

# Telspace Africa, The Blog

Hackers for hire

Thursday, July 9, 2020

## phpList – CVE-2020-15072 & CVE-2020-15073 – Story Time

phpList is currently used in 73 countries and is a popular choice for sending email newsletters, marketing campaigns and announcements. It is accessible via web browsers and is Open Source (<https://www.phplist.org>), however a paid for version also exists as a service via <https://www.phplist.com>.

Given its wide use / adoption, I decided to take a look at phpList recently, in order to give back to the Open Source community.

I would also like to give credit to phpList for responding and patching very quickly, especially to Suela at phpList. A new version of the application is now available for download.

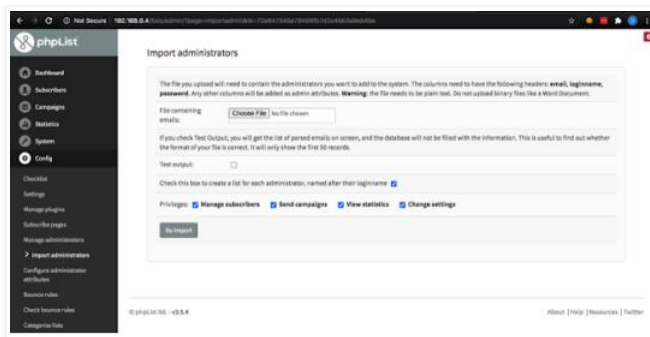
You can browse all the fixes, comments and patching by going to the following URLs:

- <https://discuss.phplist.org/t/phplist-3-5-5-has-been-released/6377>
- <https://www.phplist.org/newslist/phplist-3-5-5-release-notes/>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15072>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15073>

A walkthrough of the 2 identified vulnerabilities is given below:

### 1.) Code Injection via "Import administrators"

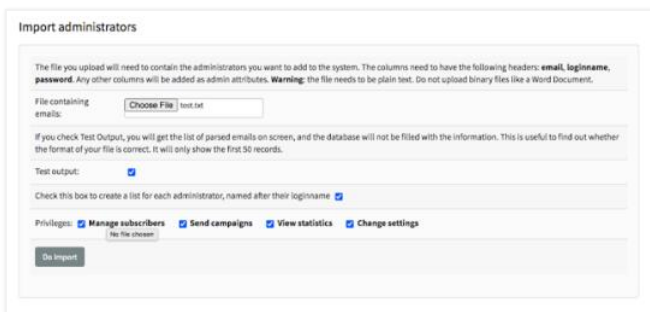
1.1) Click on "Config" then "Import administrators"



1.2) Edit a txt file to include basic headers and test (offline) as follows:

```
hacktobasics:Downloads dc$ cat test.txt
email      loginname    password
test@test.com <script>alert(document.cookie)</script> test
hacktobasics:Downloads dc$
```

1.3) Click on "Choose File" and select the text file.



1.4) Click "Do Import"

Code Injection Triggered (not stored)



www.telspace.africa

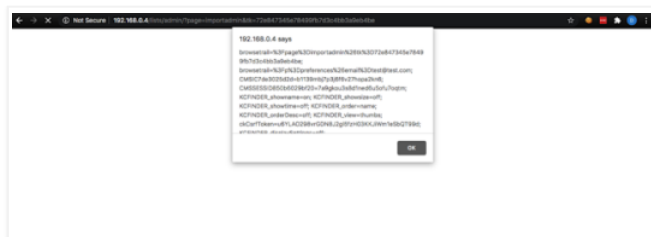
#### Blog Archive

- 2022 (2)
- 2021 (2)
- ▼ 2020 (8)
  - December (1)
  - ▼ July (1)
    - phpList – CVE-2020-15072 & CVE-2020-15073 – Story ...
- June (1)
- May (2)
- March (1)
- February (1)
- January (1)

- 2019 (8)
- 2018 (3)
- 2017 (7)
- 2016 (5)
- 2015 (7)
- 2014 (14)
- 2013 (15)
- 2012 (5)
- 2011 (11)
- 2010 (15)
- 2009 (10)
- 2008 (26)

#### Subscribe now!

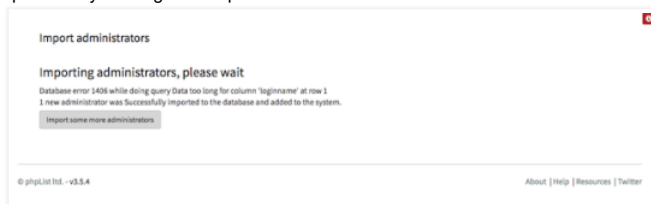
- Posts
- Comments



1.5) Go back to "Import administrators"

1.6) Untick "Test output:"

1.7) Click "Do Import" and you will get an import database error.



1.8) Edit the same text file and add another user as follows:

```
hacktobasics:Downloads dc$ cat test.txt
email loginname password
test@test.com <script>alert(document.cookie)</script> test
test2@test.com <script>alert('hi')</script> test
hacktobasics:Downloads dc$
```

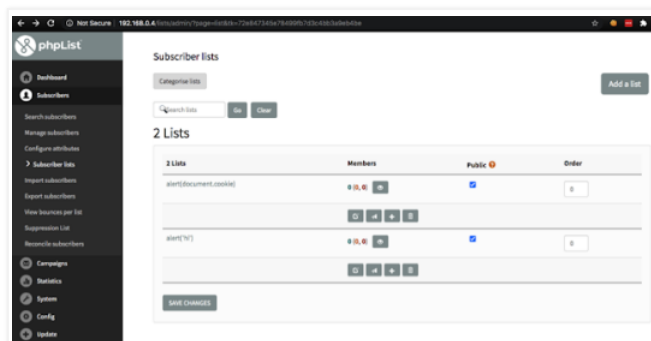
1.9) Go back to "Import administrators"

1.10) Click on "Choose File" and choose the text file.

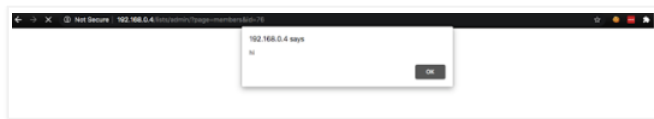
1.11) Untick "Test output:"

1.12) Click "Do Import" and you will get more import database errors

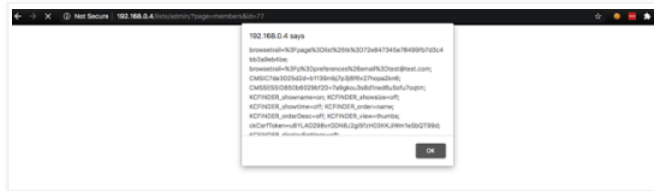
1.13) Browse to "Subscribers" then "Subscriber Lists"



1.14) Click on the first one and you'll get a "hi" popup:



1.15) Go back and click on the second one and you'll get a cookie.



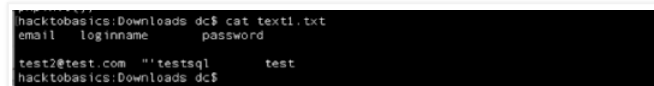
## 2.) Error based SQL Injection via "Import administrators"

2.1) Click on "Config" then "Import administrators"

2.2) Edit a txt file to include basic headers and text (offline) as follows

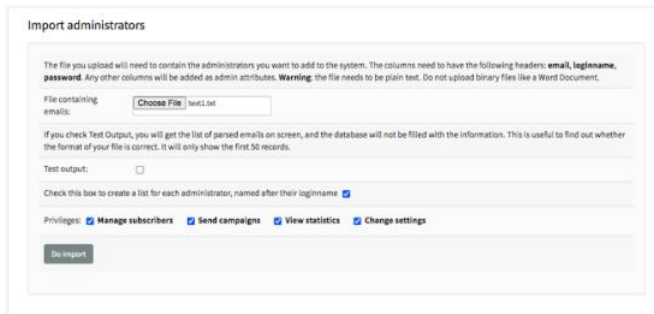
email loginname password

test2@test.com "'testsql test



2.3) Untick "Test output:"

2.4) Click on "Choose File" and choose the text file.



2.5) Click "Do Import" - you'll see the Error Based SQL injection.



Creative Commons - Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) - <https://creativecommons.org/licenses/by-sa/4.0/>

at Thursday, July 09, 2020

Labels: 2020, code injection, CVE-2020-15072, CVE-2020-15073, phpList, security advisory, sql injection

### 1 comment:

Dane said...

Keep up the great work Telspace!

July 11, 2020 at 10:12 PM

[Post a Comment](#)

[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)