Attack path:

Using gobuster, I saw that there was a todo.txt for someone named Fergus, who could be a user. After searching up Bludit exploits, I saw that there was a directory traversal attack, and an exploit that brute forces passwords. The ruby script for the brute force attack had compatibility issues with Kali, but I found a python script here:
https://rastating.github.io/bludit-brute-force-mitigation-bypass/
I made some minor changes to the script so that the targets were correct, and so that the python script received an input file from argv[1].
At first, I used dirbuster's common words and johntheripper's passwords but neither worked, so I used cewl to scrape words from the website with the command:
cewl -w wordlist.txt -d 10 -m 1 10.10.10.191.
-w is the output file
-d is the depth of the crawler
-m is the maximum length of the password
I found that the user:password was fergus:RolandDeschain
Using the credentials, I used the directory traversal attack module in Metasploit to start a meterpreter session. I found a directory called ftp in / directory, and there was a note.txt from Shaun but it didn't seem to be that useful. After a bit more enumeration, I found a /database/users.php file in /var/www, which contained a Sha-1 hash as a password for user hugo. Decoded, the sha-1 hash translates to Password120.
Using su (switch user) hugo, and entering the password, I can access the user.txt file. I then use sudo -l to look at what permissions I have. Unfortunately, I cannot sudo su into root. However, using the command sudo -u#-1 bash, I can priv esc to root. The exploit is detailed here:
https://blog.aquasec.com/cve-2019-14287-sudo-linux-vulnerability