Ethical Hacking Lab
Module 5: Hacking web servers, web applications

Assignment 5: Use of software tools and commands for hacking web servers and web applications, and generating an analysis report.

1. Hacking a Website Using Remote File Inclusion

Aim: To understand and demonstrate the exploitation of Remote File Inclusion vulnerabilities in web applications, highlighting the potential risks associated with improper input validation and file handling

Theory:

Remote File Inclusion (RFI) is a type of vulnerability that allows an attacker to include a file on a web server through the URL parameters. This type of attack is typically found in web applications that allow the inclusion of files based on user input without proper validation. RFI can lead to severe consequences, such as unauthorized access to the server, data manipulation, and execution of malicious scripts.

Key Concepts:

- Inclusion Vulnerability: Occurs when an application includes files based on user input without sufficient checks.
- File Inclusion: Attackers can specify external files (hosted on their servers) to be included in the application.
- Potential Risks: Execution of arbitrary code, data theft, server takeover, etc.

Steps to be followed:

1. Install XAMPP:

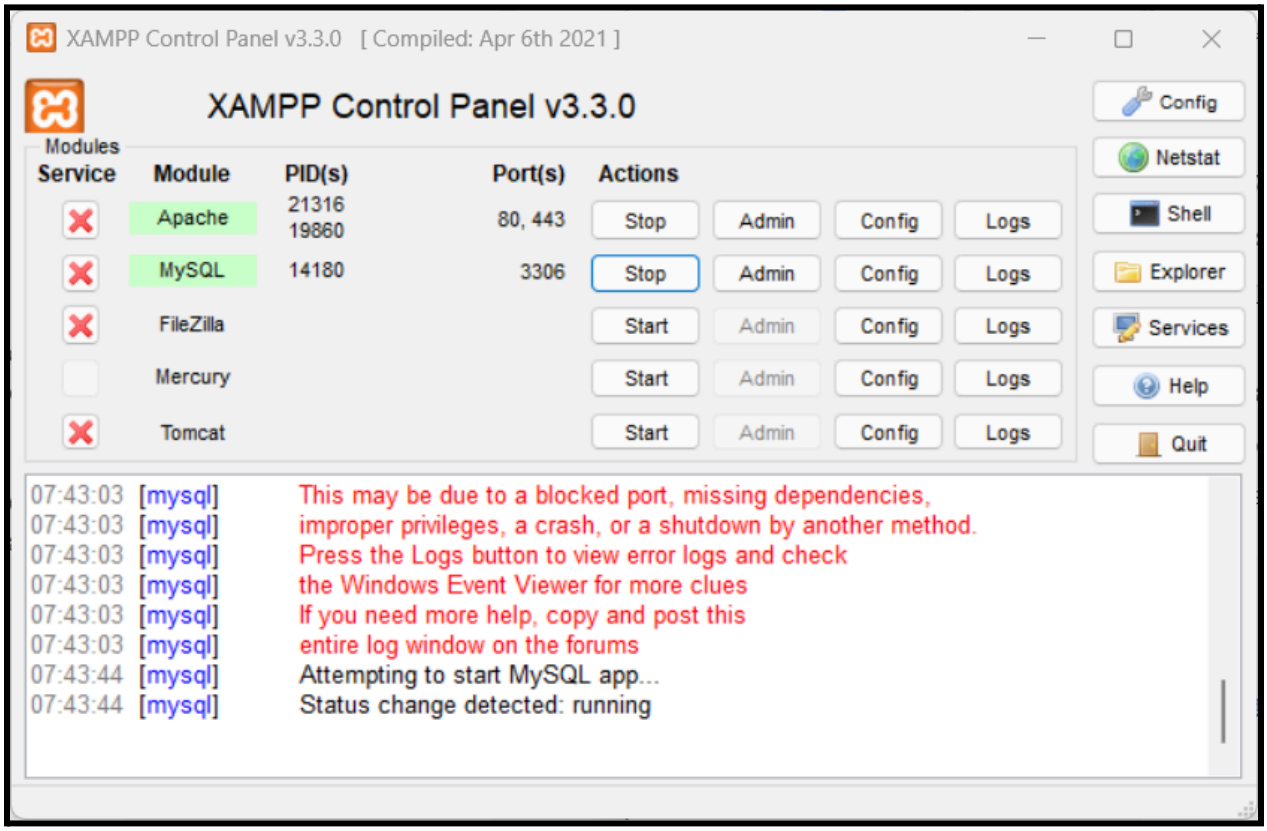
- Open the shell and type:
  # mysql -u root
- To view databases, type:
  MariaDB [(none)]> show databases;
- Create a new database with:
  MariaDB [(none)]> create database dvwa;

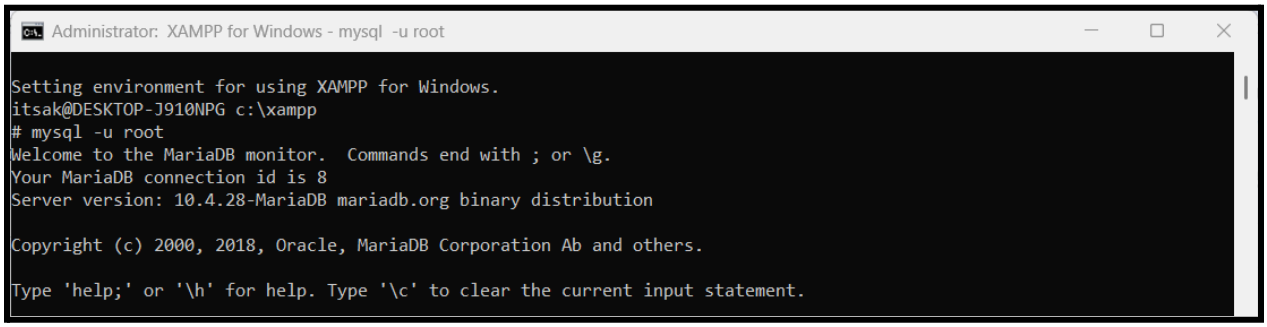
2. Download DVWA:

- Search for "DVWA master zip" on Google and download it.
- DVWA (Damn Vulnerable Web Application) is a tool designed to help security professionals test their skills, assist web developers in understanding vulnerabilities, and help students learn about web application security.

3. Set Up DVWA:
   - Copy the DVWA folder to C:/xampp/htdocs.
   - Rename the file C:/xampp/htdocs/dvwa/config/config.inc.php.dist to config.inc.php.
   - Check DVWA database settings.
4. Enable URL Inclusion:
   - In the php.ini configuration file (C:/xampp/php/php.ini), enable URL inclusion.
5. Access DVWA in the Browser:
   - Go to: http://localhost/dvwa-master/setup.php
   - Click "Create Database."
   - After this, you will be redirected to the DVWA login page. The default credentials are:
     - Username: admin
     - Password: password
6. Remote File Inclusion (RFI):
   - Set the DVWA security level to low.
   - Click on "File Inclusion."
   - In the address bar, set the page attribute to: page=https://www.google.com
7. Local File Inclusion (LFI):
   - Set the page attribute to a local file: page=file:///C:/xampp/htdocs/applications.html
8. Examples of URL Inclusion:
   - For remote file inclusion: http://localhost/dvwa/vulnerabilities/fi/?page=https://www.google.com/
   - For local file inclusion: http://localhost/dvwa/vulnerabilities/fi/?page=file:///C:/xampp/htdocs/applications.html

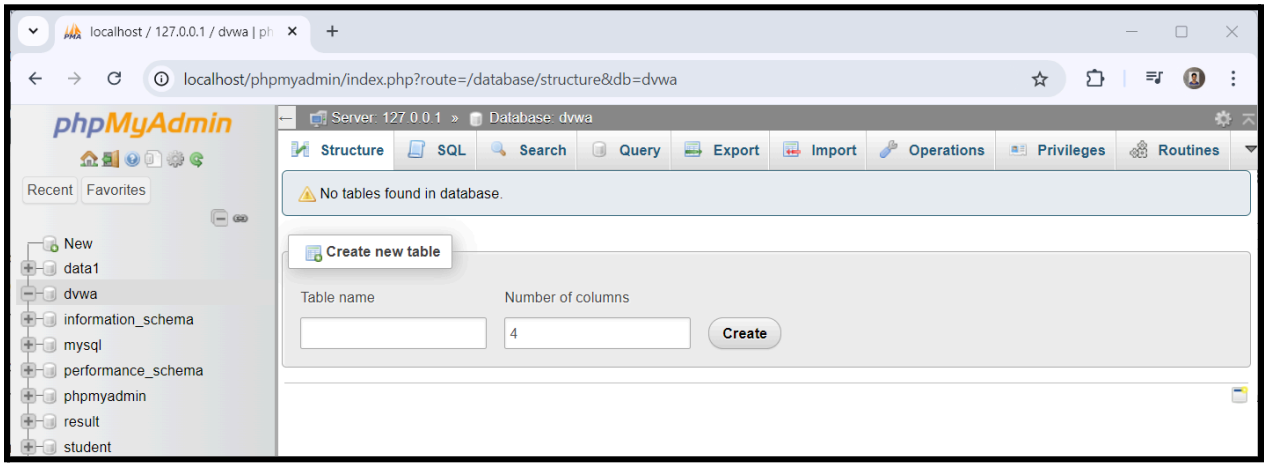
Output:

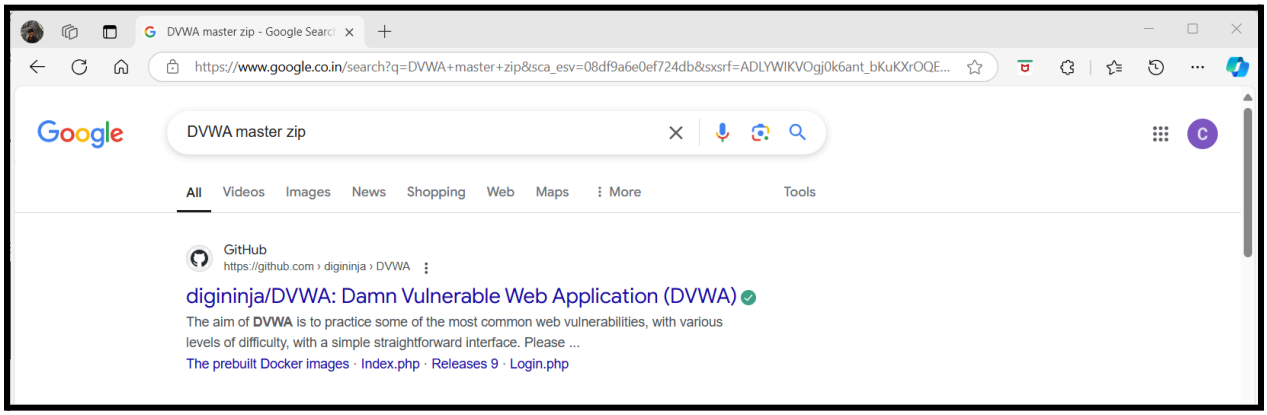

XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Modules
Service Module PID(s) Port(s) Actions
Apache 21316 19860 80, 443 Stop Admin Config Logs
MySQL 14180 3306 Stop Admin Config Logs
FileZilla Start Admin Config Logs
Mercury Start Admin Config Logs
Tomcat Start Admin Config Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
07:43:03 [mysql] This may be due to a blocked port, missing dependencies,
07:43:03 [mysql] improper privileges, a crash, or a shutdown by another method.
07:43:03 [mysql] Press the Logs button to view error logs and check
07:43:03 [mysql] the Windows Event Viewer for more clues
07:43:03 [mysql] If you need more help, copy and post this
07:43:03 [mysql] entire log window on the forums
07:43:44 [mysql] Attempting to start MySQL app...
07:43:44 [mysql] Status change detected: running

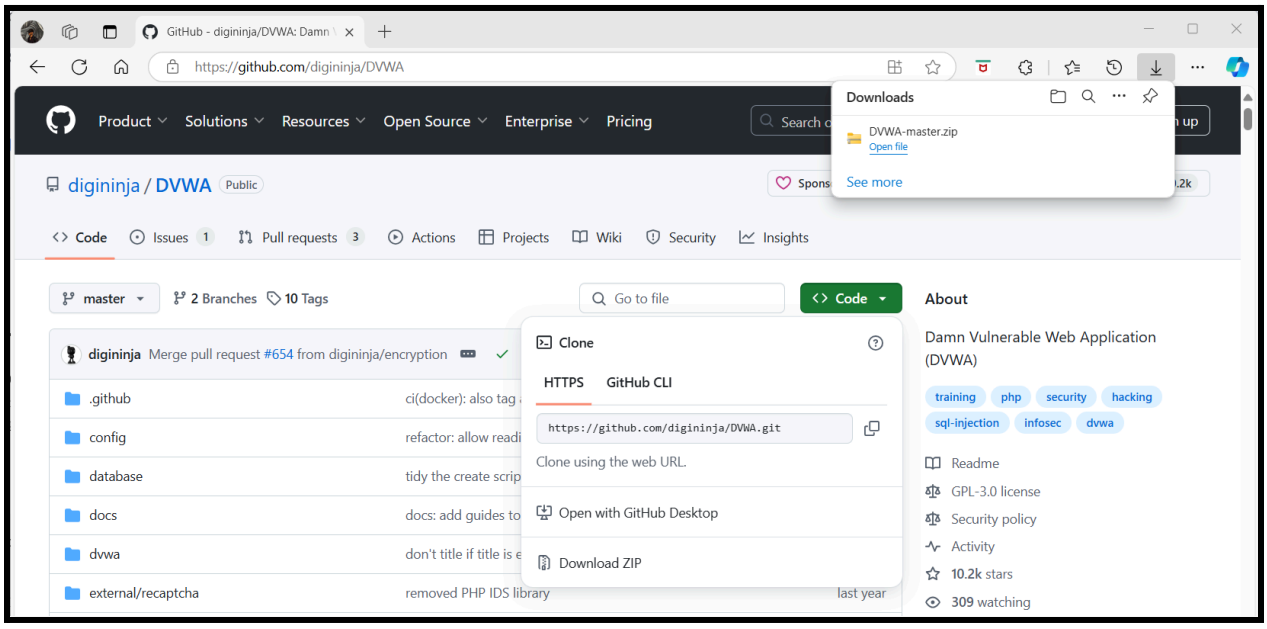

Administrator: XAMPP for Windows - mysql -u root
Setting environment for using XAMPP for Windows.
itsak@DESKTOP-J910NPG c:\xampp
mysql -u root
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 10.4.28-MariaDB mariadb.org binary distribution
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

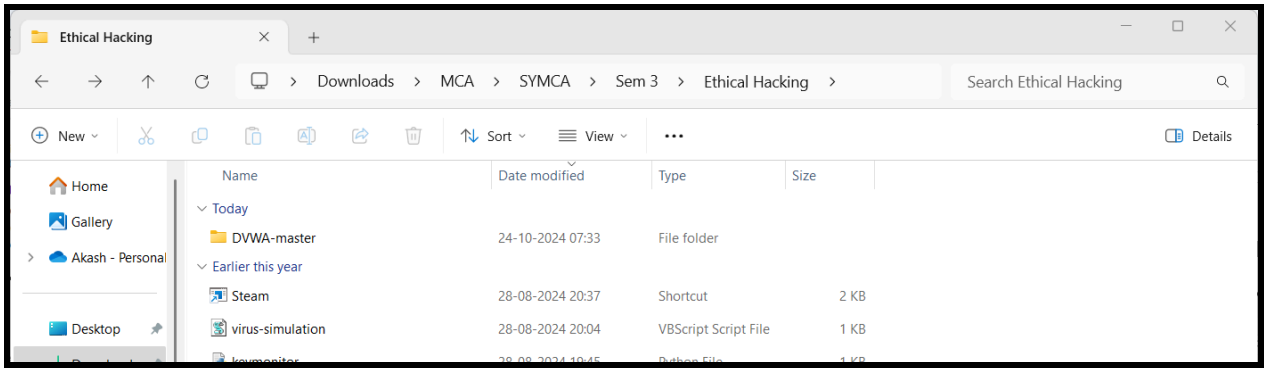

Administrator: XAMPP for Windows - mysql -u root
MariaDB [(none)]> show databases;
Database
data1
information_schema
mysql
performance_schema
phpmyadmin
result
student
test
visitor_counter
9 rows in set (0.007 sec)

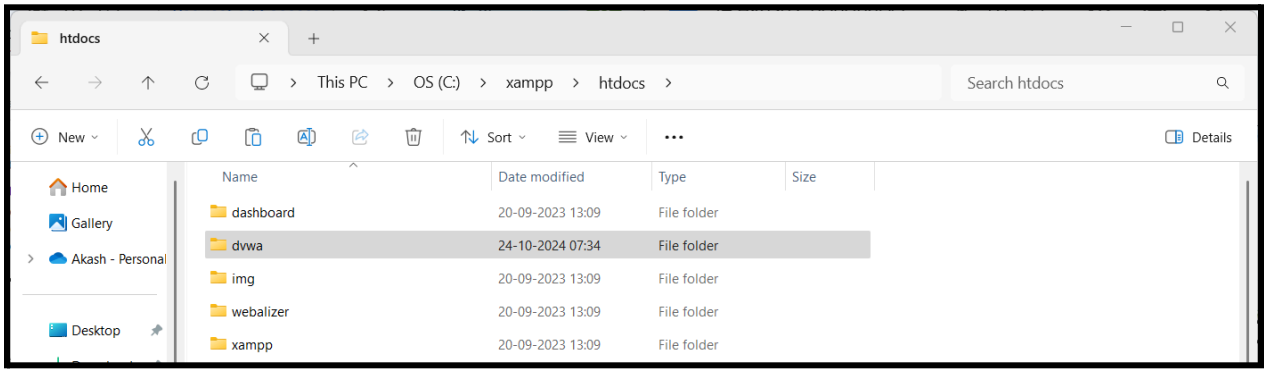

Administrator: XAMPP for Windows - mysql -u root
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.001 sec)

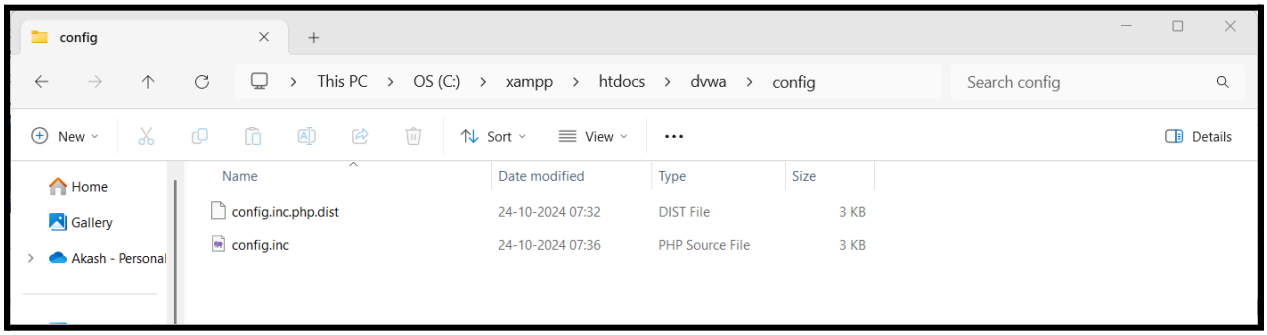

localhost / 127.0.0.1 / dvwa | ph
localhost/phpmyadmin/index.php?route=/database/structure&db=dvwa
phpMyAdmin
Recent Favorites
New
data1
dvwa
information_schema
mysql
performance_schema
phpmyadmin
result
student
Server: 127.0.0.1 » Database: dvwa
Structure SQL Search Query Export Import Operations Privileges Routines
No tables found in database.
Create new table
Table name
Number of columns
4
Create

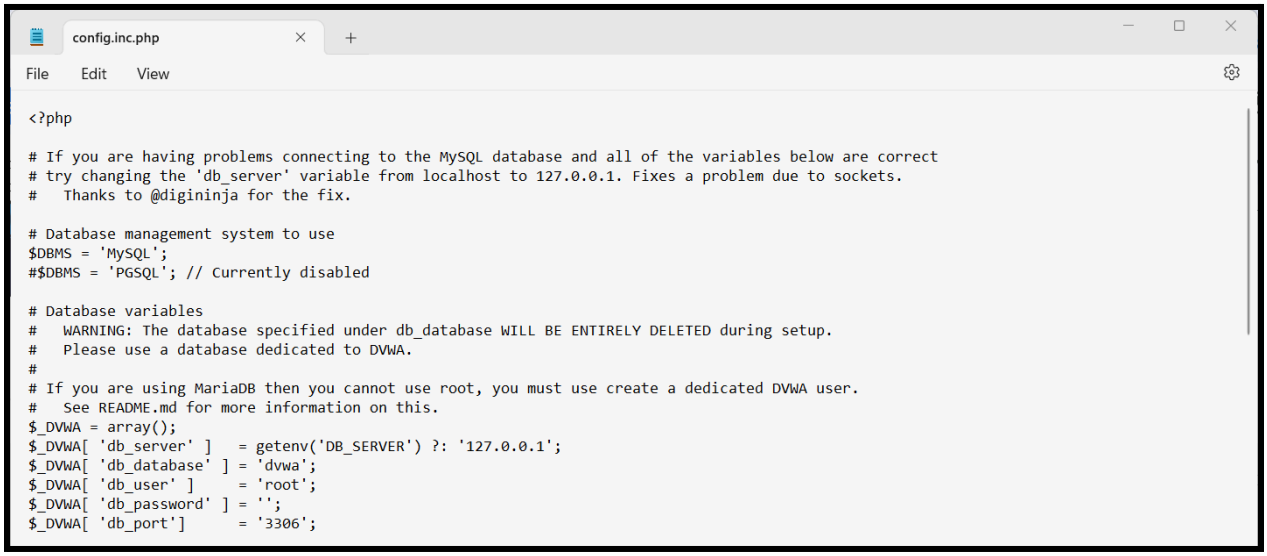

DVWA master zip - Google Searc
https://www.google.co.in/search?q=DVWA+master+zip&sca_esv=08df9a6e0ef724db&sxsrf=ADLYWIKVOgj0k6ant_bKuKXrOQE...
Google
DVWA master zip
All Videos Images News Shopping Web Maps More Tools
GitHub
https://github.com › digininja › DVWA
digininja/DVWA: Damn Vulnerable Web Application (DVWA)
The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface. Please ...
The prebuilt Docker images · Index.php · Releases 9 · Login.php

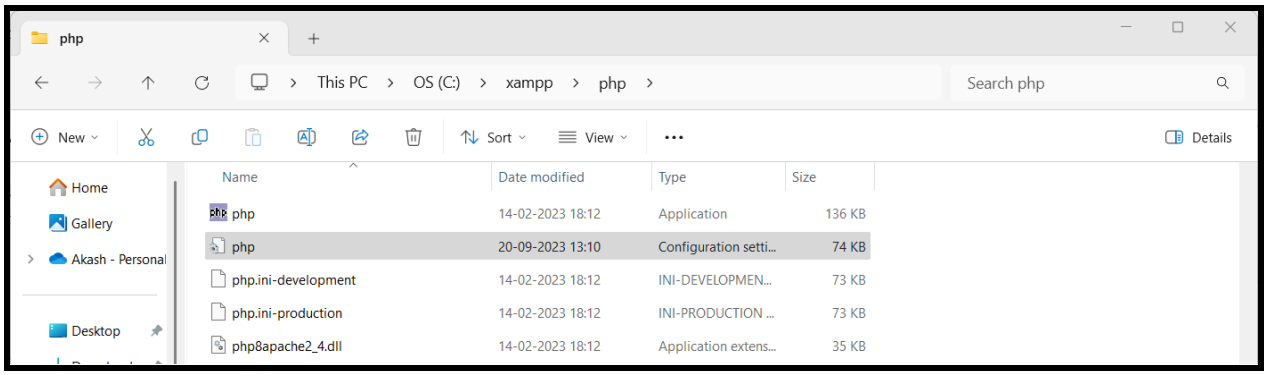

GitHub - digininja/DVWA: Damn
https://github.com/digininja/DVWA
Product Solutions Resources Open Source Enterprise Pricing
Downloads
DVWA-master.zip
Open file
See more
digininja / DVWA Public
Code Issues 1 Pull requests 3 Actions Projects Wiki Security Insights
master 2 Branches 10 Tags
Go to file
Code
About
Clone
HTTPS GitHub CLI
https://github.com/digininja/DVWA.git
Clone using the web URL.
Open with GitHub Desktop
Download ZIP
Damn Vulnerable Web Application (DVWA)
training php security hacking sql-injection infosec dvwa
Readme
GPL-3.0 license
Security policy
Activity
10.2k stars
309 watching
digininja Merge pull request #654 from digininja/encryption
.github
config
database
docs
dvwa
external/recaptcha
last year

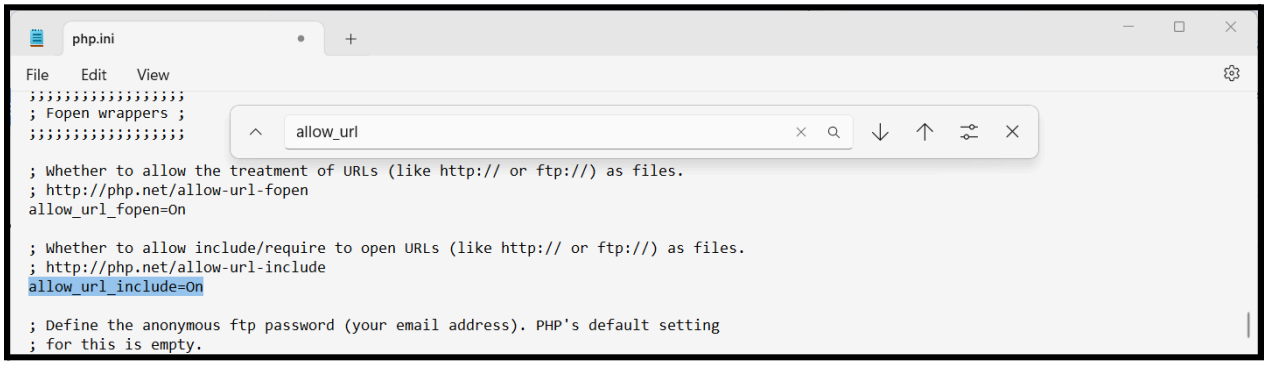

Ethical Hacking
Downloads › MCA › SYMCA › Sem 3 › Ethical Hacking ›
Search Ethical Hacking
New
Sort
View
Details
Home
Gallery
Akash - Personal
Desktop
Name
Date modified
Type
Size
Today
DVWA-master 24-10-2024 07:33 File folder
Earlier this year
Steam 28-08-2024 20:37 Shortcut 2 KB
virus-simulation 28-08-2024 20:04 VBScript Script File 1 KB

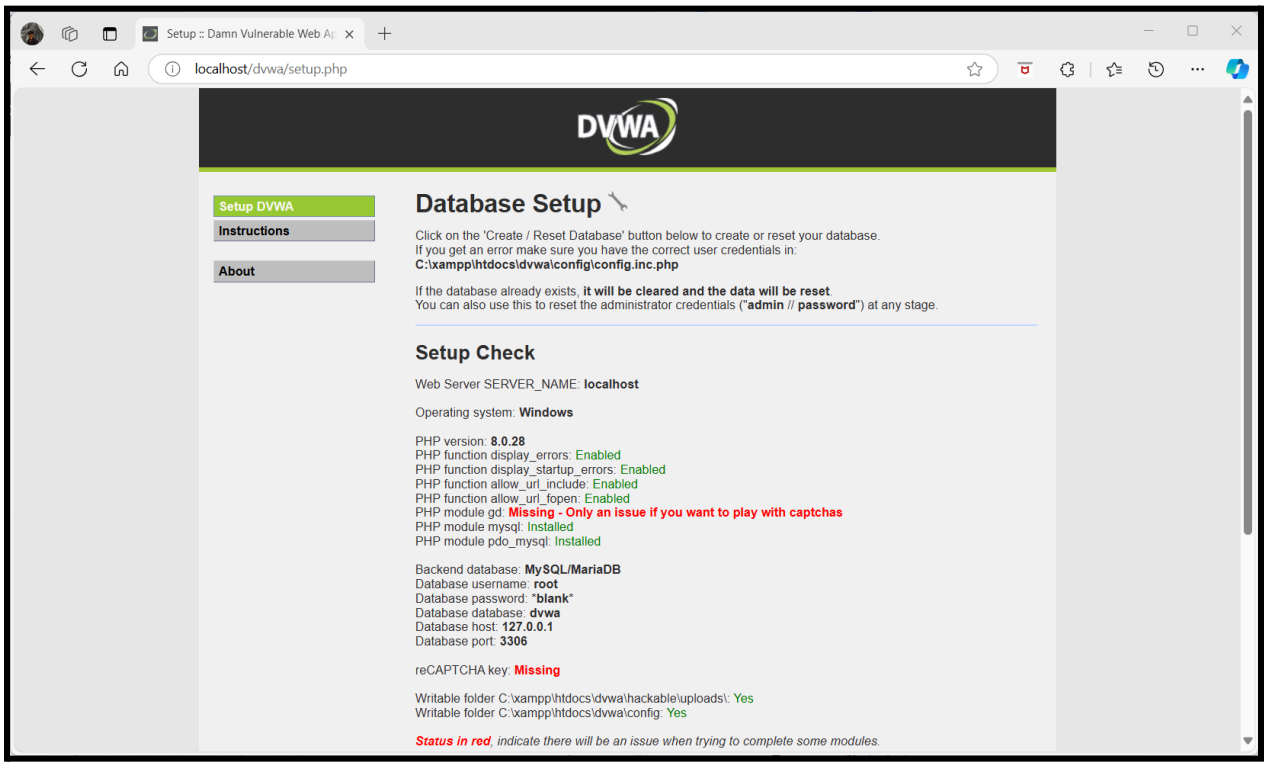

htdocs
This PC › OS (C:) › xampp › htdocs ›
Search htdocs
New
Sort
View
Details
Home
Gallery
Akash - Personal
Desktop
Name
Date modified
Type
Size
dashboard 20-09-2023 13:09 File folder
dvwa 24-10-2024 07:34 File folder
img 20-09-2023 13:09 File folder
webalizer 20-09-2023 13:09 File folder
xampp 20-09-2023 13:09 File folder

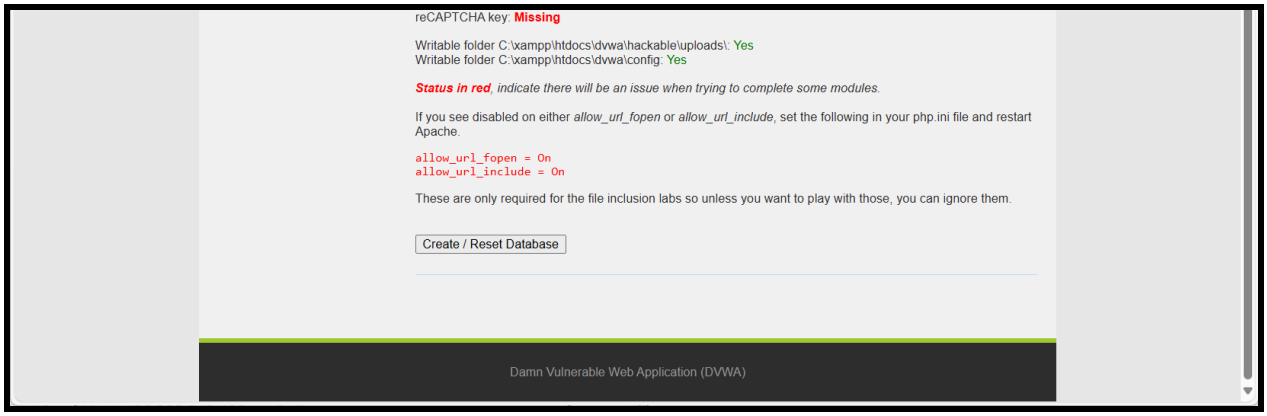

config
This PC › OS (C:) › xampp › htdocs › dvwa › config
Search config
New
Sort
View
Details
Home
Gallery
Akash - Personal
Name
Date modified
Type
Size
config.inc.php.dist 24-10-2024 07:32 DIST File 3 KB
config.inc 24-10-2024 07:36 PHP Source File 3 KB

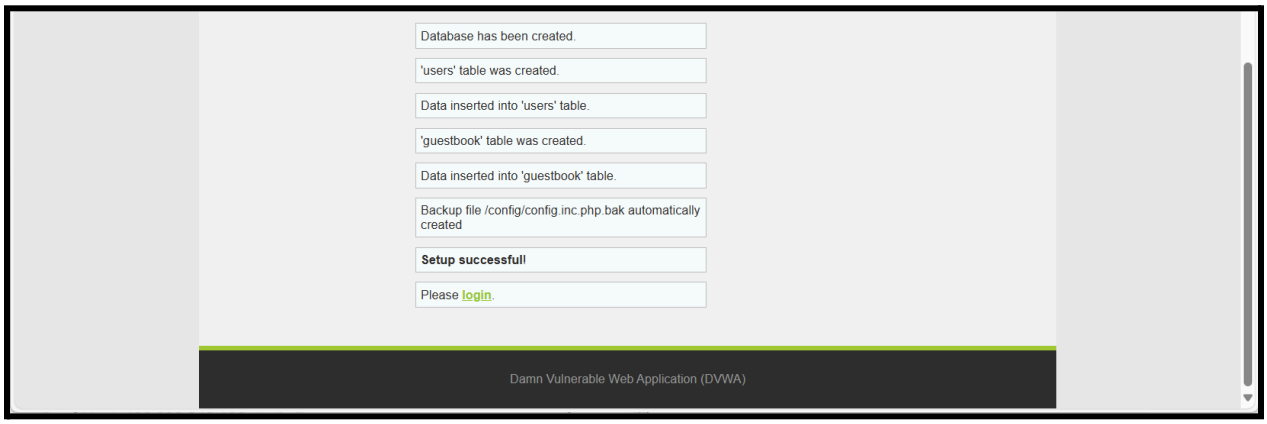

config.inc.php
File Edit View
<?php
If you are having problems connecting to the MySQL database and all of the variables below are correct
try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
Thanks to @digininja for the fix.
Database management system to 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'] = 'root';
$_DVWA['db_password'] = '';
$_DVWA['db_port'] = '3306';

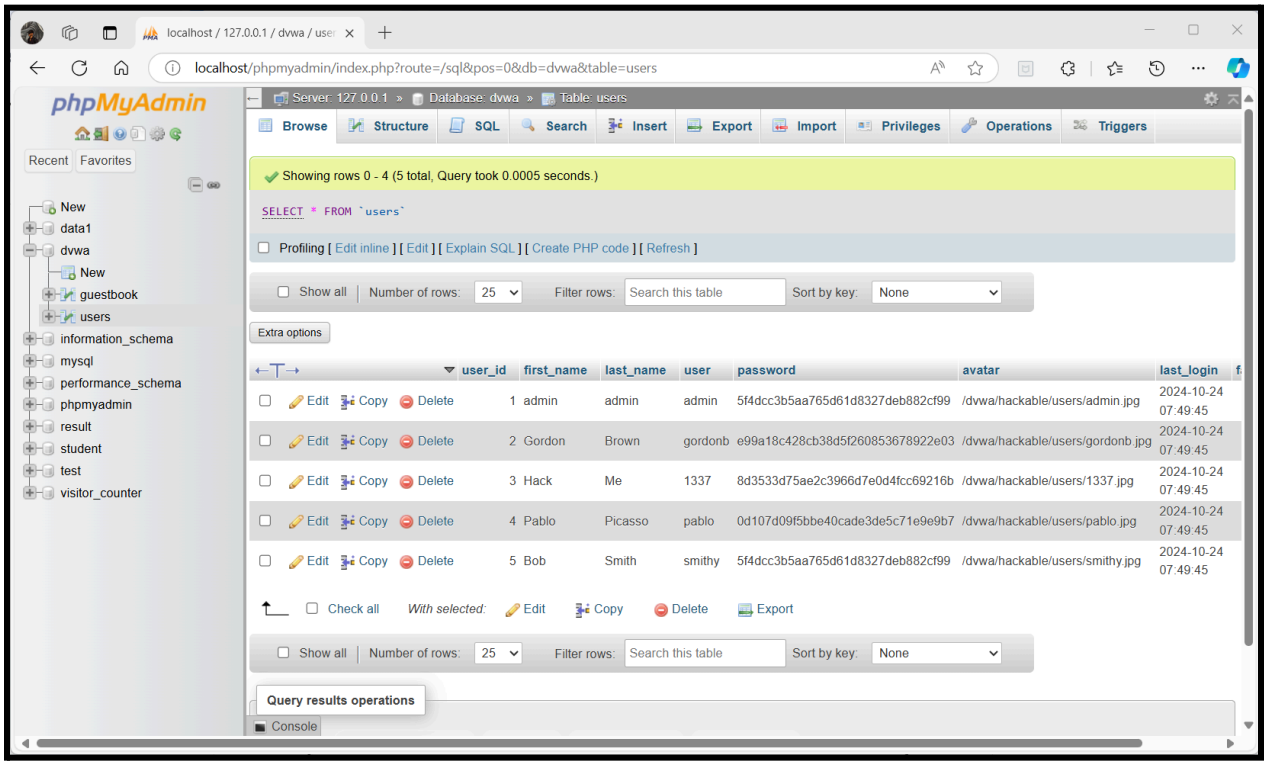

php
This PC
OS (C:)
xampp
php
Search php
New
Sort
View
Details
Home
Gallery
Akash - Personal
Desktop
Name
Date modified
Type
Size
php 14-02-2023 18:12 Application 136 KB
php 20-09-2023 13:10 Configuration setti... 74 KB
php.ini-development 14-02-2023 18:12 INI-DEVELOPMEN... 73 KB
php.ini-production 14-02-2023 18:12 INI-PRODUCTION ... 73 KB
php8apache2_4.dll 14-02-2023 18:12 Application extens... 35 KB

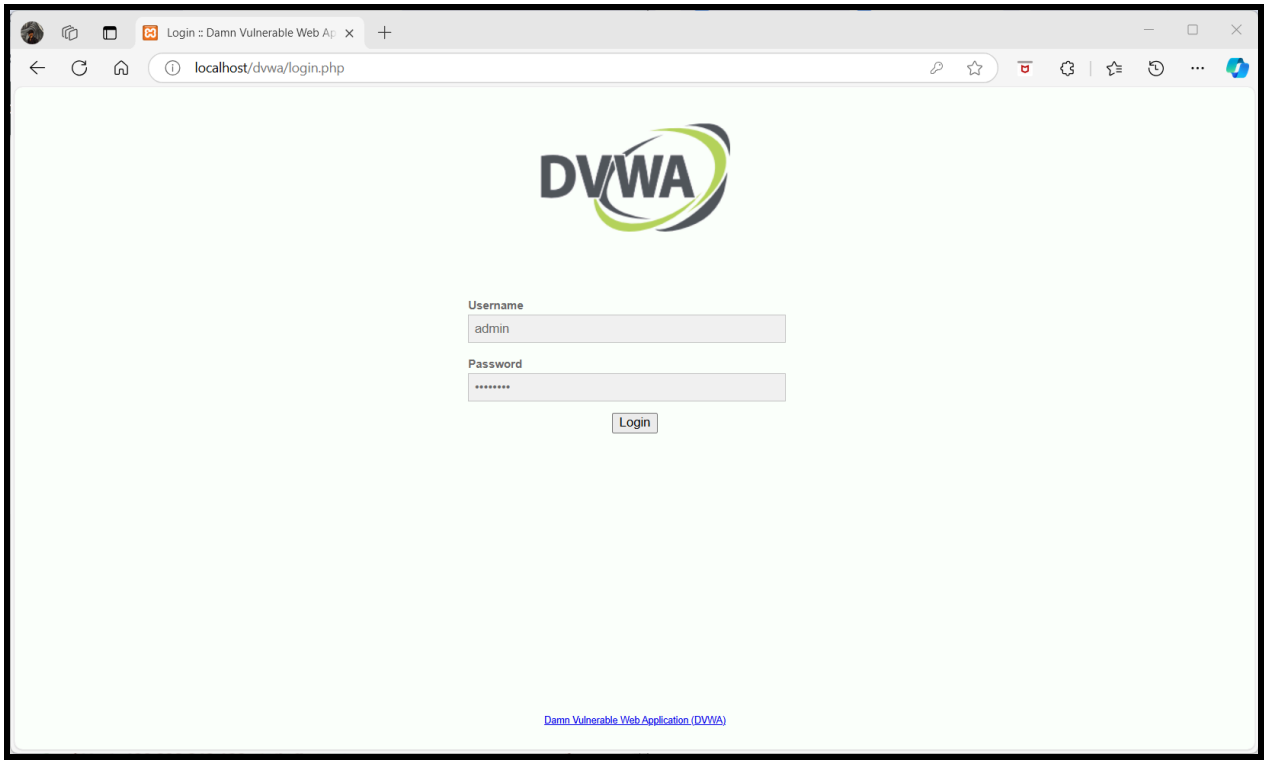

php.ini
File
Edit
View
allow_url
; Fopen wrappers ;
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen=On
; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include=On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

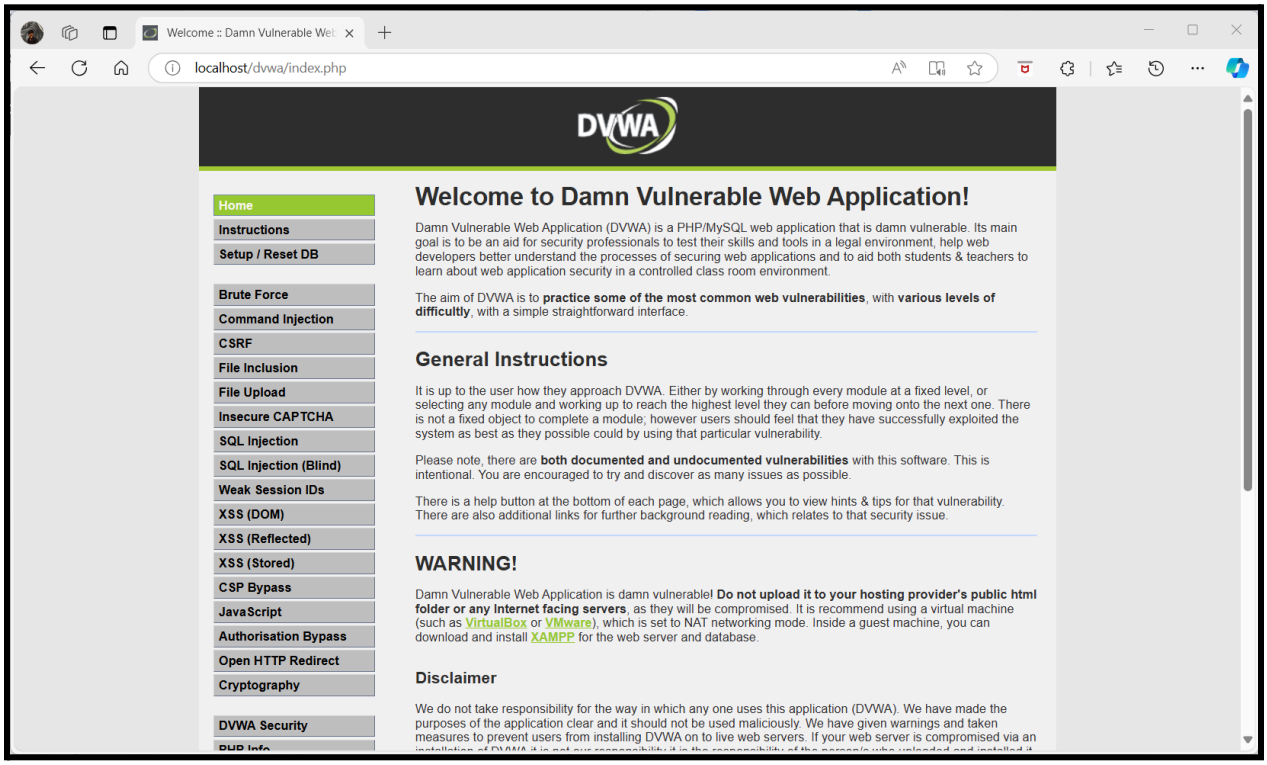

Setup :: Damn Vulnerable Web A
localhost/dvwa/setup.php
DVWA
Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in:
C:\xampp\htdocs\dvwa\config\config.inc.php
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: 8.0.28
PHP function display_errors: Enabled
PHP function display_startup_errors: Enabled
PHP function allow_url_include: Enabled
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: root
Database password: "blank"
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306
reCAPTCHA key: Missing
Writable folder C:\xampp\htdocs\dvwa\hackable\uploads\: Yes
Writable folder C:\xampp\htdocs\dvwa\config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.

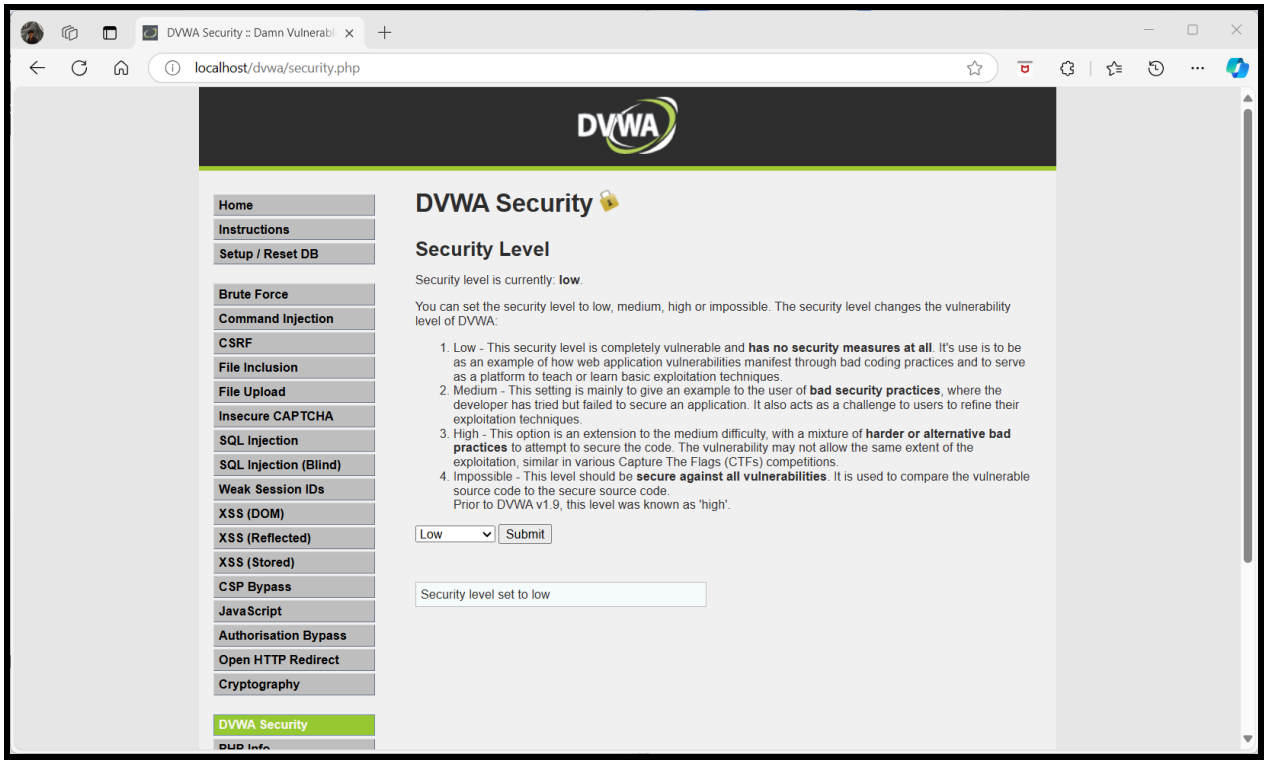

reCAPTCHA key: Missing
Writable folder C:\xampp\htdocs\dvwa\hackable\uploads\: Yes
Writable folder C:\xampp\htdocs\dvwa\config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
allow_url_fopen = On
allow_url_include = On
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.
Create / Reset Database
Damn Vulnerable Web Application (DVWA)

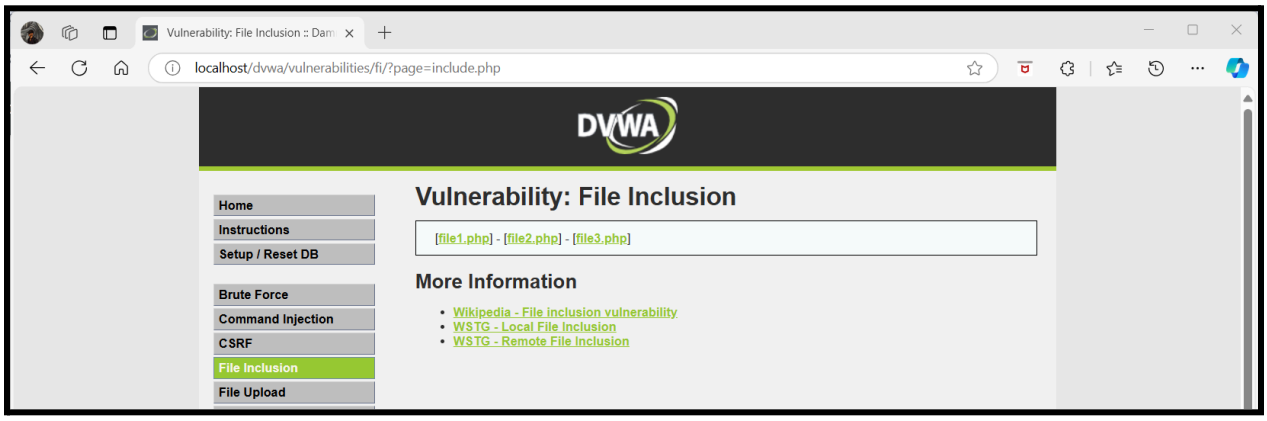

Database has been created.
'users' table was created.
Data inserted into 'users' table.
'guestbook' table was created.
Data inserted into 'guestbook' table.
Backup file /config/config.inc.php.bak automatically created
Setup successful!
Please login.
Damn Vulnerable Web Application (DVWA)

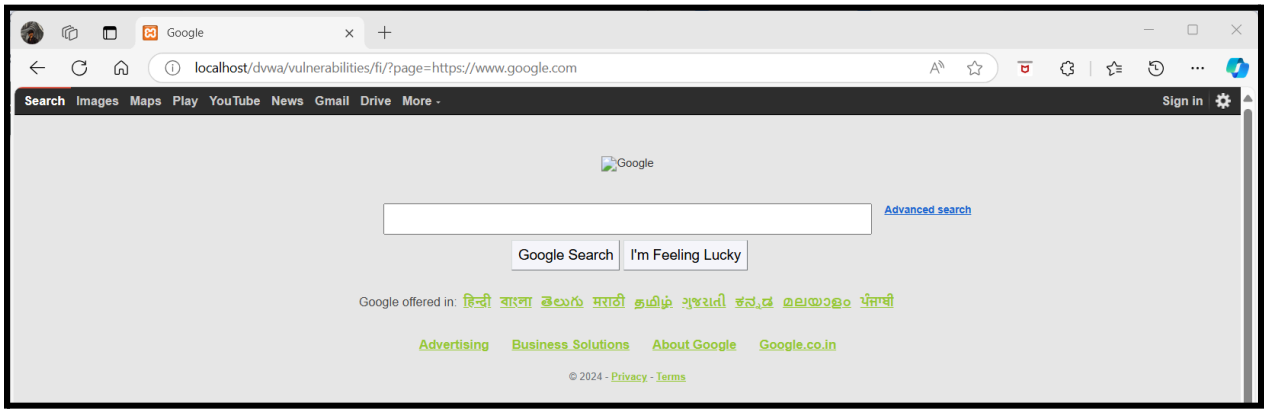

localhost/phpmyadmin/index.php?route=/sql&pos=0&db=dvwa&table=users
phpMyAdmin
Recent Favorites
New
data1
dvwa
New
guestbook
users
information_schema
mysql
performance_schema
phpmyadmin
result
student
test
visitor_counter
Server: 127.0.0.1 » Database: dvwa » Table: users
Browse Structure SQL Search Insert 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
Query results operations
Console

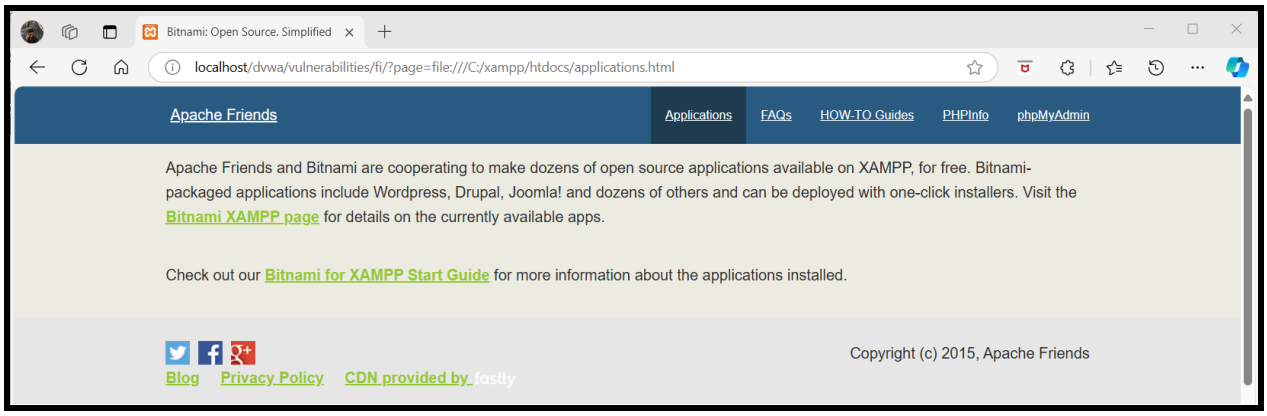

Login :: Damn Vulnerable Web Ap
localhost/dvwa/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)


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
Open HTTP Redirect
Cryptography
DVWA Security
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.
Disclaimer
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an


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
Cryptography
DVWA Security
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


Vulnerability: File Inclusion :: Dam
localhost/dvwa/vulnerabilities/fi/?page=include.php
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
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
Search Images Maps Play YouTube News Gmail Drive More
Sign in
Google
Advanced search
Google Search
I'm Feeling Lucky
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ
Advertising
Business Solutions
About Google
Google.co.in
© 2024 - Privacy - Terms


Bitnami: Open Source. Simplified
localhost/dvwa/vulnerabilities/fi/?page=file:///C:/xampp/htdocs/applications.html
Apache Friends
Applications
FAQs
HOW-TO Guides
PHPInfo
phpMyAdmin
Apache Friends and Bitnami are cooperating to make dozens of open source applications available on XAMPP, for free. Bitnami-packaged applications include Wordpress, Drupal, Joomla! and dozens of others and can be deployed with one-click installers. Visit the Bitnami XAMPP page for details on the currently available apps.
Check out our Bitnami for XAMPP Start Guide for more information about the applications installed.
Blog
Privacy Policy
CDN provided by fastly
Copyright (c) 2015, Apache Friends

2. Using Firefox to Disguise as a Google Bot to View Hidden Content on a Website

Aim: To understand how web applications can restrict access to certain content based on user-agent detection, and to demonstrate how changing the user agent in Firefox can bypass these restrictions to access hidden content

Theory:

Many websites serve different content to users based on their user agent, which identifies the browser, operating system, and device being used. For example, a website might display different pages or hide certain content from non-bot users to protect sensitive information or to manage content delivery.

By disguising as a Google bot (or another search engine bot), an ethical hacker can test the website's defenses against user-agent filtering and potentially access restricted content.

Key Concepts:

- User-Agent String: A line of text sent by a web browser to identify itself to the web server.
- User-Agent Spoofing: The practice of changing the user agent string to impersonate another browser or device.
- Search Engine Bots: Automated programs used by search engines to crawl and index web content.

Steps to be followed:

1. Determine the User Agent in Edge:
   - Open Edge and visit: http://www.proxyserverprivacy.com/
   - Select "Detector Proxy" and then "Advanced Proxy Detector."
2. Find the Googlebot User Agent String:
   - Visit: http://useragentstring.com/
   - Locate the string for Googlebot:
     Googlebot/2.1 (+http://www.googlebot.com/bot.html)
3. Configure Edge User Agent:
   - Open Developer Tools:
     - Press F12 or right-click on any webpage and select Inspect.

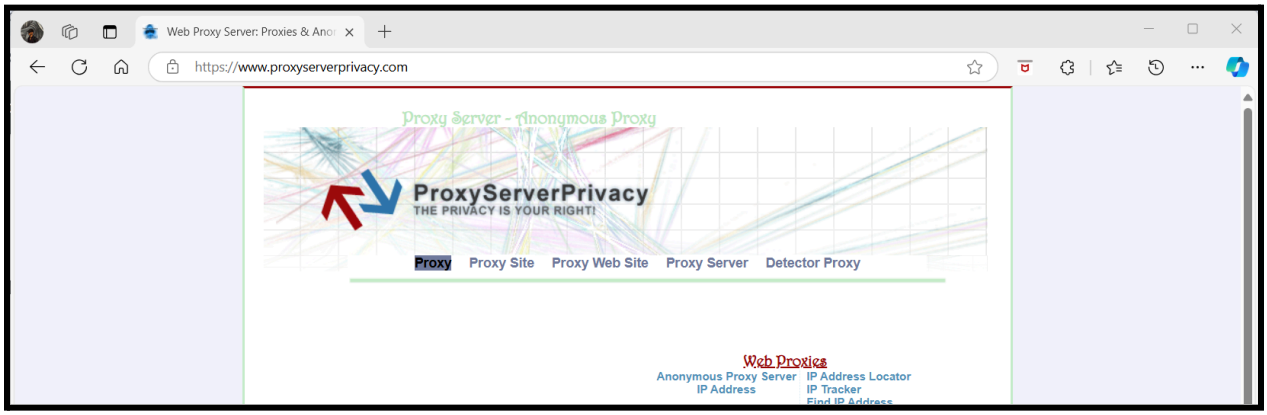
- Navigate to the "Network Conditions":
    - Click on the three dots (More options) in the Developer Tools window.
    - Select More tools > Network conditions.
- Change the User Agent:
    - Uncheck Use browser default under User agent.
    - Enter the following string to emulate Googlebot:

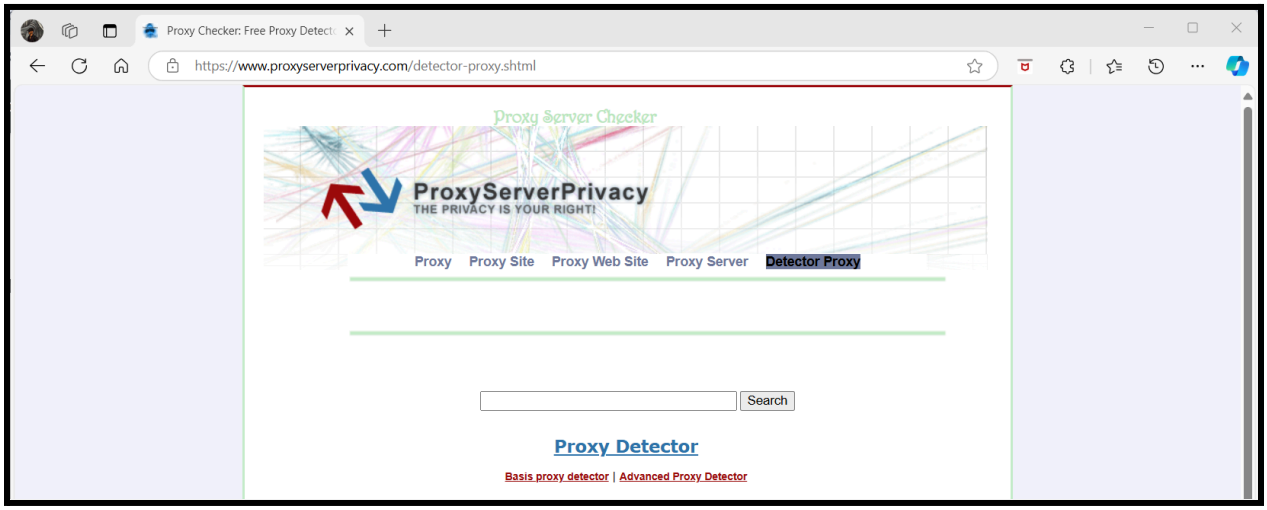
      Googlebot/2.1 (+http://www.googlebot.com/bot.html)

4. Verify the Change:

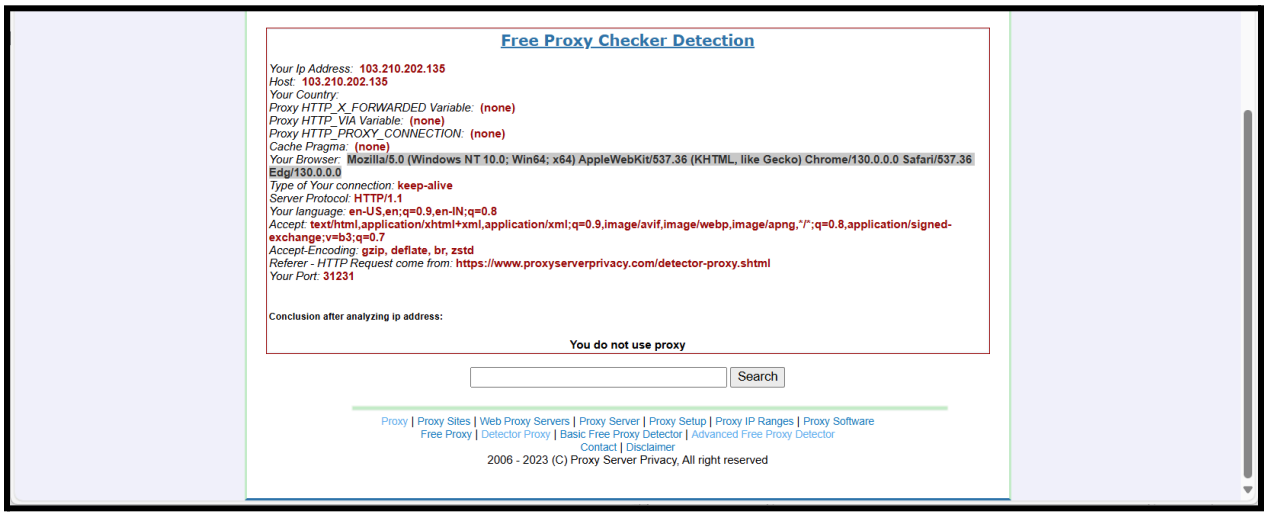
- To verify the user agent change, visit:

Output:

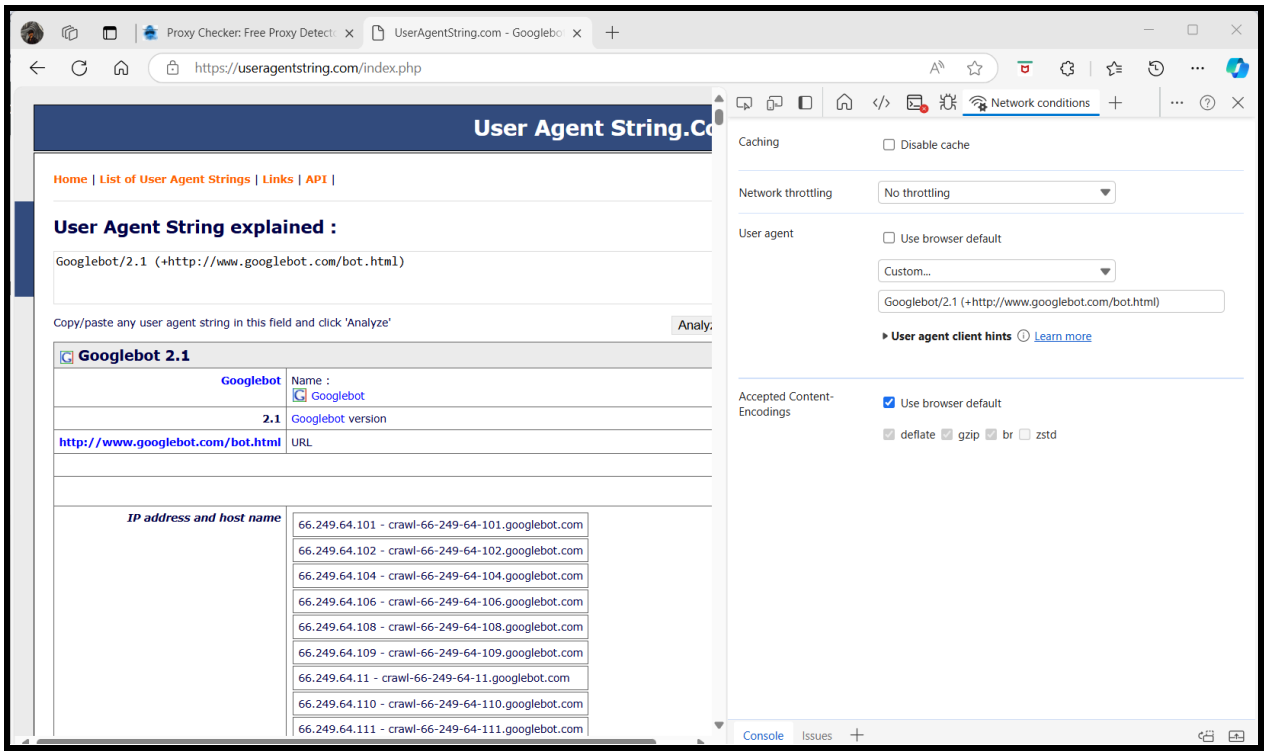


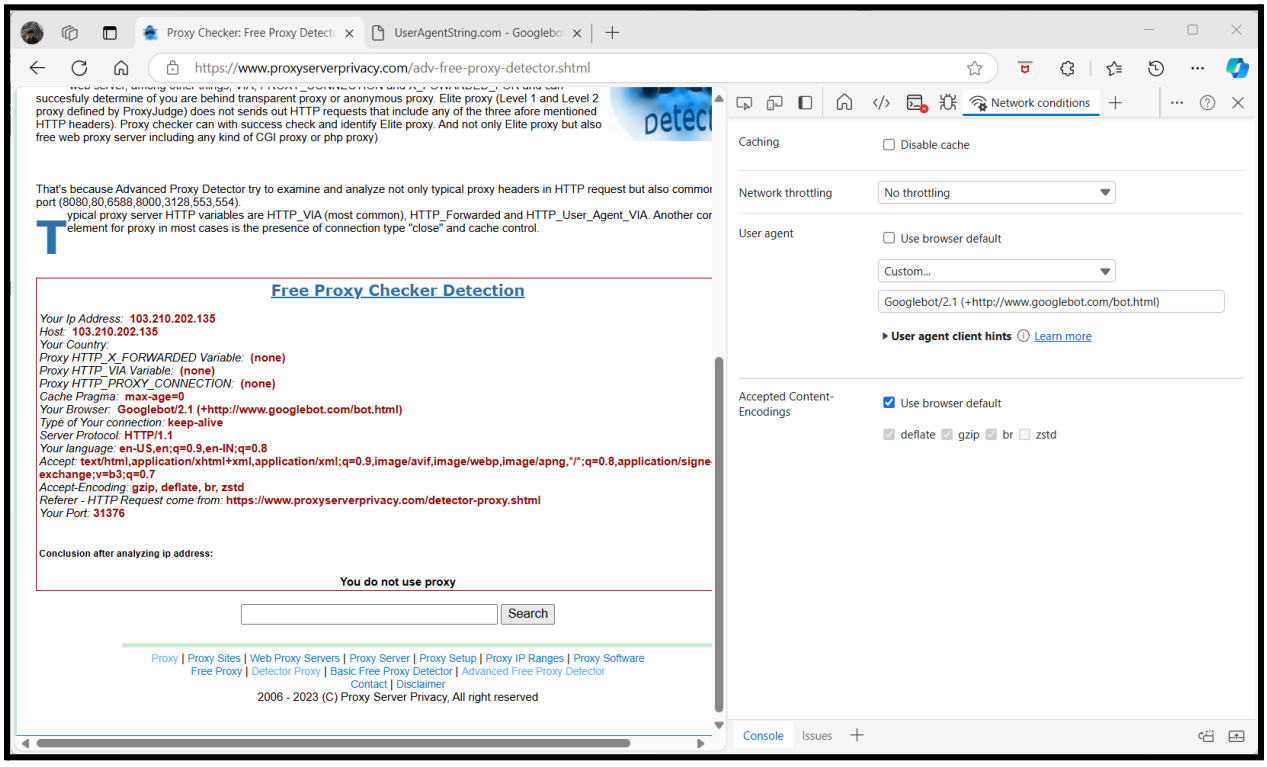



Proxy Checker: Free Proxy Detect
https://www.proxyserverprivacy.com/adv-free-proxy-detector.shtml
Proxy Server Checker
ProxyServerPrivacy
THE PRIVACY IS YOUR RIGHT!
Proxy Proxy Site Proxy Web Site Proxy Server Detector Proxy
Proxy Checker - Advanced Free Proxy Detector
Basis free proxy detector | Advanced 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
That's because Advanced Proxy Detector try to examine and analyze not only typical proxy headers in HTTP request but also common proxy 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 common 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: (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
Proxy | Proxy Sites | Web Proxy Servers | Proxy Server | Proxy Setup | Proxy IP Ranges | Proxy Software
Free Proxy | Detector Proxy | Basic Free Proxy Detector | Advanced Free Proxy Detector
Contact | Disclaimer
2006 - 2023 (C) Proxy Server Privacy, All right reserved


Proxy Checker: Free Proxy Detect
UserAgentString.com - Chrome
https://useragentstring.com
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


Proxy Checker: Free Proxy Detect
UserAgentString.com - Googlebo
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
66.249.64.11 - crawl-66-249-64-11.googlebot.com
66.249.64.110 - crawl-66-249-64-110.googlebot.com
66.249.64.111 - crawl-66-249-64-111.googlebot.com
Network conditions
Caching
Disable cache
Network throttling
No throttling
User agent
Use browser default
Custom...
Googlebot/2.1 (+http://www.googlebot.com/bot.html)
User agent client hints
Learn more
Accepted Content-Encodings
Use browser default
deflate gzip br zstd
Console
Issues


Proxy Checker: Free Proxy Detect
UserAgentString.com - Googlebo
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).
Typical 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
Proxy | Proxy Sites | Web Proxy Servers | Proxy Server | Proxy Setup | Proxy IP Ranges | Proxy Software
Free Proxy | Detector Proxy | Basic Free Proxy Detector | Advanced Free Proxy Detector
Contact | Disclaimer
2006 - 2023 (C) Proxy Server Privacy, All right reserved
Network conditions
Caching
Disable cache
Network throttling
No throttling
User agent
Use browser default
Custom...
Googlebot/2.1 (+http://www.googlebot.com/bot.html)
User agent client hints
Learn more
Accepted Content-Encodings
Use browser default
deflate gzip br zstd
Console
Issues

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

Aim: To investigate the security vulnerabilities in antivirus software like Kaspersky or Quick Heal that can be exploited to bypass licensing mechanisms and to understand the ethical implications of such actions

Theory:

Antivirus software is designed to protect computers from malware and other security threats. However, many users seek ways to use these programs for free or for an extended period beyond their intended licensing. This often involves finding vulnerabilities or exploiting loopholes in the software's licensing system.

Key Concepts:

- Licensing Mechanisms: Systems used by software vendors to control the usage and distribution of their products.
- Patching: The process of applying updates to software to fix vulnerabilities or improve functionality.
- Ethical Implications: Using pirated or patched software can lead to legal consequences and undermine the trust in software developers.

Example of Exploitation: This could involve modifying software files, using key generators, or employing techniques to disable licensing checks.

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:

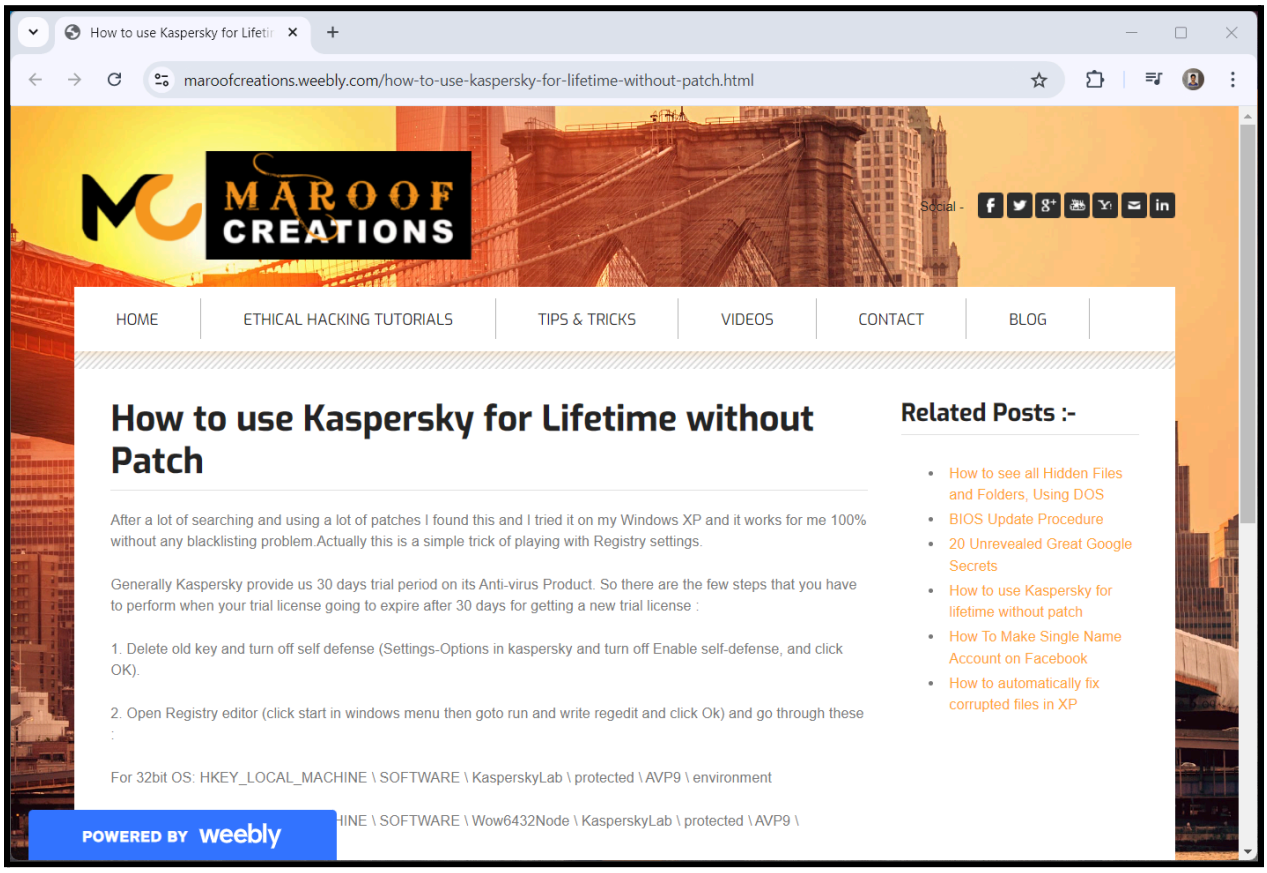
- Right-click the Kaspersky icon in the taskbar and select Exit.
- Reopen Kaspersky and activate the search for a trial license. You should receive a new 30-day trial.

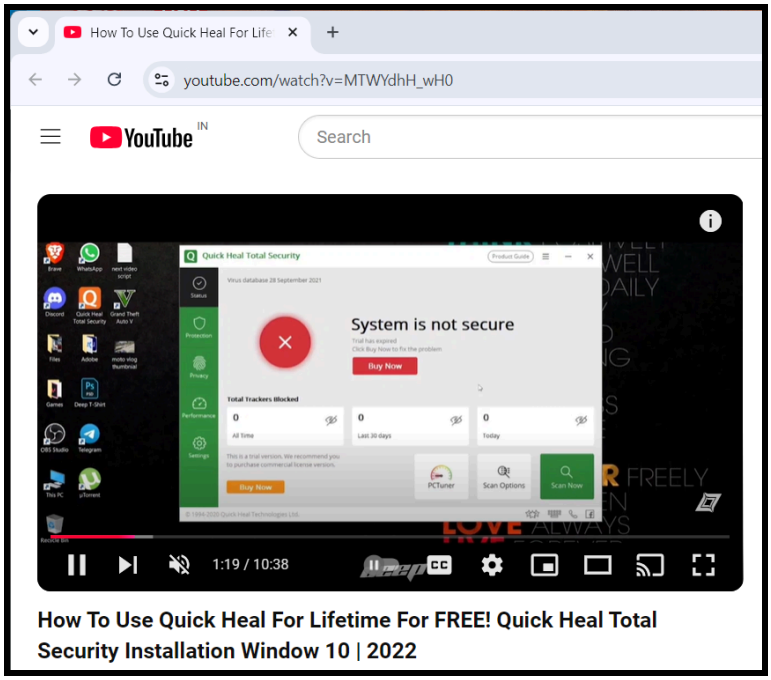
4. Re-enable Self-Defense:

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