



# 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
 <a href="#">images</a>		
 <a href="#">README.md</a>		

 [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 unauthentica 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.

The screenshot shows the Ovidentia web application interface. The browser's address bar displays the URL `/index.php?tg=admfms&idx=list`. The page header includes the Ovidentia logo and the text "Then Comes Gamma." Below the header, a navigation bar shows the path "Complete site » Administration » Ovidentia functions » File manager". The main content area is titled "File manager" and contains a table with the following columns: "Folders", "Access", "Notify", "Enabled", "Versioning", and "Hidden". The table lists the "uploads" folder with a "Rights" column containing a checkbox. Below the table is an "Update" button. The left sidebar contains a menu with sections for "Administration" (including "Currently you administer Complete site", "Add/remove programs", "Approbation schemas", "Articles", "Calendar", "Charts", "Delegation", "Directories", "FAQ", "File manager", "Forums", "Groups", "Mail", "Sections", "Sites", "Statistics", "Task Manager", "Thesaurus", "Users", "Vacations") and "Forums" (including "List of forums", "evil", "Waiting posts"). The right sidebar shows a calendar for "October 2021 W.43" and a "Users section" indicating the user is logged in as "Administrator".

Then Comes Gamma.

Complete site » Administration » Ovidentia functions » File manager

ADMINISTRATOR

Folders Add Display Purge trashes

Administration

Currently you administer Complete site

Add/remove programs

Approbation schemas

Articles

Calendar

Charts

Delegation

Directories

FAQ

File manager

Forums

Groups

Mail

Sections

Sites

Statistics

Task Manager

Thesaurus

Users

Vacations

Forums

List of forums

evil

Waiting posts

File manager

Folders	Access	Notify	Enabled	Versioning	Hidden
uploads	Rights	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Update

Webmaster - Powered by Ovidentia, Groupware Portal  
Ovidentia is a registered trademark by Cantico.

October 2021 W.43

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Users section

You are logged on as Administrator

Approbations

Articles management

Calendar

Contacts

File manager

Forums

Notes

Options

Since your last connection:

0 Article(s)

0 Comment(s)

0 Reply(ies)

0 File(s)

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.

The screenshot shows a web browser window with multiple tabs. The active tab is 'Ovidentia', displaying the application's interface. The URL bar shows 'index.php?tg=admfm&idx=rights&fid=3'. The page title is 'Then Comes Gamma.' and the breadcrumb trail is 'Complete site > Administration > Ovidentia functions > File manager'. The user is logged in as 'ADMINISTRATOR'.

The main content area is titled 'Rights of directory uploads' and contains several sections with lock icons, indicating permissions:

- Upload**: Administrators  
And the group children
- Download**
- Update**
- Manage**
- Who is notified when a new file is uploaded or updated?**
- Who can unzip archives?**

A 'Save' button is located at the bottom of the configuration area.

The left sidebar contains a navigation menu with the following items:

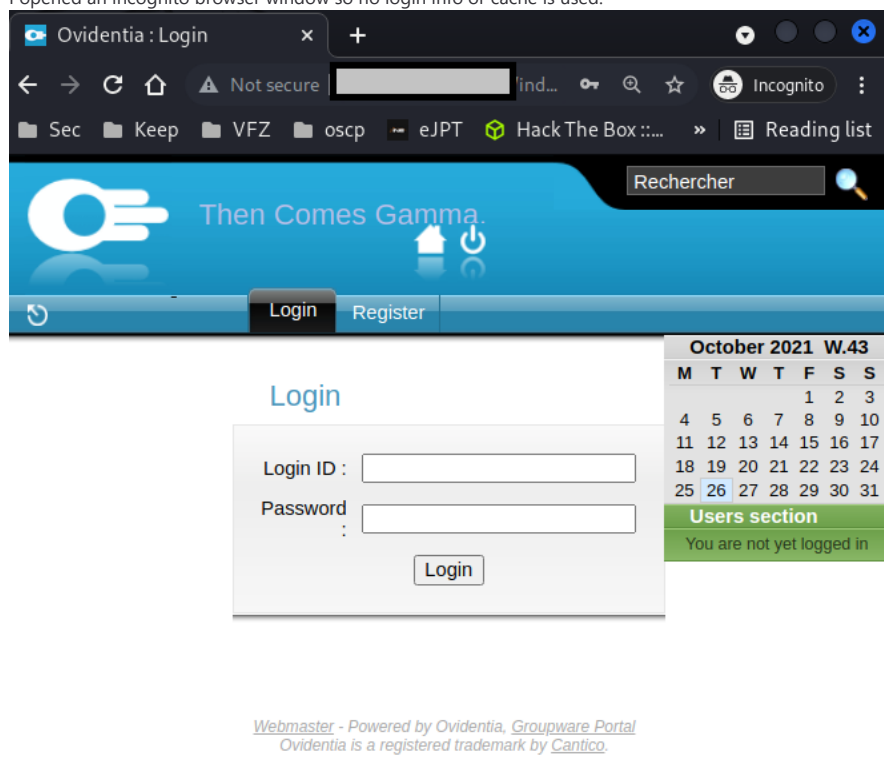
- Administration
  - Currently you administer Complete site
  - Add/remove programs
  - Approbation schemas
  - Articles
  - Calendar
  - Charts
  - Delegation
  - Directories
  - FAQ
  - File manager
  - Forums
  - Groups
  - Mail
  - Sections
  - Sites
  - Statistics
  - Task Manager
  - Thesaurus
  - Users
  - Vacations
- Forums
  - List of forums
  - evil ⚠
  - Waiting posts

The right sidebar shows a calendar for October 2021 (W.43) and a 'Users section' with the following information:

- You are logged on as Administrator
- Approbations
- Articles management
- Calendar
- Contacts
- File manager
- Forums
- Notes
- Options
- Since your last connection:
- 0 Article(s)
- 0 Comment(s)
- 0 Reply(ies)
- 0 File(s)

The footer text reads: 'Webmaster - Powered by Ovidentia, Groupware Portal'.

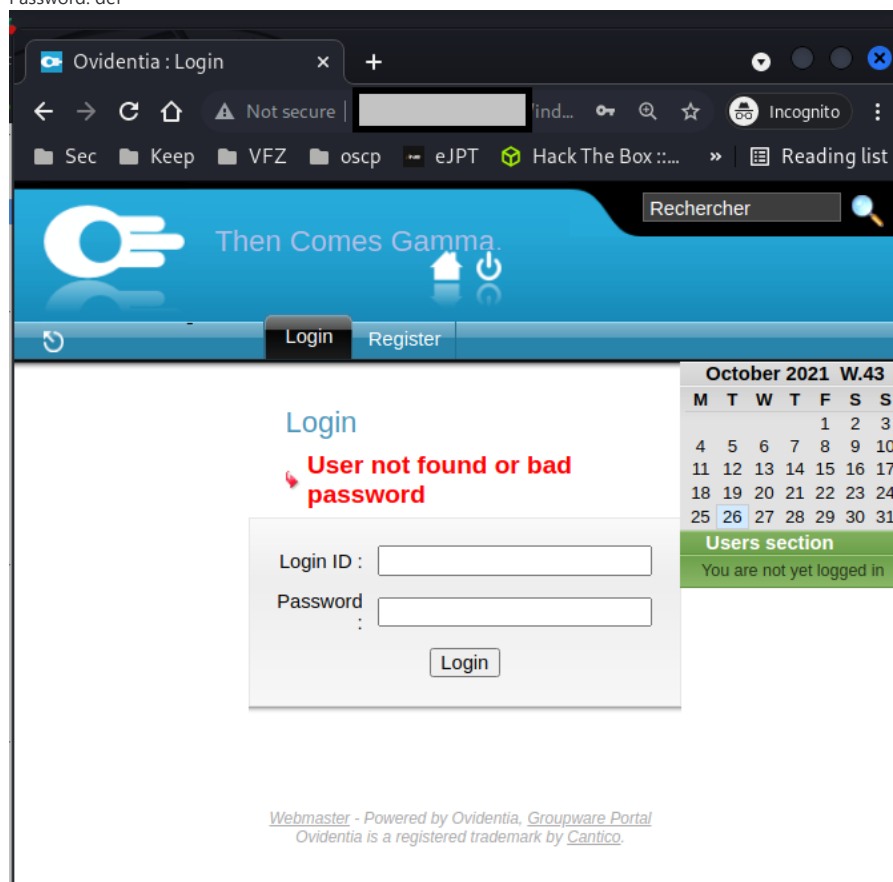
I opened an incognito browser window so no login info or cache is used.



To verify I entered wrong login credentials.

Login ID: abc

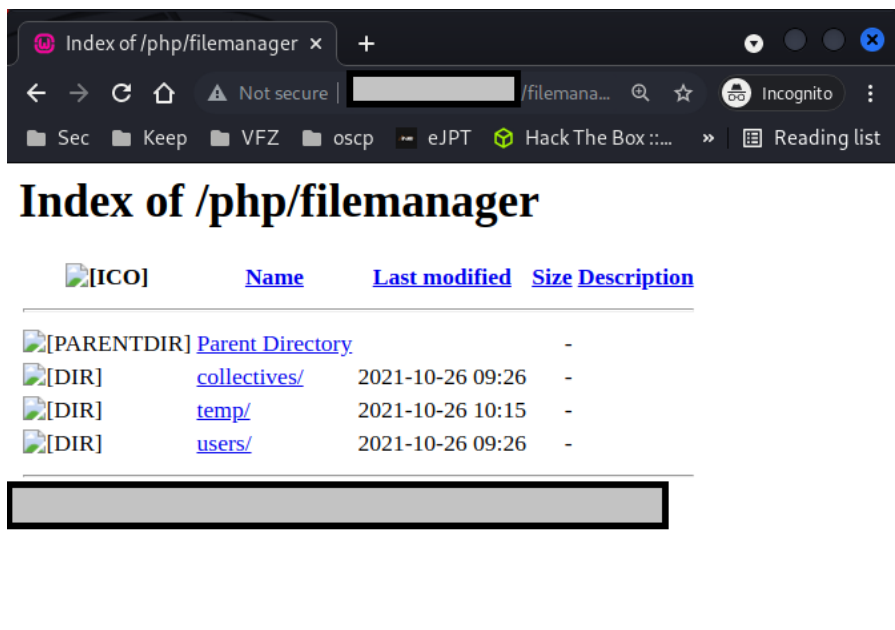
Password: def



Next, using the incognito browser window, I navigated to the Ovidentia Filemanager directory where the uploads are stored.

url: <http://IP:8080/php/filemanager>

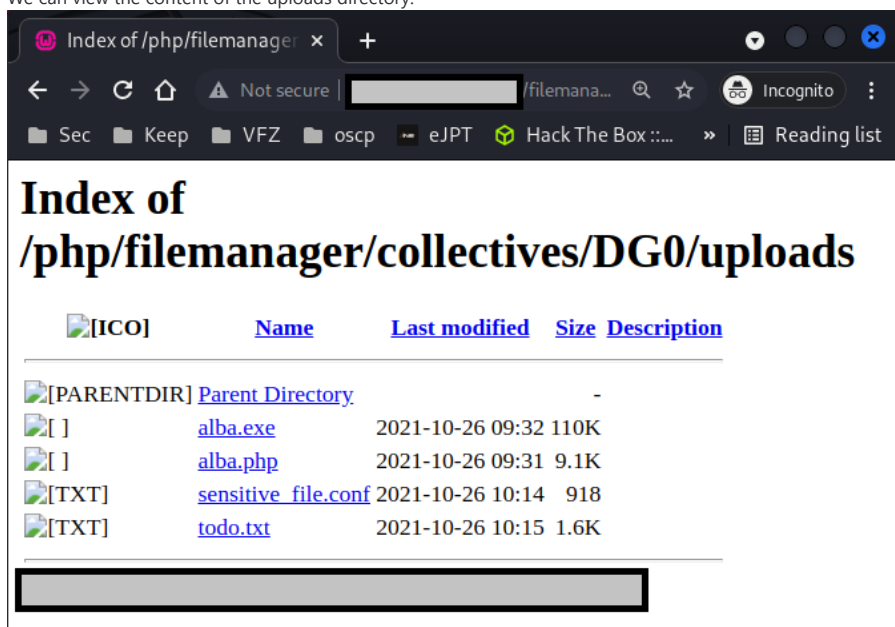
As can be seen in the screenshot below we have read access to the filemanager directory.



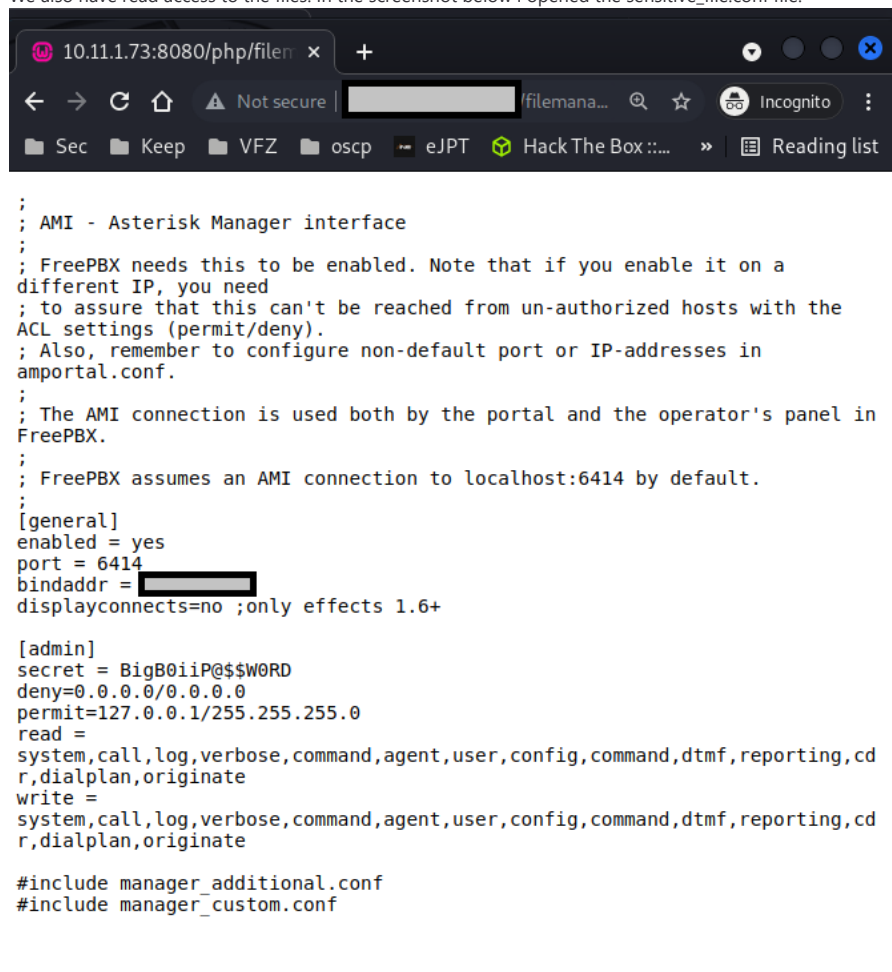
In the filemanager I navigated to:

<http://IP:8080/php/filemanager/collectives/DG0/uploads>

We can view the content of the uploads directory.



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



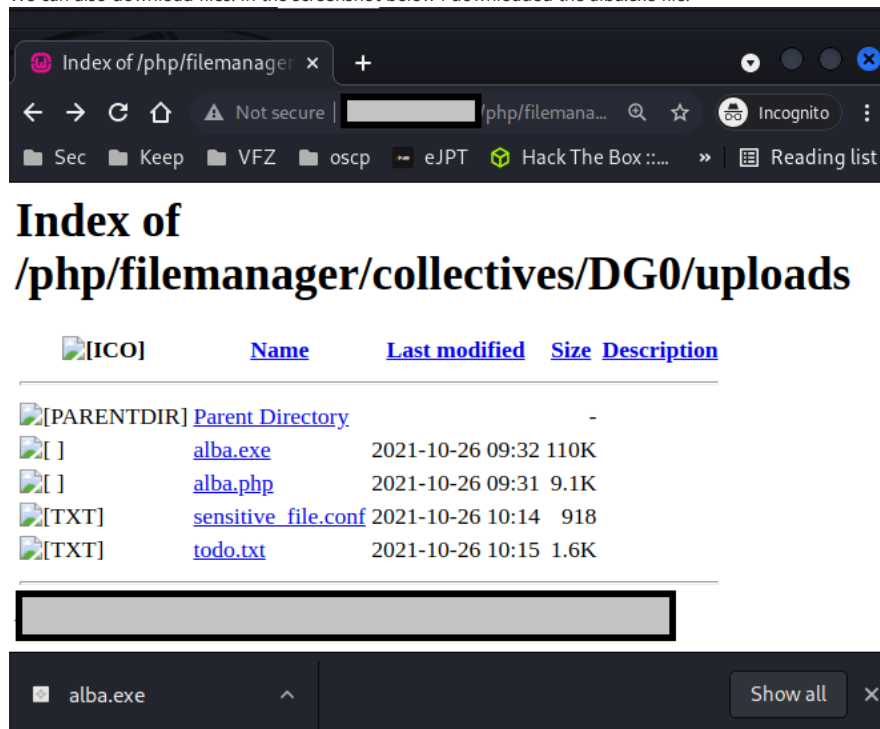
The screenshot shows a web browser window with the address bar displaying '10.11.1.73:8080/php/fileman...'. The browser is in Incognito mode. The main content area displays the configuration file 'sensitive\_file.conf'. The file contains settings for the Asterisk Manager interface (AMI), including general settings like 'enabled = yes', 'port = 6414', and 'bindaddr = [redacted]'. It also includes an '[admin]' section with 'secret = BigB0iiP0\$\$WORD', 'deny' and 'permit' rules, and 'read' and 'write' permissions. At the bottom, it includes '#include manager\_additional.conf' and '#include manager\_custom.conf'.

```
; 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 = BigB0iiP0$$WORD
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


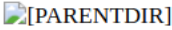




#include manager_additional.conf
#include manager_custom.conf
```



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



The screenshot shows a web browser window displaying a file index for the directory '/php/filemanager/collectives/DG0/uploads'. The index table lists files including 'alba.exe', 'alba.php', 'sensitive\_file.conf', and 'todo.txt'. Below the index, a download bar is visible, showing a file named 'alba.exe' with a download icon and a 'Show all' button.

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

	Name	Last modified	Size	Description
	<a href="#">Parent Directory</a>	-		
	<a href="#">alba.exe</a>	2021-10-26 09:32	110K	
	<a href="#">alba.php</a>	2021-10-26 09:31	9.1K	
	<a href="#">sensitive_file.conf</a>	2021-10-26 10:14	918	
	<a href="#">todo.txt</a>	2021-10-26 10:15	1.6K	

 alba.exe  Show all ×

## 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.