

TASK LEVEL(Beginner)

TASK-1

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

**Step-1:-Install Nmap:First, we need to install Nmap from the website
<https://nmap.org/download.html>.**

**Step-2:-Run Nmap Scan: Open a terminal or command prompt and use
the `nmap testphp.vulnweb.com` or `nmap --top-ports n testphp.vulnweb.com` command to perform
a port scan on the website.Then we will get all the open ports of the
website.**

```
(root@kali)-[/home/priyanshu]
# nmap testphp.vulnweb.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-15 17:37 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.46s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
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 60.72 seconds
```

OR

```
root@kali: /home/priyanshu
# nmap --top-ports 20 testphp.vulnweb.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-07 00:37 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.38s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
DNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    open  http
110/tcp   filtered pop3
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   filtered imap
443/tcp   filtered https
445/tcp   filtered microsoft-ds
993/tcp   filtered imaps
995/tcp   filtered pop3s
1723/tcp  filtered pptp
3306/tcp  filtered mysql
3389/tcp  filtered ms-wbt-server
5900/tcp  filtered vnc
8080/tcp  filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 7.70 seconds
```

TASK-2

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

Step-1:-Set Up Burp Suite:Download and Install the Burp Suite Suite from the official PortSwigger website then Install it on your machine.

Step-2:-Configure Browser to Use Burp Suite Proxy

Set Up Proxy:

(a)Open Burp Suite and go to the "Proxy" tab.

(b) Click on "Options" and ensure that the proxy listener is set to 127.0.0.1:8080

Configure Browser:

(a) Configure your web browser to use Burp Suite as a proxy (127.0.0.1:8080). This can be done in the network settings of the browser.

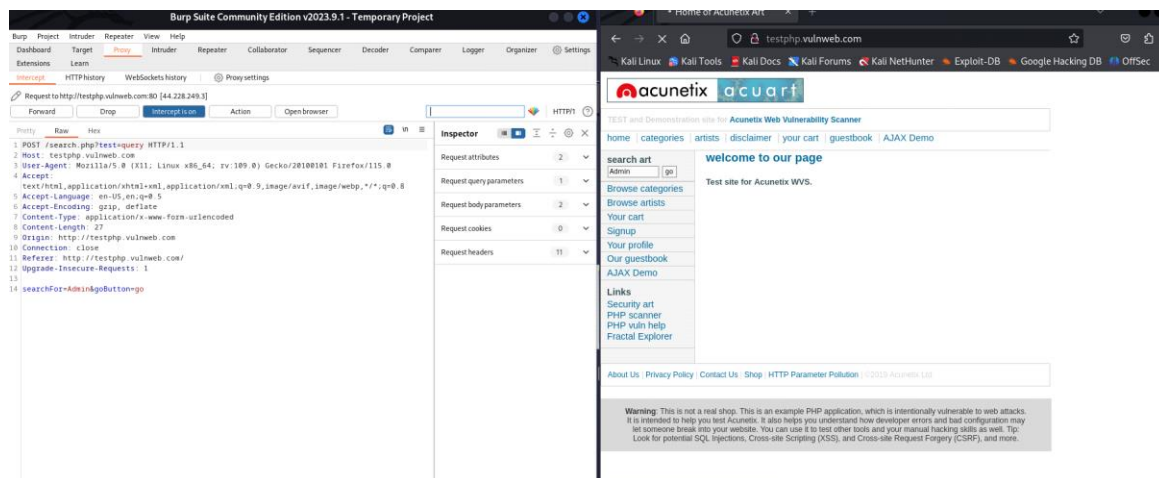
(b) Install the Burp Suite CA certificate in your browser to avoid SSL/TLS issues.

Step-3:- Intercept Traffic

Enable Interception:

(a) In Burp Suite, go to the "Proxy" tab and ensure "Intercept is on". Visit the Target Website:

(b) Open your configured browser and navigate to <http://testphp.vulnweb.com>. You should see the HTTP request being intercepted in Burp Suite.



Step-4:- Send Request to Intruder and Right-click on the request and select Send to Intruder. then Clear any pre-selected positions by clicking "Clear". & Highlight the part of the URL you want to brute force. Click "Add" to mark the highlighted section as the position to attack.

1 x 2 x +

Positions Payloads Resource pool Settings

Choose an attack type Start attack

Attack type: Cluster bomb

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: ☒ Update Host header to match target

1 POST /search.php?test=query HTTP/1.1

2 Host: testphp.vulnweb.com

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 27

9 Origin: http://testphp.vulnweb.com

10 Connection: close

11 Referer: http://testphp.vulnweb.com/

12 Upgrade-Insecure-Requests: 1

13

14 searchFor=\$Admin\$&goButton=\$go\$

2 payload positions

2 highlights Length: 534

Step-5:- Set Up Payload:Go to the "Payloads" sub-tab. and then create the two wordlist. by clicking on the payload 1 and then payload 2.

?
Payload sets
Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:

1

Payload count:
 11

Payload type:

Simple list

Request count:
 55

?
Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load...

Remove

Clear

Deduplicate

Add

username

abc

linux

root

admin

pass

password

123

xyz

ad

Enter a new item

Add from list ... [Pro version only]

?
Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Up

Enabled	Rule

(Payload-1)

1 x 2 x +

Positions Payloads Resource pool Settings

Payload sets Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 5
Payload type: Simple list Request count: 55

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load...

Remove

Clear

Deduplicate

pass1

password

door

root

linux

Add

Enter a new item

Add from list ... [Pro version only]

(Payload-2)

Step-6:-Run the attack by clicking on "start attack" button.

2. Intruder attack of http://testphp.vulnweb.com - Temporary attack - Not saved to proje...

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

request ^	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
1	username	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	4996	
2	abc	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	4999	
3	liunux	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	4994	
4	root	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	4997	
5	admin	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	4995	
6	pass	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	4996	
7	password	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	4995	
8	123	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	4999	
9	xyz	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	4994	
10	ad	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	6476	
11	alias	pass1	200	<input type="checkbox"/>	<input type="checkbox"/>	4996	

Finished

Step-7:-Click on Target. for access the directory.

Step-8:-And expand the directory for access more data.

The image shows two side-by-side screenshots. The left screenshot is from Burp Suite, displaying the 'Intruder' tab. It shows a list of requests and responses for the target URL 'http://testphp.vulnweb.com'. The 'Request' column shows a GET request to '/AJAX/index.php'. The 'Response' column shows a 200 status code. The 'Inspector' tab is also visible, showing the raw HTTP request and response details. The right screenshot is from a web browser (Kali Linux) showing the 'testphp.vulnweb.com' website. The browser's address bar shows the URL. The page content includes a search bar, a 'welcome to our page' message, and a list of categories and artists. A warning message at the bottom states: '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.'

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.

Step-1:- Set Up Wireshark:Download and Install Wireshark from the official Wireshark website.Install it on your machine.and then open it.

Step-2:-Capture Network Traffic:Select Network Interface:In Wireshark, choose the network interface that your computer is using to connect to the internet & Click on the selected interface and press the "Start capturing packets".

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
248	10.982992	2405:200:1611:1731:...	2409:4085:8db7:57de...	TCP	74	443 → 52361 [ACK]
249	10.982992	2405:200:1611:1731:...	2409:4085:8db7:57de...	TLSv1.2	109	Application Data
250	10.983141	2409:4085:8db7:57de...	2405:200:1611:1731:...	TCP	74	52361 → 443 [ACK]
251	11.014741	2405:200:1611:1731:...	2409:4085:8db7:57de...	TCP	74	443 → 52361 [ACK]
252	11.143331	2405:200:1611:1731:...	2409:4085:8db7:57de...	TLSv1.2	413	Application Data
253	11.143331	2405:200:1611:1731:...	2409:4085:8db7:57de...	TLSv1.2	105	Application Data
254	11.143462	2409:4085:8db7:57de...	2405:200:1611:1731:...	TCP	74	52361 → 443 [ACK]
255	11.441723	2409:4085:8db7:57de...	2606:4700:9640:fe72...	TCP	75	52275 → 443 [ACK]
256	11.598634	2606:4700:9640:fe72...	2409:4085:8db7:57de...	TCP	86	443 → 52275 [ACK]
257	12.140214	2409:4085:8db7:57de...	2405:200:1611:1731:...	TCP	1418	52361 → 443 [ACK]

> Frame 1: 660 bytes on wire (5280 bits), 660 by
 > Ethernet II, Src: AzureWaveTec_ad:c4:9d (50:5a
 > Internet Protocol Version 6, Src: 2409:4085:8c
 > Transmission Control Protocol, Src Port: 52367
 > Transport Layer Security

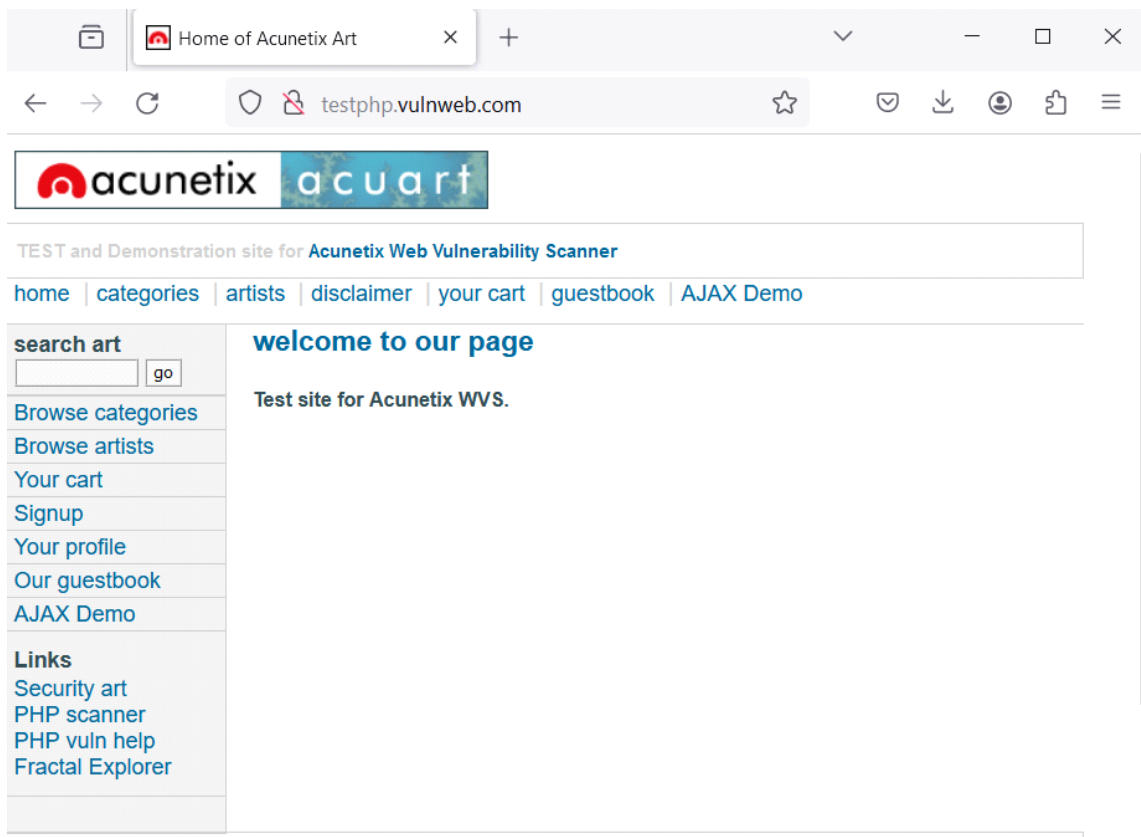
```

0000 3a 19 1b 8f a0 87 50 5a 65 ad c4 9d 86
0010 1d f2 02 5e 06 3f 24 09 40 85 8d b7 57
0020 e5 51 47 2a e2 92 00 64 ff 9b 00 00 00
0030 00 00 cc 4f c5 de cc 8f 01 bb 54 0f c8
0040 36 15 50 18 03 fe 74 22 00 00 17 03 03
0050 00 00 00 00 00 00 04 ac d4 04 dc fd 01
0060 7a cf 98 16 3f 8b 54 27 ad 00 88 64 9d
0070 06 62 d5 b3 c8 52 74 08 8a ef 3a bf 2e
0080 1f 81 ab c5 90 fb fe e6 6c 24 3c c3 d3
0090 7e e9 f2 cd 3a b1 6a 72 b8 b6 b4 42 eb
00a0 8d 69 99 ba 8d 12 6c c8 06 93 29 48 a8
00b0 f6 d1 a8 ed 70 46 45 d7 3c 2f 8a 33 a4
00c0 1d 1f 7d 57 2d 22 a3 fd 5d 57 37 cc 0e
00d0 a8 da 23 32 bc 4a 58 2a b0 a0 08 6b c9
  
```

Step-3: Perform Login on Target Website: Open web browser and navigate to <http://testphp.vulnweb.com>. Navigate to Login Page then Click on the "Login" link or navigate to the login page directly. Enter Credentials, Enter a username and password in the login form. then Click on the "Login" button to submit the form.

Username: root

Password: admin



Step-4:-Analyze Network Traffic**Filter Traffic:**In Wireshark, apply a filter to show only HTTP traffic by typing http in the filter bar and pressing Enter.

Step-5:-Find Login Request:Look through the captured packets to find the HTTP POST request that was sent when you submitted the login form. Identify the packet by looking for a POST request .

Examine Packet Details:Click on the identified packet to see its details. In the packet details pane, expand the Hypertext Transfer Protocol section to view the form data. Look for the form data containing the username and password fields.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.

Time

Source

Destination

Protocol

Length

Info

2176	95.088379	2409:4085:8db7:57de...	2600:1901:0:38d7::	HTTP	377	GET /canonical.ht
2180	95.208523	2600:1901:0:38d7::	2409:4085:8db7:57de...	HTTP	372	HTTP/1.1 200 OK
2183	95.242677	192.168.77.29	34.107.221.82	HTTP	359	GET /success.txt?
2184	95.242854	2409:4085:8db7:57de...	2600:1901:0:38d7::	HTTP	379	GET /success.txt?
2188	95.328078	34.107.221.82	192.168.77.29	HTTP	270	HTTP/1.1 200 OK
2190	95.328078	2600:1901:0:38d7::	2409:4085:8db7:57de...	HTTP	290	HTTP/1.1 200 OK
2248	107.184744	2409:4085:8db7:57de...	64:ff9b::2ce4:f903	HTTP	613	POST /userinfo.ph
2252	107.519638	64:ff9b::2ce4:f903	2409:4085:8db7:57de...	HTTP	350	HTTP/1.1 302 Foun
2253	107.528557	2409:4085:8db7:57de...	64:ff9b::2ce4:f903	HTTP	483	GET /login.php HT
2258	108.169579	64:ff9b::2ce4:f903	2409:4085:8db7:57de...	HTTP	82	HTTP/1.1 200 OK

> Frame 2248: 613 bytes on wire (4904 bits), 613

> Ethernet II, Src: AzureWaveTec_ad:c4:9d:5a

> Internet Protocol Version 6, Src: 2409:4085:8d

> Transmission Control Protocol, Src Port: 52435

> Hypertext Transfer Protocol

> HTML Form URL Encoded: application/x-www-form

> Form item: "uname" = "root"

> Form item: "pass" = "admin"

0000 3a 19 1b 8f a0 87 50 5a 65 ad c4 9d 86

0010 12 b5 02 2f 06 3f 24 09 40 85 8d b7 57

0020 e5 51 47 2a e2 92 00 64 ff 9b 00 00 00

0030 00 00 2c e4 f9 03 cc d3 00 50 ba 06 a4

0040 53 b5 50 18 00 fd a0 56 00 00 50 4f 53

0050 75 73 65 72 69 6e 66 6f 2e 70 68 70 20

0060 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20

0070 74 70 68 70 2e 76 75 6c 6e 77 65 62 2e

0080 8d 0a 55 73 65 72 2d 41 67 65 6e 74 3a

0090 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69

00a0 77 73 20 4e 54 20 31 30 2e 30 3b 20 57

00b0 34 3b 20 78 36 34 3b 20 72 76 3a 31 32

00c0 29 20 47 65 63 6b 6f 2f 32 30 31 30 30

00d0 20 46 69 72 65 66 6f 78 2f 31 32 35 2e

login page

testphp.vulnweb.com/login.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home categories artists disclaimer your cart guestbook AJAX Demo

search art go

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

Username : Password : login

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

Links Security art PHP scanner PHP vuln help Fractal Explorer

About Us | Disclaimer | Contact Us | Privacy Policy | Terms of Use