Task Level: Beginner level

Security audit for Testphp.vulnweb.com

Prepared and audited by **NIKUL PATEL** Team ShadowFox Batch 1 (June)

Table of contents

Introduction:

Testphp.vulnweb.com is a deliberately vulnerable web application created by Acunetix for security testing and educational purposes. It is used by security professionals, developers, and students to practice and learn about web application security vulnerabilities.

Key Features:

1. **Purpose**: A testing ground for web vulnerabilities, helping users understand how these can be exploited and fixed.
2. **Vulnerabilities**: Contains intentional flaws like SQL injection, cross-site scripting (XSS), file inclusion, and command injection.
3. **Educational Tool**: Provides hands-on learning for penetration testing, vulnerability assessment, and secure coding.
4. **Ethical Use**: Designed for educational purposes only, and should not be used against real- world systems without permission.
5. **Accessibility**: Freely accessible online for anyone interested in web security.
6. **Up-to-Date**: Regularly maintained to reflect current security trends.
7. **Community**: Supported by a community that shares knowledge and challenges in web security testing.

Technical Information:

- **Server-Side Scripting**: Uses PHP.
- **Database**: Utilizes MySQL or a similar relational database.
- **Web Server**: Runs on a server like Apache or Nginx that supports PHP.

Planning and Scoping the test:

Testphp.vulnweb.com is not a real online store. Instead, it's an example PHP application designed to be intentionally vulnerable to web attacks.

Purpose:

- **Testing**: It's made for testing with Acunetix, a web security tool.
- **Learning**: It helps you see how developer mistakes and poor configurations can allow someone to hack into a website.

This site is a safe place to learn about and practice web security.

All the possible attacks that can be tested here are:

1. SQL Injection
2. Cross site scripting (XSS)
3. Cross-Site request forgery
4. Man-in-the-Middle attack

Implementing the attack:

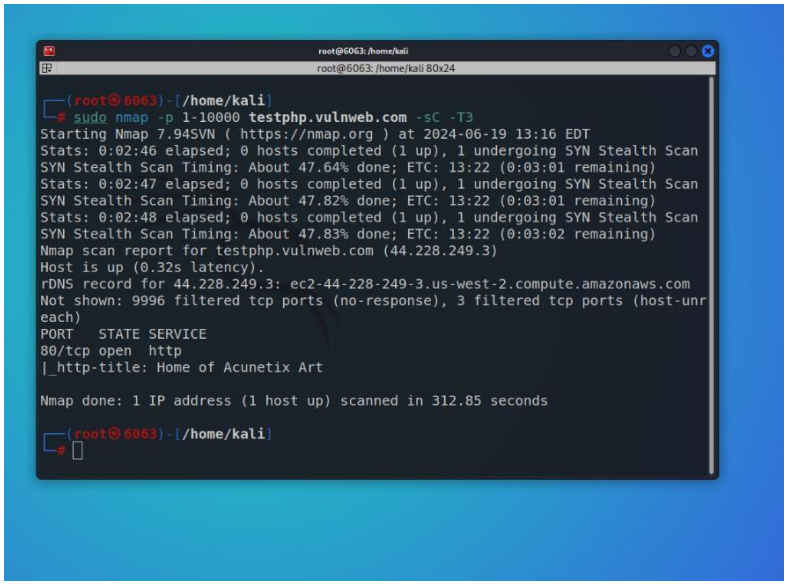
Task 1: Find all the ports that are open on the website http://testphp.vulnweb.com/

Requirements: Operating System, nmap, stable internet connection.

Step 1: Running the nmap scan for finding potential loopholes for entry pointsCommand:

Sudo nmap –p 1-10000 testphp.vulnweb.com -sC -T3

POC:



Port Scanning Findings:

```
PORT  STATE SERVICE
80/tcp open  http
|_http-title: Home of Acunetix Art
```

Vulnerability:

Cryptographic Failure (Severity: Medium)

The site does not use HTTPS, which is a more secure communication protocol than HTTP.

Without HTTPS, data transmission is not encrypted, making it possible for attackers to intercept and read the information being sent. This vulnerability increases the risk of man-in-the-middle attacks, which can be highly problematic for organizations.

The attacks which can be possible

1. Man-in-the-middle-attack
2. Network tracerouting
3. Packet sniffing

Later in task 3 we will try to understand how the packets could be sniffed over unsecure http traffic.

Task 2: Brute force the website http://testphp.vulnweb.com/ and find the directories that are present in the website.

Requirements: Operating System, Dir buster or go buster, stable internet connection

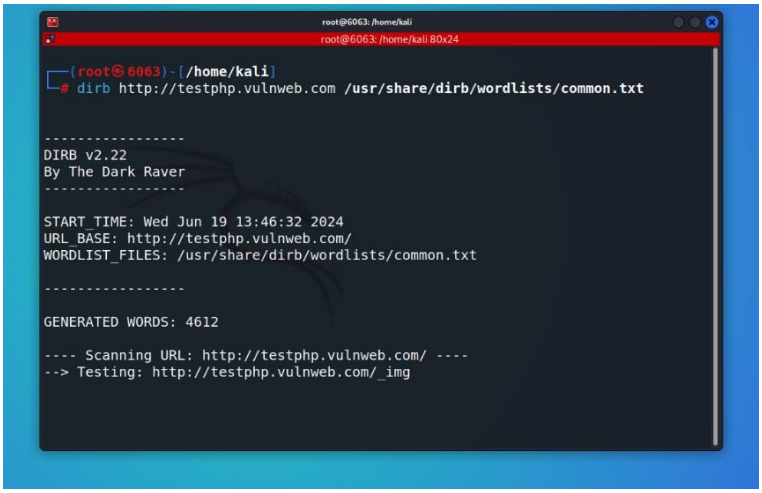
Step 1: Brute forcing the available directories using drib tool

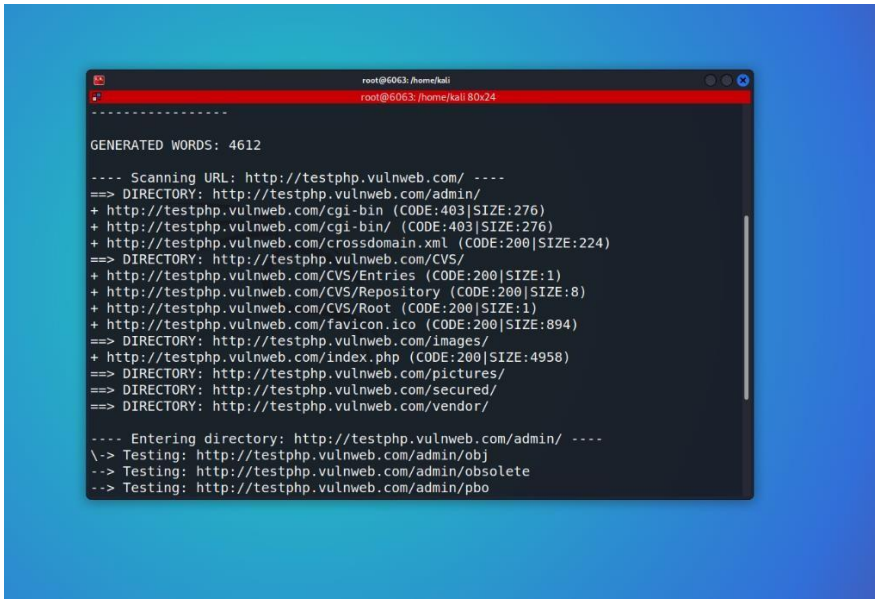
Dirb is a command-line tool used in web security assessments to discover hidden web content

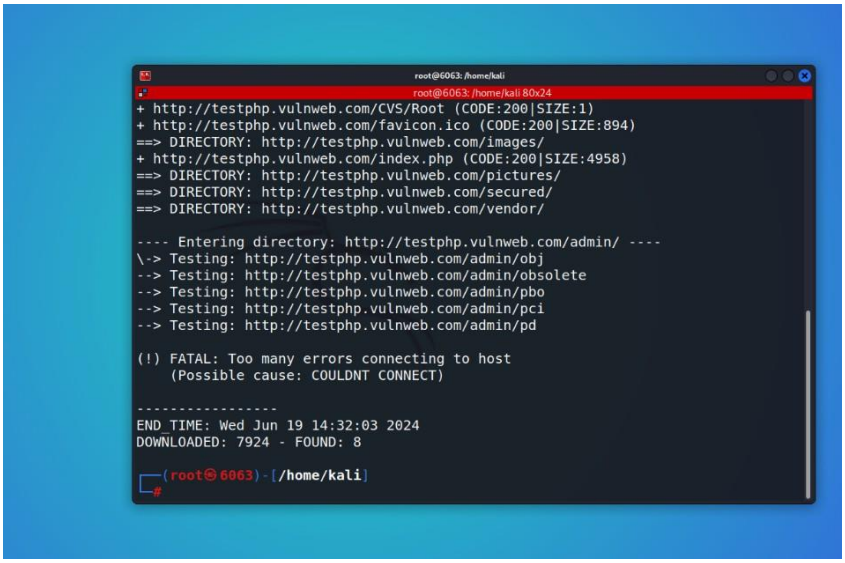
Command:

dirb http://testphp.vulnweb.com --wordlist=usr/share/dirb/common.txt

POC:







Traversing all the paths of testphp.vulnweb.com

Access to the ADMIN login panel:

Got the access to the database

(Severity : Critical)

==>DIRECTORY: http://testphp.vulnweb.com/admin/

Forbidden by the WAF Firewall:

+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)

+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)

Status code 200 OK paths:

+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)

Reveals information about nginx server and it's version (nginx/1.19.0) (Severity=Low-Medium)

Access to the directories available at website like

1. Root
2. Entries
3. Repository
4. Favicon.ico
5. Index.php

(Severity: High)

```
==>  DIRECTORY:  http://testphp.vulnweb.com/CVS/

+   http://testphp.vulnweb.com/CVS/Entries    (CODE:200|SIZE:1)

+   http://testphp.vulnweb.com/CVS/Repository    (CODE:200|SIZE:8)

+   http://testphp.vulnweb.com/CVS/Root   (CODE:200|SIZE:1)

+   http://testphp.vulnweb.com/favicon.ico    (CODE:200|SIZE:894)

  ==>  DIRECTORY:  http://testphp.vulnweb.com/images/

+   http://testphp.vulnweb.com/index.php   (CODE:200|SIZE:4958)

==>    DIRECTORY:   http://testphp.vulnweb.com/pictures/
==>    DIRECTORY:   http://testphp.vulnweb.com/secured/
==>  DIRECTORY:  http://testphp.vulnweb.com/vendor/

END_TIME: Wed Jun 19 14:32:03 2024
DOWNLOADED: 7924 - FOUND: 8
```

Task 3: Make a login in the website http://testphp.vulnweb.com/ and intercept the network traffic using Wireshark and find the credentials that were transferred through the network.

Requirements: Operating System, Wireshark, Stable Internet Connection, basic understanding of Wireshark and packet capturing.

Wireshark is a tool that helps you see what's happening on a computer network.

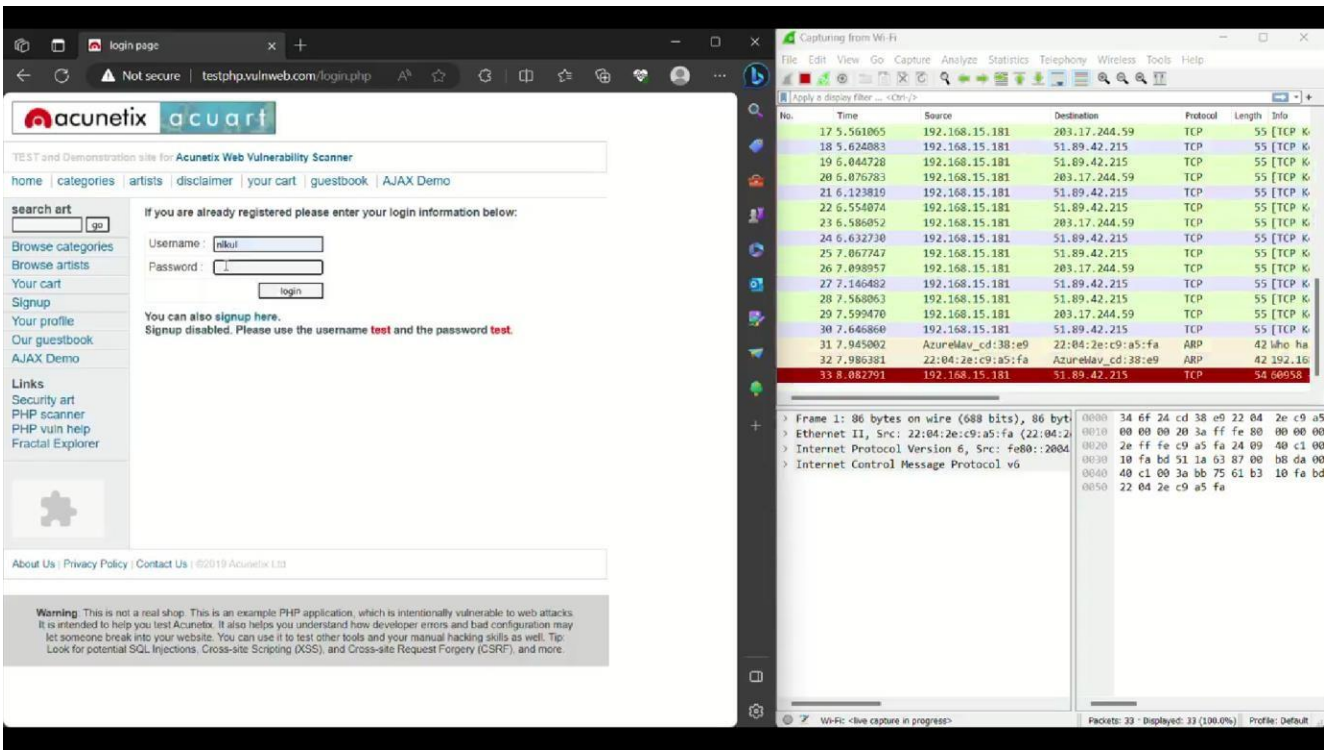
It captures all the data passing through and lets you look closely at each piece of information, like a detective examining clues. You can see where data comes from, where it's going, and what kind of data it is, like emails or web pages

This website is prone to man-in-the-middle attack. The attacker can use this vulnerability to sniff the packets transfer over the http protocol.

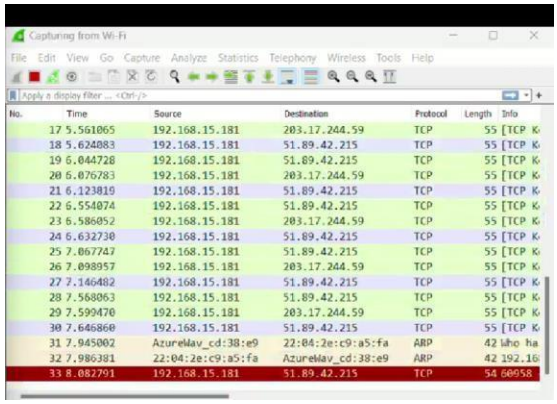
However, here is the POC

POC:

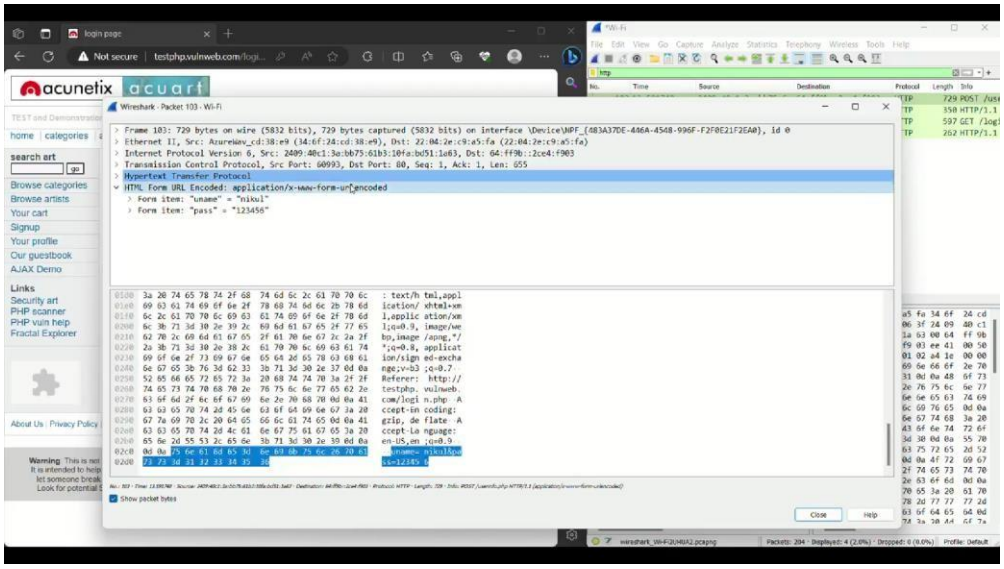
Step1: on the signup page and try to login with default credentials that are providedbelow.



Step2: Make sure to turn on the Wireshark to capture the packets before pressing login.



Step3: Analyze the captured packets and apply filter for specific http packets.



"In this scenario, the credentials we used to log in are exposed and easily readable within thepacket."

Resources Used:

1. Operating System (Windows or Linux) Linux Preferred
2. Wireshark (Packet Sniffer)
3. Nmap (Network mapper)
4. Internet
5. OSINT (Open-Source Intelligence gathering)