New issue

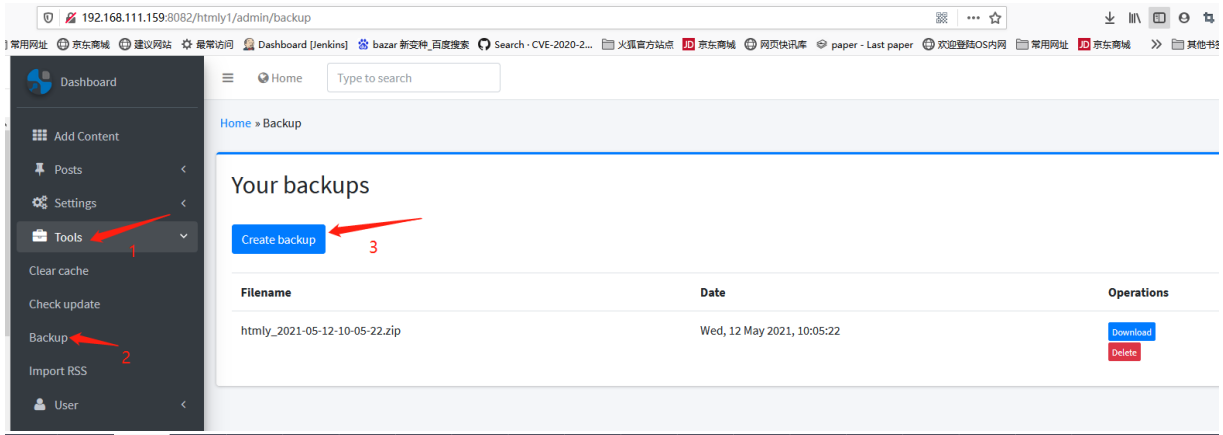
Jump to bottom

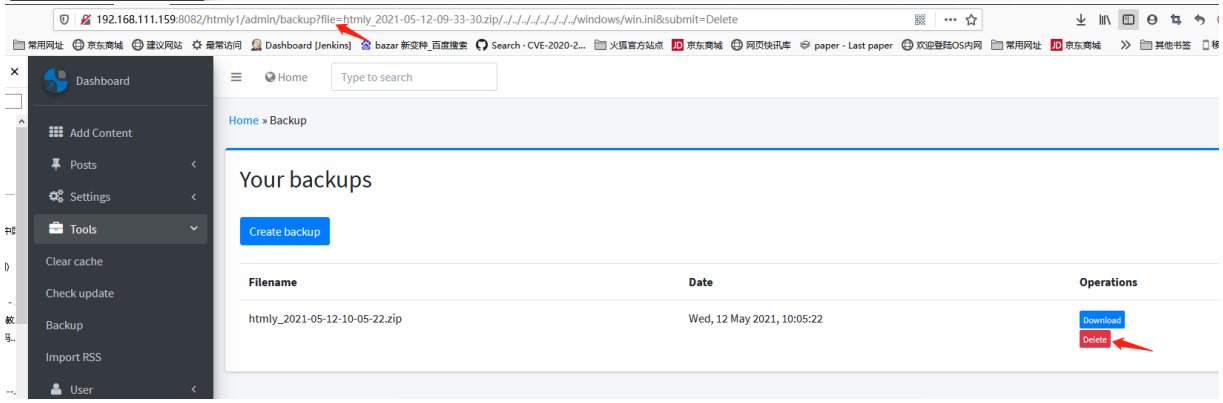
Security Issue： arbitrary file deletion vulnerability in “\system\admin\views\backup.html.php” #462

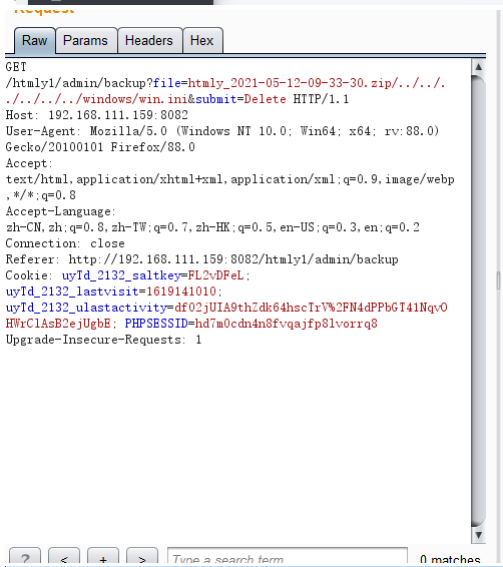
Closed **wszdhf** opened this issue on May 12, 2021 · 4 comments

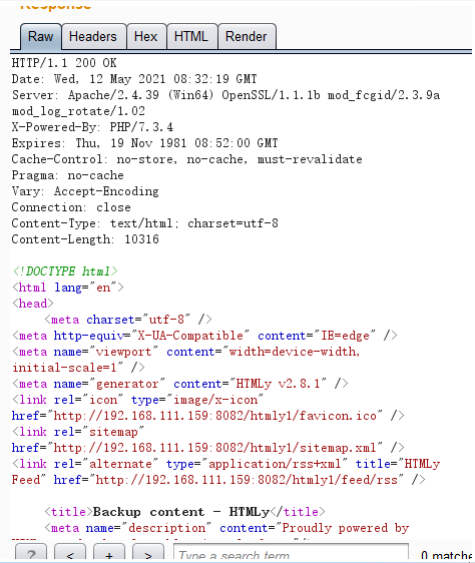
wszdhf commented on May 12, 2021 • edited

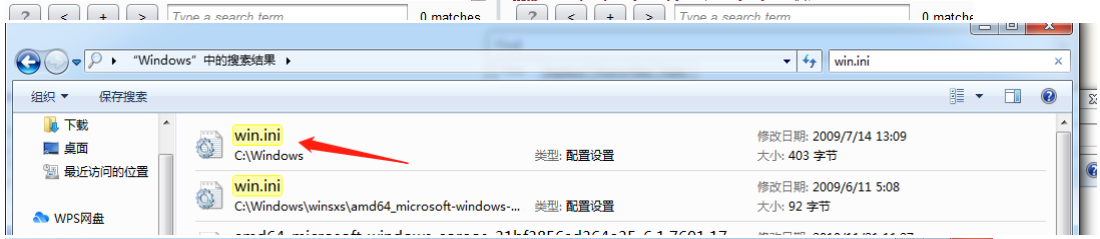
Hi there,
I found an arbitrary file deletion vulnerability in Htmly.
Proof of Concept:
tested on Windows7 and Htmly version 2.8.1 and 2.8.0
1. Log in to the dashboard，click **Tools** -->**Backup**-->**create backup** to create backup.
2. Arbitrary file deletion: click **Delete** and modify the file parameter.
payload: GET /htmly1/admin/backup?file=htmly_2021-05-12-09-33-30.zip/../../../../../windows/win.ini&submit=Delete

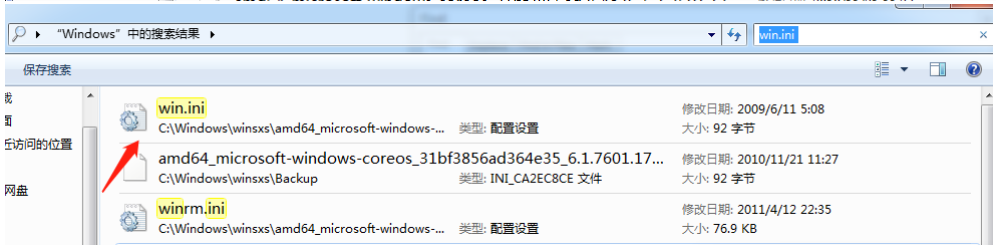












danpros commented on May 12, 2021 — Owner

Hello,

Are you sure it can delete file outside the backup folder?

I already specify:

```
if (login()) {
    if (isset($_GET['file'])) {
        $file = _h($_GET['file']);

        if (!empty($file)) {
            unlink("backup/$file");
        }

    }
}
```

So it always check if the user login or not and than always search the file inside backup folder in htmly installations folder.

ProjectPatatoe commented on May 12, 2021 — Contributor

I just confirmed this on a ubuntu/apache2. I am able to delete a file in htmly's root directory.

ProjectPatatoe added a commit to ProjectPatatoe/htmly that referenced this issue on May 12, 2021

`keep within dir for deleting backups for danpros#462` — `25cdee3`

ProjectPatatoe mentioned this issue on May 12, 2021

backup handling tweak #463

Merged

wszdhf commented on May 12, 2021 — Author

> Hello,
>
> Are you sure it can delete file outside the backup folder?
>
> I already specify:
>
> ```
> if (login()) {
>     if (isset($_GET['file'])) {
>         $file = _h($_GET['file']);
>
>         if (!empty($file)) {
>             unlink("backup/$file");
>         }
>
>     }
> }
> ```
>
> So it always check if the user login or not and than always search the file inside backup folder in htmly installations folder.

yes，it can delete file outside the backup folder. As shown in the above picture,i can delete "C:\Windows\win.ini".
you can read this： https://portswigger.net/web-security/file-path-traversal

danpros commented on May 13, 2021 — Owner

Thanks **@wszdhf** for the report and **@ProjectPatatoe** for the pull request.

wszdhf closed this as completed on Sep 29

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants