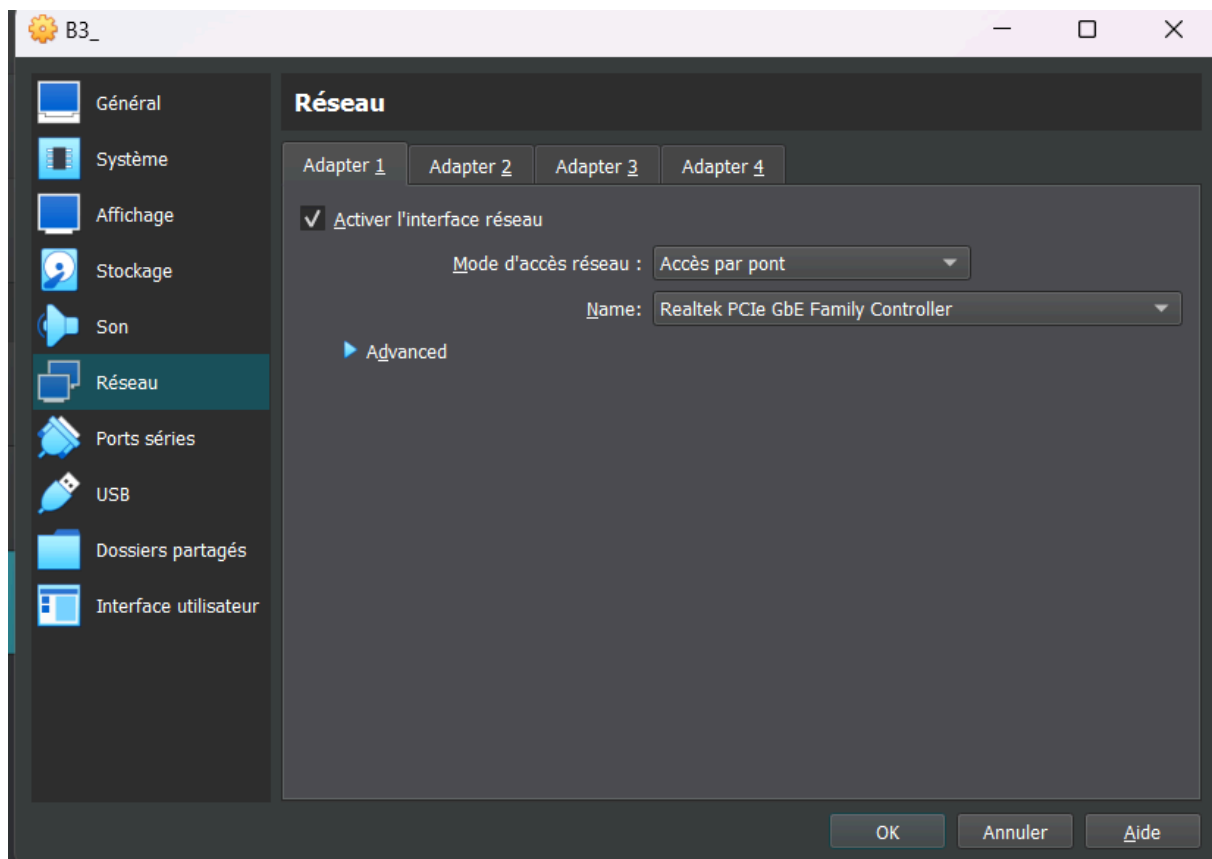
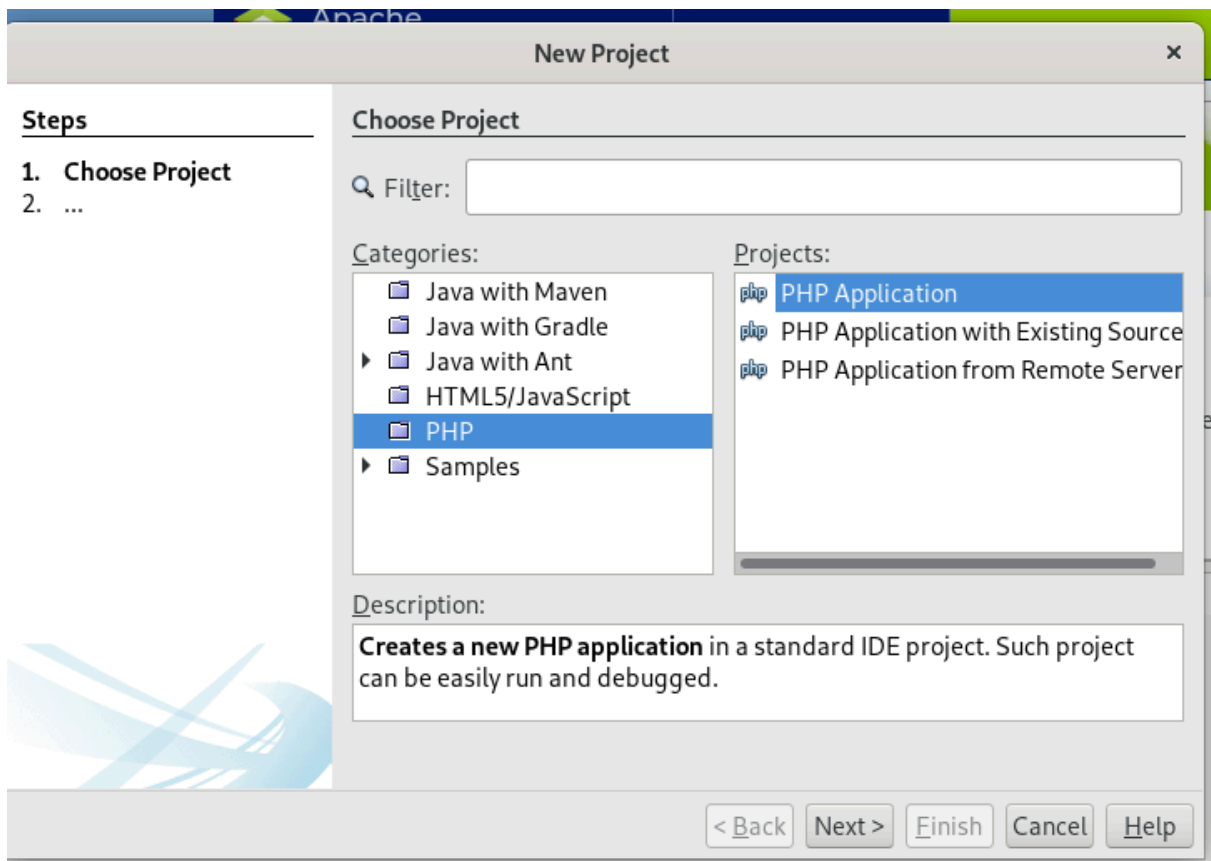
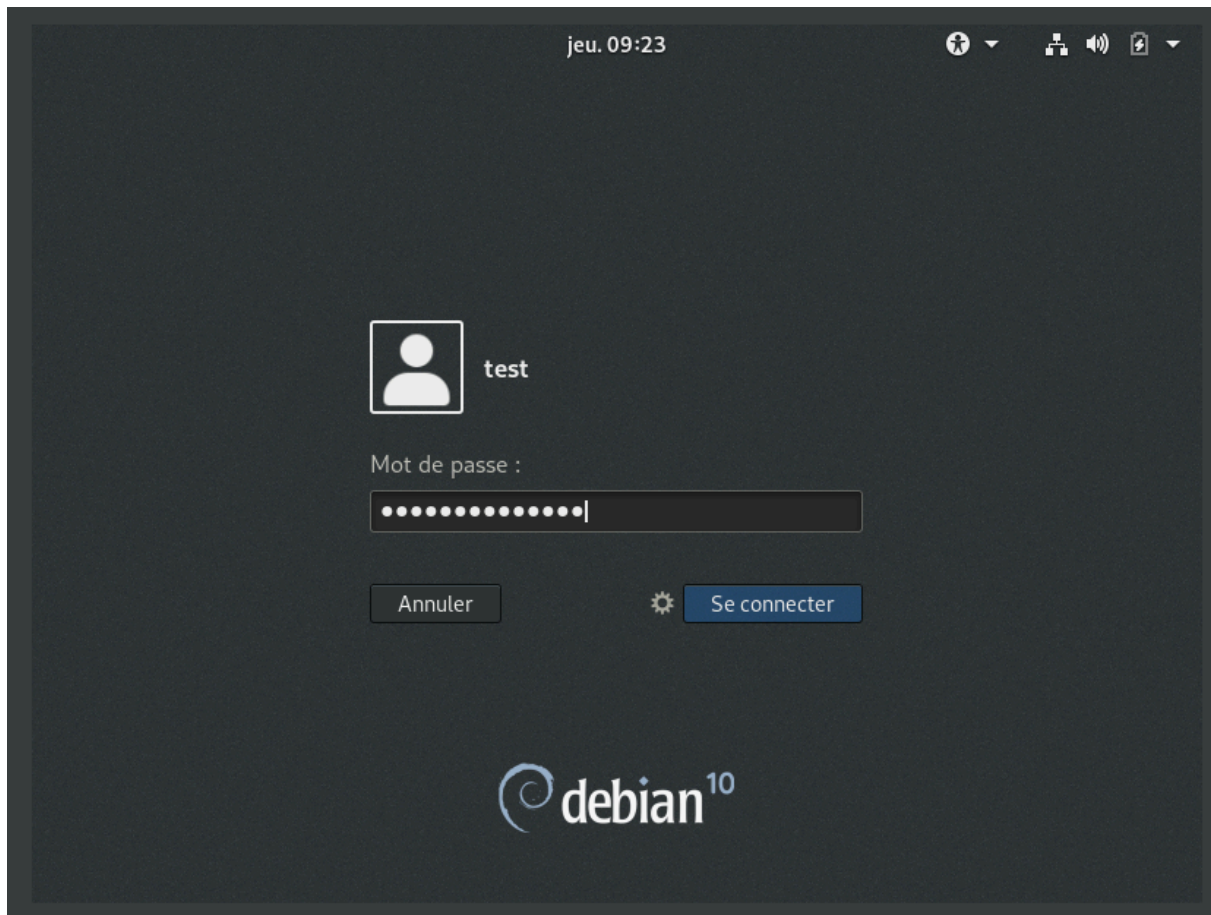


TP IMPLÉMENTATION D'UNE PROTECTION CONTRE CSRF

[SIO1-SLAM-B3-CSRF-SIMPLE-1.pdf](#)





New PHP Project

Steps

1. Choose Project
- 2. Name and Location**
3. Run Configuration
4. PHP Frameworks
5. Composer

Name and Location

Project Name:

Sources Folder:

PHP Version:
PHP version is used only for hints

Default Encoding:

☐ Put NetBeans metadata into a separate directory

Metadata Folder:

New PHP Project

Steps

1. Choose Project
2. Name and Location
- 3. Run Configuration**
4. PHP Frameworks
5. Composer

Run Configuration

Specify the way this project's files will be deployed.
 Configuration settings can be added and modified later in the Project Properties dialog box.

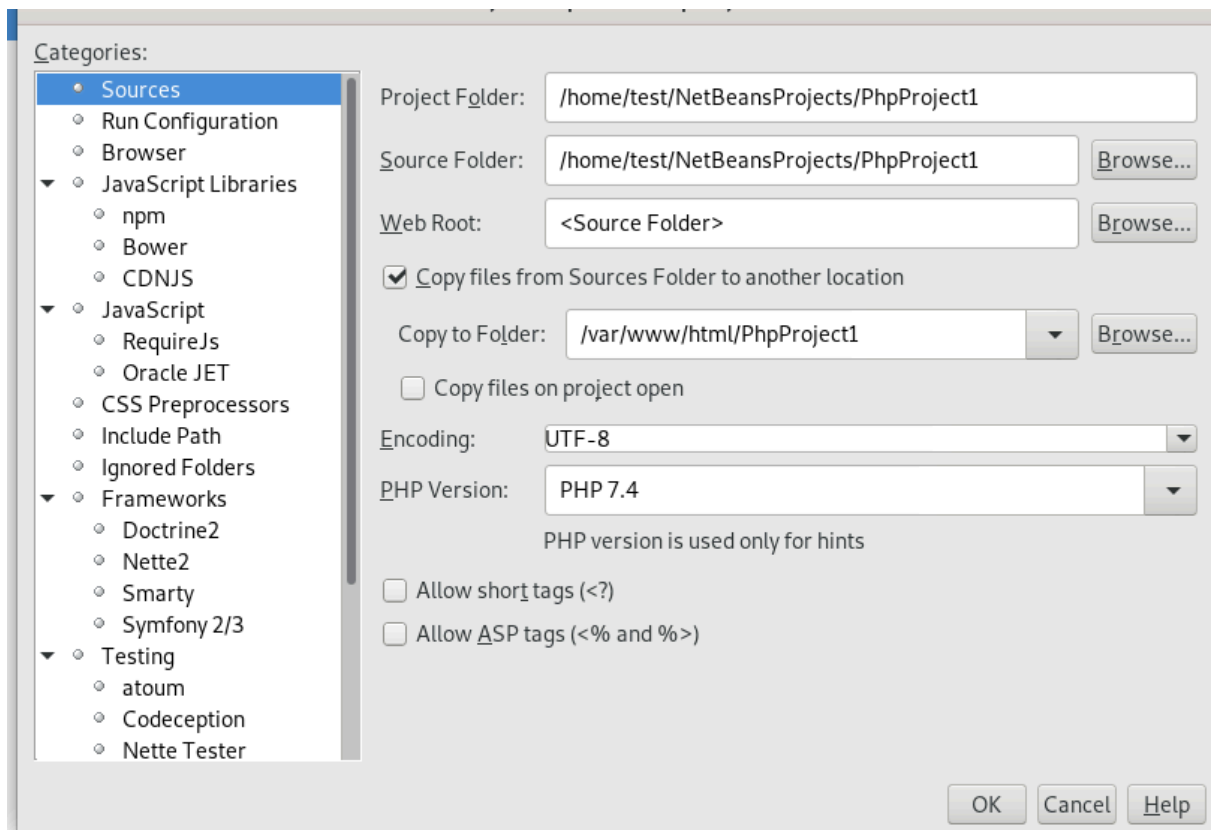
Run As:

Project URL:

☐ Copy files from Sources Folder to another location

Copy to Folder:

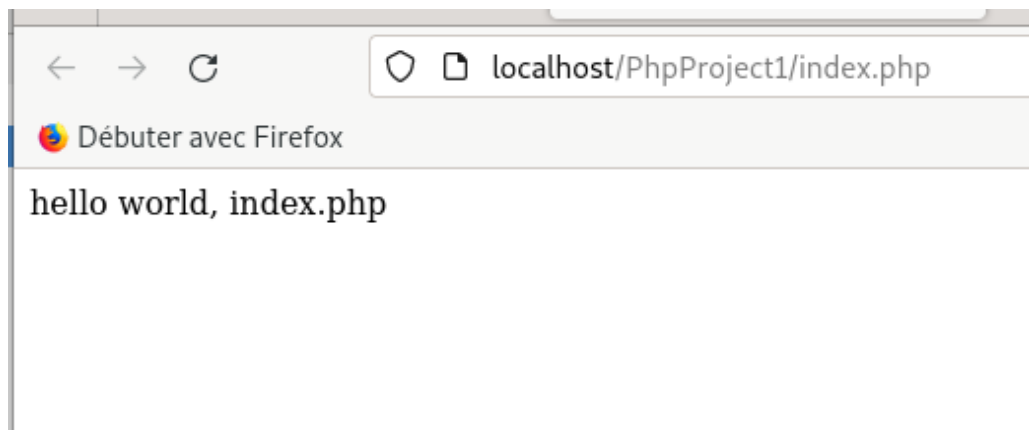
☐ Copy files on project open



```

-->
| <html>
|   <head>
|     <meta charset="UTF-8">
|     <title></title>
|   </head>
|   <body>
|     hello world, index.php
|     <?php
|       // put your code here
|     ?>
|   </body>
| </html>

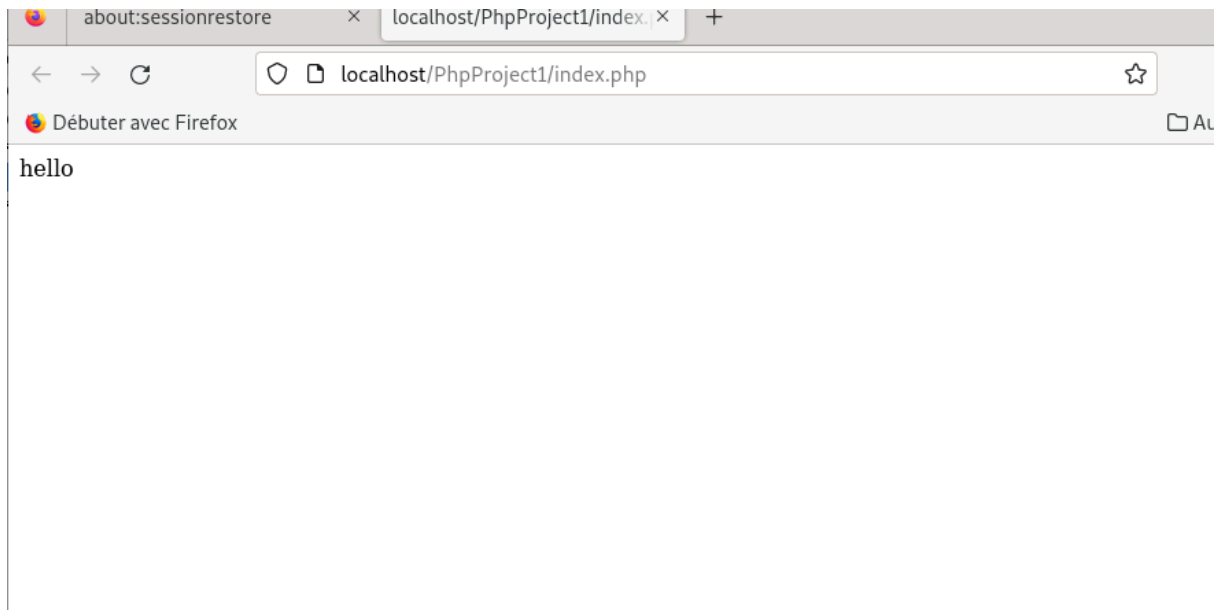
```



```
Fichier  Edition  Affichage  Rechercher  Terminal  Aide
test@debian:~$ ls /var/www/html/
index.html  PhpProject1
test@debian:~$ S
```

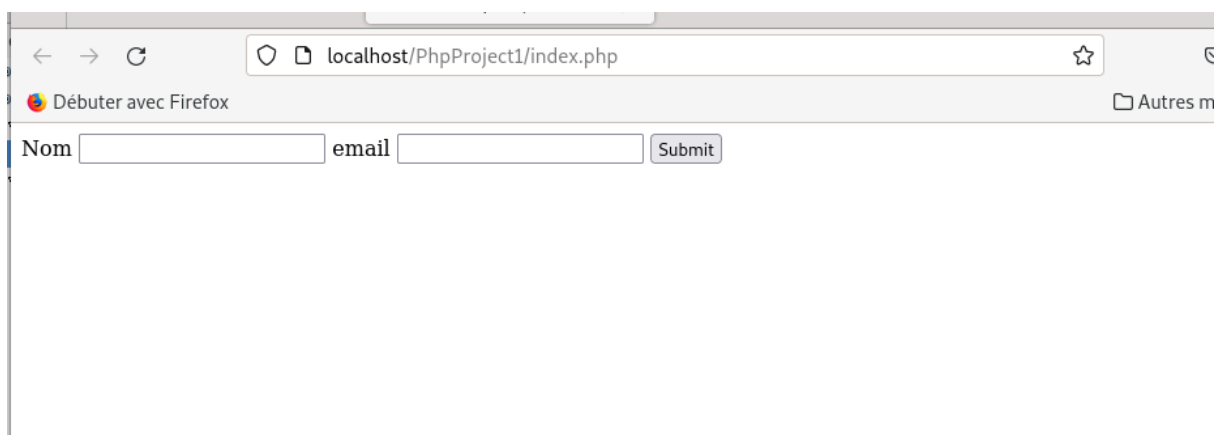
```
--More--^C
test@debian:~$ cd /var/www/html/
test@debian:/var/www/html$ ls
index.html  PhpProject1
test@debian: /var/www/html$ 11
```

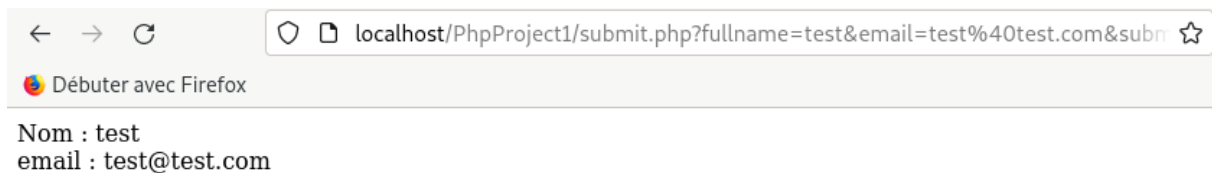
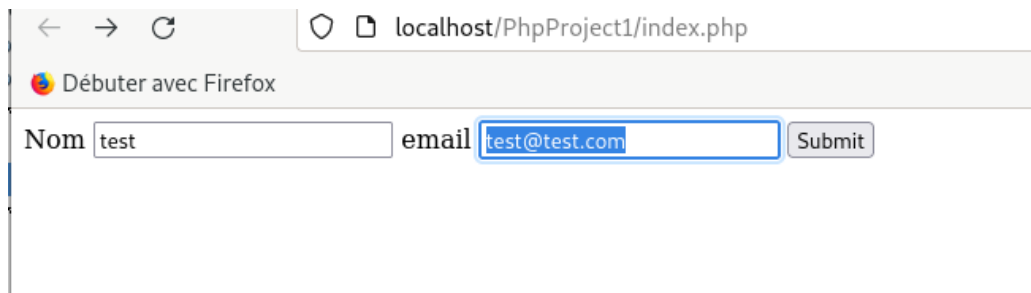
```
6  -->
7  <html>
8  <head>
9      <meta charset="UTF-8">
10     <title></title>
11 </head>
12 <body>
13     <?php
14         echo "hello";
15     ?>
16 </body>
17 </html>
18 |
```



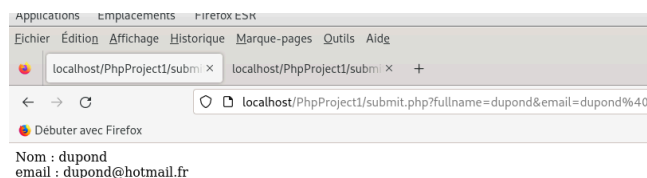
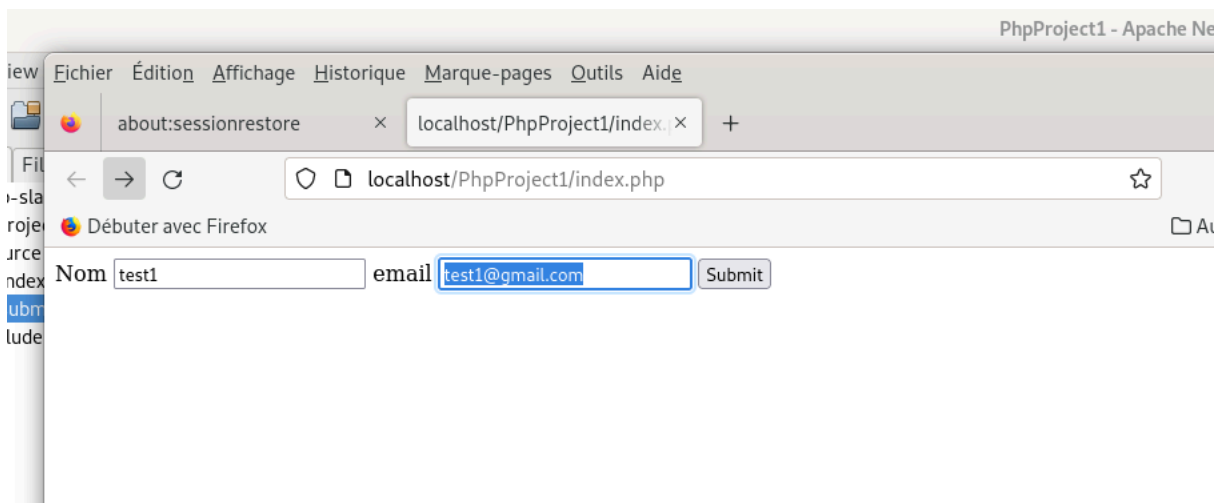
ETAPE 1:

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <title></title>
  </head>
  <body>
    <form action="submit.php" method="get">
      Nom <input type="text" id="fullname" name="fullname" />
      email <input type="email" id="email" name="email" />
      <input type="submit" name="submit" id="submit" value="Submit" />
    </form>
  </body>
</html>
```



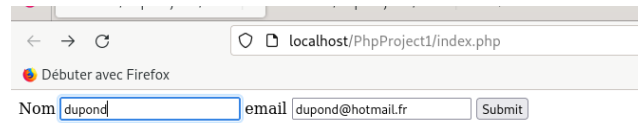


Étape 2 : usurpation par CSRF



Étape 2 : usurpation par CSRF

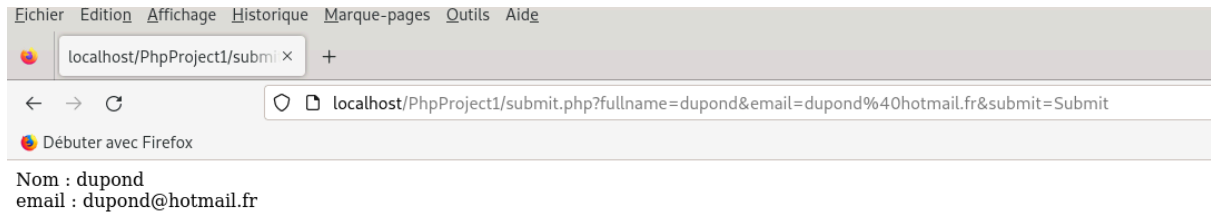
simulation par un utilisateur



localhost/PhpProject1/index.php

Débuter avec Firefox

Nom email



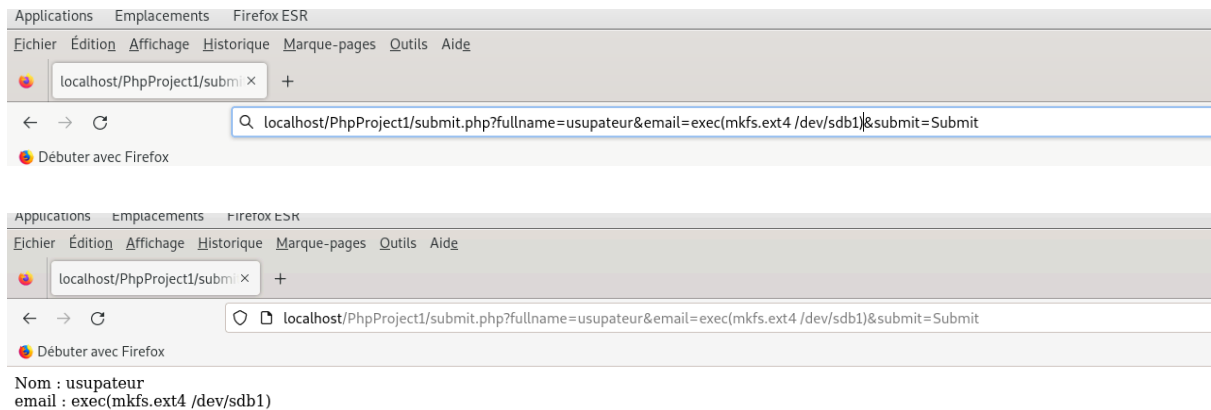
Echier Edition Affichage Historique Marque-pages Outils Aide

localhost/PhpProject1/submit.php?fullname=dupond&email=dupond%40hotmail.fr&submit=Submit

Débuter avec Firefox

Nom : dupond
email : dupond@hotmail.fr

simulation par un usupateur:



Applications Emplacements Firefox ESR

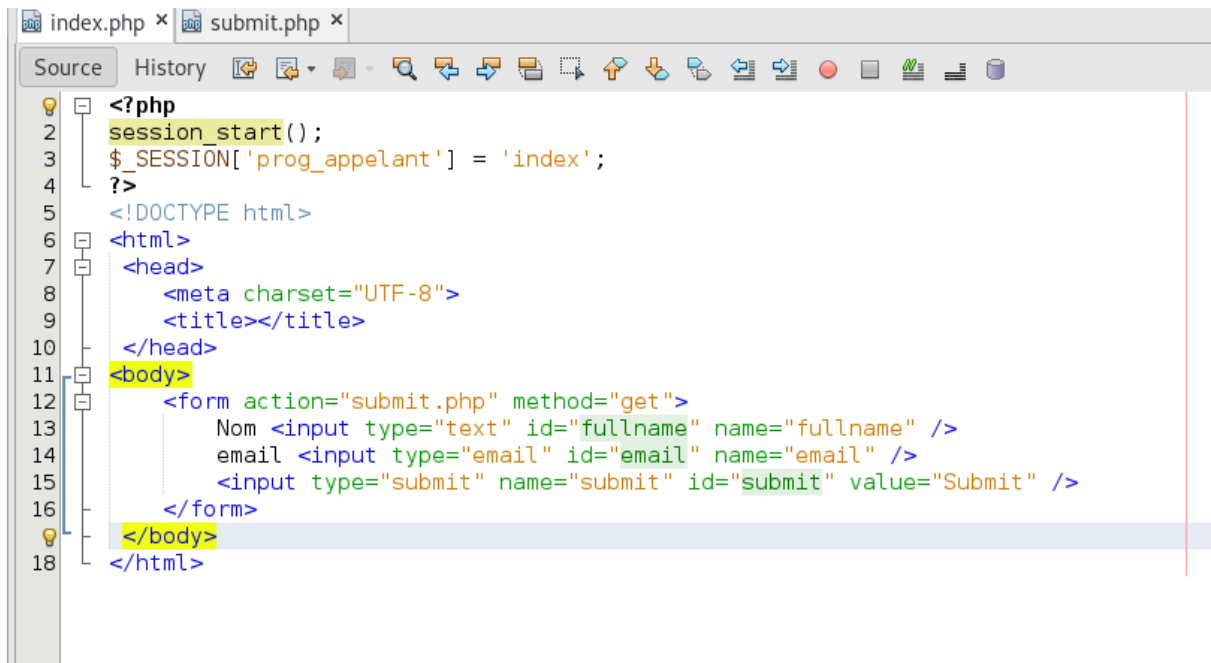
Echier Edition Affichage Historique Marque-pages Outils Aide

localhost/PhpProject1/submit.php?fullname=usupateur&email=exec(mkfs.ext4 /dev/sdb1)&submit=Submit

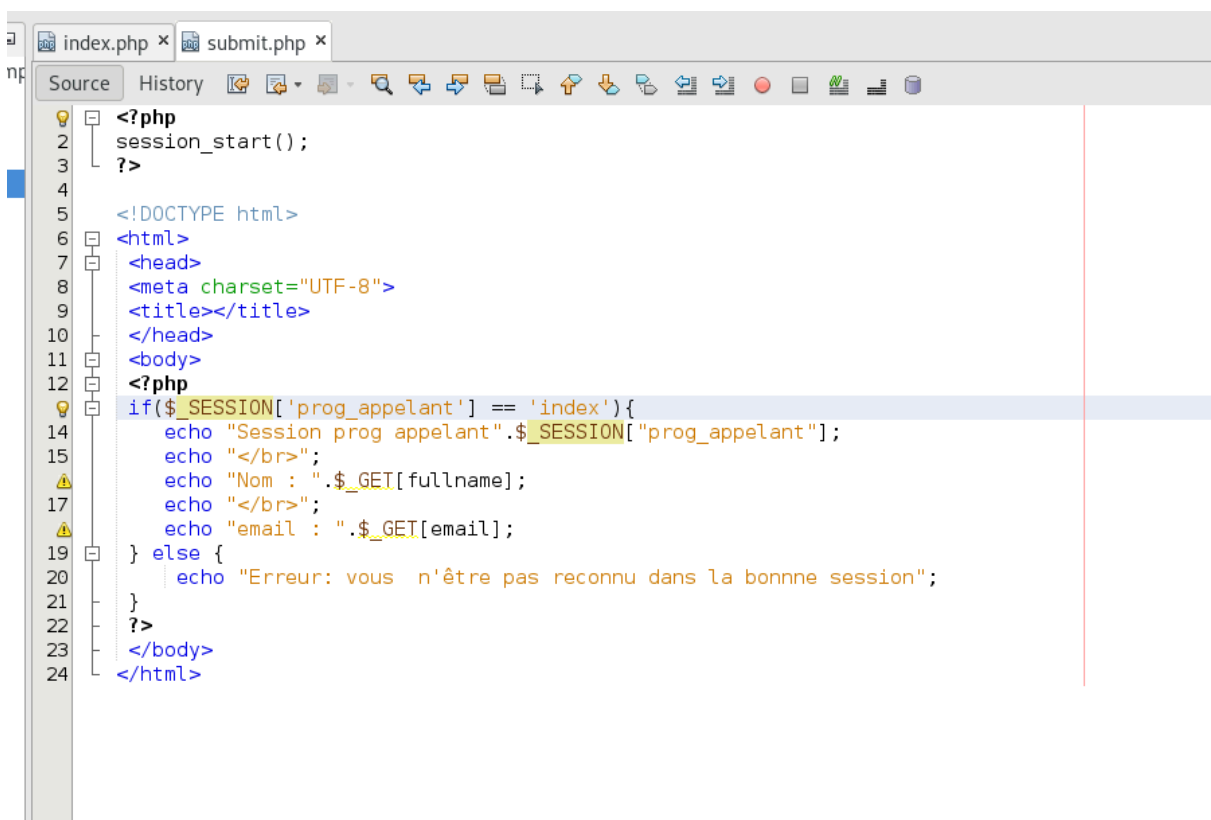
Débuter avec Firefox

Nom : usupateur
email : exec(mkfs.ext4 /dev/sdb1)

ETAPE 3: Sécurisation par session

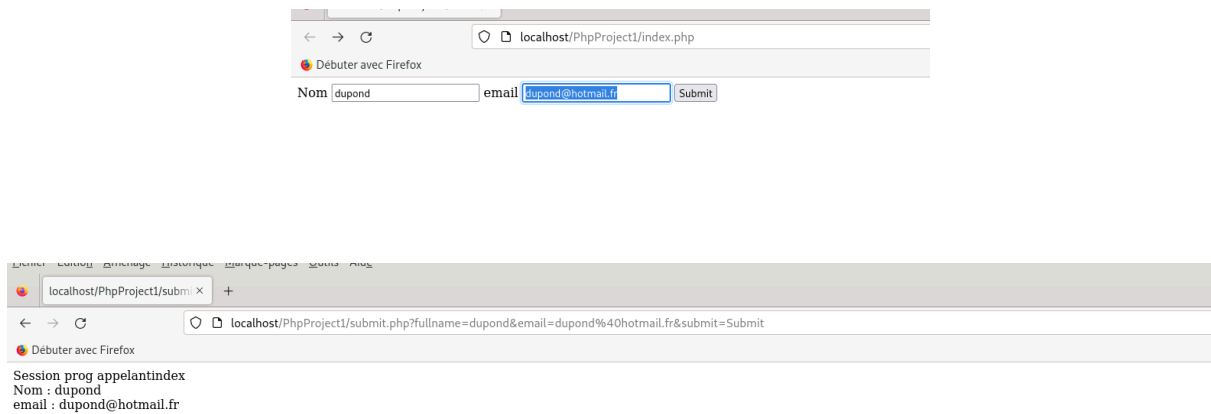


```
1 <?php
2 session_start();
3 $_SESSION['prog_appellant'] = 'index';
4 ?>
5 <!DOCTYPE html>
6 <html>
7 <head>
8 <meta charset="UTF-8">
9 <title></title>
10 </head>
11 <body>
12 <form action="submit.php" method="get">
13     Nom <input type="text" id="fullname" name="fullname" />
14     email <input type="email" id="email" name="email" />
15     <input type="submit" name="submit" id="submit" value="Submit" />
16 </form>
17 </body>
18 </html>
```

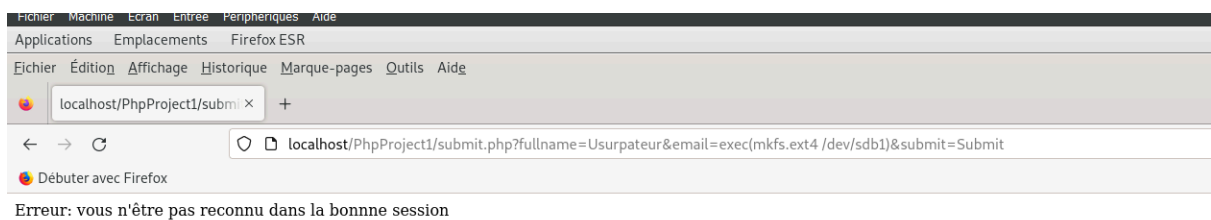


```
1 <?php
2 session_start();
3 ?>
4
5 <!DOCTYPE html>
6 <html>
7 <head>
8 <meta charset="UTF-8">
9 <title></title>
10 </head>
11 <body>
12 <?php
13 if($_SESSION['prog_appellant'] == 'index'){
14     echo "Session prog appellant".$_SESSION["prog_appellant"];
15     echo "<br>";
16     echo "Nom : ".$_GET[fullname];
17     echo "<br>";
18     echo "email : ".$_GET[email];
19 } else {
20     echo "Erreur: vous n'êtré pas reconnu dans la bonne session";
21 }
22 ?>
23 </body>
24 </html>
```

simulation par un utilisateur



simulation par un usupateur:
sur un nouvelle de session firefox



ETAPE 4: sécurisation par jeton

```
<?php
session_start();

require_once('csrf.class.php');
$csrf = new csrf();

$token_id = $csrf->get_token_id();
$token_value = $csrf->get_token($token_id);
?>

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title></title>
</head>
<body>
<form action="submit.php" method="get">
  Nom <input type="text" id="fullname" name="fullname" />
  email <input type="email" id="email" name="email" />
  <input type="submit" name="submit" id="submit" value="Submit" />
  <input type="hidden" name="csrf" id="csrf" value="<?php echo $token_value; ?>" />
</form>
</body>
</html>
```

```

1 <!DOCTYPE html>
2 <html>
3 <head>
4 <meta charset="UTF-8">
5 <title></title>
6 </head>
7 <body>
8 <?php
9 session_start();
10 require_once('csrf.class.php');
11 $csrf = new csrf();
12
13 $token_id = $csrf->get_token_id();
14
15 $token_value = $csrf->get_token($token_id);
16
17 if($csrf->check_valid('get')){
18     // affichage du jeton
19     echo "Le jeton est bon : ";
20     var_dump($_GET[$token_id]);
21     echo "<br>";
22     echo "Nom : " . $_GET["fullname"];
23     echo "<br>";
24     echo "email : " . $_GET["email"];
25 }else{
26     // affichage message d'erreur
27     echo "Le jeton n'est pas bon !";
28 }
29
30 ?>
31 </body>
32 </html>

```

simulation par un utilisateur

localhost/PhpProject1/

Debuter avec Firefox

Nom email

localhost/PhpProject1/submit.php?fullname=dupond&email=dupond%40hotmail.fr&submit=Submit&e7c3588e7e=b63ac2fc61c12016e5f7e35a83a50d4b2279003e2b43a1628992b0d74ae327bf

Debuter avec Firefox

Le jeton est bon : string(64) "b63ac2fc61c12016e5f7e35a83a50d4b2279003e2b43a1628992b0d74ae327bf"

Nom : dupond

email : dupond@hotmail.fr

simulation par un usupateur:

localhost/PhpProject1/submit.php?fullname=Dupond&email=dupond%40hotmail.fr&submit=Submit&e7c3588e7e=b63ac2fc61c12016e5f7e35a83a50d4b2279003e2b43a1628992b0d74ae327bf

Debuter avec Firefox

Le jeton n'est pas bon !