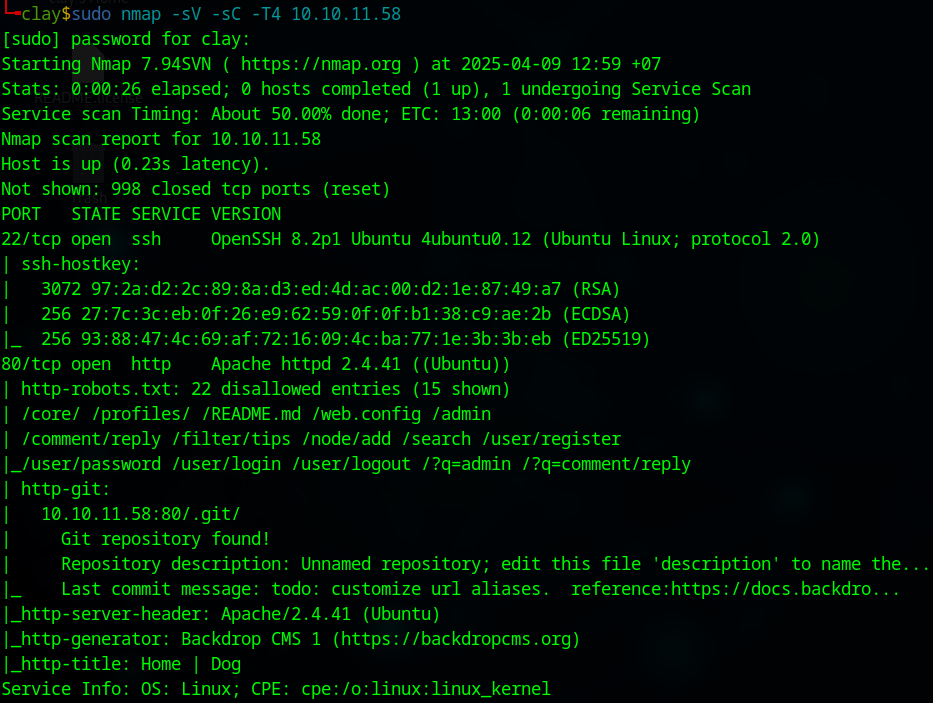
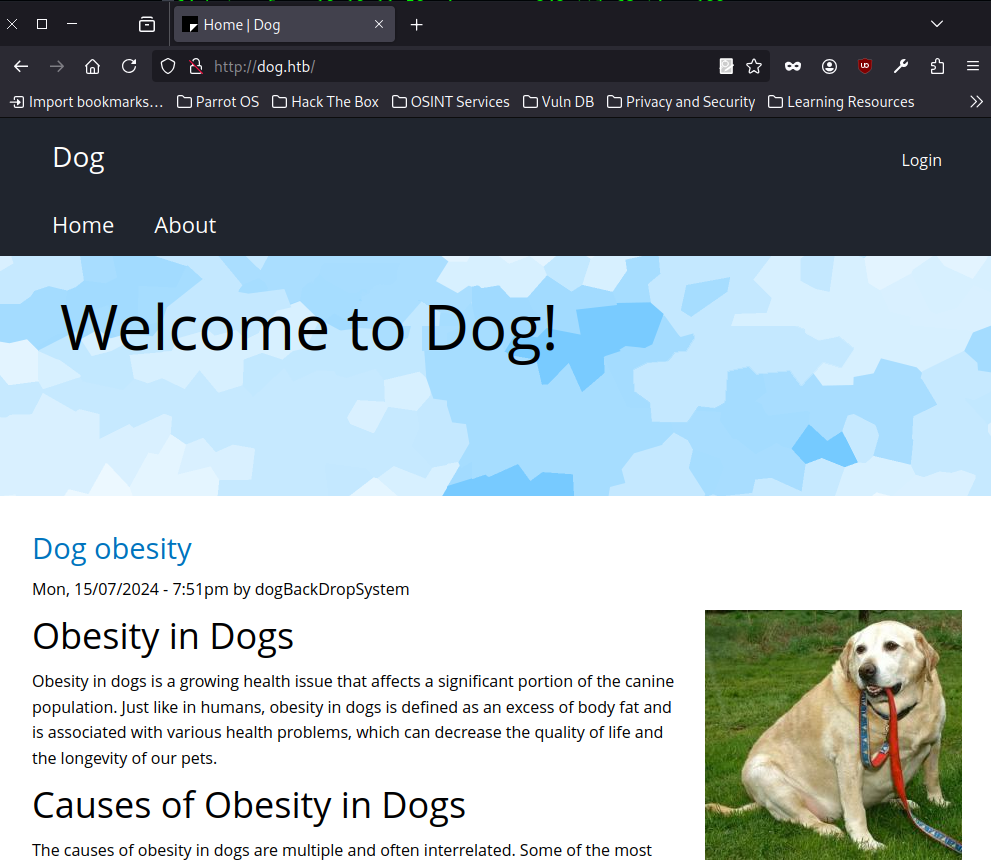
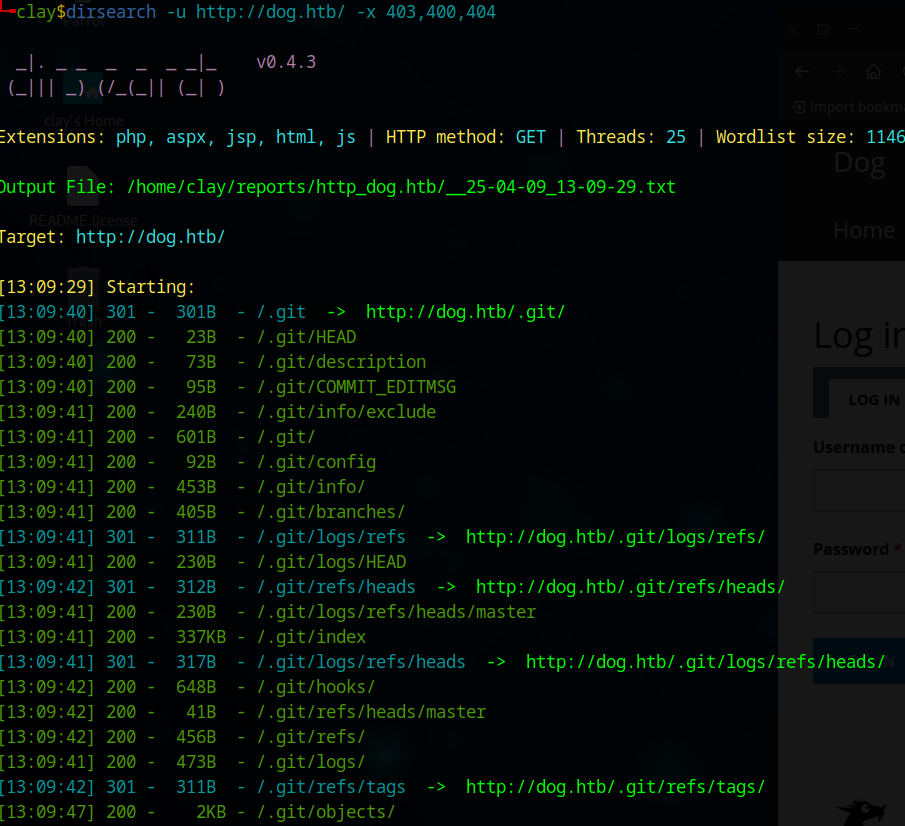
B1: Scanning and enumeration



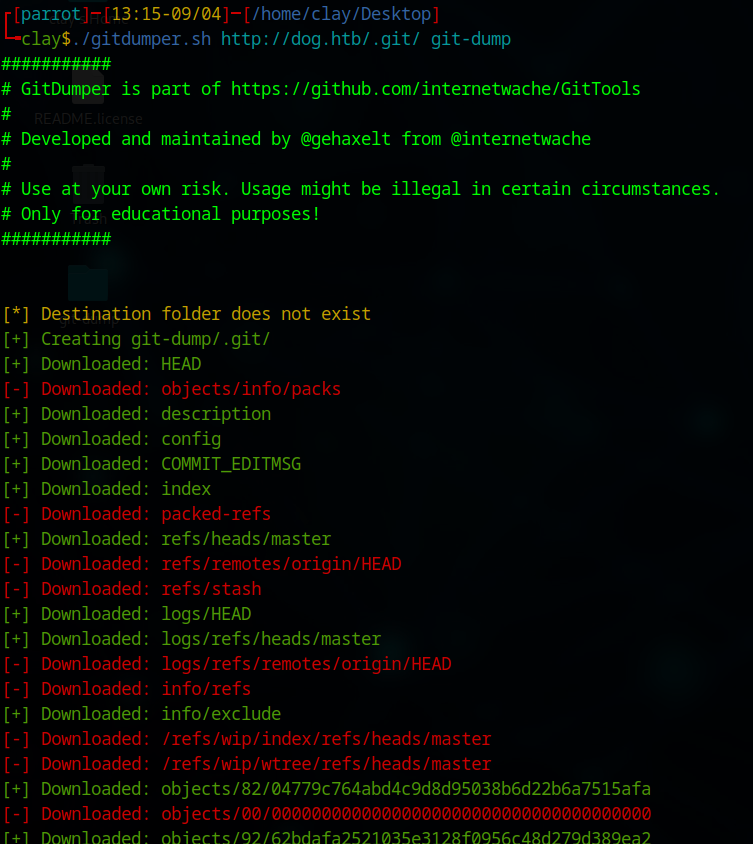
Truy cập vào trang web



Ta dùng dirsearch để xem các thư mục có trong server

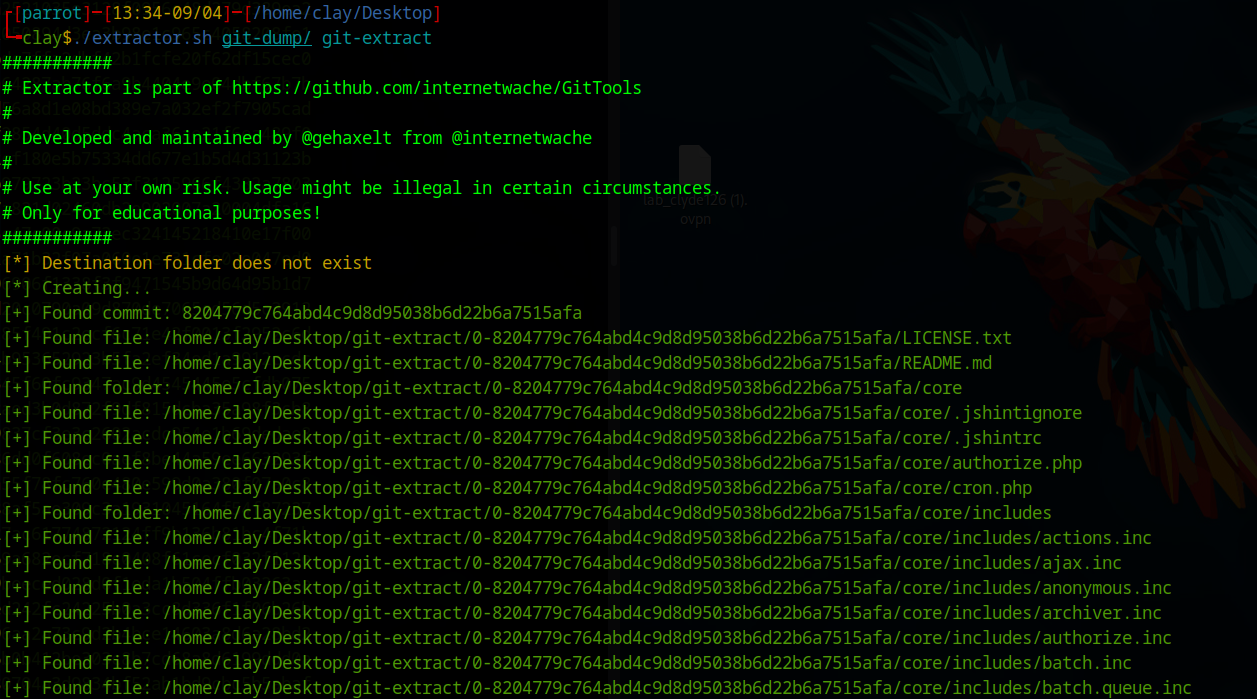


Có 1 thư mục là .git -> sử dụng git dumper để xem các thư mục hay ho

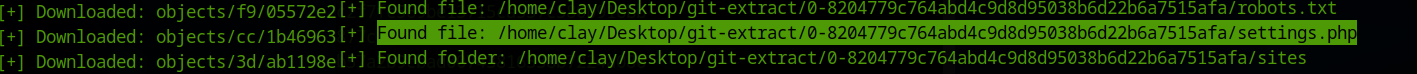


\

Sử dụng extractor

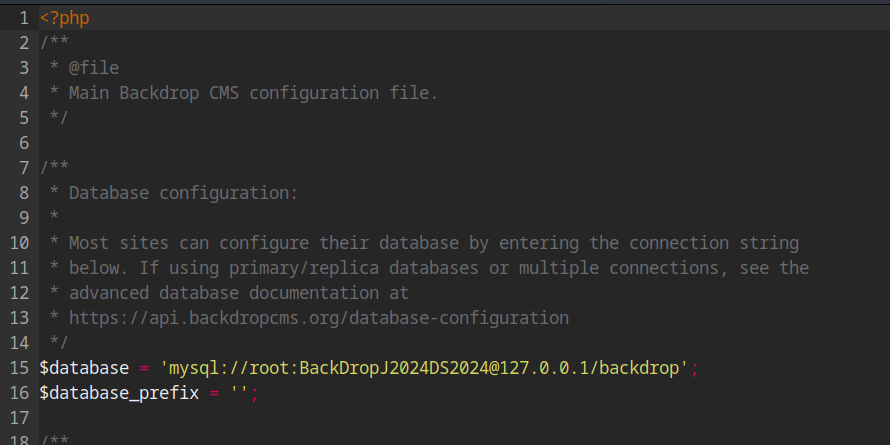


Ta thấy có 1 file setting.php



'mysql://root:BackDropJ2024DS2024@127.0.0.1/backdrop';

Ta thấy được địa chỉ của db



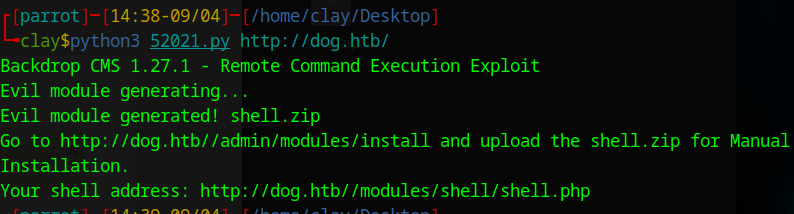
'mysql://root:BackDropJ2024DS2024@127.0.0.1/backdrop';

Ta tìm thấy tài khoản email [tiffany@dog.htb](http://tiffany@dog.htb) và kết hợp với password ở trên ta có thể đăng nhập vào với admin

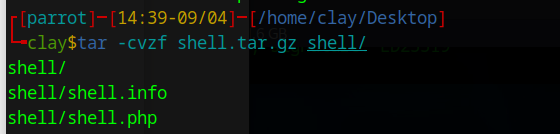
[Backdrop CMS 1.27.1 - Authenticated Remote Command Execution (RCE) - PHP webapps Exploit](https://www.exploit-db.com/exploits/52021)

Tìm thấy 1 POC trên dịch vụ backdrop cms có thể làm theo

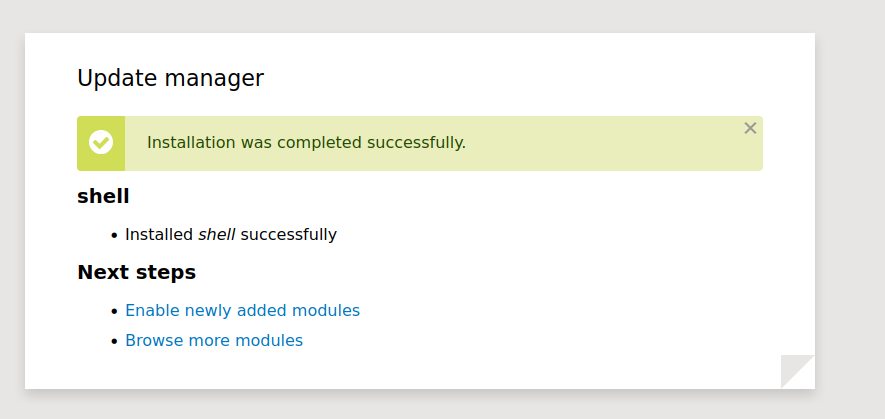
Ta chạy file .py và nhận dc 1 file zip có chứa 1 file shell.php



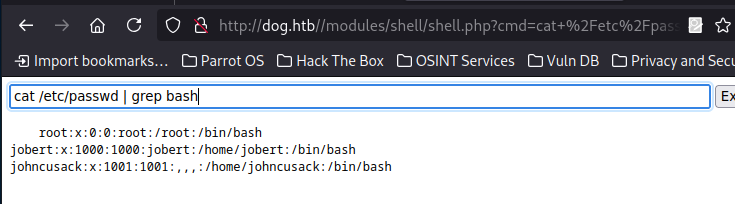
Ta nén dưới định dạng tar.gz vì web chỉ nhận định dạng này



Đăng tải file thành công lên

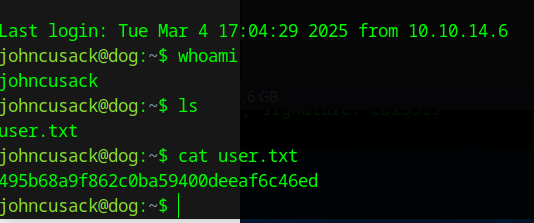


Mở được 1 shell tại địa chỉ <http://dog.htb//modules/shell/shell.php>



-> thấy được có 2 tài khoản có thể dùng dc shell.

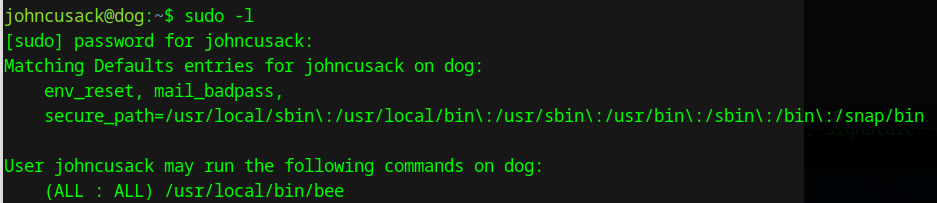
Ta ssh vào với mk có được ở trên



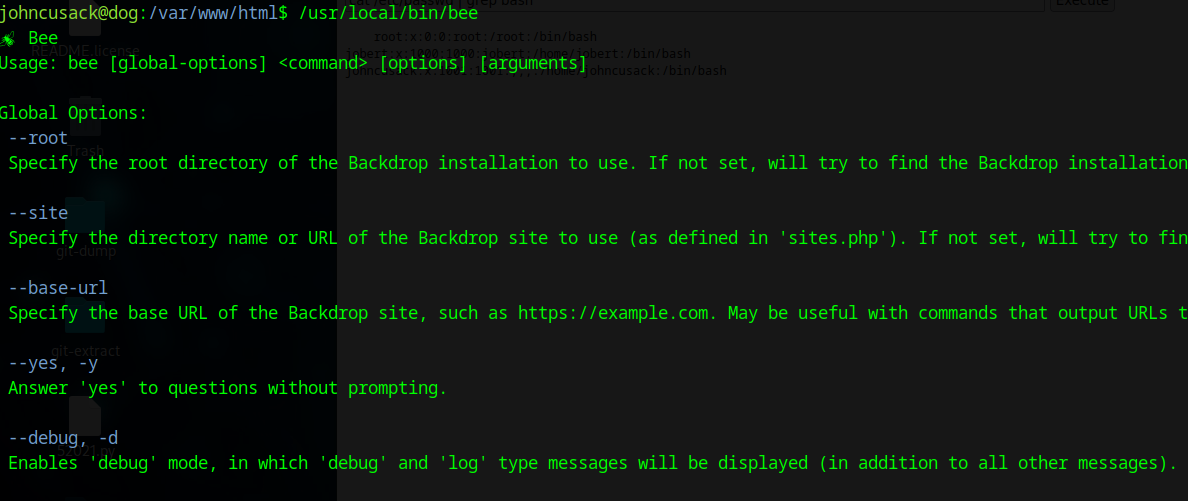
Lấy được user flag

B4 Leo thang đặc quyền lấy root

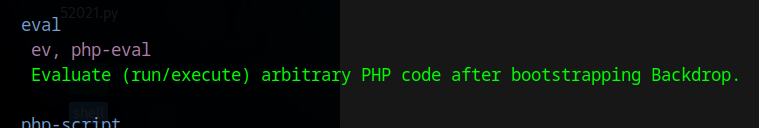
Kiểm tra các câu lệnh có thể chạy được



Xem hướng dẫn sử dụng



Tool có thể dùng để chạy code php



Ta tận dụng để có thể chạy với lựa chọn —root để lựa chọn root directory và tool này có thể thực hiện đoạn mã php, và rồi ta mở 1 shell



-> Có được root flag

