Path Traversal in filegator/filegator

0

✓ Valid Reported on May 22nd 2022

🔒 Requirements

Privilege: User

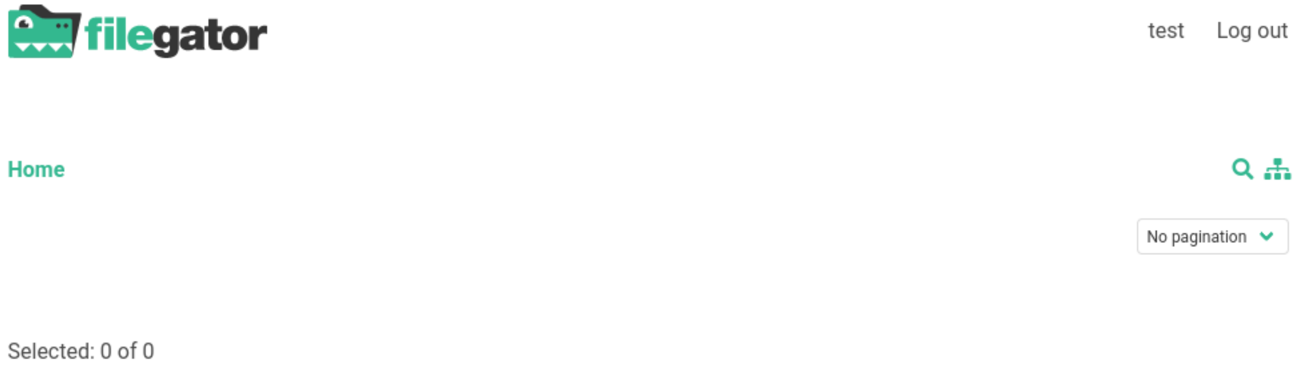
📝 Description

File path isn't properly sanitized and allow `..\` .

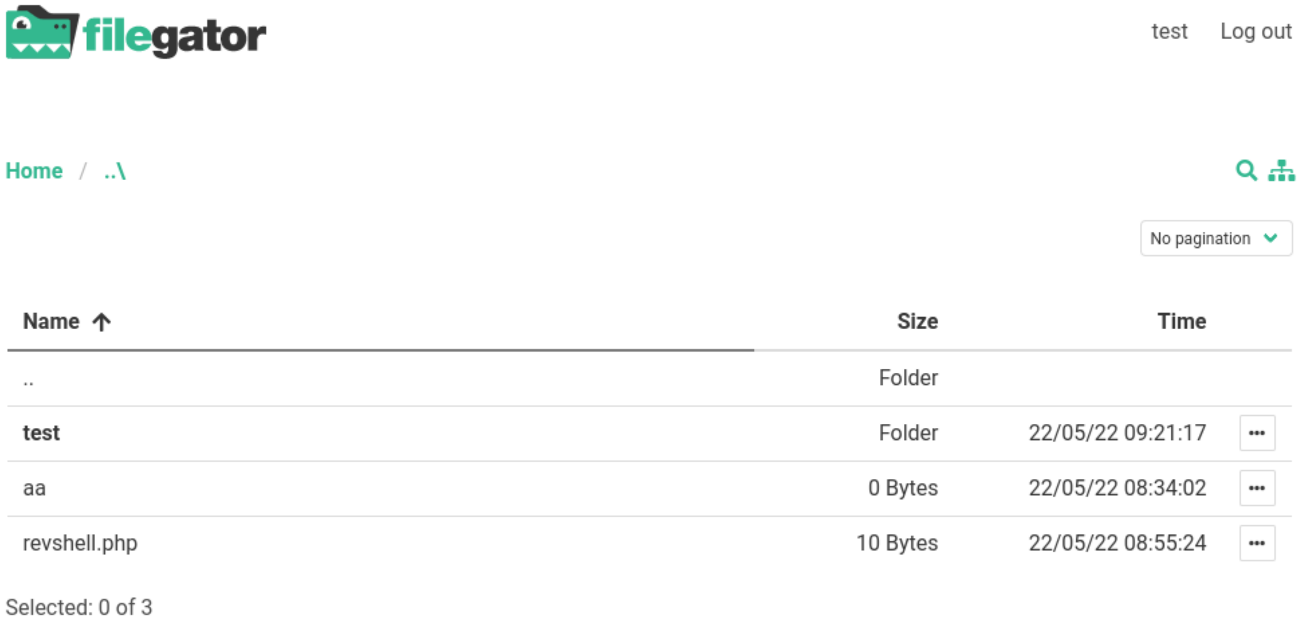
🕵️ Proof of Concept

Listing other user folder content

First, create a user with `Read` privilege and with specific home folder like `/test` . Then, Connect to his account and access the home page `http://localhost:8080/` :



From this, change folder using path traversal via `cd` parameter:



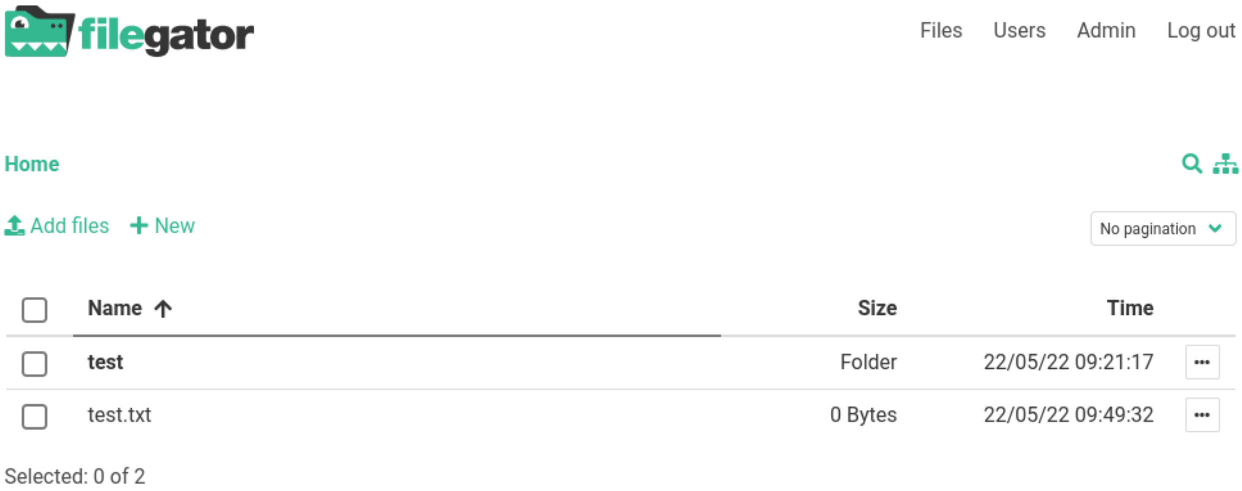
Name ↑	Size	Time	
..	Folder		
test	Folder	22/05/22 09:21:17	···
aa	0 Bytes	22/05/22 08:34:02	···
revshell.php	10 Bytes	22/05/22 08:55:24	···

Selected: 0 of 3

As you can see, we are able to view folder content.

Write file

First, create a user with `Read` and `Write` privileges and with specific home folder like `/test`. Then, Connect to his account and access the home page `http://localhost:8080/`. From here create a new file named `..\test.txt` and then go to the root folder with another account:



□	Name ↑	Size	Time	
□	**test**	Folder	22/05/22 09:21:17	···
□	test.txt	0 Bytes	22/05/22 09:49:32	···

Selected: 0 of 2

You will see that the file was created outside of the test user's folder limitation.
PS: Note that the same could be done to all features in the file `https://github.com/filegator/filegator/blob/642bb273334207359166d48b6c719a89e98a0676/backend/Controllers/FileController.php` due to:

```
$this->separator
```

Impact

An attacker can use path traversal to:
List files in folder that he shouldn't access.
Write|Move|Copy|... files in a folder that the current user hasn't the rights for.

References

- CWE 35

CVE
CVE-2022-1850
(Published)

Vulnerability Type
CWE-22: Path Traversal

Severity
Medium (5.4)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Mizu
@kevin-mizu
pro ⌄

Fixed by

Milos Stojanovic
@alcalbg
maintainer

Chat with us

This report was seen 684 times.

We are processing your report and will contact the **filegator** team within 24 hours. 6 months ago

We have contacted a member of the **filegator** team and are waiting to hear back 6 months ago

Milos Stojanovic validated this vulnerability 6 months ago

Mizu has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Milos Stojanovic marked this as fixed in **7.8.0** with commit **6e2b68** 6 months ago

Milos Stojanovic has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

part of 418sec

company

about

team

Chat with us