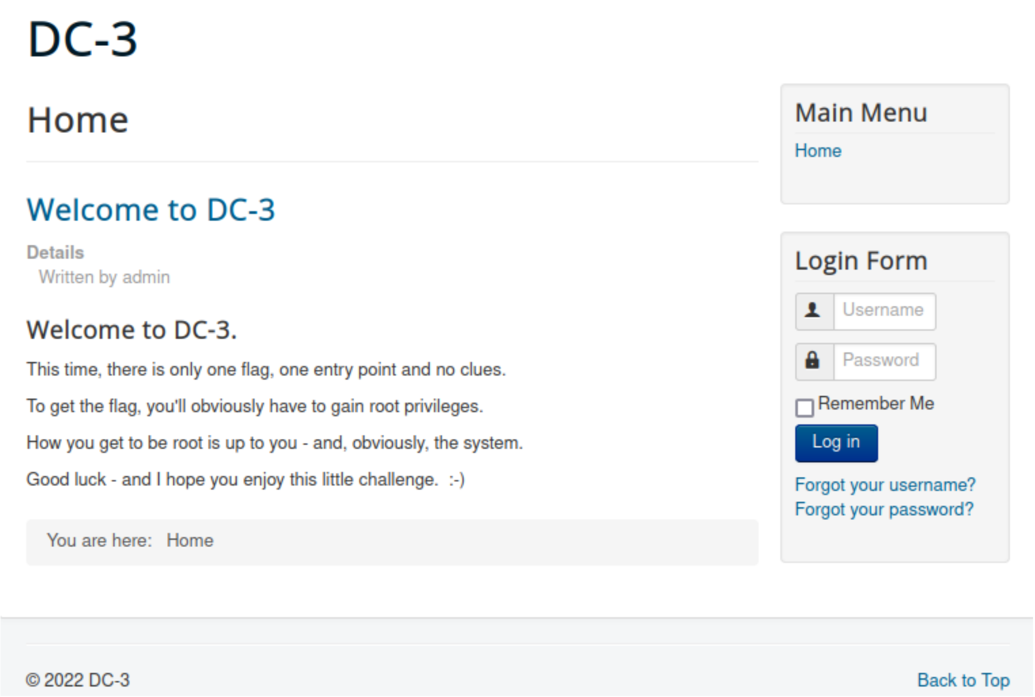
CVE-

DC 3:
https://www.vulnhub.com/entry/dc-32,312/
Write-Up by deusxmachina

Scenario :
Gain root access into a local server with address 10.0.2.10

```
# nmap -p- -A -T4 -vvv 10.0.2.10
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-title: Home
|_http-favicon: Unknown favicon MD5: 1194D7D32448E1F90741A97B42AF91FA
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

Visiting the web server on port 80 :



DC-3

Home

Welcome to DC-3

Details
Written by admin

Welcome to DC-3.

This time, there is only one flag, one entry point and no clues.

To get the flag, you'll obviously have to gain root privileges.

How you get to be root is up to you - and, obviously, the system.

Good luck - and I hope you enjoy this little challenge. :-)

You are here: Home

© 2022 DC-3

Run a scan for web content using ‘feroxbuster’ :

```
# feroxbuster -u http//10.0.2.10 -w
```

```
/usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php -x js -x html
-x old -x bak -x txt
```

-u : target url
-w : path to wordlist for matching web content
-x : file extensions to search for

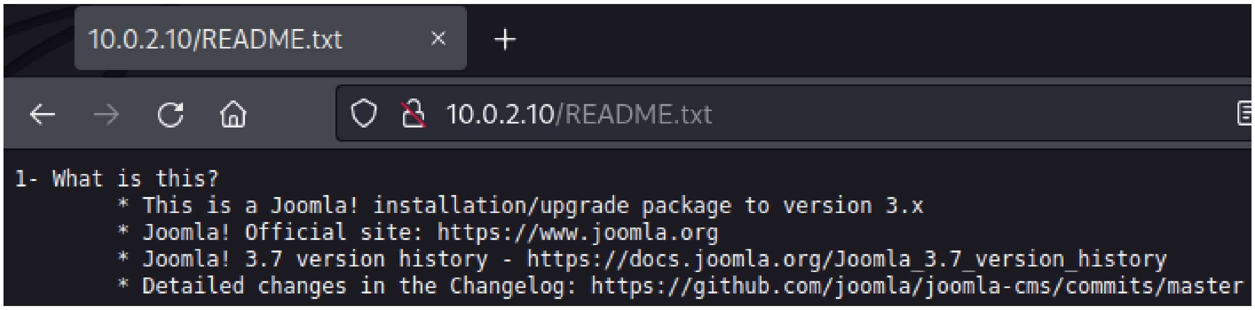
```
301    GET     9l     28w     306c http://10.0.2.10/media => http://10.0.2.10/media/
301    GET     9l     28w     310c http://10.0.2.10/templates => http://10.0.2.10/templates/
200    GET     1l      2w      31c http://10.0.2.10/templates/index.html
301    GET     9l     28w     312c http://10.0.2.10/media/media => http://10.0.2.10/media/media/
301    GET     9l     28w     307c http://10.0.2.10/images => http://10.0.2.10/images/
301    GET     9l     28w     308c http://10.0.2.10/modules => http://10.0.2.10/modules/
200    GET     1l      2w      31c http://10.0.2.10/modules/index.html
301    GET     9l     28w     304c http://10.0.2.10/bin => http://10.0.2.10/bin/
200    GET   203l    507w    7096c http://10.0.2.10/index.php
301    GET     9l     28w     308c http://10.0.2.10/plugins => http://10.0.2.10/plugins/
301    GET     9l     28w     315c http://10.0.2.10/plugins/search => http://10.0.2.10/plugins/search/
200    GET     1l      2w      31c http://10.0.2.10/plugins/index.html
301    GET     9l     28w     316c http://10.0.2.10/plugins/content => http://10.0.2.10/plugins/content/
301    GET     9l     28w     324c http://10.0.2.10/plugins/content/contact => http://10.0.2.10/plugins/content/contact/
301    GET     9l     28w     323c http://10.0.2.10/plugins/search/content => http://10.0.2.10/plugins/search/content/
200    GET     0l      0w       0c http://10.0.2.10/plugins/content/contact/contact.php
301    GET     9l     28w     313c http://10.0.2.10/plugins/user => http://10.0.2.10/plugins/user/
200    GET     0l      0w       0c http://10.0.2.10/plugins/search/content/content.php
301    GET     9l     28w     321c http://10.0.2.10/plugins/user/profile => http://10.0.2.10/plugins/user/profile/
200    GET     1l      2w      31c http://10.0.2.10/images/index.html
301    GET     9l     28w     309c http://10.0.2.10/includes => http://10.0.2.10/includes/
200    GET     1l      2w      31c http://10.0.2.10/bin/index.html
200    GET     1l      2w      31c http://10.0.2.10/media/index.html
301    GET     9l     28w     309c http://10.0.2.10/language => http://10.0.2.10/language/
301    GET     9l     28w     313c http://10.0.2.10/media/system => http://10.0.2.10/media/system/
200    GET    72l    540w    4494c http://10.0.2.10/README.txt
301    GET     9l     28w     315c http://10.0.2.10/images/banners => http://10.0.2.10/images/banners/
301    GET     9l     28w     310c http://10.0.2.10/media/cms => http://10.0.2.10/media/cms/
301    GET     9l     28w     311c http://10.0.2.10/components => http://10.0.2.10/components/
200    GET     0l      0w       0c http://10.0.2.10/plugins/user/profile/profile.php
301    GET     9l     28w     306c http://10.0.2.10/cache => http://10.0.2.10/cache/
200    GET     1l      2w      31c http://10.0.2.10/language/index.html
200    GET     1l      2w      31c http://10.0.2.10/includes/index.html
301    GET     9l     28w     310c http://10.0.2.10/libraries => http://10.0.2.10/libraries/
301    GET     9l     28w     320c http://10.0.2.10/media/system/images => http://10.0.2.10/media/system/images/
200    GET     1l      2w      31c http://10.0.2.10/libraries/index.html
200    GET     1l      2w      31c http://10.0.2.10/cache/index.html
301    GET     9l     28w     320c http://10.0.2.10/plugins/search/tags => http://10.0.2.10/plugins/search/tags/
200    GET     1l      2w      31c http://10.0.2.10/components/index.html
301    GET     9l     28w     317c http://10.0.2.10/media/system/css => http://10.0.2.10/media/system/css/
301    GET     9l     28w     319c http://10.0.2.10/media/media/images => http://10.0.2.10/media/media/images/
301    GET     9l     28w     321c http://10.0.2.10/plugins/content/vote => http://10.0.2.10/plugins/content/vote/
301    GET     9l     28w     316c http://10.0.2.10/media/system/js => http://10.0.2.10/media/system/js/
301    GET     9l     28w     316c http://10.0.2.10/media/media/css => http://10.0.2.10/media/media/css/
301    GET     9l     28w     314c http://10.0.2.10/media/editors => http://10.0.2.10/media/editors/
200    GET     1l    407w   30212c http://10.0.2.10/media/system/js/calendar.js
301    GET     9l     28w     315c http://10.0.2.10/media/media/js => http://10.0.2.10/media/media/js/
301    GET     9l     28w     314c http://10.0.2.10/libraries/cms => http://10.0.2.10/libraries/cms/
301    GET     9l     28w     319c http://10.0.2.10/libraries/cms/help => http://10.0.2.10/libraries/cms/help/
200    GET     0l      0w       0c http://10.0.2.10/libraries/cms.php
200    GET     0l      0w       0c http://10.0.2.10/libraries/cms/help/help.php
301    GET     9l     28w     316c http://10.0.2.10/plugins/editors => http://10.0.2.10/plugins/editors/
301    GET     9l     28w     330c http://10.0.2.10/plugins/user/profile/profiles => http://10.0.2.10/plugins/user/profile/profiles/
200    GET     0l      0w       0c http://10.0.2.10/plugins/search/tags/tags.php
301    GET     9l     28w     323c http://10.0.2.10/plugins/authentication => http://10.0.2.10/plugins/authentication/
301    GET     9l     28w     319c http://10.0.2.10/libraries/cms/html => http://10.0.2.10/libraries/cms/html/
200    GET     0l      0w       0c http://10.0.2.10/libraries/cms/html/links.php
200    GET     0l      0w       0c http://10.0.2.10/libraries/cms/html/list.php
301    GET     9l     28w     313c http://10.0.2.10/media/mailto => http://10.0.2.10/media/mailto/
200    GET     0l      0w       0c http://10.0.2.10/libraries/cms/html/menu.php
301    GET     9l     28w     304c http://10.0.2.10/tmp => http://10.0.2.10/tmp/
200    GET     1l     94w    7512c http://10.0.2.10/media/system/js/core.js
200    GET   339l   2968w   18092c http://10.0.2.10/LICENSE.txt
```

```
403     GET      11l      32w     300c http://10.0.2.10/libraries/vendor
200     GET       0l       0w       0c http://10.0.2.10/libraries/cms/html/tag.php
301     GET       9l      28w     321c http://10.0.2.10/libraries/cms/layout => http://10.0.2.10/libraries/cms/layout/
200     GET       0l       0w       0c http://10.0.2.10/libraries/cms/html/rules.php
301     GET       9l      28w     319c http://10.0.2.10/libraries/cms/form => http://10.0.2.10/libraries/cms/form/
301     GET       9l      28w     324c http://10.0.2.10/libraries/cms/component => http://10.0.2.10/libraries/cms/component/
301     GET       9l      28w     322c http://10.0.2.10/libraries/cms/toolbar => http://10.0.2.10/libraries/cms/toolbar/
200     GET       0l       0w       0c http://10.0.2.10/plugins/content/vote/vote.php
301     GET       9l      28w     323c http://10.0.2.10/libraries/cms/language => http://10.0.2.10/libraries/cms/language/
200     GET      89l     235w    2554c http://10.0.2.10/media/system/js/tabs.js
200     GET       0l       0w       0c http://10.0.2.10/libraries/cms/html/access.php
200     GET       0l       0w       0c http://10.0.2.10/libraries/cms/html/form.php
200     GET       0l       0w       0c http://10.0.2.10/libraries/cms/html/date.php
200     GET      80l     493w    3005c http://10.0.2.10/htaccess.txt
301     GET       9l      28w     326c http://10.0.2.10/plugins/content/vote/tmpl => http://10.0.2.10/plugins/content/vote/tmpl/
200     GET       0l       0w       0c http://10.0.2.10/libraries/loader.php
```

And because we received a lot of 300 series HTTP messages (301 code indicates the requested resource was permanently moved to url given by the Locations header), I added the ‘-r’ option :
So now we only get 200 series HTTP messages (200 code indicates that the resource has been fetched and transmitted in the message body).

```
# feroxbuster -u http//10.0.2.10 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php -x js -x html -x old -x bak -x txt -r
-r : follow redirects
200     GET       1l       2w      31c http://10.0.2.10/images/
200     GET       1l       2w      31c http://10.0.2.10/media/
200     GET       1l       2w      31c http://10.0.2.10/templates/
200     GET       1l       2w      31c http://10.0.2.10/modules/
200     GET       1l       2w      31c http://10.0.2.10/modules/index.html
200     GET       1l       2w      31c http://10.0.2.10/images/index.html
200     GET     203l     507w    7096c http://10.0.2.10/index.php
200     GET      20l      95w    1791c http://10.0.2.10/images/banners/
200     GET      18l      82w    1322c http://10.0.2.10/media/media/
200     GET       1l       2w      31c http://10.0.2.10/templates/index.html
200     GET       0l       0w       0c http://10.0.2.10/templates/system/
200     GET       1l       2w      31c http://10.0.2.10/bin/
200     GET       1l       2w      31c http://10.0.2.10/plugins/
200     GET       1l       2w      31c http://10.0.2.10/includes/
200     GET      20l      99w    1787c http://10.0.2.10/images/headers/
200     GET       1l       2w      31c http://10.0.2.10/media/index.html
200     GET      16l      59w     988c http://10.0.2.10/templates/system/html/
200     GET      24l     148w    2546c http://10.0.2.10/plugins/content/
200     GET       1l       2w      31c http://10.0.2.10/language/
200     GET       1l       2w      31c http://10.0.2.10/language/index.html
200     GET      72l     540w    4494c http://10.0.2.10/README.txt
200     GET      16l      60w     954c http://10.0.2.10/media/contacts/
200     GET       1l       2w      31c http://10.0.2.10/bin/index.html
200     GET      21l     115w    1962c http://10.0.2.10/plugins/search/
200     GET      23l     129w    2529c http://10.0.2.10/templates/system/images/
200     GET       1l       2w      31c http://10.0.2.10/includes/index.html
200     GET       0l       0w       0c http://10.0.2.10/templates/system/index.php
200     GET       1l       2w      31c http://10.0.2.10/components/
200     GET      18l      82w    1358c http://10.0.2.10/plugins/user/
200     GET       1l       2w      31c http://10.0.2.10/cache/
200     GET       1l       2w      31c http://10.0.2.10/libraries/
200     GET       1l       2w      31c http://10.0.2.10/cache/index.html
200     GET      19l      92w    1575c http://10.0.2.10/plugins/user/profile/
200     GET      17l      70w    1191c http://10.0.2.10/plugins/search/content/
200     GET       0l       0w       0c http://10.0.2.10/templates/system/html/modules.php
200     GET       1l       2w      31c http://10.0.2.10/components/index.html
200     GET      31l     225w    3922c http://10.0.2.10/plugins/system/
200     GET      23l     125w    2387c http://10.0.2.10/templates/system/css/
200     GET      28l     182w    3693c http://10.0.2.10/media/media/js/
200     GET      16l      60w     964c http://10.0.2.10/plugins/captcha/
200     GET      17l      69w    1167c http://10.0.2.10/plugins/system/log/
200     GET      18l      82w    1400c http://10.0.2.10/plugins/installer/
```

A quick look into the http://10.0.2.10/README.txt an we find that it is running Joomla version 3.7 :



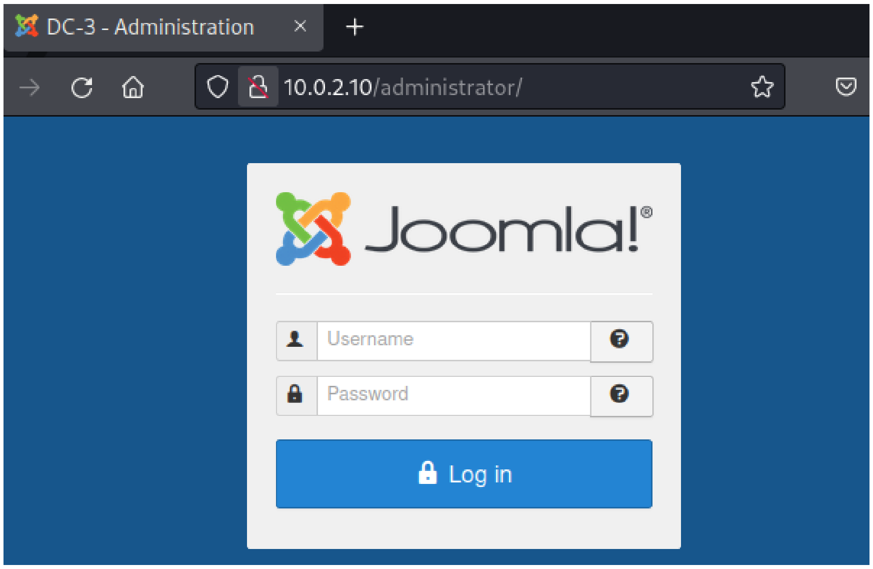
```
1- What is this?
	* This is a Joomla! installation/upgrade package to version 3.x
	* Joomla! Official site: https://www.joomla.org
	* Joomla! 3.7 version history - https://docs.joomla.org/Joomla_3.7_version_history
	* Detailed changes in the Changelog: https://github.com/joomla/joomla-cms/commits/master
```

Joomla is a content management system (CMS), similar to wordpress or drupal. We use a Joomla pentesting tool 'joomscan' to enumerate/search for weak points :

We found the administrator page where we can login!

```
# apt install joomscan -y
# joomscan -u http://10.0.2.10
[+] Detecting Joomla Version
[++] Joomla 3.7.0
[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable
[+] Checking Directory Listing
[++] directory has directory listing :
http://10.0.2.10/administrator/components
http://10.0.2.10/administrator/modules
http://10.0.2.10/administrator/templates
http://10.0.2.10/images/banners
[+] Checking apache info/status files
[++] Readable info/status files are not found
[+] admin finder
[++] Admin page : http://10.0.2.10/administrator/
```

If we get stuck along the way, we can now at least brute force logins (hopefully as a last resort).



I looked up exploits for the specific Joomla v3.7 and came up with some promising results :

```
# searchsploit joomla 3.7
----------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                            |  Path
----------------------------------------------------------------------------------------- ---------------------------------
Joomla! 3.7 - SQL Injection                                                               | php/remote/44227.php
Joomla! 3.7.0 - 'com_fields' SQL Injection                                                | php/webapps/42033.txt
Joomla! Component ARI Quiz 3.7.4 - SQL Injection                                          | php/webapps/46769.txt
Joomla! Component com_realestatemanager 3.7 - SQL Injection                               | php/webapps/38445.txt
Joomla! Component Easydiscuss < 4.0.21 - Cross-Site Scripting                             | php/webapps/43488.txt
Joomla! Component J2Store < 3.3.7 - SQL Injection                                         | php/webapps/46467.txt
Joomla! Component JomEstate PRO 3.7 - 'id' SQL Injection                                  | php/webapps/44117.txt
Joomla! Component Jtag Members Directory 5.3.7 - Arbitrary File Download                  | php/webapps/43913.txt
Joomla! Component Quiz Deluxe 3.7.4 - SQL Injection                                       | php/webapps/42589.txt
----------------------------------------------------------------------------------------- ---------------------------------
```