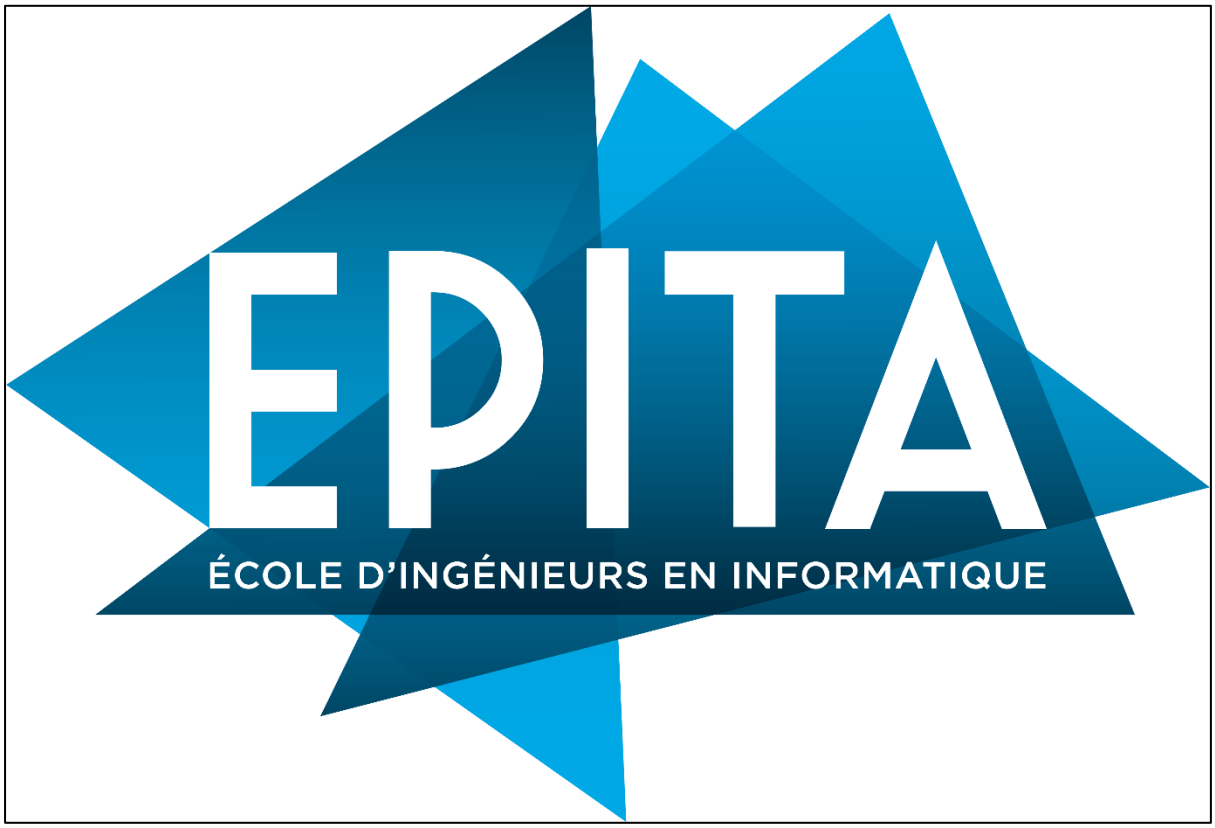
WEB APPLICATION SECURITY
Security audit report



Done by Ishwariya Mani

Summary:

Introduction:

This audit report vulnerabilities are exploited from www.e-commune.org website and it is 3-tier architecture(client..,webserver..,database). The web application is manipulated through a web navigator and it's stored on the server's side and is an interface(middle ware) between the client and the database server.

Vulnerabilities categories:

The vulnerabilities founded in this report some are highly sensitive and it contains the users personal information which is high in priority and the attackers can steal the data's and use it for other purpose. The website is not highly secured so the attackers can easily exploit the data's.

Recommendations:

Need to check that any applications or scripts that uses an latest version and also need to do an regular security audit . using an firewall for web applications.

Contents

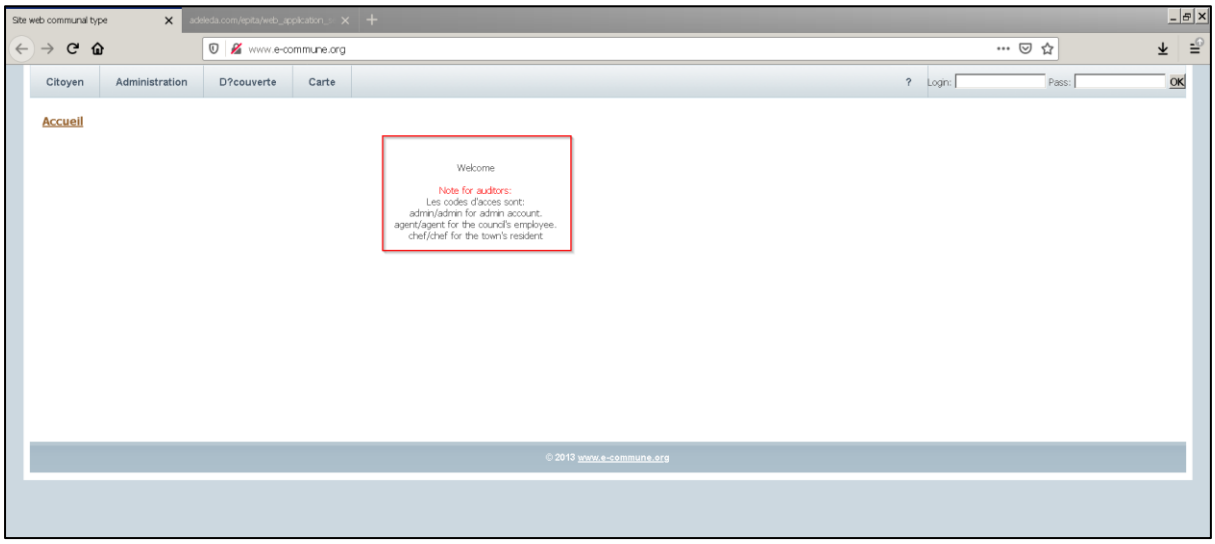
Vulnerabilities:

1. Sensitive information leakage

Indicators of criticality: high

Description: The accounts user/password are leaked on the main page and this allow the attackers to exploit the information.

Exploitation: When attackers visits the www.e-commune.org website they can see the piece of notes left in plain sight and there are many ways a website can be coaxed into revealing this type of information. It gives an attackers useful guidance for further exploitation.



Recommendations:

- need to encrypt the data and also to monitor the network access.

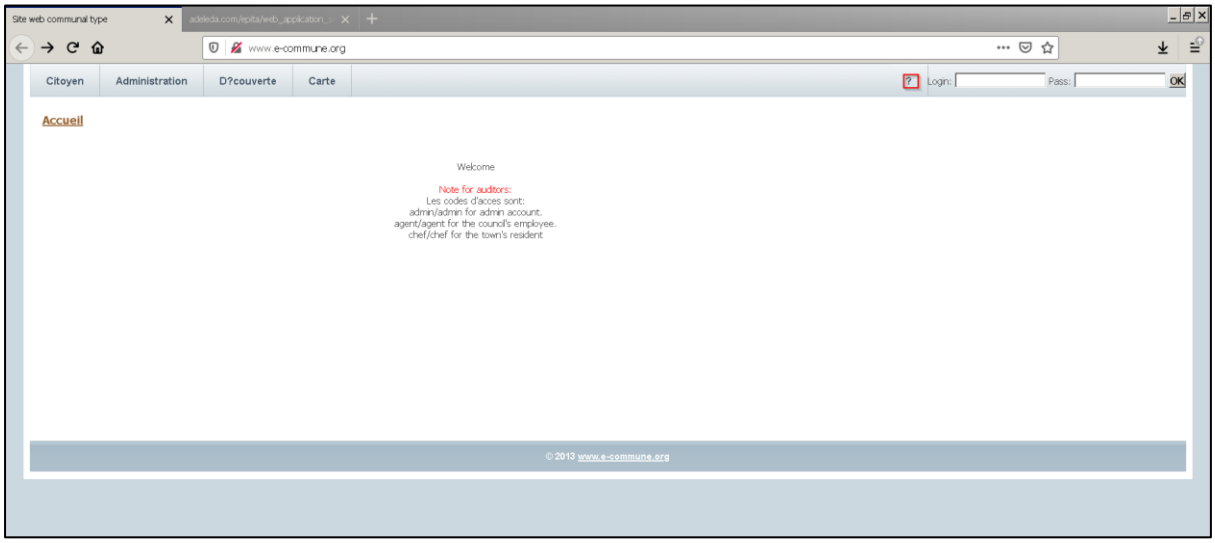
2. User enumeration (www.e-commune.org/lost_login.php)

Indicators of criticality: moderate

Description: This vulnerability occurs when attackers try to determine whether the username is valid or not valid.

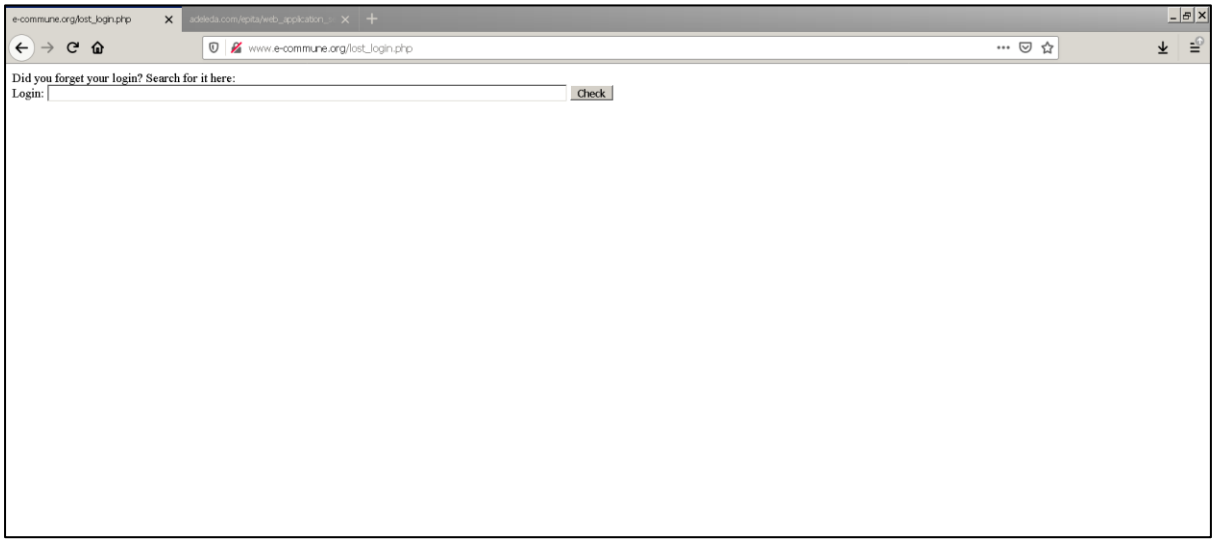
Exploitation: when attackers visit www.e-commune.org website and try to click the ? help the URL takes them to www.e-commune.org/lost_login.php page and there it will shows an feature like login and there it may leads to get data from user.

Screenshot:1



- click on ? to see the information.

Screenshot : 2



- **The login page will look like this**

Remediation:

- Do not enter user name or password until the website is secured.
- One other way to block user enumeration is with a web application firewall (WAF). To perform user enumeration, the malicious actor needs to submit lots of different usernames.

References : https://www.rapid7.com/blog/post/2017/06/15/about-user-enumeration/

3. Directory listing / open directory

Indicators of criticality: Low

Description: Contains an list of open directories this may contains an sensitive information or any secret details and it will let to access the data.

Exploitation: In www.e-commune.org website there is an list of options like (citoyen,administration,decouverte.,) .On citoyen, go to accueil > citoyen >vivre ensemble there is an image when attackers try to view the image and that image.pgp will occurs at the URL when they try to remove that image.pgp and run the URL they may see the page saying index of /imgarctile/citoyen under that there will be some an open directory may appears which contains an information for the attackers.

Screenshot :1

- **Accueil > citoyen > vivre ensemble**

Screenshot : 2

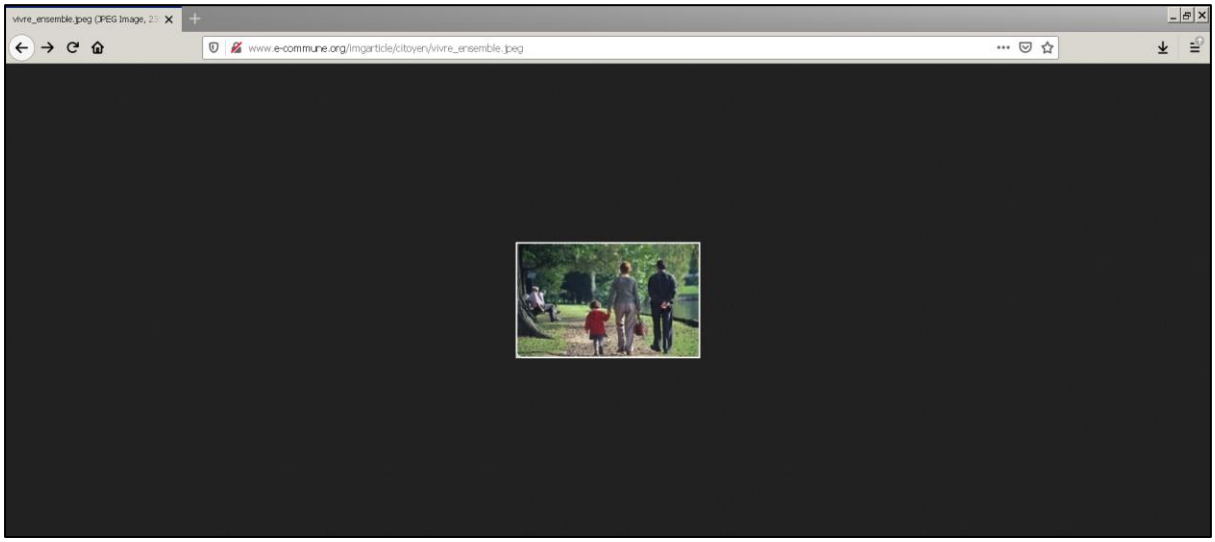


Image exploited for audit

Screenshot:3

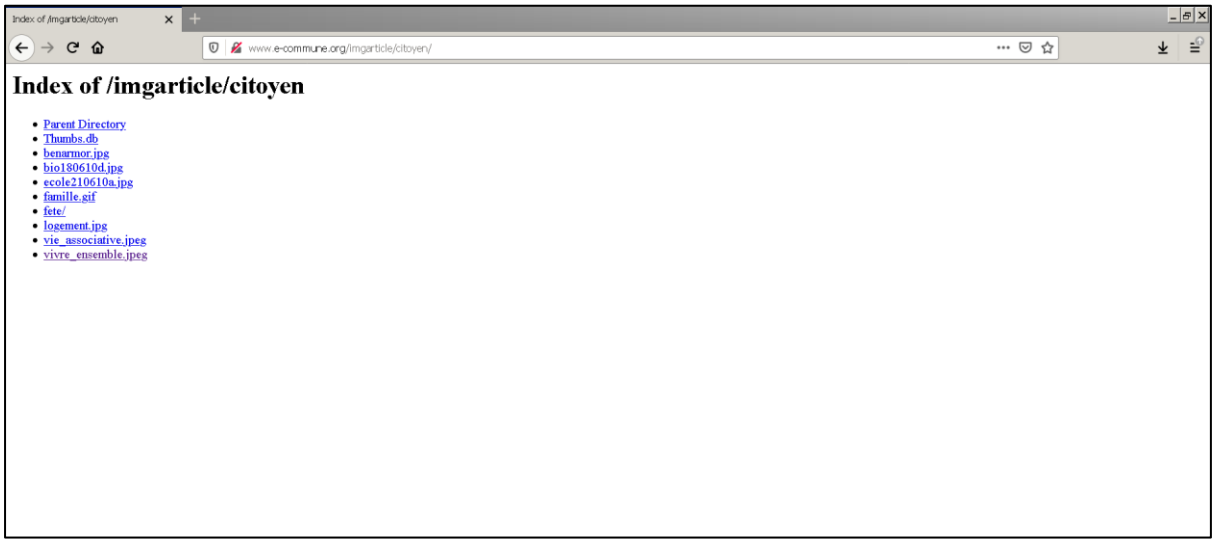


Image which shows a list of directories in www.e-commune.org

Remediations:

- Create blank index.html and place in each directory. This will prevent directory listing and display blank page in web browser. (Not a recommended method)
- Disable directory listing for entire application.
- In business needs, create a directory and enable directory listing only for that alone. All web servers have these options to configure.

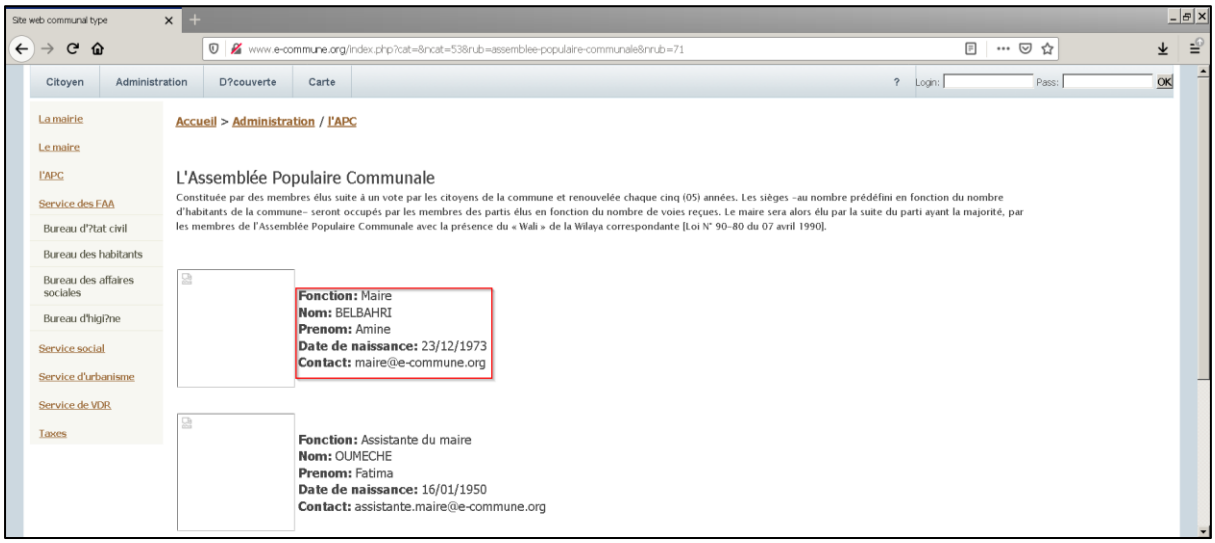
References: Directory Listing Vulnerability – Detection & Prevention - Security Investigation (socinvestigation.com)

4. Personal identifiable information leakage -I’APC

Indicators of criticality: high

Description: Users personal informations are leaked like first name , last name , date of birth and contact details.

Exploitation: On administration option when attackers try to click on gallery they can see users personal information’s like name, date of birth , contact details. By using that they can do many attacks like accessing their g-mail accounts and get one time password to open some other applications to steal the data’s.



5. Blank search

Indicators of criticality: high

Description: : leaks 2 PII leading to user account compromise

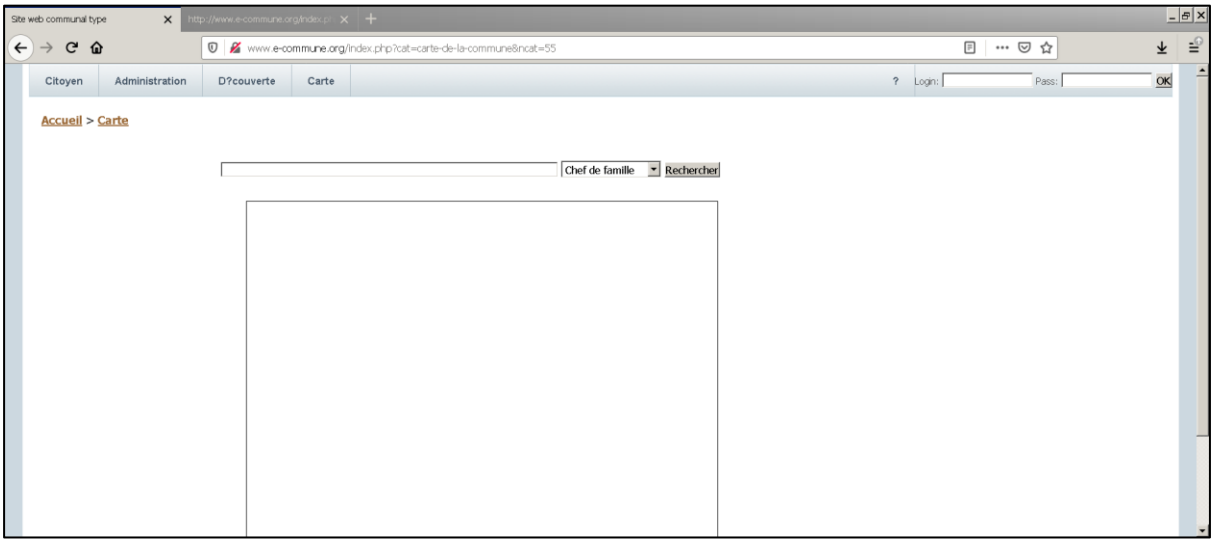
Exploitation: Inside carte if attackers do blank search it leaks 2 PII information it leads to user account a compromise.

Here if attackers do just normal blank search it just show a normal source code but when attackers entered something and did a search they may see a source code contains a personal information’s .

And also we can see a blank space between the source code like upper part of the code and lower part of code. In lower part of code we can see superadmin link when they try to access that link they can see a source code in a page and they remove a view source from the URL and do a search they can see a command search were hidden. And it seems not authentication

and if they take a look at www.e-commune.org/superadmin link they can see a index of / superadmin contains a directory and .files seems like hidden files it can open a way to see the attackers to search for personal information's.

Screenshot :1



Blank search page .

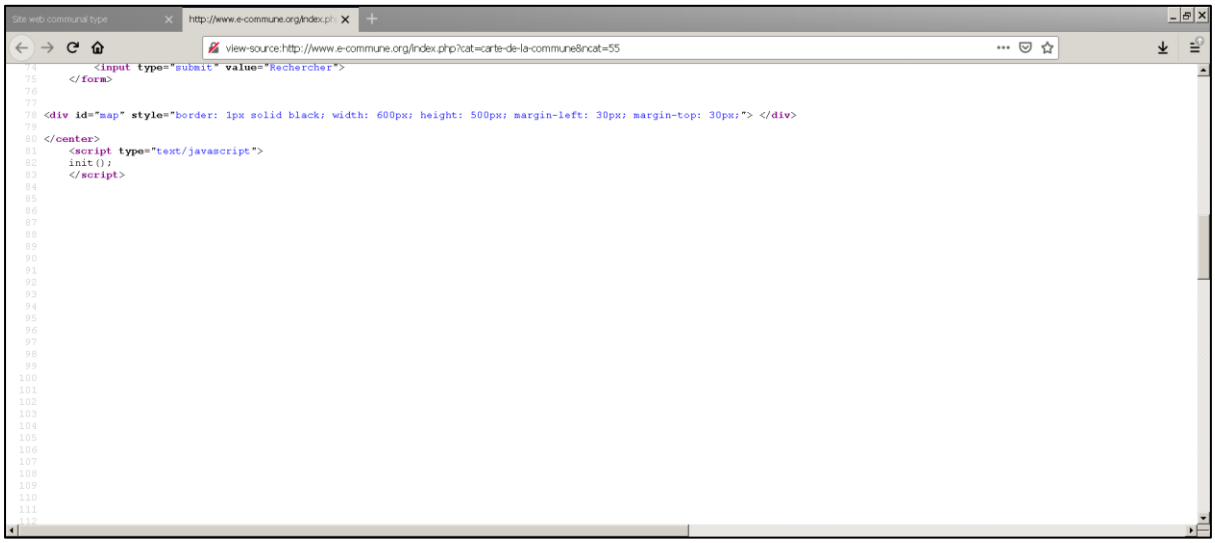
Screenshot : 2

Did blank search and it contains no personal information.

Screenshot : 3

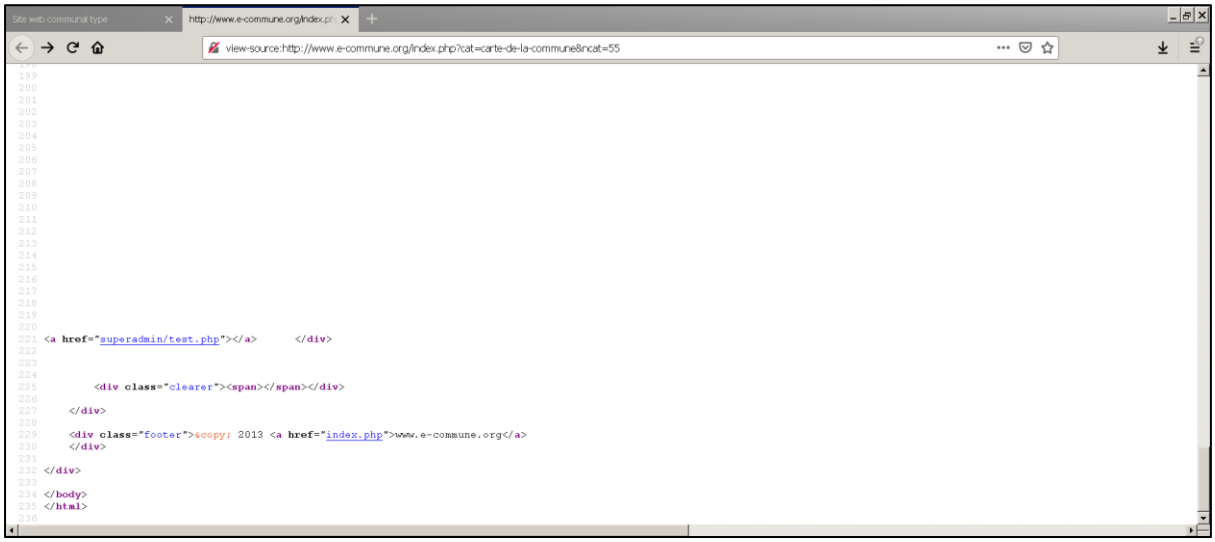
Entered a text and did a search and we can see a personal information in source code

Screenshot : 4



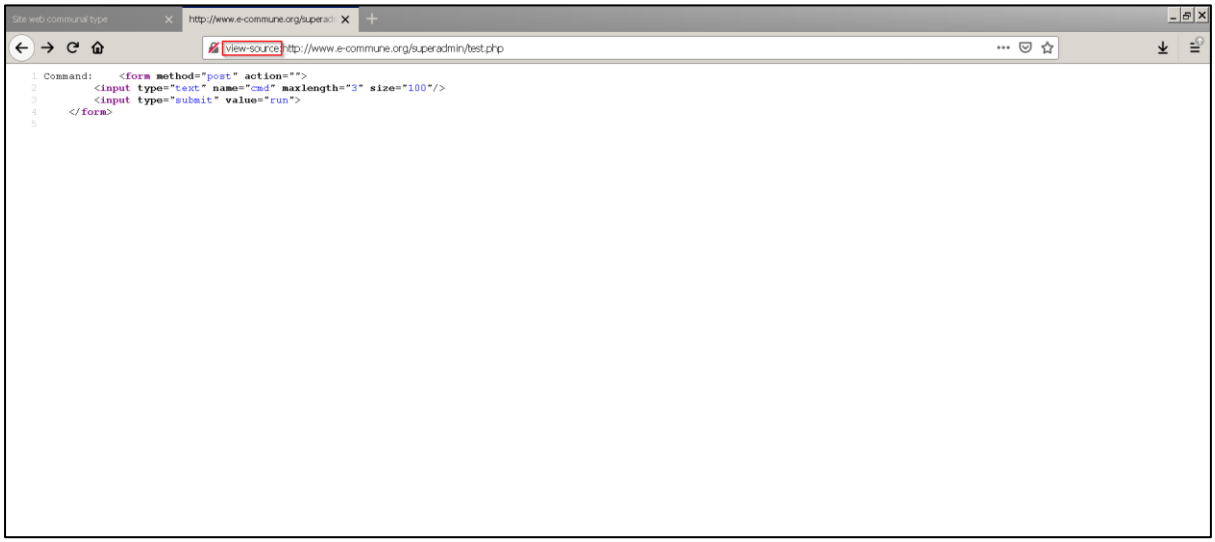
We can see a blank space between the sorce code (upper part of code)

Screenshot : 5



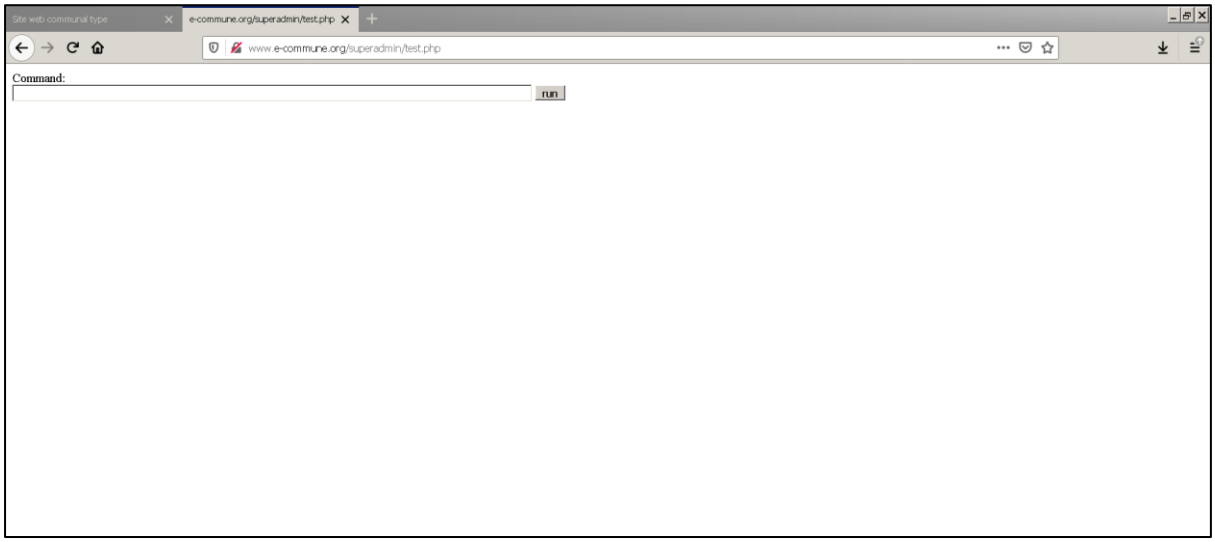
We can see a blank space between the source code (lower part of code)

Screenshot : 6



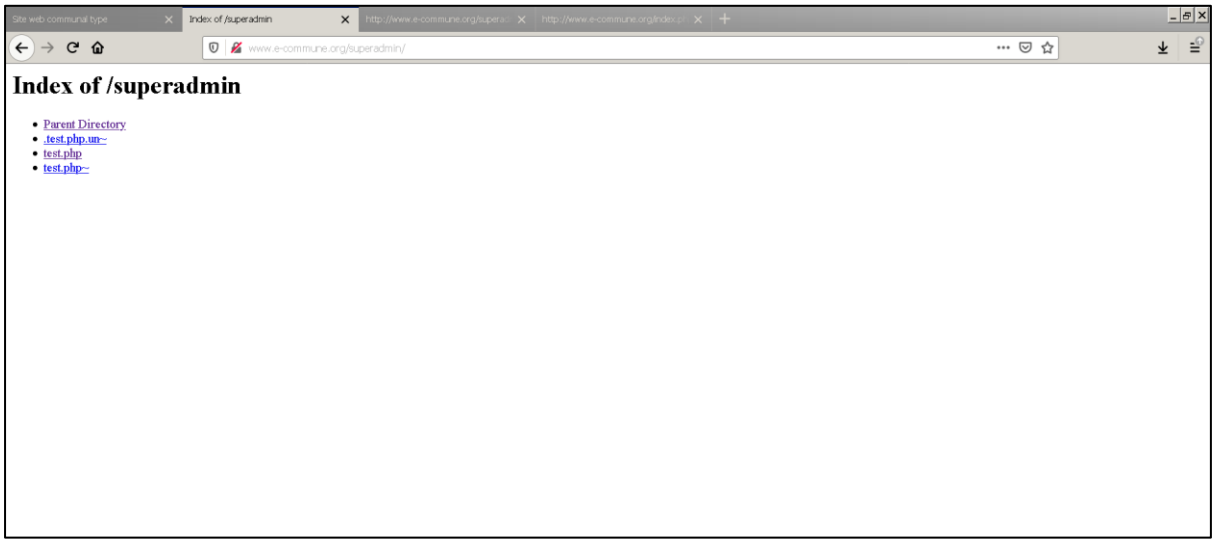
I can see a source code here from superadmin login link and then I removed a view sources from the URL to see the features.

Screenshot : 7



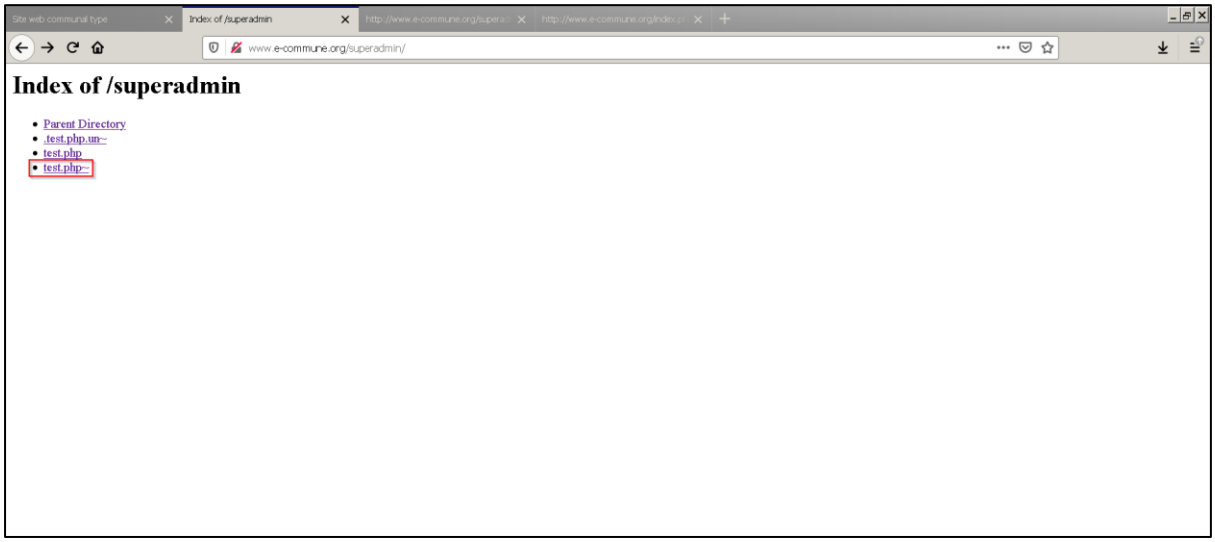
The URL takes me to this page contains a Command search box.

Screenshot : 8



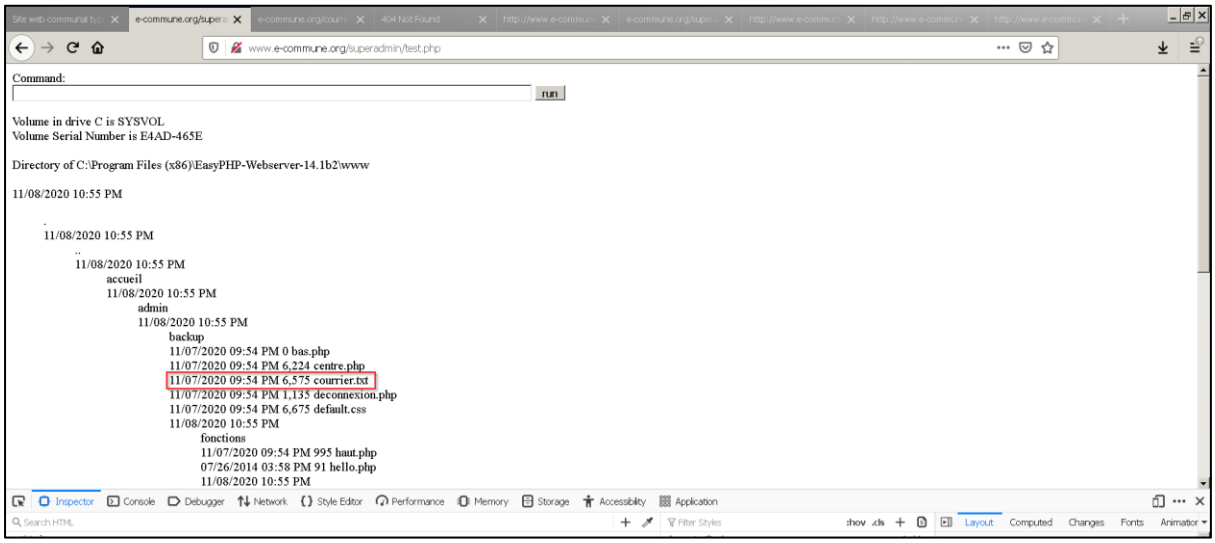
www.e-commune.org/superadmin website page contains directory and undo files.

Screenshot : 9



Index of superadmin page.

Screenshot : 10



Enter a command like dir.. and we can see backup it contains some .txt files

Recommendations:

- Monitor the network frequently and do proper authentication.
- Delete the details which is unnecessary no longer in server.

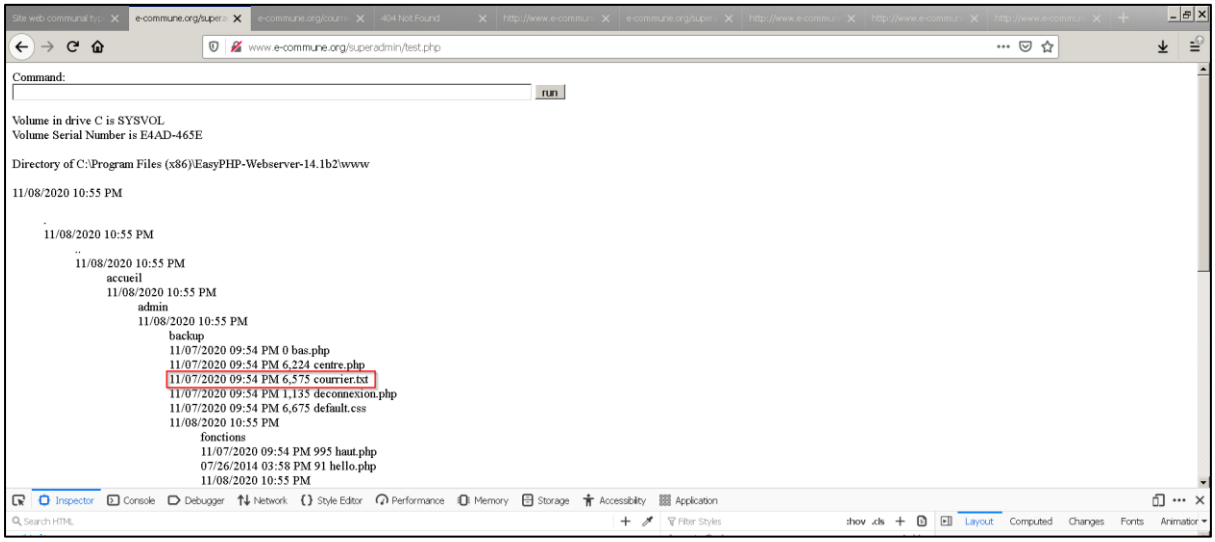
6. Sensitive information (PII + accounts information leaked in /courrier.txt)

Indicators of criticality: high

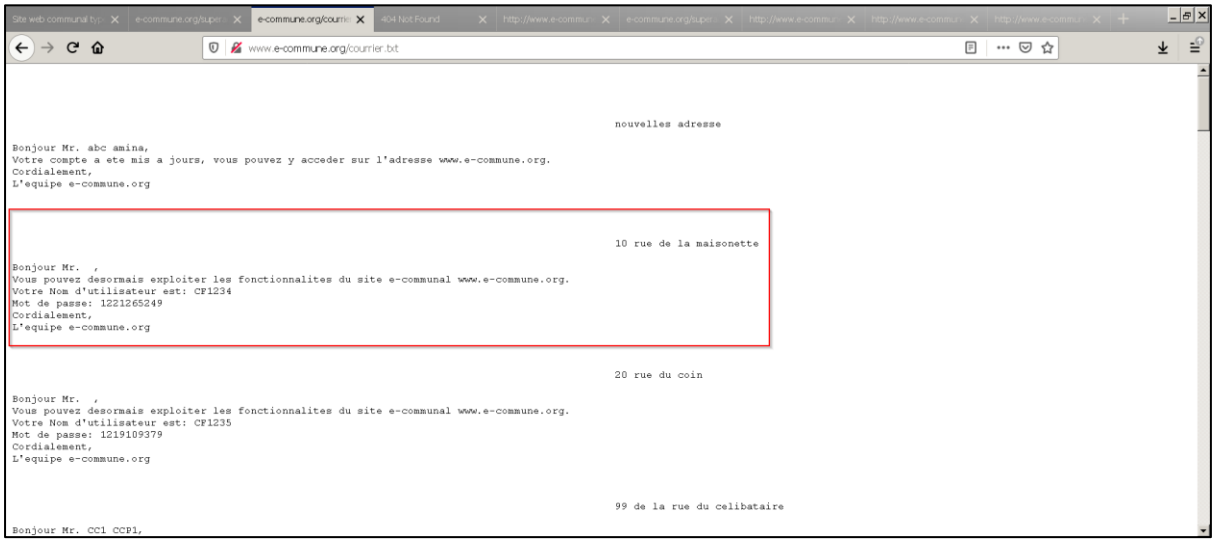
Description: This vulnerability contains an account information present in Courrier.txt file under .test.php undo file in index of super admin**.**

Exploitations:

Under the index of super admin they can see a directory which contains a backup file and some piece of information like date and time.



Under backup there is an courier.txt file



It contains an personal information’s under courier.txt file

Recommendations:

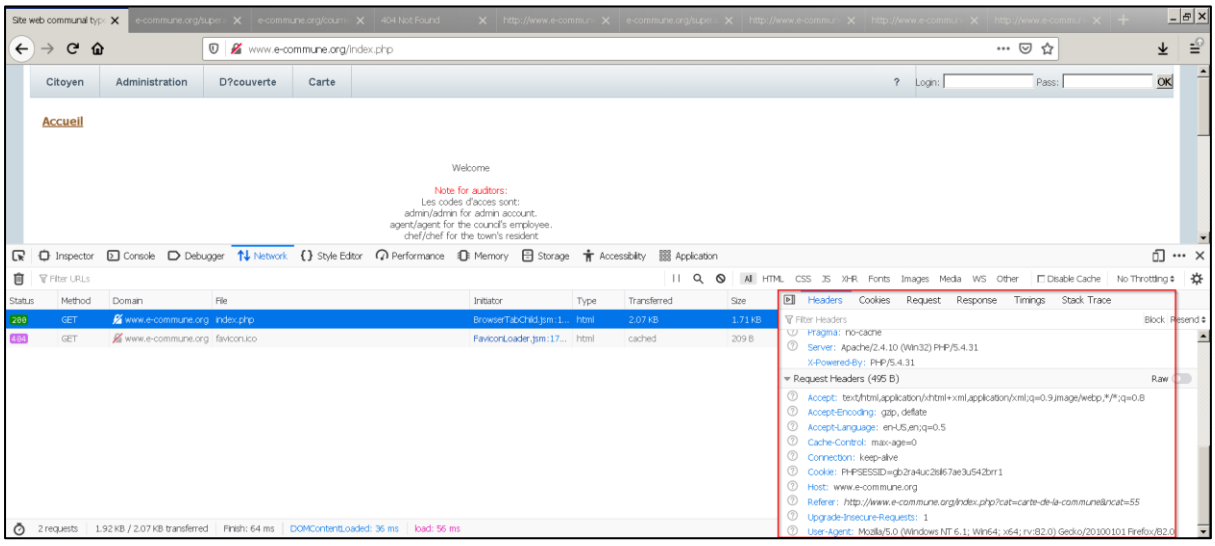
- Monitor all network access.
- Need secure endpoints
- Encrypt all the data in transit with secure protocols such as TCS with perfect forward secrecy (PFS)ciphers , cipher prioritization by the server and secure parameters.
- Enforcing encryption using directives like HTTP strict transport security (HSTS)
- Don't store sensitive unnecessarily.

7. Technication information leakage

Indicators of criticality: Moderate

Description: web server, php engine and operating system versions leakage via ...

Exploitation: in www.e-commune.org website press F12 to inspect the webpage and we can see a network and click somewhere to see the get request and clearly we can see some technical information's in the body of the get request network.



Headers contains an technical information.

Recommendations:

- Ensure that your web-server Banner is not overly-informative. That is, change the "banner" content to mislead an attacker.
- Code Review your page source, active server pages, and supporting files to ensure they are free of "application-sensitive" information that would be included in results.
- Verify that debugging is disabled in production and cannot be enabled through request parameters.
- Ensure that Web Browsers are instructed not to cache responses containing sensitive information