Grab Digital Foot-printing & its countermeasures

Ethical Hacking | Web application footprinting

CDAC, Noida

CYBER GYAN VIRTUAL INTERNSHIP PROGRAM

Submitted By:

KARTIK PAREEK

Project Trainee, (July-August) 2024

BONAFIDE CERTIFICATE

This is to certify that this project report entitled **Grab Digital Foot-printing & its Countermeasures (at least 4 tools)** submitted to CDAC Noida, is a Bonafede record of work done by **KARTIK PAREEK** under my supervision from **18 Sept 2024 to 6 Oct 2024**

Declaration by Author(s)

This is to declare that this report has been written by me/us. No part of the report is plagiarized from other sources. All information included from other sources has been duly acknowledged. I/We aver that if any part of the report is found to be plagiarized, I/we shall take full responsibility for it.

Name of Author(S): KARTIK PAREEK

TABLE OF CONTENTS

Table of Contents

ACKNOWLEDGEMENT

Overview of Digital Footprinting

Digital footprinting is the process of gathering information about a target, typically in the context of cybersecurity or ethical hacking, by utilizing publicly available data. This non-intrusive method helps identify a target's digital presence, including domain information, IP addresses, network infrastructure, emails, subdomains, and any other publicly accessible data. The primary objective is to build a detailed profile of the target, revealing potential vulnerabilities without engaging in direct interaction. Through tools like WHOIS, Nmap, TheHarvester, and wireshark, attackers can uncover weaknesses in the target's infrastructure, which can later be exploited. Ethical hackers and penetration testers use digital footprinting as a foundational step in vulnerability assessment and penetration testing (VAPT) to discover and mitigate these security risks. Properly controlling a company's digital footprint can significantly reduce exposure to threats, making it a critical part of any organization's cybersecurity strategy.

Types of Footprinting

Footprinting in cybersecurity is typically categorized into two types: passive and active footprinting.

1. Passive Footprinting: This involves gathering information about a target without directly interacting with the target's systems. It relies on publicly accessible resources such as search engines, social media, domain registration databases (WHOIS), and internet services like wireshark. Passive footprinting is stealthy, minimizing the risk of detection, as it does not engage with the target's infrastructure.
2. Active Footprinting: In contrast, active footprinting involves directly interacting with the target's network to obtain information. This can include techniques like network scanning, port scanning, or engaging with the target's systems using tools like Nmap or Netcat. Although it yields more detailed information, active footprinting runs the risk of being detected by the target's security mechanisms, such as firewalls or intrusion detection systems (IDS).

Grab Digital Foot-printing & its countermeasures

Introduction

Digital footprinting refers to the process of gathering publicly available information about a target, such as an individual, organization, or website, without direct interaction. In cybersecurity, footprinting is a crucial step in understanding a target's network, identifying vulnerabilities, and assessing risks. Ethical hackers and penetration testers can map a target's digital presence by using techniques like WHOIS lookup, Nmap scans, and Wireshark packet sniffing. This report covers the methodologies and tools employed in footprinting, uncovered vulnerabilities, and countermeasures to secure digital assets.

PROBLEM STATEMENT:

Gather the Digital Footprinting and provide its countermeasures.

Learning Objective

Understand Digital Footprinting: Learn how attackers gather publicly available information about a target, including domain details, services, and sensitive data.

Master Footprinting Tools: Gain hands-on experience using Kali Linux tools such as WHOIS, Wireshark, Google Dorking, Netcraft, and Nmap to collect data from websites.

Identify Vulnerabilities: Learn how to uncover common vulnerabilities like open ports, exposed subdomains, and sensitive files that can be exploited by attackers.

Implement Countermeasures: Develop strategies to protect against digital footprinting by using privacy settings, server hardening, and regularly monitoring the organization's digital presence.

Improve Security Awareness: Understand the importance of securing an organization's digital footprint to prevent cyberattacks, and explore real-world scenarios where these vulnerabilities were exploited.

APPROACH:

This section provides an overview of the tools and infrastructure and a diagram illustrating the environment where the assessment took place.

1.1 Tools & Technologies Used

- Operating System: Kali Linux 2024.1
- Tools:
    1. WHOIS: For retrieving domain information.
    2. Nmap: For network scanning and port detection.
    3. Google Dorking: For finding publicly accessible files and sensitive data.
    4. Netcraft: For analyzing infrastructure and uptime.
    5. Wireshark: For network sniffing and passive footprinting.
    6. Header Check: Giving information about content-encoding.
    7. Traceroutes with MTR: Hops are required to reach the web server.

1.2 Infrastructure Overview

- Target Website: http://testphp.vulnweb.com/
- Attacker Machine: Kali Linux
- Network Environment: The assessment is performed on a publicly accessible website.
- Key Components:
    - Server: Hosts the website and services.
    - Firewall: Protects the web server from external threats (hypothetical).
    - Attacker Machine: Kali Linux VM with tools for footprinting.

IP Address: **44.228.249.3**

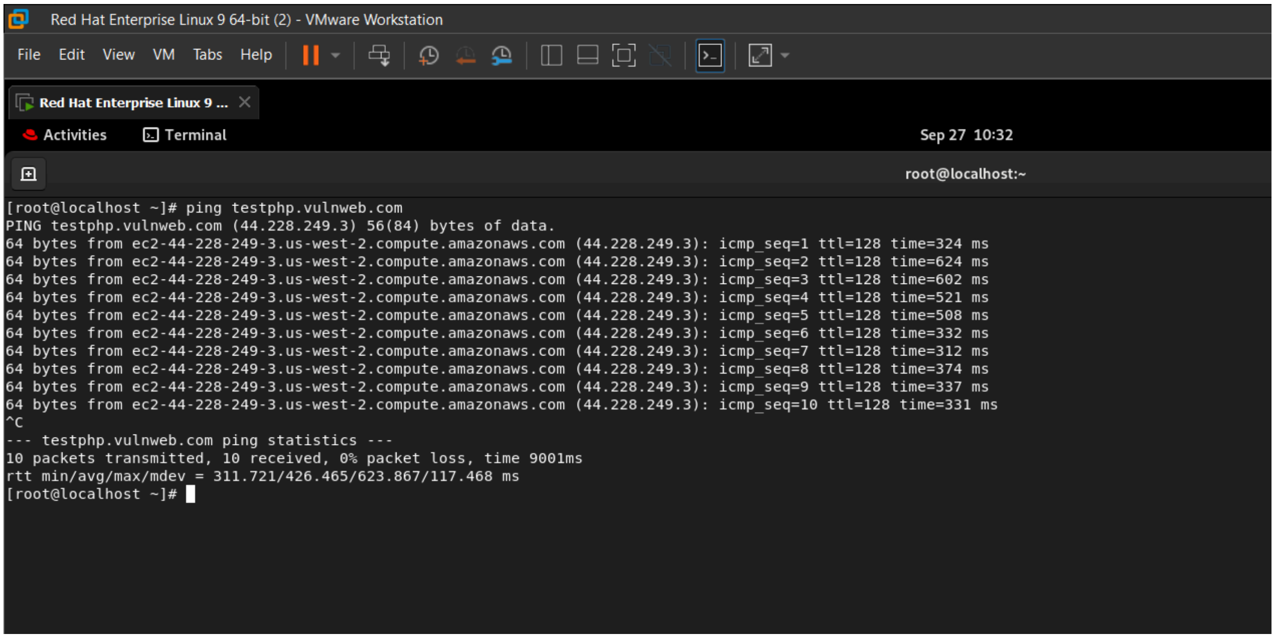
Attacker Machines: Kali Linux, Rhel 9, Ubuntu, Windows, and ParrotOS.

IMPLEMENTATION:

In this section, the step-by-step process followed during the assessment is outlined along with screenshots and commands for each step.

2.1 Passive Footprinting

- **Step 0: Ping testphp.vulnweb.com**


Red Hat Enterprise Linux 9 64-bit (2) - VMware Workstation
File Edit View VM Tabs Help
Red Hat Enterprise Linux 9 ...
Activities
Terminal
Sep 27 10:32
root@localhost:~

```
[root@localhost ~]# ping testphp.vulnweb.com
PING testphp.vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=1 ttl=128 time=324 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=2 ttl=128 time=624 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=3 ttl=128 time=602 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=4 ttl=128 time=521 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=5 ttl=128 time=508 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=6 ttl=128 time=332 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=7 ttl=128 time=312 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=8 ttl=128 time=374 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=9 ttl=128 time=337 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=10 ttl=128 time=331 ms
^C
--- testphp.vulnweb.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9001ms
rtt min/avg/max/dev = 311.721/426.465/623.867/117.468 ms
[root@localhost ~]#
```

=> Host is active on ec2- user on AWS(cloud service by amazon).

- **Step 1: WHOIS Lookup**
  - **Command**: whois testphp.vulnweb.com
  - **Purpose**: Retrieve domain registration information such as owner, registrar, and nameservers.
  - **Outcome**: Displays the target's domain details.

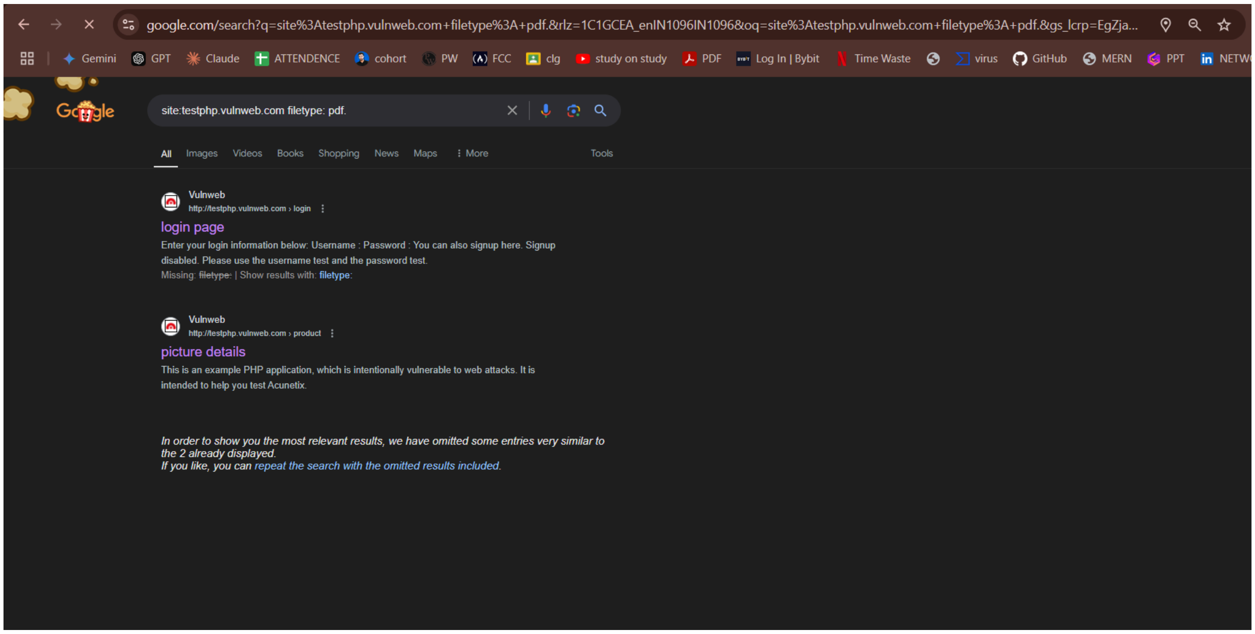
```
#

# 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.
#
# 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
Comment:       For details of this service please see
Comment:       http://ec2.amazonaws.com
Ref:           https://rdap.arin.net/registry/entity/AMAZO-4
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


OrgAbuseHandle: AEA8-ARIN
OrgAbuseName:   Amazon EC2 Abuse
OrgAbusePhone:  +1-206-555-0000
OrgAbuseEmail:  trustandsafety@support.aws.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/AEA8-ARIN


OrgRoutingHandle: IPROU3-ARIN
```

```
OrgRoutingName:   IP Routing
OrgRoutingPhone:  +1-206-555-0000
OrgRoutingEmail:  aws-routing-poc@amazon.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/IPROU3-ARIN


OrgTechHandle: ANO24-ARIN
OrgTechName:   Amazon EC2 Network Operations
OrgTechPhone:  +1-206-555-0000
OrgTechEmail:  amzn-noc-contact@amazon.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ANO24-ARIN


OrgNOCHandle: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-555-0000
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/AANO1-ARIN


# end
# start
NetRange:       44.224.0.0 - 44.255.255.255
CIDR:           44.224.0.0/11
NetName:        AMAZO-ZPDX
NetHandle:      NET-44-224-0-0-1
```

```
Parent:        AMAZO-4 (NET-44-192-0-0-1)

NetType:       Reallocated

OriginAS:

Organization:  Amazon.com, Inc. (AMAZO-47)

RegDate:       2019-08-01

Updated:       2019-08-01

Ref:           https://rdap.arin.net/registry/ip/44.224.0.0

OrgName:       Amazon.com, Inc.

OrgId:         AMAZO-47

Address:       EC2, EC2 1200 12th Ave South

City:          Seattle

StateProv:     WA

PostalCode:    98144

Country:       US

RegDate:       2011-05-10

Updated:       2021-07-22

Ref:           https://rdap.arin.net/registry/entity/AMAZO-47

OrgTechHandle: ANO24-ARIN

OrgTechName:   Amazon EC2 Network Operations

OrgTechPhone:  +1-206-555-0000

OrgTechEmail:  amzn-noc-contact@amazon.com

OrgTechRef:    https://rdap.arin.net/registry/entity/ANO24-ARIN
```

```
OrgAbuseHandle: AEA8-ARIN
OrgAbuseName:   Amazon EC2 Abuse
OrgAbusePhone:  +1-206-555-0000
OrgAbuseEmail:  trustandsafety@support.aws.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/AEA8-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: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-555-0000
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/AANO1-ARIN
OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName:   IP Routing
OrgRoutingPhone:  +1-206-555-0000
OrgRoutingEmail:  aws-routing-poc@amazon.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/IPROU3-ARIN

# end
```

- **Step 2: Google Dorking**
  - **Command**: Use Google search operators like site:testphp.vulnweb.com filetype: pdf.
  - **Purpose**: To discover files, exposed directories, and sensitive information indexed by search engines.
  - **Outcome**: A list of publicly accessible files.
- 

google.com/search?q=site%3Atestphp.vulnweb.com+filetype%3A+pdf.&rlz=1C1GCEA_enIN1096IN1096&oq=site%3Atestphp.vulnweb.com+filetype%3A+pdf.&gs_lcrp=EgZja...

site:testphp.vulnweb.com filetype: pdf.

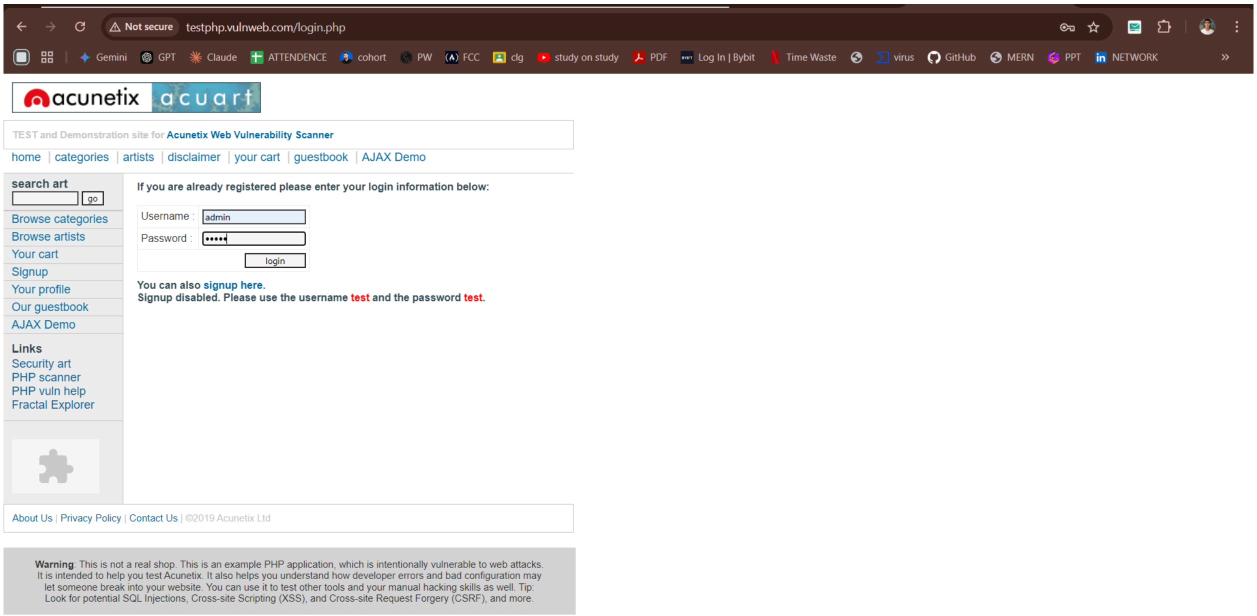
Vulnweb
http://testphp.vulnweb.com › login
login page
Enter your login information below: Username : Password : You can also signup here. Signup disabled. Please use the username test and the password test.
Missing: ~~filetype:~~ | Show results with: filetype:

Vulnweb
http://testphp.vulnweb.com › product
picture details
This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix.

In order to show you the most relevant results, we have omitted some entries very similar to the 2 already displayed.
If you like, you can repeat the search with the omitted results included.

- **Step 3: Wireshark Network Analysis**
- **Command**: Use Wireshark to capture and analyze network traffic.
  Purpose: Monitor and inspect network packets to detect any suspicious activities or unsecured protocols that may expose sensitive data.
  Outcome: A detailed view of network traffic, including any open protocols, unencrypted data transmission, and possible indications of compromise (e.g., unusual traffic patterns, exposed credentials, or sensitive information in transit).

- If an attacker is on the same network as a normal user then he/she could steal the critical information of the username and password of the user via network sniffing as shown in the images below.
- The Username and the Password are going into the network via plain text, which is a critical Vulnerability for the website, it can be fixed by using SSL and TLS certifications.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

search art [go]

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

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

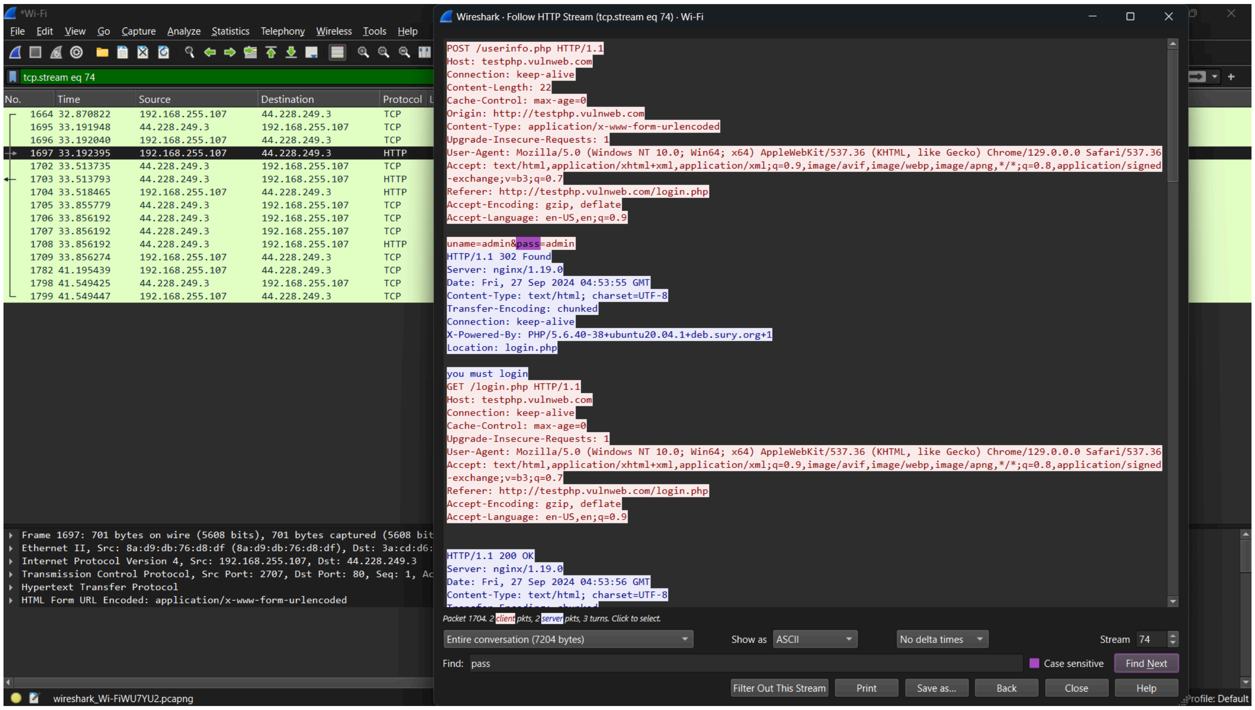
If you are already registered please enter your login information below:

Username :	admin
Password :	•••••
	login

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.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Follow HTTP Stream (tcp.stream eq 74) · Wi-Fi

tcp.stream eq 74

```
No.   Time       Source           Destination      Protocol
1664 32.870822  192.168.255.107  44.228.249.3     TCP
1695 33.191948  44.228.249.3     192.168.255.107  TCP
1696 33.192040  192.168.255.107  44.228.249.3     TCP
1697 33.192395  192.168.255.107  44.228.249.3     HTTP
1702 33.513735  44.228.249.3     192.168.255.107  TCP
1703 33.513793  44.228.249.3     192.168.255.107  HTTP
1704 33.518465  192.168.255.107  44.228.249.3     HTTP
1705 33.855779  44.228.249.3     192.168.255.107  TCP
1706 33.856192  44.228.249.3     192.168.255.107  TCP
1707 33.856192  44.228.249.3     192.168.255.107  TCP
1708 33.856192  44.228.249.3     192.168.255.107  HTTP
1709 33.856274  192.168.255.107  44.228.249.3     TCP
1782 41.195439  192.168.255.107  44.228.249.3     TCP
1798 41.549425  44.228.249.3     192.168.255.107  TCP
1799 41.549447  192.168.255.107  44.228.249.3     TCP
```

```
Frame 1697: 701 bytes on wire (5608 bits), 701 bytes captured (5608 bit
Ethernet II, Src: 8a:d9:db:76:d8:df (8a:d9:db:76:d8:df), Dst: 3a:cd:d6:
Internet Protocol Version 4, Src: 192.168.255.107, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 2707, Dst Port: 80, Seq: 1, Ac
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
```

wireshark_Wi-FiWU7YU2.pcapng

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 22
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

uname=admin&pass=admin
HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Fri, 27 Sep 2024 04:53:55 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php

you must login
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 27 Sep 2024 04:53:56 GMT
Content-Type: text/html; charset=UTF-8
```

Packet 1704. 2 client pkts, 2 server pkts, 3 turns. Click to select.

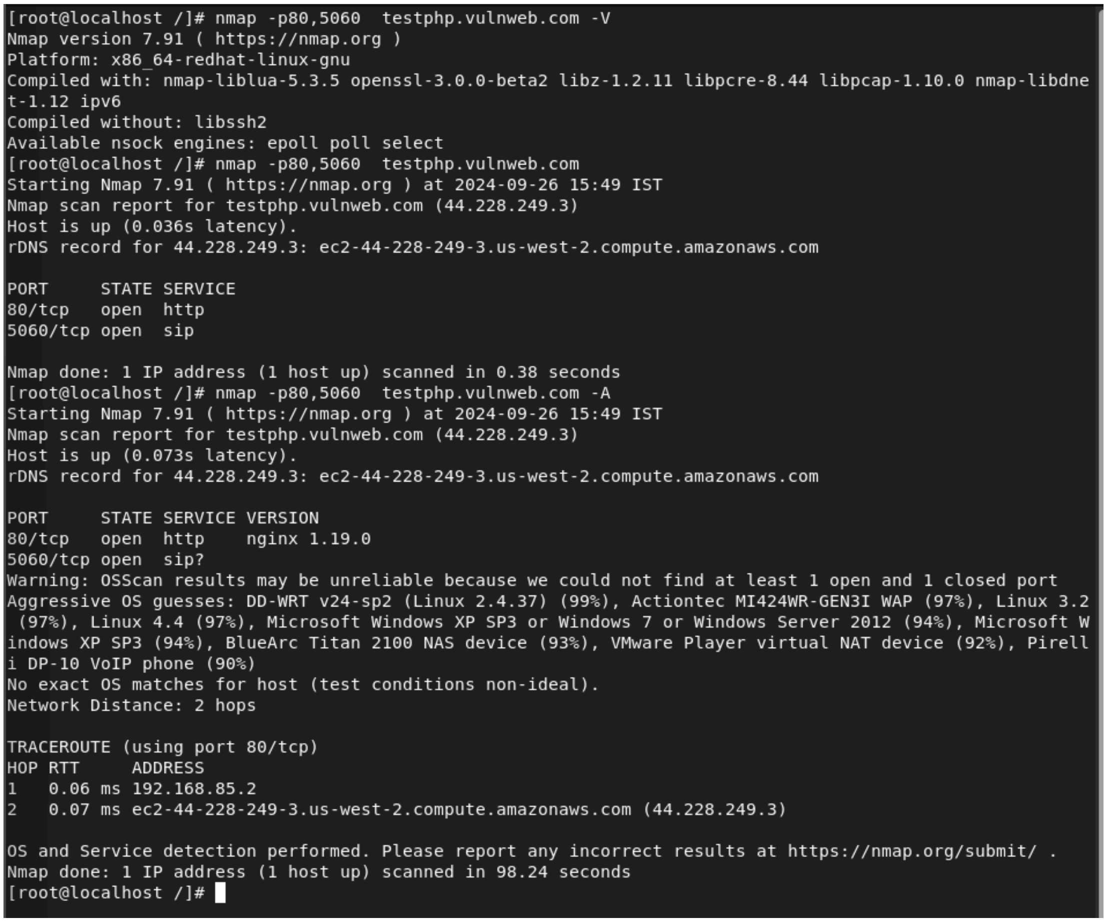
Entire conversation (7204 bytes)   Show as ASCII   No delta times   Stream 74

Find: pass   ■ Case sensitive

2.2 Active Footprinting

Step 1: Nmap Scan

- **Command**: nmap -A testphp.vulnweb.com
- **Purpose**: Scan for open ports, services, OS, and version details.
- **Outcome**: Open ports, services running, OS detection, and service versions.



```
[root@localhost /]# nmap -p80,5060  testphp.vulnweb.com -V
Nmap version 7.91 ( https://nmap.org )
Platform: x86_64-redhat-linux-gnu
Compiled with: nmap-liblua-5.3.5 openssl-3.0.0-beta2 libz-1.2.11 libpcre-8.44 libpcap-1.10.0 nmap-libdne
t-1.12 ipv6
Compiled without: libssh2
Available nsock engines: epoll poll select
[root@localhost /]# nmap -p80,5060  testphp.vulnweb.com
Starting Nmap 7.91 ( https://nmap.org ) at 2024-09-26 15:49 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.036s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

PORT     STATE SERVICE
80/tcp   open  http
5060/tcp open  sip

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
[root@localhost /]# nmap -p80,5060  testphp.vulnweb.com -A
Starting Nmap 7.91 ( https://nmap.org ) at 2024-09-26 15:49 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.073s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

PORT     STATE SERVICE VERSION
80/tcp   open  http    nginx 1.19.0
5060/tcp open  sip?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (99%), Actiontec MI424WR-GEN3I WAP (97%), Linux 3.2
 (97%), Linux 4.4 (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (94%), Microsoft W
indows XP SP3 (94%), BlueArc Titan 2100 NAS device (93%), VMware Player virtual NAT device (92%), Pirell
i DP-10 VoIP phone (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.06 ms 192.168.85.2
2   0.07 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.24 seconds
[root@localhost /]# 
```

System Information:

- **Operating System:** Likely a Linux distribution, possibly one of the following: DD-WRT v24-sp2, Actiontec MI424WR-GEN3I WAP, Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Windows 7, Windows Server 2012, Microsoft Windows XP SP3, BlueArc Titan 2100 NAS device, VMware Player virtual NAT device, Pirelli DP-10 VoIP phone.
- **Nmap Version:** 7.91
- **Platform:** x86 64-bit
- **Compiled With:** nmap-liblua-5.3.5, openssl-3.0.0-beta2, libz-1.2.11, libpcre-8.44, libpcap-1.10.0, nmap-libdne
- **Compiled Without:** libssh2

- **Available nsock Engines:** epoll, poll, select

Target Information:

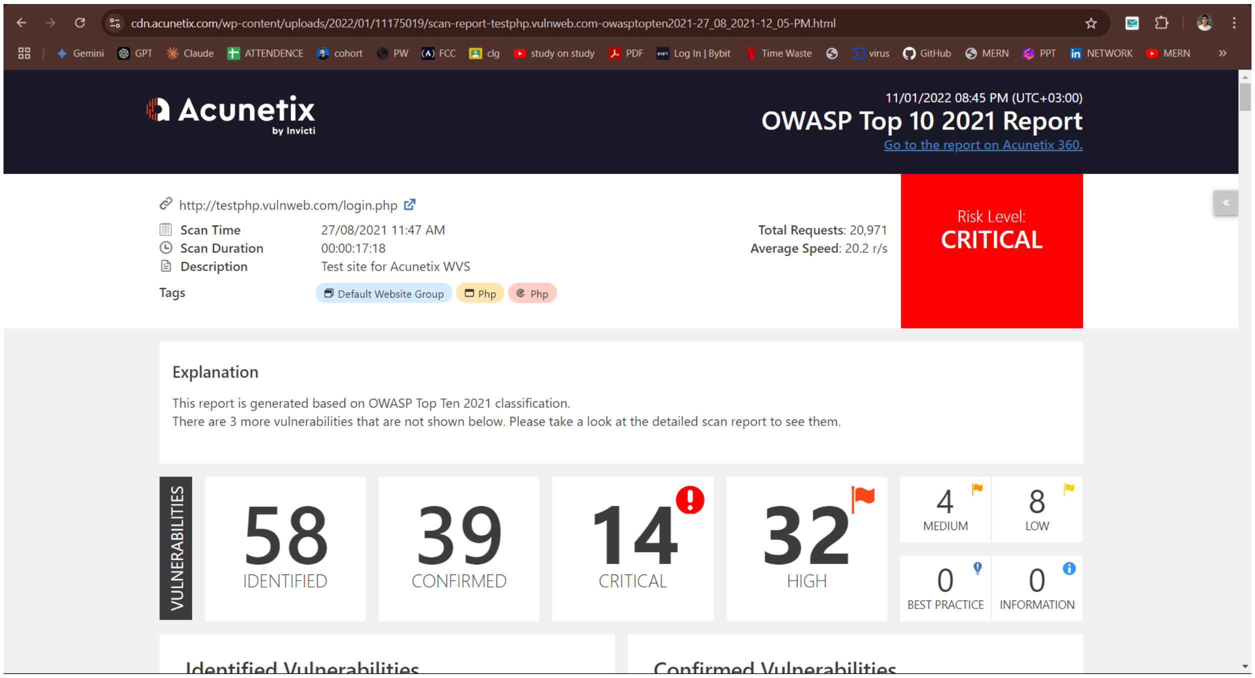
- **Hostname:** testphp.vulnweb.com
- **IP Address:** 44.228.249.3
- **rDNS Record:** ec2-44-228-249-3.us-west-2.compute.amazonaws.com
- **Host Uptime:** 0.036 seconds latency
- **Network Distance:** 2 hops

Open Ports and Services:

- **Port 80/tcp:** Open, HTTP, nginx 1.19.0
- **Port 5060/tcp:** Open, SIP (service version unknown)

Additional Notes:

- The OS guess is based on aggressive scanning and may not be entirely accurate.
- The service version for port 5060/tcp could not be reliably determined.
- Detailed traceroute information is provided.
- The results are available for further analysis and potential exploitation.



11/01/2022 08:45 PM (UTC+03:00)

OWASP Top 10 2021 Report

Go to the report on Acunetix 360.

http://testphp.vulnweb.com/login.php

Scan Time	27/08/2021 11:47 AM
Scan Duration	00:00:17:18
Description	Test site for Acunetix WVS
Tags	Default Website Group Php Php

Total Requests: 20,971
Average Speed: 20.2 r/s

Risk Level:
CRITICAL

Explanation

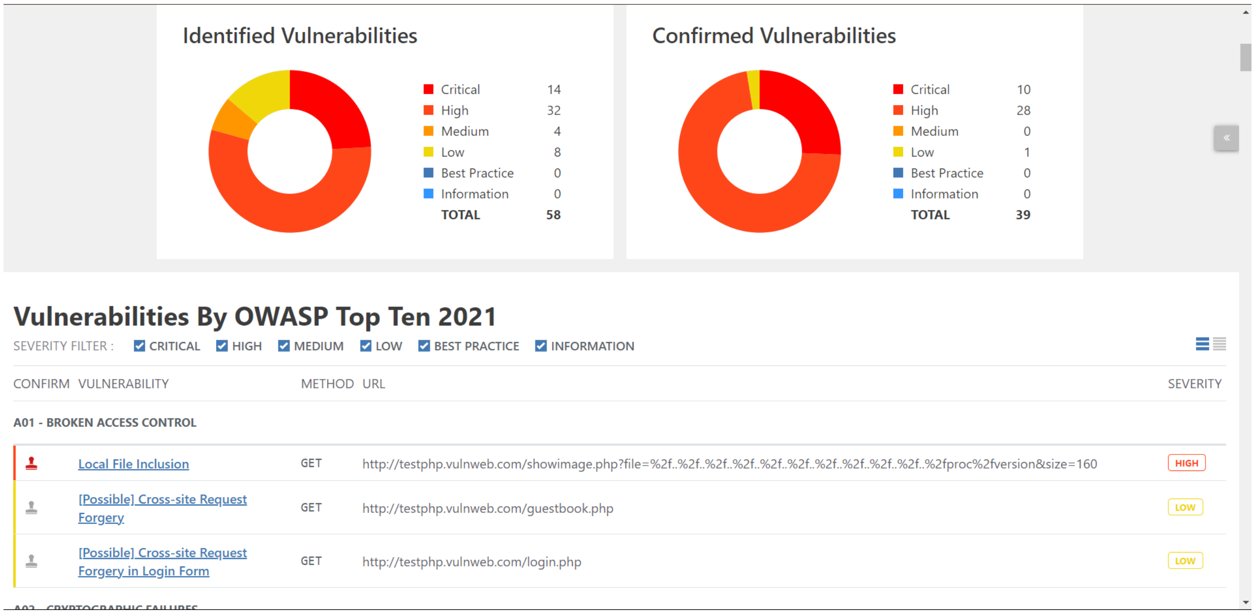
This report is generated based on OWASP Top Ten 2021 classification.
There are 3 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

VULNERABILITIES

58	39	14	32	4	8	0	0
IDENTIFIED	CONFIRMED	CRITICAL	HIGH	MEDIUM	LOW	BEST PRACTICE	INFORMATION

Identified Vulnerabilities   Confirmed Vulnerabilities

=> List of vulnerabilities listed on Acunetix, which is a source for information on the web.



Identified Vulnerabilities

🟥 Critical	14
🟧 High	32
🟧 Medium	4
🟨 Low	8
🟦 Best Practice	0
🟦 Information	0
TOTAL	**58**

Confirmed Vulnerabilities

🟥 Critical	10
🟧 High	28
🟧 Medium	0
🟨 Low	1
🟦 Best Practice	0
🟦 Information	0
TOTAL	**39**

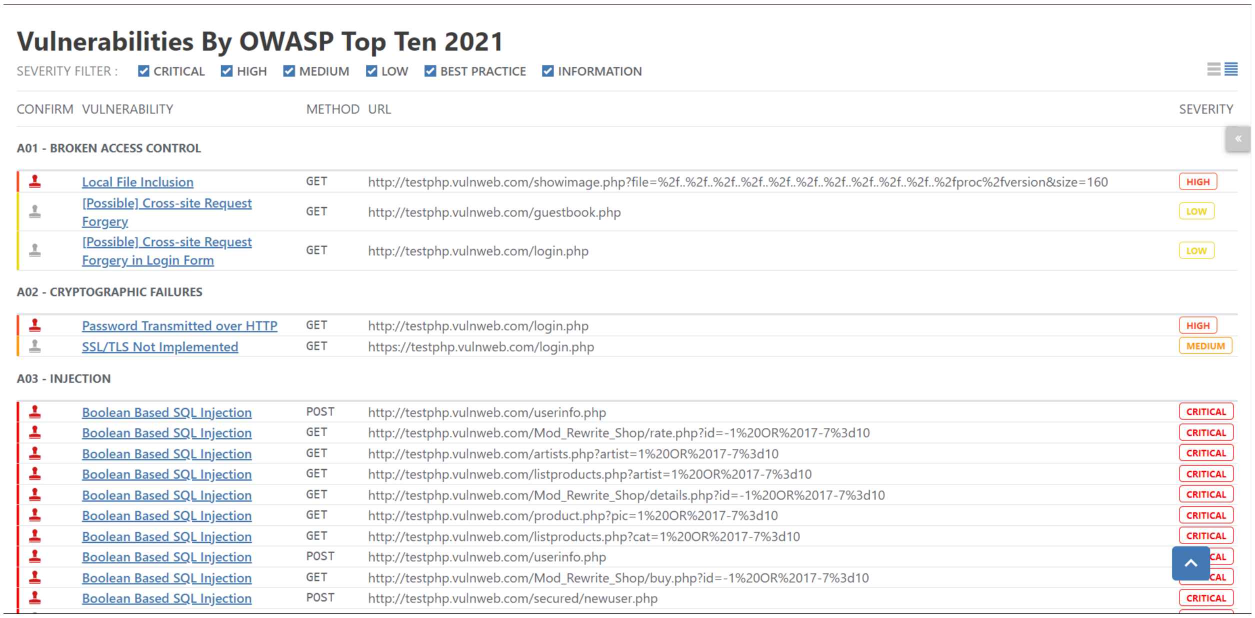
Vulnerabilities By OWASP Top Ten 2021

SEVERITY FILTER : ☑ CRITICAL ☑ HIGH ☑ MEDIUM ☑ LOW ☑ BEST PRACTICE ☑ INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A01 - BROKEN ACCESS CONTROL				
	Local File Inclusion	GET	http://testphp.vulnweb.com/showimage.php?file=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fproc%2fversion&size=160	HIGH
	[Possible] Cross-site Request Forgery	GET	http://testphp.vulnweb.com/guestbook.php	LOW
	[Possible] Cross-site Request Forgery in Login Form	GET	http://testphp.vulnweb.com/login.php	LOW

A02 - CRYPTOGRAPHIC FAILURES

=> Listed Vulnerabilities on Acunetix that can be easily bypassed by a script kiddie to gain sustainable access to the website.

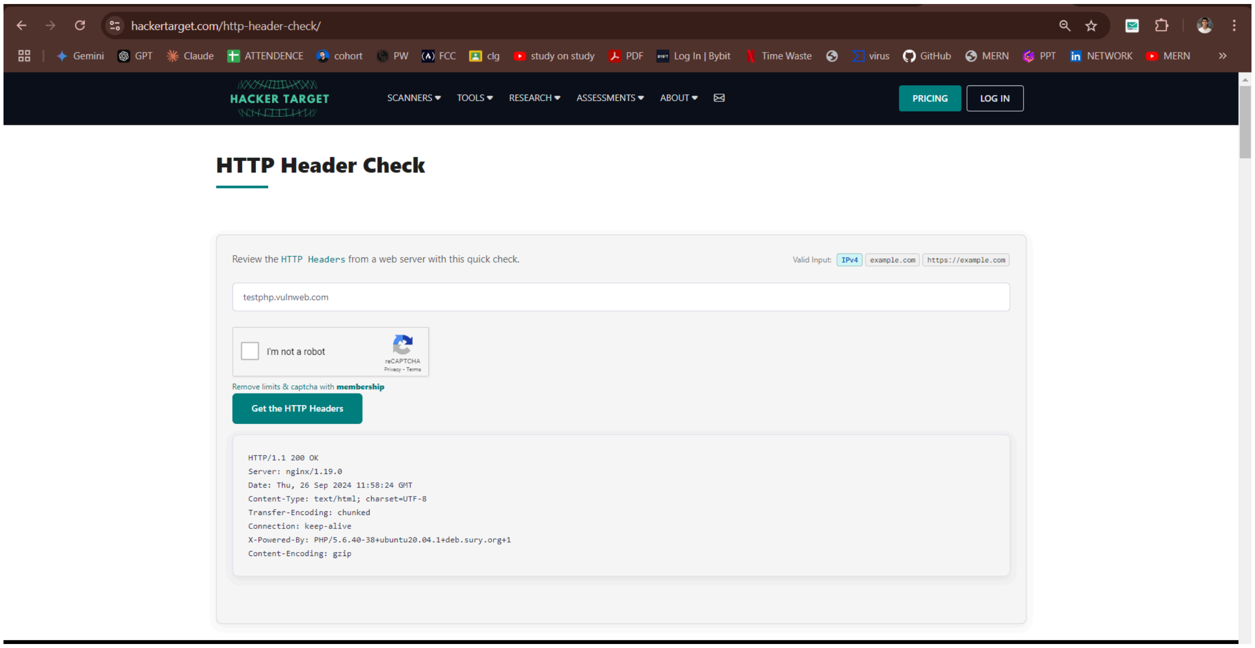


Vulnerabilities By OWASP Top Ten 2021

SEVERITY FILTER : ☑ CRITICAL ☑ HIGH ☑ MEDIUM ☑ LOW ☑ BEST PRACTICE ☑ INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
	A01 - BROKEN ACCESS CONTROL			
	Local File Inclusion	GET	http://testphp.vulnweb.com/showimage.php?file=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fproc%2fversion&size=160	HIGH
	[Possible] Cross-site Request Forgery	GET	http://testphp.vulnweb.com/guestbook.php	LOW
	[Possible] Cross-site Request Forgery in Login Form	GET	http://testphp.vulnweb.com/login.php	LOW
	A02 - CRYPTOGRAPHIC FAILURES			
	Password Transmitted over HTTP	GET	http://testphp.vulnweb.com/login.php	HIGH
	SSL/TLS Not Implemented	GET	https://testphp.vulnweb.com/login.php	MEDIUM
	A03 - INJECTION			
	Boolean Based SQL Injection	POST	http://testphp.vulnweb.com/userinfo.php	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php?id=-1%20OR%2017-7%3d10	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/artists.php?artist=1%20OR%2017-7%3d10	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/listproducts.php?artist=1%20OR%2017-7%3d10	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php?id=-1%20OR%2017-7%3d10	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/product.php?pic=1%20OR%2017-7%3d10	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/listproducts.php?cat=1%20OR%2017-7%3d10	CRITICAL
	Boolean Based SQL Injection	POST	http://testphp.vulnweb.com/userinfo.php	CAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php?id=-1%20OR%2017-7%3d10	CAL
	Boolean Based SQL Injection	POST	http://testphp.vulnweb.com/secured/newuser.php	CRITICAL

=> Gaining information on the server's version, Encoding, Hosted Operating system, and content Encoding, with content encoding techniques.



HTTP Header Check

Review the HTTP Headers from a web server with this quick check.

Valid Input: IPv4 example.com https://example.com

testphp.vulnweb.com

□ I'm not a robot

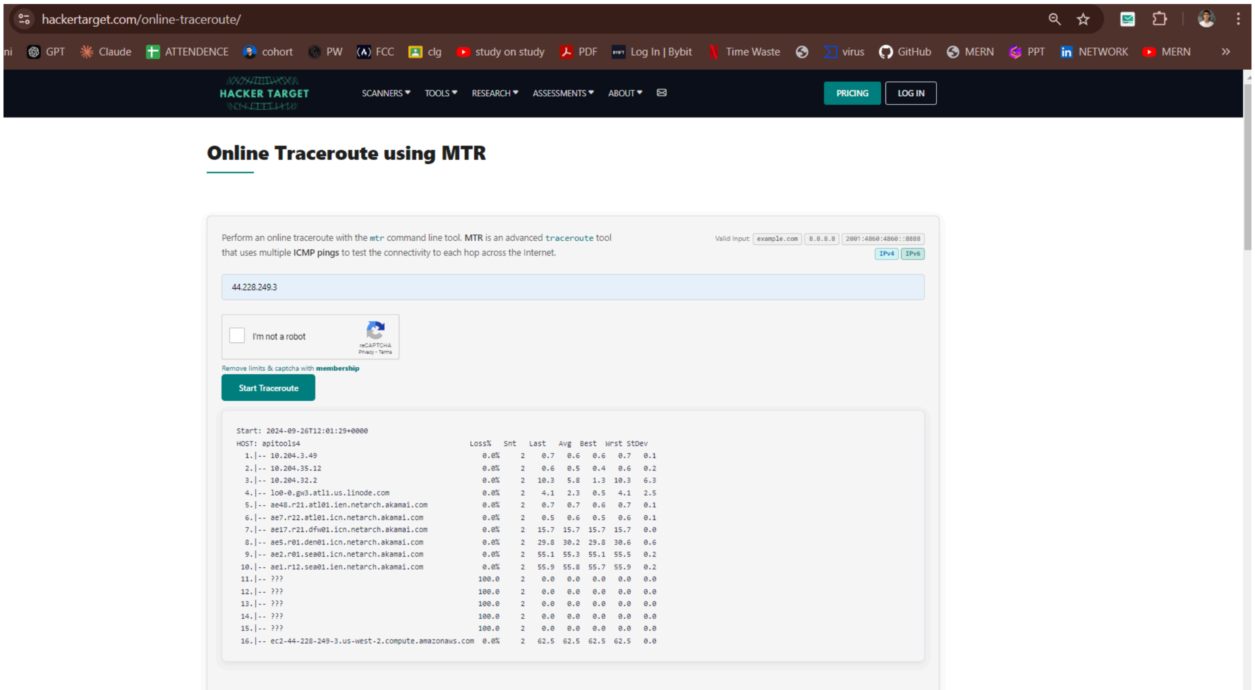
reCAPTCHA
Privacy - Terms

Remove limits & captcha with **membership**

Get the HTTP Headers

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 26 Sep 2024 11:58:24 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
```

=> Getting Traceroutes with MTR.



Online Traceroute using MTR

Perform an online traceroute with the `mtr` command line tool. **MTR** is an advanced `traceroute` tool that uses multiple **ICMP pings** to test the connectivity to each hop across the Internet.

Valid Input: `example.com` `8.8.8.8` `2001:4860:4860::8888` `IPv4` `IPv6`

44.228.249.3

□ I'm not a robot

Remove limits & captcha with **membership**

```
Start: 2024-09-26T12:01:29+0000
HOST: apitools4                                 Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 10.204.3.49                                0.0%     2    0.7   0.6   0.6   0.7   0.1
  2.|-- 10.204.35.12                               0.0%     2    0.6   0.5   0.4   0.6   0.2
  3.|-- 10.204.32.2                                0.0%     2   10.3   5.8   1.3  10.3   6.3
  4.|-- lo0-0.gw3.atl1.us.linode.com               0.0%     2    4.1   2.3   0.5   4.1   2.5
  5.|-- ae48.r21.atl01.ien.netarch.akamai.com      0.0%     2    0.7   0.7   0.6   0.7   0.1
  6.|-- ae7.r22.atl01.icn.netarch.akamai.com       0.0%     2    0.5   0.6   0.5   0.6   0.1
  7.|-- ae17.r21.dfw01.icn.netarch.akamai.com      0.0%     2   15.7  15.7  15.7  15.7   0.0
  8.|-- ae5.r01.den01.icn.netarch.akamai.com       0.0%     2   29.8  30.2  29.8  30.6   0.6
  9.|-- ae2.r01.sea01.icn.netarch.akamai.com       0.0%     2   55.1  55.3  55.1  55.5   0.2
 10.|-- ae1.r12.sea01.ien.netarch.akamai.com       0.0%     2   55.9  55.8  55.7  55.9   0.2
 11.|-- ???                                       100.0     2    0.0   0.0   0.0   0.0   0.0
 12.|-- ???                                       100.0     2    0.0   0.0   0.0   0.0   0.0
 13.|-- ???                                       100.0     2    0.0   0.0   0.0   0.0   0.0
 14.|-- ???                                       100.0     2    0.0   0.0   0.0   0.0   0.0
 15.|-- ???                                       100.0     2    0.0   0.0   0.0   0.0   0.0
 16.|-- ec2-44-228-249-3.us-west-2.compute.amazonaws.com  0.0%     2   62.5  62.5  62.5  62.5   0.0
```

2.3 Indicators of Compromise

After performing the footprinting process, the following indicators of compromise (IOCs) were identified:

- **Open Ports**: Multiple open ports were detected during the Nmap scan, revealing potentially exploitable services.
- **Subdomain Exposure**: Subdomains discovered that may not be properly secured.
- **Sensitive Files**: Files indexed by search engines that could expose sensitive data.
- **Services with Known Vulnerabilities**: Services identified via wireshark and Nmap that may be running outdated or vulnerable versions.

CONCLUSION & RECOMMENDATIONS:

3.1 Conclusion

The footprinting process revealed several security risks associated with the target website, including:

- Open ports and services exposed to the internet.
- Sensitive files and information are accessible via Google Dorking.
- Unprotected subdomains that could be leveraged in attacks.

These findings highlight the importance of maintaining strong security configurations and limiting the digital footprint of a website.

3.2 Recommendations

To mitigate the identified risks, the following countermeasures are recommended:

- **Close Unnecessary Ports**: Only open necessary ports and services. Use firewalls to restrict access.
- **Use Domain Privacy**: Protect domain information by using privacy services to prevent public access to WHOIS data.
- **Secure Subdomains**: Ensure subdomains are properly secured with authentication and SSL encryption.
- **Robust Robots.txt Configuration**: Limit search engine indexing of sensitive files through proper robots.txt configurations.
- **Monitor Vulnerabilities**: Regularly scan and patch services exposed to the internet.
- **Employee Training**: Educate employees about avoiding exposure of sensitive information and ensuring strong passwords for email and server access.

LIST OF REFERENCES:

Provide references to the tools, resources, and documentation used during the assessment. Examples include:

- **Nmap Documentation**: https://nmap.org/
- **Google Dorking Guide**: https://exploit-db.com/google-dorks/
- **Wireshark:** https://www.wireshark.org/docs/
- **QWASP Top 10 Report:** https://cdn.acunetix.com/wp-content/uploads/2022/01/11175019/scan-report-testphp.vulnweb.com-owasptopten2021-27_08_2021-12_05-PM.html
- **Traceroutes and Header Check:** https://hackertarget.com/
- **Digital Footprinting:** https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint