

SHADOW FOX

REPORT ON BEGINNER TASK

NAME:GANESH P

BATCH:B1

DOMAIN:CYBER SECURITY

BEGINNER LEVEL

1. Find all the ports that are open on the website <http://testphp.vulnweb.com>
2. Brute force the website <http://testphp.vulnweb.com/> and find the directories that are present that are present in the website
3. Make a login in the website <http://testphp.vulnweb.com/> and intercept the network traffic using wire shark and find the credentials that were transferred through the network

SHADOW FOX

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

NMAP:

NMAP(network mapper)is a powerful open sources tool used for network discovery and security auditing. It is widely utilized by network structures,discover devices,and identify open ports and service.

SOME KEY FEATURES AND FUNCTIONALITIES OF NMAP:

1. **Host directory:** identifies active devices on a network
2. **Port scanning:** determines which ports are open on a targets devices
3. **Service detection:** identifies the services and their version running on open ports

BASIC USAGE:

- **SCAN A SINGLE HOST:** 'nmap <hostname or ip>
- **SCAN A RANGE OF IPS:**'nmap <range>
- **SCAN SPECIFIC PORTS:**'NMAP -P <PORTS1,PORTS2,.....>
<host name or ip>

OUTPUT:

```
(kali㉿kali)-[~]  
$ nmap testphp.vulnweb.com  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 00:56 EDT  
Nmap scan report for testphp.vulnweb.com (44.228.249.3)  
Host is up (0.34s latency).  
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 38.67 seconds
```

MITIGATION:

1. FIREWALLS AND INTRUSION DETECTION SYSTEM(IDS):

Properly configure firewall to block unauthorized scanning activities. restrict access to critical ports and services to known IP addresses only

2. NETWORK SEGMENTATION:

Segment your network to isolate sensitive systems and limit the spread of a potential attack. Use VLANs and subnets to create boundaries within your network

3. HONEYPOTS AND HONEYNETS:

Set up honeypots to detect and analyze unauthorized scanning attempts. Honeypots can provide early warning and valuable insights into the methods attackers use.

4. SERVICE HARDENING:

Turn off services and ports that are not needed. This reduces the attack surface and makes it more difficult for attackers to find entry points.

SHADOW FOX

2. BRUTE FORCES THE WEBSITE <http://testphp.vulnweb.com/>

And find the directories that are present in the website.

TOOLS USED:dirb

COMMAND LINE:Dirb <http://vulnweb.com/>

DRIB:

Drib is a command line based web content scanner.its used to find hidden web object such as directories,files and other potential entry points on a web server.

KEY FEATURES:

1. World list based scanning:

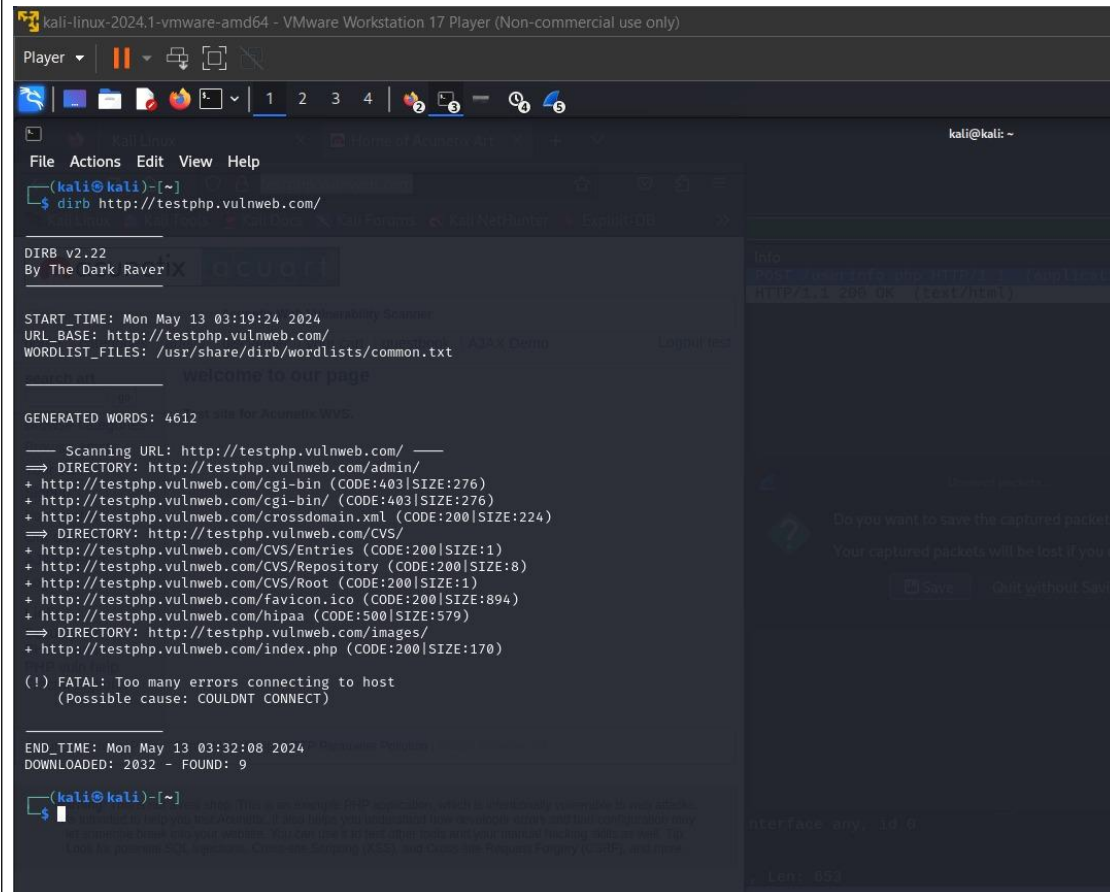
Drib uses word list to perform brute force attacks on web serves.these word lists contains common directory and file names

2. RECURSIVE SCANNING:

Drib can recursively scan found directories to discover nested directories and files.

3. EXTENSIONS SCANNING:

It can append different file extension to names in the word list to find hidden files(eg.php,html,txt)

OUTPUT:

MITIGATION:

❖ PROPER CONFIGURATION AND HARDENING:

Ensues that directory listing is disabled in your web server configuration .this prevents attacker from easily viewing the contents of directories.

❖ **OBSCURE SENSITIVE INFORMATION:**

Move sensitive files and directories to non public location and give them non obvious names to reduce their discover ability

❖ **IMPLEMENT ACCESS CONTROLS:**

Protect sensitive areas of the websites with proper authentication mechanisms.

❖ **MONITORING AND LOGGING:**

Regularly monitor web server access logs for unusual or suspicious activity that could indicates an attempted or successful scan

❖ **CONTROL SECURITY POLICIES:**

Use a WAF to block malicious traffic and prevent automated tools from performing directory scans.

❖ **SECURITY TESTING AND AUDITS:**

Conduct regular security testing and audits,including penetration testing ,to identify and remediate vulnerabilities before they can be exploited.

SHADOW FOX

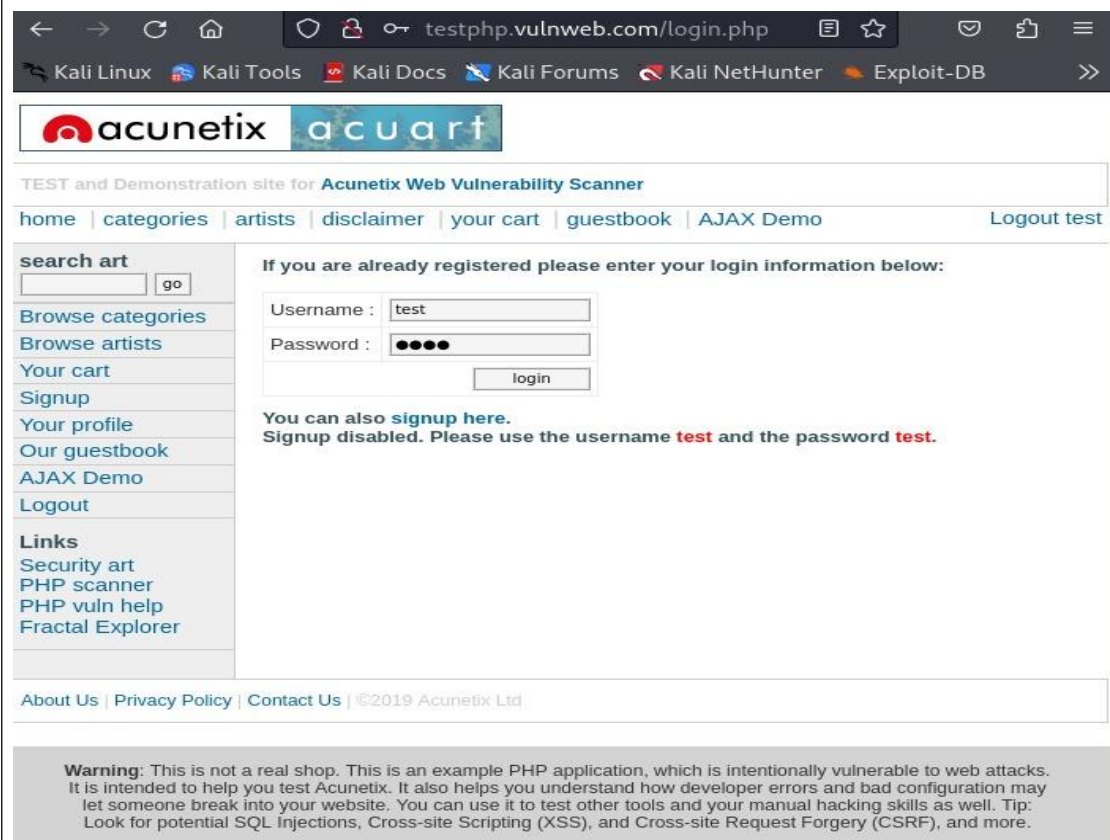
3. Make a login in the websites <http://testphp.vulnweb.com/> and intercept the network traffic using Wireshark and find the credentials that were transferred through the network

TOOL USED: Wireshark in Kali Linux

Input given : USER NAME: "test"

Password : "test"

OUTPUT:



← → ↻ 🏠 🔒 🔑 testphp.vulnweb.com/login.php 📄 ☆ 📧 📁 ≡

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB >>

acunetix **acuart**

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)
[Logout](#)

Links
[Security art](#)
[PHP scanner](#)
[PHP vuln help](#)
[Fractal Explorer](#)

If you are already registered please enter your login information below:

Username :
Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Restore Session x user info +

testphp.vulnweb.com/userinfo.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

acunetix **acuart**

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home categories artists disclaimer your cart guestbook AJAX Demo Logout test

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

ganeshP (test)

On this page you can visualize or edit your user information.

Name:	ganeshP
Credit card number:	347294893827353502
E-Mail:	ganesh@12134
Phone number:	1234896352
Address:	scotland

update

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Info	Sc
26	6.080548925	Application Data	32
27	6.082040640	Application Data	10
28	6.082715400	443 → 41150 [ACK] Seq=1036 Ack=1498 Win=65535 Len=0	34
29	6.588734676	443 → 41150 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460	34
30	6.588774965	41150 → 443 [RST] Seq=1 Win=0 Len=0	10
31	9.233818214	[TCP Previous segment not captured] POST /userinfo.php HTTP/1...	10
32	9.234569528	80 → 49220 [ACK] Seq=1 Ack=650 Win=65535 Len=0	41
33	11.230838754	38166 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSV...	10
34	11.259447855	38172 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSV...	10
35	11.302395557	Standard query 0xe602 A www.acunetix.com	10
36	11.432879342	Standard query response 0xe602 A www.acunetix.com A 104.18.17...	10

```

\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
[HTTP request 1/1]
[Response in frame: 59]
File Data: 109 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "username" = "ganeshP"
  Form item: "ucc" = "347294893827353502"
  Form item: "uemail" = "ganesh@12134"
  Form item: "uphone" = "1234896352"
  Form item: "uaddress" = "scotland"
  Form item: "update" = "update"
  
```

MITIGATIONS:

❖ SECURE NETWORK DESIGN:

Segments the network to isolated sensitive traffic. use vlans or separate physical network to keep sensitive data away from general traffic.

❖ ACCESS CONTROLS:

Restrict the use of wire shark to authorized personnel only. ensure that only network administrators and security professionals have access to the tools

❖ MONITORING AND LOGGING :

Keep track of who is using wireshark and for what purpose. Maintain logs of wireshark sessions and analyze them regularly to detect any unauthorized use

❖ USER TRAINING:

Train users on the importance of network security and the risks associated with network protocols analyzers.

CONCLUSION

The conclusion emphasizes the critical importance of a proactive and holistic approach to safeguarding digital assets .with the increasing sophistication of cyber threats,organization and individuals must prioritize continuous education ,robust security policies,and cutting edge technologies to protect against breaches.

Cyber security is not solely a technological challenges but also a human one ,requiring awareness ,vigilance and collaboration across all level of an organization. Effective cybersecurity strategies involve regular risk assessments,incident response planning and adherence to best practise and regulatory requirements.