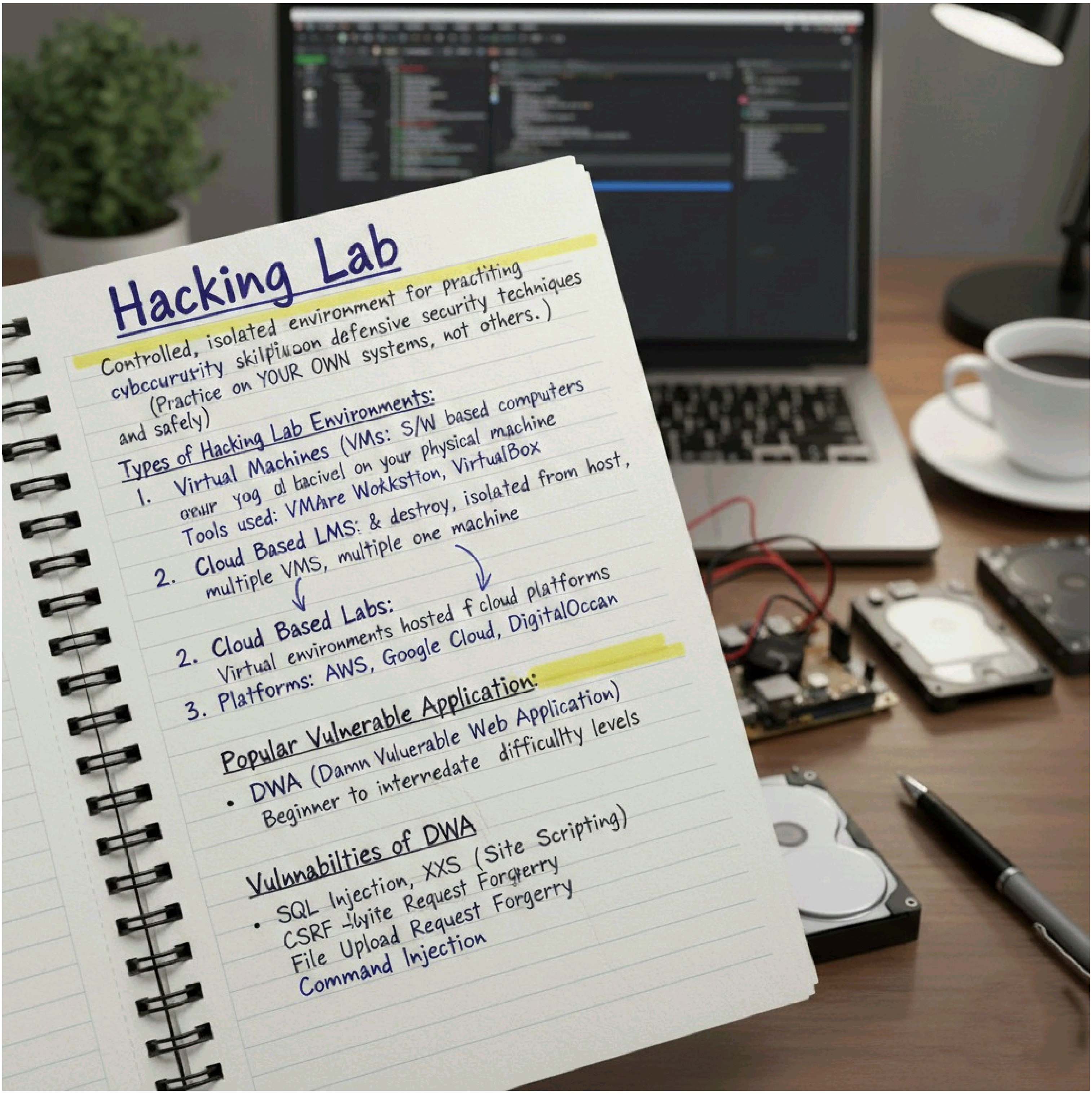


Hacking Lab

Controlled, isolated environment for practiting cybccururity skilpiмoon defensive security techniques (Practice on YOUR OWN systems, not others.) and safely)

Types of Hacking Lab Environments:

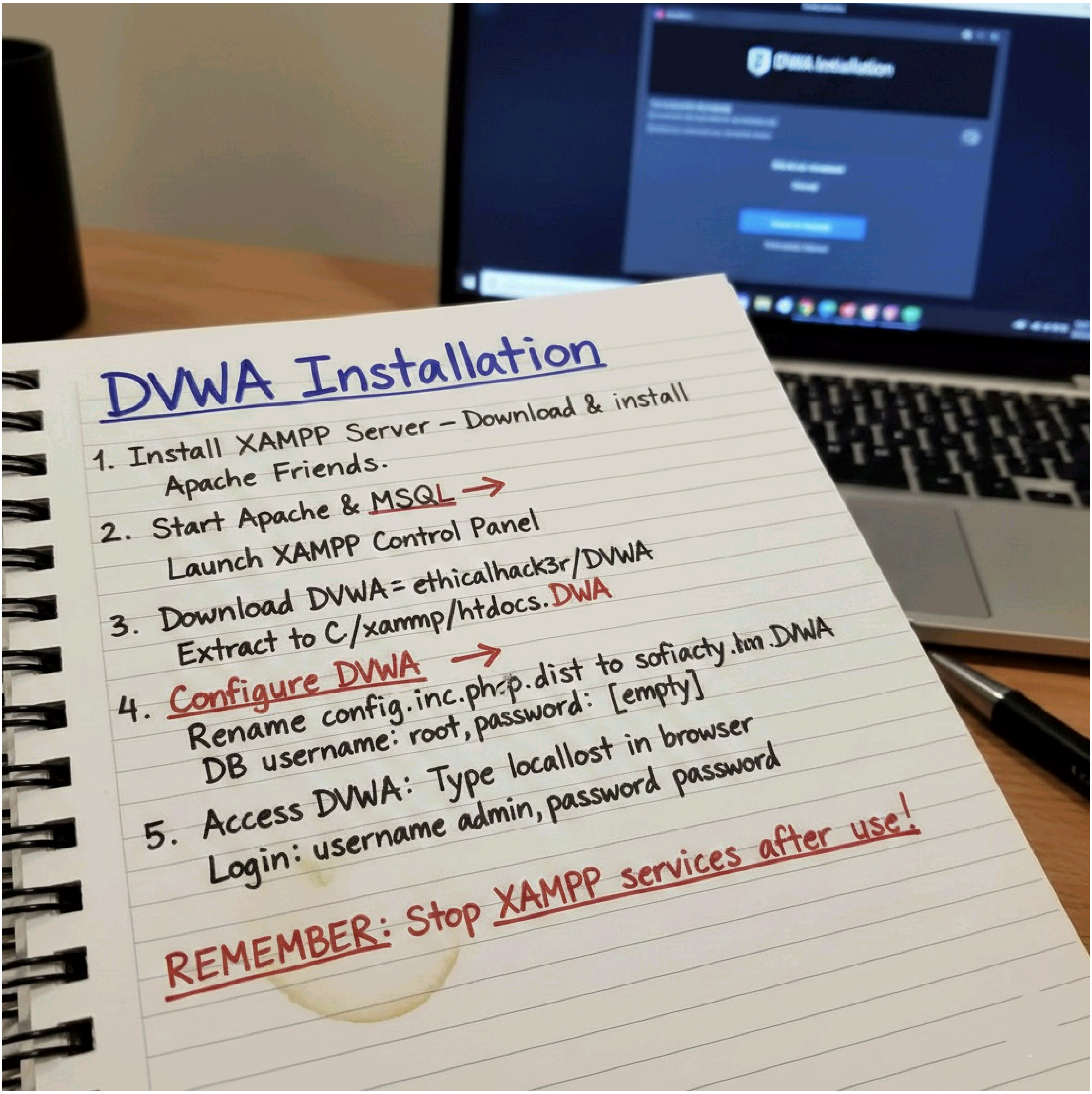
1. Virtual Machines (VMs: S/W based computers aeuır yog αl bacivel on your physical machine Tools used: VMAre Wokkstтon, VirtualBox
2. Cloud Based LMS: & destroy, isolated from host, multiple VMS, multiple one machine
2. Cloud Based Labs: Virtual environments hosted f cloud platforms
3. Platforms: AWS, Google Cloud, DigitalOccan

Popular Vulnerable Application:

- DWA (Damn Vuluerable Web Application) Beginner to internedate difficullty levels

Vulnnabilties of DWA

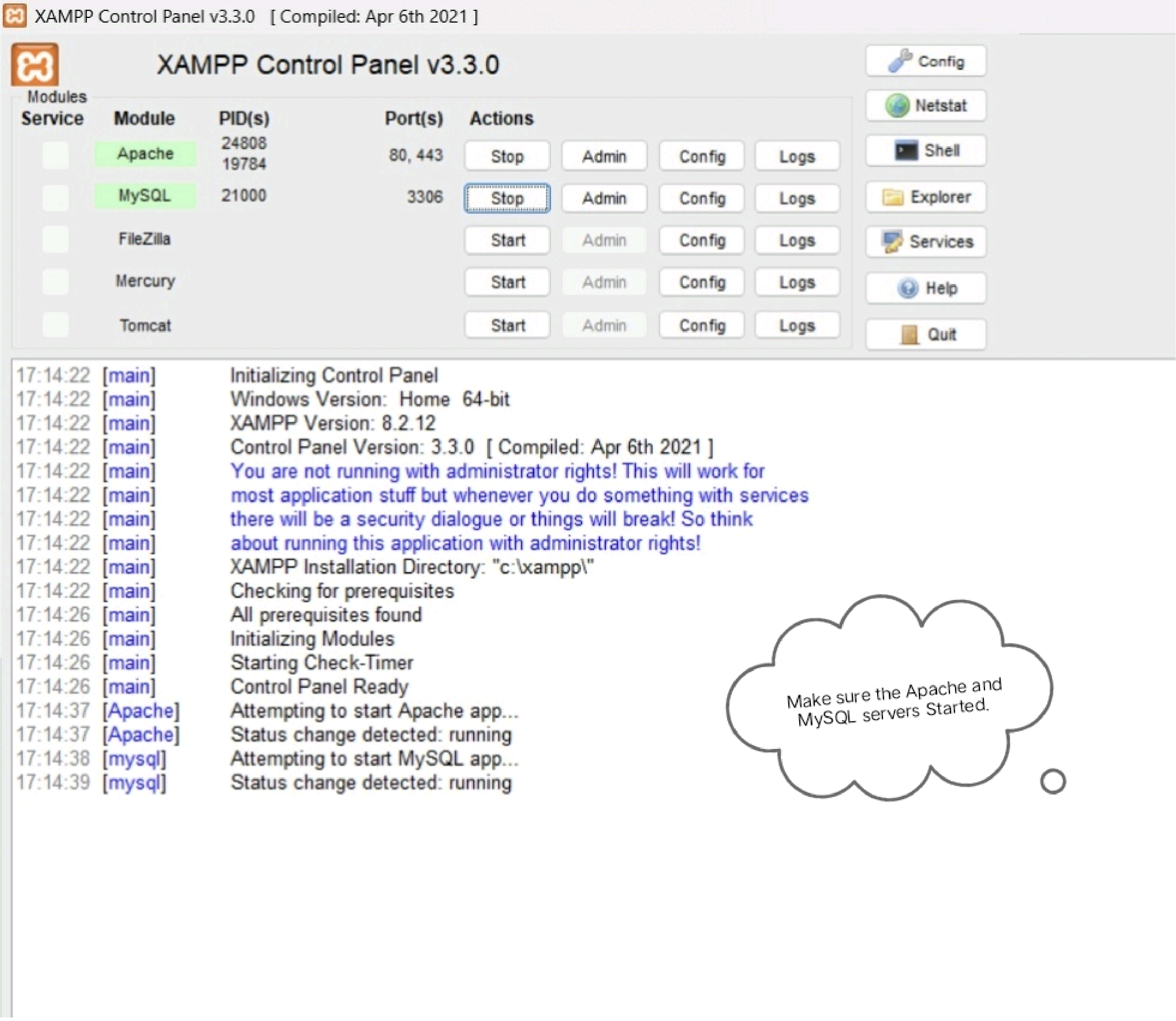
- SQL Injection, XXS (Site Scripting)
  CSRF -Иyite Request Forgrerry
  File Upload Request Forgerry
  Command Injection


DVWA Installation

DVWA Installation

1. Install XAMPP Server – Download & install
   Apache Friends.
2. Start Apache & MSQL →
   Launch XAMPP Control Panel
3. Download DVWA = ethicalhack3r/DVWA
   Extract to C/xammp/htdocs.DWA
4. Configure DVWA →
   Rename config.inc.ph:p.dist to sofiacty.lim.DWA
   DB username: root, password: [empty]
5. Access DVWA: Type locallost in browser
   Login: username admin, password password

REMEMBER: Stop XAMPP services after use!



XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]

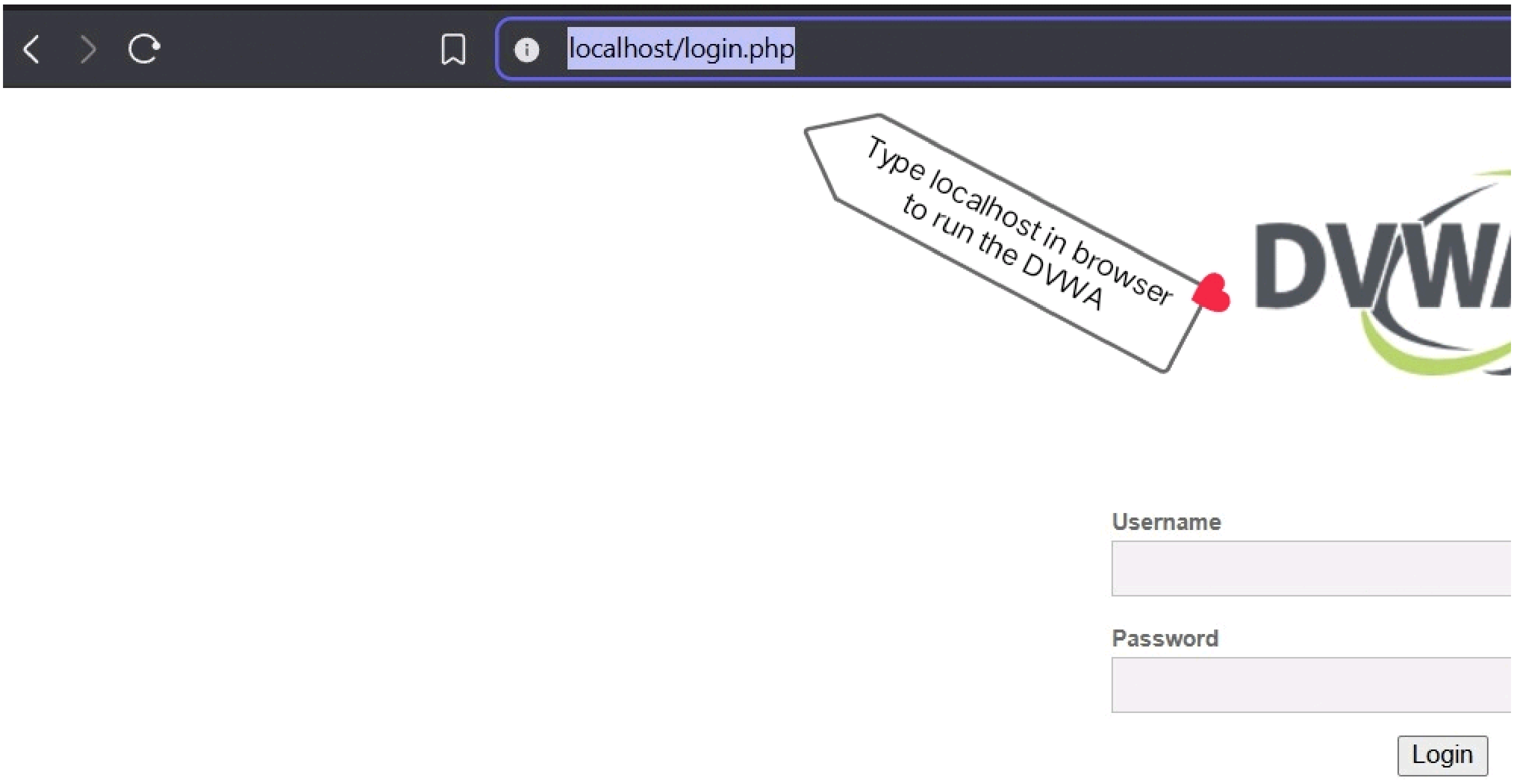
XAMPP Control Panel v3.3.0

Modules

Service	Module	PID(s)	Port(s)	Actions			
□	Apache	24808 19784	80, 443	Stop	Admin	Config	Logs
□	MySQL	21000	3306	Stop	Admin	Config	Logs
□	FileZilla			Start	Admin	Config	Logs
□	Mercury			Start	Admin	Config	Logs
□	Tomcat			Start	Admin	Config	Logs

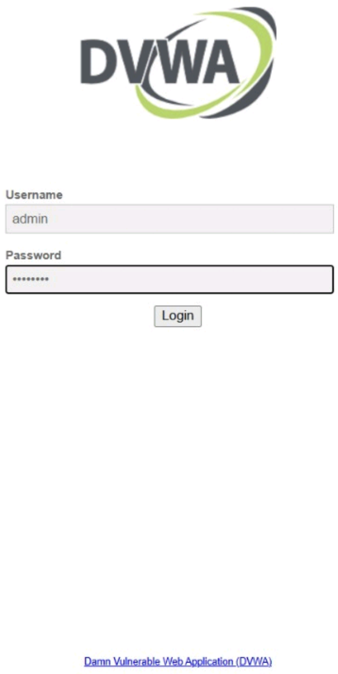
```
17:14:22  [main]     Initializing Control Panel
17:14:22  [main]     Windows Version:  Home  64-bit
17:14:22  [main]     XAMPP Version: 8.2.12
17:14:22  [main]     Control Panel Version: 3.3.0  [ Compiled: Apr 6th 2021 ]
17:14:22  [main]     You are not running with administrator rights! This will work for
17:14:22  [main]     most application stuff but whenever you do something with services
17:14:22  [main]     there will be a security dialogue or things will break! So think
17:14:22  [main]     about running this application with administrator rights!
17:14:22  [main]     XAMPP Installation Directory: "c:\xampp\"
17:14:22  [main]     Checking for prerequisites
17:14:26  [main]     All prerequisites found
17:14:26  [main]     Initializing Modules
17:14:26  [main]     Starting Check-Timer
17:14:26  [main]     Control Panel Ready
17:14:37  [Apache]   Attempting to start Apache app...
17:14:37  [Apache]   Status change detected: running
17:14:38  [mysql]    Attempting to start MySQL app...
17:14:39  [mysql]    Status change detected: running
```

Make sure the Apache and MySQL servers Started.



localhost/login.php

Type localhost in browser to run the DVWA



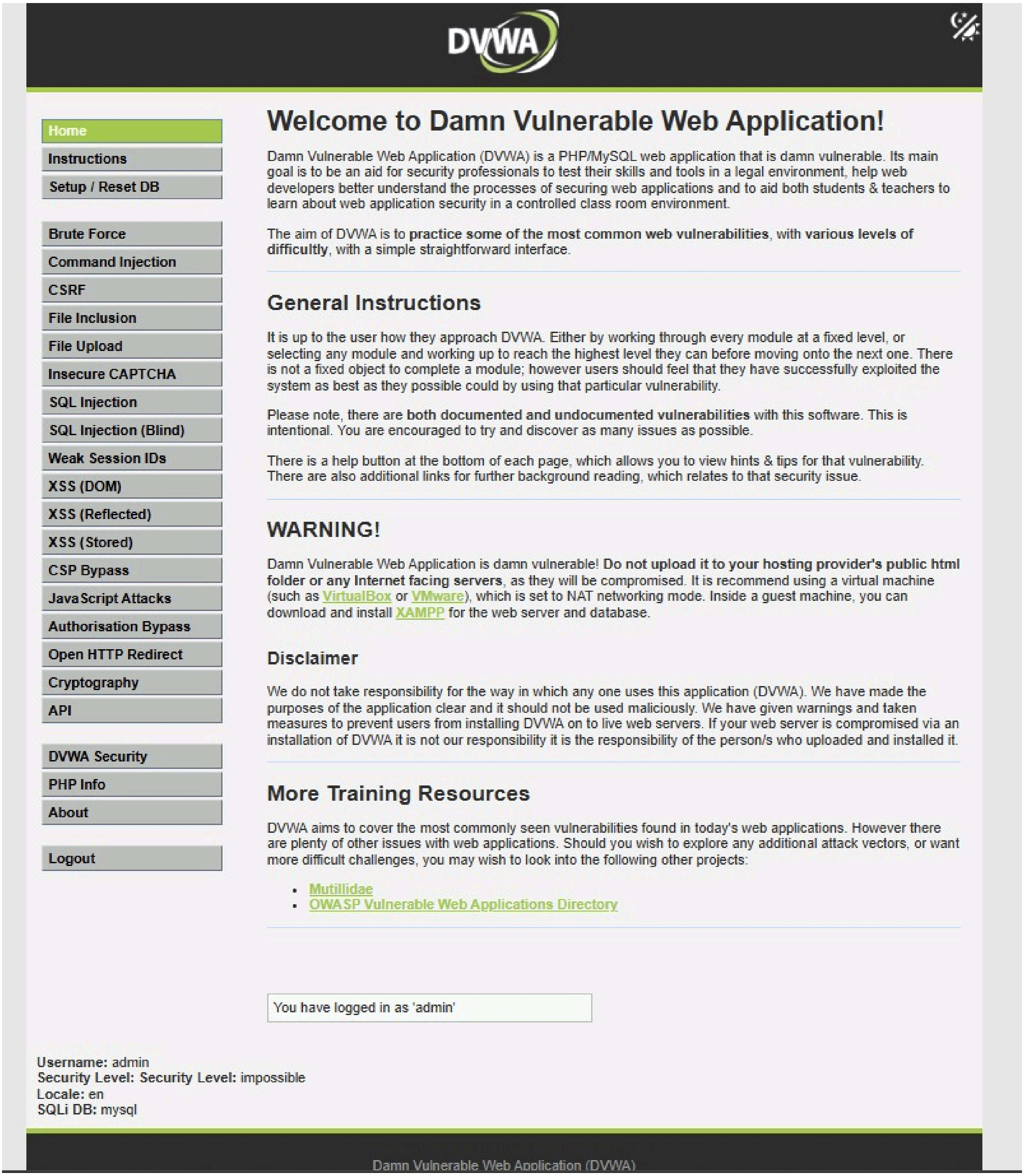
Username

admin

Password

••••••••

Damn Vulnerable Web Application (DVWA)



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

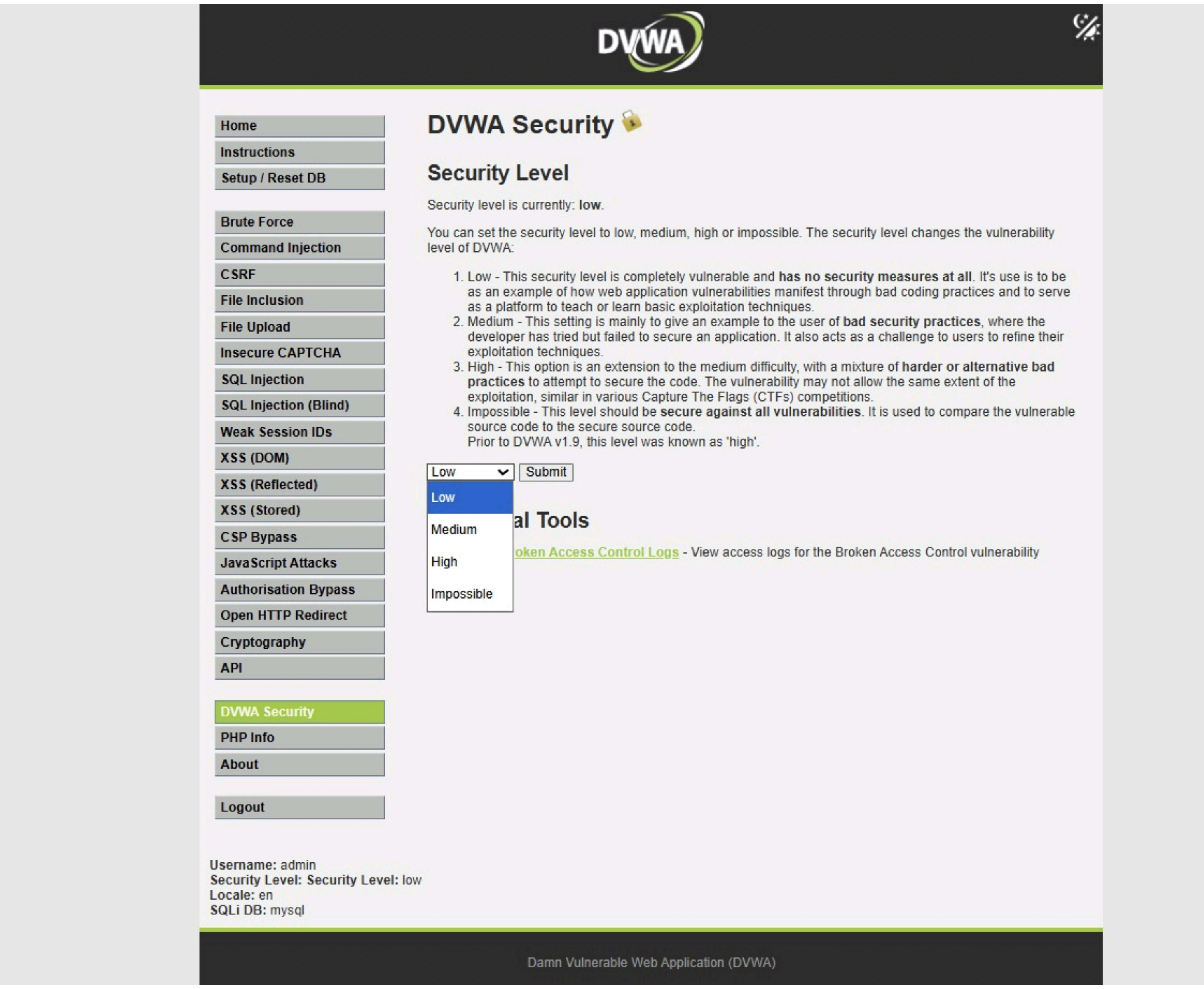
DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- Mutillidae
- OWASP Vulnerable Web Applications Directory

You have logged in as 'admin'

Username: admin
Security Level: Security Level: impossible
Locale: en
SQLi DB: mysql

Damn Vulnerable Web Application (DVWA)



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

al Tools

oken Access Control Logs - View access logs for the Broken Access Control vulnerability

Username: admin
Security Level: Security Level: low
Locale: en
SQLi DB: mysql

Damn Vulnerable Web Application (DVWA)