



## تکلیف سوم

مریم سعیدمهر  
شماره دانشجویی: ۹۶۲۹۳۷۳

### فهرست مطالب

۲	I. سوال اول
۲	II. سوال دوم
۲	III. سوال سوم
۳	IV. سوال چهارم
۴	V. سوال پنجم
۵	VI. سوال هفتم

## I. سوال اول

- (آ) غلط است :  
از آنجایی که جریان اطلاعات در BLP از پایین به بالا است پس هیچ اطلاعاتی از سطوح بالا به پایین منتقل نمیشود و در نتیجه امکان اجرای فرمان از بالا به پایین نیست. همچنین یک باگ امنیتی این مدل ، وجود کانال پنهان است که از این طریق میتوان اطلاعات را از سطوح بالا به پایین منتقل کرد.
- (ب) غلط است :  
فقط مالک اولیه مشخص میکند چه کسانی به فایل دسترسی داشته باشند.
- (ج) غلط است :  
مدل BIBA براساس صحت است نه محرمانگی.

## II. سوال دوم

- (آ) ماتریس کنترل دسترسی یا لیست توانایی ها (capability list)  
(ب) در کرنل کنترل های لازم را انجام میدهیم.
- (ج) این اصل بیان میکند که اگر قرار است سیستم پیش فرضی داشته باشد این پیش فرض امن باشد. کاربرد آن به طور مثال در ACL این است که اگر یک سبجکت در لیست یک آبجکت نباشد یعنی آن سبجکت هیچ permission روی آن آبجکت ندارد.

## III. سوال سوم

```
1      command Grant.read.file(Si, 0, Sj)
2          if own in A[Si, 0] and r in A[Si, 0] then
3              enter r into A[Sj, 0]
4          end
5
6      command Grant.write.file(Si, 0, Sj)
7          if own in A[Si, 0] and w in A[Si, 0] then
8              enter w into A[Sj, 0]
9          end
10
11     command Revoc.execution.file(Si, 0, Sj)
12         if own in A[Si, 0] then
13             delete x from A[Sj, 0]
14         end
15
16     command Create.file(Si, 0)
17         create object 0
18         enter own into A[Si, 0]
19         enter r into A[Si, 0]
20         enter w into A[Si, 0]
21         enter x into A[Si, 0]
22     end
```

- (آ) • تغییر ایجاد میشود :  
دستور Create.file(Subj1, Obj4) باعث ایجاد یک ستون جدید برای Obj4 و اضافه شدن تمام دسترسی ها برای Subj1 نسبت به Obj4 میشود
- تغییر ایجاد نمیشود :  
دستور Grant.write.file(Subj1, Obj3, Subj2) از آنجا که Subj1 مالک Obj3 نیست اجرا نمیشود.
- تغییر ایجاد میشود :  
دستور Grant.read.file(Subj1, Obj4, Subj2) چون سبجکت 1 مالک آبجکت 4 است و دسترسی خواندن نیز دارد

- تغییر ایجاد نمیشود :

دستور  $\text{Revoc.execution.file}(\text{Subj1}, \text{Obj3}, \text{Subj3})$  با توجه به اینکه ساجکت ۱ مالک آجکت ۳ نیست اجرا نمیشود.

(ب) ماتریس کنترل دسترسی نهایی :

-	Object1	Object2	Object3	Object4
Subject1	ORWX	R	RWX	ORWX
Subject2	R	RW	R	R
Subject3	RW	ORW	ORWX	-

(ج) ACL و CL نهایی :

Access Control List :

Object1 = (Subject1, ORWX), (Subject2, R), (Subject3, RW)

Object2 = (Subject1, R), (Subject2, RW), (Subject3, ORW)

Object3 = (Subject1, RWX), (Subject2, R), (Subject3, ORWX)

Object4 = (Subject1, ORWX), (Subject2, R)

Capability List :

Subject1 = (Object1, ORWX), (Object2, R), (Object3, RWX), (Object4, ORWX)

Subject2 = (Object1, R), (Object2, RW), (Object3, R), (Object4, R)

Subject3 = (Object1, RW), (Object2, ORW), (Object3, ORWX)

#### IV. سوال چهارم

با سناریو زیر و مدل BLP :

$L(S1, O1) = \text{Confidential}, A, B$

$L(S2, O2) = \text{Top Secret}, B, C$

$L(S3, O3) = \text{Secret}, A$

$L(S4, O4) = \text{Unclassified}$

(آ) آیا ساجکت ۲ به آجکت ۱ دسترسی خواندن و نوشتن دارد ؟  
دسترسی خواندن : اگر  $L(\text{subject})$  به  $L(\text{object})$  غلبه کند  
دسترسی نوشتن : اگر  $L(\text{object})$  به  $L(\text{subject})$  غلبه کند

- دسترسی خواندن : ندارد زیرا  $\{A, B\} \not\subset \{B, C\}$
- دسترسی نوشتن : ندارد زیرا  $\text{Confidential} < \text{Top secret}$  and  $\{B, C\} \not\subset \{A, B\}$

(ب) آیا ساجکت ۳ به آجکت ۲ دسترسی خواندن و نوشتن دارد ؟  
دسترسی خواندن : اگر  $L(\text{subject})$  به  $L(\text{object})$  غلبه کند  
دسترسی نوشتن : اگر  $L(\text{object})$  به  $L(\text{subject})$  غلبه کند

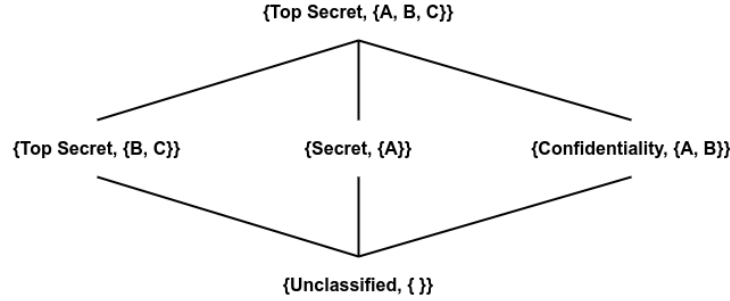
- دسترسی خواندن : ندارد زیرا  $\text{Secret} < \text{Top secret}$  and  $\{B, C\} \not\subset \{A\}$
- دسترسی نوشتن : ندارد زیرا  $\{A\} \not\subset \{B, C\}$

(ج) آیا ساجکت ۱ به آجکت ۳ دسترسی خواندن و نوشتن دارد ؟  
دسترسی خواندن : اگر  $L(\text{subject})$  به  $L(\text{object})$  غلبه کند  
دسترسی نوشتن : اگر  $L(\text{object})$  به  $L(\text{subject})$  غلبه کند

- دسترسی خواندن : ندارد زیرا  $\text{Confidential} < \text{Secret}$
- دسترسی نوشتن : ندارد زیرا  $\{A, B\} \not\subset \{A\}$

(د) جریان اطلاعات از پابین به بالاست یا برعکس ؟  
جریان اطلاعات از پابین به بالاست

(ه) رسم شبکه lattice نظیر مدل :



با سناریو زیر و مدل BIBA :

$L(S1, O1) = \text{Very Trusted, A, B}$   
 $L(S2, O2) = \text{Trusted, B, C}$   
 $L(S3, O3) = \text{Slightly Trusted, A}$   
 $L(S4, O4) = \text{Untrusted}$

(آ) آیا سابیجکت ۲ به آبیجکت ۱ دسترسی خواندن و نوشتن دارد ؟  
 دسترسی خواندن : اگر  $\text{Integrity(object)}$  به  $\text{Integrity(subject)}$  غلبه کند  
 دسترسی نوشتن : اگر  $\text{Integrity(object)}$  به  $\text{Integrity(subject)}$  غلبه کند

- دسترسی خواندن : ندارد زیرا  $\{B, C\} \not\subset \{A, B\}$
- دسترسی نوشتن : ندارد زیرا  $\text{Trusted} < \text{Very Trusted}$  and  $\{A, B\} \not\subset \{B, C\}$

(ب) آیا سابیجکت ۳ به آبیجکت ۲ دسترسی خواندن و نوشتن دارد ؟  
 دسترسی خواندن : اگر  $\text{Integrity(object)}$  به  $\text{Integrity(subject)}$  غلبه کند  
 دسترسی نوشتن : اگر  $\text{Integrity(object)}$  به  $\text{Integrity(subject)}$  غلبه کند

- دسترسی خواندن : ندارد زیرا  $\{A\} \not\subset \{B, C\}$
- دسترسی نوشتن : ندارد زیرا  $\text{Slightly Trusted} < \text{Trusted}$  and  $\{B, C\} \not\subset \{A\}$

(ج) آیا سابیجکت ۱ به آبیجکت ۳ دسترسی خواندن و نوشتن دارد ؟  
 دسترسی خواندن : اگر  $\text{Integrity(object)}$  به  $\text{Integrity(subject)}$  غلبه کند  
 دسترسی نوشتن : اگر  $\text{Integrity(object)}$  به  $\text{Integrity(subject)}$  غلبه کند

- دسترسی خواندن : ندارد زیرا  $\text{Very Trusted} < \text{Trusted}$  and  $\{A, B\} \not\subset \{A\}$
- دسترسی نوشتن : دارد زیرا  $\text{Trusted} < \text{Very Trusted}$  and  $\{A\} \subset \{A, B\}$

(د) جریان اطلاعات از پایین به بالاست یا برعکس ؟  
جریان اطلاعات از بالا به پایین است

V. سوال پنجم

(آ) مزایا و معایب :

مزیت آن این است که revocation خیلی آسان تر است مثلاً اگر OR-Access داریم و میخواهیم دسترسی را از سابیجکتی که  $K_j$  را در دست دارد بگیریم کافیه آن نسخه از آبیجکت که با  $K_j$  رمز شده را حذف کنیم. یکی از معایب آن این است که ریزدانی دسترسی که در لیست ها داشتیم را اینجا نداریم. مثلاً read یا write خیلی معنی نمیدهد اینجا، در عمل یک قفل داریم که یا باز میشود یا نمیشود. برای اینکه این مشکل حل بشود کافیه کلیدهای مختلف برای دسترسی های مختلف در نظر بگیریم و سیستم عامل کلید را که گرفت تشخیص بدهد این کلید read است و مثلاً فقط نسخه read-only فایل را باز کند.

ب) معادله  $5024x^2 + 1234x + 1523$  : مقدار threshold برابر است (معادله درجه می باشد) و مقدار secret نیز 1523 است. ابتدا آجکت موردنظر رو با کلید متقارن 1523 رمز میکنیم و سه کلید  $K_0, K_1, K_2$  را به سه نفر میدهیم (هر نفر یک کلید)

$$y = 5024x^2 + 1234x + 1523 \implies \begin{cases} k_1 = (2, 24087) \\ k_2 = (1, 7781) \\ k_3 = (-1, 5313) \end{cases}$$

$$y = ax^2 + bx + c$$

حالا باید این سه نفر همفکری کنند. یعنی :

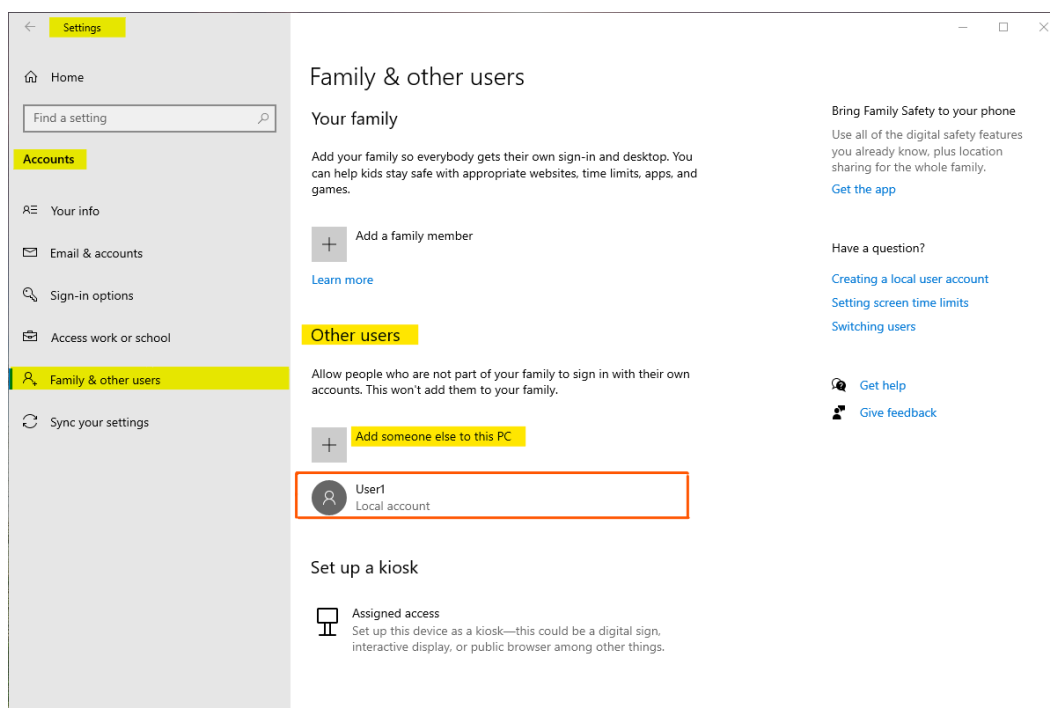
$$\begin{cases} 24087 = 4a + 2b + c \\ 7781 = a + b + c \\ 5313 = a - b + c \end{cases}$$

در این جا سه معادله و سه مجهول داریم لذا دستگاه قابل حل است و به این ترتیب مقدار c نیز قابل محاسبه است و لذا با یافتن c رمز آجکت باز میشود.

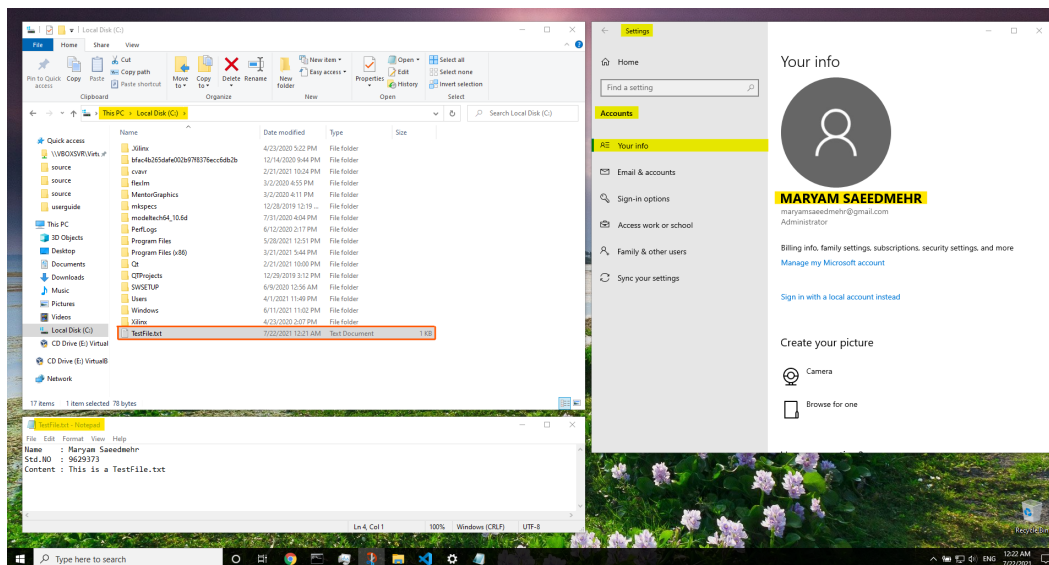
## VI. سوال هفتم

(آ) کنترل دسترسی تفویضی :

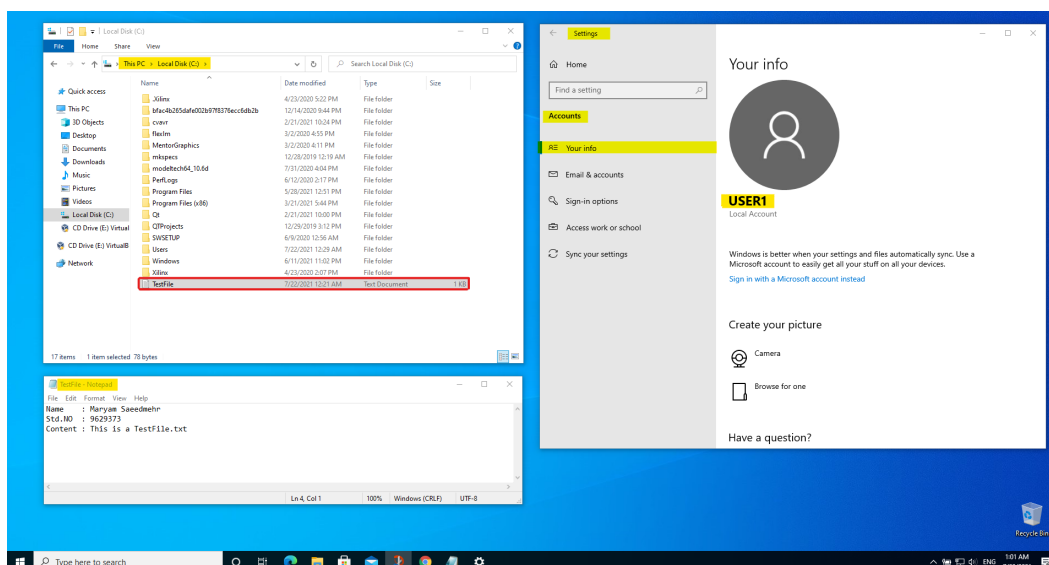
(آ) ترتیب کارها به شکل زیر بود :



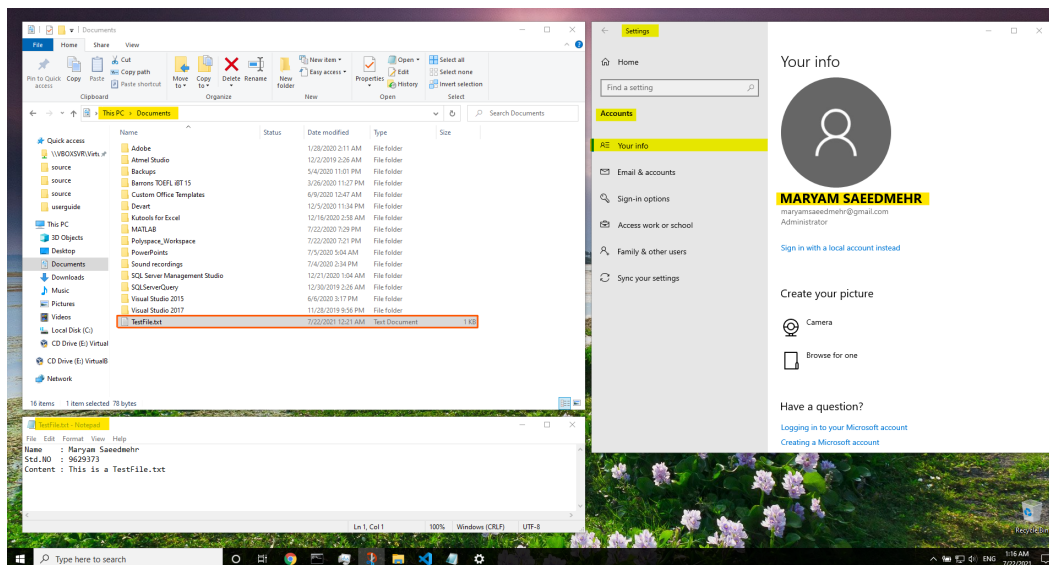
شکل ۱: ایجاد کاربر جدید



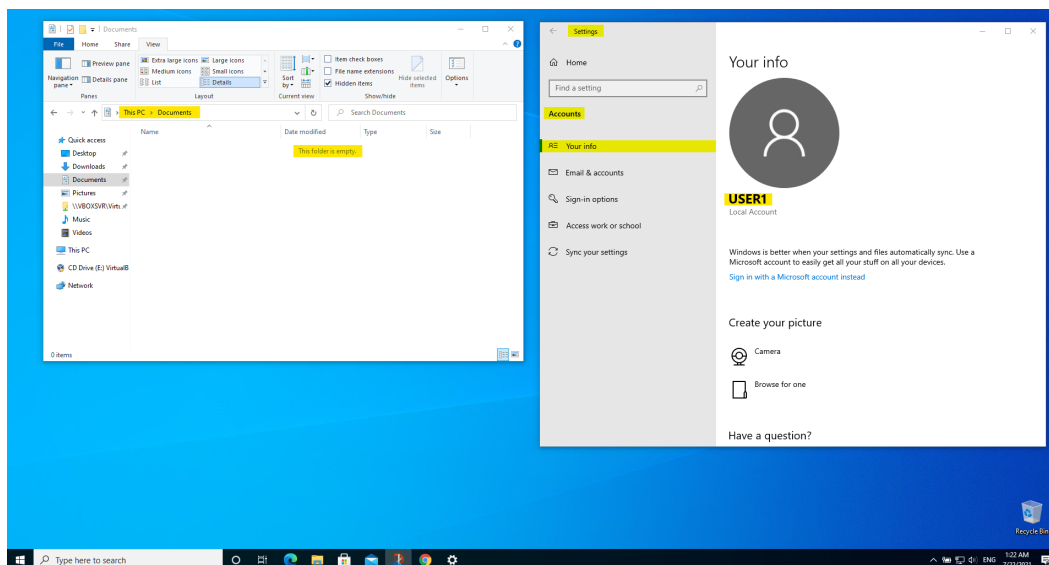
شکل ۲: فایل TestFile.txt در دایرکتوری ریشه درایو C برای یوزر فعلی ام قابل روئت بود



شکل ۳: فایل TestFile.txt در دایرکتوری ریشه درایو C برای یوزر User1 قابل روئت بود



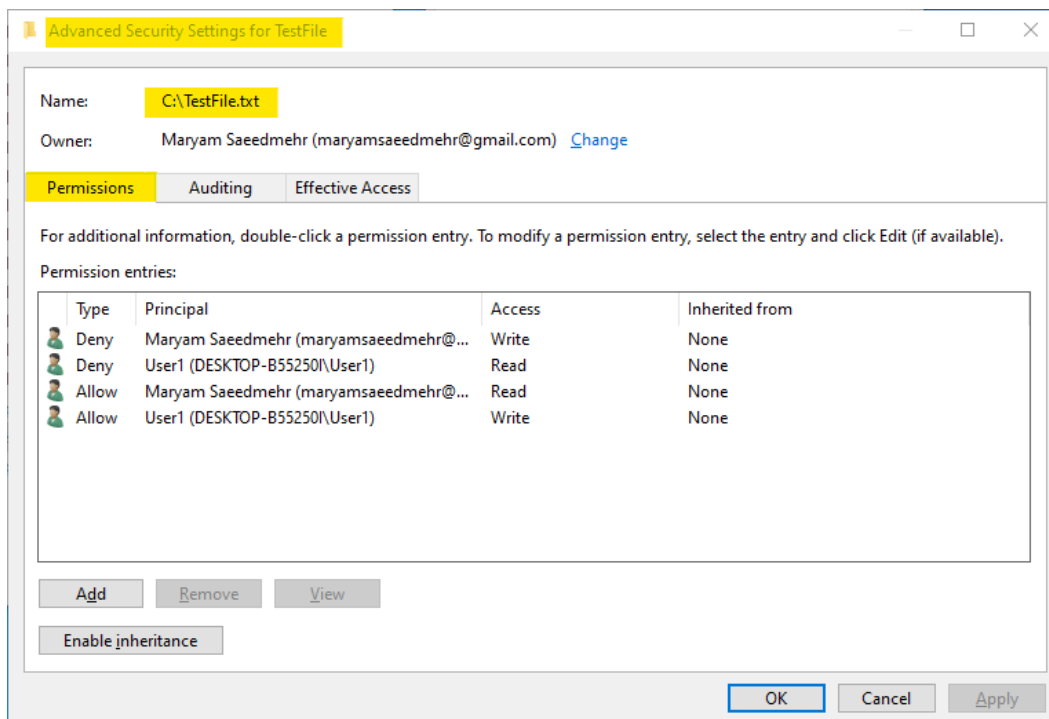
شکل ۴: فایل TestFile.txt در دایرکتوری Documents برای یوزر فعلی ام قابل رویت بود



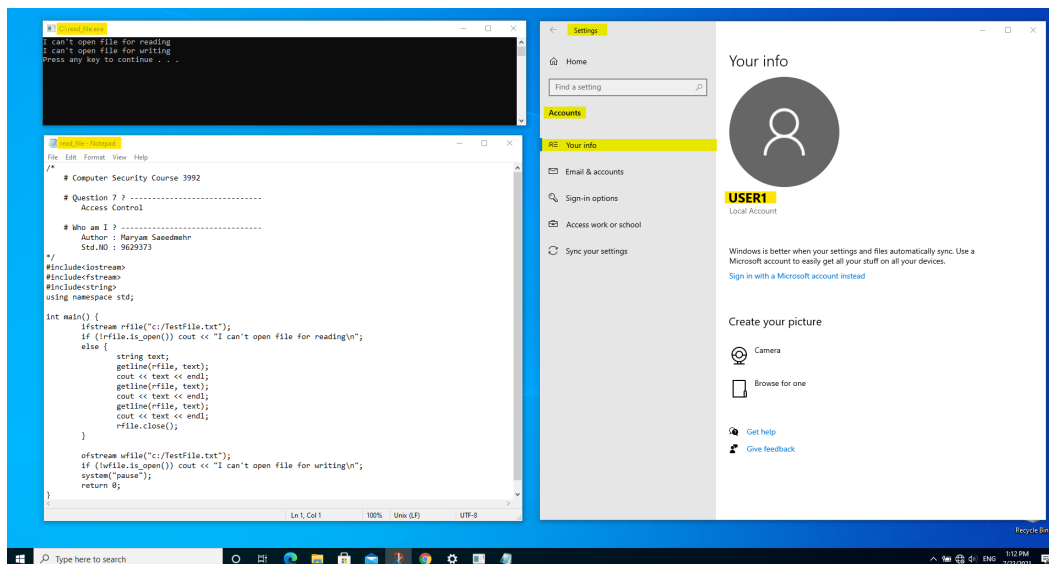
شکل ۵: فایل TestFile.txt در دایرکتوری Documents برای یوزر User1 قابل رویت نبود

به طور کلی فولدرهای دسکتاپ و documents و pictures و ... همگی فولدرهای شخصی کاربر محسوب میشوند و تمام فایل هایی که داخل این فولدرها هستند برای بقیه یوزرها قابل مشاهده و دسترسی نیستند.

(ب) فایل های read\_file.cpp, write\_file.cpp, read\_file.exe, write\_file.exe ضمیمه شده اند

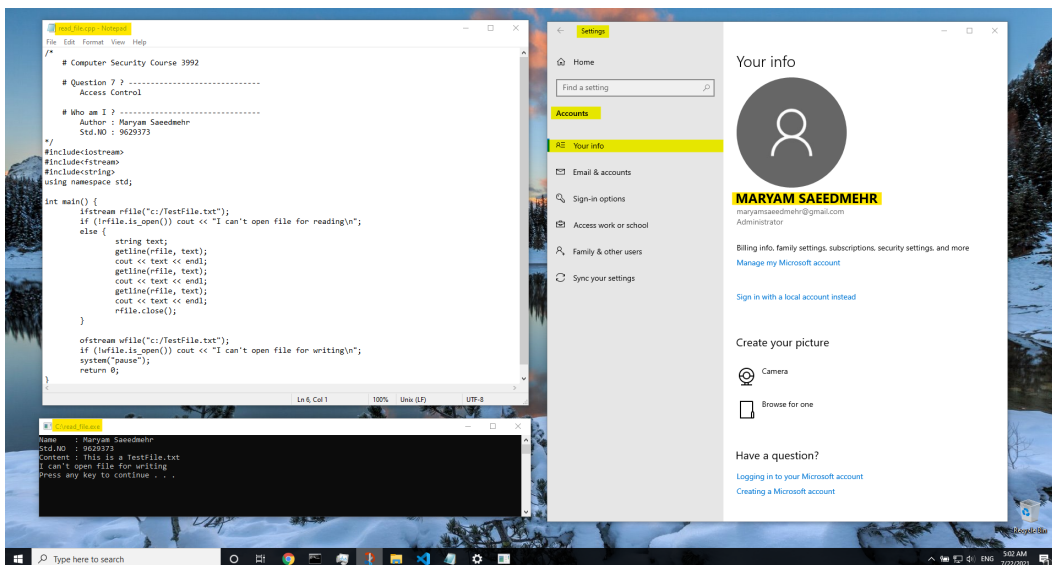


شکل ۶: کنترل دسترسی یوزرها به فایل TestFile.txt



شکل ۷: تست دسترسی خواندن و نوشتن یوزر User1 به فایل TestFile.txt

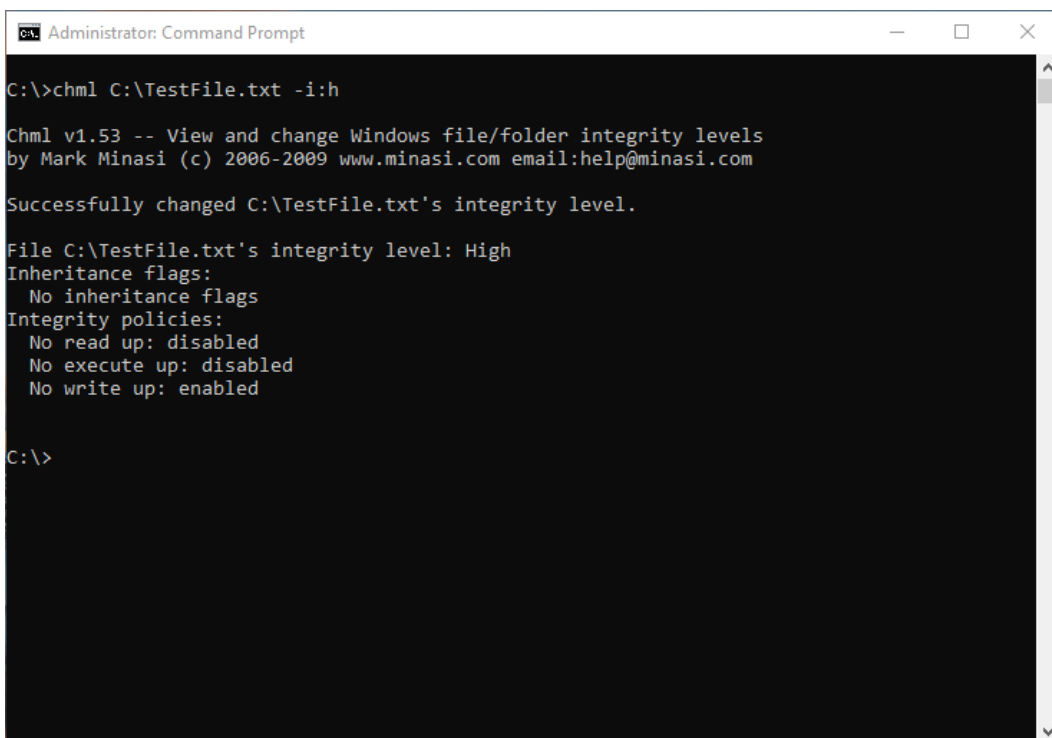




شکل ۸: تست دسترسی خواندن و نوشتن یوزر فعلی ام به فایل TestFile.txt

(ب) کنترل دسترسی اجباری :

(آ) فایل TestFile.txt جدیدی با محتوای This is part B of Question7 در دایرکتوری ریشه درایو C ایجاد کردم.



شکل ۹: اعطای سطح صحت High به فایل TestFile.txt

```
Command Prompt

C:\>more TestFile.txt
This is part B of Question7

C:\>echo Hello > TestFile.txt
Access is denied.

C:\>
```

شکل ۱۰: تست خواندن از و نوشتن در فایل TestFile.txt بعد از اعطای سطح صحت High

(ب) اعمال سیاست No Read Up و تکرار مرحله قبل

```
Administrator: Command Prompt

C:\>chml C:\TestFile.txt -i:h

Chml v1.53 -- View and change Windows file/folder integrity levels
by Mark Minasi (c) 2006-2009 www.minasi.com email:help@minasi.com

Successfully changed C:\TestFile.txt's integrity level.

File C:\TestFile.txt's integrity level: High
Inheritance flags:
  No inheritance flags
Integrity policies:
  No read up: disabled
  No execute up: disabled
  No write up: enabled

C:\>chml C:\TestFile.txt -i:h -nr

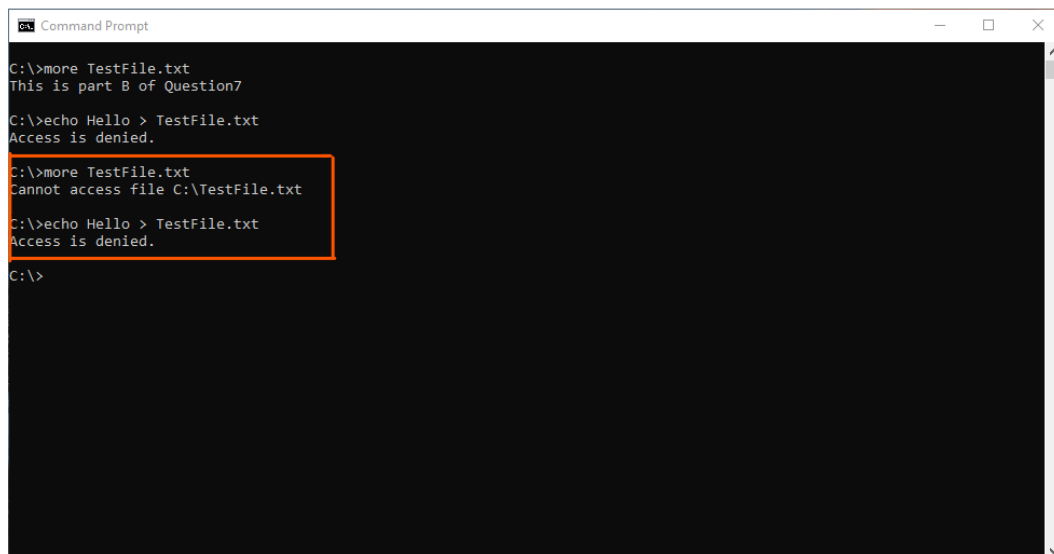
Chml v1.53 -- View and change Windows file/folder integrity levels
by Mark Minasi (c) 2006-2009 www.minasi.com email:help@minasi.com

Successfully changed C:\TestFile.txt's integrity level.

File C:\TestFile.txt's integrity level: High
Inheritance flags:
  No inheritance flags
Integrity policies:
  No read up: enabled
  No execute up: disabled
  No write up: disabled

C:\>
```

شکل ۱۱: اعطای سطح صحت High به فایل TestFile.txt و اعمال سیاست No Read Up



```
Command Prompt
C:\>more TestFile.txt
This is part B of Question7
C:\>echo Hello > TestFile.txt
Access is denied.
C:\>more TestFile.txt
Cannot access file C:\TestFile.txt
C:\>echo Hello > TestFile.txt
Access is denied.
C:\>
```

شکل ۱۲: تست خواندن از و نوشتن در فایل TestFile.txt بعد از اعمال سیاست No Read Up  
(ج) فایل read&write.exe, read&write.cpp ضمیمه شده اند.

(د) اعطای سطح صحت medium به فایل متنی و low به فایل exe خروجی از قسمت سوم

```
Administrator: Command Prompt

C:\>chml C:\TestFile.txt -i:m

Chml v1.53 -- View and change Windows file/folder integrity levels
by Mark Minasi (c) 2006-2009 www.minasi.com email:help@minasi.com

Successfully changed C:\TestFile.txt's integrity level.

File C:\TestFile.txt's integrity level: Medium
Inheritance flags:
  No inheritance flags
Integrity policies:
  No read up: disabled
  No execute up: disabled
  No write up: enabled

C:\>chml "C:\read&write.exe" -i:l

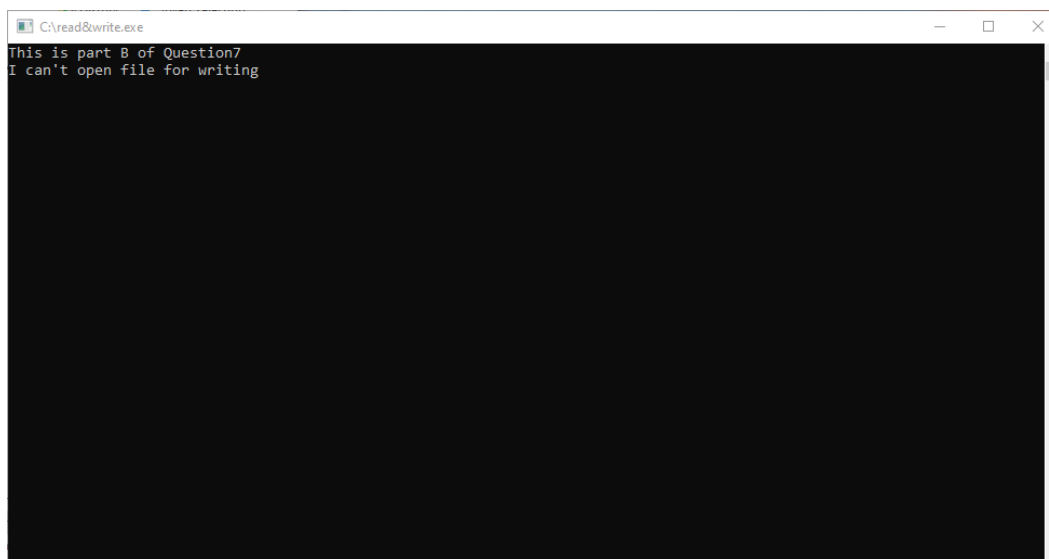
Chml v1.53 -- View and change Windows file/folder integrity levels
by Mark Minasi (c) 2006-2009 www.minasi.com email:help@minasi.com

Successfully changed C:\read&write.exe's integrity level.

File C:\read&write.exe's integrity level: Low
Inheritance flags:
  No inheritance flags
Integrity policies:
  No read up: disabled
  No execute up: disabled
  No write up: enabled

C:\>
```

شکل ۱۳: اعطای سطح صحت medium به فایل TestFile.txt و اعطای سطح صحت low به فایل exe خروجی از قسمت سوم



شکل ۱۴: اجرای read&write.exe بعد از اعمال سطح دسترسی های فوق به فایل متنی و فایل قابل اجرا