Project Documentation: Extracting Credentials Using Burp Suite & DVWA

Introduction

This document outlines the process of capturing login credentials on **DVWA** using **Burp Suite** in a controlled penetration testing environment. The objective is to understand how insecure authentication mechanisms work and how to mitigate such vulnerabilities.

Project Details

Project Title: Credential Extraction via Burp Suite
Date: February 2025

Phase 1: Setup

Required Tools

- **VirtualBox** → https://www.virtualbox.org/
- **Kali Linux** → https://www.kali.org/get-kali/#kali-platforms
- **DVWA (Damn Vulnerable Web App)** → https://github.com/digininja/DVWA (Refer to the video guide for proper setup)
- **Apache & MariaDB** (for hosting DVWA locally)
- **Burp Suite** → https://portswigger.net/burp/documentation/desktop/getting-started/download-and-install

Installation Guide

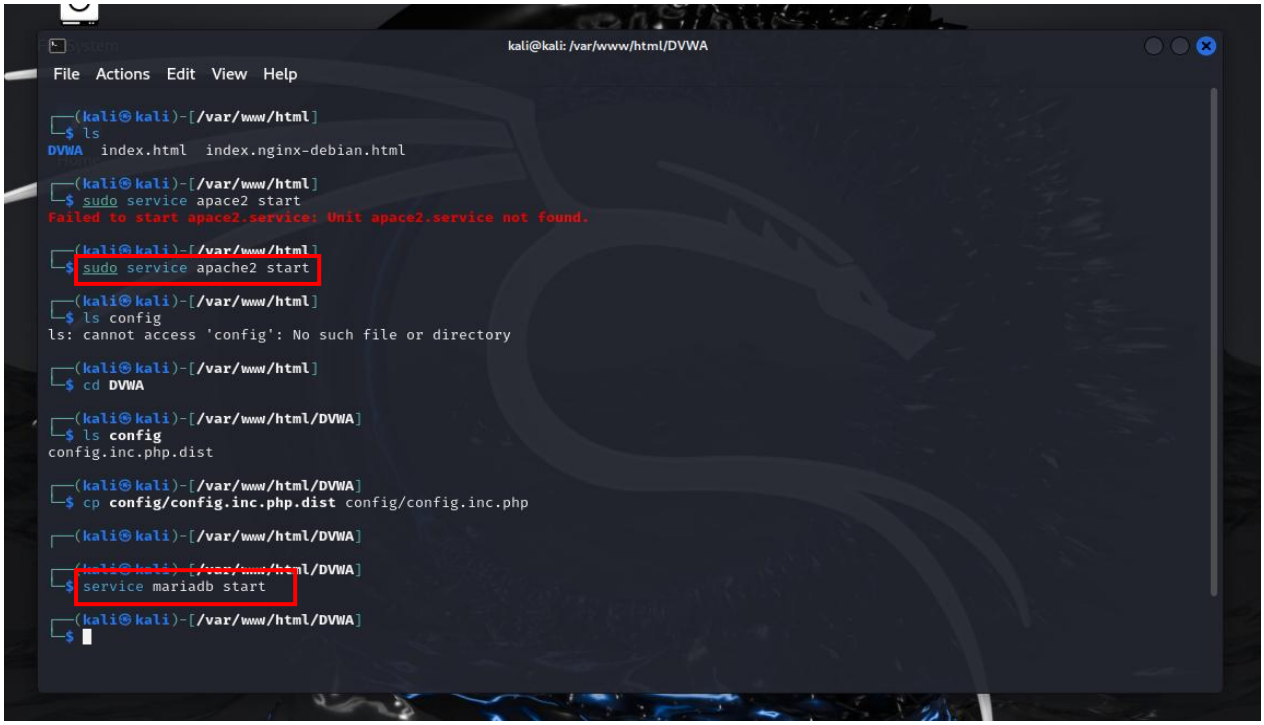
1. Install **VirtualBox** and set up **Kali Linux**.
2. Configure **Apache & MariaDB** using the following commands:

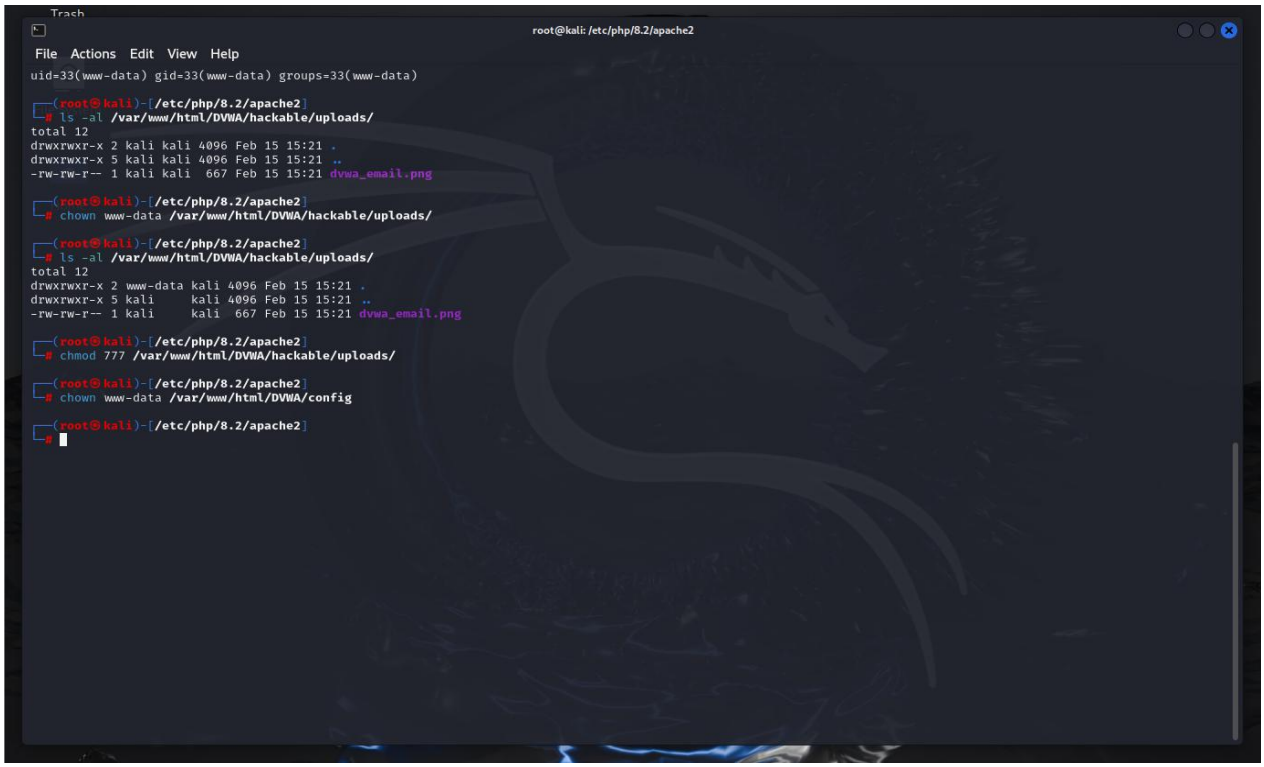
3. sudo service apache2 start
4. sudo service mariadb start
5. Download and configure **DVWA**:
    - Open http://localhost/DVWA in a browser. (case sensitive)
    - Complete the database setup by referring to the video resources provided below.
6. Install and configure **Burp Suite** for intercepting requests.

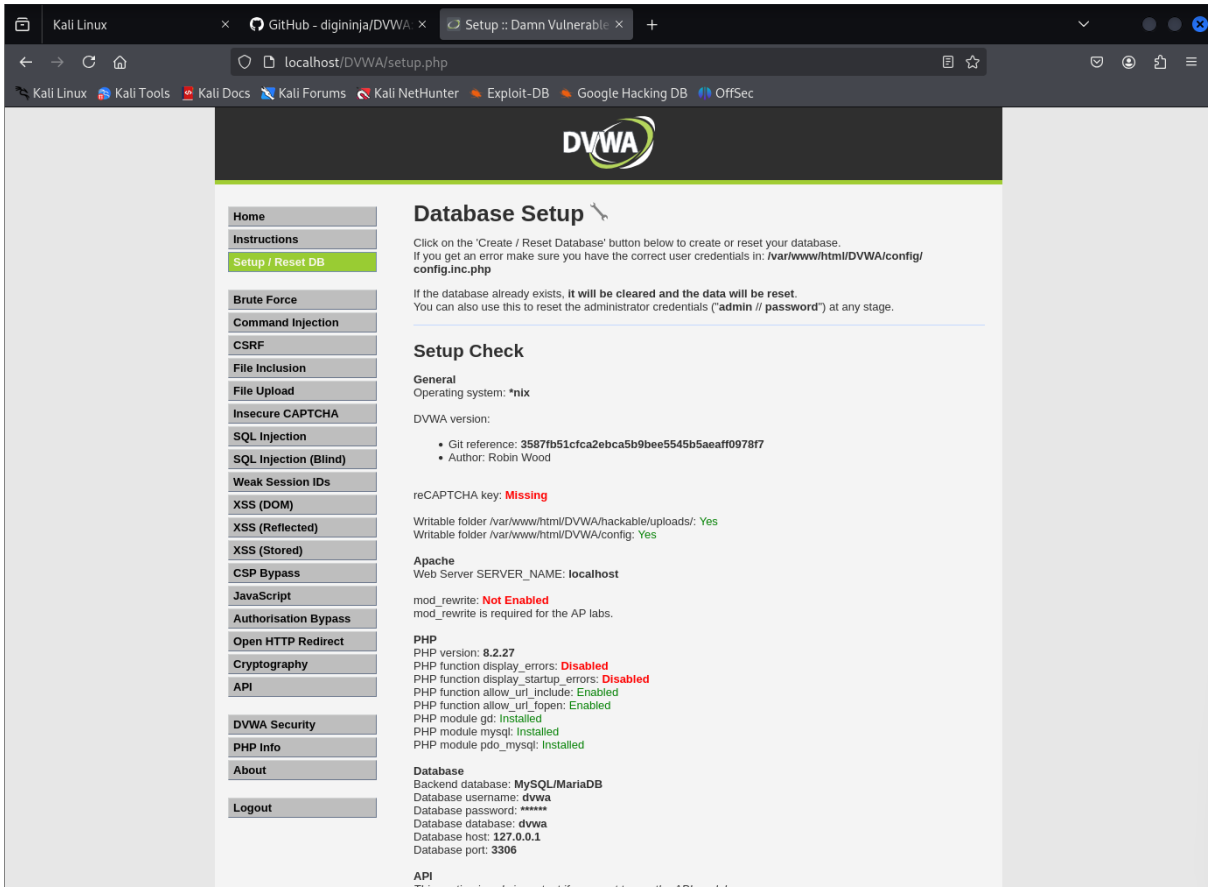
Video Resources:

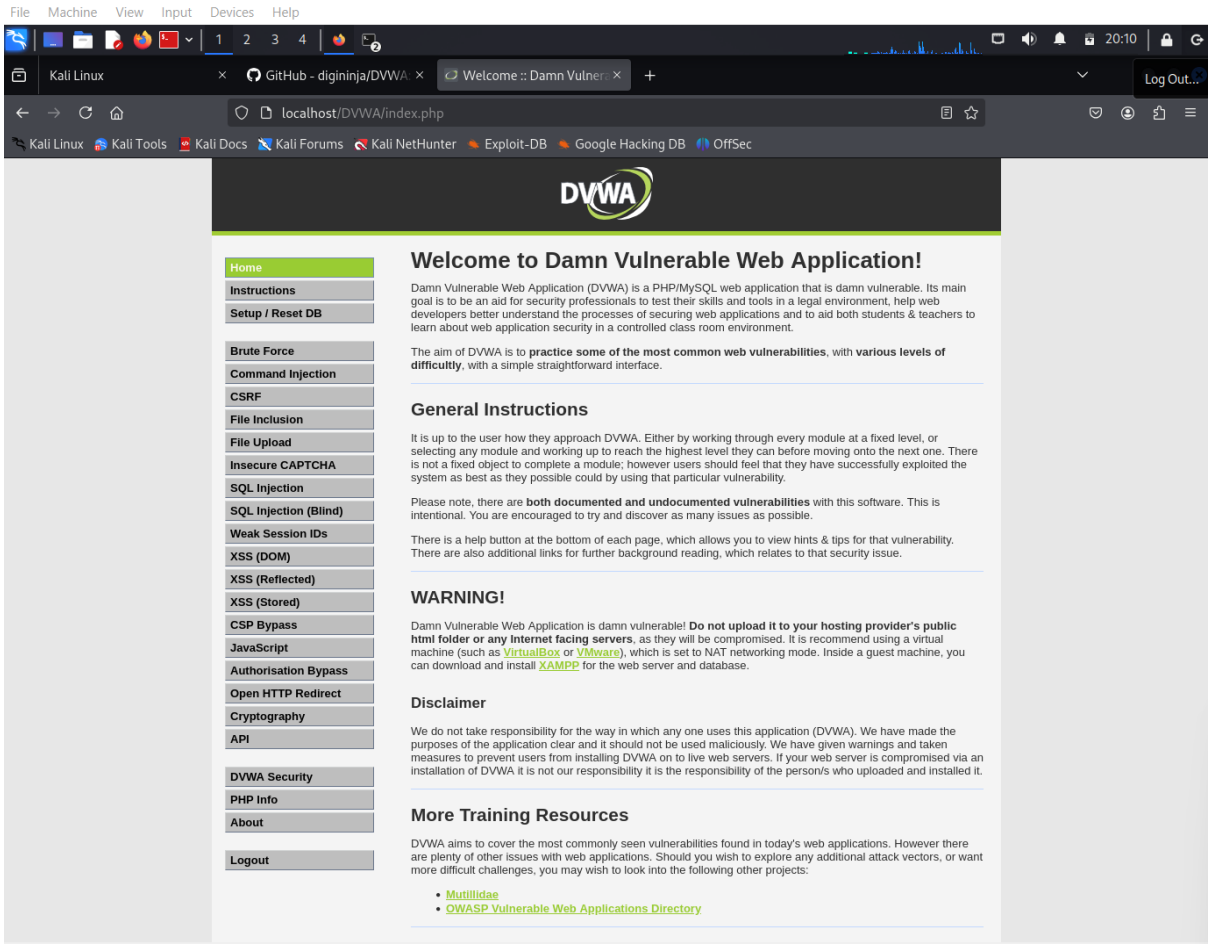
- Virtual Box & Kali Linux Setup
- DVWA Setup
- Burp Suite Setup

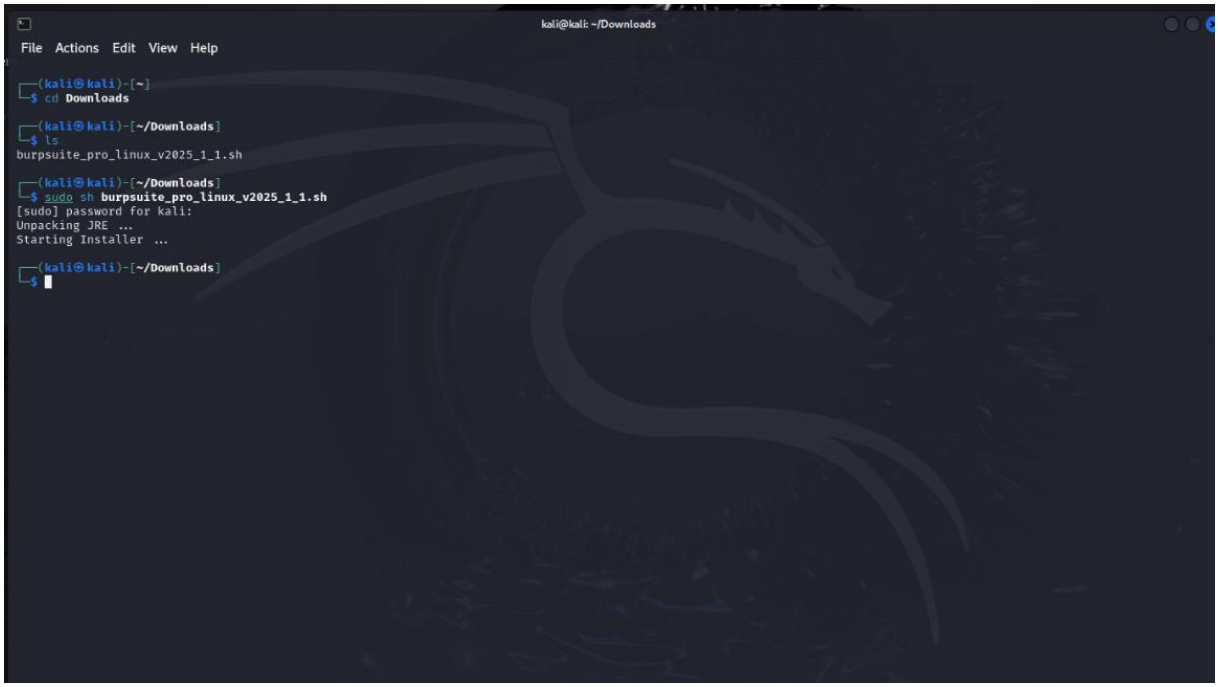
Screenshots:

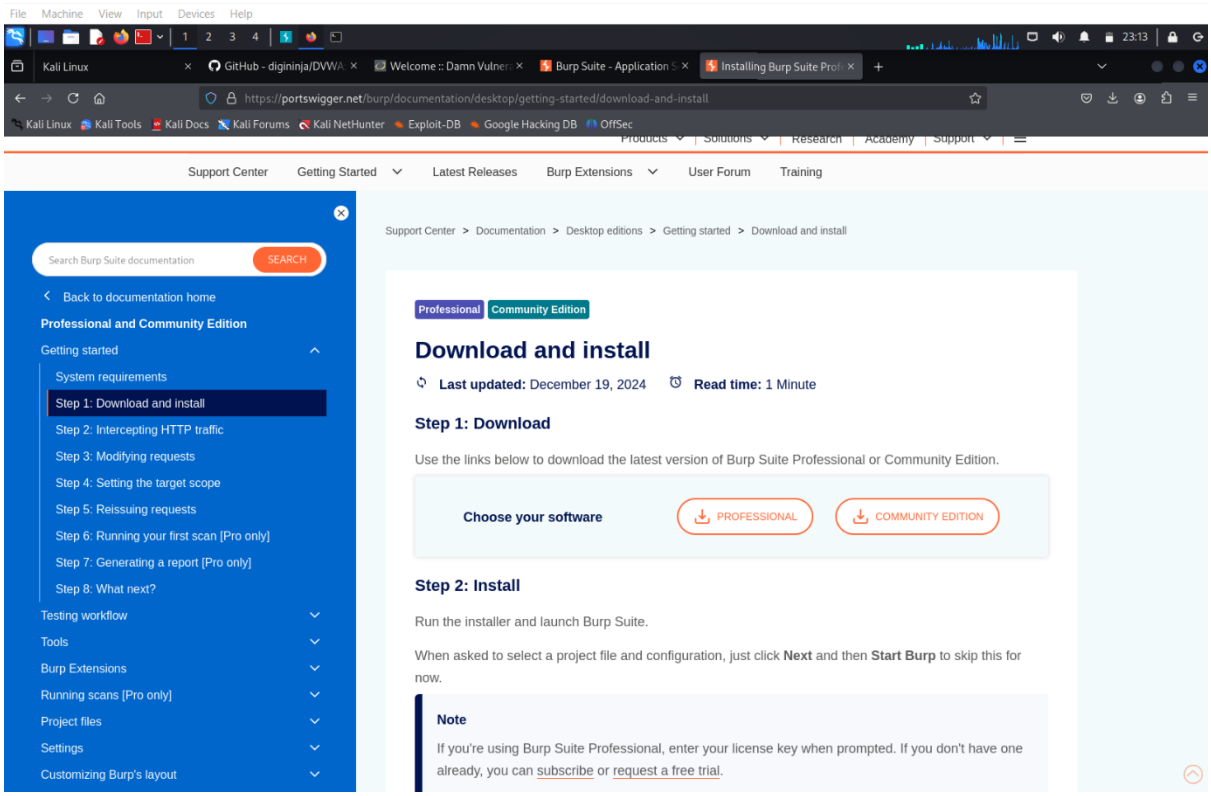

kali@kali: /var/www/html/DVWA
File Actions Edit View Help
┌──(kali㉿kali)-[/var/www/html]
└─$ ls
DVWA index.html index.nginx-debian.html
┌──(kali㉿kali)-[/var/www/html]
└─$ sudo service apace2 start
Failed to start apace2.service: Unit apace2.service not found.
┌──(kali㉿kali)-[/var/www/html]
└─$ sudo service apache2 start
┌──(kali㉿kali)-[/var/www/html]
└─$ ls config
ls: cannot access 'config': No such file or directory
┌──(kali㉿kali)-[/var/www/html]
└─$ cd DVWA
┌──(kali㉿kali)-[/var/www/html/DVWA]
└─$ ls config
config.inc.php.dist
┌──(kali㉿kali)-[/var/www/html/DVWA]
└─$ cp config/config.inc.php.dist config/config.inc.php
┌──(kali㉿kali)-[/var/www/html/DVWA]
┌──(kali㉿kali)-[/var/www/html/DVWA]
└─$ service mariadb start
┌──(kali㉿kali)-[/var/www/html/DVWA]
└─$

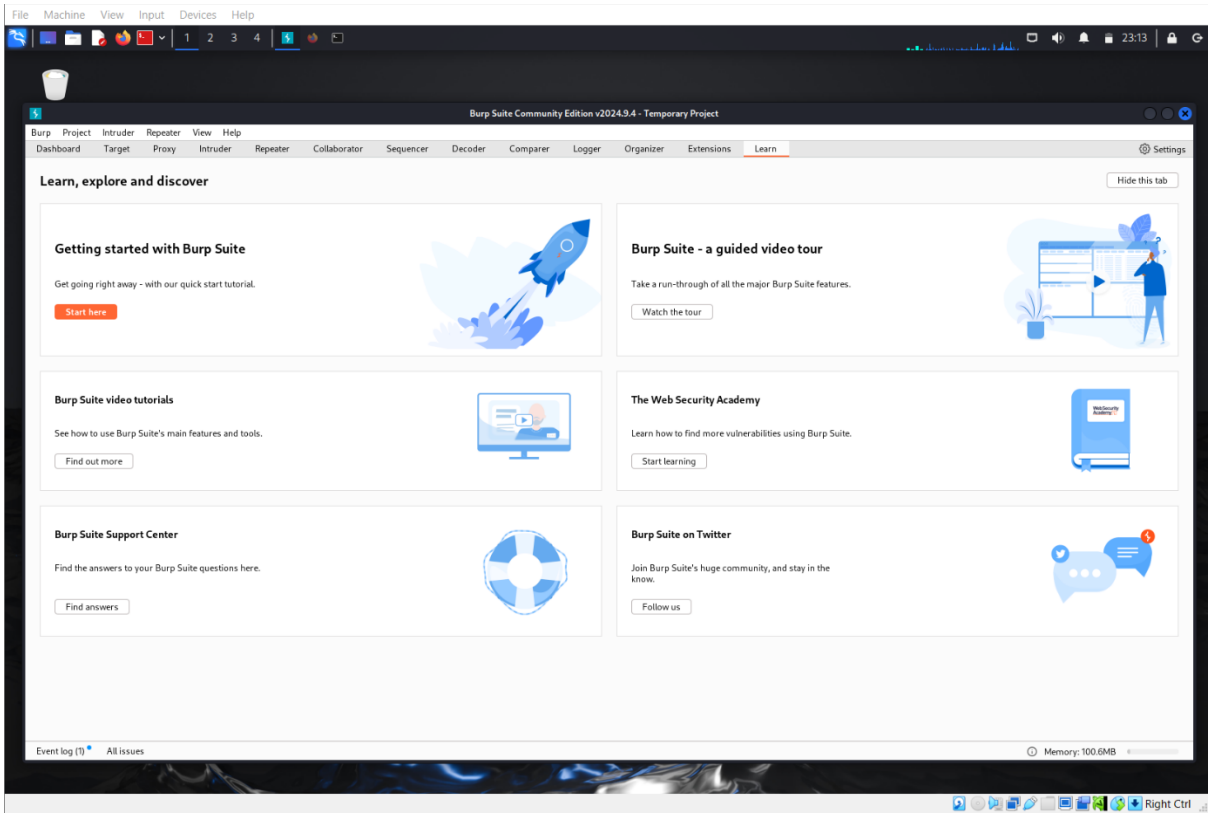

root@kali: /etc/php/8.2/apache2
File Actions Edit View Help
uid=33(www-data) gid=33(www-data) groups=33(www-data)
┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# ls -al /var/www/html/DVWA/hackable/uploads/
total 12
drwxrwxr-x 2 kali kali 4096 Feb 15 15:21 .
drwxrwxr-x 5 kali kali 4096 Feb 15 15:21 ..
-rw-rw-r-- 1 kali kali 667 Feb 15 15:21 dvwa_email.png
┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# chown www-data /var/www/html/DVWA/hackable/uploads/
┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# ls -al /var/www/html/DVWA/hackable/uploads/
total 12
drwxrwxr-x 2 www-data kali 4096 Feb 15 15:21 .
drwxrwxr-x 5 kali   kali 4096 Feb 15 15:21 ..
-rw-rw-r-- 1 kali   kali 667 Feb 15 15:21 dvwa_email.png
┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# chmod 777 /var/www/html/DVWA/hackable/uploads/
┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# chown www-data /var/www/html/DVWA/config
┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─#


Kali Linux
GitHub - digininja/DVWA
Setup :: Damn Vulnerable
localhost/DVWA/setup.php
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
API
DVWA Security
PHP Info
About
Logout
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: /var/www/html/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
General
Operating system: *nix
DVWA version:
Git reference: 3587fb51cfca2ebca5b9bee5545b5aeaff0978f7
Author: Robin Wood
reCAPTCHA key: Missing
Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
Writable folder /var/www/html/DVWA/config: Yes
Apache
Web Server SERVER_NAME: localhost
mod_rewrite: Not Enabled
mod_rewrite is required for the AP labs.
PHP
PHP version: 8.2.27
PHP function display_errors: Disabled
PHP function display_startup_errors: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed
Database
Backend database: MySQL/MariaDB
Database username: dvwa
Database password: ******
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306
API


File Machine View Input Devices Help
1 2 3 4
20:10
Kali Linux
GitHub - digininja/DVWA
Welcome :: Damn Vulner
Log Out...
localhost/DVWA/index.php
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
API
DVWA Security
PHP Info
About
Logout
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 installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
More Training Resources
DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:
Mutillidae
OWASP Vulnerable Web Applications Directory


kali@kali: ~/Downloads
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd Downloads
(kali㉿kali)-[~/Downloads]
$ ls
burpsuite_pro_linux_v2025_1_1.sh
(kali㉿kali)-[~/Downloads]
$ sudo sh burpsuite_pro_linux_v2025_1_1.sh
[sudo] password for kali:
Unpacking JRE ...
Starting Installer ...
(kali㉿kali)-[~/Downloads]
$

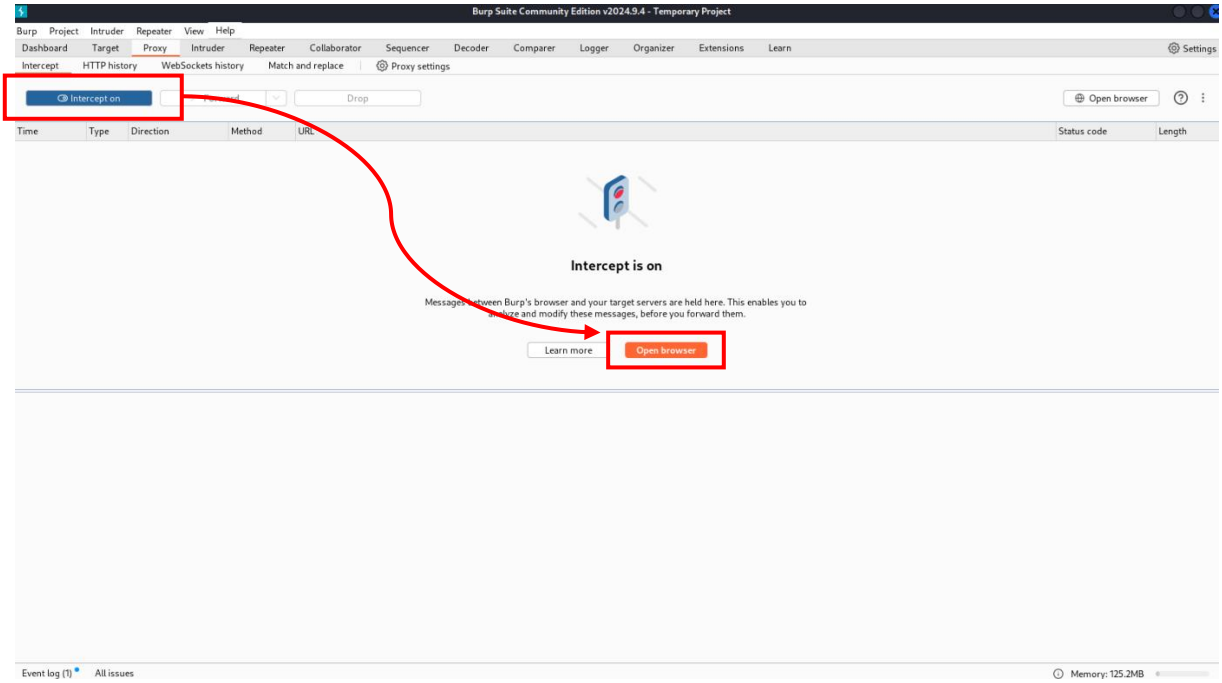

File Machine View Input Devices Help
Kali Linux
GitHub - digininja/DVWA
Welcome :: Damn Vulner
Burp Suite - Application
Installing Burp Suite Prof
https://portswigger.net/burp/documentation/desktop/getting-started/download-and-install
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Support Center
Getting Started
Latest Releases
Burp Extensions
User Forum
Training
Search Burp Suite documentation
SEARCH
Back to documentation home
Professional and Community Edition
Getting started
System requirements
Step 1: Download and install
Step 2: Intercepting HTTP traffic
Step 3: Modifying requests
Step 4: Setting the target scope
Step 5: Reissuing requests
Step 6: Running your first scan [Pro only]
Step 7: Generating a report [Pro only]
Step 8: What next?
Testing workflow
Tools
Burp Extensions
Running scans [Pro only]
Project files
Settings
Customizing Burp's layout
Support Center > Documentation > Desktop editions > Getting started > Download and install
Professional
Community Edition
Download and install
Last updated: December 19, 2024
Read time: 1 Minute
Step 1: Download
Use the links below to download the latest version of Burp Suite Professional or Community Edition.
Choose your software
PROFESSIONAL
COMMUNITY EDITION
Step 2: Install
Run the installer and launch Burp Suite.
When asked to select a project file and configuration, just click Next and then Start Burp to skip this for now.
Note
If you're using Burp Suite Professional, enter your license key when prompted. If you don't have one already, you can subscribe or request a free trial.

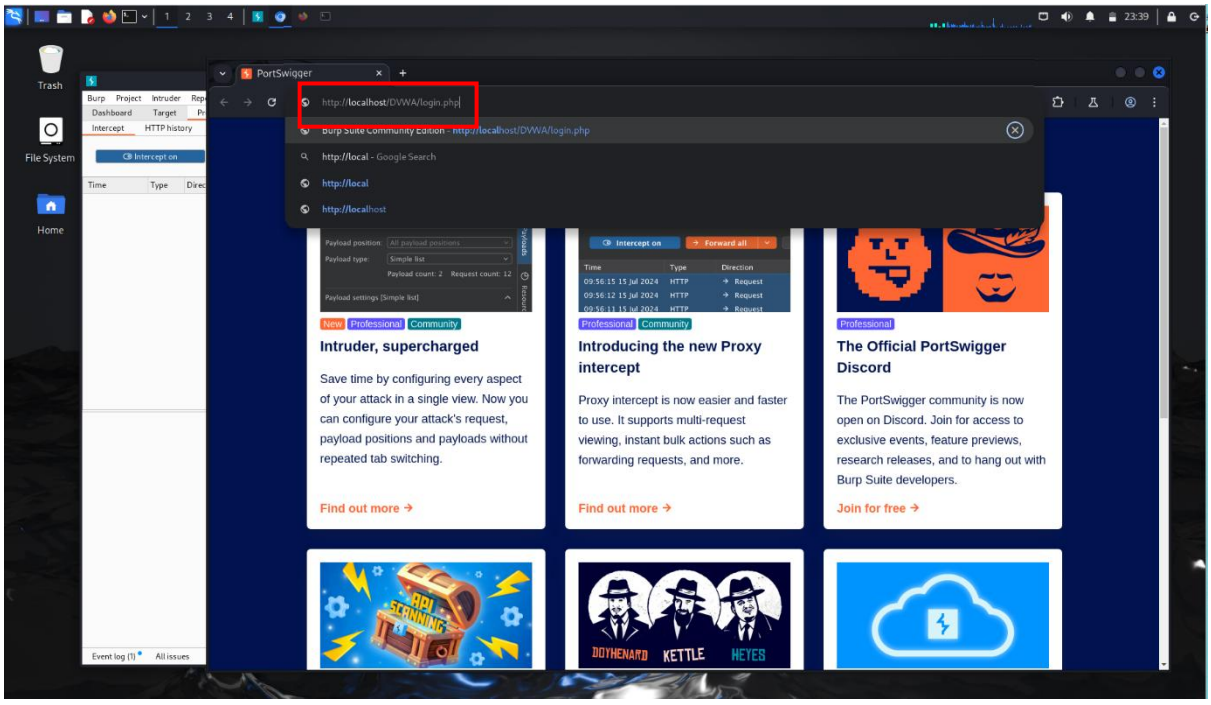


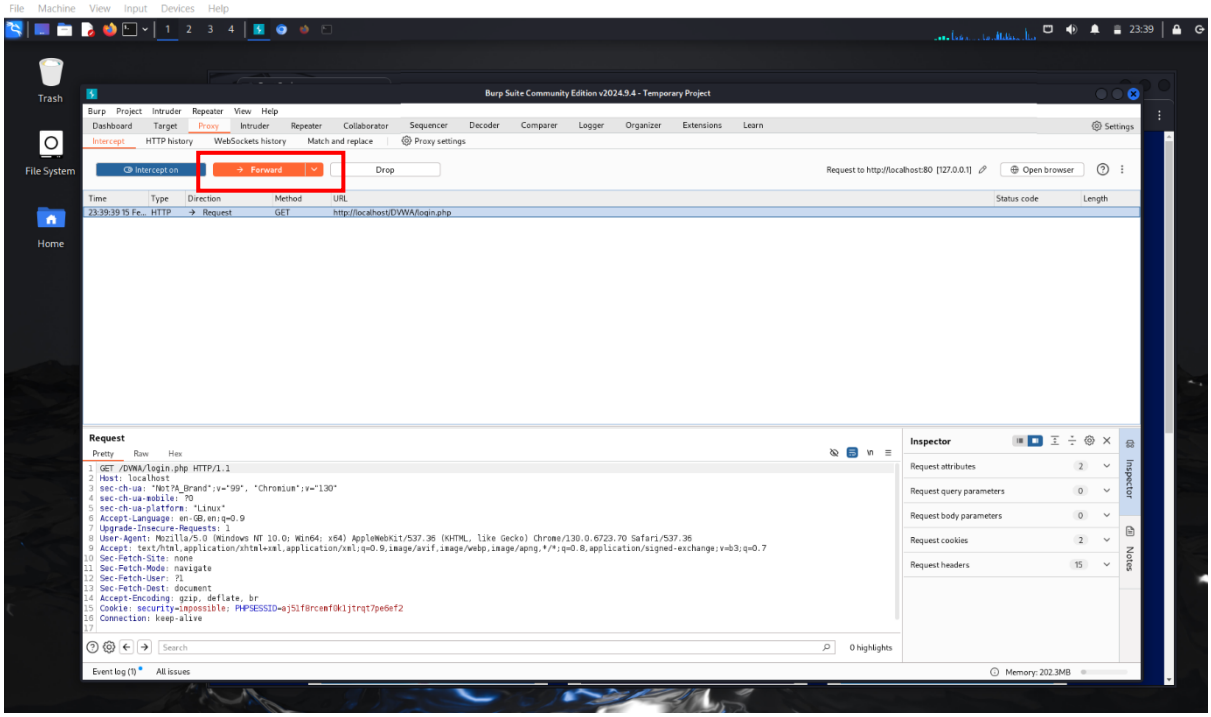
Phase 2: Capturing Credentials

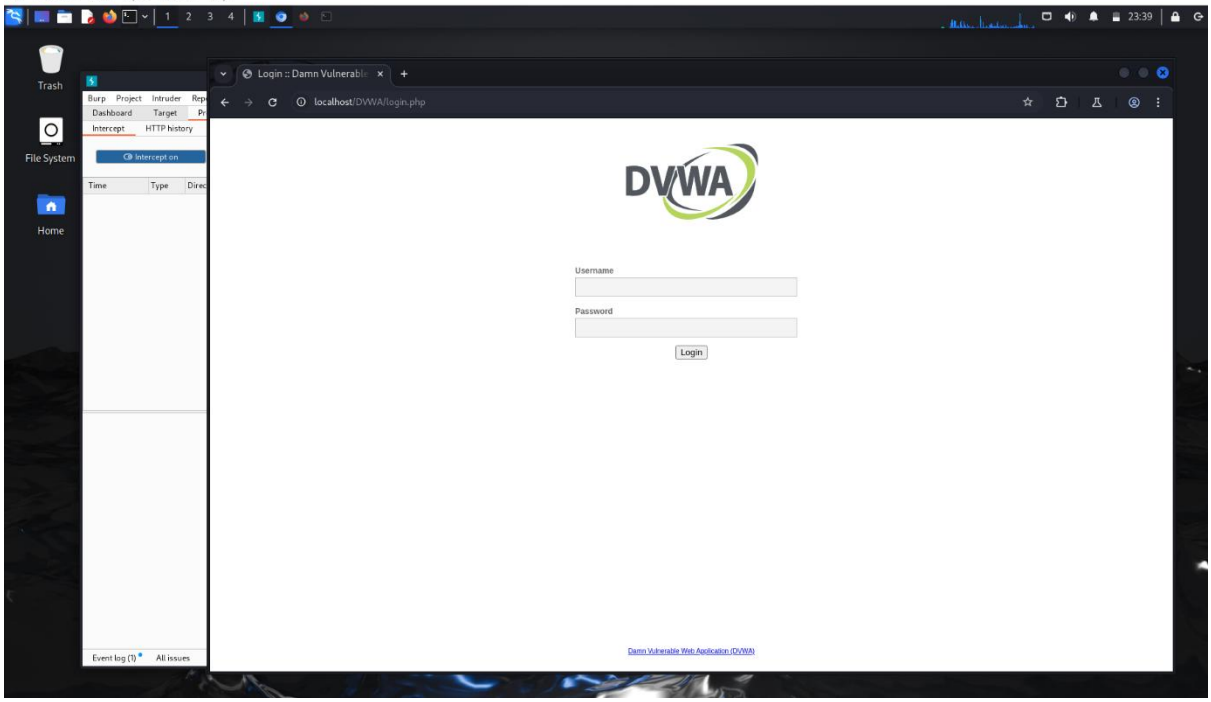
Intercepting Login Requests with Burp Suite

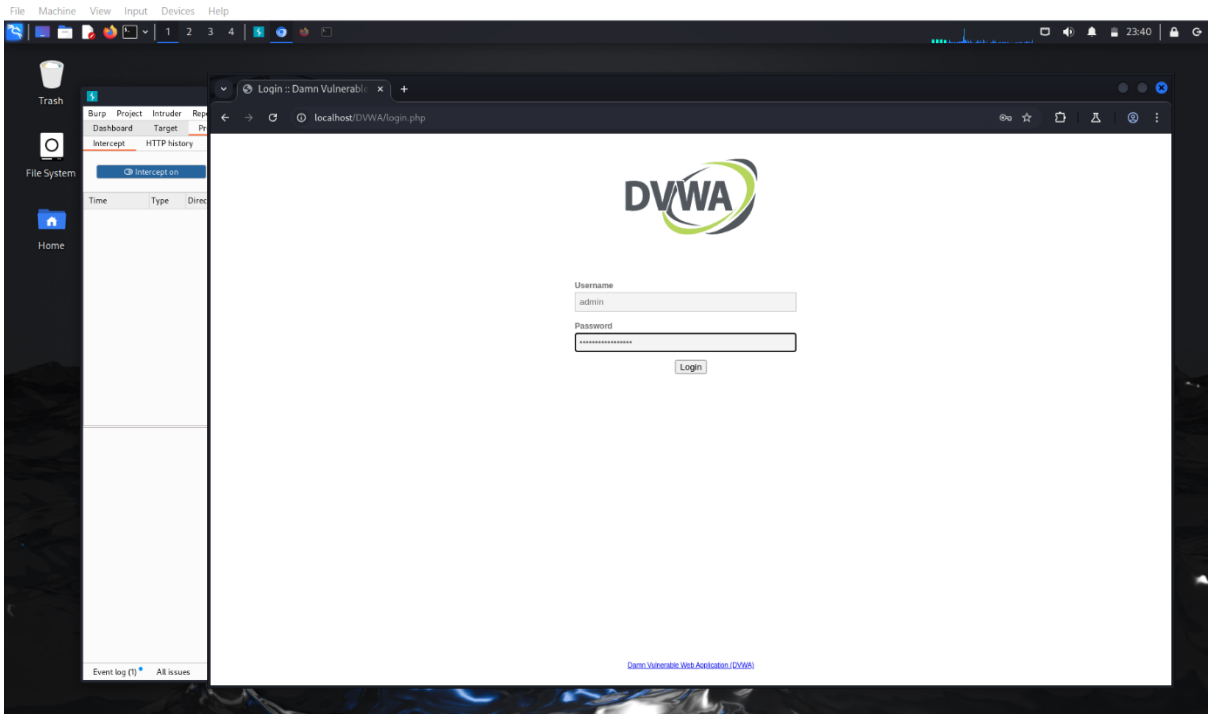
1. Open **Burp Suite**, go to **Proxy > Intercept**, and ensure **Intercept is ON**.
2. Use **Burp Suite's browser** to navigate to http://localhost/DVWA/login.php.
3. Click **Forward** in Burp Suite to allow the captured request to proceed to the server.
4. Enter **any credentials** (e.g., admin/password123) and attempt to log in.
5. The intercepted **HTTP request** will display the credentials in plaintext.


Burp Suite Community Edition v2024.9.4 - Temporary Project
Intercept on
Drop
Open browser
Intercept is on
Learn more
Open browser


PortSwigger
http://localhost/DVWA/login.php
Intruder, supercharged
Introducing the new Proxy intercept
The Official PortSwigger Discord
Find out more →
Find out more →
Join for free →

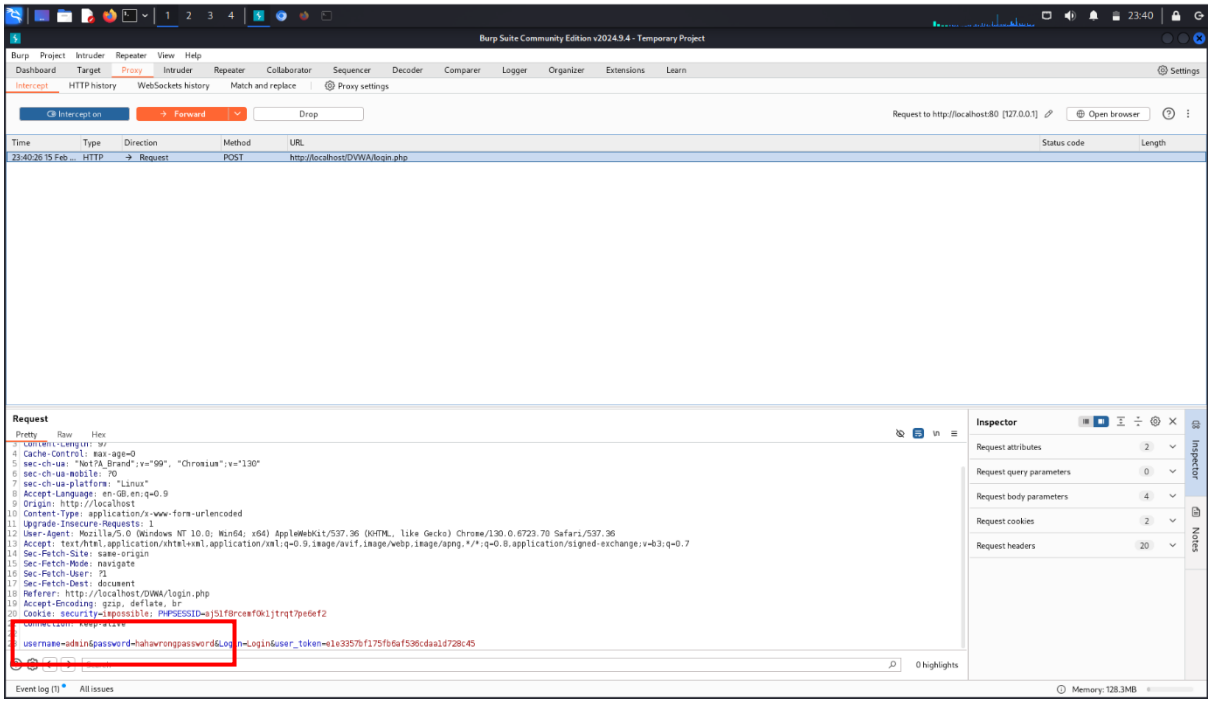

Burp Suite Community Edition v2024.9.4 - Temporary Project
Intercept on
Forward
Drop
Request
Pretty
Raw
Hex
GET /DVWA/login.php HTTP/1.1
Host: localhost
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers


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



Phase 3: Extracting Credentials

Captured HTTP Request Example



Key Findings

- The username and password are transmitted in plaintext, making them **vulnerable to interception**.
- This highlights security flaws in **unencrypted authentication systems**.

Phase 4: Implications and Prevention

What This Demonstrates

- Understanding **vulnerabilities in login mechanisms**.
- Practical application of **Burp Suite for security testing**.
- How attackers can exploit **unencrypted credential transmission**.

Prevention

- **Secure Authentication:** Implement strong password hashing (e.g., bcrypt, Argon2) and multi-factor authentication (MFA) to protect user credentials.
- **Use HTTPS:** Enforce HTTPS with SSL/TLS certificates to encrypt data in transit and prevent man-in-the-middle attacks.
- **Secure Sessions:** Implement secure session management with HTTP-only, secure, and same-site cookies to prevent session hijacking.

Important Reference Resources

- **Basic Project Idea:** https://www.instagram.com/reel/DGBWj5LtEOs/?igsh=NHV3bmc0Zm5ybzFi
- **DVWA GitHub Repository:** https://github.com/digininja/DVWA
- **DVWA Setup Guide:** https://www.youtube.com/watch?v=WkyDxNJkgQ4
- **Burp Suite Download:** https://portswigger.net/burp/documentation/desktop/getting-started/download-and-install
- **Burp Suite Configuration:** https://www.youtube.com/watch?v=ZWKqxQF6aow&t=21s

---