INFO:

given admin login screen

Process of Solving:

found <form action="index.php?file=login.php" method="post"> in source code, and saw file variable used.
added ?file=password.php to URL and was given:
administrator:3e0f84

Writeup:

Congratulations on beating the mission again.
No credits were rewarded, but it's good to see you're testing your skills again.
Return to Enigma Main

Way to go! This challenge brought to light the basis of all exploits: using the script against itself. When you attempt to log in, you get an error. Remember what we learned earlier? Always pay attention to the error messages. In this error, we see that it is trying to compare our information given with something stored in password.php. But what happened when you tried to view this file? We got told "Access Denied."

To get around this, we had to use the script against itself. You noticed the structure of the URL with its "?file=login.php". Hopefully, you could put the pieces together yourself. By replacing "login.php" with "password.php" we were able to view the contents of the file.

But why? Why were we capable viewing the contents the way we did but not directly like we tried first? The reason could be one of two possibilities. The file \"password.php\" may have had a block on it preventing it from being viewed directly. This can be done easily with one line of PHP.

The other possibility is that the file was restricted to everybody but the server. When we used the script to view the file, it may have appeared that the web server itself was viewing the file, not us.