New issue

Jump to bottom

Stored XSS on ImpressCMS 1.4.0 #659

Closed **Applebois** opened this issue on Jun 18, 2020 · 11 comments · Fixed by #660

Assignees

Labels bug security vulnerability

Projects ImpressCMS v1.x

Milestone 1.4.1

Applebois commented on Jun 18, 2020

Payload = **<script>alert('AppleBois');</script>**

Vulnerable URL :modules/system/admin.php?fct=adsense&op=mod&adsenseid=4
Vulnerable TextBar : ID of the [adsense tag to display this ad]

Vulnerable URL :/modules/system/admin.php?fct=customtag&op=mod
Vulnerable TextBar : Name

Reference
https://medium.com/@tehwinsam/impresscms-1-4-0-3aaf1825e6d5

fiammybe self-assigned this on Jun 19, 2020

fiammybe added this to the **1.4.1** milestone on Jun 19, 2020

fiammybe added bug security vulnerability labels on Jun 19, 2020

fiammybe added this to **To do** in **ImpressCMS v1.x** via automation on Jun 19, 2020

fiammybe commented on Jun 19, 2020 Member

Hi, the medium reference is not working.

Keep in mind that you have to be logged in and need to have access to the administration section before you have access to that page. Because of that, I consider it a low-risk vulnerability, but thank you for the ticket, I'll get on it straight away.

Applebois commented on Jun 19, 2020 Author

https://medium.com/@tehwinsam/impresscms-1-4-0-3aaf1825e6d5
Totally agree on that you mentioned.

However, there a function/feature in 'AutoTask '. i don't know you consider
it as a feature or risk.
Because it allow Authenticated User to execute *ANY php command *which
allow BAD GUY interact 'MySQL'(assume db is localhost, with default
credential) or gain 'RCE' from the php code
...

fiammybe commented on Jun 19, 2020 Member

Yes,those are the administration functionalities that should only be handled by trusted admin users. As a matter of fact, it can be used to clean up database entries (for example to follow the retention period for certain data, you can run an autotask every day to remove old data).

fiammybe commented on Jun 19, 2020 Member

We have a presence on HackerOne : https://hackerone.com/impresscms . It is still in 'startup' phase because we haven't had enough vulnerability notifications passing through there in order to qualify for a full presence, but you can still use it if you want. You will need to create a HackerOne account though.
I will verify if that is mentioned in the security documentation. Follow-up there should be easier in the future.

Applebois commented on Jun 19, 2020 Author

I've created an account .
https://hackerone.com/tehwinsam is my profile
...

fiammybe commented on Jun 19, 2020 Member

Could you enter this bug report also there? It would give me an opportunity to see if everything works as expected :-)

Applebois commented on Jun 19, 2020 — Author

Unfortunately, when i browse the URL https://hackerone.com/impresscms, it
pop out 'Page not Found' , but i have manually submitted a report to
support@hackerone.com and waiting for their response
...

fiammybe commented on Jun 19, 2020 — Member

Thanks! It's unclear to me how this works, the 'private' repository thing of HackerOne :-(We'll see what they anwser

Applebois commented on Jun 19, 2020 — Author

Alright.

Applebois commented on Jun 19, 2020 — Author

amigo, below is the reply from HackerOne.

Thank you for reaching out to HackerOne Support about submitting your report. We are not able to review or validate reports on behalf of the companies that use our platform or even our own program.

If the company is listed in our directory (https://hackerone.com/directory) we recommend that you go to their page and submit the report through the method they have provided. If the program has a pink submit button they have a program on our platform.

If they have a directory page but are not using our platform then they will be a community updated page. These community updated pages have the following message on them:

'''HackerOne Directory [?]
Information is provided and moderated by members of the community. Accuracy has not been validated by HackerOne.'''

If the company does not have a directory page with us you may want to try reporting it to our Disclosure Assistance team. You can find more information about how Disclosure Assistance works in this article:

https://docs.hackerone.com/programs/disclosure-assistance.html#___gatsby

MekDrop mentioned this issue on Jun 20, 2020

This probably should fix #659 #660

Merged

fiammybe pushed a commit that referenced this issue on Jun 25, 2020

`this probably should fix the XSS issue in #659 (#660)` `b0e9b97`

fiammybe commented on Jul 7, 2020 — Member

Hi, I tested this under the 1.4.1 beta, and the behaviour is now as expected : the system does not execute the javascript, but simply shows it in the box. I think we can close this and release 1.4.1 final then.

fiammybe linked a pull request on Jul 7, 2020 that will close this issue

This probably should fix #659 #660 — Merged

fiammybe closed this as completed on Jul 7, 2020

ImpressCMS v1.x automation moved this from **To do** to **Done** on Jul 7, 2020

Assignees

fiammybe

Labels

bug security vulnerability

Projects

ImpressCMS v1.x

Done

Milestone

1.4.1

Development

Successfully merging a pull request may close this issue.

This probably should fix #659

2 participants