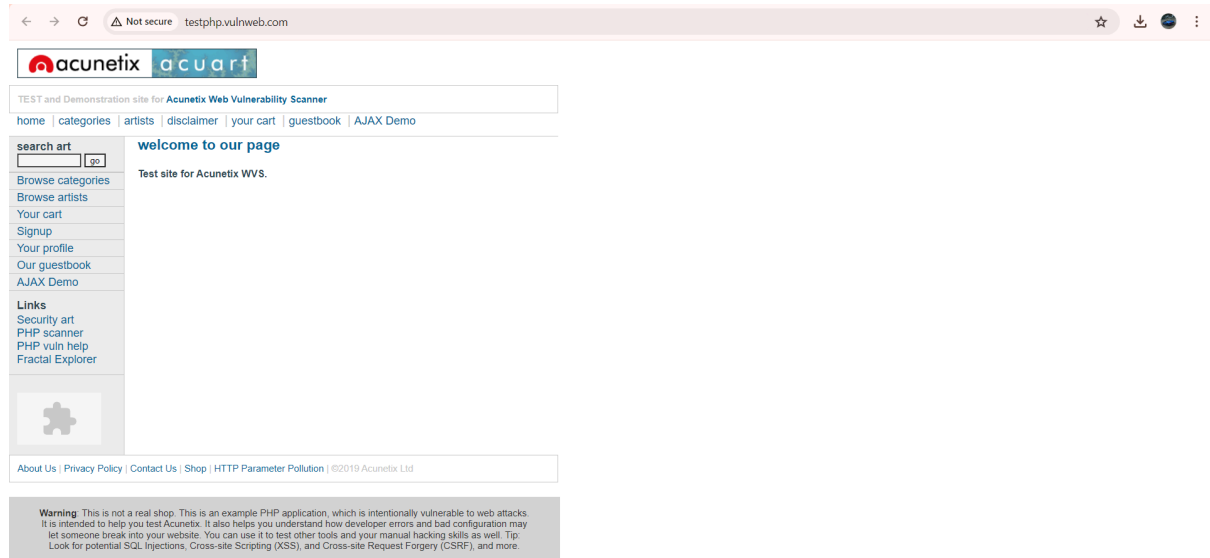


Assignment 1

Step 1 -

The demo site is <http://testphp.vulnweb.com/>



Step 2: Perform footprinting and reconnaissance -

Using nslookup find the ip address of the target and use whois command to get further details

```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nslookup http://testphp.vulnweb.com/
Server:      192.168.139.93
Address:     192.168.139.93#53

** server can't find http://testphp.vulnweb.com/: NXDOMAIN

(root@kali)-[/home/kali]
# nslookup testphp.vulnweb.com
Server:      192.168.139.93
Address:     192.168.139.93#53

Non-authoritative answer:
Name:   testphp.vulnweb.com
Address: 44.228.249.3

(root@kali)-[/home/kali]
# whois 44.228.249.3

#
# ARIN WHOIS data and services are subject to the Terms of Use
```

The ip address is 44.228.249.3

```
root@kali: /home/kali
File Actions Edit View Help

# start

NetRange:      44.192.0.0 - 44.255.255.255
CIDR:          44.192.0.0/10
NetName:       AMAZO-4
NetHandle:     NET-44-192-0-0-1
Parent:        NET44 (NET-44-0-0-0-0)
NetType:       Direct Allocation
OriginAS:
Organization:  Amazon.com, Inc. (AMAZO-4)
RegDate:       2019-07-18
Updated:        2019-07-18
Ref:           https://rdap.arin.net/registry/ip/44.192.0.0

OrgName:       Amazon.com, Inc.
OrgId:         AMAZO-4
Address:       Amazon Web Services, Inc.
Address:       P.O. Box 81226
City:          Seattle
StateProv:     WA
PostalCode:    98108-1226
Country:       US
RegDate:       2005-09-29
Updated:       2022-09-30
```

```
root@kali: /home/kali
File Actions Edit View Help

Country:       US
RegDate:       2005-09-29
Updated:       2022-09-30
Comment:       For details of this service please see
Comment:       http://ec2.amazonaws.com
Ref:           https://rdap.arin.net/registry/entity/AMAZO-4

OrgAbuseHandle: AEAS-ARIN
OrgAbuseName:   Amazon EC2 Abuse
OrgAbusePhone:  +1-206-555-0000
OrgAbuseEmail:  abuse@amazonaws.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/AEAS-ARIN

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName: AWS RPKI Management POC
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-rpki-routing-poc@amazon.com
OrgRoutingRef:  https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgNOCHandle:  AAN01-ARIN
OrgNOCHandle:  Amazon AWS Network Operations
OrgNOCHandle:  +1-206-555-0000
OrgNOCHandle:  amzn-noc-contact@amazon.com
OrgNOCHandle:  https://rdap.arin.net/registry/entity/AAN01-ARIN

OrgRoutingHandle: IPROU3-ARIN
```

```
root@kali: /home/kali
File Actions Edit View Help

OrgAbuseHandle: AEAS-ARIN
OrgAbuseName:   Amazon EC2 Abuse
OrgAbusePhone:  +1-206-555-0000
OrgAbuseEmail:  abuse@amazonaws.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/AEAS-ARIN

OrgNOCHandle:  AAN01-ARIN
OrgNOCHandle:  Amazon AWS Network Operations
OrgNOCHandle:  +1-206-555-0000
OrgNOCHandle:  amzn-noc-contact@amazon.com
OrgNOCHandle:  https://rdap.arin.net/registry/entity/AAN01-ARIN

# end

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
```

Step 3: Using Nmap, a network scanning tool -

```
(root@kali)-[/home/kali]
# nmap testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 14:34 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.044s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.co
m
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 17.05 seconds
```

After using nmap it is clearly found that one port is open.