CONTENTS

Chapter 1 INTRODUCTION

1.1 Overview

Penetration testing or Pen Test is the most commonly used security testing technique for web applications.

Website penetration testing is a simulated hacker-style attack on a website aimed at identifying and gauging the gravity of existing vulnerabilities in order to protect the website from malicious attacks. This is to say, Penetration Testing focuses more on how each of these vulnerabilities could be exploited as opposed to Vulnerability Assessment, which merely identifies and lists all existing vulnerabilities in your website.

For example, consider a thief trying to enter your house to rob you and you want to take security measures so that the thief won't be able to enter your house. Here, vulnerability assessment is similar to making sure you have all your house windows and doors closed. And a penetration testing service is akin to checking the strength or any weaknesses of your windows or doors. So that even if a thief tries to enter, they will not find any entry points to enter your house and you can have a peaceful sleep.

1.2 Problem Statement

Web application penetration testing is the practice of simulating attacks on a system in an attempt to gain access to sensitive data, with the purpose of determining whether a system is secure. These attacks are performed either internally or externally on a system, and they help provide information about the target system, identify vulnerabilities within them, and uncover exploits that could actually compromise the system. It is an essential health check of a system that informs testers whether remediation and security measures are needed.

1.3 Objectives

There are three key steps to performing penetration testing on web applications and which is our objective:

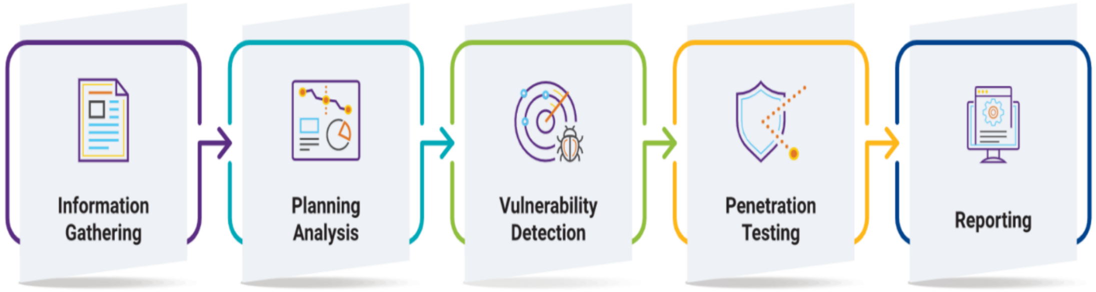
- **Configure our tests:** Before you get started, defining the scope and goals of the testing project is important. Identifying whether your goal is it to fulfil compliance needs or check overall performance will guide which tests you perform. After you decide what you're testing for, you should gather key information you need to perform your tests. This includes your web architecture, information about things like APIs, and general infrastructure information.
- **Execute our tests:** Usually, your tests will be simulated attacks that are attempting to see whether a hacker could actually gain access to an application. Two key types of tests you might run include
  - External penetration tests that analyze components accessible to hackers via the internet, like web apps or websites
  - Internal penetration tests that simulate a scenario in which a hacker has access to an application *behind* your firewalls
- **Analyze our tests:** After testing is complete, analyze your results. Vulnerabilities and sensitive data exposures should be discussed. After analysis, needed changes and improvements can be implemented.

In a nutshell, web app penetration testing can helps us to achieve following aspects:

- To identify and fix security flaws in your website.
- Penetration testing emulates real-life attack scenarios and helps in mitigating risks.
- It can help you in achieving certain compliance requirements such as GDPR, ISO 27001, PCI-DSS, HIPAA, and more.
- It enables you to uncover potential vulnerabilities in your site.
- It can save you from legal consequences and hefty penalties under data security policies.
- It helps in preparing your security team to cope with a real-life cyber-attack.

CHAPTER 2: SYSTEM ARCHITECTURE / BLOCK DIAGRAM

Web app penetration testing can be broken down into 5 stages:



CHAPTER 3: SYSTEM REQUIREMENT SPECIFICATIONS

Kali Linux requires:

- A minimum of 20GB hard disk space for installation depending on the version, Version 2020.2 requires at least 20GB.[16]
- A minimum of 2GB RAM for i386 and AMD64 architectures.
- A bootable CD-DVD drive or a USB stick.
- A minimum of an Intel Core i3 or an AMD E1 processor for good performance.

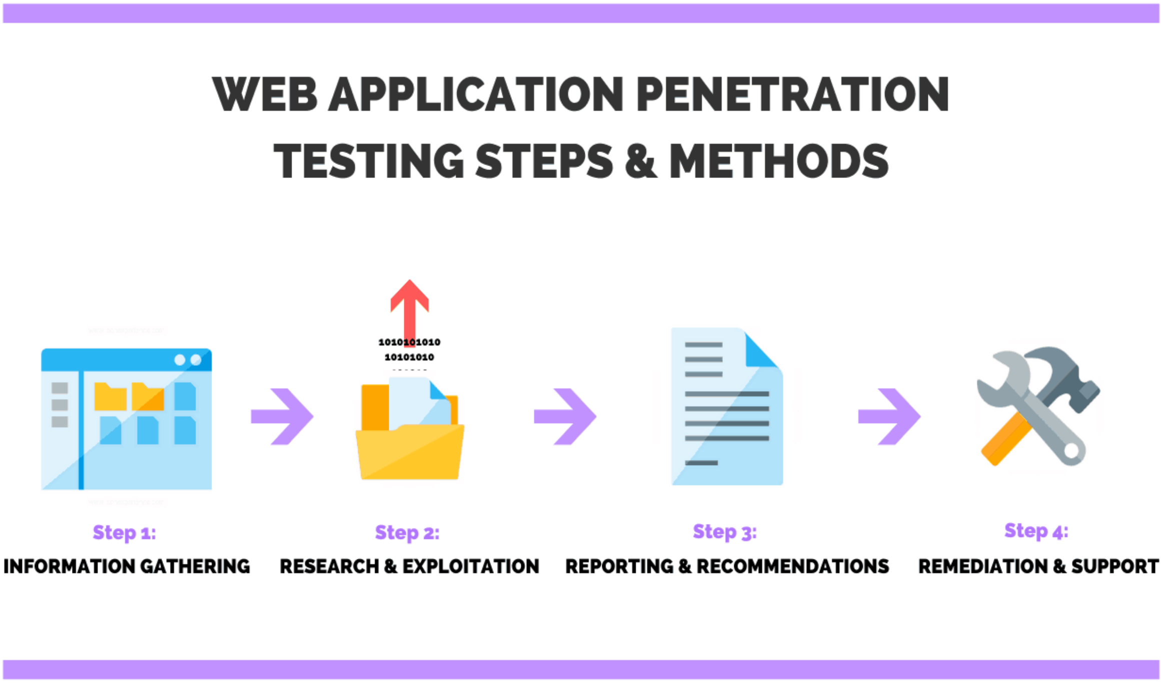
The recommended hardware specification for a smooth experience is

- 50 GB of hard disk space, SSD preferred
- At least 2GB of RAM

Tools used:

- Metasploit: - amazing tool for penetration testing, Metasploit is a framework and not a specific application, meaning it is possible to build custom tools for specific tasks.
- OWASP-ZAP: - OWASP Zed Attack Proxy (ZAP) is widely used web app scanner. It is free and open source.

Chapter 4: DESIGN



Step 1: Information Gathering

Information gathering, or the reconnaissance phase, is the most important step in any penetration testing process as it provides you with a wealth of information to identify vulnerabilities easily and exploit them later. There are two types of reconnaissance depending on the type of interaction you want to achieve with the target system:

1. Active Reconnaissance
2. Passive Reconnaissance

Step 2: Research and Exploitation

There is a sea of security tools when it comes to performing web app penetration testing and most of them are open source.

Not only you find all the necessary information you need in order to find vulnerabilities and exploits later on, but you also narrow down the attack vectors, and hence, the tools you can use to accomplish your goal.

Step 3: Reporting and Recommendations

The structure of the report should be clear and concise with adequate amount of data to support your findings. Make sure to stick to what methods worked and be as descriptive as possible.

By writing down the successful exploits and categorizing them by criticality, you will help the client company focus its efforts in fixing the most critical parts of their system.

Step 4: Remediation and Ongoing Support

It is best practice to mitigate critical and high vulnerabilities first and focus on the medium and low afterwards. Prioritization plays a big role as the likelihood of each vulnerability being exploited varies.

Some vulnerabilities detected are possible but not without previous access to the internal system, and some vulnerabilities carry the risk of remote code execution and should be adequately prioritized to reflect the likelihood and impact.

CHAPTER 5: IMPLEMENTATION

5.1 Modules Description

- METASPLOIT Framework:

  Metasploit is simple to use and is designed with ease-of-use in mind to aid Penetration Testers.

  Metasploit Framework follows these common steps while exploiting any target system

1. Select and configure the exploit to be targeted. This is the code that will be targeted toward a system with the intention of taking advantage of a defect in the software. Validate whether the chosen system is susceptible to the chosen exploit.
2. Lect and configure a payload that will be used. This payload represents the code that will be run on a system after a loop-hole has been found in the system and an entry point is set.t.
3. Select and configure the encoding schema to be used to make sure that the payload can evade Intrusion Detection Systems with ease.

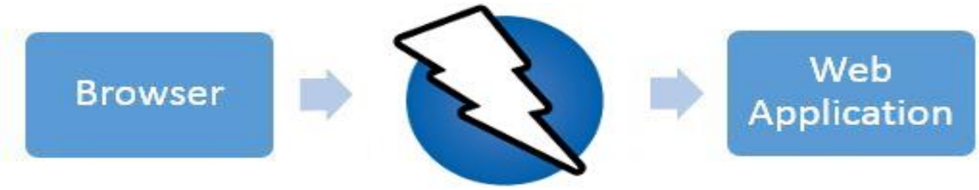
The module is a software application in the Metasploit framework that carries out task like exploiting and scanning the targets. There are key components in the framework and can be broken down into 7 types below:

1. Exploits
2. Payloads
3. Auxiliaries
4. Encoders
5. Evasions
6. Nops
7. Post

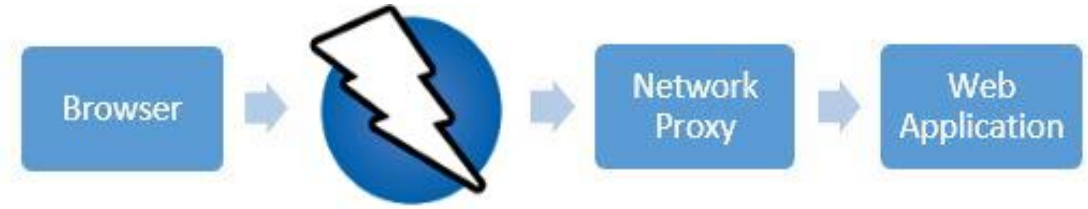
- <u>OWASP ZAP tool:</u>

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible.

At its core, ZAP is what is known as a “man-in-the-middle proxy.” It stands between the tester’s browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination. It can be used as a stand-alone application, and as a daemon process.



If there is another network proxy already in use, as in many corporate environments, ZAP can be configured to connect to that proxy.

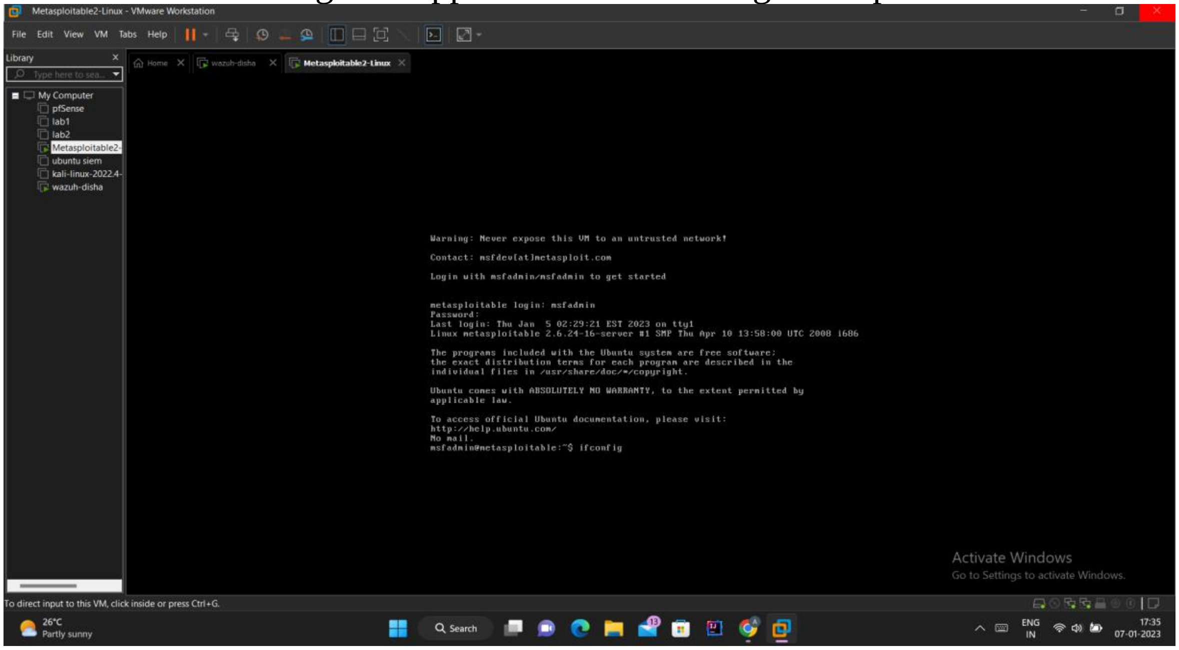


ZAP provides functionality for a range of skill levels – from developers, to testers new to security testing, to security testing specialists. ZAP has versions for each major OS and Docker, so you are not tied to a single OS.

Because ZAP is open-source, the source code can be examined to see exactly how the functionality is implemented. Anyone can volunteer to work on ZAP, fix bugs, add features, create pull requests to pull fixes into the project, and author add-ons to support specialized situations.

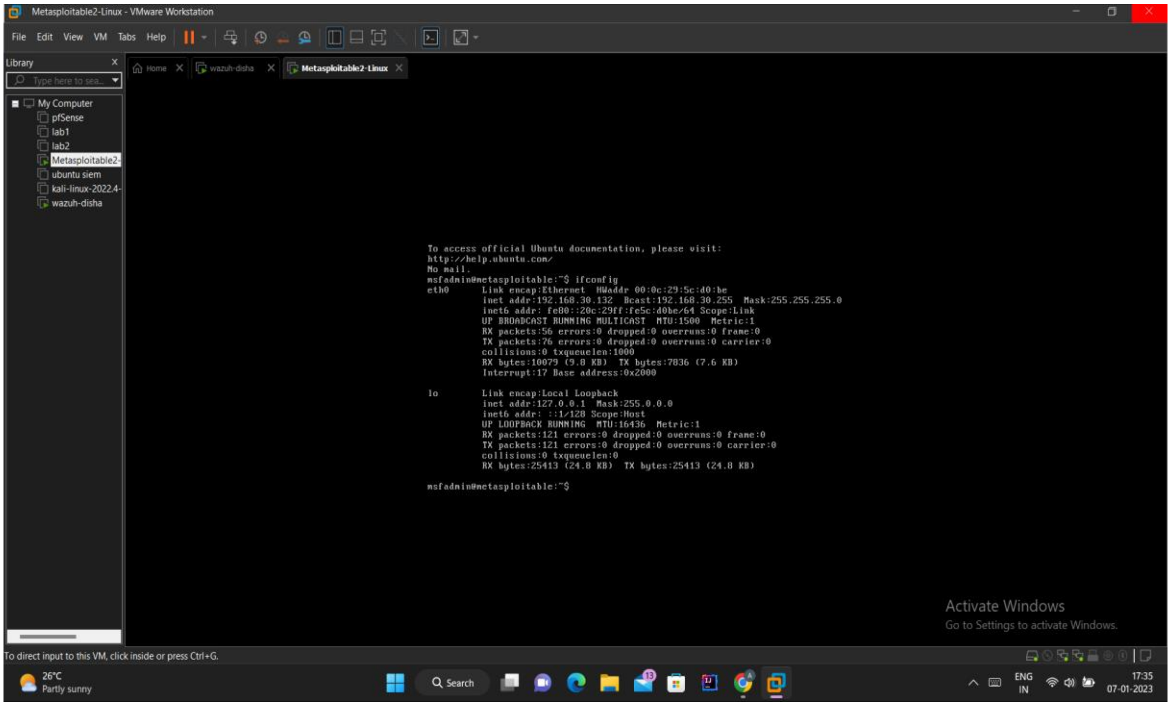
CHAPTER 6: RESULTS/SNAPSHOTS

➔ Running web application server using Metasploit framework



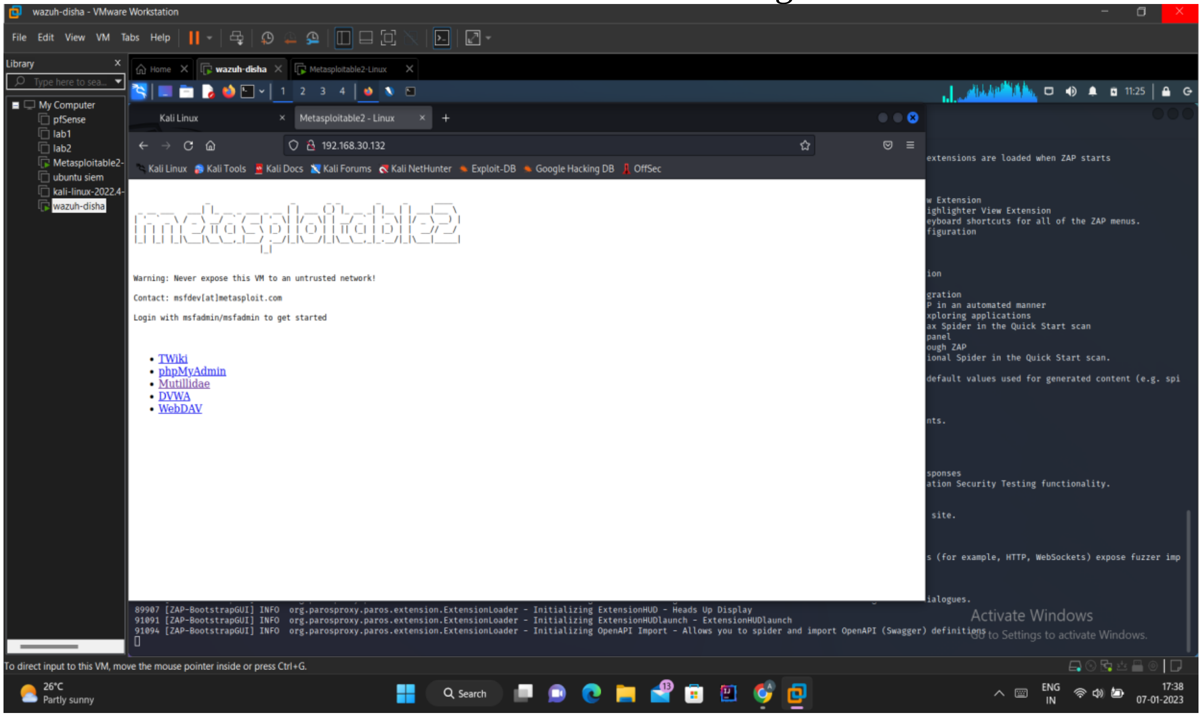
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Thu Jan  5 02:29:21 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
```

➔ When we enter **$ifconfig** command, we can see that the IP address obtained is **192.168.30.132**



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:5c:d0:be
          inet addr:192.168.30.132  Bcast:192.168.30.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe5c:d0be/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:56 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10079 (9.8 KB)  TX bytes:7836 (7.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25413 (24.8 KB)  TX bytes:25413 (24.8 KB)

msfadmin@metasploitable:~$
```

➔ We will go and enter the obtained IP address in Firefox browser of Kali Linux. We can go into mutillidae which is born to be hacked website meant for hacking


192.168.30.132

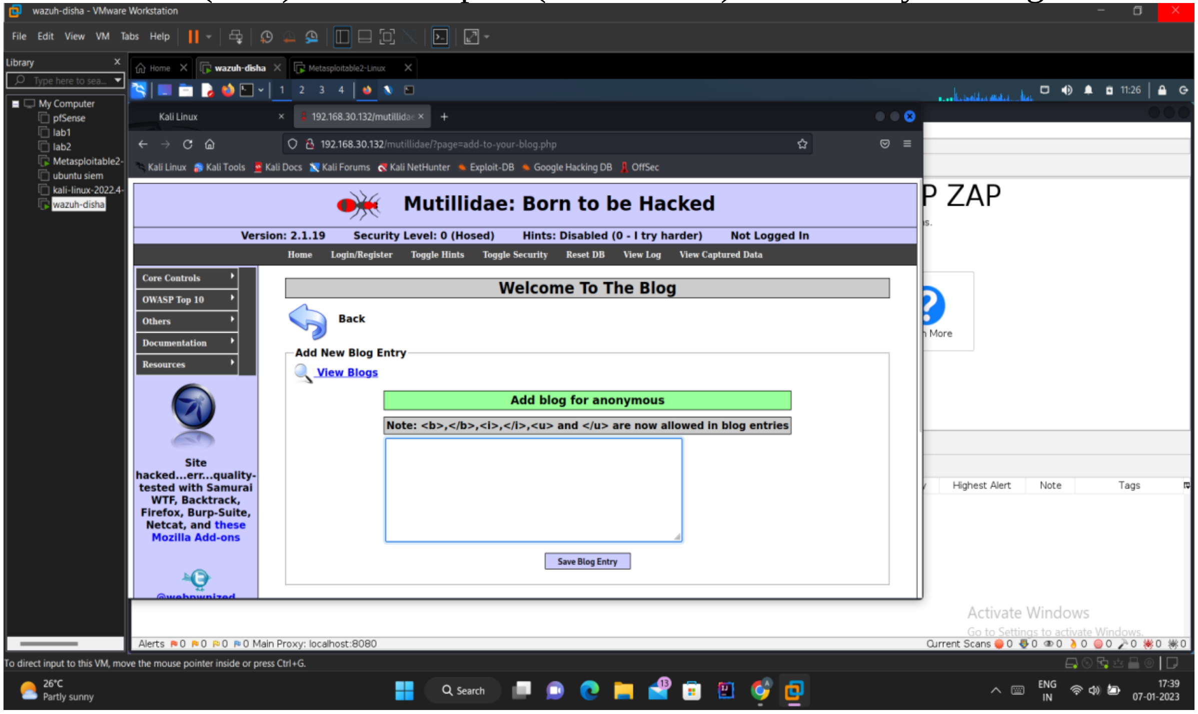
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

```
89907 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing ExtensionHUD - Heads Up Display
91091 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing ExtensionHUDlaunch - ExtensionHUDlaunch
91094 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing OpenAPI Import - Allows you to spider and import OpenAPI (Swagger) definitions
```

wazuh-disha - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
pfSense
lab1
lab2
Metasploitable2-
ubuntu siem
kali-linux-2022.4-
wazuh-disha
Home
Metasploitable2-Linux
Kali Linux
Metasploitable2 - Linux
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
11:25
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Partly sunny
Search
ENG
IN
17:38
07-01-2023

➔ Copy browser link of the below screenshot which is obtained when clicked on OWASP Top 10 → A2 Cross Site Scripting (XSS) → Via "Input" (GET/POST) → Add to your blog


192.168.30.132/mutillidae/?page=add-to-your-blog.php

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Welcome To The Blog

Add New Blog Entry

View Blogs

Add blog for anonymous

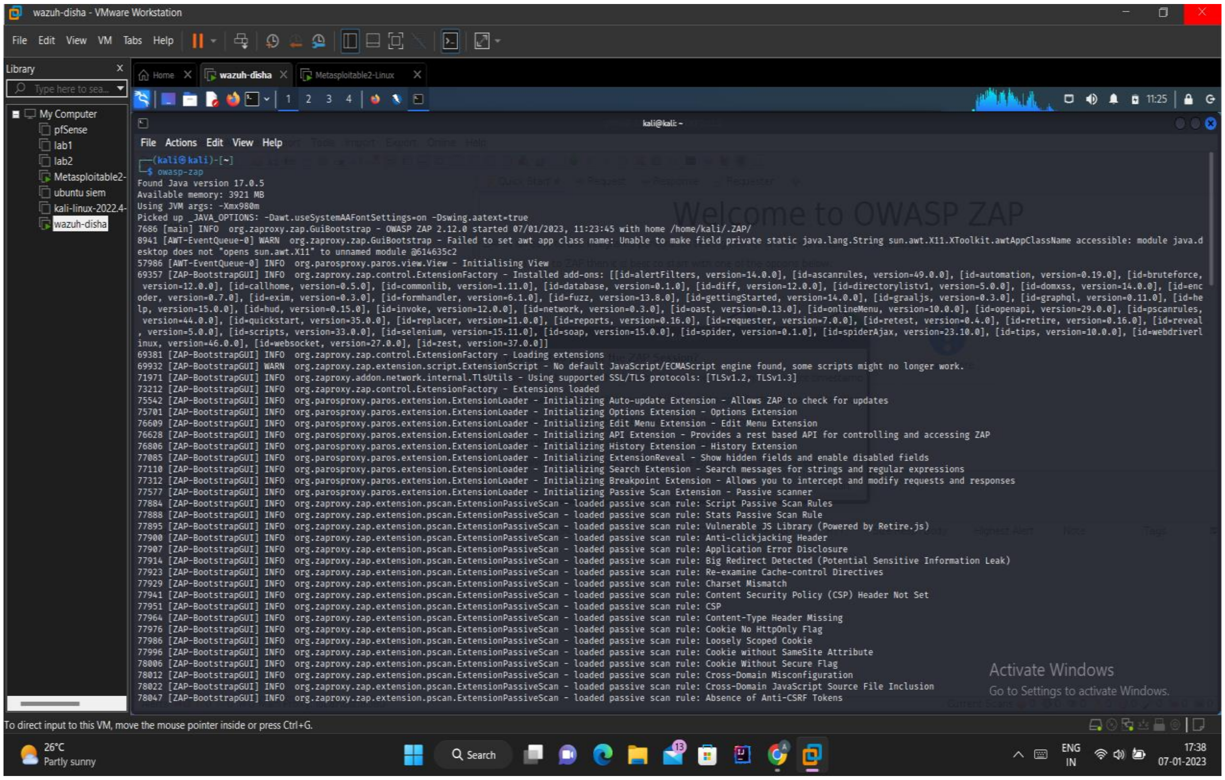
Note: <b>,</b>,<i>,</i>,<u> and </u> are now allowed in blog entries

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

Alerts 0 0 0 0 Main Proxy: localhost:8080

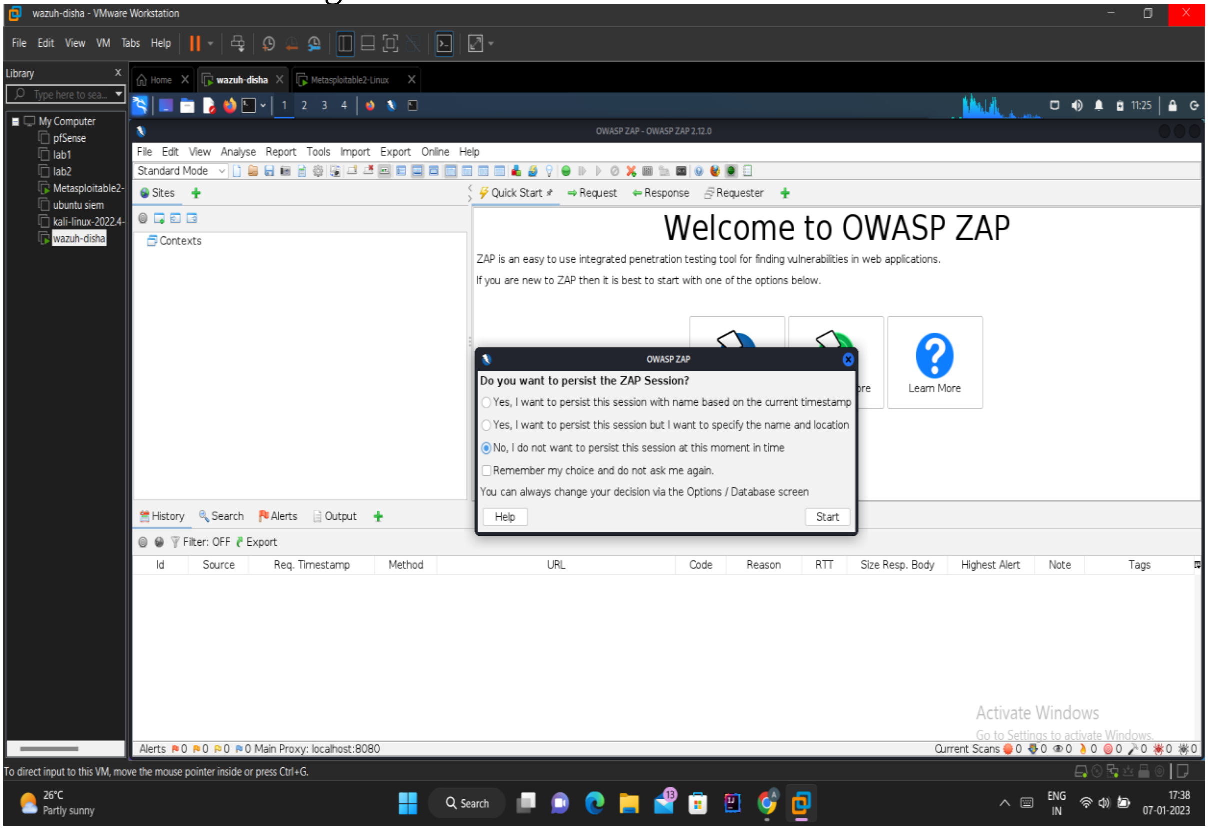
wazuh-disha - VMware Workstation
File Edit View VM Tabs Help
Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Back
Save Blog Entry
@webpwnized
P ZAP
More
Highest Alert
Note
Tags
Current Scans
11:26
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Partly sunny
Search
ENG
IN
17:39
07-01-2023

➔ Run OWASP-ZAP in the Kali Linux terminal


wazuh-disha - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
pfSense
lab1
lab2
Metasploitable2-
ubuntu siem
kali-linux-2022.4-
wazuh-disha
Home
wazuh-disha
Metasploitable2-Linux
kali@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Partly sunny
Search
ENG
IN
17:38
07-01-2023

```
┌──(kali㉿kali)-[~]
└─$ owasp-zap
Found Java version 17.0.5
Available memory: 3921 MB
Using JVM args: -Xmx980m
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
7686 [main] INFO  org.zaproxy.zap.GuiBootstrap - OWASP ZAP 2.12.0 started 07/01/2023, 11:23:45 with home /home/kali/.ZAP/
8941 [AWT-EventQueue-0] WARN  org.zaproxy.zap.GuiBootstrap - Failed to set awt app class name: Unable to make field private static java.lang.String sun.awt.X11.XToolkit.awtAppClassName accessible: module java.d
esktop does not "opens sun.awt.X11" to unnamed module @614635c2
57986 [AWT-EventQueue-0] INFO  org.parosproxy.paros.view.View - Initialising View
69357 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.control.ExtensionFactory - Installed add-ons: [[id=alertFilters, version=14.0.0], [id=ascanrules, version=49.0.0], [id=automation, version=0.19.0], [id=bruteforce,
 version=12.0.0], [id=callhome, version=0.5.0], [id=commonlib, version=1.11.0], [id=database, version=0.1.0], [id=diff, version=12.0.0], [id=directorylistv1, version=5.0.0], [id=domxss, version=14.0.0], [id=enc
oder, version=0.7.0], [id=exim, version=0.3.0], [id=formhandler, version=6.1.0], [id=fuzz, version=13.8.0], [id=gettingStarted, version=14.0.0], [id=graaljs, version=0.3.0], [id=graphql, version=0.11.0], [id=he
lp, version=15.0.0], [id=hud, version=0.15.0], [id=invoke, version=12.0.0], [id=network, version=0.3.0], [id=oast, version=0.13.0], [id=onlineMenu, version=10.0.0], [id=openapi, version=29.0.0], [id=pscanrules,
 version=44.0.0], [id=quickstart, version=35.0.0], [id=replacer, version=11.0.0], [id=reports, version=0.16.0], [id=requester, version=7.0.0], [id=retest, version=0.4.0], [id=retire, version=0.16.0], [id=reveal
, version=5.0.0], [id=scripts, version=33.0.0], [id=selenium, version=15.11.0], [id=soap, version=15.0.0], [id=spider, version=0.1.0], [id=spiderAjax, version=23.10.0], [id=tips, version=10.0.0], [id=webdriverl
inux, version=46.0.0], [id=websocket, version=27.0.0], [id=zest, version=37.0.0]]
69381 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.control.ExtensionFactory - Loading extensions
69932 [ZAP-BootstrapGUI] WARN  org.zaproxy.zap.extension.script.ExtensionScript - No default JavaScript/ECMAScript engine found, some scripts might no longer work.
71971 [ZAP-BootstrapGUI] INFO  org.zaproxy.addon.network.internal.TlsUtils - Using supported SSL/TLS protocols: [TLSv1.2, TLSv1.3]
73212 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.control.ExtensionFactory - Extensions loaded
75542 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Auto-update Extension - Allows ZAP to check for updates
75701 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Options Extension - Options Extension
76609 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Edit Menu Extension - Edit Menu Extension
76628 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing API Extension - Provides a rest based API for controlling and accessing ZAP
76806 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing History Extension - History Extension
77085 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing ExtensionReveal - Show hidden fields and enable disabled fields
77110 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Search Extension - Search messages for strings and regular expressions
77312 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Breakpoint Extension - Allows you to intercept and modify requests and responses
77577 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Passive Scan Extension - Passive scanner
77884 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Script Passive Scan Rules
77888 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Stats Passive Scan Rule
77895 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Vulnerable JS Library (Powered by Retire.js)
77900 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Anti-clickjacking Header
77907 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Application Error Disclosure
77914 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Big Redirect Detected (Potential Sensitive Information Leak)
77923 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Re-examine Cache-control Directives
77929 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Charset Mismatch
77941 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Content Security Policy (CSP) Header Not Set
77951 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: CSP
77964 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Content-Type Header Missing
77976 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Cookie No HttpOnly Flag
77986 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Loosely Scoped Cookie
77996 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Cookie without SameSite Attribute
78006 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Cookie Without Secure Flag
78012 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Cross-Domain Misconfiguration
78022 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Cross-Domain JavaScript Source File Inclusion
78047 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - loaded passive scan rule: Absence of Anti-CSRF Tokens
```

➔ Persisting a Session



Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

OWASP ZAP

Do you want to persist the ZAP Session?

○ Yes, I want to persist this session with name based on the current timestamp

○ Yes, I want to persist this session but I want to specify the name and location

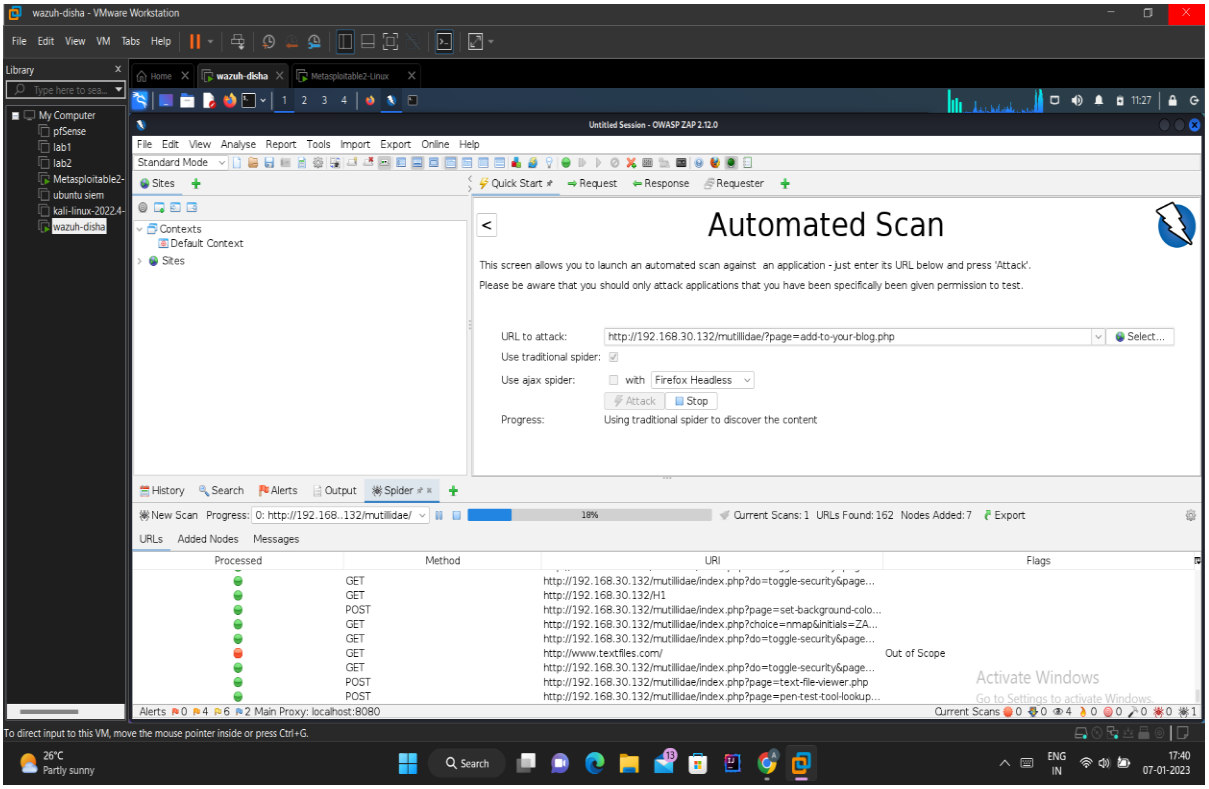
● No, I do not want to persist this session at this moment in time

□ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

Help Start

➔ Running an Automated Scan



wazuh-disha - VMware Workstation
Untitled Session - OWASP ZAP 2.12.0
Quick Start
Request
Response
Requester

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://192.168.30.132/mutillidae/?page=add-to-your-blog.php

Use traditional spider: ☑

Use ajax spider: ☐ with Firefox Headless

Attack Stop

Progress: Using traditional spider to discover the content

New Scan Progress: 0: http://192.168..132/mutillidae/ 18% Current Scans: 1 URLs Found: 162 Nodes Added: 7 Export

Processed	Method	URI	Flags
●	GET	http://192.168.30.132/mutillidae/index.php?do=toggle-security&page...	
●	GET	http://192.168.30.132/H1	
●	POST	http://192.168.30.132/mutillidae/index.php?page=set-background-colo...	
●	GET	http://192.168.30.132/mutillidae/index.php?choice=nmap&initials=ZA...	
●	GET	http://192.168.30.132/mutillidae/index.php?do=toggle-security&page...	
●	GET	http://www.textfiles.com/	Out of Scope
●	GET	http://192.168.30.132/mutillidae/index.php?do=toggle-security&page...	
●	POST	http://192.168.30.132/mutillidae/index.php?page=text-file-viewer.php	
●	POST	http://192.168.30.132/mutillidae/index.php?page=pen-test-tool-lookup...	

Alerts 0 4 6 2 Main Proxy: localhost:8080

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

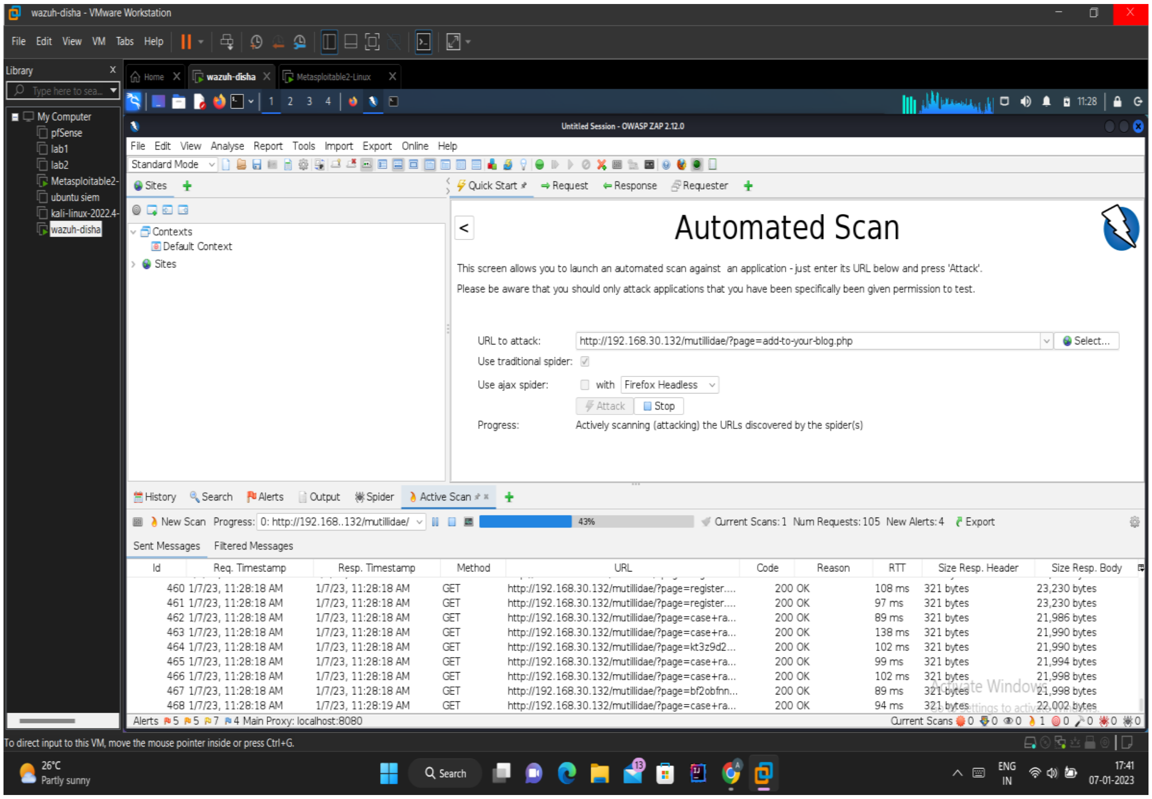
The easiest way to start using ZAP is via the Quick Start tab. Quick Start is a ZAP add-on that is included automatically when you installed ZAP.

To run a Quick Start Automated Scan:

1. Start ZAP and click the **Quick Start** tab of the Workspace Window.
2. Click the large Automated Scan button.
3. In the **URL to attack** text box, enter the full URL of the web application you want to attack.
4. Click the **Attack**

ZAP will proceed to crawl the web application with its spider and passively scan each page it finds. Then ZAP will use the active scanner to attack all of the discovered pages, functionality, and parameters.

ZAP provides 2 spiders for crawling web applications; you can use either or both of them from this screen. The traditional ZAP spider which discovers links by examining the HTML in responses from the web application. This spider is fast, but it is not always effective when exploring an AJAX web application that generates links using JavaScript.


wazuh-disha - VMware Workstation
Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
History
Search
Alerts
Output
Spider
Active Scan

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://192.168.30.132/mutillidae/?page=add-to-your-blog.php

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Attack Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

New Scan Progress: 0: http://192.168..132/mutillidae/ 43% Current Scans: 1 Num Requests: 105 New Alerts: 4 Export

Sent Messages Filtered Messages

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
460	1/7/23, 11:28:18 AM	1/7/23, 11:28:18 AM	GET	http://192.168.30.132/mutillidae/?page=register....	200	OK	108 ms	321 bytes	23,230 bytes
461	1/7/23, 11:28:18 AM	1/7/23, 11:28:18 AM	GET	http://192.168.30.132/mutillidae/?page=register....	200	OK	97 ms	321 bytes	23,230 bytes
462	1/7/23, 11:28:18 AM	1/7/23, 11:28:18 AM	GET	http://192.168.30.132/mutillidae/?page=case+ra...	200	OK	89 ms	321 bytes	21,986 bytes
463	1/7/23, 11:28:18 AM	1/7/23, 11:28:18 AM	GET	http://192.168.30.132/mutillidae/?page=case+ra...	200	OK	138 ms	321 bytes	21,990 bytes
464	1/7/23, 11:28:18 AM	1/7/23, 11:28:18 AM	GET	http://192.168.30.132/mutillidae/?page=kt3z9d2...	200	OK	102 ms	321 bytes	21,990 bytes
465	1/7/23, 11:28:18 AM	1/7/23, 11:28:18 AM	GET	http://192.168.30.132/mutillidae/?page=case+ra...	200	OK	99 ms	321 bytes	21,994 bytes
466	1/7/23, 11:28:18 AM	1/7/23, 11:28:18 AM	GET	http://192.168.30.132/mutillidae/?page=case+ra...	200	OK	102 ms	321 bytes	21,998 bytes
467	1/7/23, 11:28:18 AM	1/7/23, 11:28:18 AM	GET	http://192.168.30.132/mutillidae/?page=bf2obfnn...	200	OK	89 ms	321 bytes	21,998 bytes
468	1/7/23, 11:28:18 AM	1/7/23, 11:28:19 AM	GET	http://192.168.30.132/mutillidae/?page=case+ra...	200	OK	94 ms	321 bytes	22,002 bytes

Alerts 5 5 7 4 Main Proxy: localhost:8080 Current Scans 0 0 0 1 0 0 0 0

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

ZAP will passively scan all of the requests and responses proxied through it. So far ZAP has only carried out passive scans of your web application. Passive scanning does not change responses in any way and is considered safe. Scanning is also performed in a background thread to not slow down exploration. Passive scanning is good at finding some vulnerabilities and as a way to get a feel for the basic security state of a web application and locate where more investigation may be warranted.

Active scanning, however, attempts to find other vulnerabilities by using known attacks against the selected targets. Active scanning is a real attack on those targets and can put the targets at risk, so do not use active scanning against targets you do not have permission to test.

Interpret Your Test Results

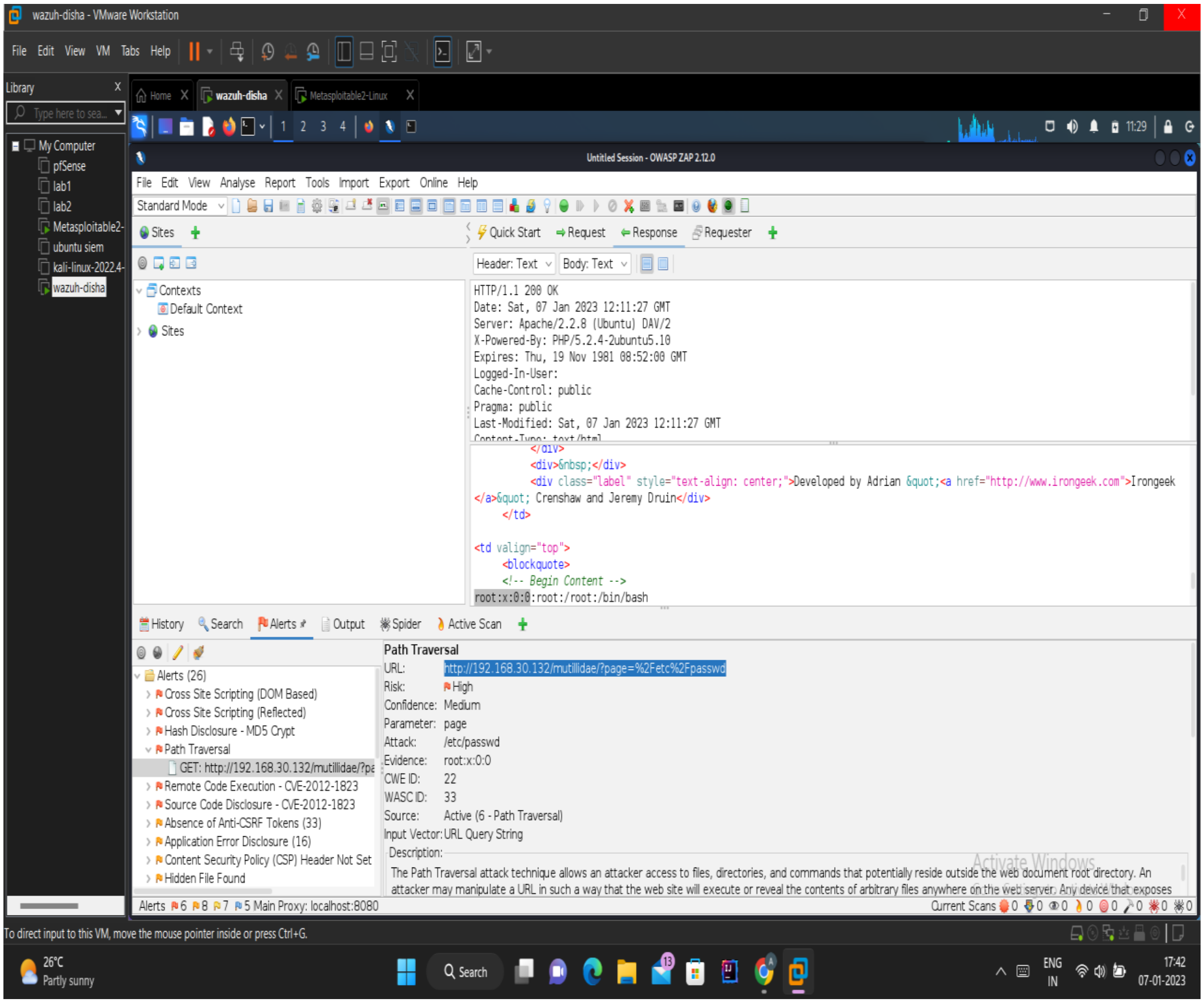
As ZAP spiders your web application, it constructs a map of your web applications' pages and the resources used to render those pages. Then it records the requests and responses sent to each page and creates alerts if there is something potentially wrong with a request or response.

➔ View Alerts and Alert details

The left-hand side of the Footer contains a count of the Alerts found during your test, broken out into risk categories.

To view the alerts created during your test:

1. Click the **Alerts** tab in the Information Window.
2. Click each alert displayed in that window to display the URL and the vulnerability detected in the right side of the Information Window.
3. In the Workspace Windows, click the **Response** tab to see the contents of the header and body of the response. The part of the response that generated the alert will be highlighted.



```
HTTP/1.1 200 OK
Date: Sat, 07 Jan 2023 12:11:27 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Logged-In-User:
Cache-Control: public
Pragma: public
Last-Modified: Sat, 07 Jan 2023 12:11:27 GMT
Content-Type: text/html
```

```
            </div>
            <div>&nbsp;</div>
            <div class="label" style="text-align: center;">Developed by Adrian &quot;<a href="http://www.irongeek.com">Irongeek
</a>&quot; Crenshaw and Jeremy Druin</div>
        </td>

<td valign="top">
        <blockquote>
        <!-- Begin Content -->
root:x:0:0:root:/root:/bin/bash
```

- Alerts (26)
  - Cross Site Scripting (DOM Based)
  - Cross Site Scripting (Reflected)
  - Hash Disclosure - MD5 Crypt
  - Path Traversal
    - GET: http://192.168.30.132/mutillidae/?pa
  - Remote Code Execution - CVE-2012-1823
  - Source Code Disclosure - CVE-2012-1823
  - Absence of Anti-CSRF Tokens (33)
  - Application Error Disclosure (16)
  - Content Security Policy (CSP) Header Not Set
  - Hidden File Found

Path Traversal

URL:	http://192.168.30.132/mutillidae/?page=%2Fetc%2Fpasswd
Risk:	High
Confidence:	Medium
Parameter:	page
Attack:	/etc/passwd
Evidence:	root:x:0:0
CWE ID:	22
WASC ID:	33
Source:	Active (6 - Path Traversal)
Input Vector:	URL Query String

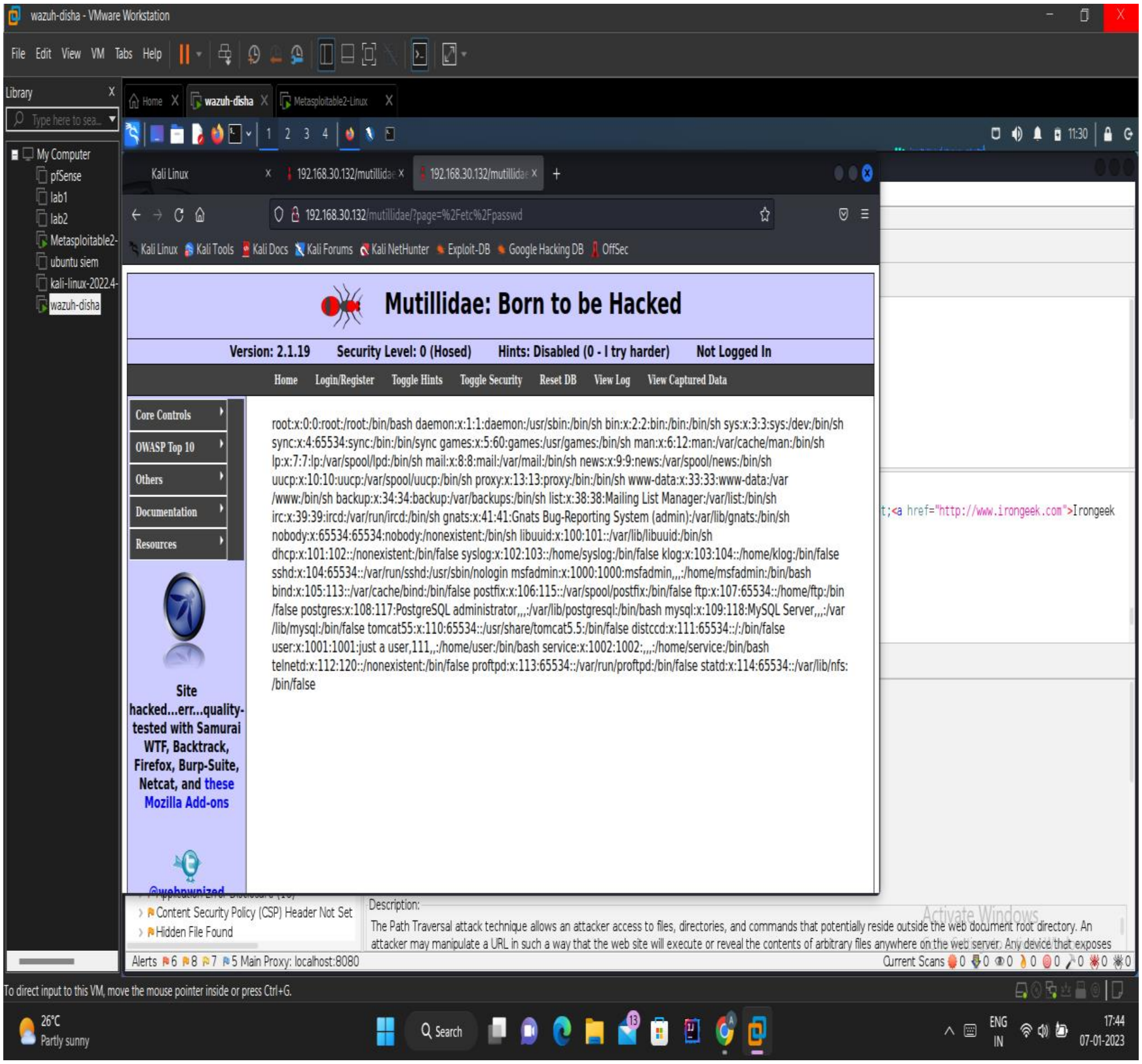
Description:

The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes

Alerts 6 8 7 5 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

➔ Exploit through the link obtained in path traversal

Copy the link and paste it in Firefox to see the Usernames of the mutillidae vulnerable website and know various things.



wazuh-disha - VMware Workstation
192.168.30.132/mutillidae/?page=%2Fetc%2Fpasswd
Mutillidae: Born to be Hacked
Version: 2.1.19
Security Level: 0 (Hosed)
Hints: Disabled (0 - I try harder)
Not Logged In
Home
Login/Register
Toggle Hints
Toggle Security
Reset DB
View Log
View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var
/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin
/false postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var
/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:
/bin/false
```

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
Content Security Policy (CSP) Header Not Set
Hidden File Found

Description:
The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes

Alerts 6 8 7 5 Main Proxy: localhost:8080
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C Partly sunny
17:44 07-01-2023

CHAPTER 7: APPLICATIONS

- **It helps you satisfy compliance requirements.** Pen testing is explicitly required in some industries, and performing web application pen testing helps meet this requirement.
- **It helps you assess your infrastructure.** Infrastructure, like firewalls and DNS servers, is public-facing. Any changes made to the infrastructure can make a system vulnerable. Web application pen testing helps identify real-world attacks that could succeed at accessing these systems.
- **It identifies vulnerabilities.** Web application pen testing identifies loopholes in applications or vulnerable routes in infrastructure—before an attacker does.
- **It helps confirm security policies**. Web application pen testing assesses existing security policies for any weaknesses.
- **Identify Cybersecurity Weaknesses.** Cybersecurity weaknesses can range from outdated software to weak admin passwords. They can create unauthorized entry points for malicious actors to gain access. Being able to see those holes is the first step to mending them.
- **Validate Cybersecurity Policies.** Cybersecurity policies and controls are great ways to document and maintain a culture of security, but they need to work properly to be effective. Websites need to have secure input validation rules to keep the backend working correctly. Web App engineers can validate the efficacy of these rules.
- **Test Digital Infrastructure.** Although smaller websites and older websites are more prone to security vulnerabilities, all websites have some level of risk. If it has been a while since your website has been evaluated for security, it might be time for a check-up.
- **Ensure Cybersecurity Is Compliant.** Many industries are tied to compliance standards that require specific security controls. Websites are also subject to compliance, and they need to be verified and documented as safe in order to manage liability.

CHAPTER 8: CONCLUSION

Unlike the “old school” applications, web applications offer a lot to the market in terms of commerciality and usefulness. They bring functionality to the internet but for a cost.

These systems are usually publicly available and hence exposed to the internet at all times. Because of the growing popularity and presence on the internet, web applications usually carry vulnerabilities in their design and configuration which malicious hackers find and exploit. Since these systems are almost always internet facing, they carry a greater risk with them and should automatically be a priority when it comes to penetration testing.

If the application handles some credit card data, personal information or even health records, it would be in a company’s best interest to perform annual web application penetration testing in order to meet regulatory compliance that most of the data requires. In cases where penetration testing is not required, it is highly recommended as the best mean to meet the best security standards, then to avoid performing it.

With varying tools to choose from, web application penetration testing has developed a much more structured approach to automated and manual testing. Choosing any open-source security solutions is highly recommended with the availability of commercial versions of the same tool with upgraded capabilities.

To end with, web application penetration testing involves testing the application’s environment, database connectivity, source code, bad data and error data in order to find vulnerabilities and exploit them.