xiahao90 / **CVEproject** Public

Code Issues Pull requests Actions Projects Security Insights

main

CVEproject / DolphinPHPV1.5.0_xss.md

xiahao90 Update DolphinPHPV1.5.0_xss.md History

1 contributor

```
24 lines (21 sloc) | 1.54 KB
```

DolphinPHP<=1.5.0 Authenticated Stored Cross-Site Scripting(XSS)

Description

```
The system Client doesn't properly sanitise POST parameter, which result into a
Stored Cross-Site Scripting(XSS).
```

Vendor Homepage

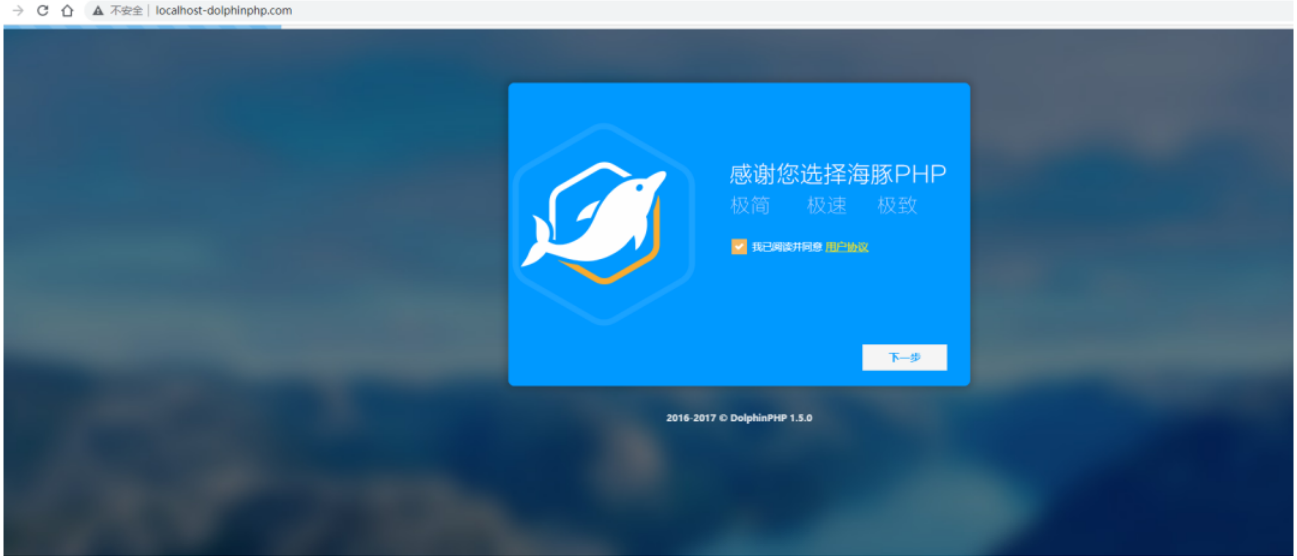
```
https://dolphinphp.com/
https://github.com/caiweiming/DolphinPHP
```

Author

```
webraybtl@webray.com.cn inc
```

Proof of Concept

1,After the system installation is completed, log in to the background

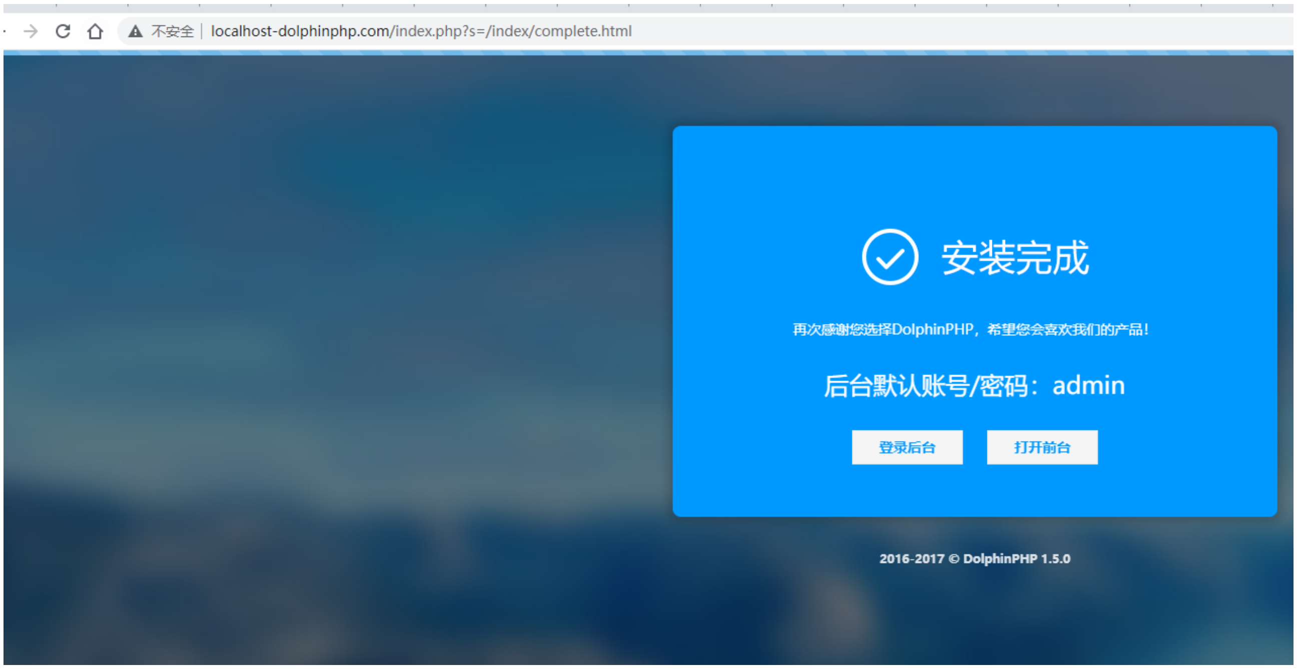


感谢您选择海豚PHP

极简 极速 极致

☑ 我已阅读并同意 用户协议

2016-2017 © DolphinPHP 1.5.0



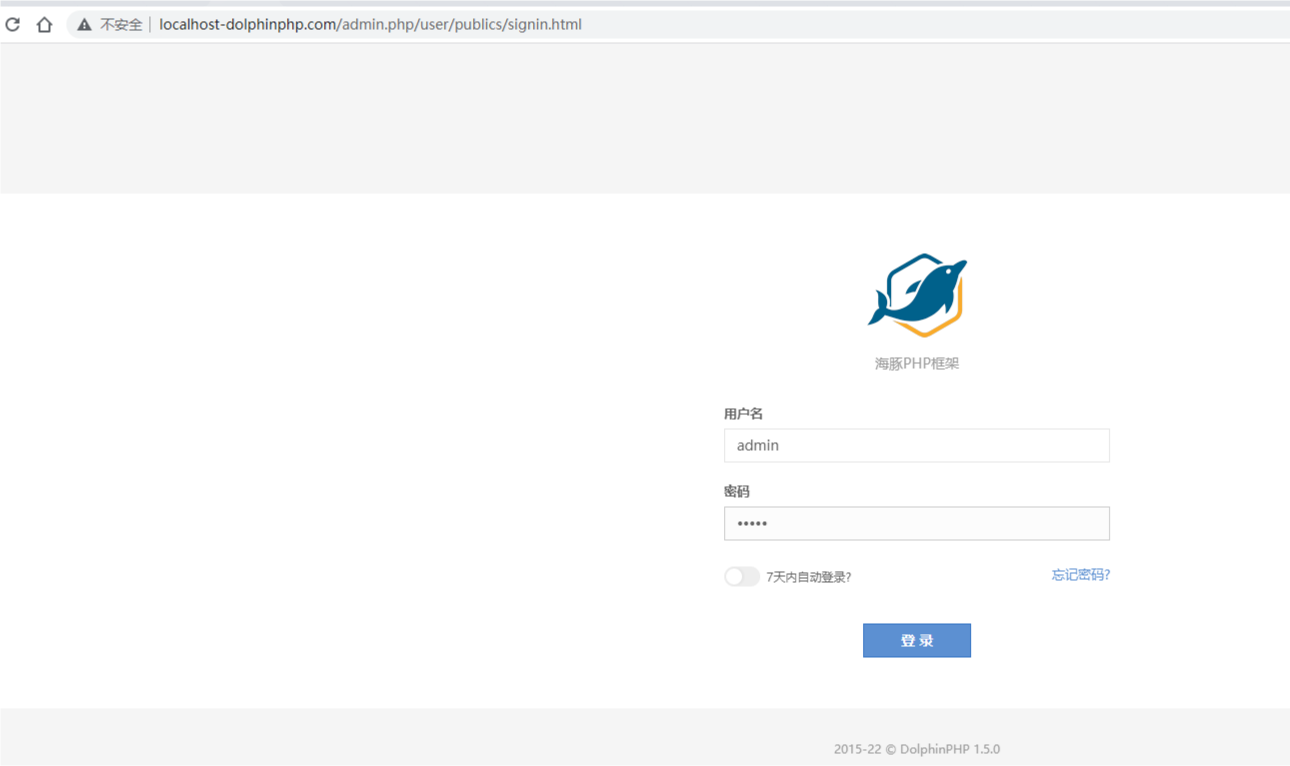
不安全 | localhost-dolphinphp.com/index.php?s=/index/complete.html

安装完成

再次感谢您选择DolphinPHP，希望您会喜欢我们的产品！

后台默认账号/密码：admin

2016-2017 © DolphinPHP 1.5.0



不安全 | localhost-dolphinphp.com/admin.php/user/publics/signin.html

海豚PHP框架

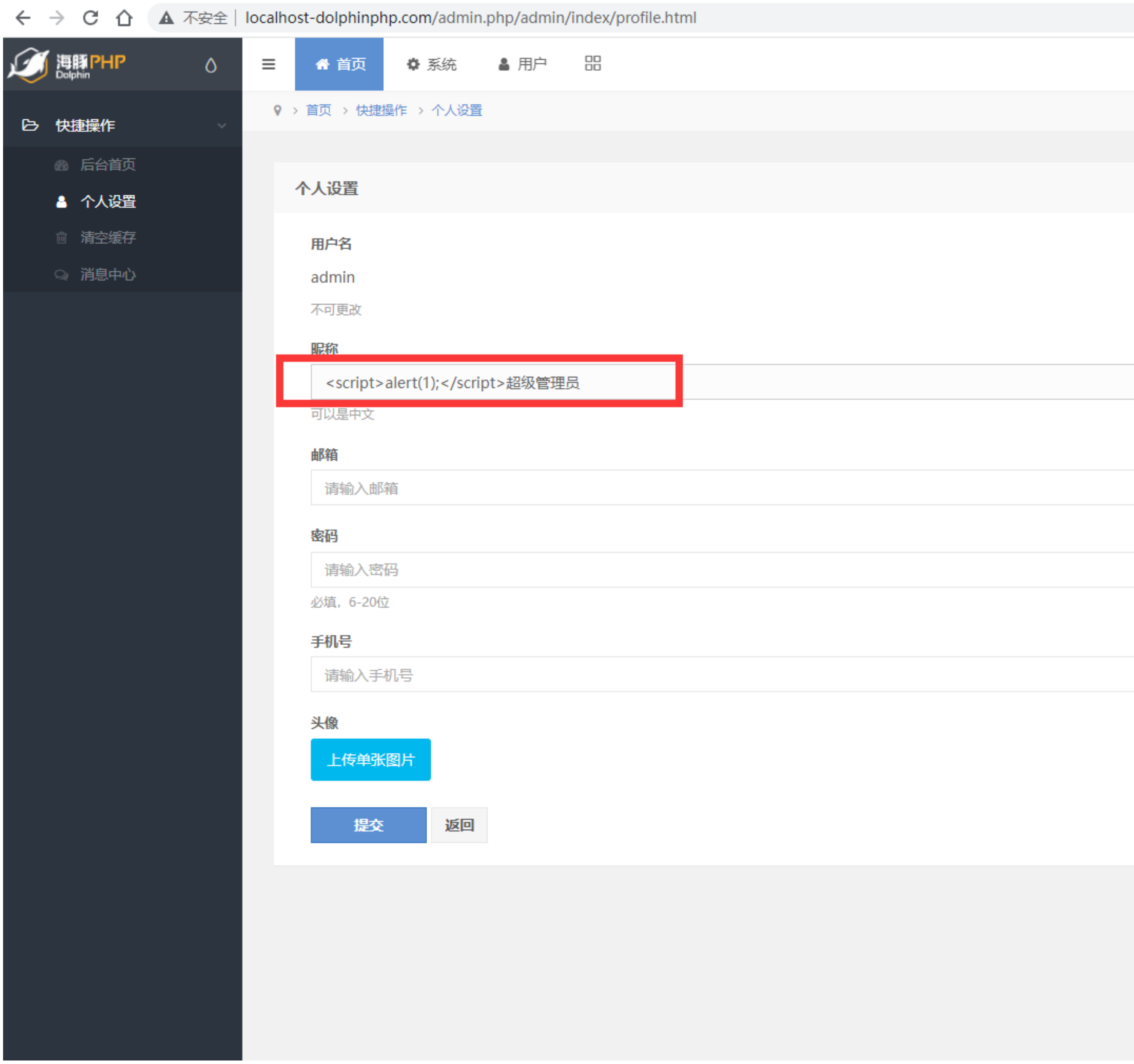
用户名: admin

密码: •••••

2015-22 © DolphinPHP 1.5.0

2,Insert a danger code where the nickname is modified in the personal settings

```
<script>alert(1);</script>超级管理员
```



个人设置

用户名

admin

不可更改

昵称

<script>alert(1);</script>超级管理员

可以是中文

邮箱

请输入邮箱

密码

请输入密码

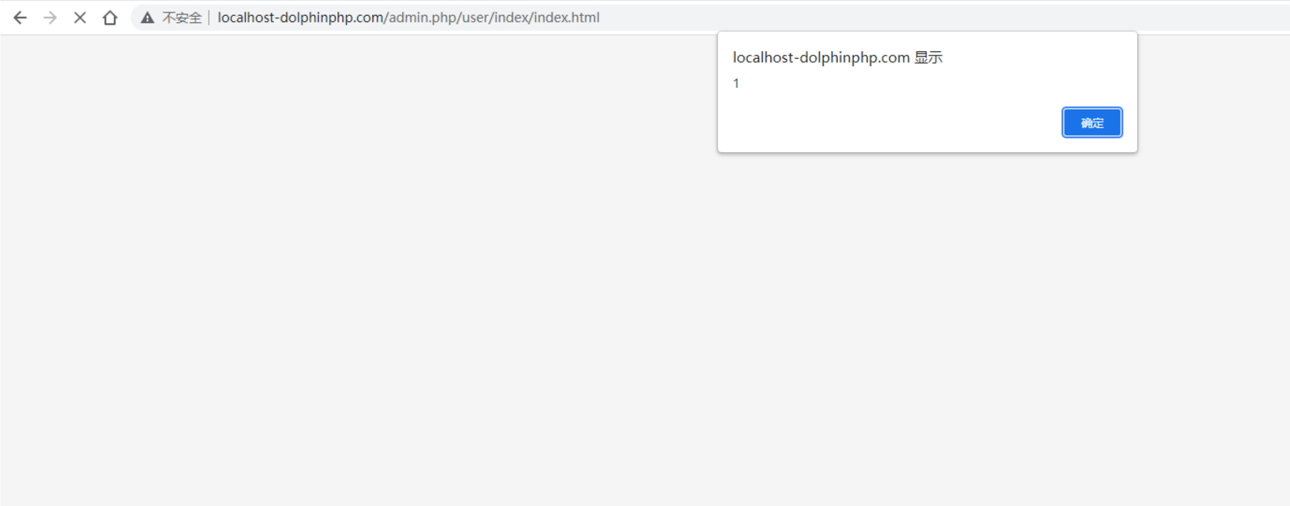
必填，6-20位

手机号

请输入手机号

头像

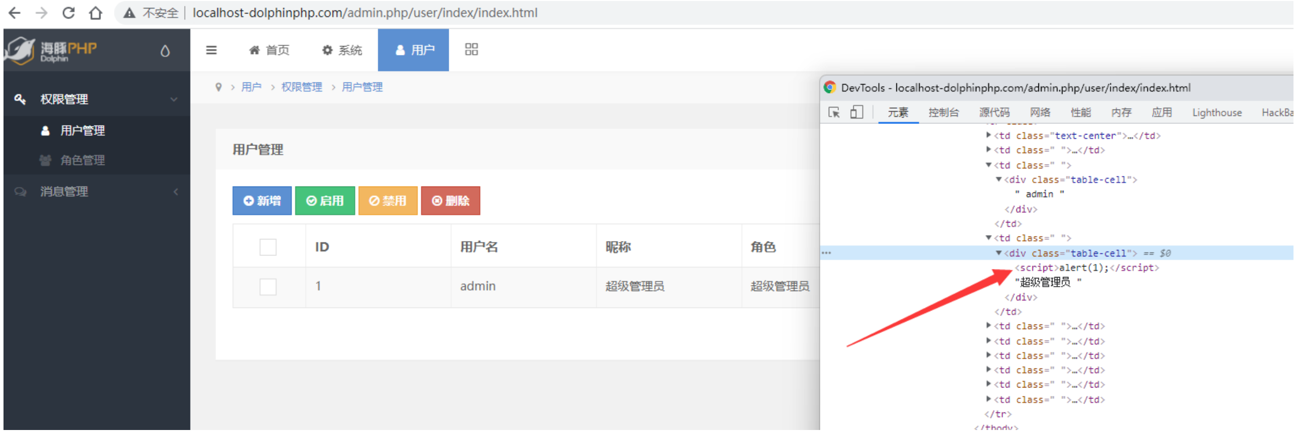
3,Click "user" - > "permission management" - > "user management" to execute the code



localhost-dolphinphp.com/admin.php/user/index/index.html

localhost-dolphinphp.com 显示

1



localhost-dolphinphp.com/admin.php/user/index/index.html

用户管理

	ID	用户名	昵称	角色
□	1	admin	超级管理员	超级管理员

DevTools - localhost-dolphinphp.com/admin.php/user/index/index.html

```
▶<td class="text-center">…</td>
▶<td class=" ">…</td>
▼<td class=" ">
  ▼<div class="table-cell">
     " admin "
   </div>
 </td>
▼<td class=" ">
  ▼<div class="table-cell"> == $0
     <script>alert(1);</script>
     "超级管理员 "
   </div>
 </td>
▶<td class=" ">…</td>
▶<td class=" ">…</td>
▶<td class=" ">…</td>
▶<td class=" ">…</td>
▶<td class=" ">…</td>
▶<td class=" ">…</td>
</tr>
</tbody>
```