Bilet 6

Oybek Boltaboyev

1-savol:
Linux terminal komandalarini bilish qanday vazifalarda qo'l keladi ?

2-savol:
Linux tizimida Python virtual muhiti yaratish va paketlarni o'rnatish qanday amalga oshiriladi?

3-savol: Kali Linux va Windows ni virtual mashina ishlatishning muhim jihatlari qanday?

1-topshiriq: Linux terminalda df va du buyruqlarini ishlatib, diskdagi bo'sh joy va fayl tizimining hajmini tahlil qiling. Buyruqlarni yozing va natijalarni ko'rsating.

2-topshiriq: Burp suite yordamida veb-saytdagi ma'lum bir zaiflikni toping va report yozing.

3-topshiriq: Pythonda matnli fayldagi barcha elektron pochta manzillarini topib, ularni alohida faylga yozish skriptini yozing. Kodni va natijalarni ko'rsating.

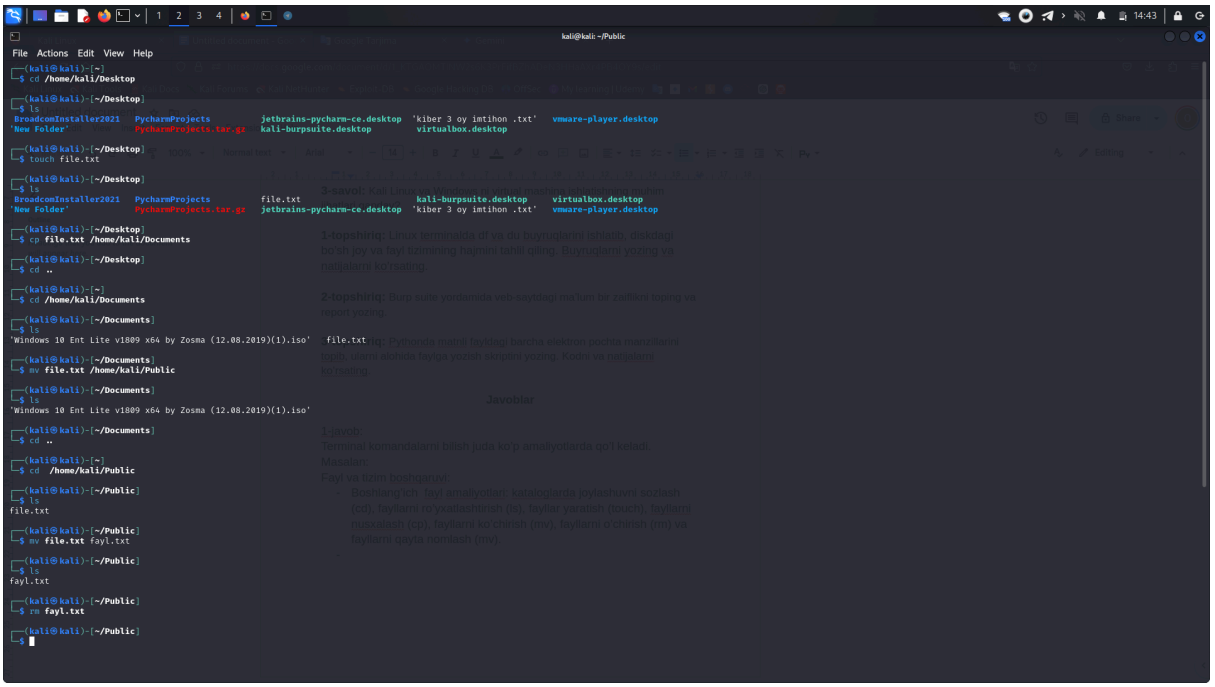
Javoblar

1-javob:

Terminal komandalarni bilish keng ko'lamli vazifalrda foydalidir, asosan texnik bosqichda kompyuterlar va serverlar bilan ishlovchilar uchun.
Masalan:
Fayl va tizim boshqaruvi:

- Boshlang'ich fayl amaliyotlari: kataloglarda joylashuvni sozlash (cd), fayllarni ro'yxatlashtirish (ls), fayllar yaratish (touch), fayllarni nusxalash (cp), fayllarni ko'chirish (mv), fayllarni o'chirish (rm) va fayllarni qayta nomlash (mv).

- Ruxsatlar va egalik : fayl ruxsatlarini (chmod, chown) va kirish nazoratini boshqarish.
- Disk foydalanilishi: qurilmangizda qancha ko’p bo’sh joy mavjudligini ko’rish uchun disk foydalanilishini tekshiring (df).



Dasturiy ta’minot o’rnatish va boshqarish:

- Paket boshqaruvi: dasturiy ta’minot paketlarini o’rnatish, yangilash va olib tashlash uchun apt-get yoki yum kabi paket menejerlaridan foydalaning.
- Bog’liqlikni boshqarish: Dasturiy ta’minotni o’rnatayotganda bog’liqlikni boshqaring, barcha talab qilingan paketlar o’rnatilganiga ishonch hosil qiling.

2-javob:

Linux tizimizda python muhitini yaratish va o’rnatish bir necha bosqichlarni o’z ichiga oladi.

Dastlab, Python va pip (python uchun paket o’rnatuvchi) tizimingizda o’rnatilganiga ishonch hosil qiling. Agar unday bo’lmasa, versiyangizning paket boshqaruvchisi yordamida ularni o’rnata olasiz.

Keyin ‘venv’ modulidan foydalanib virtual muhit yarating. Bu modul Python va paketlarning turli xil versiyalari mavjud bo’lgan izolatsiya-

langan Python muhitini yaratishga imkon beradi. Yangi virtual muhit yaratish uchun ‘python -m venv myenv’ buyrug’ini ‘myenv’ o’rniga o’zingizning virtual muhitingizni nomiga almashtirib bajaring.

VM yaratilgandan so’ng uni ‘source/myenv/bin/activate’ buyrug’ini bajarish bilan faollashtiringiz mumkin. Bu hozir virtual muhitda ishlayotganingizni bildirish uchun terminalingiz so‘rovini o‘zgartiradi.

VM ichida siz pip dan foydalanib paketlarni o’rnatishingiz mumkin. Misol uchun, ‘requests’ kutubxonasini o’rnatish uchun, ‘pip install requests’ buyrug’ini bajaring. Bir vaqtning o’zida bir nechta paketlarni birdan yuklab olishingiz mumkinn. Buning uchun ularning orasini bo’shliq bilan ajratib yozishingiz kerak:’pip install requests beatifulsoup4’

VM bilan ishingizni tugatganingizda siz ‘deactivate’ buyrug’ini bajarish bilan faoliyatni to’xtatolasiz. Bu sizning tizimingizni standart python muhitiga qaytaradi.

Bu qadamlarga ergashish orqali siz linux tizimida istalgan python moduli yaratishingiz va kerakli bo’lgan paketlarni o’rnaishingiz mumkin. Yana bular orqali siz loyihalaringiz kerakli bog’liklariga ega bo’lishini va boshqa loyihalarga tizimning standart Pythin muhitiga xalaqit bermasligiga ishonch hosil qilishingiz mumkin.

3-javob:

Ushbu savolga javob berishdan oldin shuni eslatib o’tishimiz kerakki, kali va/yoki windowsni virtual muhit sifatida ishlatish uchun sizning qurilmangiz uchun ba’zi ta’lablar mavjud:

1. VT-x yoki AMD-V: sizning CPU ingiz uskuna virtualizatsiyasini ta’minlashiga ishonch hosil qiling(Intel uchun VT-x yoki AMD uchun AMD-V)
2. RAM taqsimoti: VM ga yetarlicha RAM ajrating. Ishlatayotganingiz operaatsion tizim va ishlanmalarni hisobga oling. Minimal 4 GB tavsiya etiladi, lekin 8 GB yoki undan ko'p ideal bo’ladi.

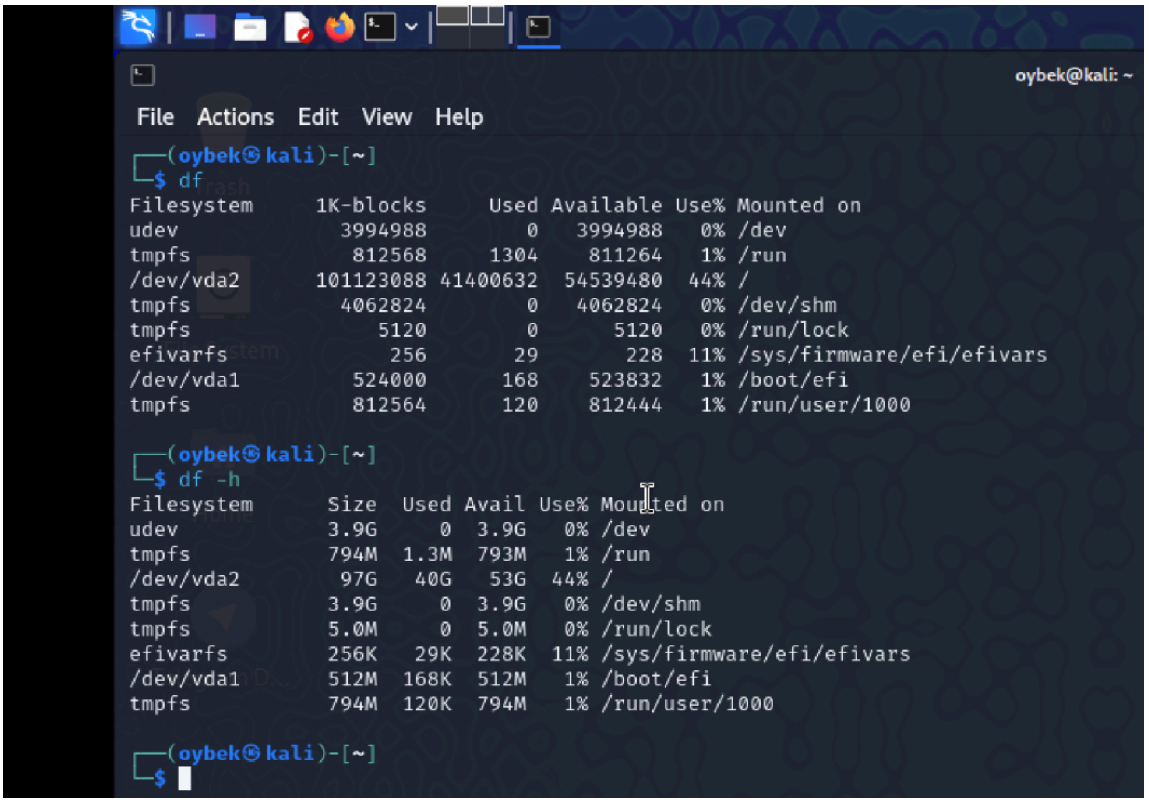
Bulardan keyin ham operatsion tizim, fayllar, tarmoqlar va parollar bilan bog’liq ba’zi bir sozlamalarni amalga oshirishingiz kerak bo’ladi. Shundagina siz hackerlik mahoratingizni nazorat qilingan muhitda sinash va mashq qilish imkonini beruvchi Kali Linux va Windows OTlarini virtual mashina sifatida ishlata olasiz. Virtualizatsiya sizga qurilmalar xaridi, sozlamalari kabi real voqealikda qiyinchilik tug’diradigan ko’pgina

jihatlarda qo’l kelishi mumkin. Va yana bu hakerlik mahorati ustida ishlashning ancha bezarar yo’lidir.

1-amaliyot. ‘df’ va ‘du’ buyruqlari disk hajmi va fayl tizim o’lchamini tahlil qilish uchun muhim vositalardir. Quyida ulardan qanday foydalanishni ko’rib chiqamiz:

df buyrug’i “erkin disk” degan ma’noni anglatadi v ao’rnatilgan fayl tizmida mavjud disk hajmini ko’rsatish uchun ishlatiladi. U fayl tizimi, ishlatilgan qismi, bo’sh qismi va ishlatilgan qismning foizi haqidagi axborot bilan ta’minlaydi.

Buyruqdan foydalanish uchun shunchaki terminalda df deb yozib, enterni bosish kifoya va displayda barcha o’rnatilgan fayl tizimlari, ularning umumiy hajmi, ishlatilgan va bo’sh qimi bilan birga aks etadi.



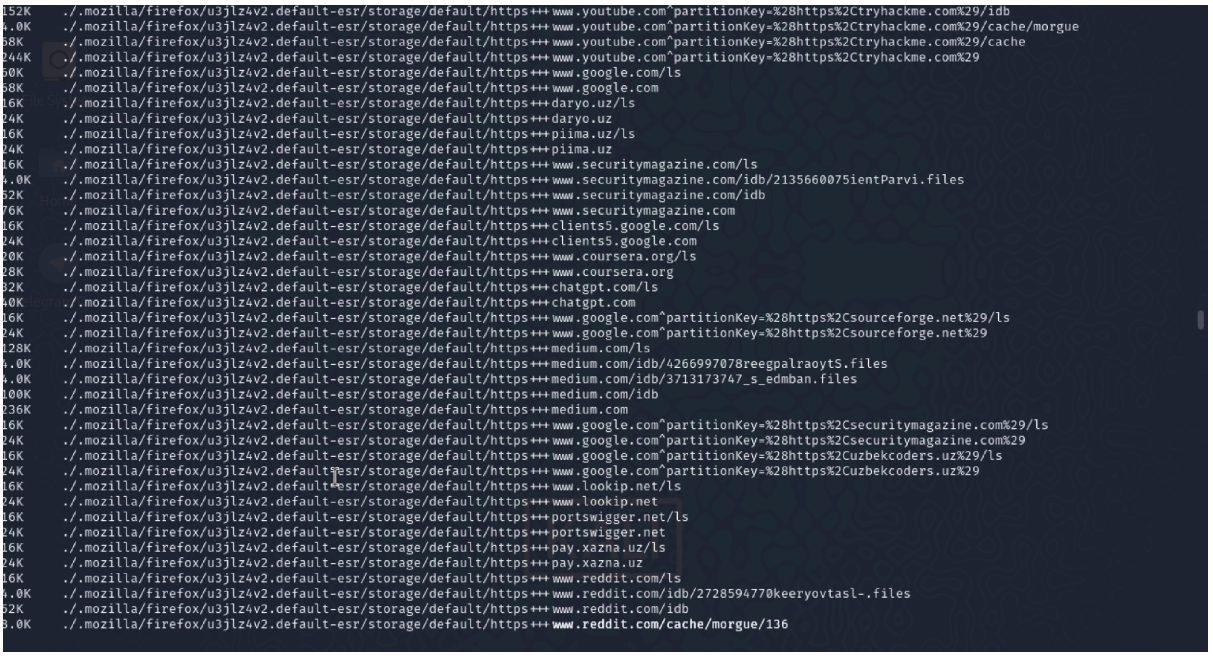
Bu yerda ‘-h’ qo’shimchasi inson ma’lumot hajmini GB, MB kabi inson tushunadigan tilda aks ettirish uchun qo’llanildi.

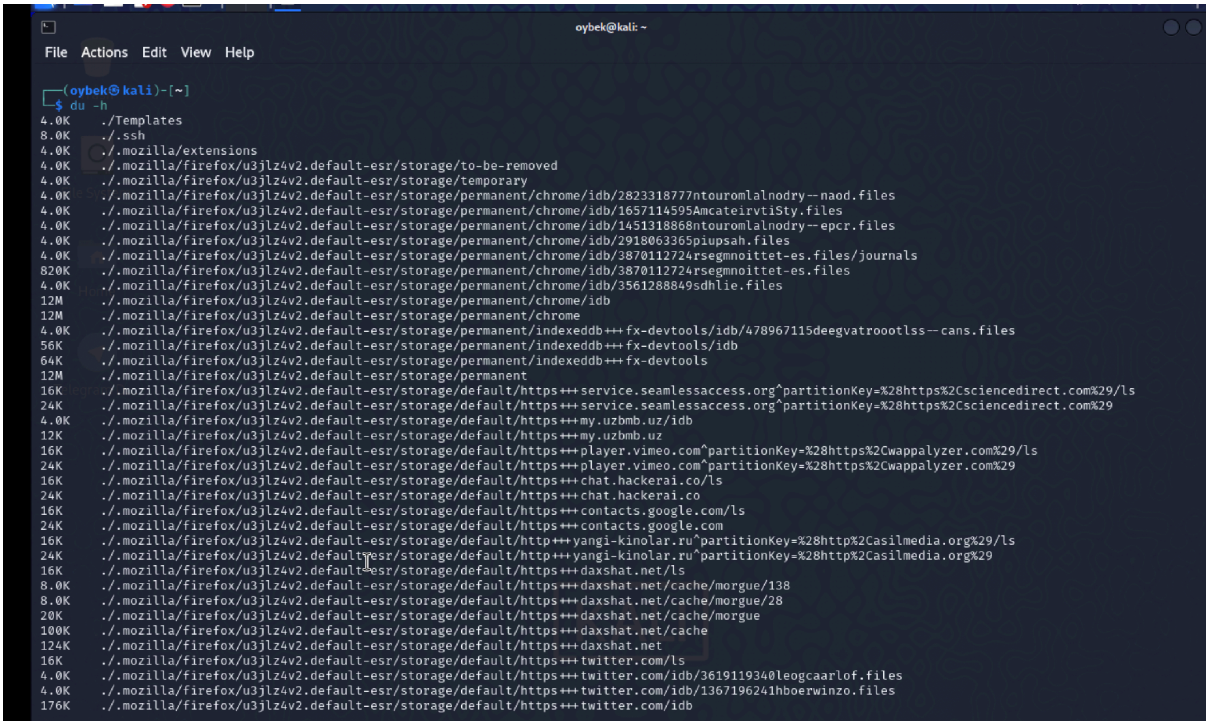
Ustunlarda ko’rstailgan:

- Filesystem: hisobot berilayotgan fayl tizimi.
- Size: fayl tizimining umumiy hajmi
- Used: fayl tizimida ishlatilgan hajm miqdori
- Avail: fayl tizimida mavjud hajm miqdori

- Use%: fayl tizimida ishlatilgan hajm foizi.
- Mounted on: fayl tizimining o’rnatilgan nuqtasi (ya’ni, u o’rnatilgan katalog).

du buyrug’i disk foydalanilishi degan ma’noni anglatadi va katalog/fayl hajmini baholash uchun ishlatiladi. U fayl/katalog hajmi haqidagi axborotni uning subkatalog va fayllari haqidagi ma’lumot bilan birga ta’minlaydi.





Displayda fayl/katalogning hajmi bilan birga unga olib boradigan yo’nalish ham aks ettiriladi.

2- topshiriq: Report yozish.

Tavsifi: aks ettiriladigan tomonlararo skript zaifligi(XSS).

Sinalgan URL: 192.168.154.202/dvwa/vulnerabilities/xss_r/

Yuklama: `<script>alert('XSS')</script>`

Bajarilishi: burpsuite da pakeni ushlab olib cookie qismidagi xavfsizlik darajasini pasaytiramiz.

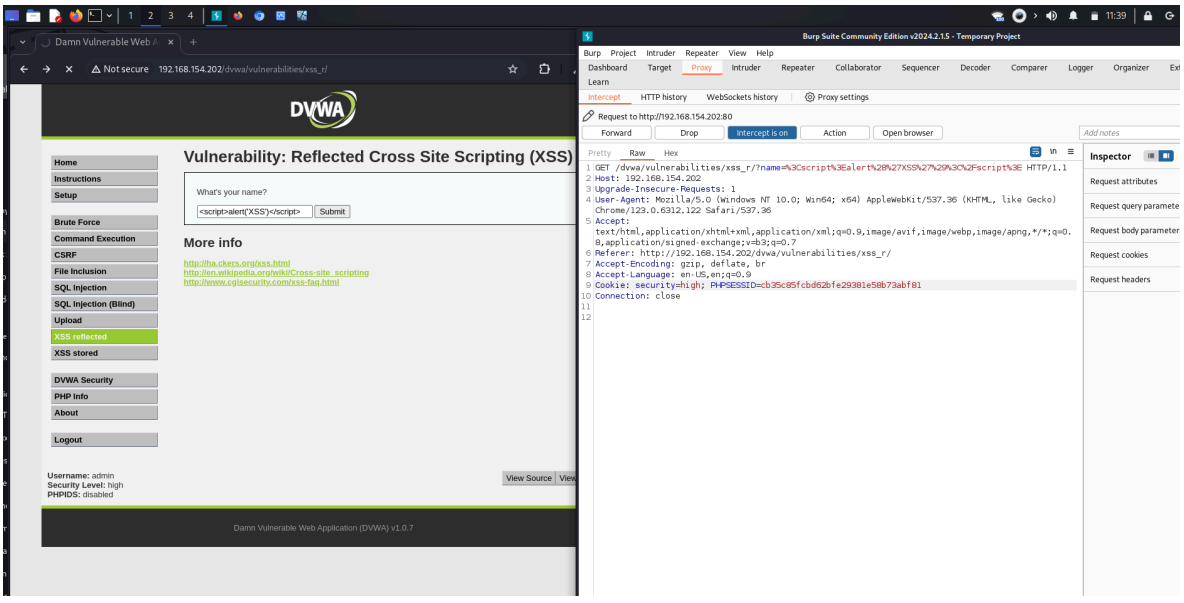
Ta’siri: bu zaiflikni egallash orqali hujumchilar quyidagilarni bajarishi mumkin:

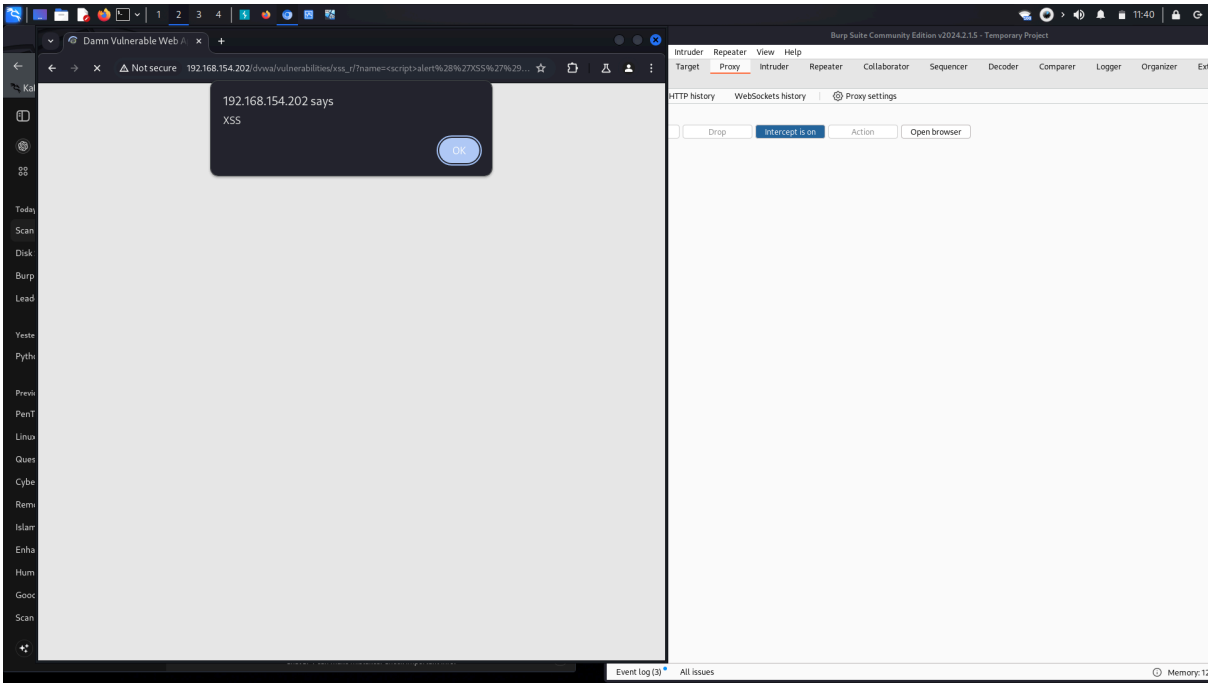
- foydalanuvchi sessiyalarini o’g’irlash va ularga taqlid qilish.
- Cookie lar va sessiya xotirasida saqlangan muhim ma’lumotlarni qo’lga kiritish.

Tavsiyalar:

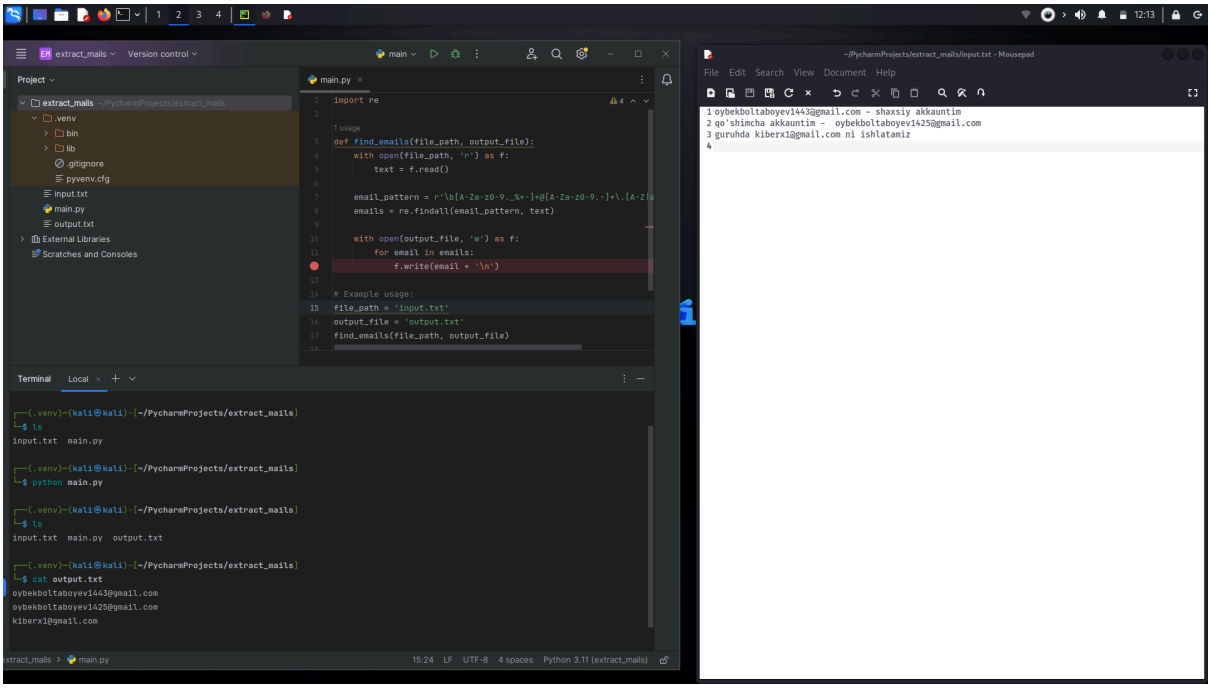
- Kiritmani yaroqlilashtirish: kiritmalarni qabul qilinishi mumkin bo’lgan skriplarga qarshi yaroqlilashtirish.
- Natijani shifrlash: <, >, va “ kabi belgilarni shifrlash uchun mavjud usullardan foydalaning.
- CSP (kontent xavfsizligi siyosati) sarlavhalari: bajarilishi mumkin bo’lgan skriptlar manbasini cheklash uchun CSP ni sozlang.

Hodisa:




Damn Vulnerable Web
Not secure 192.168.154.202/dvwa/vulnerabilities/xss_r/?name=<script>alert%28%27XSS%27%29...
192.168.154.202 says
XSS
OK
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Intruder Repeater View Help
Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
HTTP history WebSockets history Proxy settings
Drop Intercept is on Action Open browser
Event log (3) All issues

3-topshiriq:


extract_mails Version control
Project
extract_mails ~/PycharmProjects/extract_mails
.venv
bin
lib
.gitignore
pyvenv.cfg
input.txt
main.py
output.txt
External Libraries
Scratches and Consoles
main.py
import re
1 usage
def find_emails(file_path, output_file):
with open(file_path, 'r') as f:
text = f.read()
email_pattern = r'\b[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Z|a
emails = re.findall(email_pattern, text)
with open(output_file, 'w') as f:
for email in emails:
f.write(email + '\n')
# Example usage:
file_path = 'input.txt'
output_file = 'output.txt'
find_emails(file_path, output_file)
Terminal Local
(.venv)-(kali㉿kali)-[~/PycharmProjects/extract_mails]
$ ls
input.txt main.py
(.venv)-(kali㉿kali)-[~/PycharmProjects/extract_mails]
$ python main.py
(.venv)-(kali㉿kali)-[~/PycharmProjects/extract_mails]
$ ls
input.txt main.py output.txt
(.venv)-(kali㉿kali)-[~/PycharmProjects/extract_mails]
$ cat output.txt
oybekboltaboyev1443@gmail.com
oybekboltaboyev1425@gmail.com
kiberx1@gmail.com
15:24 LF UTF-8 4 spaces Python 3.11 (extract_mails)
~/PycharmProjects/extract_mails/input.txt - Mousepad
File Edit Search View Document Help
1 oybekboltaboyev1443@gmail.com - shaxsiy akkauntim
2 qo'shimcha akkauntim - oybekboltaboyev1425@gmail.com
3 guruhda kiberx1@gmail.com ni ishlatamiz
4