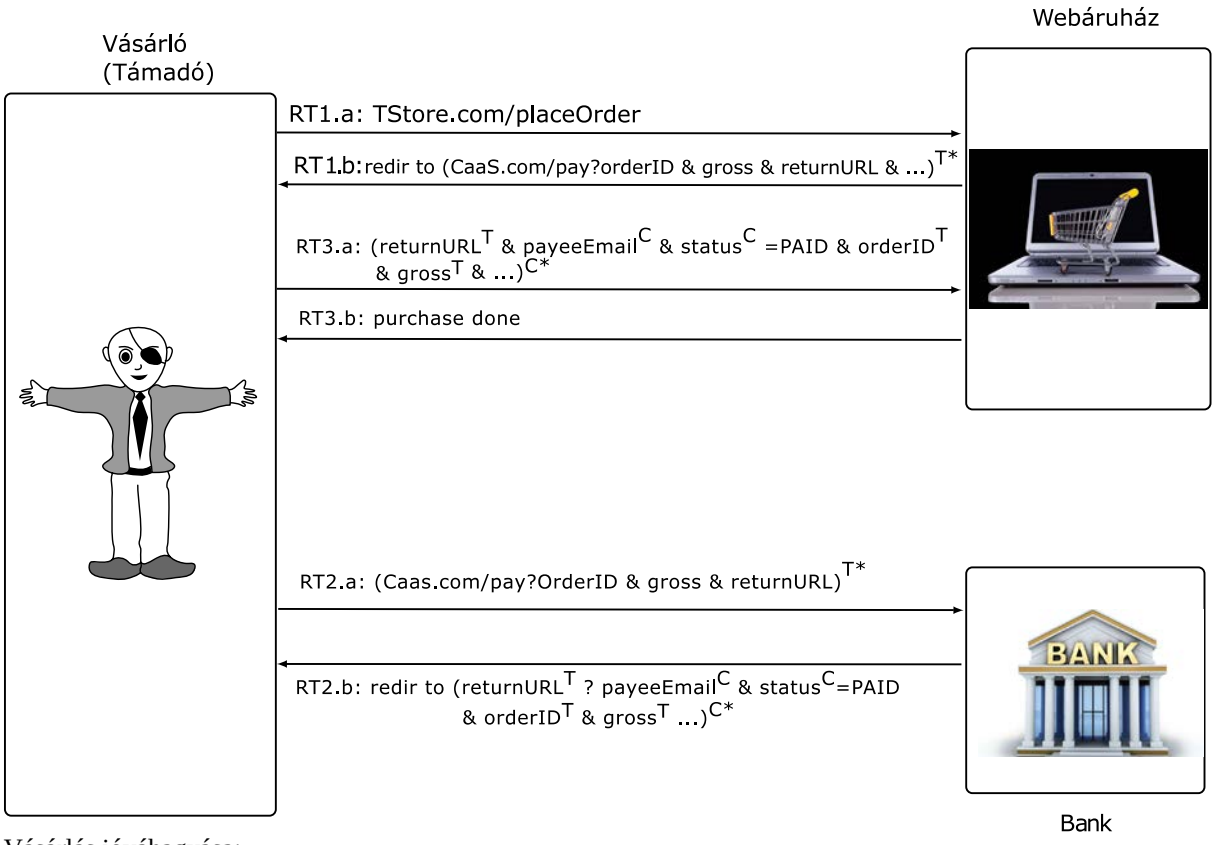
1. Adja meg a web-es vásárlás biztonságos lebonyolításának a feltételét. (4 pont)

Teljes válasz megtalálható a „Beágyazott web szolgáltatások biztonsága” tananyag 3. fóliáján.



Vásárlás jóváhagyása:

```
TStore.com/placeOrder:
  orderID=InsertPendingOrder ()

TStore.com/finishOrder  handler of RT3.a:
  if( verifySignature(RT3.a) != CaaS) exit;
   /*payment status*/
  if( GetMsgField("status") != PAID) exit;
  order= GetOrderByID(orderID);
  if( order==NULL or order.status != PENDING) exit;
  order.status=PAID;
```

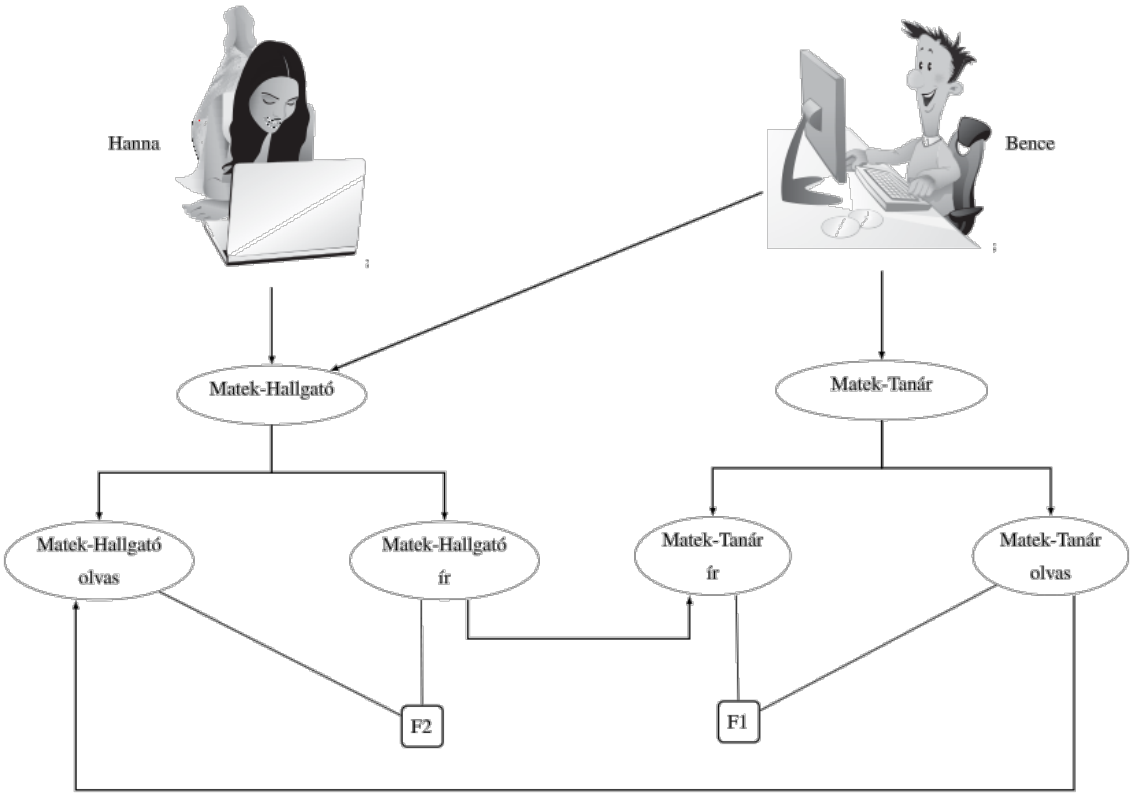
Mit nem ellenőriz a kereskedő? (2 pont)

Hogyan lehet kihasználni a webkereskedés gyengeségét? (3 pont)

A kereskedő nem ellenőrzi, hogy neki fizették ki a pénzt!
A támadó egyben nyit egy webáruházat …

Teljes válasz megtalálható a „Beágyazott web szolgáltatások biztonsága” tananyag 10 -11-es fóliáján.

2.



a) A CIA modell alapján nevezze meg, hogy melyiket biztosítja a Bell-LaPadula modell! **(1p)**

b) Sorolja fel a Bell-LaPadula modell két főbb szabályát! **(2p)**

c) Adja meg, hogy a fenti ábrán az F1 és F2 fájlokat a Bell-LaPadula model első két szabálya alapján (ss-tulajdonság és *-tulajdonság) ki írhatja, illetve ki olvashatja. Tudjuk, hogy Bence magasabb biztonsági kategóriában van, mint Hanna. **(3p)**

a) adatok bizalmassága

b) No read up, no write down (kifejtve)

c) F2 Hanna írhatja és olvashatja, Bence olvashatja, de csak diák szerepkörben írhatja, F1 Bence olvashatja és írhatja, Hanna írhatja, de nem olvashatja.

Teljes válasz megtalálható az "Erőforrások hozzáférésének szabályozása" tananyag 5 –7-es fóliáján.

3. Tekintsük az alábbi `/etc/passwd` file részletet:

```
panka:x:1001:1002::/home/panka:/bin/bash
aliz:x:1002:1003::/home/aliz:/bin/bash
dani:x:1003:1004::/home/dani:/bin/bash
```

Az `/etc/group` file releváns része:

```
panka:x:1002:
aliz:x:1003:
dani:x:1004:
teacher:x:1001:panka,aliz
```

A fájl hozzáférési jogosultságok az alábbiak:

```
root /home #: ls -al /home
drwxr-xr-x  7 root  root  4096 dec   13 12.52 .
drwxr-xr-x 17 root  root  4096 2014 nov    4 ..
drwx------  3 aliz  aliz  4096 nov   23 00.03 aliz
drwx------  3 dani   dani 4096 nov   22 11.42 dani
drwxr-xr-x  7 panka panka 4096 nov   29 01.30 panka
drwxr-xr-x  4 root  root  4096 dec   13 12.53 munka

root /home #: ls -al /home/munka
drwxr-xr-x 4 root  root    4096 dec   13 12.53 .
drwxr-xr-x 7 root  root    4096 dec   13 12.52 ..
drwxrwxr-x 2 panka teacher 4096 dec   13 13.18 d1
drwxr-xr-- 2 aliz  teacher 4096 dec   13 13.57 d2

root /home #: ls -al /home/munka/d1
drwxrwxr-x 2 panka teacher 4096 dec   13 13.18 .
drwxr-xr-x 4 root  root    4096 dec   13 12.53 ..
-rw-rw---- 1 panka dani       7 dec   13 13.33 f1
-rw-rw-r-- 1 panka teacher    7 dec   13 13.18 f2

root /home #: ls -al /home/munka/d2
drwxr-xr-- 2 aliz  teacher 4096 dec   13 13.57 .
drwxr-xr-x 4 root  root    4096 dec   13 12.53 ..
-rw-rw-rw- 1 aliz  dani       7 dec   13 13.56 f3
-rw-r--r-- 1 root  root       7 dec   13 13.57 f4
-rw-r--r-- 1 panka aliz       7 dec   13 13.57 f5
```

Minden felhasználó a saját `home` könyvtárában található.

a) Mely felhasználók tudják olvasni az `f1` fájlt? (`cat home/munka/d1/f1`) **(2 p)**
b) Mely felhasználók tudják törölni az `f1` fájlt? (`rm /home/munka/d1/f1`) **(2 p)**
c) ki tudja végrehajtani sikeresen az `f2` fájl végrehajtási jogának megadását minden csoportra? (`chmod a+x /home/munka/d1/f2`) **(2 p)**
d) a root felhasználó mely fájlokat tudja törölni a `d2` alkönyvtárban (`rm /home/munka/d1/*`)? **(2 p)**
e) Ki tudja írni a d2 directoryban lévő `f3` fájlt? (`echo "AAA" >> /home/munka/d2/f3`) **(2 p)**

Megoldás:

a) *panka, dani (fájl jogok alapján) + root*
b) *panka, aliz (directory jog alapján) + root*
c) *panka (a tulajdonos) + root*
d) *mind*
e) *panka,aliz (a világnak a d2 directoryra nincs megadva az x jog, tehát nem fér hozzá az i-node bejegyzéshez) + root*

Megj. Ha valaki nem írta oda a root-ot a megoldásba, az nem jelentett hibát.

4.

a) Mi a ROP (return oriented programming) lényege. (2 pont)
b) Mikor használja ezt a módszert a támadó. (2 pont)
c) Hogyan védekezhetünk a támadás ellen. (2 pont)

Megoldás:

a) *Return utasításra végződő kódokat keresünk (gadged), és azokból állítjuk össze a támadás kivitelezéséhez a kódot. A stackra ezeknek a gadget-ek kezdőcíme kerül.*
b) *Ha nem lehet kódot futtatni a stacken (DEP védelem esetén).*
c) *Az DLL-ek, a stack és a program betöltési címének változtatgatásával. ASLR (address space layout randomization)*