New issue

\c\g.php has an arbitrary file download vulnerability #6

⊘ Closed   **ddddbhm** opened this issue on Dec 19, 2020 · 1 comment

---

ddddbhm commented on Dec 19, 2020

If you don't think it's important, you can ignore me.

As you can see, we need to go through two levels to get to the castle.

These data are not filtered.

We need to bypass the logic here. What should we do?

Yes, we just need to replace '../' with '..\'

POC:

POST /c/g.php?type=getpage

data: mode=normal&p=..\a\edit

SomeBottle commented on May 30, 2021   Owner

thx!

SomeBottle closed this as completed on May 30, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

---

2 participants