t

Clear Text Passwords in Files  
(Orange)

Text

Description automatically generated

Summary

Target Address: 172.26.1.229

Target Account: [Brailee.ogdenz@windomain.local](mailto:Brailee.ogdenz@windomain.local)

Account Found: qd Password: qdDBPasswrod7

Target OS: qdpm Targeted Files: databases.yml

Tools: SearchExploit, Python Script,

In the login, to exploit furthermore, we can see the qdpM 9.1 for the php server, we can see the website software version, so we can google that it has vulnerability about the web build

Graphical user interface, application

Description automatically generated

We can search any exploit and payloads can be found in kali linux. I found the version match qdPM 9.1 match in the kali linux exploit database. So we can use cross-site scripting that can be found in Google.

Graphical user interface, application

Description automatically generated

So I use the python script I found online, and make a the script to execute cross-site scripting to create a backdoor.

Text

Description automatically generated

Executing the python script by implementing the credential I found from previous attack. As long as I upload the script, it creates a link which is the backdoor.

Text

Description automatically generated with medium confidence

After pasting the url link, by modefing the command line after the equal sign, we can execute the commands to the server by using the back door like.

A screenshot of a computer

Description automatically generated with medium confidence

As we can see, we can execute “cat /etc/passwd” to find out more about users and so on.

Graphical user interface, text, application

Description automatically generated

Add “cat /var/www/html/core/config/databases.yml” after cmd= to file the target file

Graphical user interface, text, application

Description automatically generated

Use “cat” to display the content in the target file.

Graphical user interface, text, application

Description automatically generated

Add the “view-source:” in front of the url, this will allow the content of the target file displays the clear password, and the password is ‘qdDBPasswrod7’

Graphical user interface, text, application

Description automatically generated