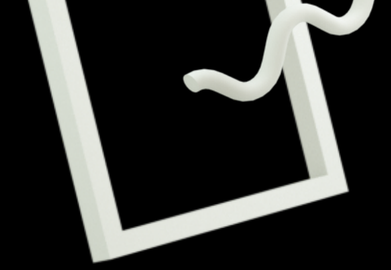
Pen-Testing Tools in Kali.

E.Pushya Saie Raag.

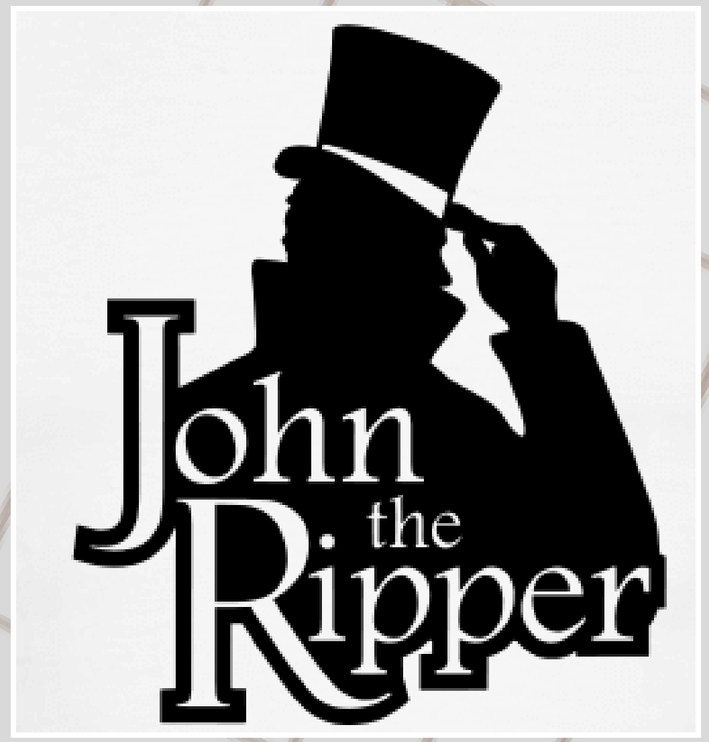


John The Ripper

password-cracking tool, to determine the strength of a password.

- ts primary purpose is to test the strength of passwords and identify potential vulnerabilities.
- John the Ripper supports various password encryption types, including UNIX, Windows, and Kerberos.
- With its flexibility and extensive capabilities, it has become a go-to tool for security professionals.

Use Cases for John the Ripper



It is commonly used to audit password security within organizations.

By running John the Ripper against password databases, analysts can identify weak or easily guessable passwords.

The tool helps educate users about password best practices and strengthens overall system security.

How does John The Ripper work?

- John the Ripper utilizes several techniques to crack passwords effectively.
- It employs dictionary-based attacks, which involve trying a large set of common words and phrases as passwords.
- Brute-force attacks are also used, systematically trying every possible combination until the correct password is found.
- Additionally, John the Ripper can perform hybrid attacks, combining dictionary words with additional characters and variations.

Modes of Operation.

- You will be using one of these three for most of your use cases.
- **Single crack mode**
- **Wordlist mode**
- **Incremental mode**

Single crack

- In single-crack mode, John takes a string and generates variations of that string in order to generate a set of passwords

- For example, if our username is “stealth” and the password is “StEaLtH”, we can use the single mode of John to generate password variations (STEALTH, Stealth, STealth, and so on)

- We use the “format” flag to specify the hash type and the “single” flag to let John know we want to use the single crack mode. We will also create a crack.txt file which will contain the username and the hash value of the password.

Dictionary

- In dictionary mode, we will provide John with a list of passwords. John will generate hashes for these on the fly and compare them with our password hash.

- For this example, we will use the RockYou wordlist. If you are using Kali, you can find it at /usr/share/wordlists/rockyou.txt. We will also have a crack.txt file with just the password hash.

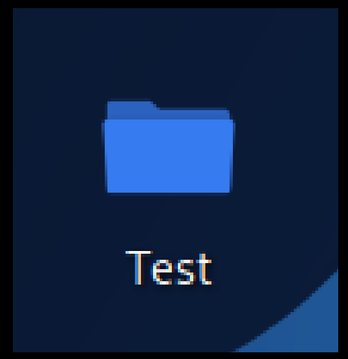
Incremental

- Incremental mode is the most powerful mode provided by John. It tries all possible character combinations as passwords.

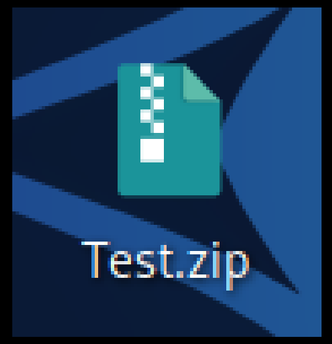
- This sounds great, but there is a problem. The cracking can go on for a long time if the password is too long or if it's a combination of alphanumeric characters and symbols.

- You will rarely use this mode unless you have no other option. In typical cases, a combination of Social Engineering attacks and wordlist mode will help you crack most of the hashes.

JTR Example

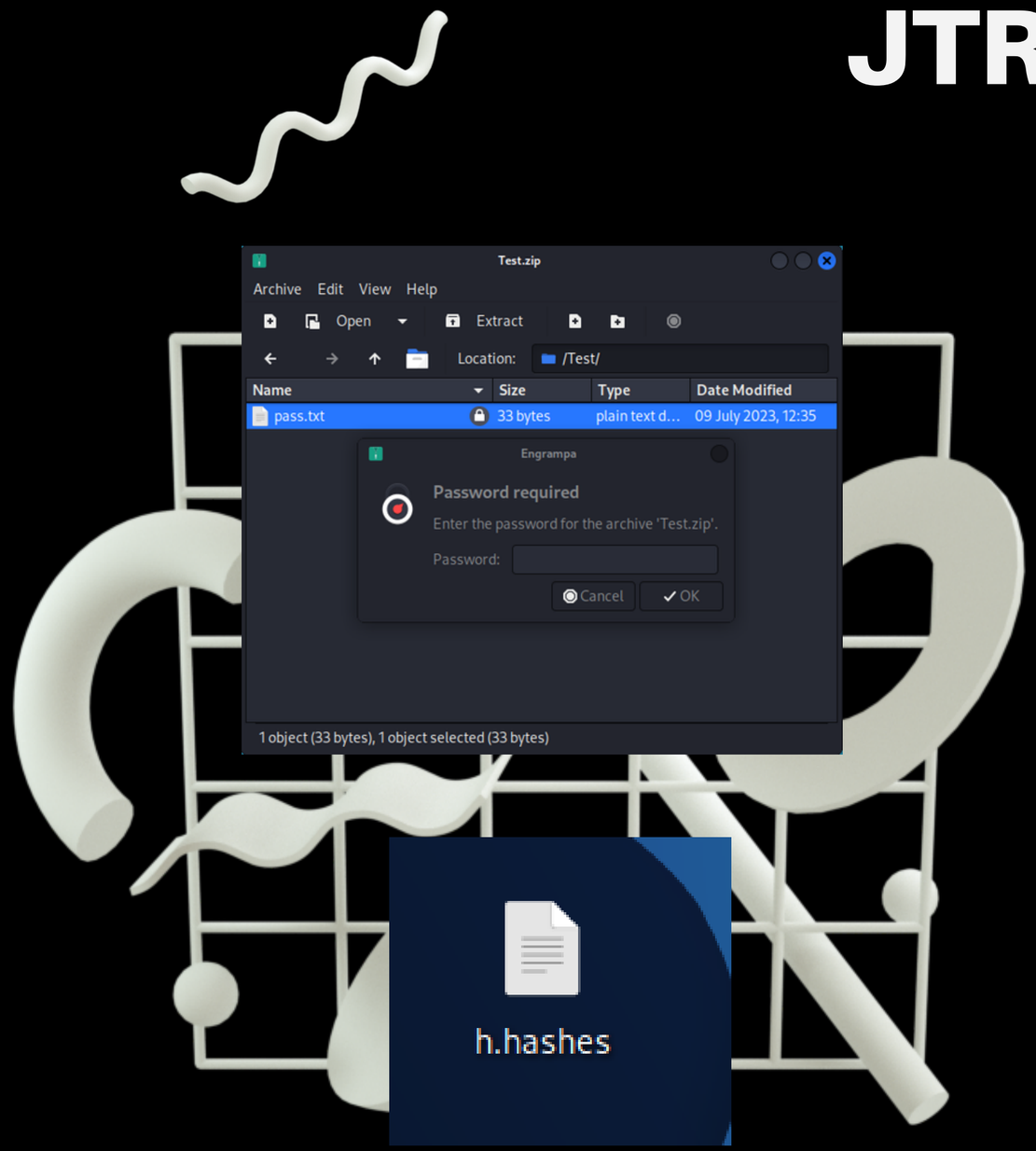


Take a folder with information and we will try to secure it by making a zip file



The file can me made into a zip file and make it secured with a password

JTR Example



After making the zip file we can see that it requires a password. By using John The Ripper, we can try brute forcing the password.

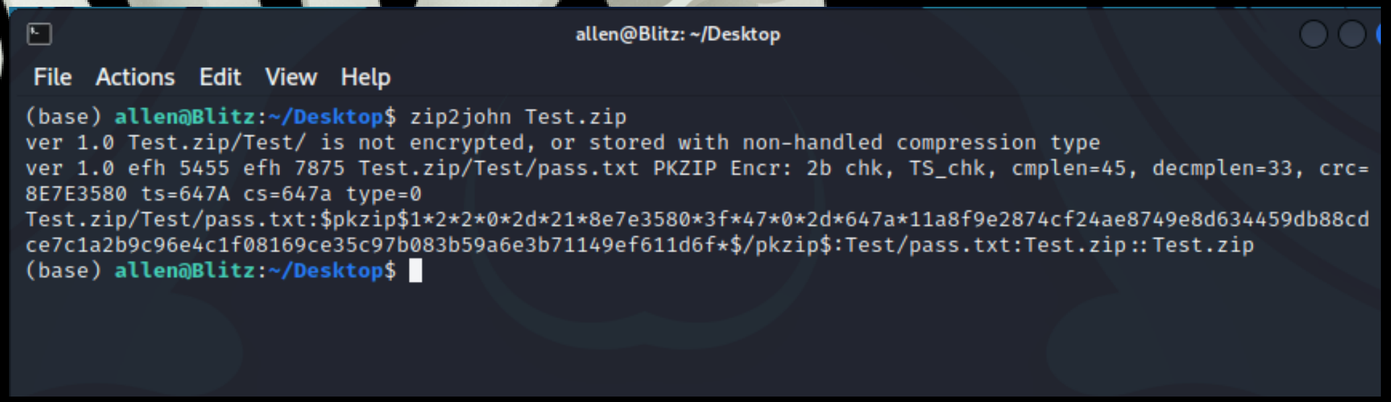
we also add a hash file depending on the preferred mode.

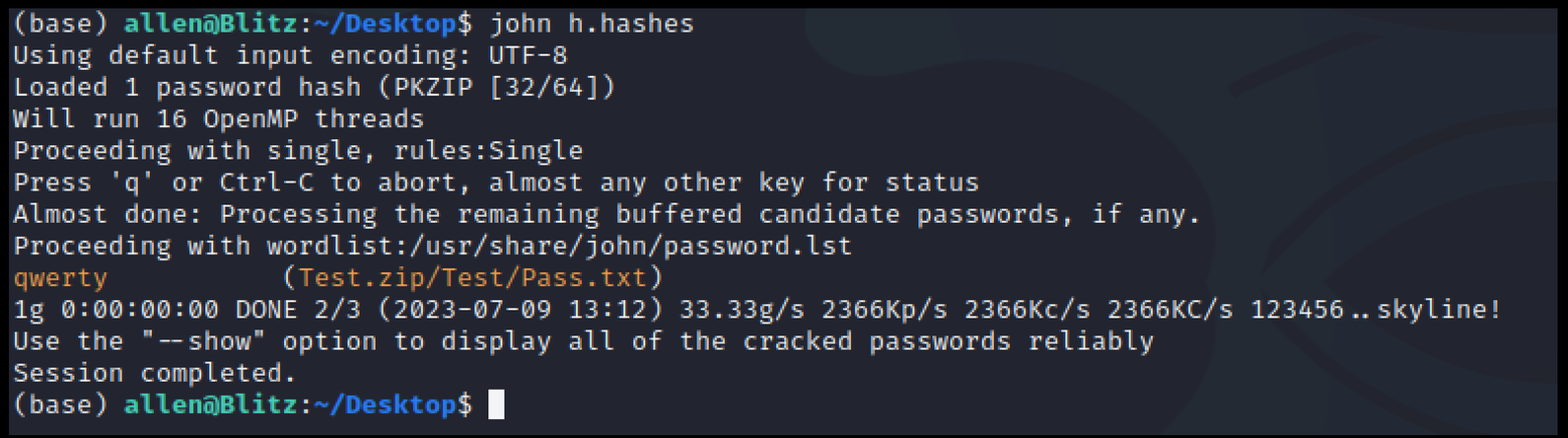
JTR

By using the command, "zip2john <filename> > <hash file name>" in our terminal we can execute JTR.

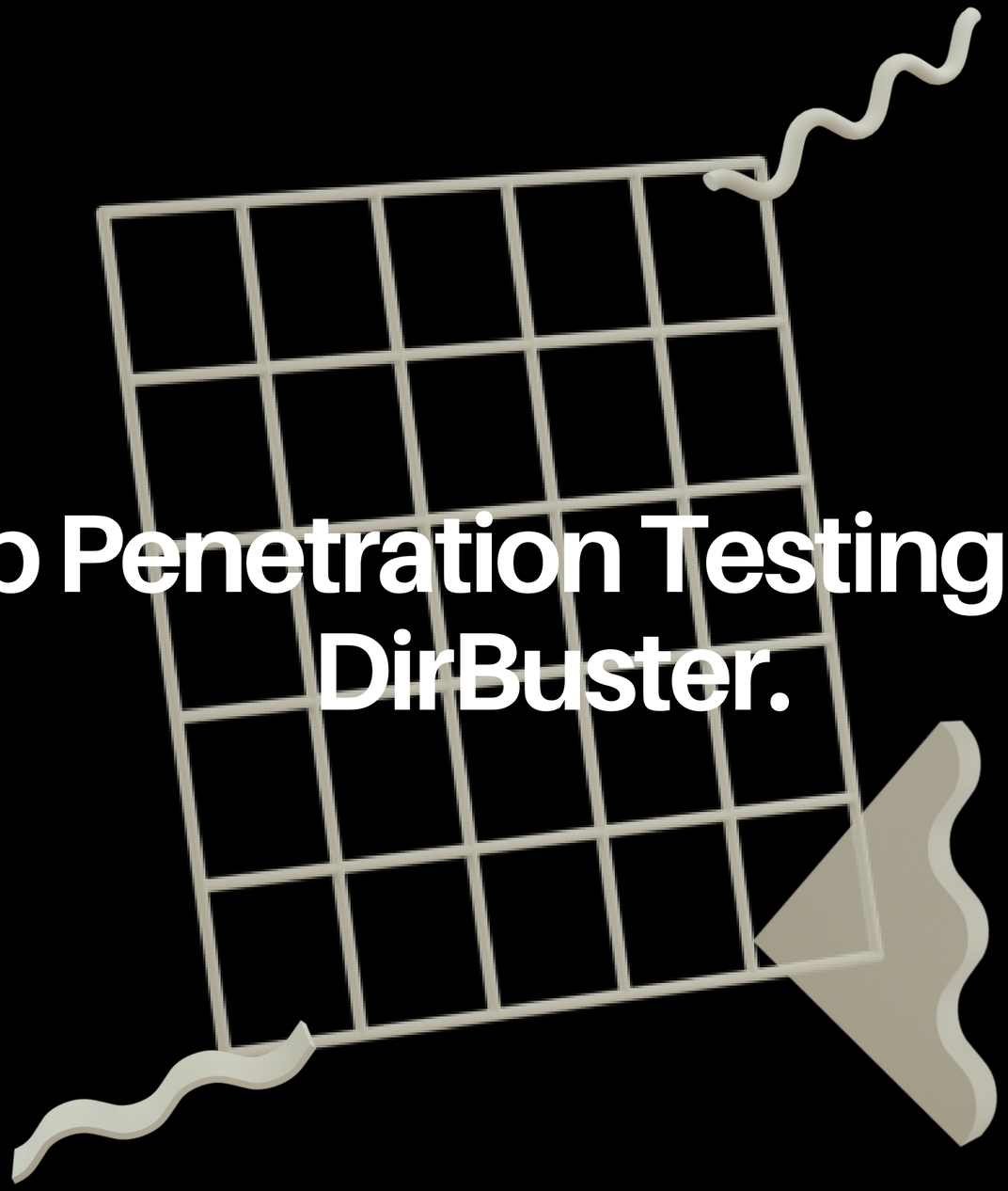
JTR Example

output execution

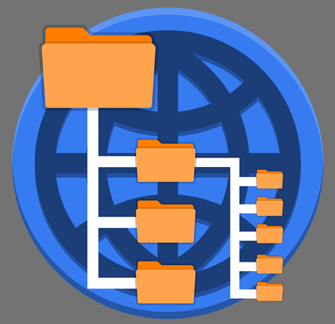




Web Penetration Testing using DirBuster.



DirBuster



- DirBuster is a popular web directory and file brute-forcing tool used for website enumeration and discovery. It is specifically designed to help security professionals identify hidden directories and files on web servers
- DirBuster can be helpful in penetration testing and web application security assessments to uncover sensitive information, misconfigurations, or hidden resources that may not be readily accessible through normal navigation

1. Directory and File Bruteforcing: DirBuster automates the process of testing different directory and file names by sending HTTP requests and analyzing the responses. It allows you to customize the wordlists used for brute-forcing.

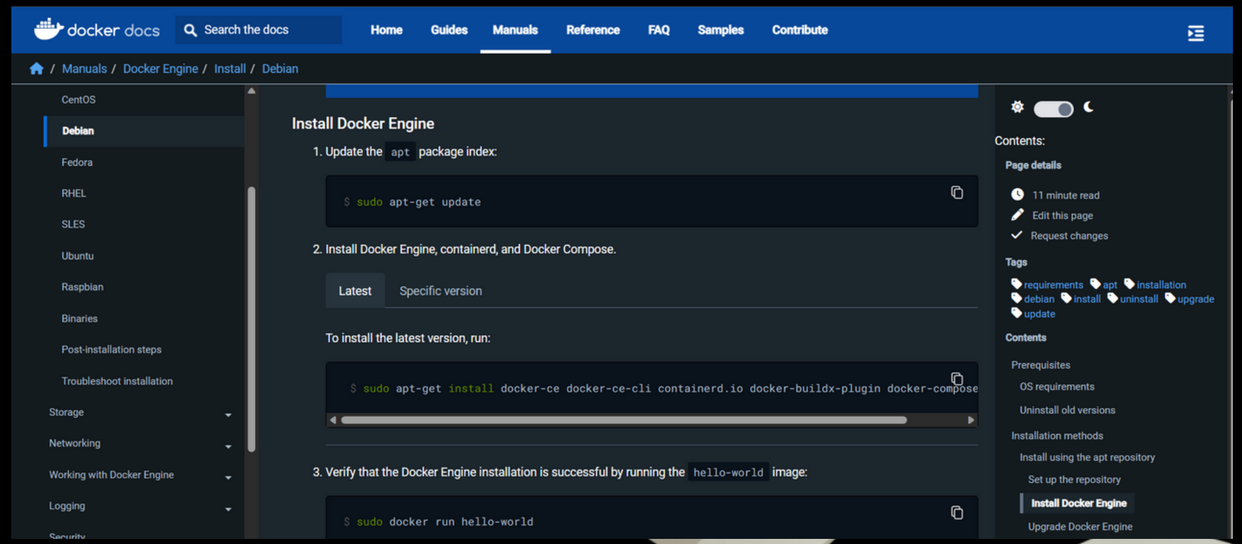
1. Multi-threaded Operation: DirBuster utilizes multi-threading, allowing it to perform concurrent requests to speed up the scanning process and improve efficiency.

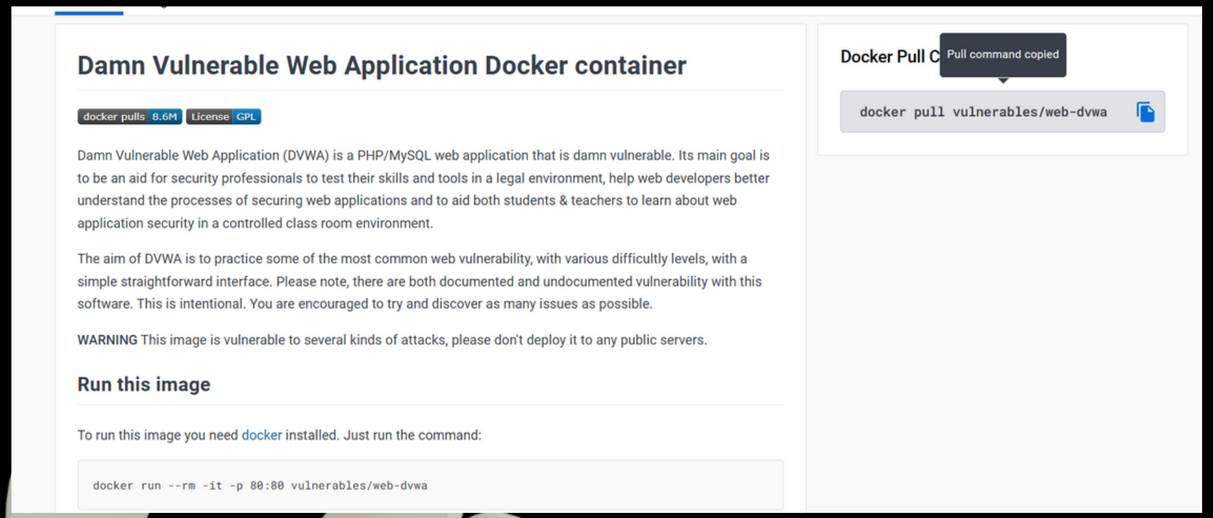
1. Recursive Scanning: DirBuster has the capability to recursively scan discovered directories, exploring deeper into the web server's directory structure to find additional hidden content.

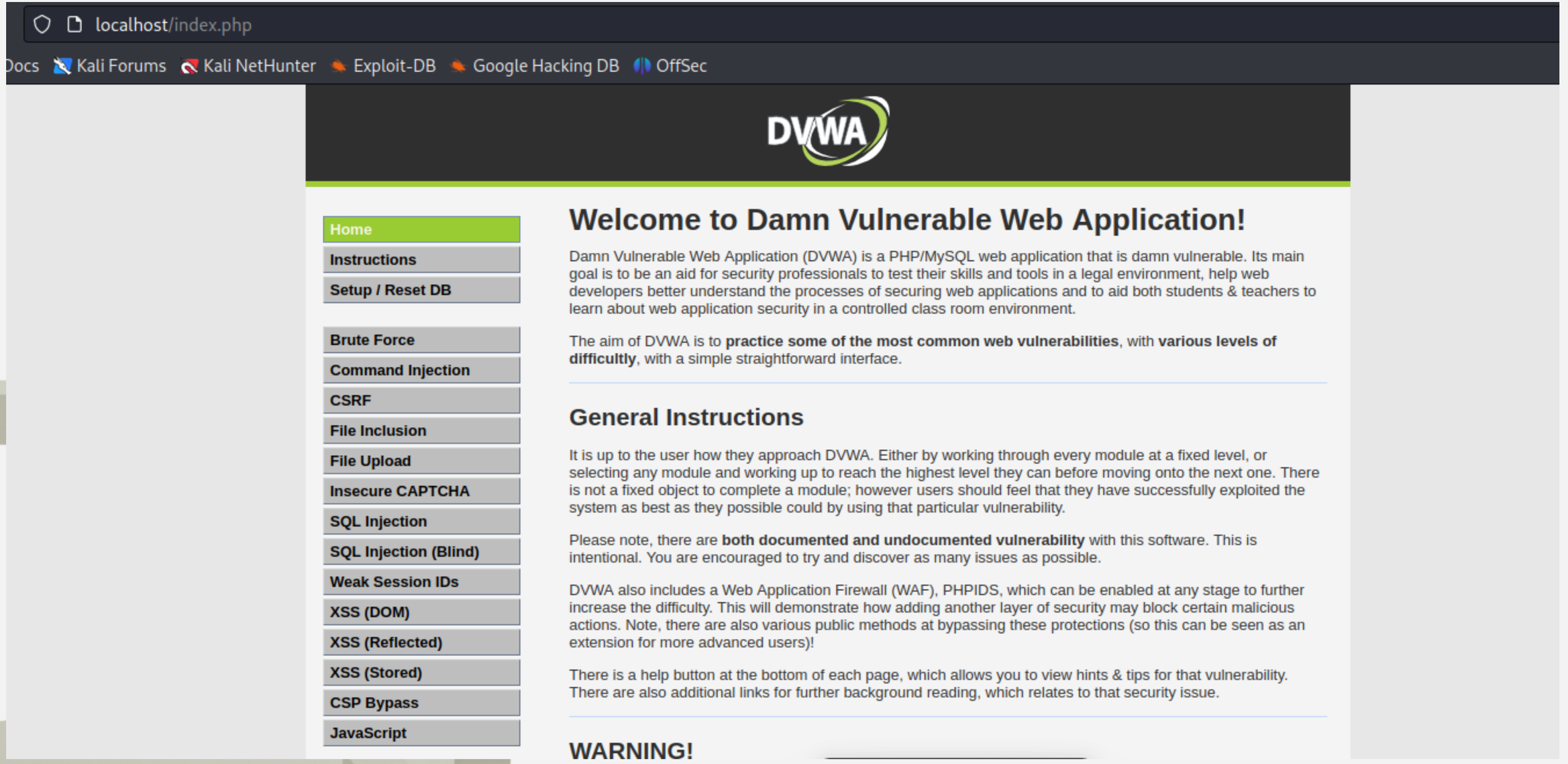
1. Proxy Support: It supports proxy settings, allowing you to configure and route the HTTP requests through a proxy server for anonymity or bypassing certain restrictions.

Setting up a host to penetrate

To penetrate a web application, we need permission from their administrators, so for demonstration purposes, we will be using the Damn Vulnerable Web Apllication hosted locally using Docker

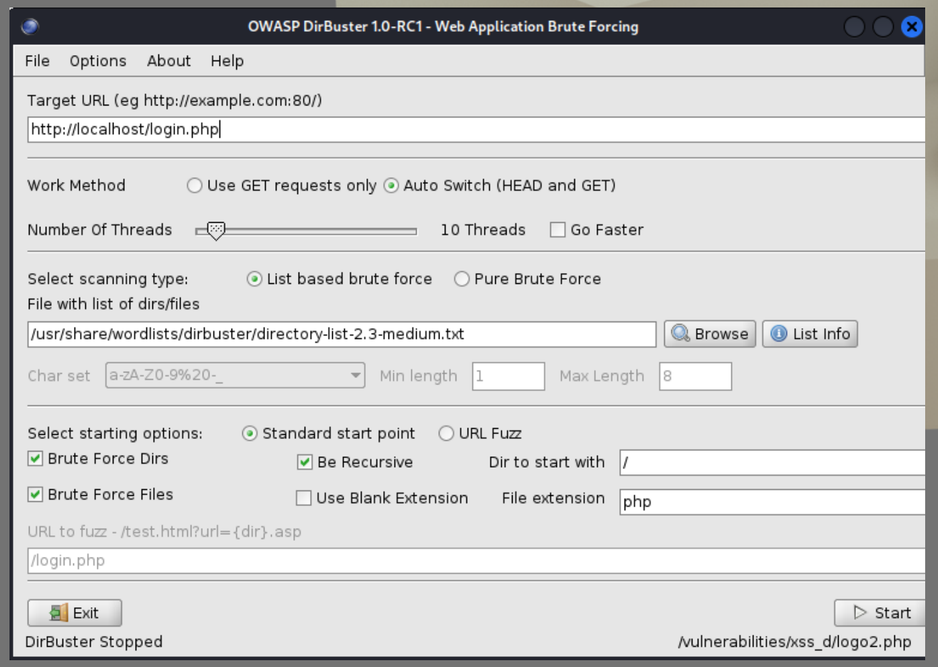





localhost/index.php
Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Welcome to Damn Vulnerable Web Application!
Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.
The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficultly, with a simple straightforward interface.
General Instructions
It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.
Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!
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!

Dirbuster Scan

- Open up DirBuster from Menu
- Provide Target link (in this case the local host)
- Specify the Wordlist to search for in the webpage
- Select no of threads and start the scan



Dirbuster Output

- The scan will start and will show you the available webpages in the web application one-by-one
- This helps us identify the hidden files and directories in the web application