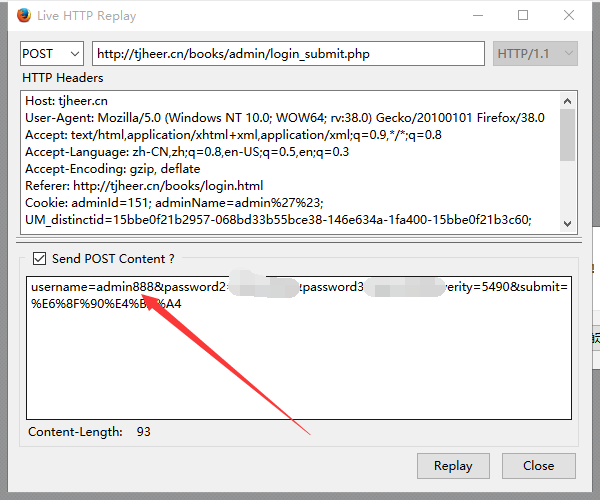
点击提交

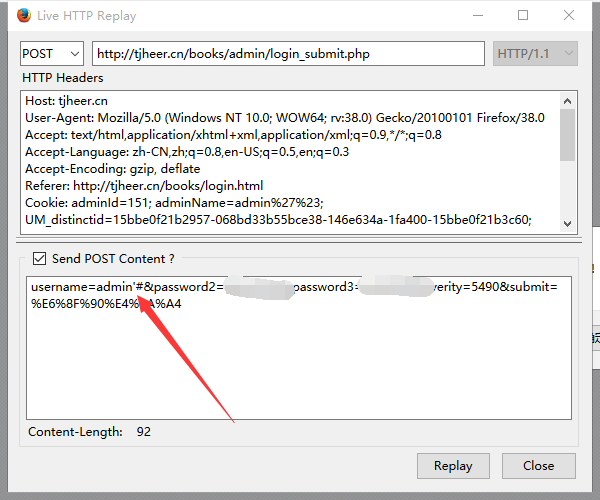


成功注册此时看抓包工具也已经抓到包



然后开始修改Post请求





因为我已经注册了,不能重复注册,我们去登陆看一下



成功登陆



此时我们的ID是admin’#



但是到了后台管理我们发现ID变成了admin



权限也是1管理员权限



因为可以直接文件操作Shell很好拿就不写出来了

漏洞文件:

dologin.php（登陆）和login\_submit.php（注册）:

Dologin.php

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

$password= md5($\_POST['password']);

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

$verify=$\_POST['verity'];

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

//无任何过滤可截断Sql语句

$sql="SELECT \* FROM imooc\_admin where username='{$username}' and password='{$password}'";

$res=mysql\_query($sql);

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

Login\_submit.php

<?php

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

$password=$\_POST['password2'];

$password1=$\_POST['password3'];

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

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

$zhucetime=date("Y-m-d H:i:s");

$nname=$\_POST['username'];

if($verity==$verify1){

}else{

alertMes('验证码错误！','login.html');

}

if($password==$password1){

} else{

alertMes('用户名或密码错！','login.html');

}

//echo $zhucetime;

//echo $sql.'<br>' ;

$sql="SELECT \* FROM imooc\_admin where username='{$username}'";

$res=mysql\_query($sql);

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

//echo $res1.'<br>' ;

//print\_r($res1);

//return ;

//print\_r($\_POST);

//echo $verity ;

//echo $verify1 ;

if($res1){

//if(!empty($res1)){

//echo "nono用户存在，请重新输入" ;

alertMes("用户存在，请重新输入！","login.html");

//alertMes("nono用户存在，请重新输入！","");

}else{

// alertMes("yes 可以添加！！","");

$password=md5($password);

$sql="insert into imooc\_admin (id,username,password,zhucetime,quanxian,nname)values(null,'$username','$password','$zhucetime','0','$nname')" ;

//echo $sql;

$rowrr=mysql\_query($sql);

//echo "yes 可以添加！" .$rowrr;

if($rowrr){

alertMes("注册成功！返回登陆！","login.html");

//echo '[]'.$rowrr;

}

}

?>

通过分析以上代码得到结论：

①登陆和注册未对用户名过滤

②存在Sql注入漏洞 并且在验证管理员权限的时候直接将 Session内容拿去拼凑SQL语句 ,导致截断SQL语句成功拿到管理员权限

③有的代码没有发出来 请自行测试