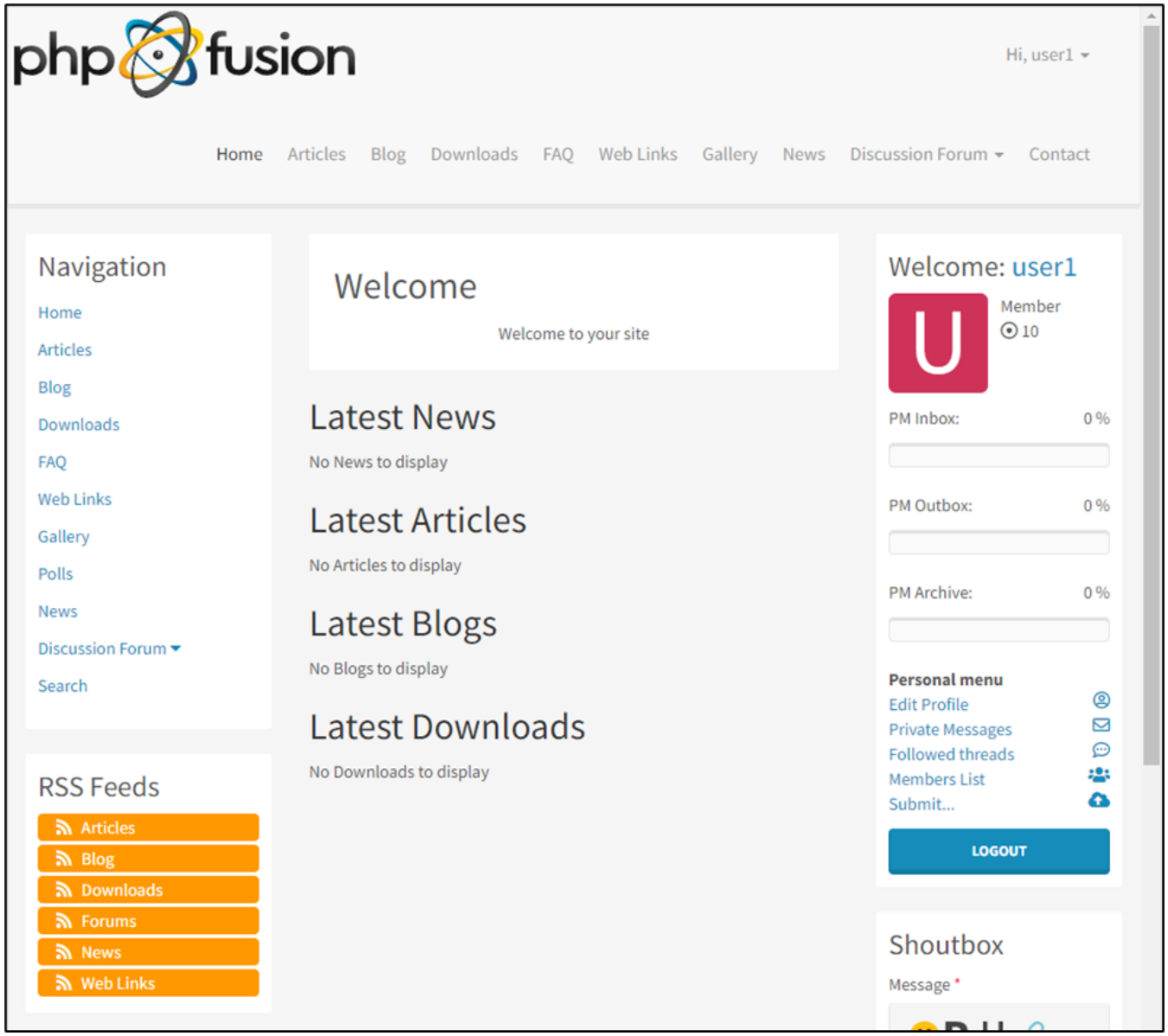
# Full account takeover in phpfusion/phpfusion



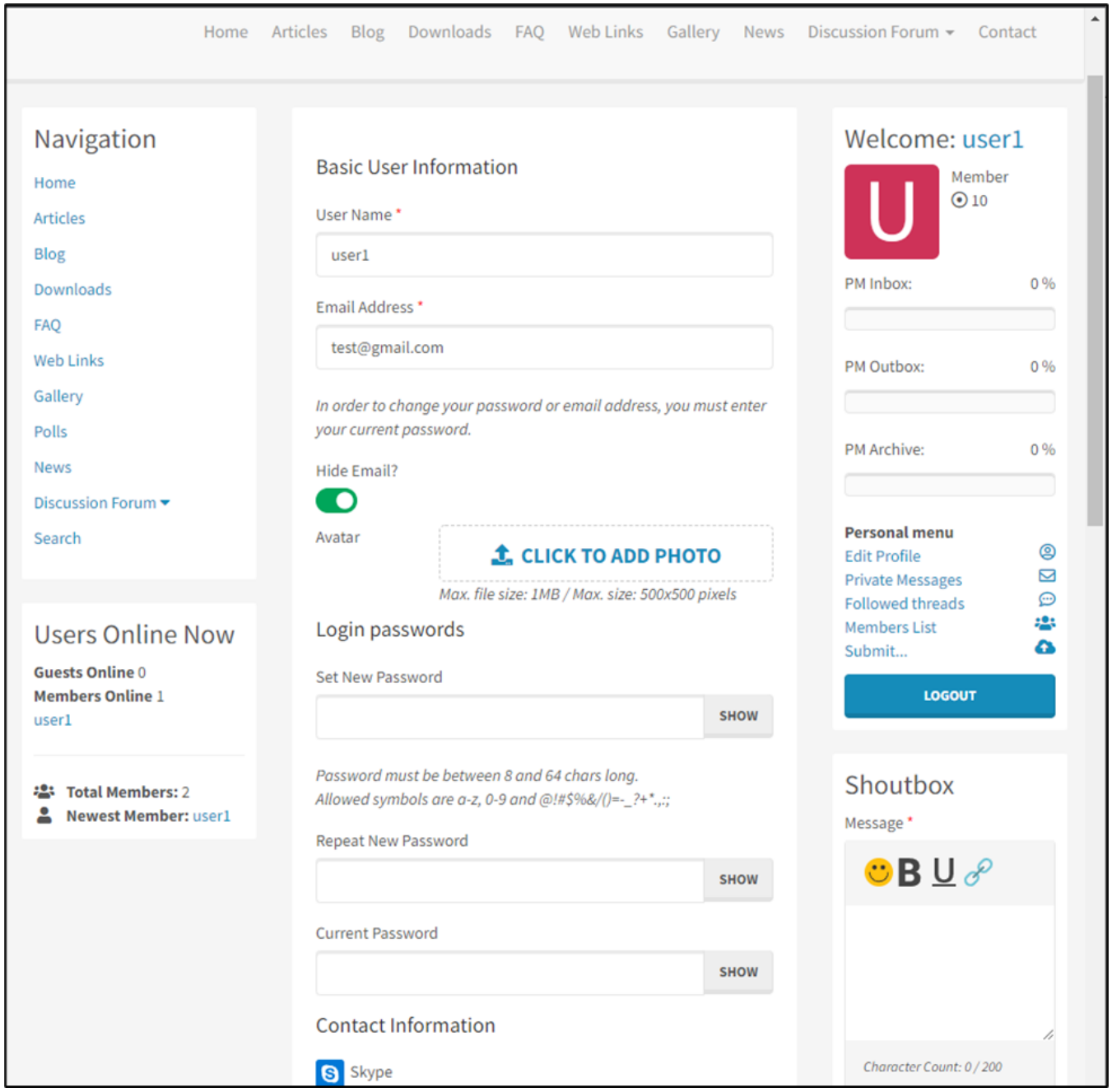
Valid Reported on Aug 19th 2022

**POC:**

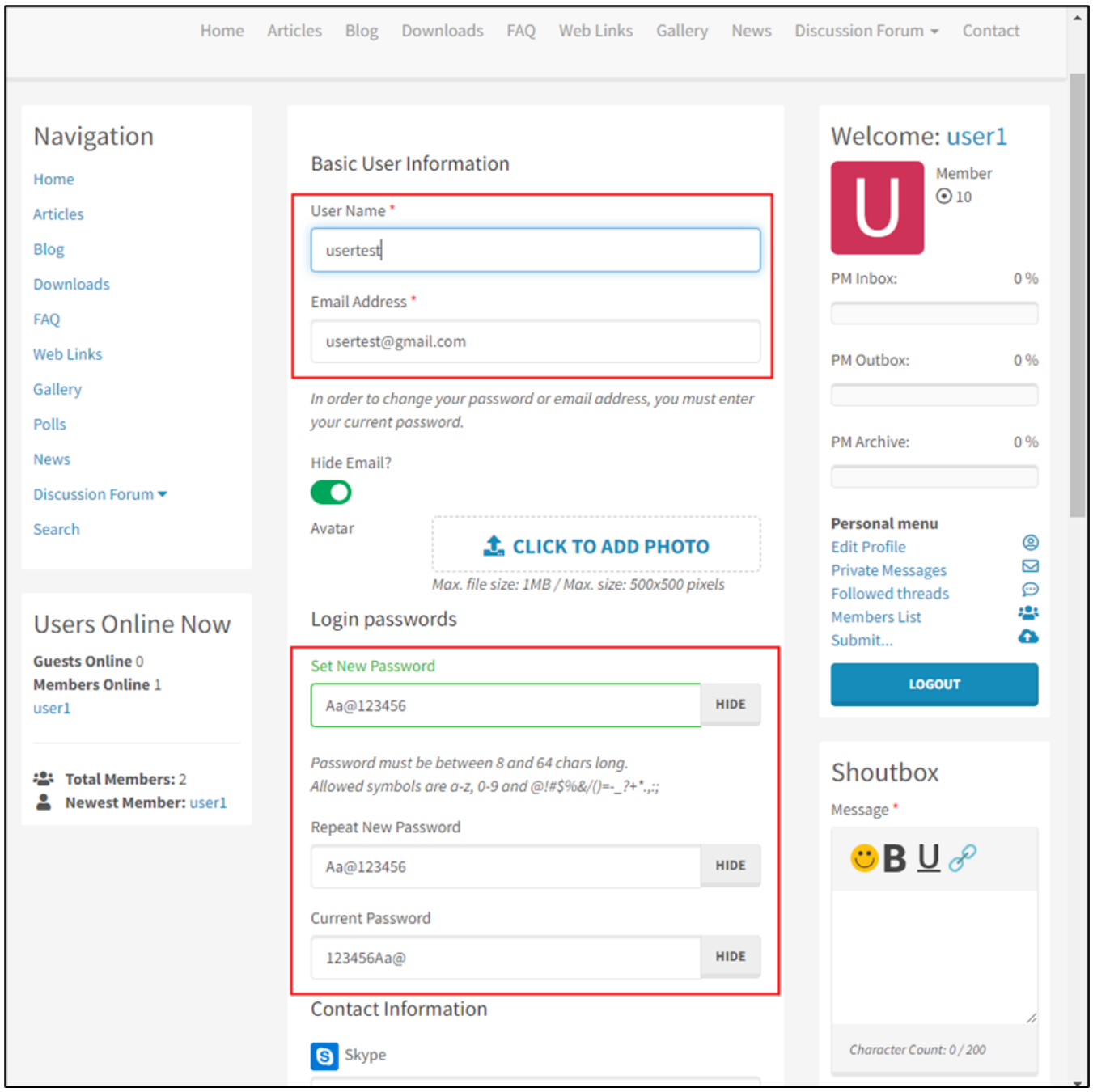
**Step 1:** Use a normal user account



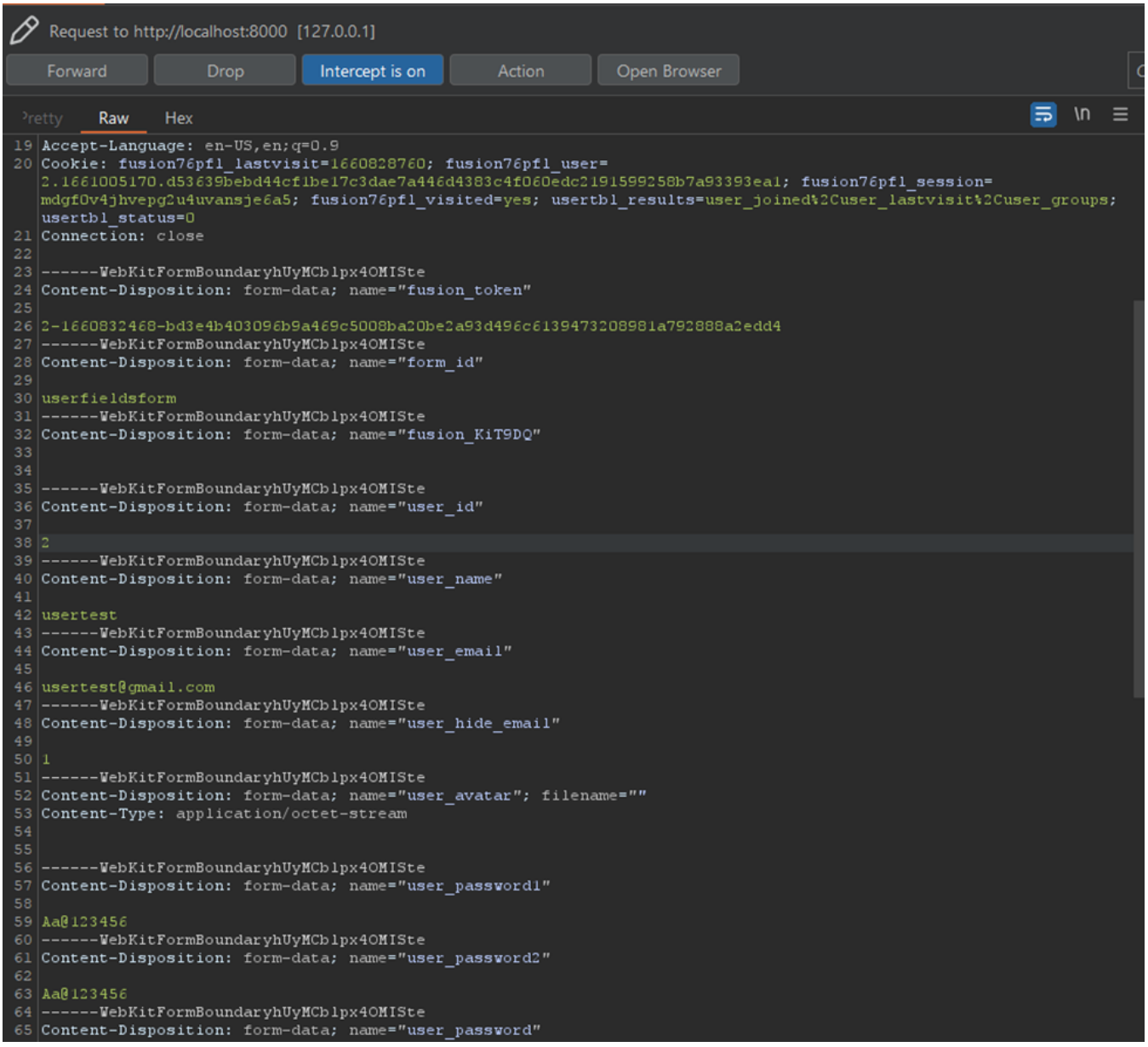

**Step 2:** Change user password in edit profile function



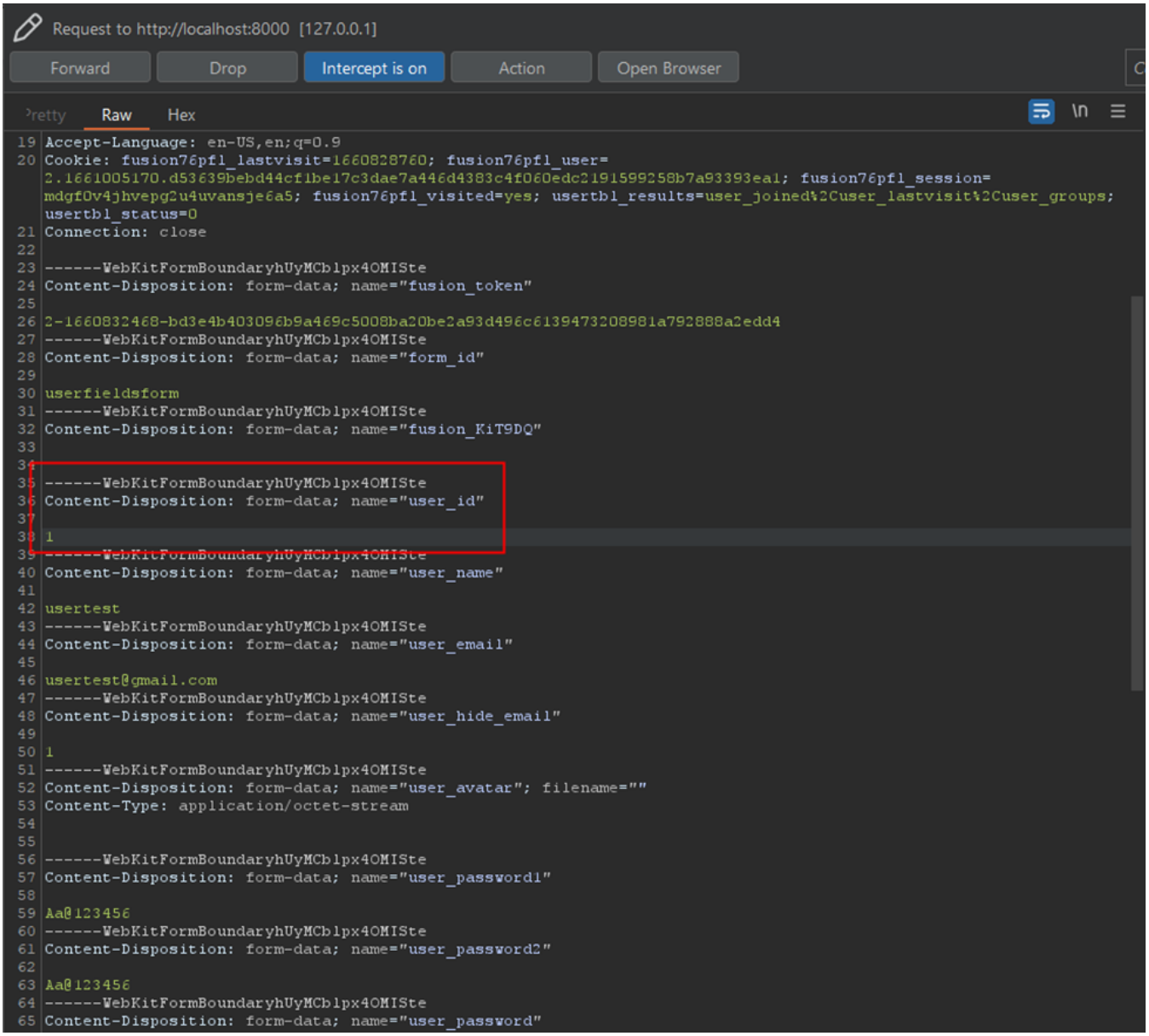

**Step 3:** Enter data fields that change normally




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




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




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


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


## 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

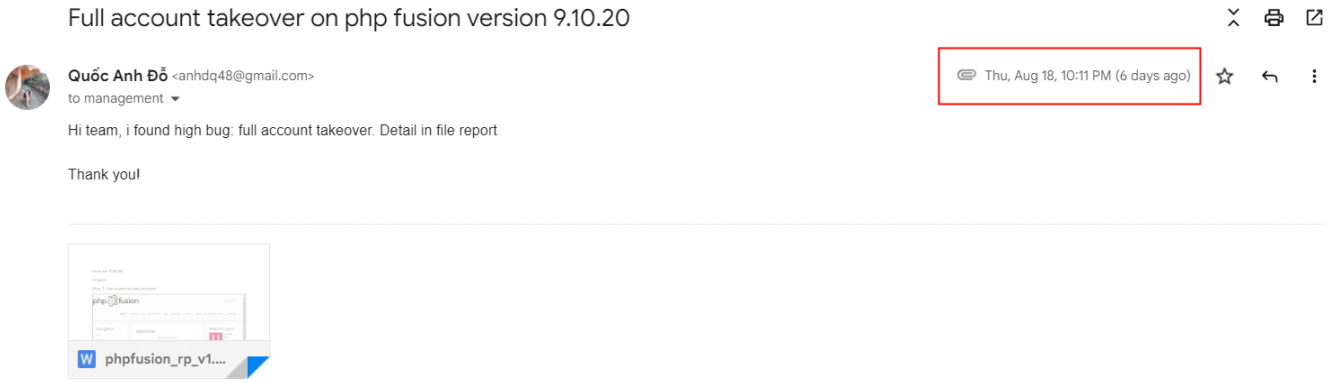
alex 3 months ago Researcher

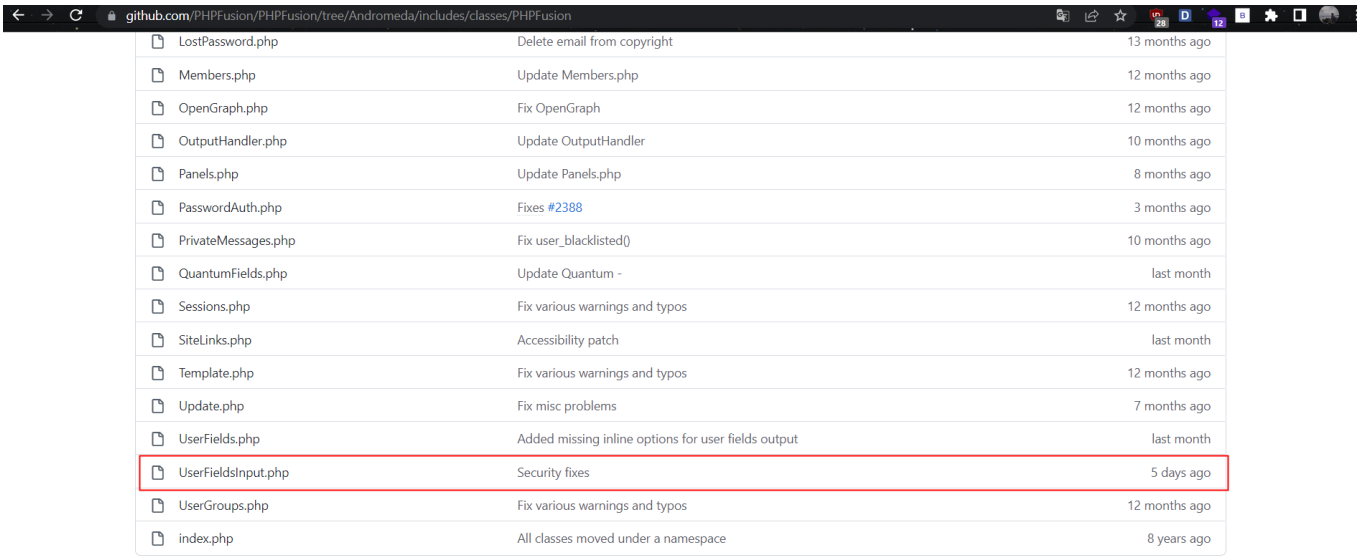
I sent an email yesterday at 22:11(GTM+7), Aug 18, 2022, but so far no reply

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.




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 nu
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

Thank you

Thank you

Sign in to join this conversation