New issue

Jump to bottom

User Enumeration in Sign in page #2346

Closed **oosman-rak** opened this issue on Dec 21, 2020 · 6 comments

oosman-rak commented on Dec 21, 2020

Describe the bug
It was observed that the login page of the php-fusion throwed different messages upon different username entries. This shows that the product is vulnerable to user enumeration vulnerability.

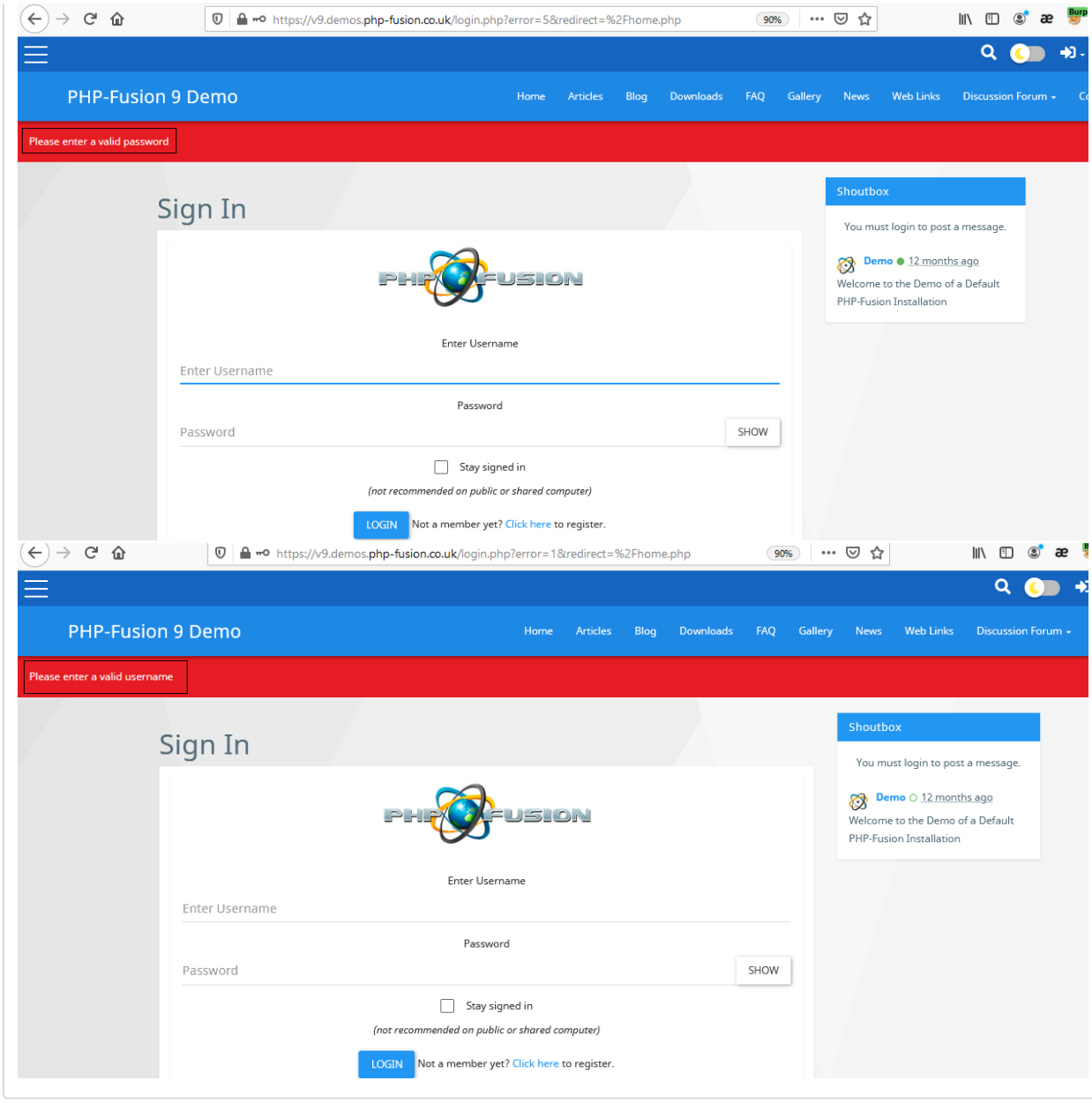
Version
PHP-Fusion latest version 9.03.90.

To Reproduce
Steps to reproduce the behavior:

1. Go to 'https://v9.demos.php-fusion.co.uk/administration/members.php'
2. Login using valid credentials
3. Add a new user.
4. Now open a separate private tab, access the URL: https://v9.demos.php-fusion.co.uk/login.php.
5. Try logging in with username that we created with wrong password, Observe the product throws message 'Enter valid Password'
6. Now, try logging in with wrong/non-existing username and password. Observe the application throws different message.
7. This difference in error message leads an attacker to collect valid usernames which can ease brute forcing or logging in attempt.

Expected behavior
Display a common message for any combination of wrong username/password.

Screenshots



oosman-rak commented on Dec 22, 2020 — Author

@FrederickChan @RobiNN1 any updates on this?

RobiNN1 closed this as completed in cbe8775 on Dec 30, 2020

---

oosman-rak commented on Jan 2, 2021 — Author

Hi @RobiNN1 ,

Can i raise a CVE request for this now?

Thanks,
Mohamed Oosman B S

RobiNN1 commented on Jan 3, 2021 — Contributor

I don't care about CVE but do what you want. It's already fixed.

RobiNN1 reopened this on Jan 3, 2021

RobiNN1 closed this as completed on Jan 3, 2021

JoakimFalk commented on Jan 3, 2021 • edited — Contributor

@oosman-rak I really hope you guys do not run penetration tests on our live sites. We had a huge traffic spikes in January, on demos to be specific.
That is considered flooding at best and DDoS attempts at worst. In fact our logs was several hundreds of GB large due to this causing major issues and in essence halted server.
I will only say this once, Please run test on your local host or not at all, I will take actions if my notification here is not taken serious.

oosman-rak commented on Jan 3, 2021 • edited — Author

Hi **@JoakimFalk**,
Nope, I guess there is a misunderstanding on your side. I had just done a basic logical testing (just like a normal user performs) in mid December and have not performed any kind of automation to generate this huge traffic. Not really sure about the spike in January you are talking about because I haven't even visited the demo site since then .

JoakimFalk commented on Jan 4, 2021 — Contributor

Hi !
Thank you for clarifying, was required to mention it since I know you been doing some tests. Good to hear that you are not running any automated scripts for penetration testing on live sites.

RobiNN1 mentioned this issue on Feb 19, 2021

Login to site - missing Errors notices. #2142

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants