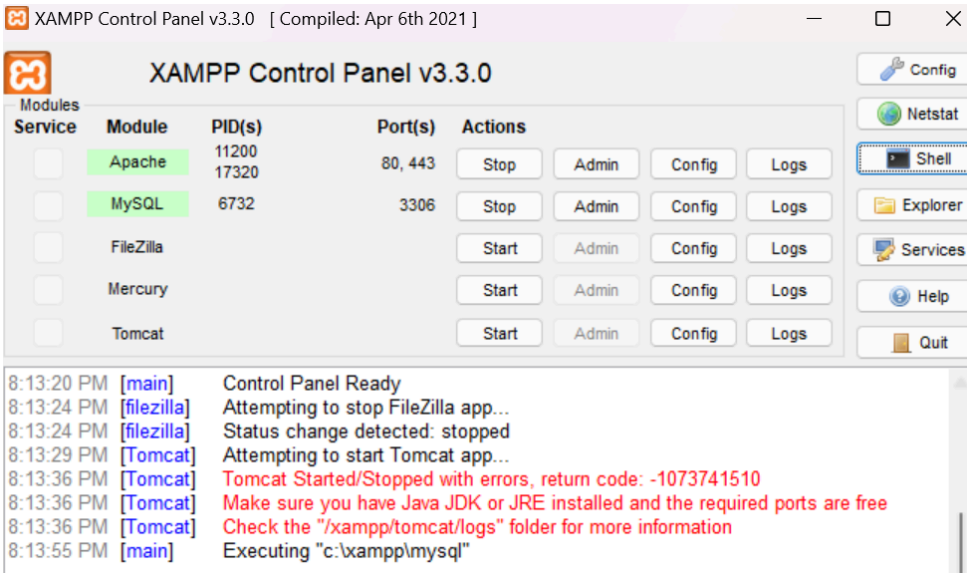
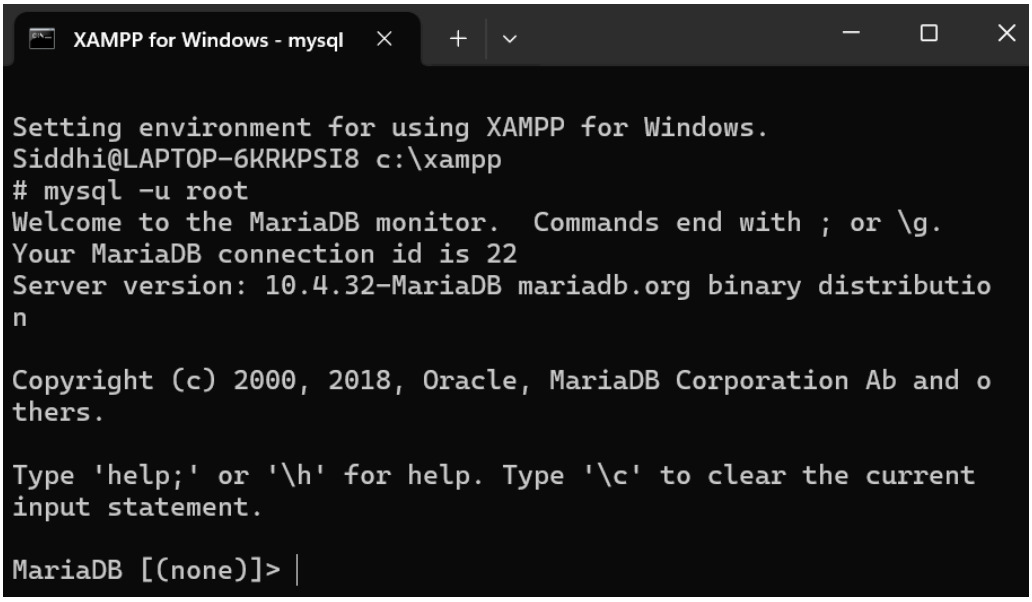
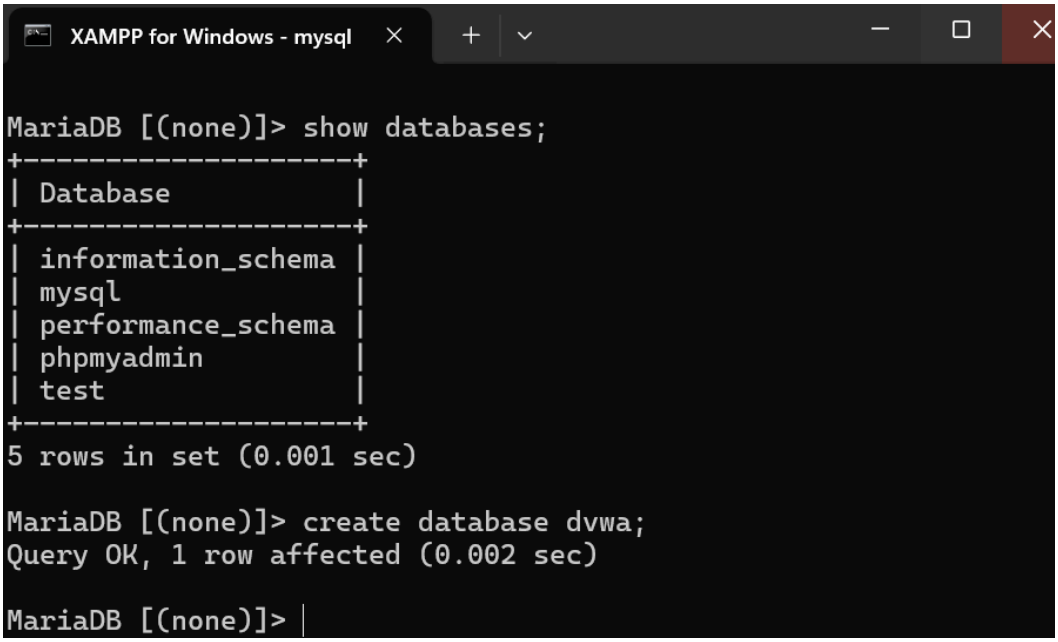
Module 5
Ethical Hacking Lab

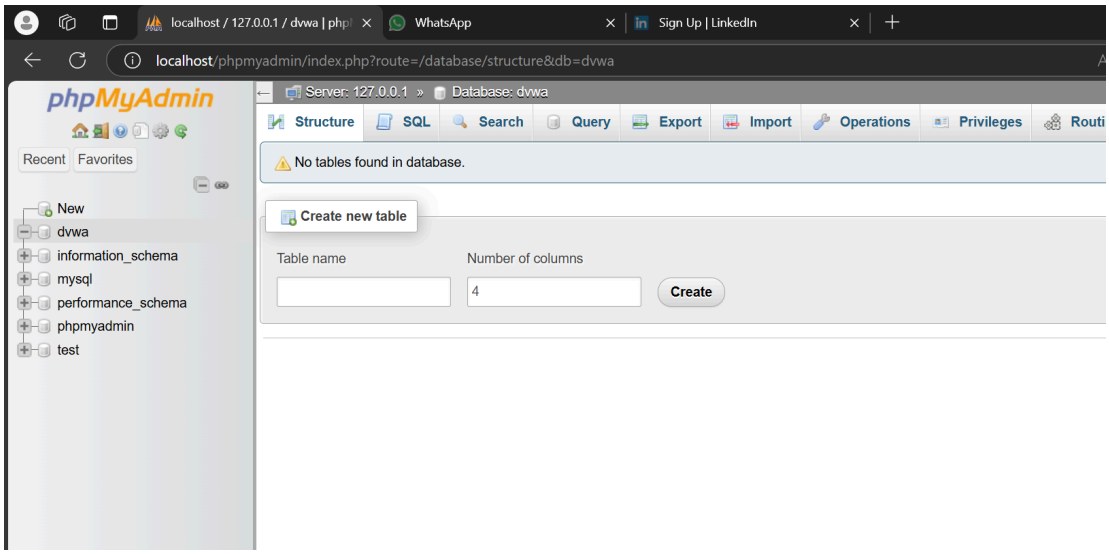
Practical 1:
Aim: 1. Hack a website using remote file inclusion:
A. Building a web hacking lab.
B. Install Xampp
Theory:
A web hacking lab allows security professionals, developers, and students to practice their skills without causing harm to real-world systems. The lab setup includes tools that simulate vulnerabilities found in actual web applications. By working in this environment, users can understand and learn how to exploit and mitigate security flaws in a controlled manner.
Steps:
1.Install xampp
Go to shell
mysql -u root
Show databases
Create database
2.download Dvwa master zip
Enter dvwa download in google
To aid security professionals to test their skills (Certified Ethical hacking course)
Helps web developers to understand the process
And helps students to learn the web application security
3.Copy dvwa folder in c:/xamp/htdocs
4.Change the file name c:/xamp/htdocs/dvwa/config/config.inc.php.dist to config.inc.php
Check dvwa dabatase settings
5.Enter in the browser
http://localhost/dvwa-master/setup.php
a.Click on create database
b.It will redirect you to dvwa login
admin
password
6.Remote file inclusion
Dvwa security should be made low
Click on file inclusion :
In the address bar set page attribute to google.com
7.Local file inclusion
Set the page attribute to local file
8. Enable url inclusion in htdocs/php/php.ini file(configuration file)

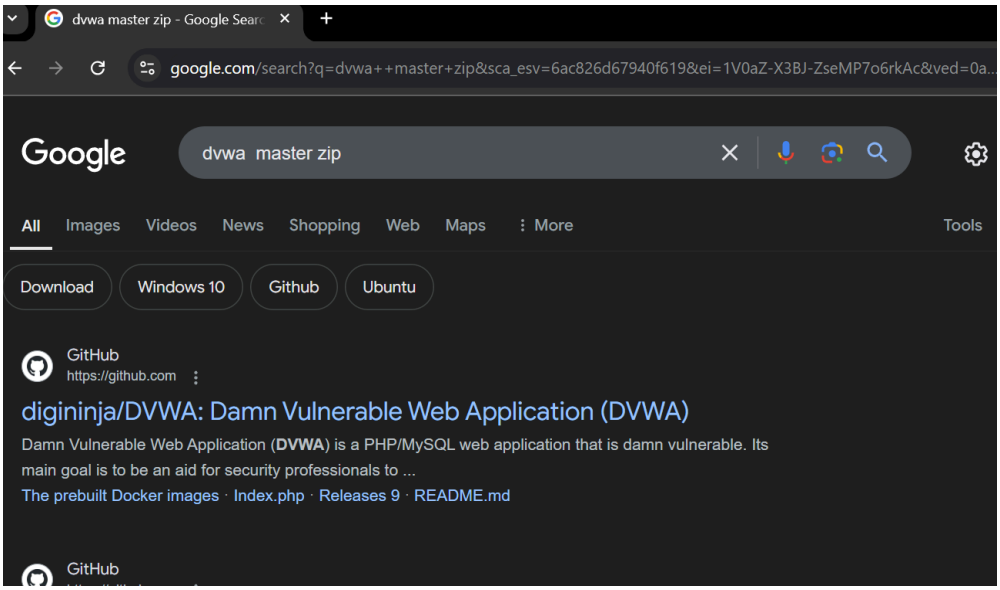
Note: Include urls in:
Ex: http://localhost/dvwa/vulnerabilities/fi/?page=https://www.google.com/
http://localhost/dvwa/vulnerabilities/fi/?page=file:///C:/xampp/htdocs/applications.html

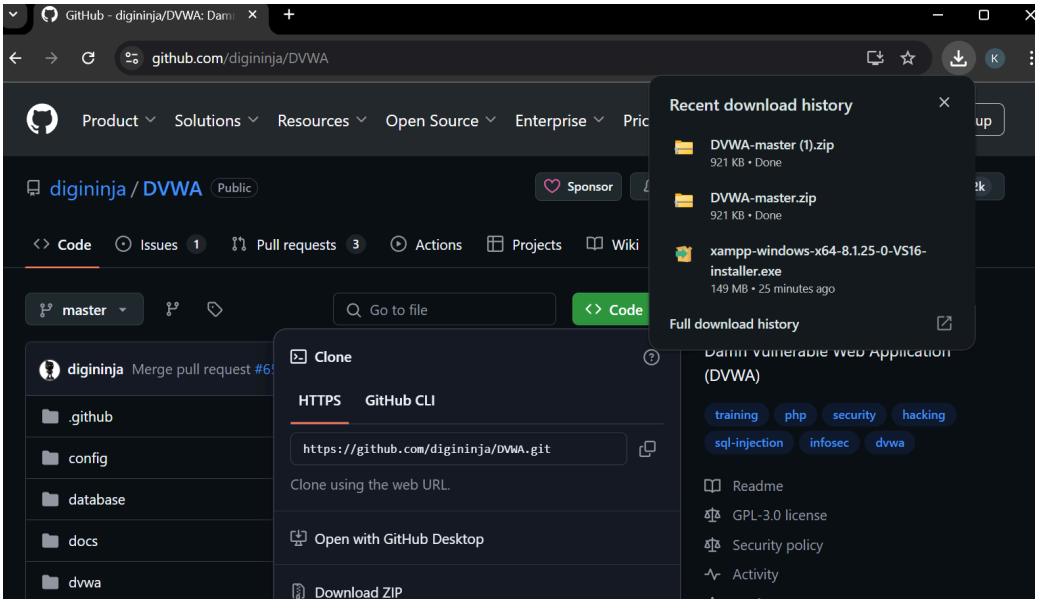

XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Modules
Service
Module
PID(s)
Port(s)
Actions
Apache
11200
17320
80, 443
Stop
Admin
Config
Logs
MySQL
6732
3306
Stop
Admin
Config
Logs
FileZilla
Start
Admin
Config
Logs
Mercury
Start
Admin
Config
Logs
Tomcat
Start
Admin
Config
Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
8:13:20 PM [main] Control Panel Ready
8:13:24 PM [filezilla] Attempting to stop FileZilla app...
8:13:24 PM [filezilla] Status change detected: stopped
8:13:29 PM [Tomcat] Attempting to start Tomcat app...
8:13:36 PM [Tomcat] Tomcat Started/Stopped with errors, return code: -1073741510
8:13:36 PM [Tomcat] Make sure you have Java JDK or JRE installed and the required ports are free
8:13:36 PM [Tomcat] Check the "/xampp/tomcat/logs" folder for more information
8:13:55 PM [main] Executing "c:\xampp\mysql"

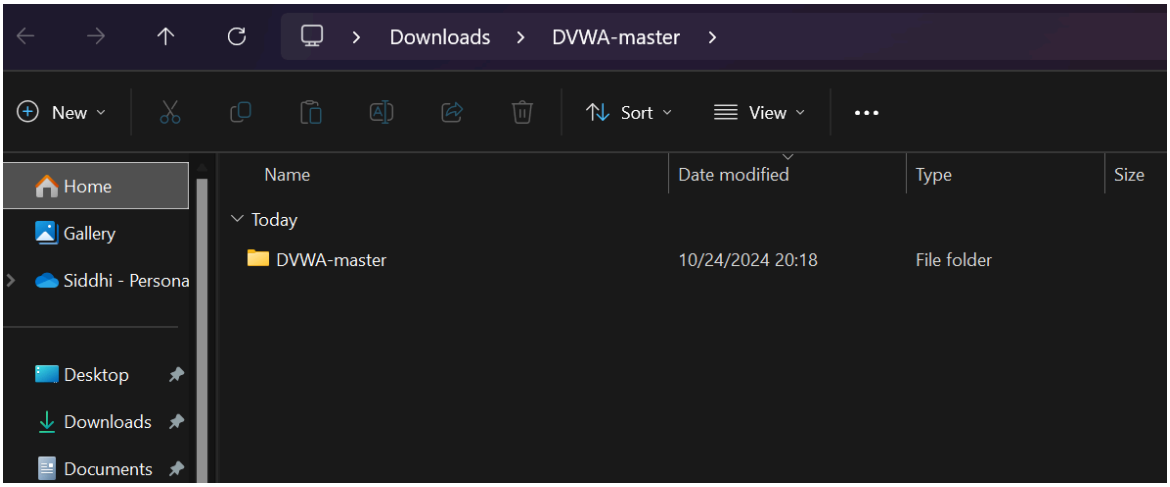

XAMPP for Windows - mysql
Setting environment for using XAMPP for Windows.
Siddhi@LAPTOP-6KRKPSI8 c:\xampp
mysql -u root
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 22
Server version: 10.4.32-MariaDB mariadb.org binary distributio
n
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and o
thers.
Type 'help;' or '\h' for help. Type '\c' to clear the current
input statement.
MariaDB [(none)]>

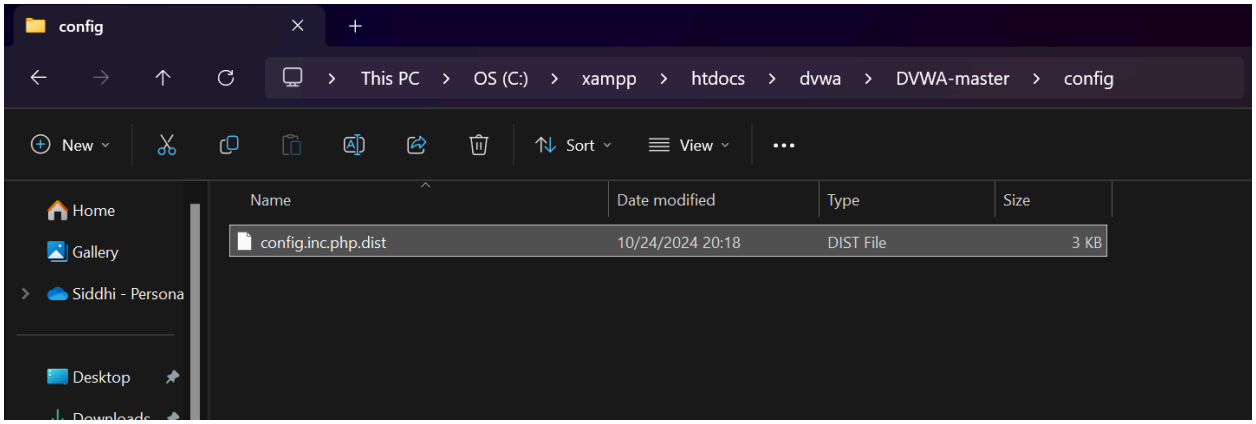

XAMPP for Windows - mysql
MariaDB [(none)]> show databases;
+--------------------+
| Database |
+--------------------+
| information_schema |
| mysql |
| performance_schema |
| phpmyadmin |
| test |
+--------------------+
5 rows in set (0.001 sec)
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.002 sec)
MariaDB [(none)]>

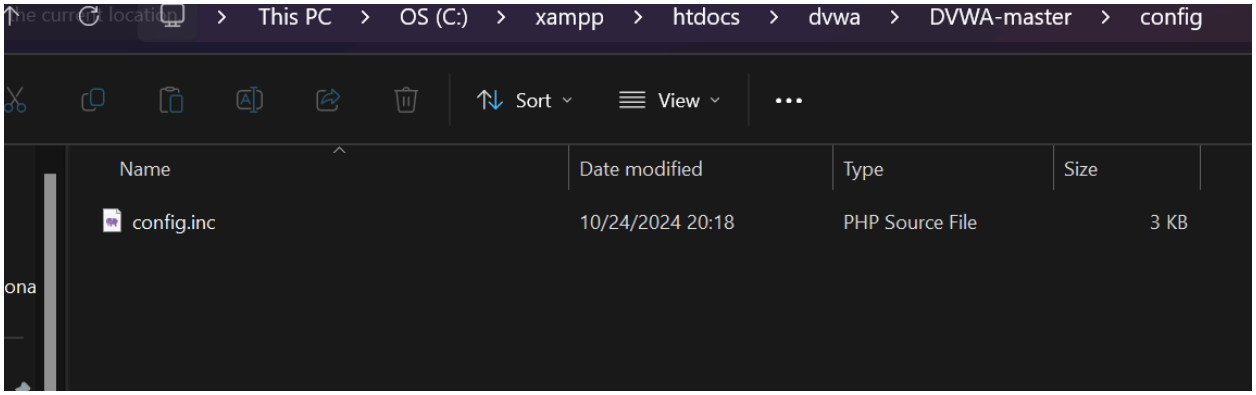

localhost / 127.0.0.1 / dvwa | php
WhatsApp
Sign Up | LinkedIn
localhost/phpmyadmin/index.php?route=/database/structure&db=dvwa
phpMyAdmin
Recent
Favorites
New
dvwa
information_schema
mysql
performance_schema
phpmyadmin
test
Server: 127.0.0.1 » Database: dvwa
Structure
SQL
Search
Query
Export
Import
Operations
Privileges
No tables found in database.
Create new table
Table name
Number of columns
4
Create

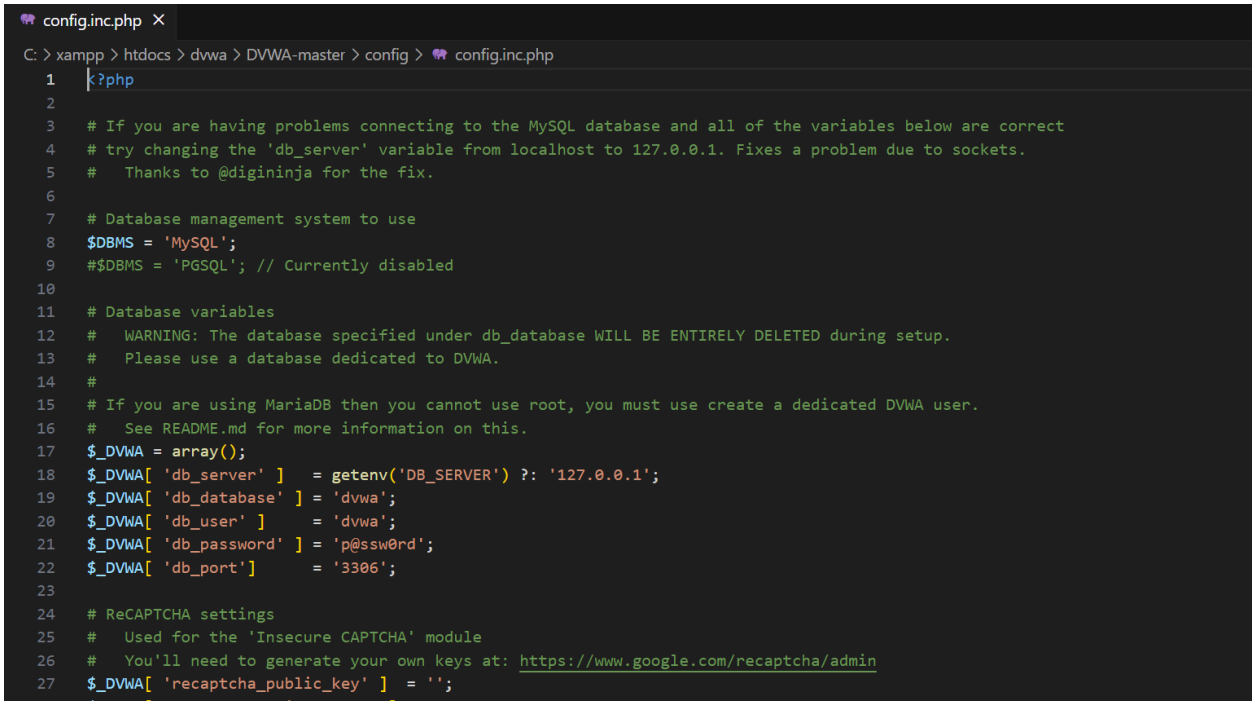

dvwa master zip - Google Sear
google.com/search?q=dvwa++master+zip&sca_esv=6ac826d67940f619&ei=1V0aZ-X3BJ-ZseMP7o6rkAc&ved=0a...
Google
dvwa master zip
All
Images
Videos
News
Shopping
Web
Maps
More
Tools
Download
Windows 10
Github
Ubuntu
GitHub
https://github.com
digininja/DVWA: Damn Vulnerable Web Application (DVWA)
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 ...
The prebuilt Docker images · Index.php · Releases 9 · README.md
GitHub

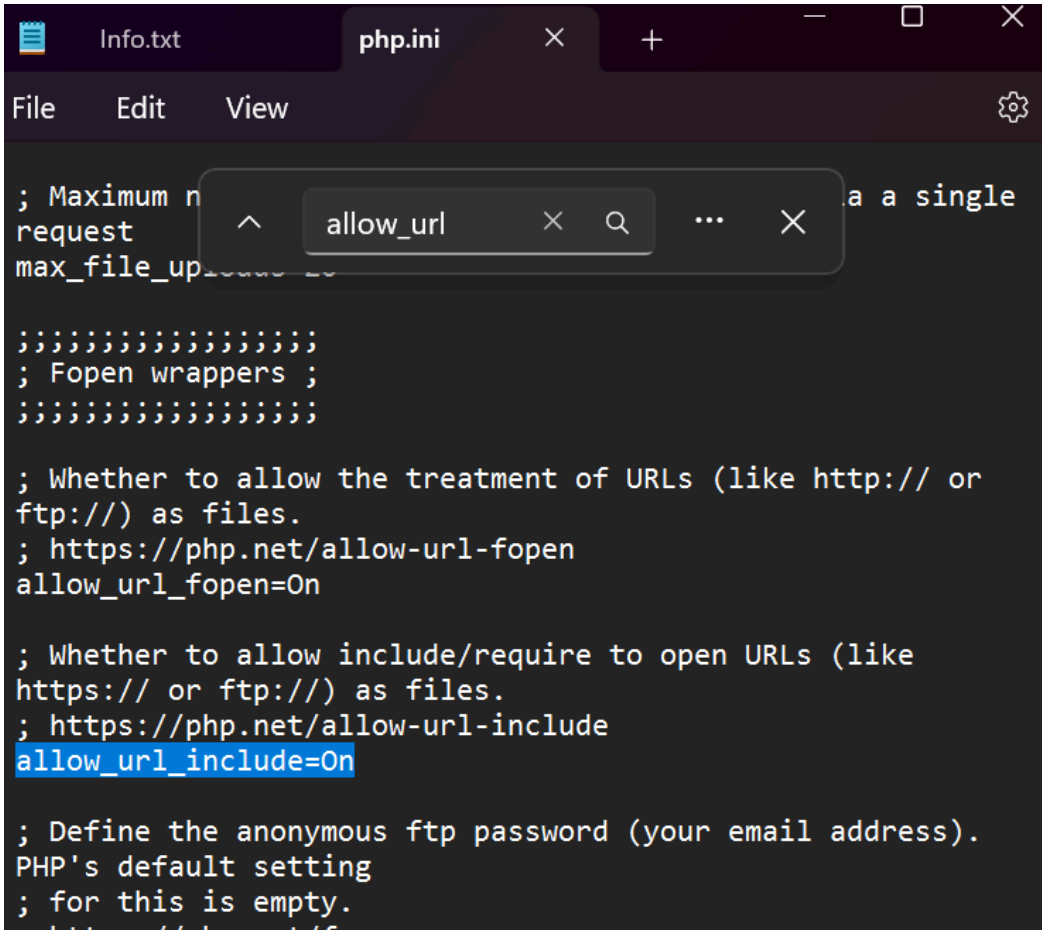

GitHub - digininja/DVWA: Dam
github.com/digininja/DVWA
Product
Solutions
Resources
Open Source
Enterprise
Recent download history
DVWA-master (1).zip
921 KB • Done
DVWA-master.zip
921 KB • Done
xampp-windows-x64-8.1.25-0-VS16-installer.exe
149 MB • 25 minutes ago
Full download history
digininja / DVWA
Public
Sponsor
Code
Issues 1
Pull requests 3
Actions
Projects
Wiki
master
Go to file
Code
digininja Merge pull request #6
.github
config
database
docs
dvwa
Clone
HTTPS
GitHub CLI
https://github.com/digininja/DVWA.git
Clone using the web URL.
Open with GitHub Desktop
Download ZIP
(DVWA)
training
php
security
hacking
sql-injection
infosec
dvwa
Readme
GPL-3.0 license
Security policy
Activity

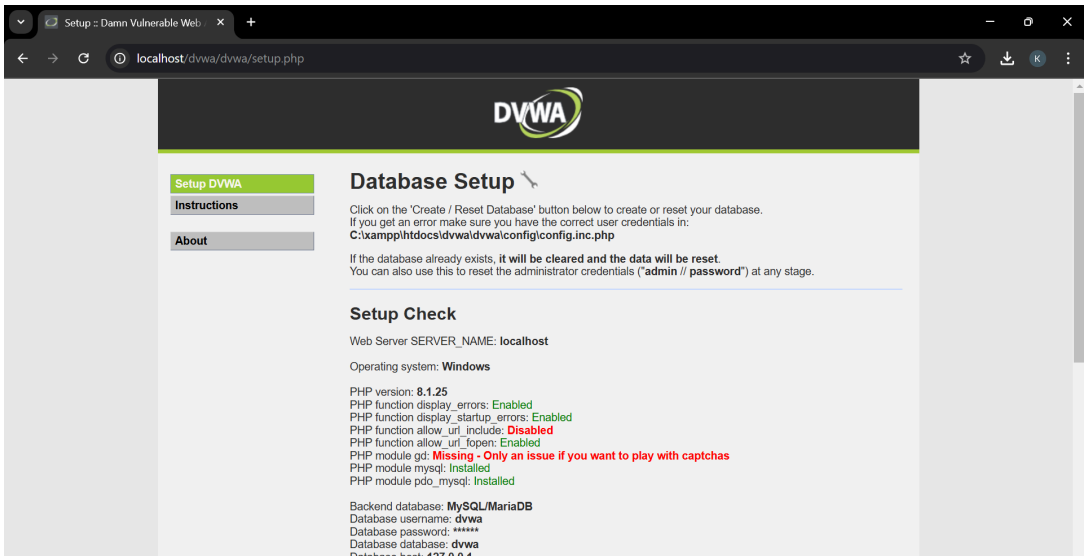

Downloads
DVWA-master
New
Sort
View
Home
Gallery
Siddhi - Persona
Desktop
Downloads
Documents
Name
Date modified
Type
Size
Today
DVWA-master
10/24/2024 20:18
File folder

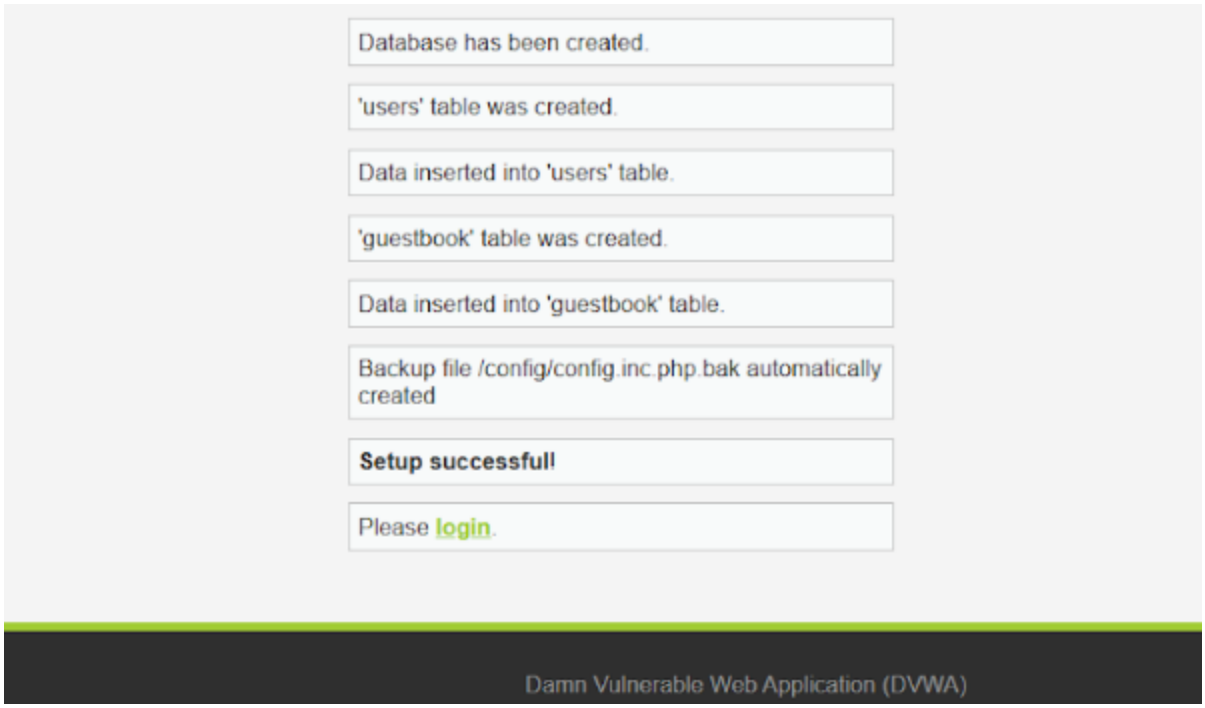

config
This PC
OS (C:)
xampp
htdocs
dvwa
DVWA-master
config
New
Sort
View
Home
Gallery
Siddhi - Persona
Desktop
Name
Date modified
Type
Size
config.inc.php.dist
10/24/2024 20:18
DIST File
3 KB

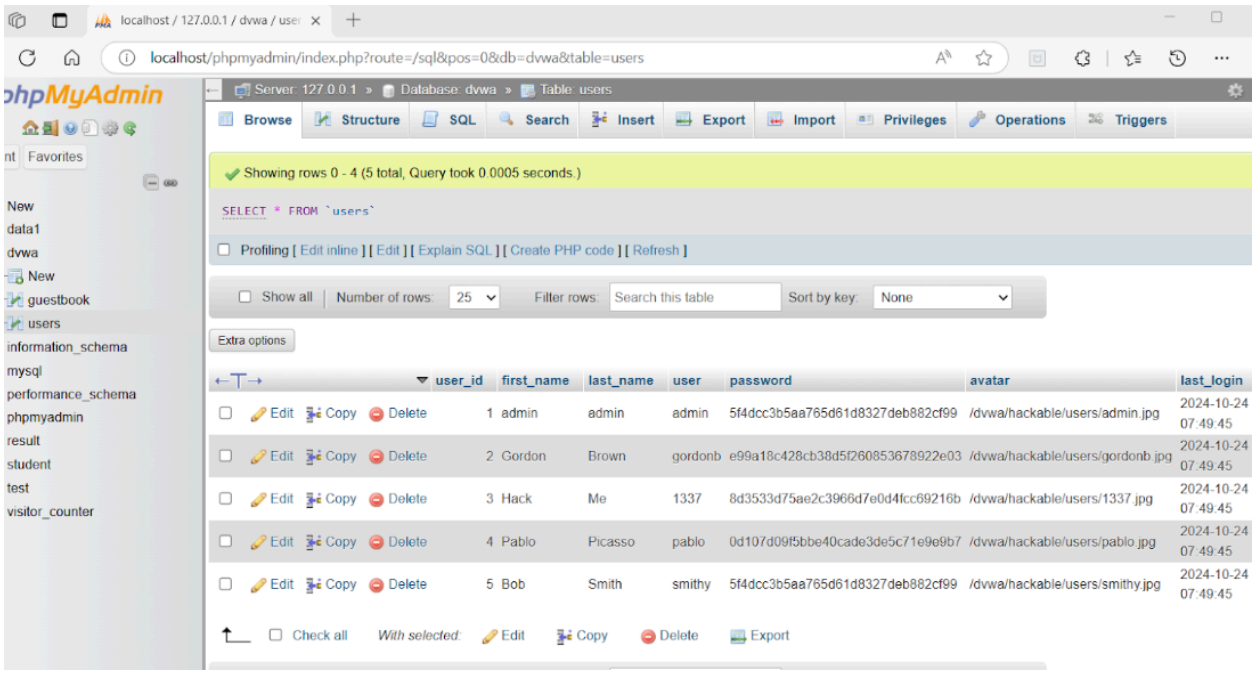

This PC
OS (C:)
xampp
htdocs
dvwa
DVWA-master
config
Sort
View
Name
Date modified
Type
Size
config.inc
10/24/2024 20:18
PHP Source File
3 KB

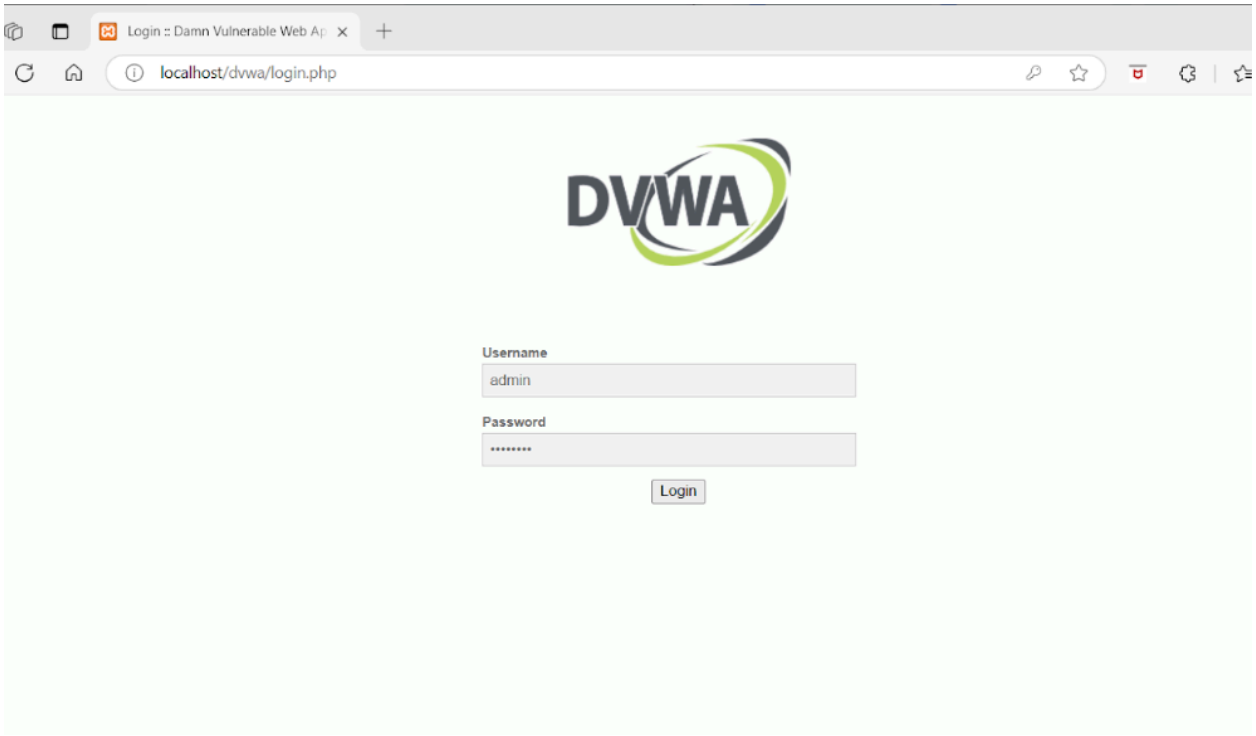

config.inc.php
C: > xampp > htdocs > dvwa > DVWA-master > config > config.inc.php
<?php
If you are having problems connecting to the MySQL database and all of the variables below are correct
try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
Thanks to @digininja for the fix.
Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled
Database variables
WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
Please use a database dedicated to DVWA.
#
If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server'] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'dvwa';
$_DVWA['db_password'] = 'p@ssw0rd';
$_DVWA['db_port'] = '3306';
ReCAPTCHA settings
Used for the 'Insecure CAPTCHA' module
You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA['recaptcha_public_key'] = '';

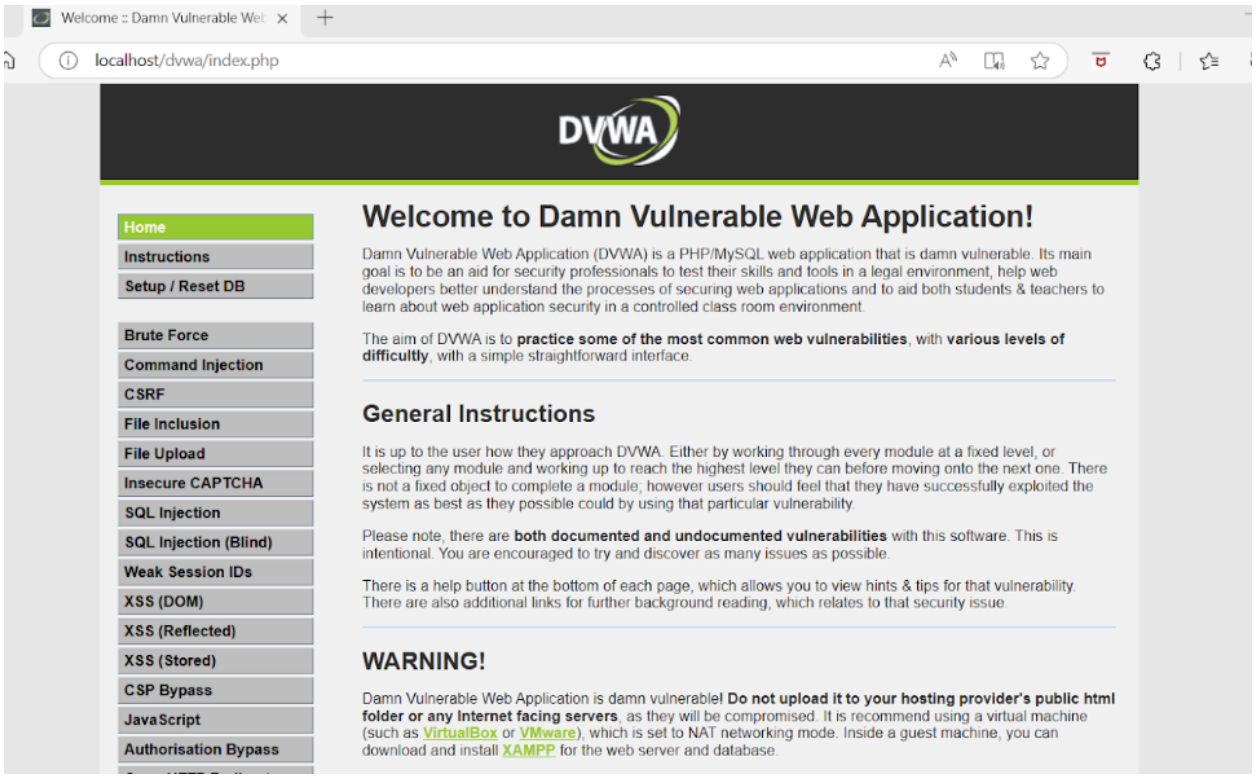

Info.txt
php.ini
File
Edit
View
allow_url
; Maximum n
a a single
request
max_file_up
;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;
; Whether to allow the treatment of URLs (like http:// or
ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen=On
; Whether to allow include/require to open URLs (like
https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include=On
; Define the anonymous ftp password (your email address).
PHP's default setting
; for this is empty.

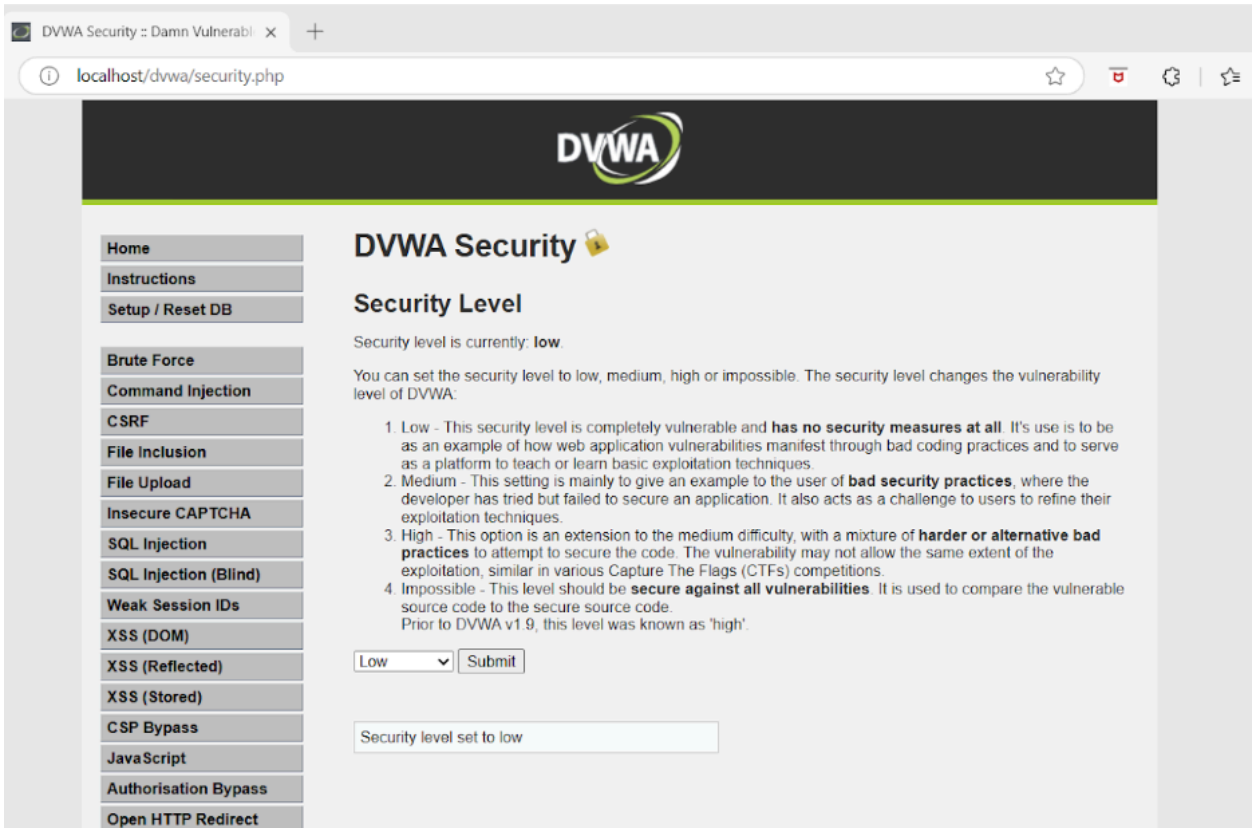

Setup :: Damn Vulnerable Web
localhost/dvwa/dvwa/setup.php
DVWA
Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in:
C:\xampp\htdocs\dvwa\dvwa\config\config.inc.php
If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.
Setup Check
Web Server SERVER_NAME: localhost
Operating system: Windows
PHP version: 8.1.25
PHP function display_errors: Enabled
PHP function display_startup_errors: Enabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed
Backend database: MySQL/MariaDB
Database username: dvwa
Database password: ******
Database database: dvwa


Database has been created.
'users' table was created.
Data inserted into 'users' table.
'guestbook' table was created.
Data inserted into 'guestbook' table.
Backup file /config/config.inc.php.bak automatically created
Setup successful!
Please login.
Damn Vulnerable Web Application (DVWA)

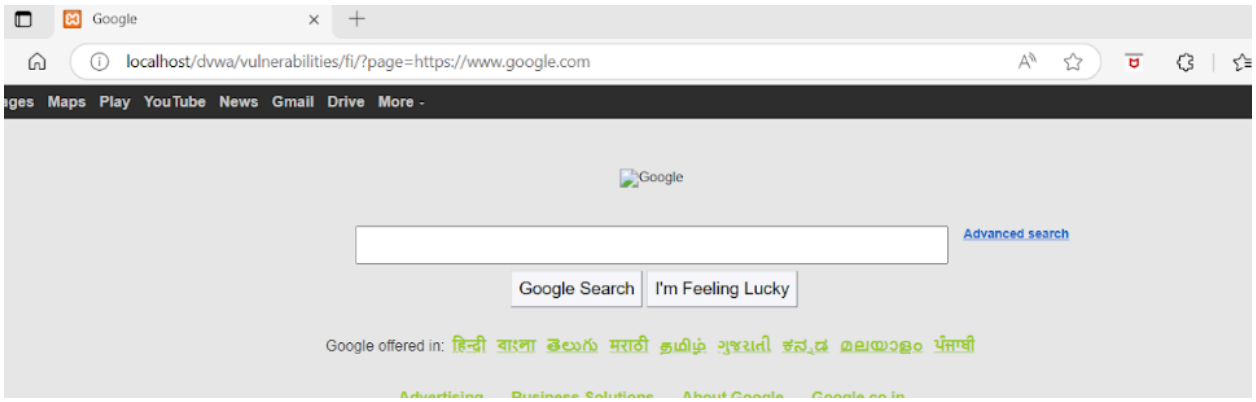

localhost / 127.0.0.1 / dvwa / user
localhost/phpmyadmin/index.php?route=/sql&pos=0&db=dvwa&table=users
phpMyAdmin
Server: 127.0.0.1 » Database: dvwa » Table: users
Browse
Structure
SQL
Search
Insert
Export
Import
Privileges
Operations
Triggers
Showing rows 0 - 4 (5 total, Query took 0.0005 seconds.)
SELECT * FROM `users`
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all
Number of rows: 25
Filter rows: Search this table
Sort by key: None
Extra options
user_id first_name last_name user password avatar last_login
1 admin admin admin 5f4dcc3b5aa765d61d8327deb882cf99 /dvwa/hackable/users/admin.jpg 2024-10-24 07:49:45
2 Gordon Brown gordonb e99a18c428cb38d5f260853678922e03 /dvwa/hackable/users/gordonb.jpg 2024-10-24 07:49:45
3 Hack Me 1337 8d3533d75ae2c3966d7e0d4fcc69216b /dvwa/hackable/users/1337.jpg 2024-10-24 07:49:45
4 Pablo Picasso pablo 0d107d09f5bbe40cade3de5c71e9e9b7 /dvwa/hackable/users/pablo.jpg 2024-10-24 07:49:45
5 Bob Smith smithy 5f4dcc3b5aa765d61d8327deb882cf99 /dvwa/hackable/users/smithy.jpg 2024-10-24 07:49:45
Edit Copy Delete
Check all
With selected:
Edit
Copy
Delete
Export
New
data1
dvwa
New
guestbook
users
information_schema
mysql
performance_schema
phpmyadmin
result
student
test
visitor_counter


Login :: Damn Vulnerable Web A
localhost/dvwa/login.php
DVWA
Username
admin
Password
Login


Welcome :: Damn Vulnerable Wel
localhost/dvwa/index.php
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
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 vulnerabilities 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.


DVWA Security :: Damn Vulnerabl
localhost/dvwa/security.php
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
DVWA Security
Security Level
Security level is currently: low.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.
Low
Submit
Security level set to low


localhost/dvwa/vulnerabilities/fi/?page=include.php
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
Vulnerability: File Inclusion
[file1.php] - [file2.php] - [file3.php]
More Information
Wikipedia - File inclusion vulnerability
WSTG - Local File Inclusion
WSTG - Remote File Inclusion


Google
localhost/dvwa/vulnerabilities/fi/?page=https://www.google.com
Maps
Play
YouTube
News
Gmail
Drive
More -
Google
Advanced search
Google Search
I'm Feeling Lucky
Google offered in:

SIDDHI S. KOTRE
ROLL NO: 50

Practical 2: 2. Using firefox, disguise/emulate as google bot to view hidden content of a Website.

Theory:

Websites often display different content to search engine crawlers like Googlebot compared to normal visitors. By emulating Googlebot in your browser, you can sometimes gain access to hidden or SEO-specific content. Below are the detailed steps to disguise Firefox as Googlebot.

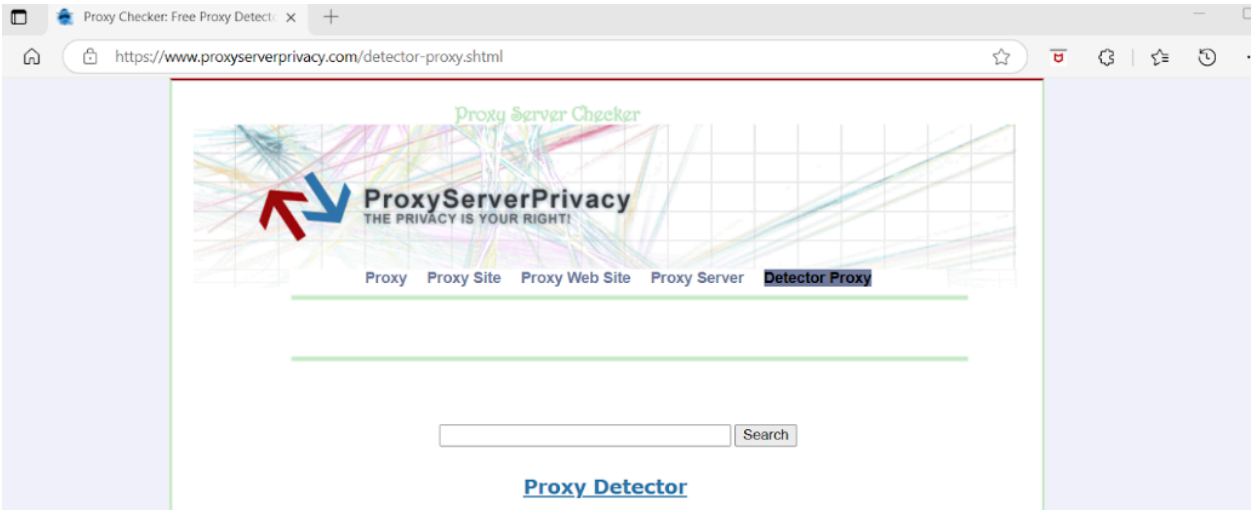
Steps:

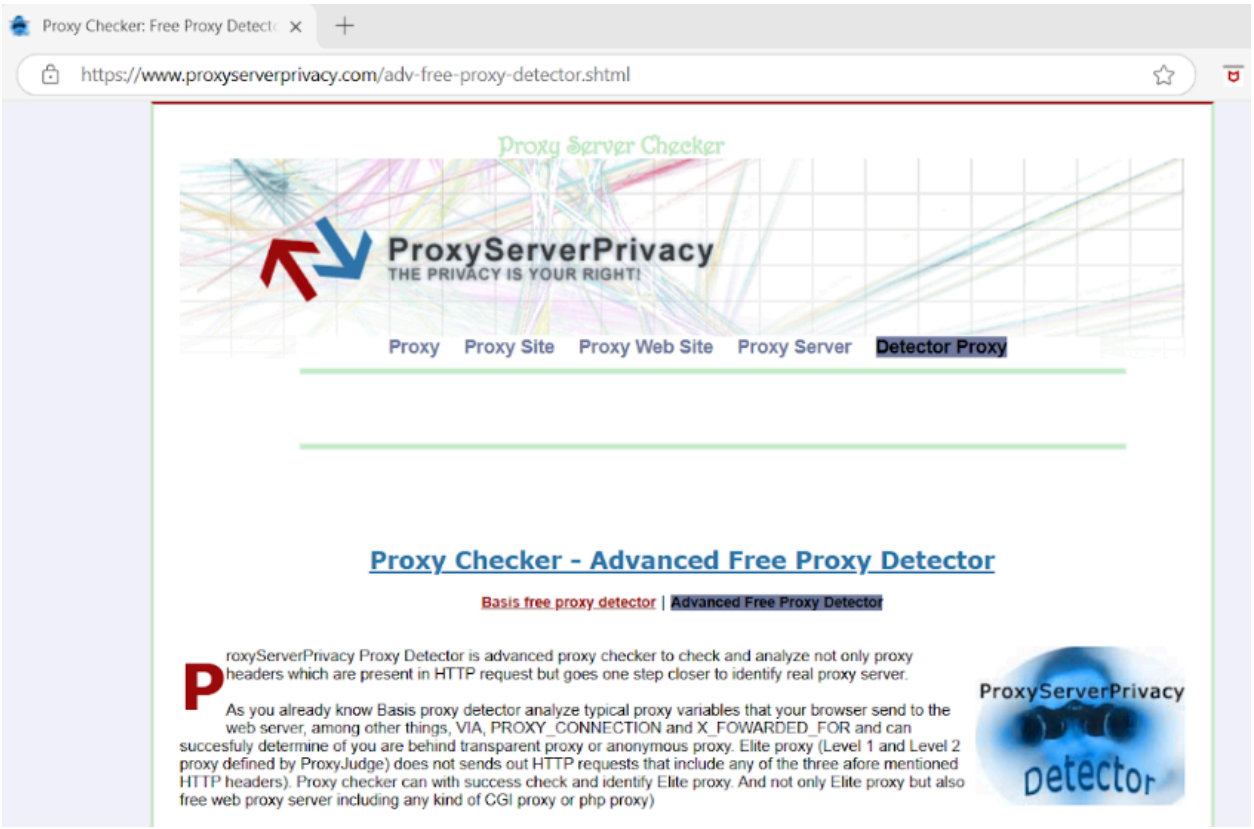
Step 1 :To determine the user agent of firefox.
a. Go to firefox - http://www.proxyserverprivacy.com/
b. Select detector proxy
c. Select advanced proxy detector.

Step 2 : To find out the string for google bot
To change above useragent to googlebot
a. Goto http://useragentstring.com/

b. Locate the string for google bot
Googlebot/2.1(+http://www.googlebot.com/bot.html)

Step 3 : Configure
a. Goto firefox
b. Type about:config
c. Type general.useragent.overrride and assign Googlebot/2.1
d. Goto http://www.proxyserverprivacy.com/ to check that the useragent in googlebot
3. Use Kaspersky/Quick heal for lifetime without patch
a. Explain the steps to use KasperKey / Quickheal for lifetime without patch.
References:
http://maroofcreations.weebly.com/how-to-use-kaspersky-for-lifetime-without-patch.html
https://youtu.be/DbSk10kX09s
https://www.youtube.com/watch?v=MTWYdhH_wH0


Proxy Checker: Free Proxy Detect
https://www.proxyserverprivacy.com/detector-proxy.shtml
Proxy Server Checker
ProxyServerPrivacy
THE PRIVACY IS YOUR RIGHT!
Proxy
Proxy Site
Proxy Web Site
Proxy Server
Detector Proxy
Search
Proxy Detector


Proxy Checker: Free Proxy Detect
https://www.proxyserverprivacy.com/adv-free-proxy-detector.shtml
Proxy Server Checker
ProxyServerPrivacy
THE PRIVACY IS YOUR RIGHT!
Proxy
Proxy Site
Proxy Web Site
Proxy Server
Detector Proxy
Proxy Checker - Advanced Free Proxy Detector
Basis free proxy detector | Advanced Free Proxy Detector
roxyServerPrivacy Proxy Detector is advanced proxy checker to check and analyze not only proxy headers which are present in HTTP request but goes one step closer to identify real proxy server.
As you already know Basis proxy detector analyze typical proxy variables that your browser send to the web server, among other things, VIA, PROXY_CONNECTION and X_FOWARDED_FOR and can succesfuly determine of you are behind transparent proxy or anonymous proxy. Elite proxy (Level 1 and Level 2 proxy defined by ProxyJudge) does not sends out HTTP requests that include any of the three afore mentioned HTTP headers). Proxy checker can with success check and identify Elite proxy. And not only Elite proxy but also free web proxy server including any kind of CGI proxy or php proxy)
ProxyServerPrivacy
detector

Free Proxy Checker Detection

Your Ip Address: **103.210.202.135**
Host: **103.210.202.135**
Your Country:
Proxy HTTP_X_FORWARDED Variable: **(none)**
Proxy HTTP_VIA Variable: **(none)**
Proxy HTTP_PROXY_CONNECTION: **(none)**
Cache Pragma: **(none)**
Your Browser: **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36 Edg/130.0.0.0**
Type of Your connection: **keep-alive**
Server Protocol: **HTTP/1.1**
Your language: **en-US,en;q=0.9,en-IN;q=0.8**
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**
Accept-Encoding: **gzip, deflate, br, zstd**
Referer - HTTP Request come from: **https://www.proxyserverprivacy.com/detector-proxy.shtml**
Your Port: **31231**

Conclusion after analyzing ip address:

You do not use proxy

Search

User Agent String.Com

Home | List of User Agent Strings | Links | API |

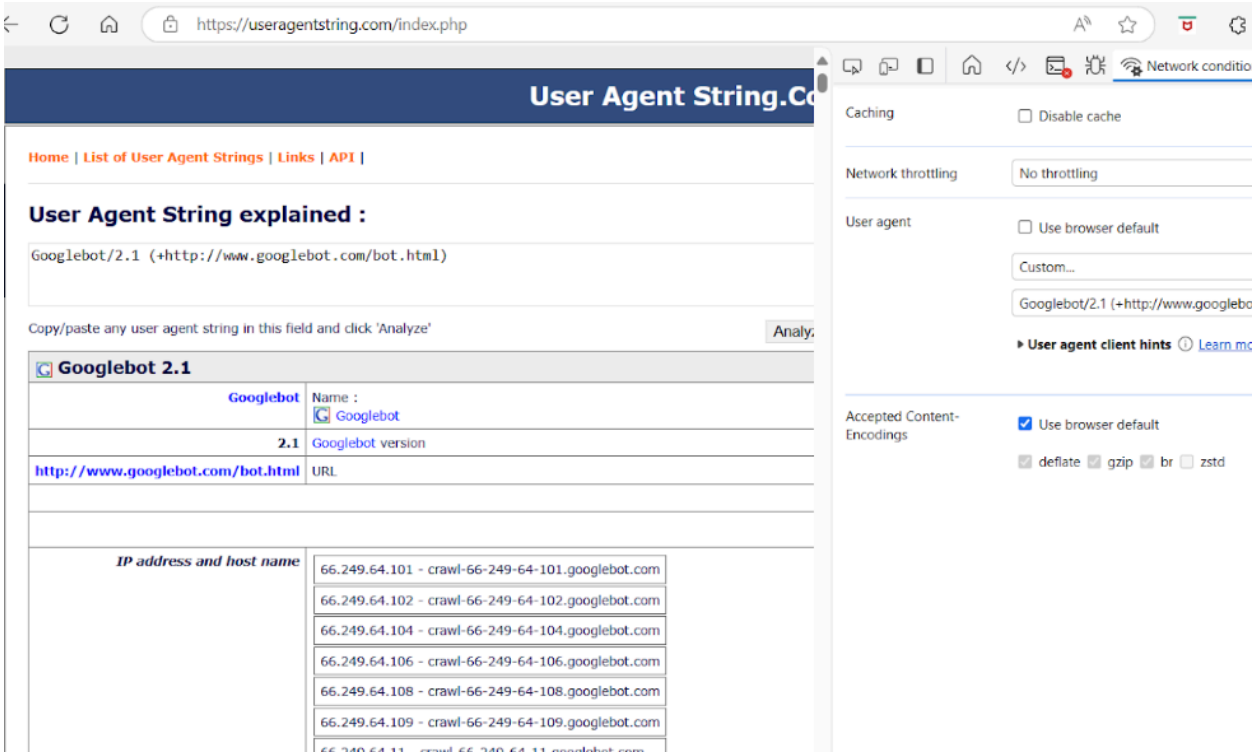
User Agent String explained :

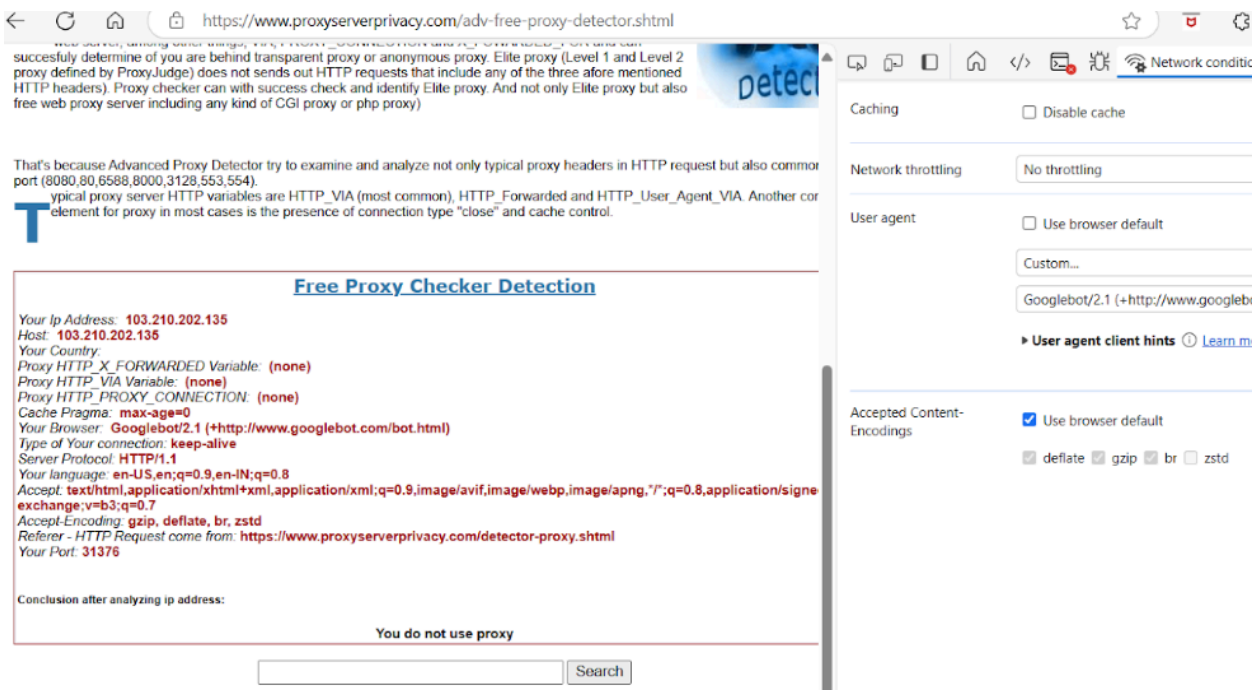
```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/130.0.0.0 Safari/537.36 Edg/130.0.0.0
```

Copy/paste any user agent string in this field and click 'Analyze' Analyze

Chrome 130.0.0.0

Mozilla	MozillaProductSlice. Claims to be a Mozilla based user agent, which is only true for Gecko browsers like Firefox and Netscape. For all other user agents it means 'Mozilla-compatible'. In


https://useragentstring.com/index.php
User Agent String.Co
Home | List of User Agent Strings | Links | API |
User Agent String explained :
Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Copy/paste any user agent string in this field and click 'Analyze'
Analy
Googlebot 2.1
Googlebot
Name :
Googlebot
2.1
Googlebot version
http://www.googlebot.com/bot.html
URL
IP address and host name
66.249.64.101 - crawl-66-249-64-101.googlebot.com
66.249.64.102 - crawl-66-249-64-102.googlebot.com
66.249.64.104 - crawl-66-249-64-104.googlebot.com
66.249.64.106 - crawl-66-249-64-106.googlebot.com
66.249.64.108 - crawl-66-249-64-108.googlebot.com
66.249.64.109 - crawl-66-249-64-109.googlebot.com
Network conditio
Caching
Disable cache
Network throttling
No throttling
User agent
Use browser default
Custom...
Googlebot/2.1 (+http://www.googlebo
User agent client hints
Learn mo
Accepted Content-Encodings
Use browser default
deflate
gzip
br
zstd


https://www.proxyserverprivacy.com/adv-free-proxy-detector.shtml
succesfully determine of you are behind transparent proxy or anonymous proxy. Elite proxy (Level 1 and Level 2 proxy defined by ProxyJudge) does not sends out HTTP requests that include any of the three afore mentioned HTTP headers). Proxy checker can with success check and identify Elite proxy. And not only Elite proxy but also free web proxy server including any kind of CGI proxy or php proxy)
That's because Advanced Proxy Detector try to examine and analyze not only typical proxy headers in HTTP request but also commor
port (8080,80,6588,8000,3128,553,554).
ypical proxy server HTTP variables are HTTP_VIA (most common), HTTP_Forwarded and HTTP_User_Agent_VIA. Another cor
element for proxy in most cases is the presence of connection type "close" and cache control.
Free Proxy Checker Detection
Your Ip Address: 103.210.202.135
Host: 103.210.202.135
Your Country:
Proxy HTTP_X_FORWARDED Variable: (none)
Proxy HTTP_VIA Variable: (none)
Proxy HTTP_PROXY_CONNECTION: (none)
Cache Pragma: max-age=0
Your Browser: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Type of Your connection: keep-alive
Server Protocol: HTTP/1.1
Your language: en-US,en;q=0.9,en-IN;q=0.8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signe
exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br, zstd
Referer - HTTP Request come from: https://www.proxyserverprivacy.com/detector-proxy.shtml
Your Port: 31376
Conclusion after analyzing ip address:
You do not use proxy
Search
Network conditic
Caching
Disable cache
Network throttling
No throttling
User agent
Use browser default
Custom...
Googlebot/2.1 (+http://www.googlebo
User agent client hints
Learn m
Accepted Content-Encodings
Use browser default
deflate
gzip
br
zstd

3. Using Kaspersky/Quick Heal for a Lifetime Without a Patch

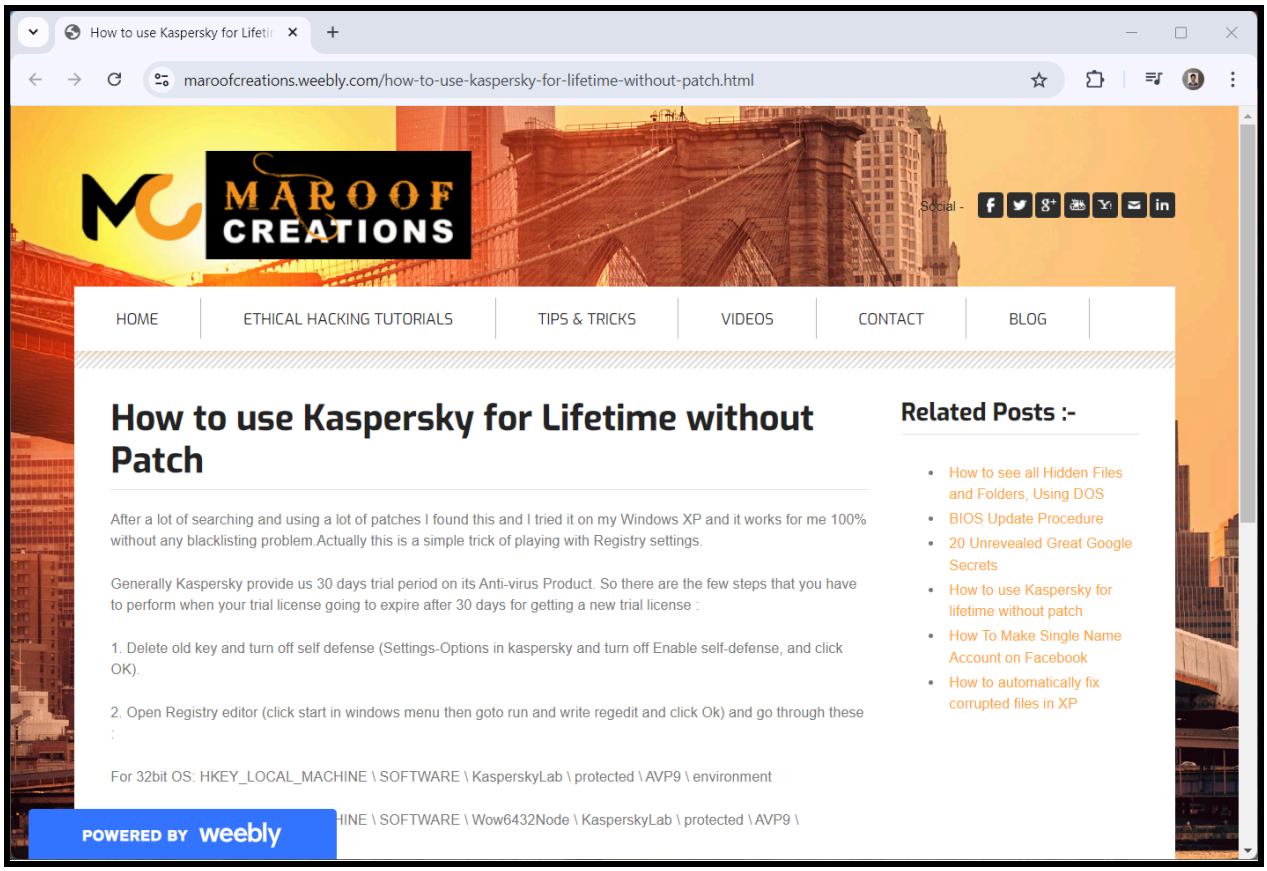
Steps to be followed:

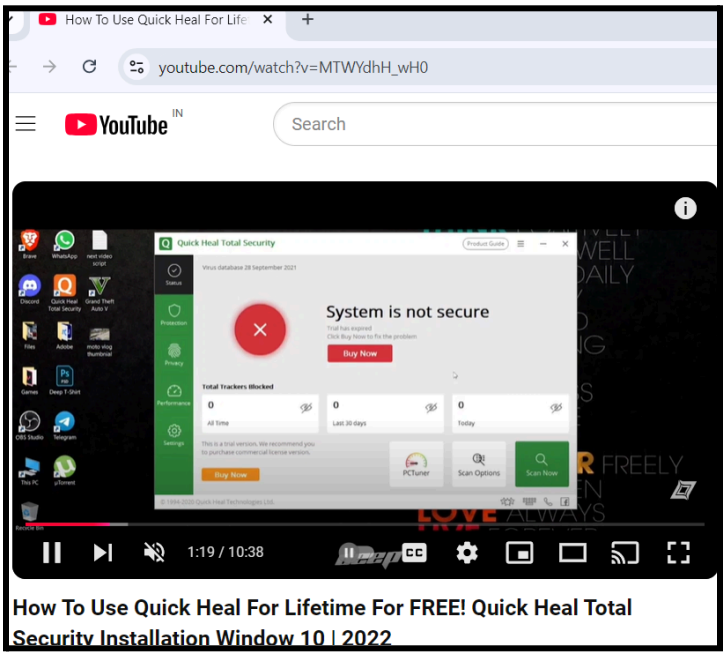
Kaspersky typically provides a 30-day trial for its antivirus products. To renew your trial license ethically without using patches, follow these steps:

1. Disable Self-Defense:
   - Open Kaspersky and go to Settings > Options.
   - Turn off Enable Self-Defense and click OK.
2. Edit Registry:
   - Open the Registry Editor by pressing Win + R, typing regedit, and hitting Enter.
   - Navigate to the following paths:
     - For 32-bit OS: HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\AVP9\environment
     - For 64-bit OS: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\protected\AVP9\environment
   - Locate PCID, right-click, and modify the last three or four characters (e.g., change 8F10C22F-6EF6-4378-BAB1-34722F6D454 to a different combination).
3. Restart Kaspersky:
   - Right-click the Kaspersky icon in the taskbar and select Exit.
   - Reopen Kaspersky and activate the search for a trial license. You should receive a new 30-day trial.
4. Re-enable Self-Defense:
   - Go back to Settings and turn Enable Self-Defense back on.

Note: This method modifies registry settings to change your PC's identification to Kaspersky servers, allowing you to obtain a new trial license. Ensure this process is done ethically and within legal boundaries.

Output:


How to use Kaspersky for Lifetir
maroofcreations.weebly.com/how-to-use-kaspersky-for-lifetime-without-patch.html
MAROOF CREATIONS
Social -
HOME
ETHICAL HACKING TUTORIALS
TIPS & TRICKS
VIDEOS
CONTACT
BLOG
How to use Kaspersky for Lifetime without Patch
After a lot of searching and using a lot of patches I found this and I tried it on my Windows XP and it works for me 100% without any blacklisting problem.Actually this is a simple trick of playing with Registry settings.
Generally Kaspersky provide us 30 days trial period on its Anti-virus Product. So there are the few steps that you have to perform when your trial license going to expire after 30 days for getting a new trial license :
1. Delete old key and turn off self defense (Settings-Options in kaspersky and turn off Enable self-defense, and click OK).
2. Open Registry editor (click start in windows menu then goto run and write regedit and click Ok) and go through these :
For 32bit OS: HKEY_LOCAL_MACHINE \ SOFTWARE \ KasperskyLab \ protected \ AVP9 \ environment
HINE \ SOFTWARE \ Wow6432Node \ KasperskyLab \ protected \ AVP9 \
Related Posts :-
How to see all Hidden Files and Folders, Using DOS
BIOS Update Procedure
20 Unrevealed Great Google Secrets
How to use Kaspersky for lifetime without patch
How To Make Single Name Account on Facebook
How to automatically fix corrupted files in XP
POWERED BY weebly


How To Use Quick Heal For Life
youtube.com/watch?v=MTWYdhH_wH0
YouTube IN
Search
Quick Heal Total Security
System is not secure
Buy Now
1:19 / 10:38
How To Use Quick Heal For Lifetime For FREE! Quick Heal Total Security Installation Window 10 | 2022