

## 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 vazifalarda 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).

```

File Actions Edit View Help
File cd /home/kali/Desktop
(kali㉿kali)-[~/Desktop]
ls
BroadcomInstaller2021 PycharmProjects
'New Folder' PycharmProjects.tar.gz jetbrains-pycharm-ce.desktop 'kiber 3 oy intihon .txt' vmware-player.desktop
ls
touch file.txt
(kali㉿kali)-[~/Desktop]
ls
BroadcomInstaller2021 PycharmProjects
'New Folder' PycharmProjects.tar.gz file.txt jetbrains-pycharm-ce.desktop 'kiber 3 oy intihon .txt' vmware-player.desktop
cp file.txt /home/kali/Documents
(kali㉿kali)-[~/Desktop]
cd ..
ls
cd /home/kali/Documents
ls
Windows 10 Ent Lite v1809 x64 by Zosma (12.08.2019)(1).iso
ls
av file.txt /home/kali/Public
(kali㉿kali)-[~/Documents]
ls
Windows 10 Ent Lite v1809 x64 by Zosma (12.08.2019)(1).iso
Javoblar
ls
cd ..
ls
(kali㉿kali)-[~/Public]
ls
file.txt
mv file.txt fayl.txt
ls
fayl.txt
rm fayl.txt
(kali㉿kali)-[~/Public]
ls

```

### 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'rnatna 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 foydalaniib 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’rnatishingiz mumkin. Yana bular orqali siz loyihalaringiz kerakli bog’liklariga ega bo’lishini va boshqa loyihalarga tizimning standart Python 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 tavsija 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.

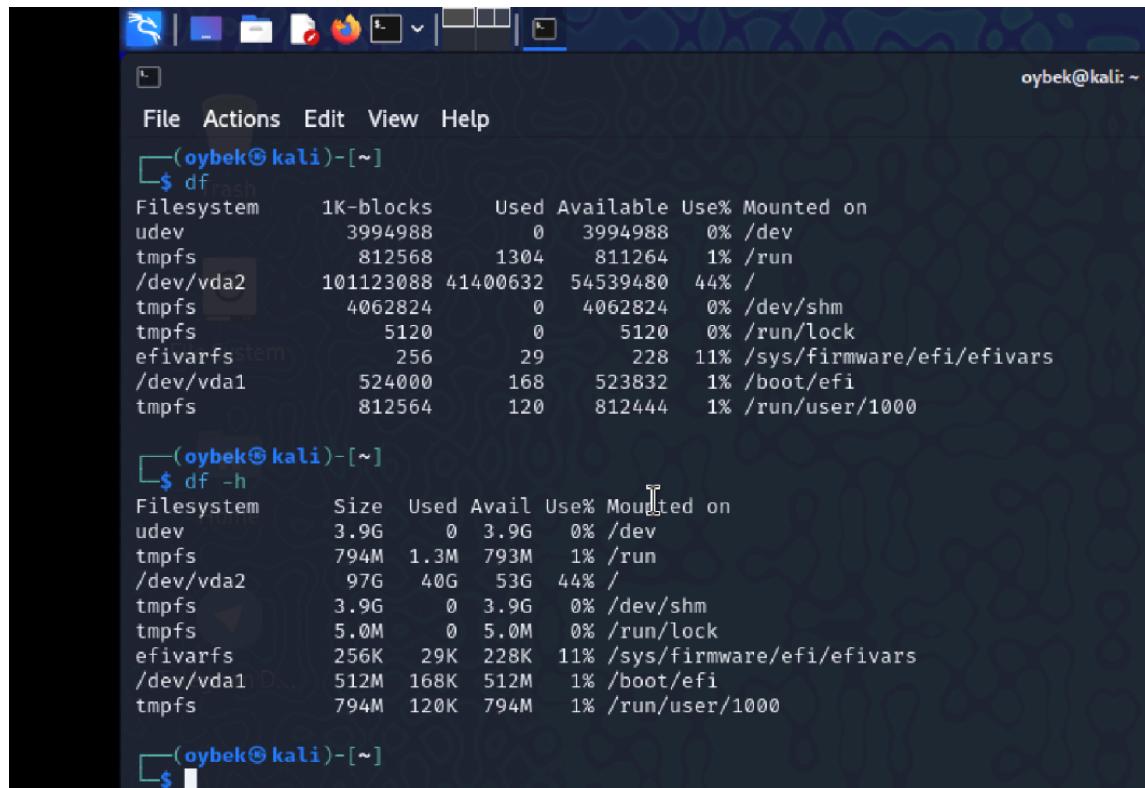
Shundagina siz hackerlik mahoratingizni nazorat qilingan muhitda sinash va mashq qilish imkonini beruvchi Kali Linux va Windows OTIlarini virtual mashina sifatida ishlata olasiz. Virtualizatsiya sizga qurilmalar xaridi, sozlamalari kabi real voqealikda qiyinchilik tug’diradigan ko’pgina

jihatlarda qo'l kelishi mumkin. Va yana bu hakerlik mahorati ustida ishslashning 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.



```
oybek@kali: ~
File Actions Edit View Help
(oybek@kali)-[~]
$ df
Filesystem 1K-blocks Used Available Use% Mounted on
udev 3994988 0 3994988 0% /dev
tmpfs 812568 1304 811264 1% /run
/dev/vda2 101123088 41400632 54539480 44% /
tmpfs 4062824 0 4062824 0% /dev/shm
tmpfs 5120 0 5120 0% /run/lock
efivarfs 256 29 228 11% /sys/firmware/efi/efivars
/dev/vda1 524000 168 523832 1% /boot/efi
tmpfs 812564 120 812444 1% /run/user/1000

(oybek@kali)-[~]
$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 3.9G 0 3.9G 0% /dev
tmpfs 794M 1.3M 793M 1% /run
/dev/vda2 97G 40G 53G 44% /
tmpfs 3.9G 0 3.9G 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
efivarfs 256K 29K 228K 11% /sys/firmware/efi/efivars
/dev/vda1 512M 168K 512M 1% /boot/efi
tmpfs 794M 120K 794M 1% /run/user/1000

(oybek@kali)-[~]
$
```

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 ishlatalilgan 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 ishlataladi. U fayl/katalog hajmi haqidagi axborotni uning subkatalog va fayllari haqidagi ma'lumot bilan birga ta'minlaydi.

```

152K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.youtube.com/partitionKey=%28https%2Ctryhackme.com%29/idb
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.youtube.com/partitionKey=%28https%2Ctryhackme.com%29/cache/morgue
58K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.youtube.com/partitionKey=%28https%2Ctryhackme.com%29/cache
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.youtube.com/partitionKey=%28https%2Ctryhackme.com%29
50K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.google.com/ls
58K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.google.com
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://daryo.uz/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://daryo.uz
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://piima.uz/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://piima.uz
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://securitymagazine.com/ls
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.securitymagazine.com/idb/2135660075ientParvi.files
52K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.securitymagazine.com/idb
76K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.securitymagazine.com
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://clients5.google.com/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://clients5.google.com
20K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://coursera.org/ls
28K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.coursera.org
82K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://chatgpt.com/ls
40K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://chatgpt.com
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.google.com/partitionKey=%28https%2Csourceforge.net%29/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.google.com/partitionKey=%28https%2Csourceforge.net%29
128K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://medium.com/ls
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://medium.com/idb/2266997078reegpalraoytS.files
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://medium.com/idb/371373747_s_edmban.files
100K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://medium.com/idb
236K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://medium.com
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.google.com/partitionKey=%28https%2Csecuritymagazine.com%29/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.google.com/partitionKey=%28https%2Csecuritymagazine.com%29
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.google.com/partitionKey=%28https%2Cuzbekcoders.uz%29/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.google.com/partitionKey=%28https%2Cuzbekcoders.uz%29
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.lookup.net/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.lookup.net
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://portswigger.net/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://portswigger.net
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://pay.xazna.uz/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://pay.xazna.uz
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.reddit.com/ls
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.reddit.com/idb/2728594770keeryovtasl-.files
52K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.reddit.com/idb
8.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://www.reddit.com/cache/morgue/136

```

```

oybek@kali:~$ du -h
File Actions Edit View Help
(oybek@kali)-[~]
$ du -h
4.0K ./Templates
8.0K ./ssh
4.0K ./mozilla/extensions
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/to-be-removed
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/temporary
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/chrome/idb/2823318777ntouromlalnodyn--naod.files
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/chrome/idb/1657114595Amcateirvtisty.files
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/chrome/idb/1451318868ntouromlalnodyn--epcr.files
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/chrome/idb/3870112724rsegmnottet-es.files/journals
820K ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/chrome/idb/3870112724rsegmnottet-es.files
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/chrome/idb/3561288849sdhlie.files
12M ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/chrome/idb
12M ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/chrome/ls
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/indexedb++fx-devtools/idb/478967115devgvatrootlss--cans.files
56K ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/indexedb++fx-devtools/idb
64K ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent/indexedb++fx-devtools
12M ./mozilla/firefox/u3jlz4v2.default-esr/storage/permanent
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://service.seamlessaccess.org/partitionKey=%28https%2Csciedirect.com%29/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://service.seamlessaccess.org/partitionKey=%28https%2Csciedirect.com%29
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://my.uzbmb.uz/ls
12K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://my.uzbmb.uz
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://player.vimeo.com/partitionKey=%28https%2Cwappalyzer.com%29/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://player.vimeo.com/partitionKey=%28https%2Cwappalyzer.com%29
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://chat.hackerai.co/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://chat.hackerai.co
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://contacts.google.com/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://contacts.google.com
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://yangi-kinolar.ru/partitionKey=%28http%2Casilmedia.org%29/ls
24K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://yangi-kinolar.ru/partitionKey=%28http%2Casilmedia.org%29
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://daxshat.net/ls
8.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://daxshat.net/cache/morgue/138
8.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://daxshat.net/cache/morgue/28
20K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://daxshat.net/cache/morgue
100K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://daxshat.net/cache
124K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://daxshat.net
16K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://twitter.com/ls
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://twitter.com/idb/3619119340leogaarlol.files
4.0K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://twitter.com/idb/1367196241hboerwinzo.files
176K ./mozilla/firefox/u3jlz4v2.default-esr/storage/default/https://twitter.com/idb

```

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.

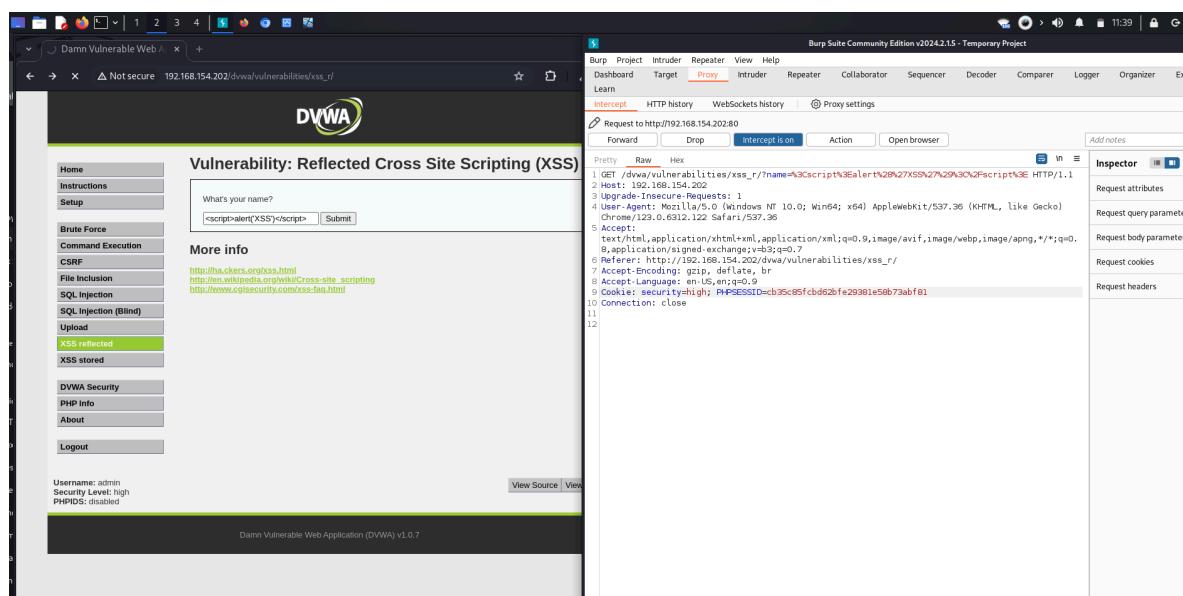
Ta'siri: bu zaiflikni egallash orqali hujumchilar quydagilarni bajarishi mumkin:

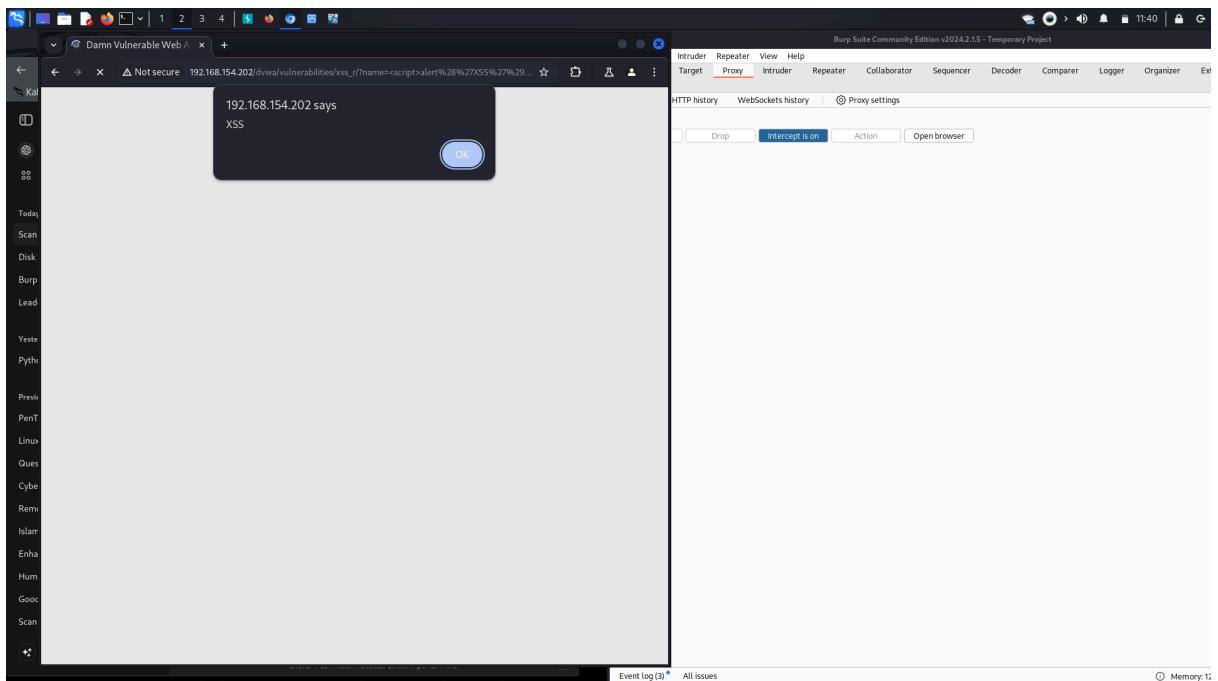
- foydalanuvchi sessiyalarini o'g'irlash va ularga taqlid qilish.
- Cookie lar va sessiya xotirasida saqlangan muhim ma'lumotlarni qo'lga kiritish.

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:





### 3-topshiriq:

