EPITA

ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

WEB SECURITY REPORTING

Report by: YOGITHA SATYA SAI PANTHAM

SUMMARY

Introduction:

This report shows security audit and vulnerabilities associated with www.e-commune.org website and the potential risks when they are exploited, as well as recommendations for avoiding such vulnerabilities.

Vulnerabilities:

1) User enumeration
2) Network traffic not encrypted
3) Weak passwords are allowed
4) Technical information leakage
   a) Login form
   b) Password field
   c) Form submitted
5) Directory listing
6) Presence of backdoor on the server

Recommendations:

1) We need to use Web application firewall.
2) The data must be encrypted with some high secured tools like SSL protocol.
3) We have to give prompts near the passwords. So that the user will use one uppercase letter, one symbol and one numeric number.
4) we should not provide any details about the password and logins in the html pages.
5) We have to remove the directory listing option from apache tomcat server and restart.
6) We should not leak the sensitive data in the html pages as mentioned above and also should allow the arbitrary command line execution.

INDEX

VULNERABILITIES

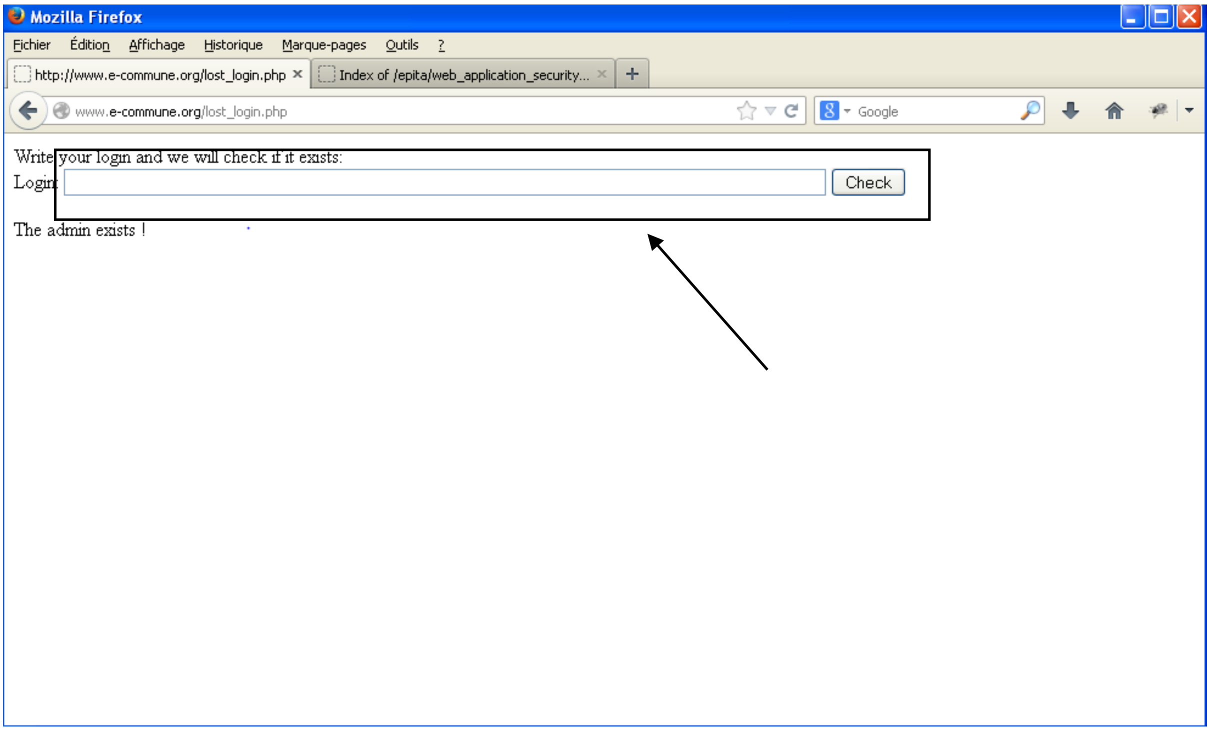
Vulnerability 1: "User enumeration"

Description:

We are currently working on the www.e-commune.org website and we can see that when we use the brute force. We can find it by the user authentication.

Exploitation:

In http://www.e-commune.org/lost_login.php we can see an option to check for any existing user.


Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
http://www.e-commune.org/lost_login.php
Index of /epita/web_application_security...
www.e-commune.org/lost_login.php
Google
Check

Write your login and we will check if it exists:

Login:

The admin exists !

I have used "admin" as my login and it has given a result "the admin exists!"

Recommendation:

1) To secure the existing users data, we need to use Web application firewall.
2) By using this, it hides the data of the users and give error.

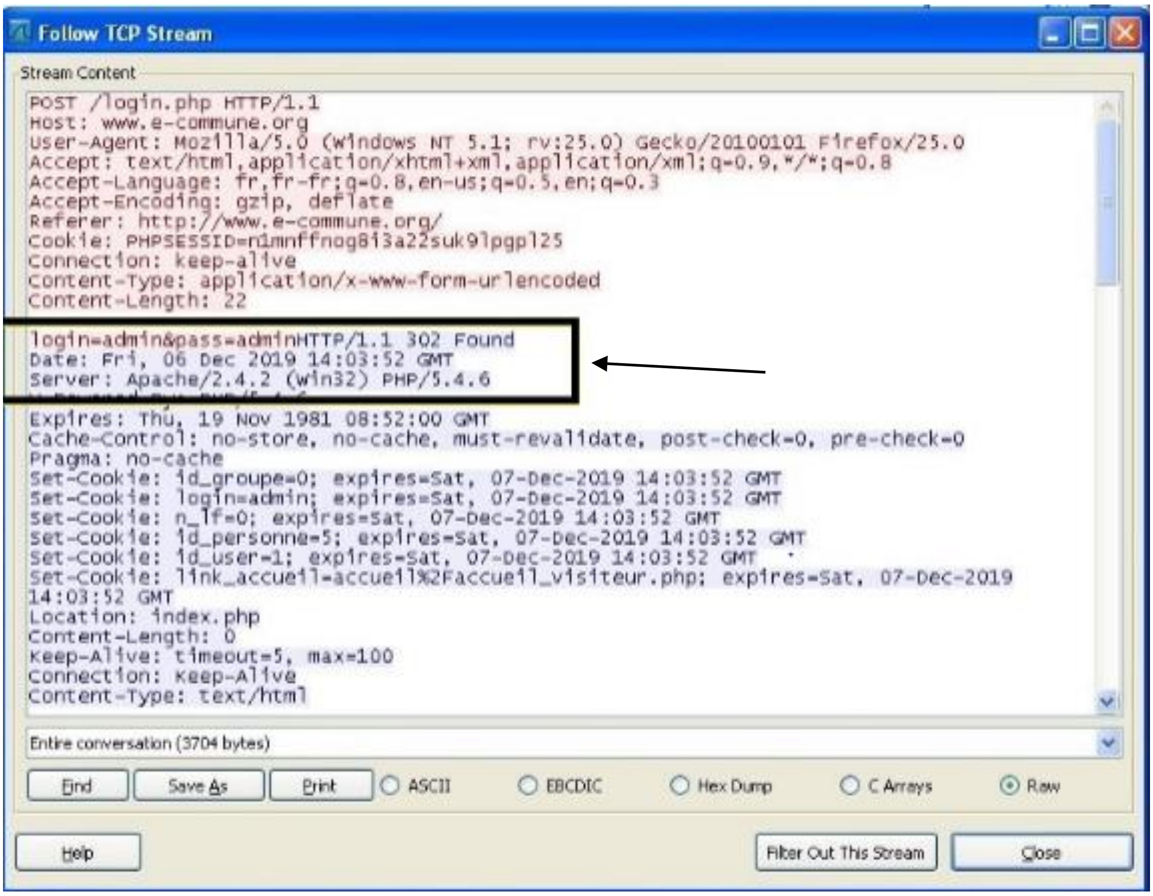
Vulnerability 2: “Network traffic not encrypted”

Description:

If the data is not encrypted, it can be exploited easily by using Wireshark or the other tools which are available for everyone these days.

Exploitation:

Attacker can see all the sensitive data by using Wireshark as shown below.



```
POST /login.php HTTP/1.1
Host: www.e-commune.org
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:25.0) Gecko/20100101 Firefox/25.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.e-commune.org/
Cookie: PHPSESSID=n1mnffnog813a22suk91pgpl25
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 22

login=admin&pass=adminHTTP/1.1 302 Found
Date: Fri, 06 Dec 2019 14:03:52 GMT
Server: Apache/2.4.2 (Win32) PHP/5.4.6
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: id_groupe=0; expires=Sat, 07-Dec-2019 14:03:52 GMT
Set-Cookie: login=admin; expires=Sat, 07-Dec-2019 14:03:52 GMT
Set-Cookie: n_lf=0; expires=Sat, 07-Dec-2019 14:03:52 GMT
Set-Cookie: id_personne=5; expires=Sat, 07-Dec-2019 14:03:52 GMT
Set-Cookie: id_user=1; expires=Sat, 07-Dec-2019 14:03:52 GMT
Set-Cookie: link_accueil=accueil%2Faccueil_visiteur.php; expires=Sat, 07-Dec-2019
14:03:52 GMT
Location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Entire conversation (3704 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Recommendation:

To secure this vulnerability the data must be encrypted with some high secured tools like SSL protocol.

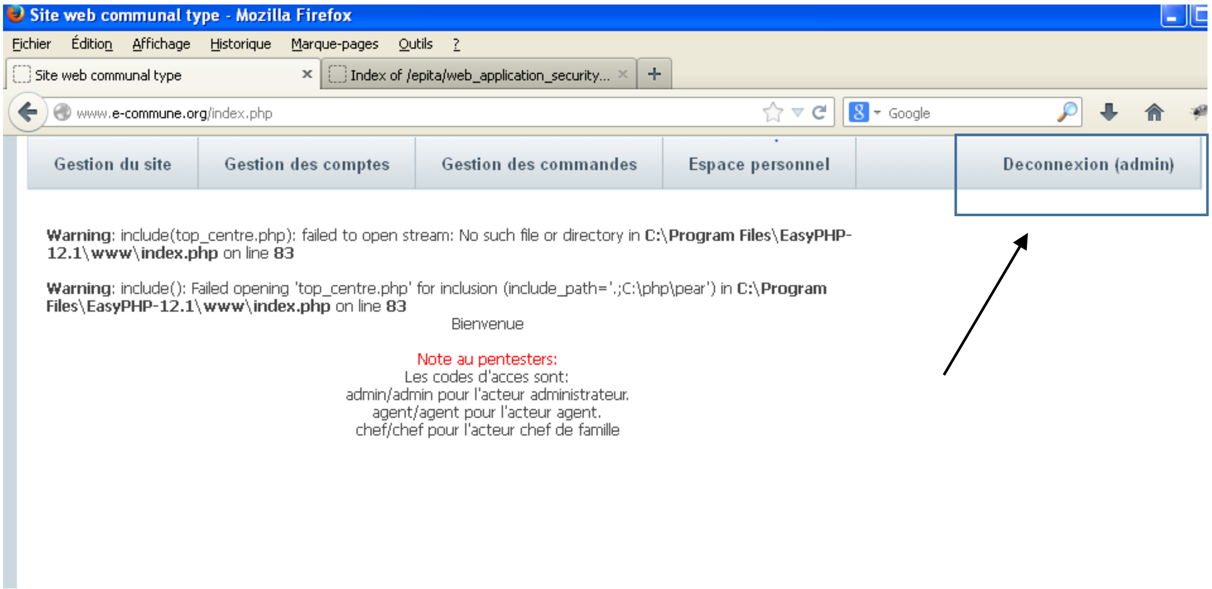
Vulnerability 3: “Weak passwords are allowed”

Description:

In the existing world passwords are the physical lock for all kinds of data. It can be hacked easily, if it is weak.

Exploitation:

The passwords should be as hard as it can. Here, the password is very weak. In this type of cases hackers or attackers can crack it very easily.


Site web communal type - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
Site web communal type
Index of /epita/web_application_security...
www.e-commune.org/index.php
Google
Gestion du site
Gestion des comptes
Gestion des commandes
Espace personnel
Deconnexion (admin)

Warning: include(top_centre.php): failed to open stream: No such file or directory in **C:\Program Files\EasyPHP-12.1\www\index.php** on line **83**

Warning: include(): Failed opening 'top_centre.php' for inclusion (include_path='.;C:\php\pear') in **C:\Program Files\EasyPHP-12.1\www\index.php** on line **83**

Bienvenue

Note au pentesters:
Les codes d'acces sont:
admin/admin pour l'acteur administrateur.
agent/agent pour l'acteur agent.
chef/chef pour l'acteur chef de famille

I have used the USERNAME as “admin” and PASSWORD as “admin”. As you can see I am able to login to the website.

Recommendation:

To secure this kind of vulnerabilities, we have to give prompts near the passwords. So that the user will use one uppercase letter, one symbol and one numeric number.

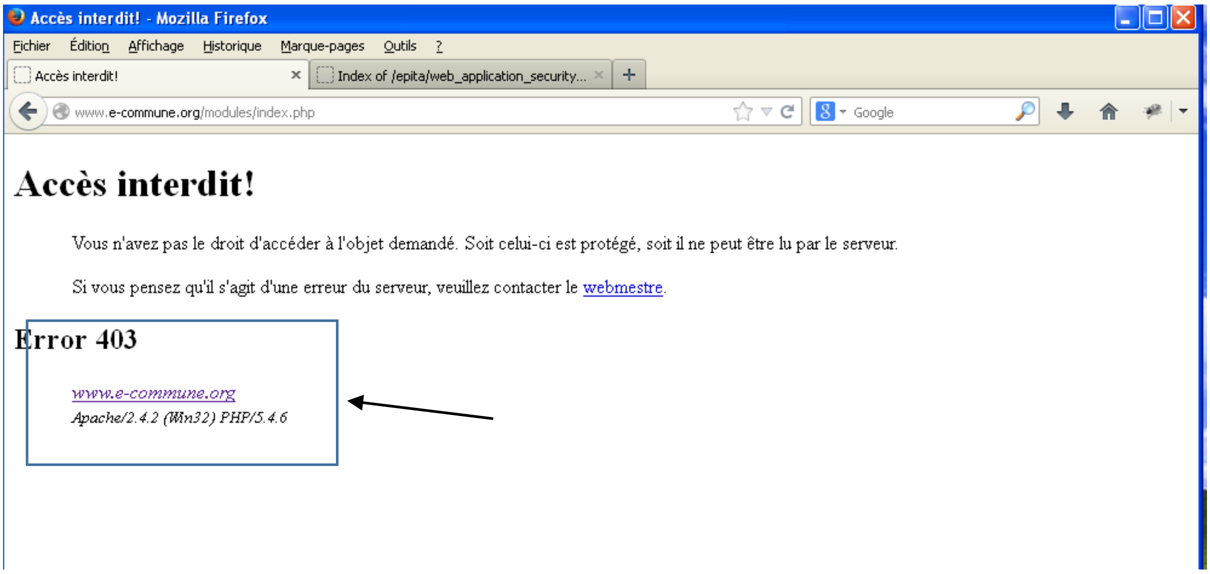
Vulnerability 4: “Technical information leakage”

Description:

Whatever the data is either internal or external containing sensitive info can lead to exploitation.

Exploitation:

There will be an error message and in that we can clearly find the sensitive data as “Apache/2.4.2 (Win32) PHP/5.4.6. This can leads to an exploitation. We can see clearly in the below image.


Accès interdit! - Mozilla Firefox
Fichier
Édition
Affichage
Historique
Marque-pages
Outils
?
Accès interdit!
Index of /epita/web_application_security...
www.e-commune.org/modules/index.php
Google

Accès interdit!

Vous n'avez pas le droit d'accéder à l'objet demandé. Soit celui-ci est protégé, soit il ne peut être lu par le serveur.

Si vous pensez qu'il s'agit d'une erreur du serveur, veuillez contacter le webmestre.

Error 403

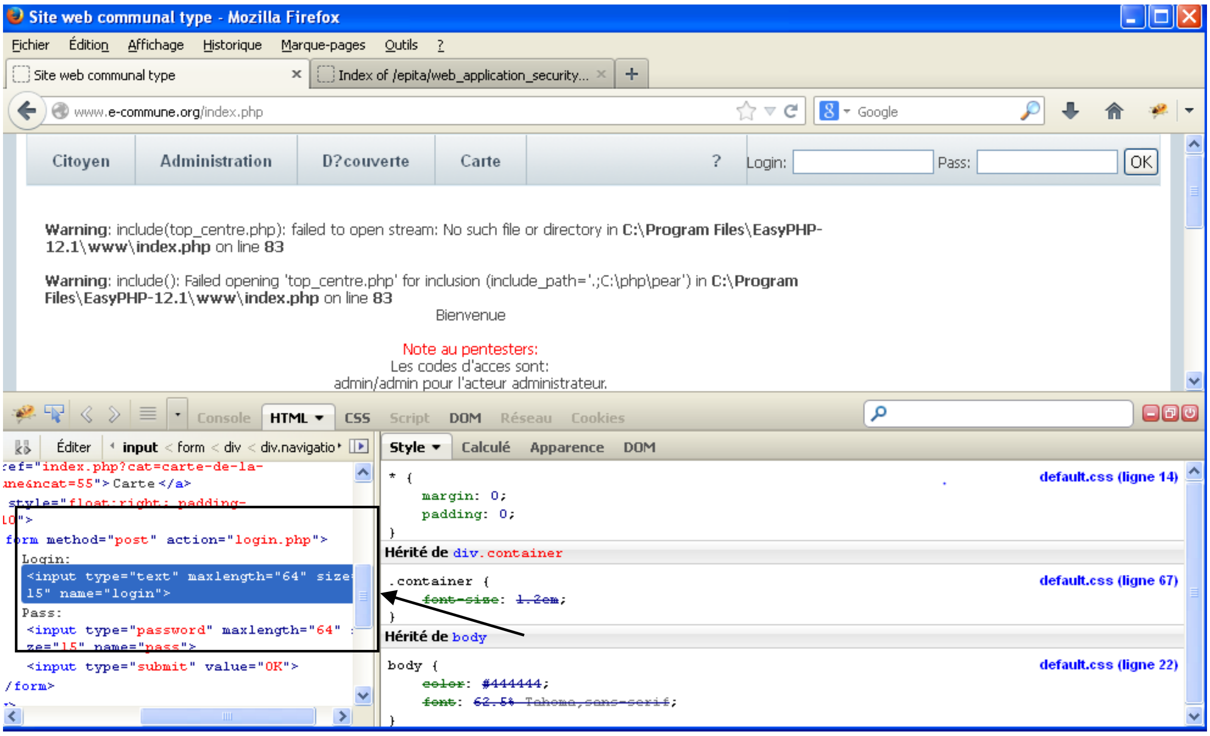
www.e-commune.org
Apache/2.4.2 (Win32) PHP/5.4.6

We have some more leakages found in this website.

a) Login form
b) Password field
c) Form submitted

a) Login form edited using firebug:

We can find the login details by the inspect option.


Site web communal type - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
Site web communal type
Index of /epita/web_application_security...
www.e-commune.org/index.php
Google
Citoyen Administration D?couverte Carte ?
Login: Pass: OK
Console HTML CSS Script DOM Réseau Cookies
Éditer input < form < div < div.navigatio
Style Calculé Apparence DOM

Warning: include(top_centre.php): failed to open stream: No such file or directory in **C:\Program Files\EasyPHP-12.1\www\index.php** on line **83**

Warning: include(): Failed opening 'top_centre.php' for inclusion (include_path='.;C:\php\pear') in **C:\Program Files\EasyPHP-12.1\www\index.php** on line **83**

Bienvenue

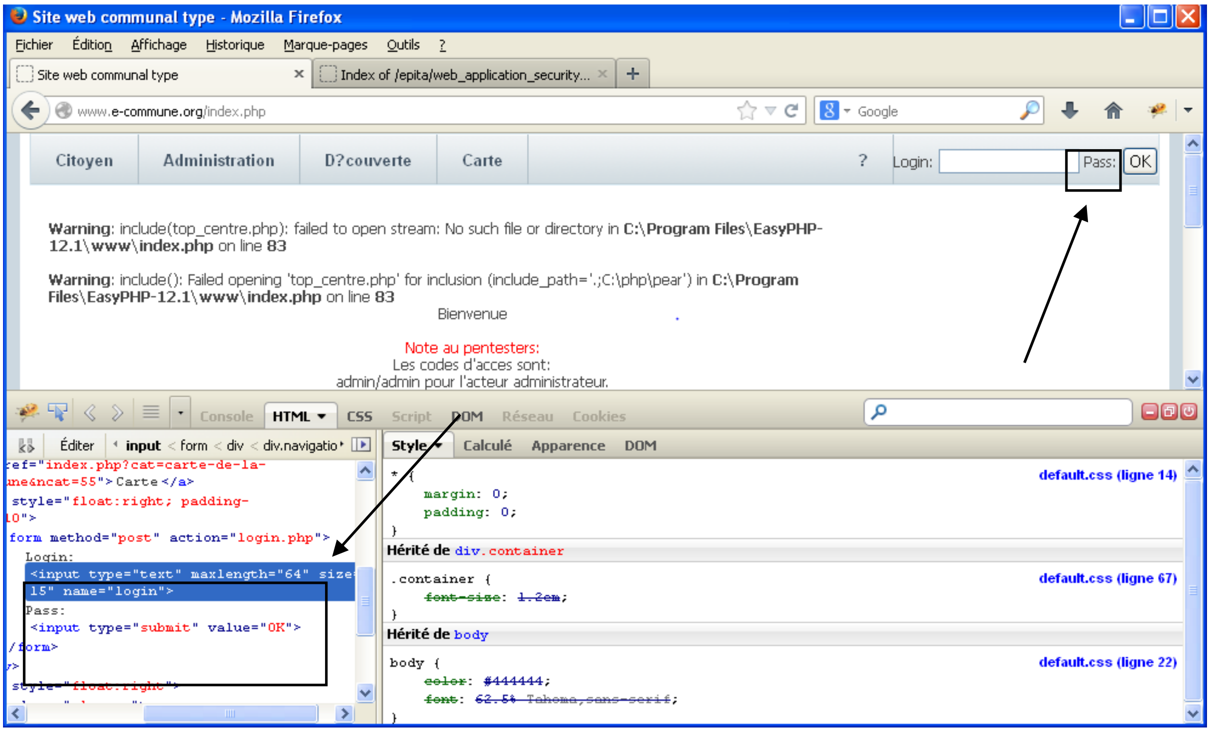
Note au pentesters:
Les codes d'acces sont:
admin/admin pour l'acteur administrateur.

```
ref="index.php?cat=carte-de-la-
ne&ncat=55">Carte</a>
style="float:right; padding-
10">
form method="post" action="login.php">
  Login:
  <input type="text" maxlength="64" size
  15" name="login">
  Pass:
  <input type="password" maxlength="64"
  ze="15" name="pass">
  <input type="submit" value="OK">
/form>
```

```
* {                                   default.css (ligne 14)
    margin: 0;
    padding: 0;
}
Hérité de div.container
.container {                          default.css (ligne 67)
    ~~font-size: 1.2em;~~
}
Hérité de body
body {                                default.css (ligne 22)
    ~~color: #444444;~~
    ~~font: 62.5% Tahoma,sans-serif;~~
}
```

b) Password field removed:

We can easily remove the password field by editing it.


Site web communal type - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
Site web communal type
Index of /epita/web_application_security...
www.e-commune.org/index.php
Google
Citoyen Administration D?couverte Carte ?
Login: Pass: OK
Console HTML CSS Script DOM Réseau Cookies
Éditer input < form < div < div.navigatio
Style Calculé Apparence DOM

Warning: include(top_centre.php): failed to open stream: No such file or directory in **C:\Program Files\EasyPHP-12.1\www\index.php** on line **83**

Warning: include(): Failed opening 'top_centre.php' for inclusion (include_path='.;C:\php\pear') in **C:\Program Files\EasyPHP-12.1\www\index.php** on line **83**

Bienvenue

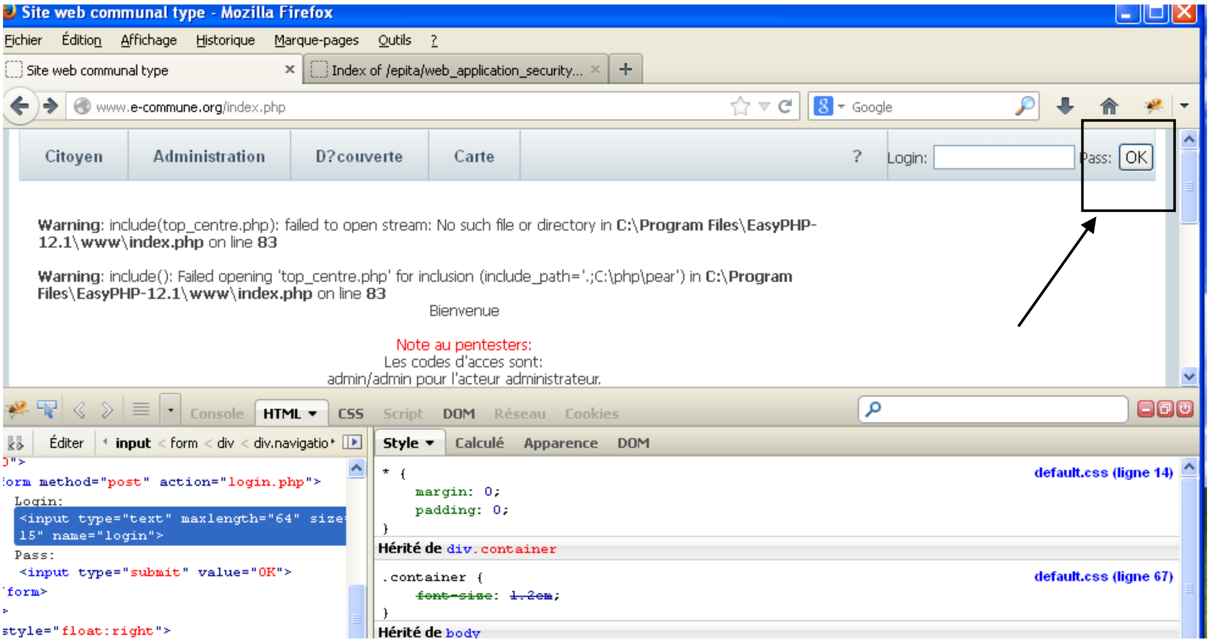
Note au pentesters:
Les codes d'acces sont:
admin/admin pour l'acteur administrateur.

```
ef="index.php?cat=carte-de-la-
ne&ncat=55">Carte</a>
style="float:right; padding-
10">
form method="post" action="login.php">
  Login:
  <input type="text" maxlength="64" size
  15" name="login">
  Pass:
  <input type="submit" value="OK">
/form>
>
style="float:right">
```

```
* {                                   default.css (ligne 14)
    margin: 0;
    padding: 0;
}
Hérité de div.container
.container {                          default.css (ligne 67)
    ~~font-size: 1.2em;~~
}
Hérité de body
body {                                default.css (ligne 22)
    ~~color: #444444;~~
    ~~font: 62.5% Tahoma,sans-serif;~~
}
```

c) Form submitted by pressing “ok”

We can continue the above process and submit the form by pressing “OK”



Site web communal type - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
Site web communal type
Index of /epita/web_application_security...
www.e-commune.org/index.php
Google
Citoyen
Administration
D?couverte
Carte
?
Login:
Pass:
OK

Warning: include(top_centre.php): failed to open stream: No such file or directory in **C:\Program Files\EasyPHP-12.1\www\index.php** on line **83**

Warning: include(): Failed opening 'top_centre.php' for inclusion (include_path='.;C:\php\pear') in **C:\Program Files\EasyPHP-12.1\www\index.php** on line **83**

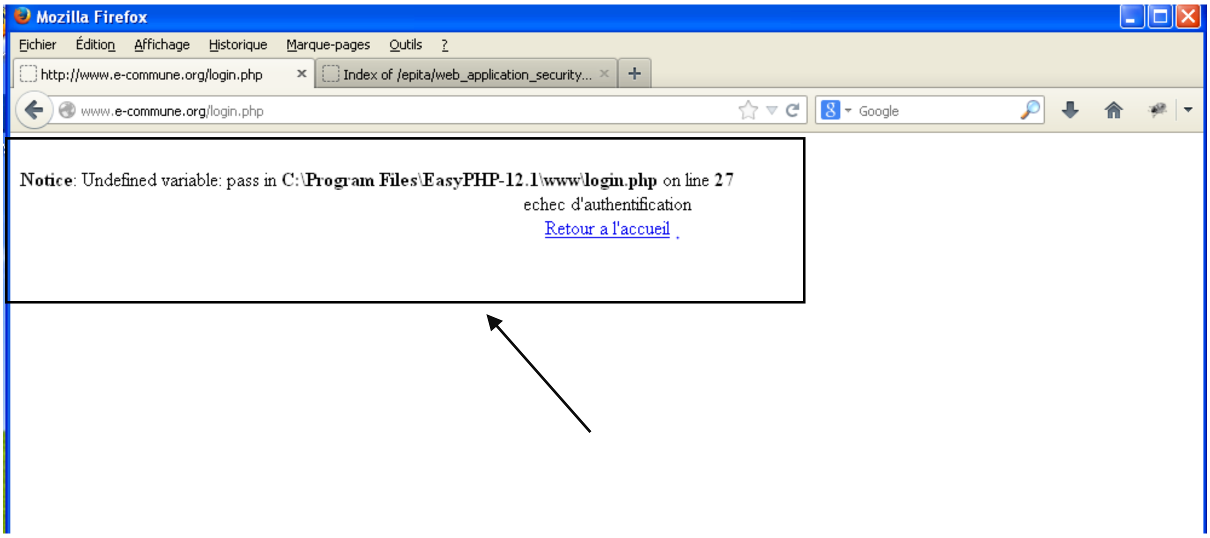
Bienvenue

Note au pentesters:
Les codes d'acces sont:
admin/admin pour l'acteur administrateur.

```
)">
orm method="post" action="login.php">
  Login:
   <input type="text" maxlength="64" size=
   15" name="login">
  Pass:
   <input type="submit" value="OK">
 form>
>
style="float:right">
```

```
* {                                   default.css (ligne 14)
    margin: 0;
    padding: 0;
}
Hérité de div.container
.container {                          default.css (ligne 67)
    ~~font-size~~: ~~1.2em~~;
}
Hérité de body
```

And also we can find the form submitted after clicking “OK”



Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
http://www.e-commune.org/login.php
Index of /epita/web_application_security...
www.e-commune.org/login.php
Google

Notice: Undefined variable: pass in **C:\Program Files\EasyPHP-12.1\www\login.php** on line **27**

echec d'authentification

Retour a l'accueil

Recommendation:

To secure this, we should not provide any details about the password and logins in the html pages.

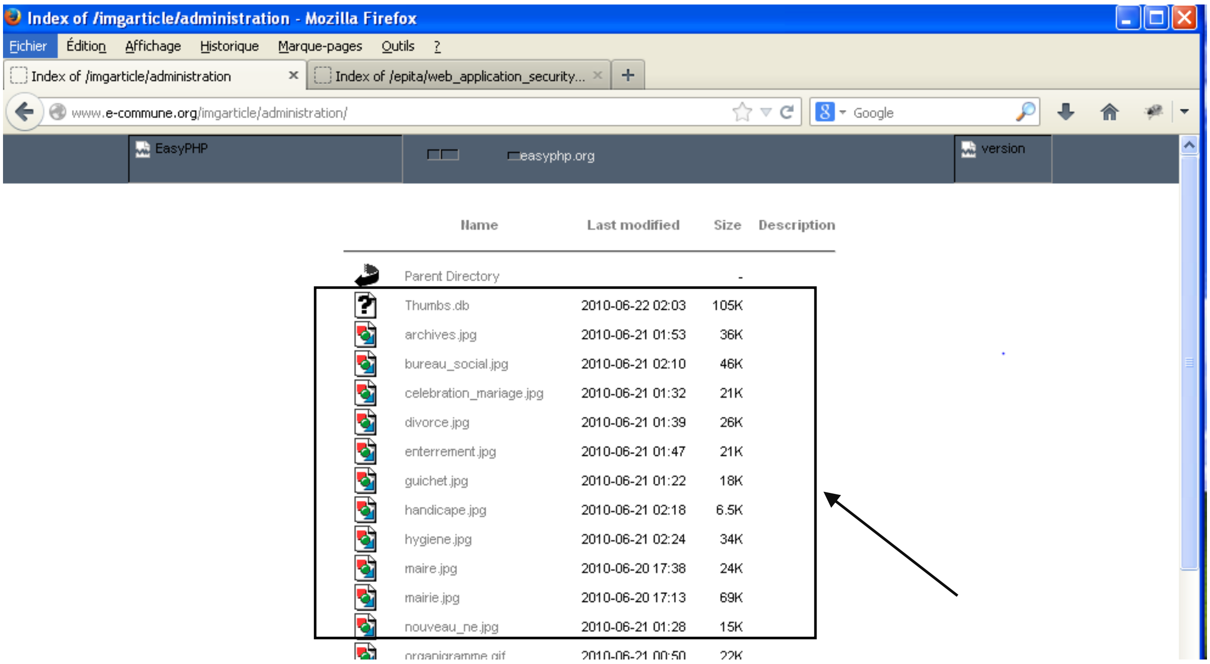
Vulnerability 5: “Directory Listing”

Description:

There shouldn’t be any listing files in the directory of the server, as the hacker/attacker can access through the files and can expoit using the tools.

Exploitation:

The attacker can brute force the files using Custom word list generator dictionary.


Index of /imgarticle/administration - Mozilla Firefox
Fichier
Édition
Affichage
Historique
Marque-pages
Outils
?
Index of /imgarticle/administration
Index of /epita/web_application_security...
www.e-commune.org/imgarticle/administration/
Google
EasyPHP
easyphp.org
version

Name	Last modified	Size	Description
Parent Directory		-	
Thumbs.db	2010-06-22 02:03	105K	
archives.jpg	2010-06-21 01:53	36K	
bureau_social.jpg	2010-06-21 02:10	46K	
celebration_mariage.jpg	2010-06-21 01:32	21K	
divorce.jpg	2010-06-21 01:39	26K	
enterrement.jpg	2010-06-21 01:47	21K	
guichet.jpg	2010-06-21 01:22	18K	
handicape.jpg	2010-06-21 02:18	6.5K	
hygiene.jpg	2010-06-21 02:24	34K	
maire.jpg	2010-06-20 17:38	24K	
mairie.jpg	2010-06-20 17:13	69K	
nouveau_ne.jpg	2010-06-21 01:28	15K	
organigramme.gif	2010-06-21 00:50	22K	

Recommendation:

To secure this, we have to remove the directory listing option from apache tomcat server and restart.

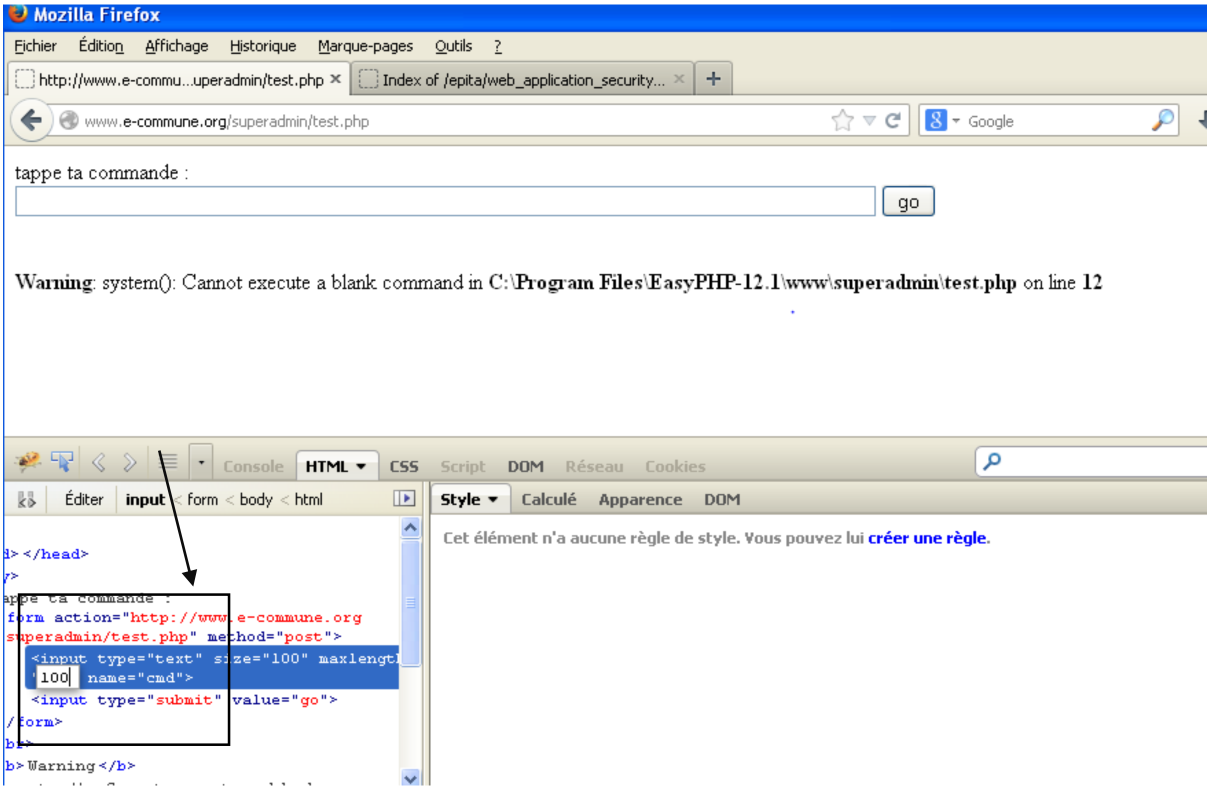
Vulnerability 6: “Presence of backdoor on server”

Description:

We should keep an option available in the backdoor. Beacause the hacker/attacker can easily access through the backdoor and can get access.

Exploitation:

In this, it is complicated to give availability to shut-down the other server using shutdown –l command in the backdoor. This can be effected by the attacker. He can modify the code and he can change the editing criteria as shown below.



Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
http://www.e-commu...uperadmin/test.php
Index of /epita/web_application_security...
www.e-commune.org/superadmin/test.php
Google
go
Console HTML CSS Script DOM Réseau Cookies
Éditer input < form < body < html
Style Calculé Apparence DOM

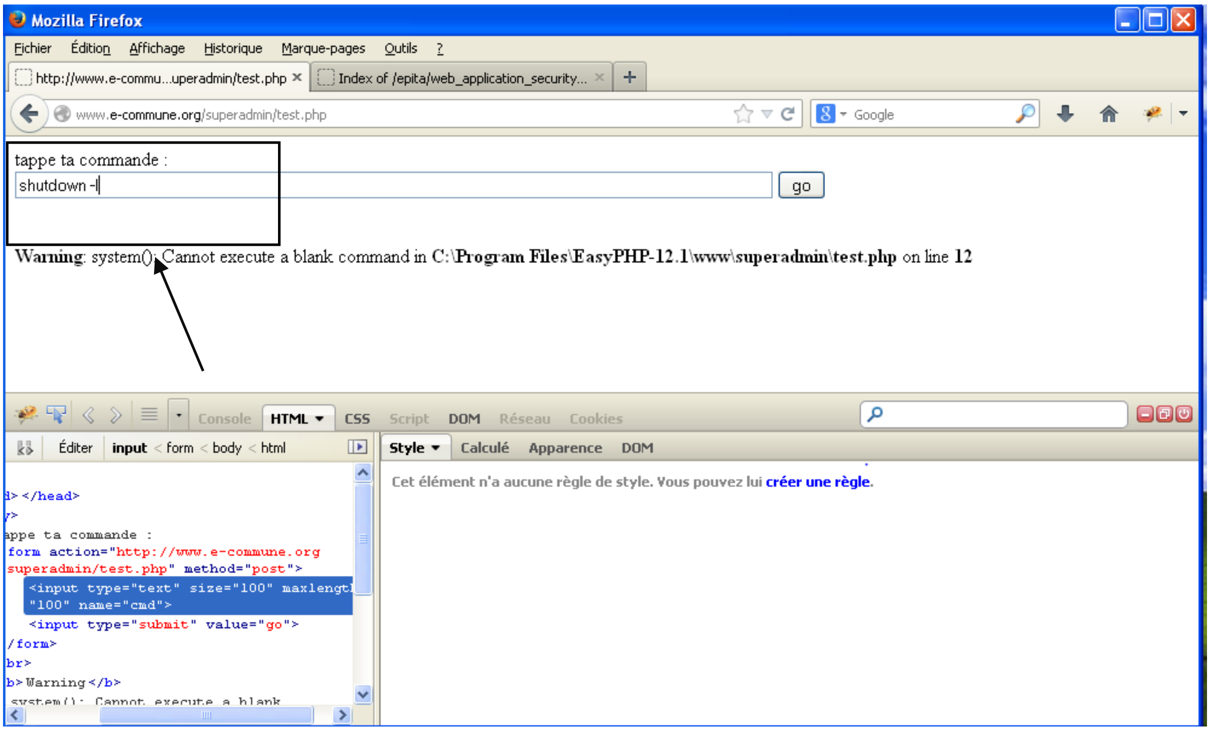
tappe ta commande :

Warning: system(): Cannot execute a blank command in C:\Program Files\EasyPHP-12.1\www\superadmin\test.php on line 12

```
d> </head>
y>
appe ta commande :
form action="http://www.e-commune.org
superadmin/test.php" method="post">
  <input type="text" size="100" maxlengt
  '100 name="cmd">
  <input type="submit" value="go">
/form>
br>
b> Warning </b>
```

Cet élément n'a aucune règle de style. Vous pouvez lui créer une règle.

We can also see the command after modifying the code below.



Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
http://www.e-commu...uperadmin/test.php
Index of /epita/web_application_security...
www.e-commune.org/superadmin/test.php
Google
go
Console HTML CSS Script DOM Réseau Cookies
Éditer input < form < body < html
Style Calculé Apparence DOM

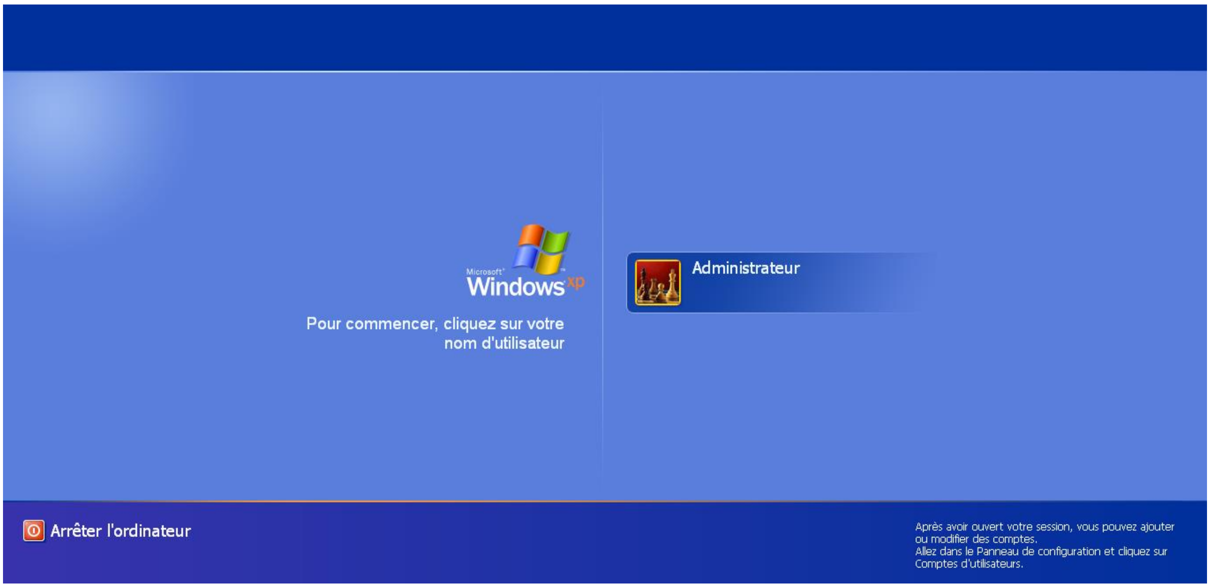
tappe ta commande :
shutdown -l

Warning: system(): Cannot execute a blank command in **C:\Program Files\EasyPHP-12.1\www\superadmin\test.php** on line **12**

```
d> </head>
y>
appe ta commande :
form action="http://www.e-commune.org
superadmin/test.php" method="post">
   <input type="text" size="100" maxlengt
   "100" name="cmd">
   <input type="submit" value="go">
/form>
br>
b>Warning</b>
system(): Cannot execute a blank
```

Cet élément n'a aucune règle de style. Vous pouvez lui créer une règle.

Now, we can see the backdoor getting shutdown below.



Pour commencer, cliquez sur votre nom d'utilisateur

Après avoir ouvert votre session, vous pouvez ajouter ou modifier des comptes.
Allez dans le Panneau de configuration et cliquez sur Comptes d'utilisateurs.

Recommendation:

To secure this, we should not leak the sensitive data in the html pages as mentioned above and also should allow the arbitrary command line execution.