

Realistic

PRACTICAL WORK 4

Table of Contents

I. PyRat Encheres	2
1. Flag	2
2. Proofs	2
3. Explanation	2
4. Patch	5
5. References	5

I. PyRat Encheres

1. Flag

- roxxor1337kik00_

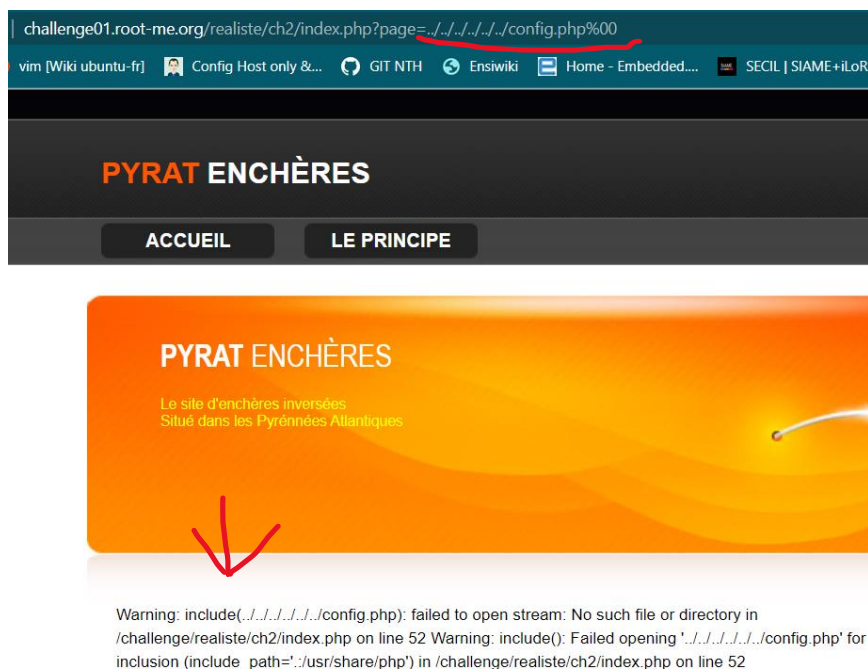
2. Proofs

roxxor1337kik00_

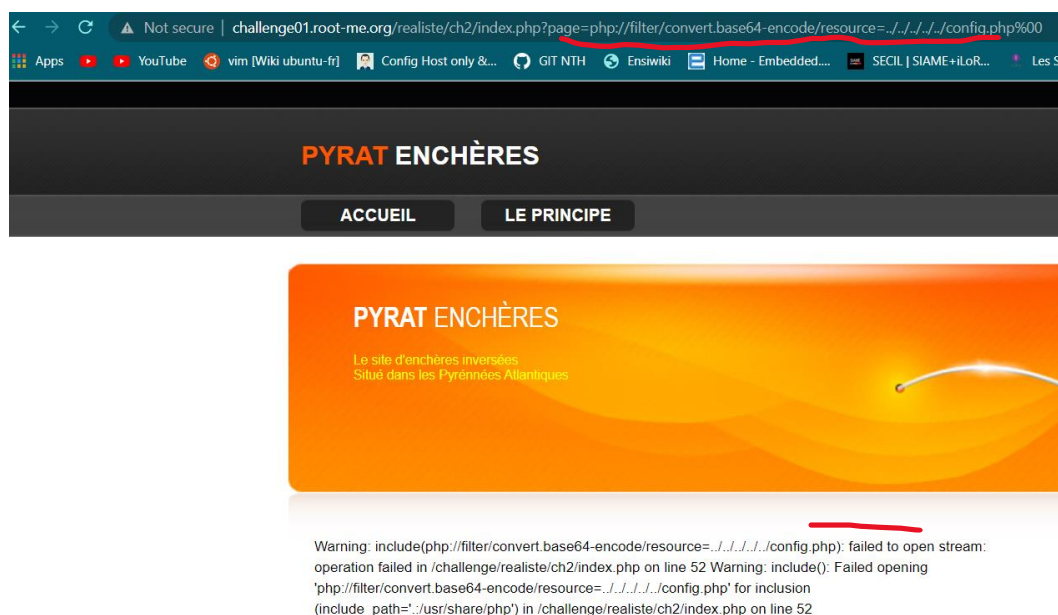
3. Explanation

As the URL ends with “page=encheres”, we thought using a LFI or RFI method. Thus by entering the following new URL, we got that a message that proves the include function is present inside the code.

We add a null byte “%00” to stop the execution of the URL before the “.php” of the include function.



By using a PHP wrapper with the following URL, we still couldn't find the “config.php” source code



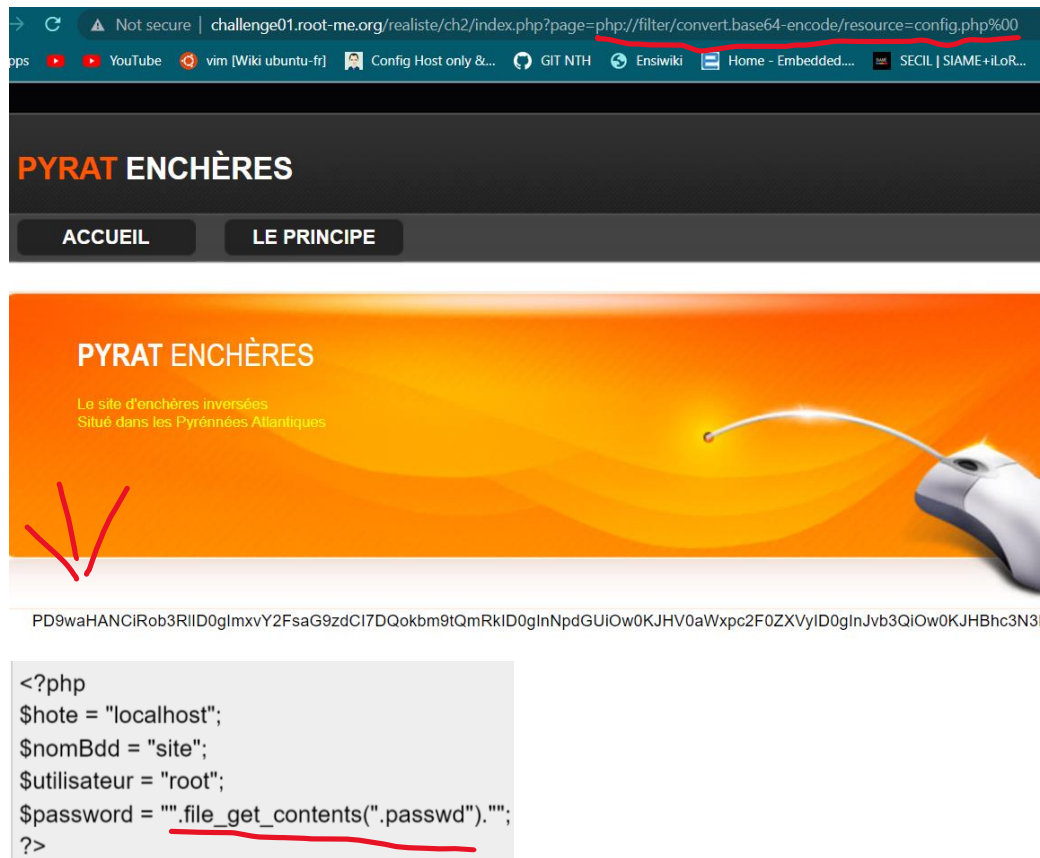
Therefore, we thought we could get more information on the “index.php” source code. Finally we obtained a base64 encoded source code. It seems that we don’t have the access to go anywhere else expect the location of the “index.php” file.



After decoding that line we found that the location of the “config.php” file was on the same location that “index.php” file.

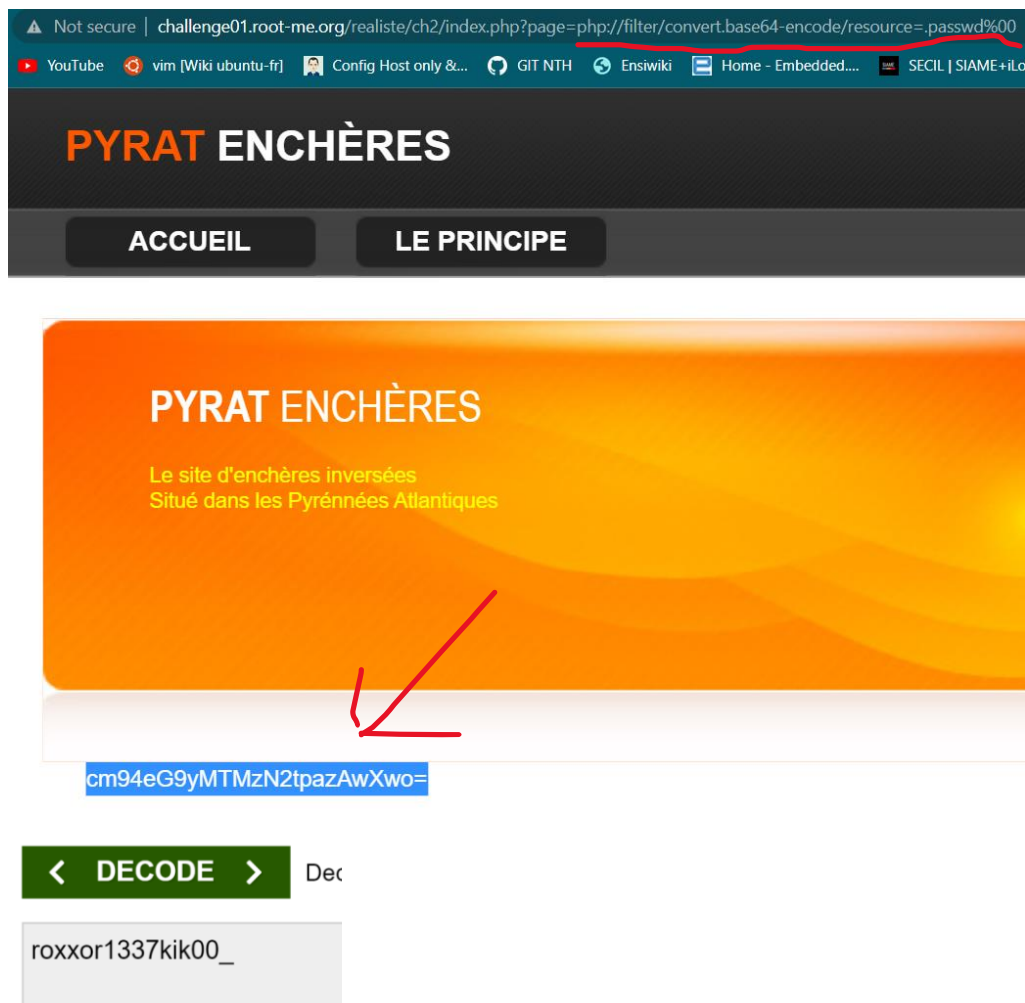
```
include("config.php");  
?>  
<!DOCTYPE html PUBLIC "-//W3
```

Now, by typing the following URL we received a base64 encoded source code of the “config.php” file and after decoding that file, we obtained all sensitive information it contained.



```
<?php
$hote = "localhost";
$nomBdd = "site";
$utilisateur = "root";
$password = "".file_get_contents(".passwd")."";
?>
```

Finally, we repeated the action to get the password with the following URL.



4. Patch

To patch Local File Intrusion we must :

- Secure system files to not make them accessible to unauthorized person
- Apply a white list on allowed characters
- Use input filtering to not make executable characters like "%00"
- Not use the include function
- Not use PHP as the programming language ;)

5. References

PHP wrappers :

<https://www.php.net/manual/en/wrappers.php>

<https://blog.eleven-labs.com/fr/php-stream-wrappers-filters/>

<https://www.youtube.com/watch?v=dK3O3A2-J00>