New issue

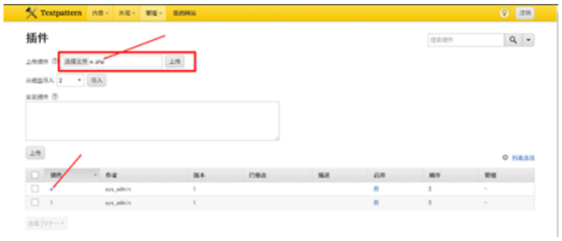
Jump to bottom

Hi I found two loopholes. #1655

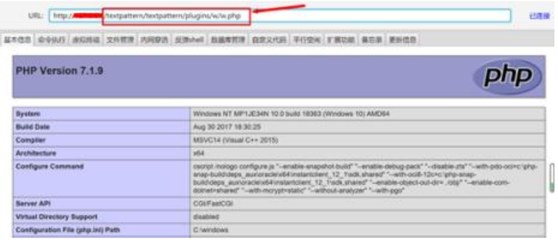
Closed · **reasdf** opened this issue on Mar 18, 2021 · 3 comments

reasdf commented on Mar 18, 2021

Hi I found two loopholes.
In version V4.8.4。
The first one: The location where the plug-in is uploaded in the background without any security verification. You can upload Trojan files to obtain system permissions.
The second one: the storage type xss exists in the place where the article is written.
Next are the details of the exploit:
The first vulnerability: Because the backend login location does not have a verification code and no lock policy is set, if an attacker enters the backend through brute force cracking, the attacker can upload the php Trojan file, because the file path after saving is regular , So the attacker can connect to the Trojan horse file through a hacker tool to obtain system permissions.



Access to Trojan files to verify that the vulnerability exists.

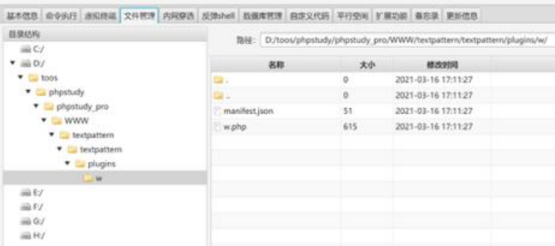


URL: http://[redacted]/textpattern/textpattern/plugins/w/w.php

PHP Version 7.1.9

System	Windows NT MP1JE34N 10.0 build 18363 (Windows 10) AMD64
Build Date	Aug 30 2017 18:30:25
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\windows

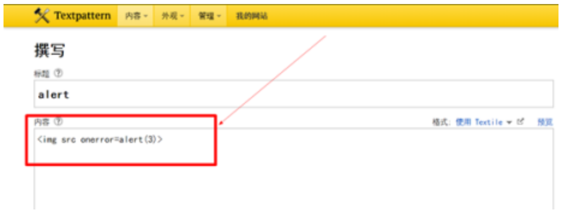
Hacking tools connect to Trojan files to obtain system permissions.



路径: D:/tools/phpstudy/phpstudy_pro/WWW/textpattern/textpattern/plugins/w/

名称	大小	修改时间
.	0	2021-03-16 17:11:27
..	0	2021-03-16 17:11:27
manifest.json	51	2021-03-16 17:11:27
w.php	615	2021-03-16 17:11:27

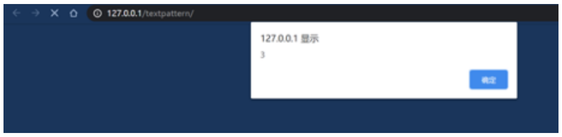
The second vulnerability: If a low-privilege user uses the vulnerability to write malicious code and publish it, all people who view this article will be attacked. He can obtain the administrator’s cookie information, and the administrator’s cookie can be used directly by the administrator. Log in to the background system with permission. You can also continue to exploit the first vulnerability after logging in.



标题
alert

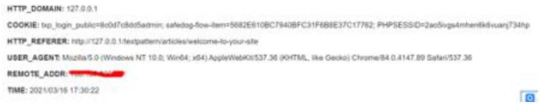
内容
<img src onerror=alert(3)>

The administrator's access to the article triggers a pop-up window to verify that the vulnerability exists.



127.0.0.1 显示
3

The attacker obtains the administrator cookie.



```
HTTP_DOMAIN: 127.0.0.1
COOKIE: txp_login_public=8c0d7c8dd5admin; safedog-flow-item=5682E610BC7940BFC31F6B8E37C17762; PHPSESSID=2ao5ivgs4mhen6k6vuanj734hp
HTTP_REFERER: http://127.0.0.1/textpattern/articles/welcome-to-your-site
USER_AGENT Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36
REMOTE_ADDR: [redacted]
TIME: 2021/03/16 17:30:22
```

Repair suggestions:
The first vulnerability: verify the format of the uploaded file, verify the content of the file, and set the uploaded file name to random.
The second vulnerability: html entity conversion or filtering of sensitive words input by the user, such as <, >,', ", script.

petecooper commented on Mar 21, 2021 Member

Hi **@reasdf** - thanks for your report. We have discussed your issue internally within the development team, please find a summary / response below.

Your first observation relating to plugin upload has been addressed in the upcoming Textpattern 4.9 release, and we are researching possible ways to relocate the plugin directory without breaking existing installations. There are existing user privilege levels already in place that restrict uploading and activating plugins, so only trusted higher-privilege users can perform this action. Randomising plugin names would not be appropriate in this case as it would break existing Textpattern installations.

Your second observation relating to article body content is something we receive communications about from time to time. We have summarised our stance here:

https://textpattern.com/weblog/security-considerations-and-user-privileges-in-textpattern#exploit1

Note that again this is partially a user privilege / trust issue. Lower tier users have fewer user privileges, and any instance of Textpattern should be secured with passwords according to the organisation's guidelines. Administrators should ensure *any* system they maintain is securely managed, including password strength & rotation, user privilege sanity checking and other industry standard security practices for self-hosted software.

I will leave this issue open for a short while for any other team members to comment on.

We appreciate your communication. Please refer to https://textpattern.com/contact for the preferred way of contacting us regarding vulnerabilities, loopholes and similar security issues.

Thank you, and best wishes.

petecooper closed this as completed on Mar 23, 2021

abergmann commented on Apr 16, 2021

CVE-2021-30209 was assigned to this issue.

petecooper commented on Apr 16, 2021 Member

Thanks for the notification, **@abergmann**.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants