

Task2 Report



Web Open Source Intelligence (WebOSINT) focuses on gathering and analyzing publicly accessible data specifically from the web. It includes sources like websites, blogs, forums, and social media platforms. WebOSINT is widely used in cybersecurity, digital forensics, and market research. Ensuring ethical use and respecting privacy are crucial when conducting WebOSINT investigations.

Table of Contents

1.0 Future Intern Task2 Report	2
1.1 Introduction	2
2.0 Executive Summary	2
2.1 Executive Summary - Recommendations	2
3.0 Information Gathering	2
3.1.1 Whois Lookup	3
3.1.2 Ip address	4
3.1.3 Archive.org	5

1.0 Future Intern Task2 Report

1.1 Introduction

The Offensive Security Lab and Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security course. This report should contain all items that were used to pass the overall exam and it will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

2.0 Executive Summary

Conducted penetration test uncovered several security weaknesses present in web applications owned by testphp.vulnweb.com website

When performing the penetration test, there were several alarming vulnerabilities that were identified on testphp.vulnweb.com networks. When performing the attacks, I was able to find different information, primarily due to outdated patches and poor security configurations.

2.1 Executive Summary - Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3.0 Information Gathering

We try to get information about testphp.vulnweb.com website. We use many tools and websites for this.

3.1.1 Whois Lookup

WHOIS lookup involves querying databases to obtain information about domain names and IP addresses. It provides details such as the registrant's name, contact information, registration dates, and domain status. This tool is essential for managing internet resources, ensuring security, and conducting digital investigations. Ethical use and privacy respect are vital when performing WHOIS lookups. We use [Whois.com](https://whois.com) website to get information.

The image displays two screenshots of the Whois.com website, showing the results of a WHOIS lookup for the domain vulnweb.com. The top screenshot shows the 'Raw Whois Data' section, and the bottom screenshot shows a formatted view of the same data.

Raw Whois Data:

```
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: legal@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
Registrant Fax:
Registrant Email: administrator@acunetix.com
```

Formatted View:

```
Admin Name: Acunetix Acunetix
Admin Organization: Acunetix Ltd
Admin Street: 3rd Floor,, J&C Building,, Road Town
Admin City: Tortola
Admin State/Province:
Admin Postal Code: VG1110
Admin Country: VG
Admin Phone: +1.23456789
Admin Fax:
Admin Email: administrator@acunetix.com
Registry Tech ID:
Tech Name: Acunetix Acunetix
Tech Organization: Acunetix Ltd
Tech Street: 3rd Floor,, J&C Building,, Road Town
Tech City: Tortola
Tech State/Province:
Tech Postal Code: VG1110
Tech Country: VG
Tech Phone: +1.23456789
Tech Fax:
Tech Email: administrator@acunetix.com
Name Server: ns1.eurodns.com
Name Server: ns2.eurodns.com
Name Server: ns3.eurodns.com
Name Server: ns4.eurodns.com
DNSSEC: unsigned
```

We can see company name, phone number, email, registrant name, country, name serves etc.

3.2.2 Ip address

Ip address is the critical factor for websites because when we get an ip address we can scan the ip address with nmap or we can do other things.

```
imranmelikov@Imran-MacBook-Air ~ % ping testphp.vulnweb.com
PING testphp.vulnweb.com (44.228.249.3): 56 data bytes
64 bytes from 44.228.249.3: icmp_seq=0 ttl=47 time=381.512 ms
64 bytes from 44.228.249.3: icmp_seq=1 ttl=47 time=401.463 ms
64 bytes from 44.228.249.3: icmp_seq=2 ttl=47 time=316.675 ms
^C
--- testphp.vulnweb.com ping statistics ---
4 packets transmitted, 3 packets received, 25.0% packet loss
round-trip min/avg/max/stddev = 316.675/366.550/401.463/36.195 ms
imranmelikov@Imran-MacBook-Air ~ %
```

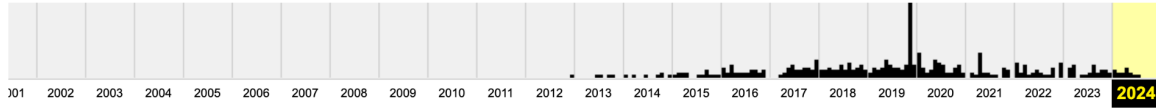
We use the ping command to learn the ip address. After this if we want we can scan the ip address with nmap. Our target ip is 44.228.249.3.

3.3.3 Archive.org

[Archive.org](https://archive.org/), also known as the Internet Archive, is a digital library that provides free access to a vast collection of digital content. It includes websites, books, audio recordings, videos, and software. The Wayback Machine, a prominent feature, allows users to view archived versions of web pages across different times. Archive.org supports research, historical preservation, and access to cultural artifacts. We can see last snapshots about the target.

Calendar · Collections · Changes · Summary · Site Map · URLs

Saved **368** times between December 6, 2012 and July 1, 2024.



JAN						FEB						MAR						APR												
1	2	3	4	5	6					1	2	3					1	2			1	2	3	4	5	6				
7	8	9	10	11	12	13		4	5	6	7	8	9	10		3	4	5	6	7	8	9		7	8	9	10	11	12	13
14	15	16	17	18	19	20		11	12	13	14	15	16	17		10	11	12	13	14	15	16		14	15	16	17	18	19	20
21	22	23	24	25	26	27		18	19	20	21	22	23	24		17	18	19	20	21	22	23		21	22	23	24	25	26	27
28	29	30	31					25	26	27	28	29				24	25	26	27	28	29	30		28	29	30				
												31																		
MAY				JUN				JUL				AUG																		
	1	2	3	4							1					1	2	3	4	5	6						1	2	3	