New issue

Jump to bottom

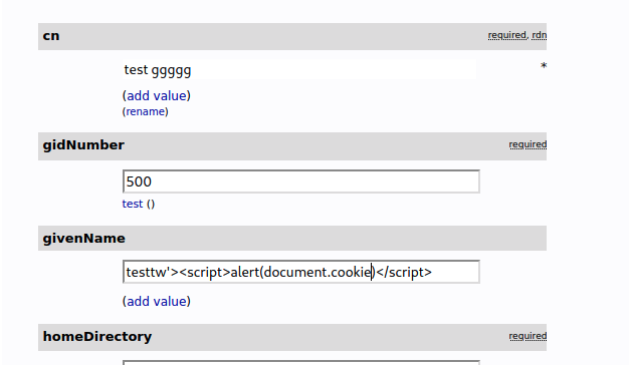
XSS in cmd.php for 1.2.5 #130

Closed **4ndygu** opened this issue on Dec 1, 2020 · 15 comments

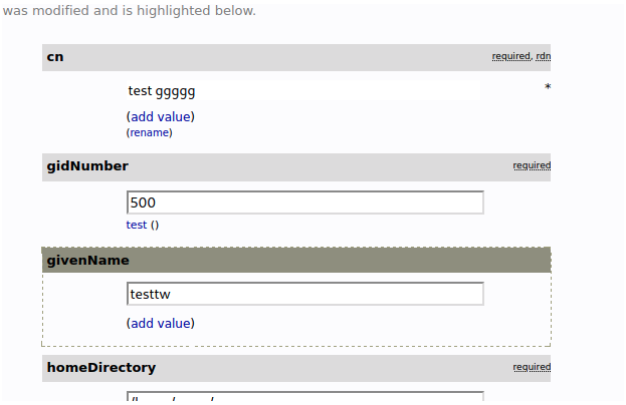
4ndygu commented on Dec 1, 2020

A user can set a field to an XSS payload, which triggers when the confirmation screen for whether to confirm the change is raised.

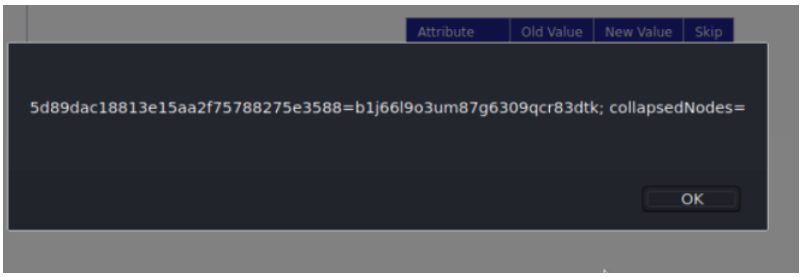
From cmd.php, say I have an attribute set to the following:



Then, say I am an admin and would like to change that field back:



When the field prompts me for a change, the payload is triggered. A user can log into user 1 and request a change, then wait for an admin to try deleting the field, which would trigger the payload for that user.



leenooks commented on Dec 1, 2020 Owner

Problem doesnt appear to be in 1.2.6.2 - please let me know if it is.

leenooks closed this as completed on Dec 1, 2020

setharnold commented on Dec 2, 2020

I didn't look exhaustively but this commit appears likely to have addressed the issue:

c87571f

Do you know if a CVE has been assigned for this issue yet?

Thanks

4ndygu commented on Dec 2, 2020 Author

Hi!

I don't think so -- do you know how I can go about this? I apologize for the lack of knowledge / context here. If it helps, I filed a report at https://bugs.launchpad.net/ubuntu/+source/phpldapadmin, but the ticket should be private since it's a security issue.

- Andy

setharnold commented on Dec 2, 2020

> On Wed, Dec 02, 2020 at 01:00:07PM -0800, Andy Gu wrote:
> I don't think so -- do you know how I can go about this? I apologize for the lack of knowledge / context here. If it helps, I filed a report at https://bugs.launchpad.net/ubuntu/+source/phpldapadmin, but the ticket should be private since it's a security issue.

I opened the launchpad bug because all the details are public on the github issue.

Because compiling all the necessary information for a CVE takes time, and because duplicate CVE assignments cost all CVE consumers time, I'd like to make sure that this doesn't already have a CVE number assigned before asking MITRE to assign one.

Thanks

4ndygu commented on Dec 2, 2020 Author

Cool, thanks! It seems like you confirmed it here: https://bugs.launchpad.net/ubuntu/+source/phpldapadmin/+bug/1906474. No CVE number is currently assigned.

alexmurray commented on Dec 10, 2020

This was assigned CVE-2020-35132 by MITRE.

epozuelo commented on Dec 15, 2020

@leenooks **@4ndygu** are you sure this is fixed in 1.2.6.2? I can still reproduce this issue with that version.

epozuelo commented on Jan 5, 2021

ping? I think this is unfixed, can someone double check & reopen?

4ndygu commented on Jan 5, 2021 Author

@leenooks Can we take a second look at the fix if possible? I am currently indisposed and have nuked my environment but can spin it back up in a few weeks otherwise to confirm **@epozuelo**.

epozuelo commented on Jan 26, 2021

any news on this? can this issue be reopened to match its current status?

4ndygu commented on Jan 30, 2021 Author

Hey **@epozuelo** ! I don't think I have permissions here to re-open, but **@leenooks** should. I wonder if it would make sense in this case to open a new issue for visibility.

setharnold commented on Feb 1, 2021

My suggestion is to open a new issue -- anyone can do that, it'll help reduce confusion, etc. It'd be best to include a small reproducer that can be clearly used to demonstrate when the issue has been fixed.

Thanks

epozuelo mentioned this issue on Feb 24, 2021

XSS from CVE-2020-35132 (#130) still unfixed #137

Open

epozuelo commented on Feb 24, 2021

I have opened #137. Please someone double check if you can also reproduce this issue with 1.2.6.2 and report there. Thanks!

epozuelo commented on May 21, 2021

> **@leenooks** Can we take a second look at the fix if possible? I am currently indisposed and have nuked my environment but can spin it back up in a few weeks otherwise to confirm **@epozuelo**.

@4ndygu any chance you can retest with current git master? I'd like to verify if this is still unfixed as I found in my tests. Thanks!

epozuelo commented on May 21, 2021

> **@leenooks** Can we take a second look at the fix if possible? I am currently indisposed and have nuked my environment but can spin it back up in a few weeks otherwise to confirm **@epozuelo**.
>
> **@4ndygu** any chance you can retest with current git master? I'd like to verify if this is still unfixed as I found in my tests. Thanks!

Sorry I meant BRANCH-1.2 (or 1.2.6.2), not git master which is 2.x (although the same problem probably applies to the master branch)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants