Sérülékenységek

LEFT/RIGHT OUTER JOIN, HAVING

A feladat során különböző sérülékenységekkel kapcslatos kérdéseket kell megválaszolnia!

A lekérdezések során csak a feltétlenül szükséges táblákat kösse össze!

Az elsődleges kulcs [PK]-val lett jelölve, míg az idegen kulcs [FK]-val.

eszlelesek(eszleles_id, host_id, vuln_id, elso_eszleles, utolso_eszleles, javitva)

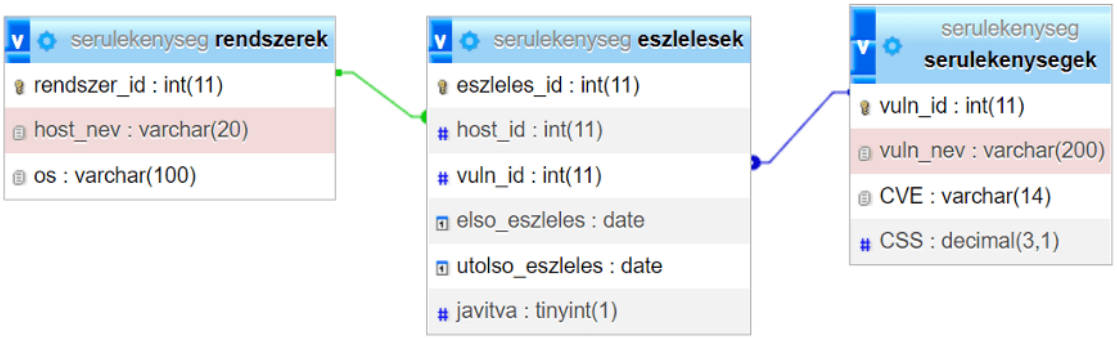
eszleles_id	Egész	Az észlelés azonosítója [PK]
host_id	Egész	A rendszer azonosítója [FK]
vuln_id	Egész	A sérülékenység azonosítója [FK]
elso_eszleles	Dátum	Először mikor láttuk ezen a rendszeren
utolso_eszleles	Dátum	Utoljára ekkor láttuk ezen a rendszeren
javitva	Egész	Megtörtént -e a sérülékenység javítása

rendszerek(rendszer_id, host_nev, os)

rendszer_id	Egész	A rendszer azonosítója [PK]
host_nev	Szöveg(20)	A rendszer neve
os	Szöveg(100)	Az operációs rendszer

serulekenysegek(vuln_id, vuln_nev, CVE, CVSS)

vuln_id	Egész	A sérülékenység azonosítója [PK]
vuln_nev	Szöveg(200)	A sérülékenység neve
CVE	Szöveg(14)	A hivatalos azonosítója a sérülékenységnek
CVSS	decimal(3,1)	A kritikussági pontszáma



1. A `serulekenyseg.sql` fájl futtatásával importálja be a `serulekenyseg` adatbázist a `eszlelesek`,`rendszerek`, és `serulekenysegek` táblákkal és adataikkal együtt.

> **Figyelem!**
>
> Amennyiben már létezik a `serulekenyseg` adatbázis, az törlésre kerül!

2. Nevezze át a `megoldas-ures.sql` fájlt `vezeteknev-keresztnev-serulekenyseg.sql`-re. Ügyeljen oda, hogy a fájlnév csak kisbetűket és kötőjelet tartalmazzon, ékezetet és szóközt ne!
   A következő feladatokra a választ ebben a fájlban, a feladat sorszámát tartalmazó megjegyzést követő sorba készítse el.
3. Melyik rendszereknél nem találtunk soha sérülékenységet? Listázza ki ezen rendszerek nevét és operációs rendszerét, név szerint növekvő sorrendben.

host_nev	**os**
newton	AIX 7.2

4. Melyik sérülékenységet nem azonosítottuk egyetlen rendszernél sem? Listázza ki ezen sérülékenységek nevét, CVE azonosítóját és CVSS pontszámát, a CVE azonosítója alapján növekvően rendezze.

vuln_nev	**CVE**	**CVSS**
Cisco Identity Services Engine Cross-Site Scripting Vulnerability	CVE-2022-20959	5.4
Cisco IP Telefophone Stack Overflow	CVE-2022-20968	8.5
Spring4Shell	CVE-2022-22965	9.8
...	...	...

5. Melyik sérülékenységet azonosítottuk a legtöbb rendszerben?

vuln_nev
Log4Shell

6. Melyik a legmagasabb a sérülékenységi pontszám, amit egy gépen észleltünk? (A gépet érintő összes sérülékenység összesített CVSS pontszáma) A számított mező neve legyen: `cvss_osszesen`.

cvss_osszesen
46.9

7. Melyik sérülékenység a legveszélyesebb a szervezetre nézve? (Ahol a sérülékenység pontszáma szorozva az érintett gépek számával a legmagasabb)

vuln_nev
Log4Shell

8. Jelenítse meg azon rendszerek nevét, mely Windows alapú, és amelyen legfeljebb 2 sérülékenységet azonosítottunk?

host_nev
mailgw
bulbasaur
venusaur
...

9. Mennyi sérülékenységet javítottuk a legrövidebb idő alatt? (javított állapotban van, és az első és utolsó szkennelés különbsége a legkisebb) A számított mező alias neve legyen `legkevesebb`!

vuln_nev
Imagemagick outside the range of representative value of type unsigned long

10. Mennyi a sérülékenységek átlagos javítási ideje? Egy tizedesjegyre kerekítve jelenítse meg az eredményt! A számított mező neve legyen: `atlagos_javitasi_ido`.

atlagos_javitasi_ido
26.5

11. Melyik a legrégebb óta nem javított sérülékenység?

vuln_nev
Oracle MySQL Denial of Service

12. Listázza ki azon kritikus sérülékenységeket (azt tekintjük kritikusnak, ahol a CVSS pontszám legalább 9), amelyek legalább 3 gépen nincsenek még javítva.

vuln_nev
Log4Shell