Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 1

Aim: 1. Configuration of Burp Suite
2. Installation of Mutillidae

Lab Outcome: To configure and install various web application security Tools

Theory:

Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

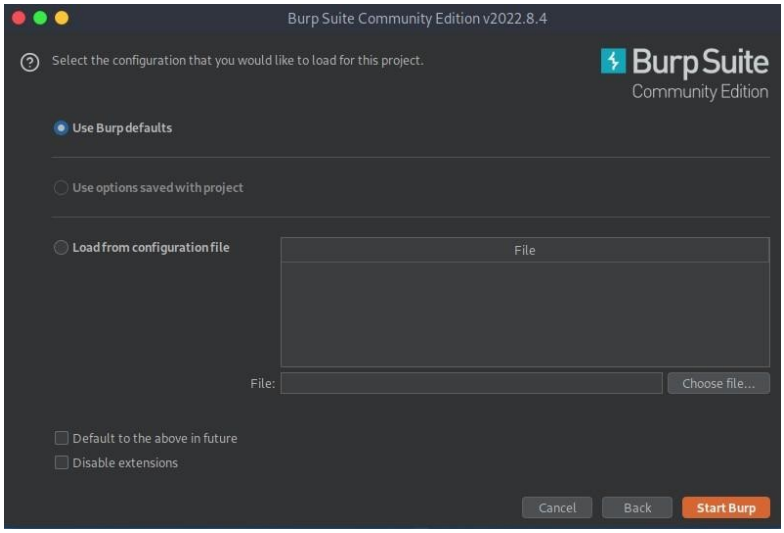
Mutillidae

It is a web application deliberately created for the purpose of teaching and practicing web application security testing. It is often referred to as "OWASP Mutillidae II" because it is a part of the OWASP (Open Web Application Security Project) project.

OWASP Mutillidae II is designed as a vulnerable web application, meaning it contains various security flaws and vulnerabilities intentionally introduced into its codebase. These vulnerabilities represent common issues found in real-world web applications and are meant to be used as a training platform for security professionals, penetration testers, and developers to learn how to identify and address such security weaknesses.

The primary goal of Mutillidae is to provide a safe and controlled environment where individuals can practice their web application security testing skills without the risk of affecting real applications or networks. Users can test various techniques, tools, and methodologies to discover and exploit the vulnerabilities within Mutillidae.

Output: Burp suite



Mutillidae:

1. Install Metasploitable 2 https://sourceforge.net/projects/metasploitable/
2. Start Metasploitable 2 in Virtual Machine.
3. Then put login id and password as “msfadmin”

```
 * Starting periodic command scheduler crond                       [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                        [ OK ]
 * Starting web server apache2                                     [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                  [ OK ]

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: _
```

1. Enter the below command

```
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc_
```

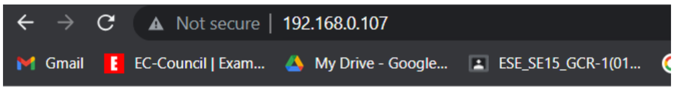
2. Change the dbname from metasploit to owasp10

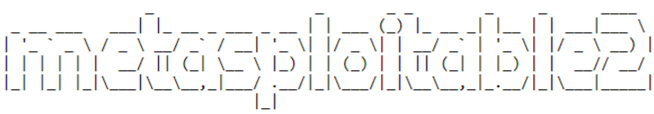
```
  GNU nano 2.0.7       File: /var/www/mutillidae/config.inc

<?php
        /* NOTE: On Samurai, the $dbpass password is "samurai" rather than blan$

        $dbhost = 'localhost';
        $dbuser = 'root';
        $dbpass = '';
        $dbname = 'metasploit';
?>

                [ Read 8 lines (Converted from DOS format) ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

```
  GNU nano 2.0.7       File: /var/www/mutillidae/config.inc          Modified

<?php
        /* NOTE: On Samurai, the $dbpass password is "samurai" rather than blan$

        $dbhost = 'localhost';
        $dbuser = 'root';
        $dbpass = '';
        $dbname = 'owasp10';
?>

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

3. Query the Metasploitable machine for its ip-address and paste it in the browser.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:1e:7f:2d
          inet addr:192.168.0.107  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1e:7f2d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9613 (9.3 KB)  TX bytes:8086 (7.8 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:101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23573 (23.0 KB)  TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$
```

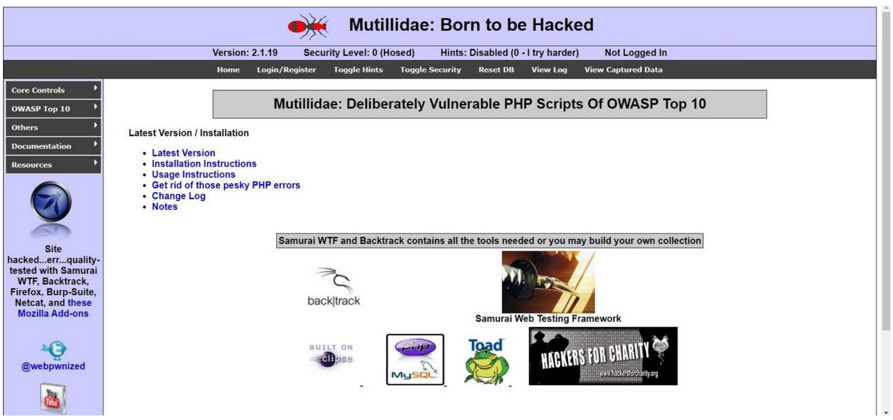




```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

4. Then select the Mutillidae option.



Conclusion:

Here we successfully configured and installed Burp Suite and Mutillidae.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 2

Aim: Crawling the web application using Burp Spider/Site map.

Lab Outcome: To identify and manage vulnerabilities of web Applications and execute mitigation plans.

Theory:
In Burp Suite, the "Site Map" is a comprehensive representation of all the requests and responses made by the web application being tested. It provides an organized and structured view of the application's entire communication with the server, allowing security testers and developers to analyze and interact with the captured data.

The Site Map in Burp Suite includes the following components:

URLs: The URLs of all the requests made by the web application are listed in the Site Map. Each URL represents a unique endpoint that the application interacts with.

HTTP Requests and Responses: For each URL, Burp Suite records the corresponding HTTP requests sent by the application and the corresponding server responses.

Parameters: Burp Suite extracts and lists all the parameters (query parameters, form parameters, cookies, etc.) present in the requests.

HTTP Methods: The HTTP methods (GET, POST, PUT, DELETE, etc.) used by the application are identified and displayed in the Site Map.

Status Codes: The status codes returned by the server in response to each request are recorded, providing valuable information about the success or failure of the requests.

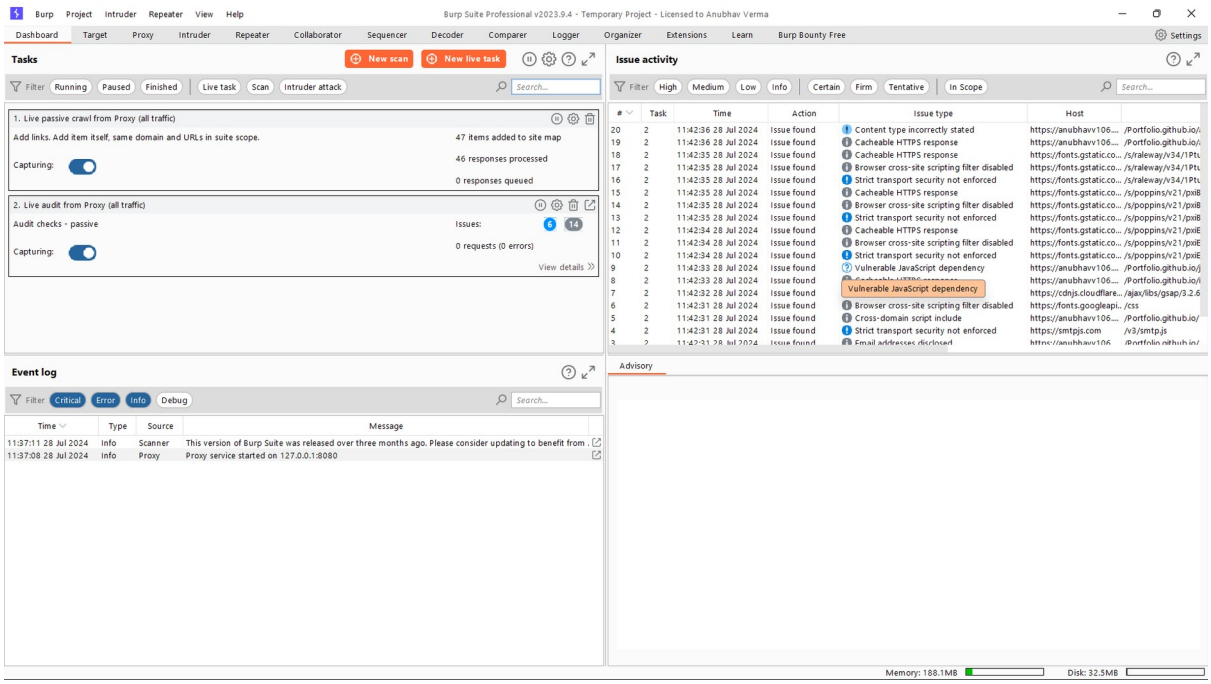
Request and Response Details: By clicking on a specific request or response in the Site Map, you can view the detailed information, including headers, cookies, and body data.

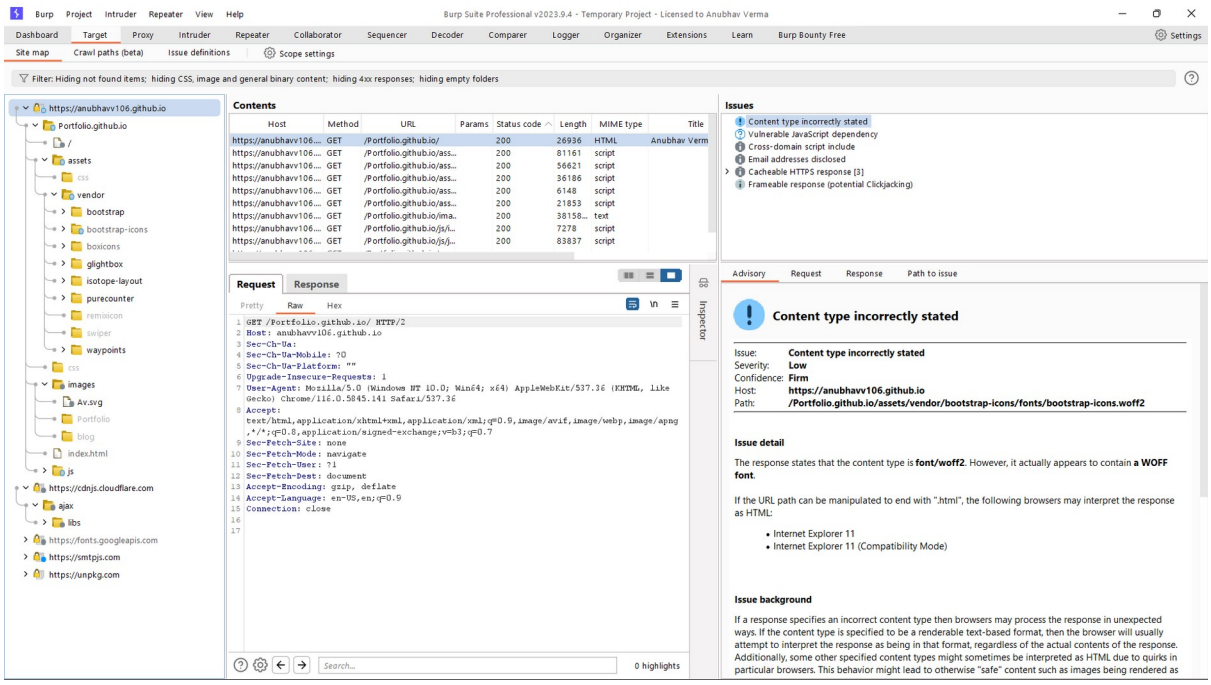
Session Management: Burp Suite automatically manages session information, such as session cookies, which helps maintain the state during testing.

Filtering and Searching: Burp Suite allows you to filter and search the Site Map based on specific criteria, making it easier to locate and analyze relevant requests.

The Site Map is an essential feature in Burp Suite as it serves as a central hub for all captured communication between the client (web browser or application) and the server. It provides testers with a complete overview of how the application interacts with the server, making it easier to identify security vulnerabilities, analyze requests and responses, and perform targeted testing.

Output:





Conclusion:

Here we have crawled the web application using Burp Spider/Site map.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 3

Aim: Identify and Manage vulnerabilities by Replaying web requests using the Repeater tab

Lab Outcome: To identify and manage vulnerabilities of web Applications and execute mitigation plans.

Theory:
Repeater is best suited for the kind of task where we need to send the same request numerous times, usually with small changes in between requests. For example, we may wish to manually test for an SQL Injection vulnerability, attempt to bypass a web application firewall filter, or simply add or change parameters in a form submission.

Here's how the Repeater tool typically works:

1. Capture Request: The first step is to capture an HTTP request using Burp Suite's proxy functionality. This can be done by setting up your browser or other applications to route their traffic through Burp's proxy. As you browse the web application, Burp Suite captures all the requests and responses, allowing you to analyze and manipulate them later.

2. Send to Repeater: Once you've captured a request that you're interested in, you can send it to the Repeater tool for further analysis and testing. In the Repeater tab, you'll see the captured request in its entirety.

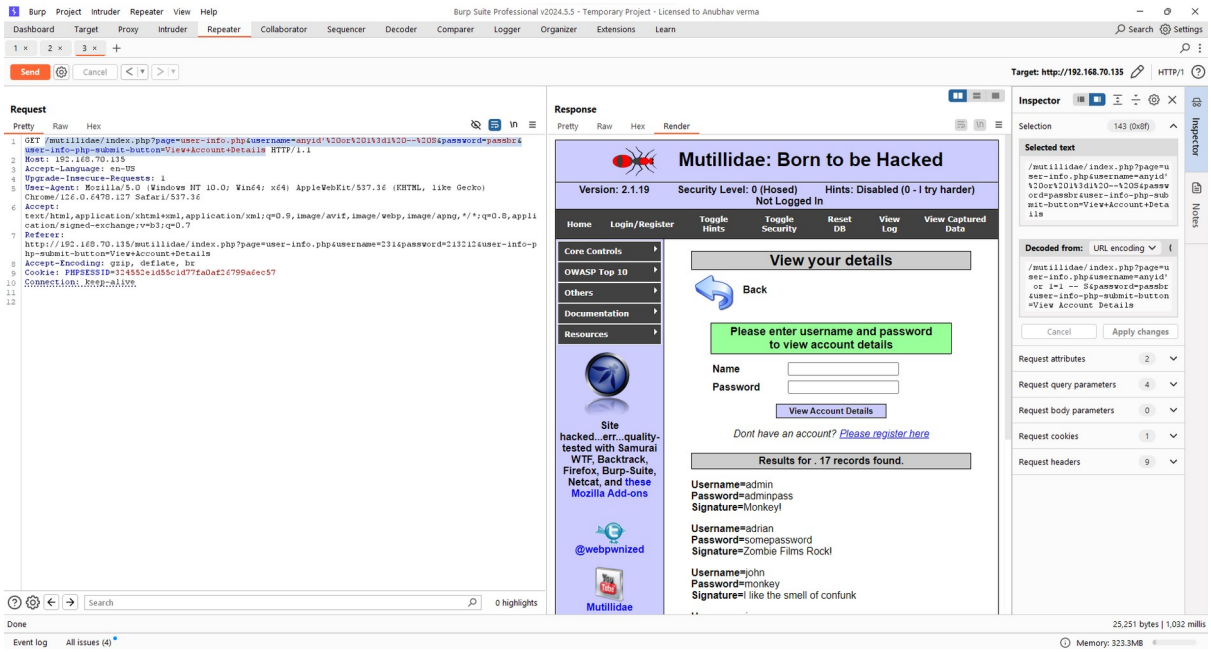
3. Manual Manipulation: In the Repeater interface, you can manually modify various aspects of the request, such as headers, parameters, cookies, and request body. This allows you to test for vulnerabilities like SQL injection, Cross-Site Scripting (XSS), and other security issues by injecting payloads and observing the application's response.

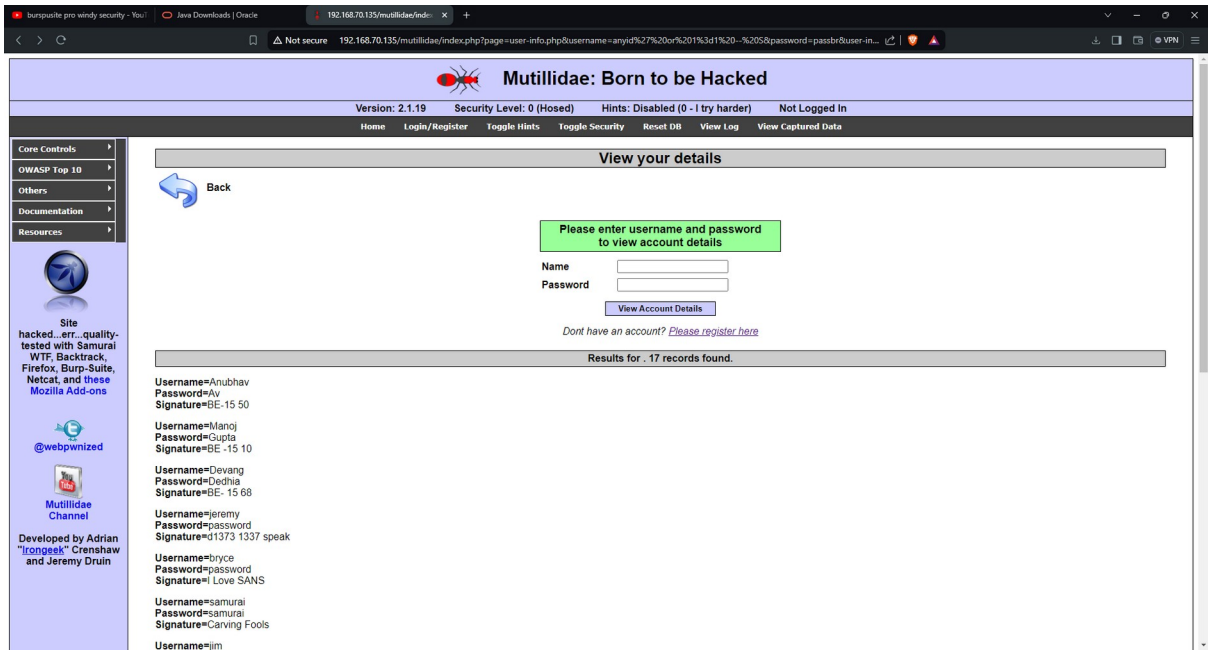
4. Resend and Observe: After making changes to the request, you can resend it to the target web application and observe how the application responds. The responses are displayed in the Repeater interface, providing valuable insight into how the application handles different inputs.

5. Iterative Testing: The Repeater tool is particularly useful for iterative testing. You can make small changes to the request, observe the effects, and then adjust your inputs based on the application's responses. This helps security testers fine-tune their attack payloads and gain a deeper understanding of the application's behavior.

6. Response Analysis: The Repeater interface displays both the raw response content and any associated details, such as HTTP status codes, headers, and response times. This information is critical for identifying potential vulnerabilities and understanding the application's behavior.

Output:





Conclusion:

Here we were able to identify and manage vulnerabilities by replaying web requests using the Repeater tab.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 4

Aim: Identify the target web application and gather relevant information such as the application's technology stack, URLs, endpoints, and any other publicly available information.

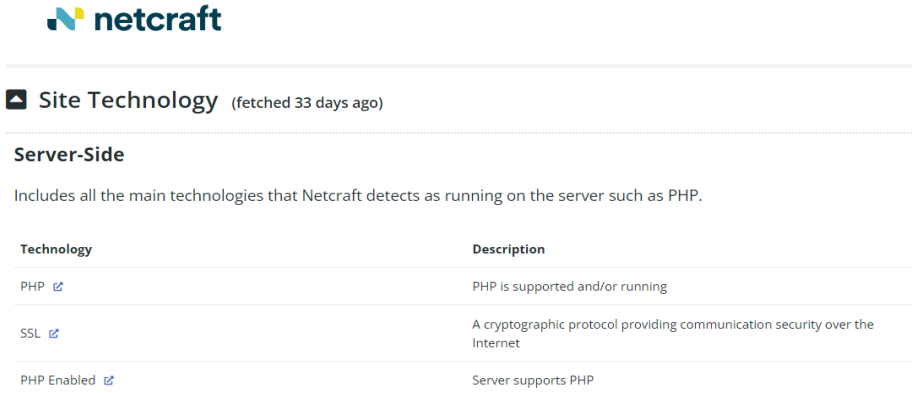
Lab Outcome: To perform web penetration testing and organize a checklist using burp suite.

Theory:

Definition and Scope:
OSINT refers to the collection and analysis of information that is publicly accessible through open sources. These sources encompass a wide range of materials, including online content, media, publications, and publicly available documents. OSINT doesn't involve any covert or classified methods; instead, it focuses on utilizing data that is openly accessible.

Key Principles:
1. Legality and Ethics: OSINT practitioners must operate within legal boundaries and adhere to ethical standards. Respect for privacy, copyright, terms of service, and local laws is paramount.
2. Verification: Information collected through OSINT should be verified and cross-referenced to ensure accuracy and reliability.
3. Contextualization: Understanding information within its context is crucial to draw accurate conclusions.
4. Holistic Approach: OSINT involves collecting data from various sources to form a complete picture.
5. Continuous Monitoring: The digital landscape is dynamic; ongoing monitoring ensures up-to-date information.

Output:
Netcraft: Netcraft provides information about the website's hosting infrastructure, server software, and historical data related to the domain.



Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

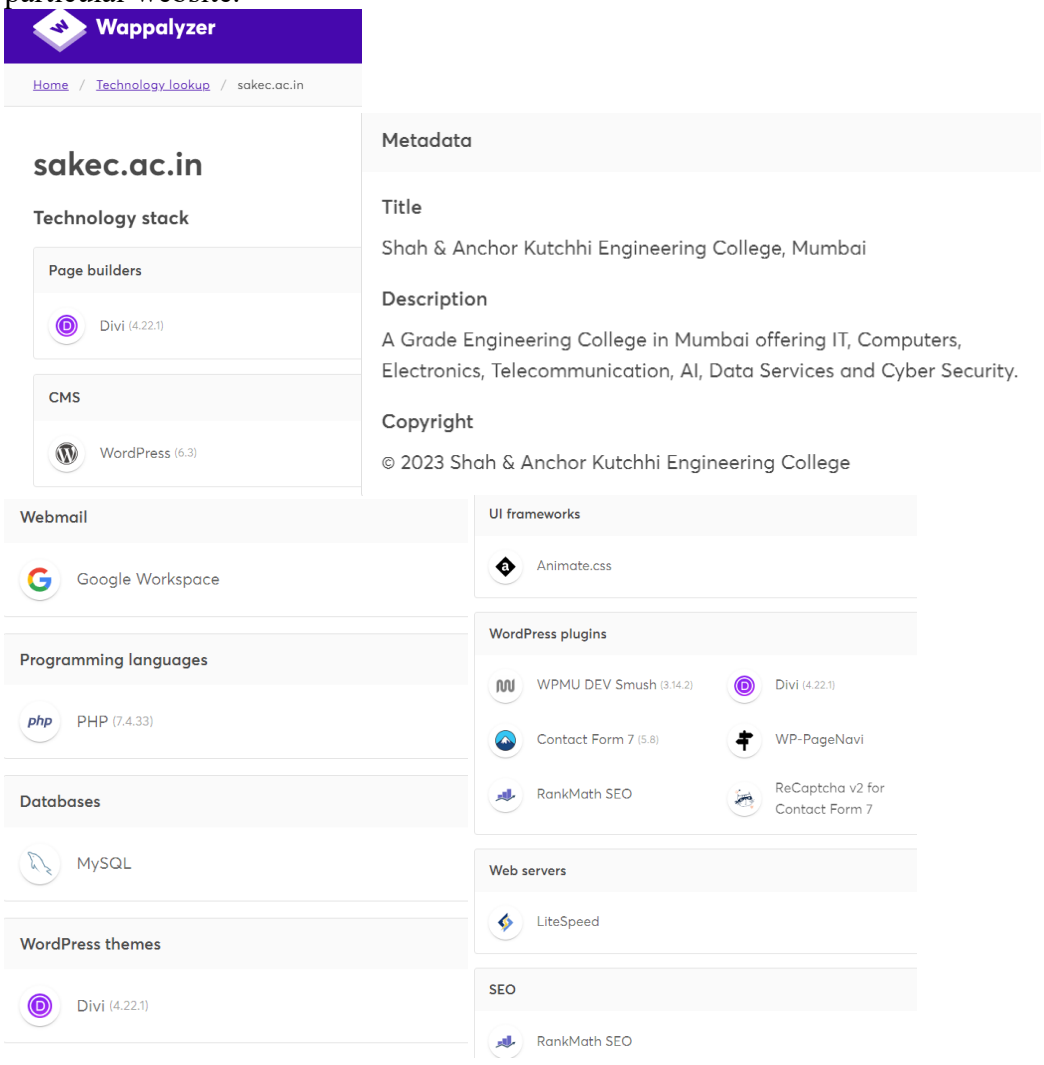
Technology	Description
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites

PHP Application

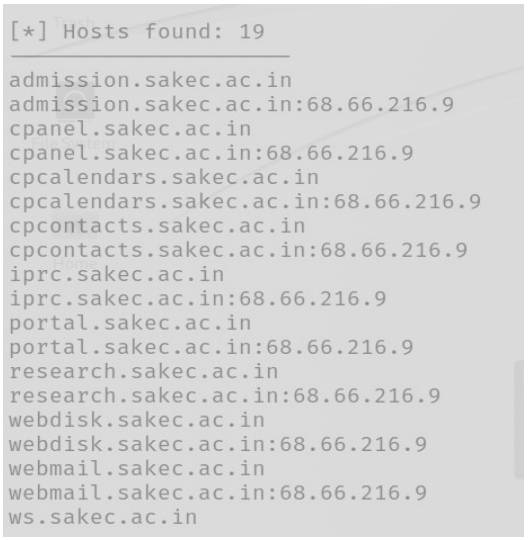
PHP is an open source server-side scripting language designed for Web development to produce dynamic Web pages.

Technology	Description
WordPress	Free and open source blogging tool and a content management system (CMS) based on PHP and MySQL

Wappalyzer: Here also we were able to get information about the technologies used by the particular website.

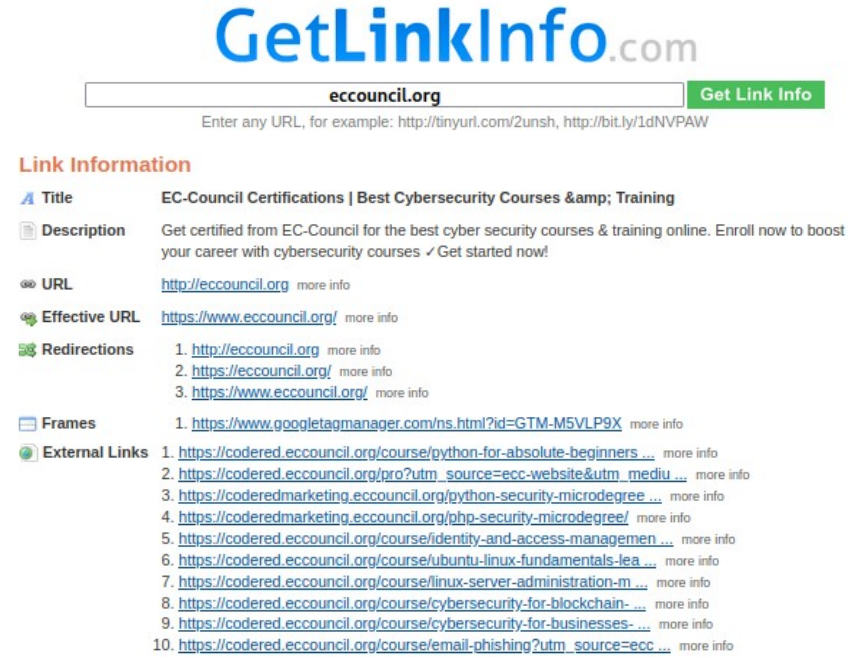


theHarvester: Here we were able to enumerate the host and email addresses associated with the particular domain.



Dnsdumpster: Dnsdumpster helps identify IP addresses associated with domains and provides insights into domain relationships and DNS information.

GetLinkInfo: This tool is used to extract detailed information from URLs, including title, description, external links, and redirections.



Conclusion:
Here we were able to gather information and perform reconnaissance using OSINT.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 5

Aim: Use open-source intelligence (OSINT) techniques to gather information about the application, its infrastructure, and potential vulnerabilities.

Lab Outcome: To perform web penetration testing and organize a checklist using burp suite.

Theory:

Open-Source Intelligence (OSINT) is a multifaceted discipline that involves collecting, analyzing, and utilizing information from publicly available sources to generate actionable insights. OSINT serves various purposes, including intelligence gathering, threat assessment, risk analysis, decision-making, and more.

Here's a comprehensive theoretical overview of OSINT:

Definition and Scope:
OSINT refers to the collection and analysis of information that is publicly accessible through open sources. These sources encompass a wide range of materials, including online content, media, publications, and publicly available documents. OSINT doesn't involve any covert or classified methods; instead, it focuses on utilizing data that is openly accessible.

Key Principles:

1. Legality and Ethics: OSINT practitioners must operate within legal boundaries and adhere to ethical standards. Respect for privacy, copyright, terms of service, and local laws is paramount.

2. Verification: Information collected through OSINT should be verified and cross-referenced to ensure accuracy and reliability.

3. Contextualization: Understanding information within its context is crucial to draw accurate conclusions.

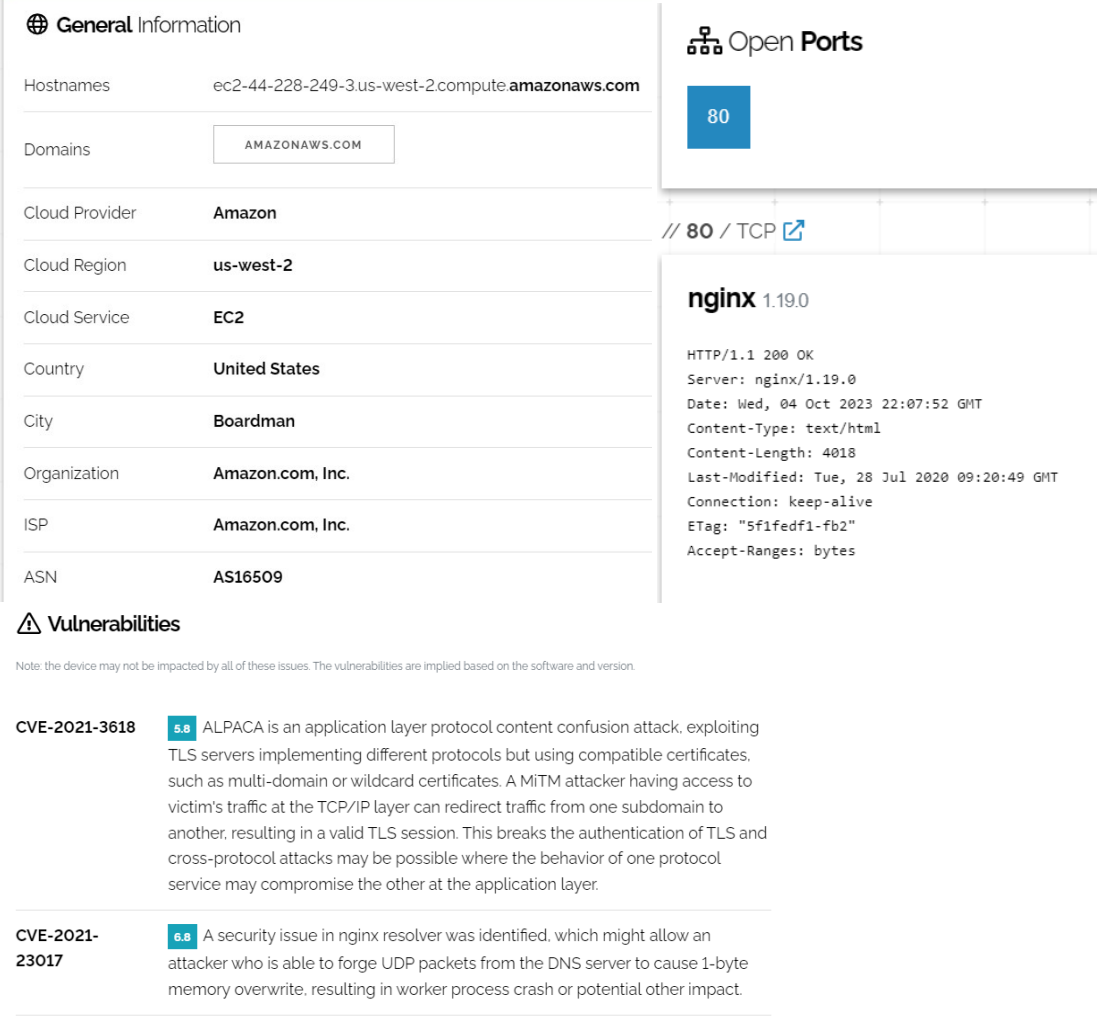
4. Holistic Approach: OSINT involves collecting data from various sources to form a complete picture.

5. Continuous Monitoring: The digital landscape is dynamic; ongoing monitoring ensures up-to-date information.

Output:

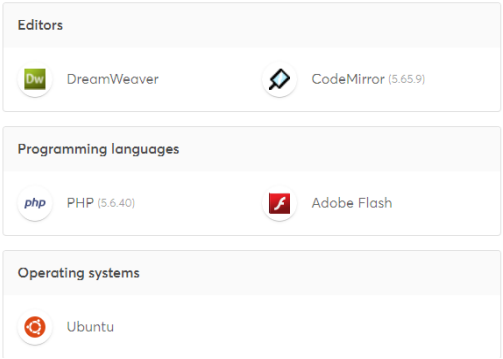
Shodan:

Here we were able to gather information about the infrastructure (technologies used by a web application) using **SHODAN**.



Wappalyzer:

Here also we were able to get information about the technologies used by the particular website.



Nikto:

Here we got information about the vulnerabilities that is present in the particular domain

```
┌──(kali㉿kali)-[~]
└─$ nikto -url http://testphp.vulnweb.com/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2023-10-09 07:23:57 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/do
ions
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of t
to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-t
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.com/en-us/previous-vers
-windows-silverlight/cc197955(v=vs.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards
/vulnerabilities/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdom
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2023-10-09 07:26:04 (GMT-4) (127 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

WhatWeb:

Here we got more information about the plugins as well as it also identifies version numbers, web framework modules, etc

```
└─$ whatweb -a 1 -v http://testphp.vulnweb.com/
WhatWeb report for http://testphp.vulnweb.com/
Status    : 200 OK
Title     : Home of Acunetix Art
IP        : 44.228.249.3
Country   : UNITED STATES, US

Summary   : ActiveX[D27CDB6E-AE6D-11cf-96B8-444553540000], Adobe-Flash, Email[wvs@acunetix.com], HTTPServer[n
ginx/1.19.0], nginx[1.19.0], Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#versi
on=6,0,29,0][clsid:D27CDB6E-AE6D-11cf-96B8-444553540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1], Script
[text/JavaScript], X-Powered-By[PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1]

Detected Plugins:
[ ActiveX ]
        ActiveX is a framework based on Microsoft's Component
        Object Model (COM) and Object Linking and Embedding (OLE)
        technologies. ActiveX components officially operate only
        with Microsoft's Internet Explorer web browser and the
        Microsoft Windows operating system. - More info:
        http://en.wikipedia.org/wiki/ActiveX

        Module       : D27CDB6E-AE6D-11cf-96B8-444553540000

[ Adobe-Flash ]
        This plugin identifies instances of embedded adobe flash
        files.

        Google Dorks: (1)
        Website     : https://get.adobe.com/flashplayer/
```

```
[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
        tags. We match syntactically invalid links containing
        mailto: to catch anti-spam email addresses, eg. bob at
        gmail.com. This uses the simplified email regular
        expression from
        http://www.regular-expressions.info/email.html for valid
        email address matching.

        String       : wvs@acunetix.com
        String       : wvs@acunetix.com

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : nginx/1.19.0 (from server string)

[ Object ]
        HTML object tag. This can be audio, video, Flash, ActiveX,
        Python, etc. More info:
        http://www.w3schools.com/tags/tag_object.asp

        Module       : clsid:D27CDB6E-AE6D-11cf-96B8-444553540000 (from classid)
        String       : http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0
```

```
[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 5.6.40-38+ubuntu20.04.1+deb.sury.org+1
        Google Dorks: (2)
        Website      : http://www.php.net/

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       : text/JavaScript

[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 (from x-powered-by string)

[ nginx ]
        Nginx (Engine-X) is a free, open-source, high-performance
        HTTP server and reverse proxy, as well as an IMAP/POP3
        proxy server.

        Version      : 1.19.0
        Website      : http://nginx.net/
```

```
HTTP Headers:
        HTTP/1.1 200 OK
        Server: nginx/1.19.0
        Date: Mon, 09 Oct 2023 11:28:49 GMT
        Content-Type: text/html; charset=UTF-8
        Transfer-Encoding: chunked
        Connection: close
        X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
        Content-Encoding: gzip


┌──(kali㉿kali)-[~]
└─$ whatweb -a 3  http://testphp.vulnweb.com/
http://testphp.vulnweb.com/ [200 OK] ActiveX[D27CDB6E-AE6D-11cf-96B8-444553540000], Adobe-Flash, Country[UNITED STATES][US], Email[wvs@acunetix.com], HTTPServer[nginx/1.19.0], IP[44.228.249.3], Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0][clsid:D27CDB6E-AE6D-11cf-96B8-444553540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1], Script[text/JavaScript], Title[Home of Acunetix Art], X-Powered-By[PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1], nginx[1.19.0]
```

Conclusion:

Use open-source intelligence (OSINT) techniques to gather information about the application, its infrastructure, and potential vulnerabilities.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 1

Aim: a) Perform Email Header Analysis for extracting valuable information like sender IP address, email servers, and routing information.

b) Conduct email address enumeration by attempting to verify the existence of email addresses within a target domain. Use tools like the Harvester or thehunter.io to search for email addresses associated with a specific domain. This can help identify valid email addresses within an organization
c) Analyze the metadata of an email, including date and time stamps, email clients used, or the originating IP address, email's origin, potential geographic location of the sender, or possible email routing

Lab outcome: Conduct advanced searches to gather intelligence and apply advanced OSINT search techniques and tools.

Theory:
Email header analysis is a process of examining the header section of an email to extract valuable information about the email's origin, path, and routing details. This information can be useful for various purposes, such as identifying the source of spam or phishing emails, tracing the origin of suspicious emails, and understanding the email delivery path.

The email header is a crucial part of an email message and contains essential metadata about the message's journey from the sender to the recipient. It consists of various fields, each providing specific details about the email's origin, routing, and delivery. Some of the key fields that can be analyzed for extracting valuable information are:

From: This field contains the email address of the sender. It is essential to verify the sender's address to identify possible spoofing or phishing attempts.

Received: This field appears multiple times in the email header, and each occurrence indicates a hop in the email delivery path. The received field typically includes the IP address of the email server that handled the message, along with the timestamp. By analyzing these entries, it's possible to trace the email's route and identify any suspicious or unauthorized servers in the path.

Return-Path: This field indicates the email address to which delivery errors and bounce-backs will be sent. It is used by mail servers to handle undeliverable emails.

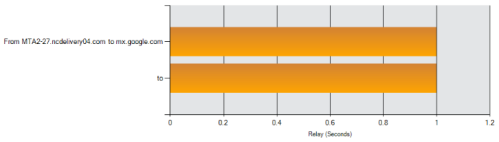
Received-SPF: Sender Policy Framework (SPF) is an email authentication method that helps prevent email spoofing. This field indicates whether the email passed SPF authentication and can provide insights into the email's legitimacy.

Output:

MXtoolbox: MXtoolbox provides email-related diagnostic tools, including the ability to analyze email headers. It can extract information like sender IP addresses, sender domains, and mail server details from email headers.

Relay Information

Received Delay:	0 seconds



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	MTA2-27.ncdelivery04.com 103.52.180.27	mx.google.com	ESMTP	8/3/2023 11:59:03 AM	
2	0 seconds		2002:a05:6359:5ea5:b0:121:40d8:e401	SMTP	8/3/2023 11:59:03 AM	

SPF and DKIM Information

dmarc:internshala.com Show Solve Email Delivery Problems

```
v=DMARC1; p=reject;  pct=100; rua=mailto:aseem@internshala.com; ruf=mailto:aseem@internshala.com; sp=reject; ri=21600
```

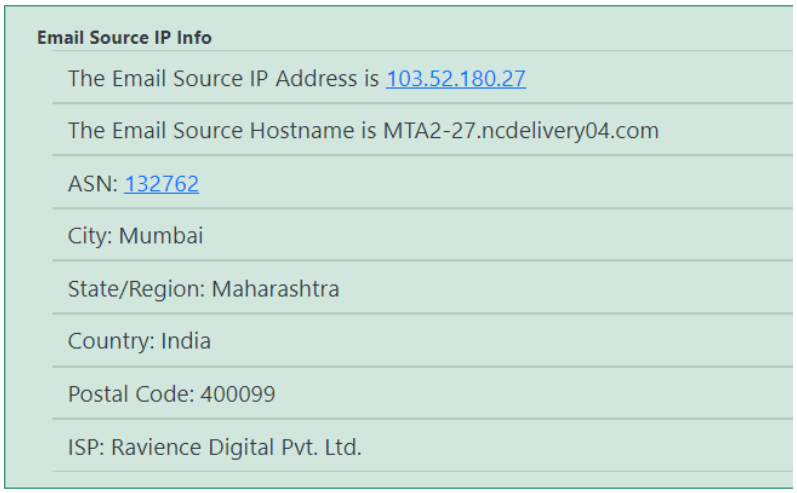
spf:env.updates.internshala.com:103.52.180.27 Hide Solve Email Delivery Problems

```
v=spf1 include:ncapp02.com ip4:162.243.208.38/32 ip4:162.243.45.184/32 ip4:104.131.205.189/32 ip4:165.227.80.60/32 ip4:208.116.243.11/27 ip4:67.205.65.51/29 ~all
```

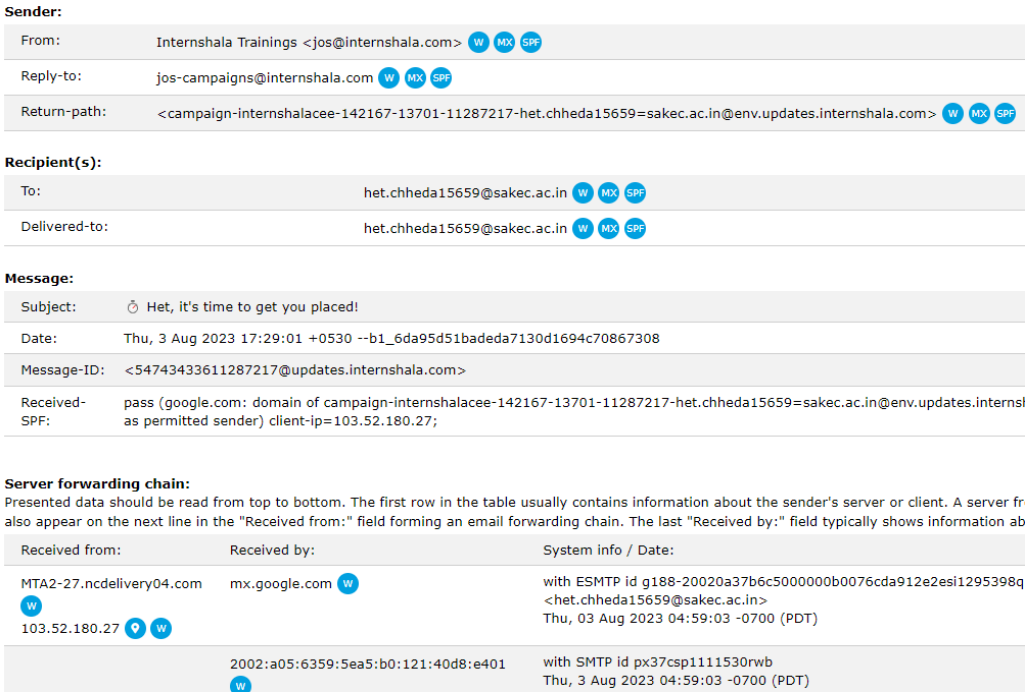
Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	include	ncapp02.com	Pass	The specified domain is searched for an 'allow'.
+	ip4	162.243.208.38/32	Pass	Match if IP is in the given range.
+	ip4	162.243.45.184/32	Pass	Match if IP is in the given range.
+	ip4	104.131.205.189/32	Pass	Match if IP is in the given range.
+	ip4	165.227.80.60/32	Pass	Match if IP is in the given range.
+	ip4	208.116.243.11/27	Pass	Match if IP is in the given range.
+	ip4	67.205.65.51/29	Pass	Match if IP is in the given range.
~	all		SoftFail	Always matches. It goes at the end of your record

	Test	Result
✓	SPF Record Published	SPF Record found
✓	SPF Record Deprecated	No deprecated records found
✓	SPF Multiple Records	Less than two records found
✓	SPF Alignment	Domain found in SPF
✓	SPF Contains characters after ALL	No items after 'ALL'.

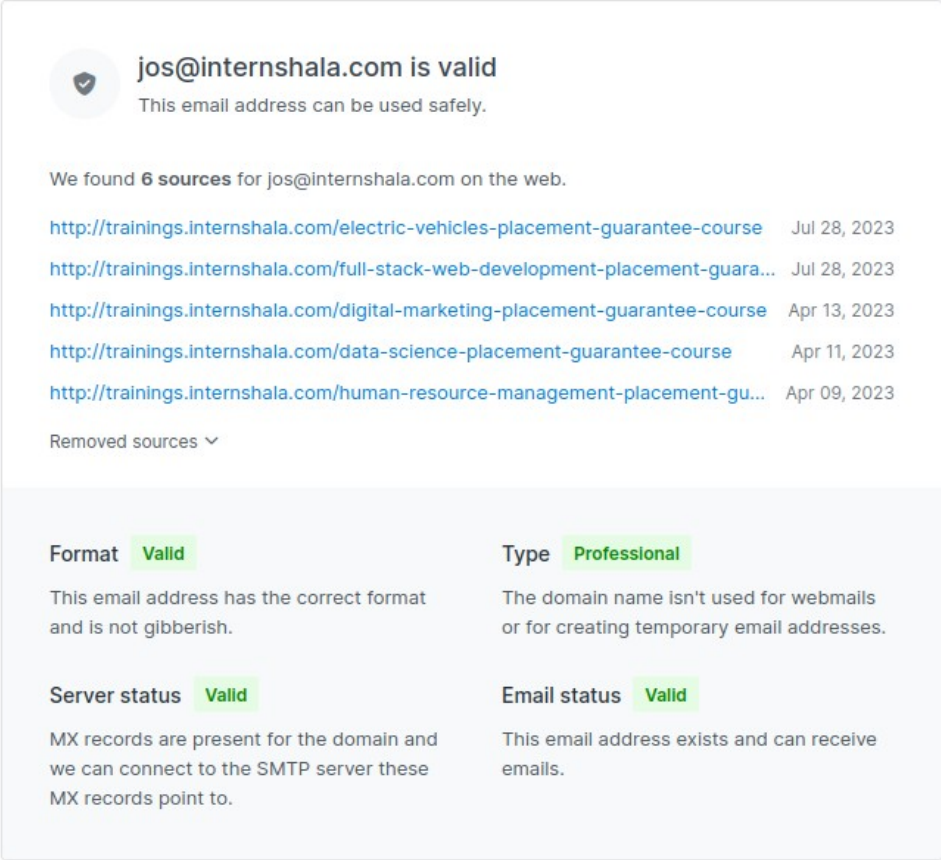
WhatIsMyIP: This tool allows you to identify the sender's IP address from the email header. It helps you determine the geographical location and other information associated with the IP.



Wintelguy: Wintelguy offers a range of networking tools, including email header analysis. It can reveal sender IP addresses and provide details about the route the email took.



Hunter.io: Hunter.io is a tool designed for email-related tasks, including email verification and discovery. It may provide additional context to the analysis by identifying the domain's characteristics.



Conclusion: Through email header analysis using tools like mxtoolbox, WhatIsMyIP, and wintelguy, & hunter.io we successfully extracted valuable information from the headers, including sender IP addresses, email server details, and routing information.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 3

Aim: To perform the reverse Image analysis for finding the physical location where the content was captured. Use OSINT tool to use image metadata, landmarks, street signs, or other visual cues to identify the geo-location accurately.

Lab Outcome: Gather information/metadata about Maps to performance detailed map profiling.

Theory:
Reverse image analysis refers to the process of extracting information or insights from an image, often by analyzing its visual content, metadata, or other related data. While the term isn't widely used, it can encompass several techniques and theories related to image processing, computer vision, and data analysis. Here's an overview of the theory and techniques involved in reverse image analysis:

Image Processing and Computer Vision: Image processing involves manipulating and enhancing images to extract relevant information. Computer vision goes a step further by enabling computers to interpret and understand visual information. Techniques like filtering, edge detection, and feature extraction are used to process images and identify important elements.

Feature Extraction: In reverse image analysis, feature extraction refers to identifying distinct visual characteristics or patterns from an image. This could include identifying objects, shapes, textures, colors, and more. These features are often used as input for further analysis or classification.

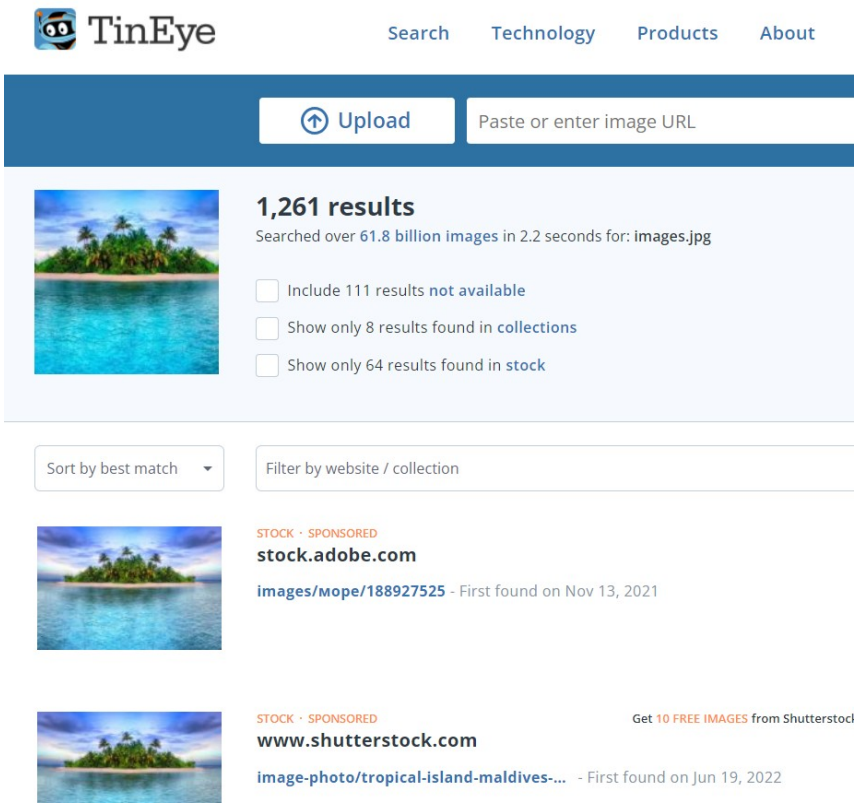
Object Recognition and Classification: Reverse image analysis can involve identifying and classifying objects within an image. This could be achieved through various methods, such as machine learning algorithms like convolutional neural networks (CNNs) or traditional computer vision techniques like template matching.

Metadata Analysis: Images often contain metadata, which is information about the image itself. This could include details such as the camera type, date and time the photo was taken, location, and more. Metadata can provide context and additional information for reverse image analysis.

Reverse Image Search: Reverse image search is a technique where an image is used as input to find similar or related images on the internet. Search engines or specialized tools can match the visual characteristics of the input image to images in their database, potentially leading to the source of the image or related information.

Output:
Image used for reverse engineering

TinEye: Use to find out where an image came from, how it is being used, if modified versions of the image exist or to find a higher resolution version.



Exiftool: Use to find metadata of the images

```
┌──(kali㉿kali)-[~/Downloads]
└─$ exiftool images.jpeg
ExifTool Version Number         : 12.49
File Name                       : images.jpeg
Directory                       : .
File Size                       : 9.8 kB
File Modification Date/Time     : 2023:08:18 05:07:46-04:00
File Access Date/Time           : 2023:08:18 05:08:00-04:00
File Inode Change Date/Time     : 2023:08:18 05:08:32-04:00
File Permissions                : -rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 225
Image Height                    : 225
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 225×225
Megapixels                      : 0.051
```

FotoForensic: It is used to find metadata and geolocation of an image

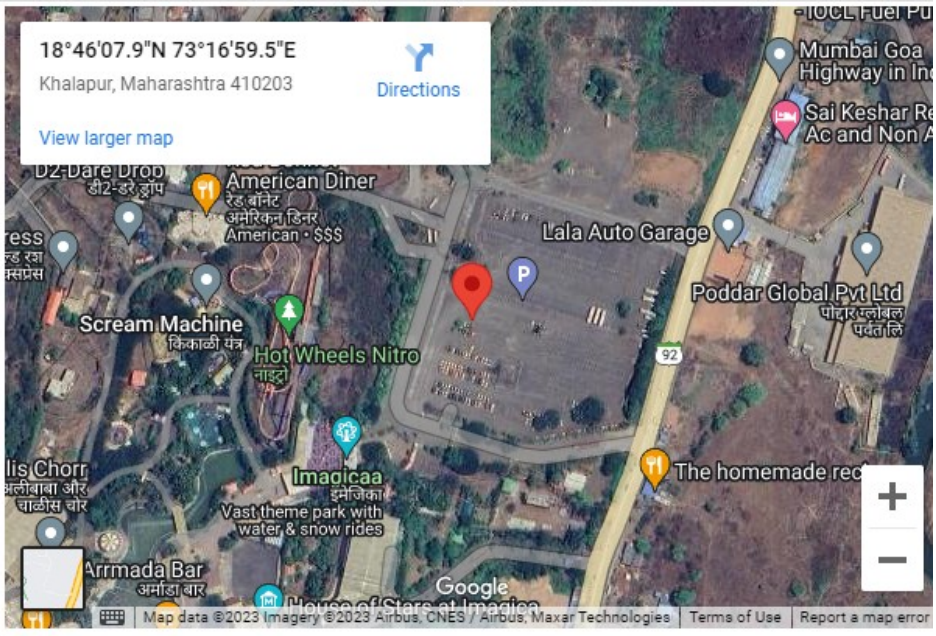
s

File	
File Type	HEIC
File Type Extension	heic
MIME Type	image/heic
Exif Byte Order	Big-endian (Motorola, MM)
Image Width	4032
Image Height	3024
QuickTime	
Major Brand	High Efficiency Image Format HEVC still image (.HEIC)
Minor Version	0.0.0
Compatible Brands	mif1, MiHE, MiPr, miaf, MiHB, heic
Handler Type	Picture
Primary Item Reference	49
Meta Image Size	4032x3024
HEVC Configuration Version	1
General Profile Space	Conforming
General Tier Flag	Main Tier
General Profile IDC	Main Still Picture
Gen Profile Compatibility Flags	Main Still Picture, Main 10, Main
Constraint Indicator Flags	176 0 0 0 0 0
General Level IDC	90 (level 3.0)

Approximate GPS Location

This information is interpreted from the GPS metadata. **Locations are approximate**

Approximate Coordinates	18.768861,73.283189
Approximate Location	4.27 miles (6.87 km) WSW of Khopoli, IN
Approximate Range	+/- 24.2475212 meters (79.6 feet)



Conclusion: Here we were able to perform the reverse Image analysis for finding the physical location where the content was captured using the OSINT tools.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 2

Aim: Using OSINT tool such as (Harvester) you can gather information like emails, subdomains, hosts, employee names, open ports, and banners from different public sources like search engines, PGP key server

Lab outcome: Conduct advanced searches to gather intelligence from social media sites and understand the use of Public Records for corporate and business intelligence etc.

Theory:
TheHarvester is a powerful OSINT (Open-Source Intelligence) tool designed to collect information from various public sources. It allows investigators to gather valuable data related to a target, such as email addresses, subdomains, online profiles, and more. The tool utilizes search engines, social media platforms, and other online resources to compile a comprehensive overview of the digital footprint associated with a specific domain.

Installation:
In terminal type:

sudo apt-get theHarvester

If it does not work, you can try to clone it directly from git using the following commands

```
git clone https://github.com/laramies/theHarvester.git
cd theHarvester
sudo python ./theHarvester.py
```

Output
Use theHarvester tool to scan emails, hosts, etc of domain sakec.ac.in

```
└─$ theHarvester -b all -d sakec.ac.in -f output.txt  -l 100
*******************************************************************
*  _   _                                             _            *
* | |_| |__   ___    ^  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.1                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: sakec.ac.in
```

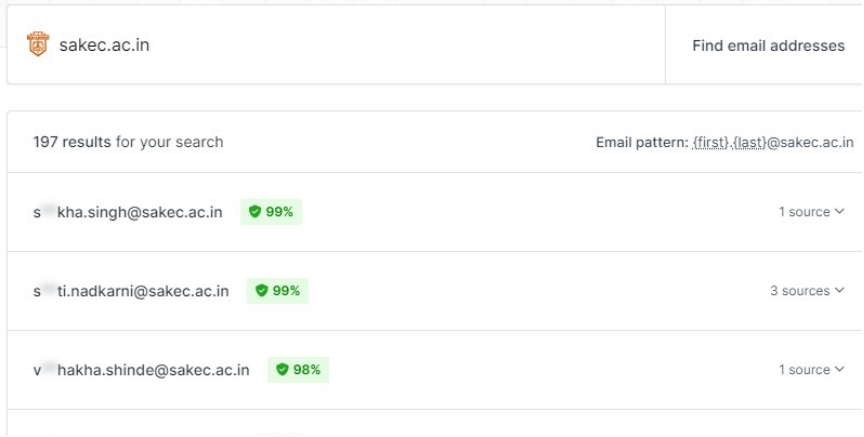
Found IP and emails

```
[*] LinkedIn Links found: 0
──────────────────────

[*] IPs found: 1
──────────────────
68.66.216.9

[*] Emails found: 4
──────────────────────
bhavesh.patel@sakec.ac.in
moiz.rajkotwala15496@sakec.ac.in
nilakshi.jain@sakec.ac.in
uday.bhave@sakec.ac.in
```

Found hosts

```
[*] Hosts found: 19
──────────────────────
admission.sakec.ac.in
admission.sakec.ac.in:68.66.216.9
cpanel.sakec.ac.in
cpanel.sakec.ac.in:68.66.216.9
cpcalendars.sakec.ac.in
cpcalendars.sakec.ac.in:68.66.216.9
cpcontacts.sakec.ac.in
cpcontacts.sakec.ac.in:68.66.216.9
iprc.sakec.ac.in
iprc.sakec.ac.in:68.66.216.9
portal.sakec.ac.in
portal.sakec.ac.in:68.66.216.9
research.sakec.ac.in
research.sakec.ac.in:68.66.216.9
webdisk.sakec.ac.in
webdisk.sakec.ac.in:68.66.216.9
webmail.sakec.ac.in
webmail.sakec.ac.in:68.66.216.9
ws.sakec.ac.in
```

Hunter
To find email address



Dnsdumpster
Used for server & asn detection, subdomain & IP

```
┌──(kali㉿kali)-[~/dnsdumpster]
└─$ python3 dnsdumpster.py -d sakec.ac.in
Starting dns dump against sakec.ac.in
Searching using engine DNSdumpster
Searching using engine Netcraft
Searching using engine Virustotal
Searching using engine SSL Certificates
[Virustotal] ERROR [Errno Expecting value] : 0 status code 403
[Virustotal] ERROR 'NoneType' object has no attribute 'get'
{
    "asn": null,
    "host": "sakec.ac.in",
    "mx": [],
    "ns": [
        {
            "ip": "",
            "ns": "ns3.supercp.com."
        },
        {
            "ip": "162.159.25.237",
            "ns": "ns4.supercp.com."
        },
        {
            "ip": "162.159.25.30",
            "ns": "ns2.supercp.com."
        },
        {
            "ip": "162.159.24.43",
            "ns": "ns1.supercp.com."
        }
    ],
```

```
"server": "LiteSpeed",
"subdomains": [
    {
        "asn": {
            "asn": "55293",
            "asn_cidr": "68.66.216.0/21",
            "asn_country_code": "US",
            "asn_date": "2009-09-01",
            "asn_registry": "arin"
        },
        "server": "LiteSpeed",
        "subdomain": "www.sakec.ac.in",
        "subdomain_ip": "68.66.216.9"
    },
    {
        "asn": {
            "asn": "55293",
            "asn_cidr": "68.66.216.0/21",
            "asn_country_code": "US",
            "asn_date": "2009-09-01",
            "asn_registry": "arin"
        },
        "server": "LiteSpeed",
        "subdomain": "admission.sakec.ac.in",
        "subdomain_ip": "68.66.216.9"
    },
    {
        "asn": {
            "asn": "55293",
            "asn_cidr": "68.66.216.0/21",
            "asn_country_code": "US",
            "asn_date": "2009-09-01",
            "asn_registry": "arin"
        },
        "server": "LiteSpeed",
        "subdomain": "www.admission.sakec.ac.in",
        "subdomain_ip": "68.66.216.9"
    },
```


Conclusion: By utilizing theHarvester, Dnsdumpster & Hunter we successfully collected a variety of information from diverse sources related to the target domain. The tool's capabilities allowed us to gather email addresses, IP, and other relevant data, providing a comprehensive overview of the digital footprint associated with the domain.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 4

Aim: Utilize website crawling OSINT tools to gather a comprehensive list of URLs, internal links, and structure of the website.

Lab outcome: Conduct advanced searches to gather intelligence and apply advanced OSINT search techniques and tools.

Theory:
Website crawling OSINT (Open-Source Intelligence) tools are valuable for extracting information about a website's structure, content, and internal links. They help investigators gain insights into a website's architecture and the relationships between its pages.

Here are the tools mentioned and their roles:

1. **GetLinkInfo:** GetLinkInfo is an OSINT tool that can extract information about a website's internal and external links. It provides details such as the anchor text, target URLs, and the relationships between various pages. This tool is useful for understanding a website's linking structure.

2. **Urlscan.io:** Urlscan.io is a service that allows you to scan and analyze websites for various security and information gathering purposes. While it's primarily used for security assessments, it can provide insights into a website's structure, including the identification of subdomains, associated domains, and potential vulnerabilities.

3. **Dnsdumpster:** Dnsdumpster is an OSINT tool that focuses on DNS (Domain Name System) information. It can be used to discover subdomains associated with a target domain. Subdomains are often indicative of a website's structure, and identifying them can aid in comprehensive information gathering.

Output

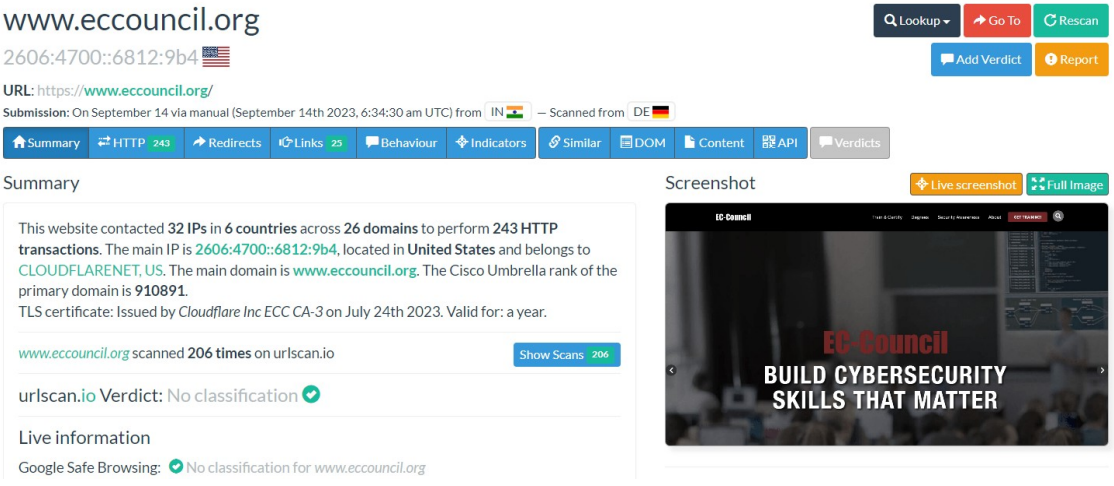
GetLinkInfo
This tool is used to extract detailed information from URLs, including title, description, external links, and redirections.

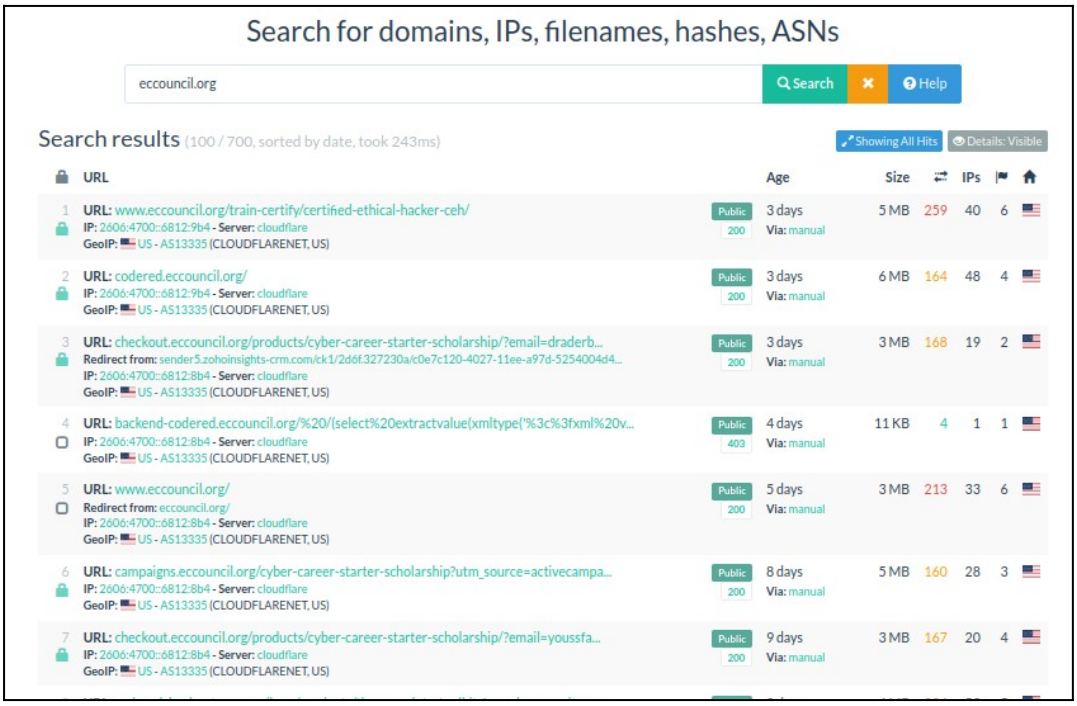
Link Information

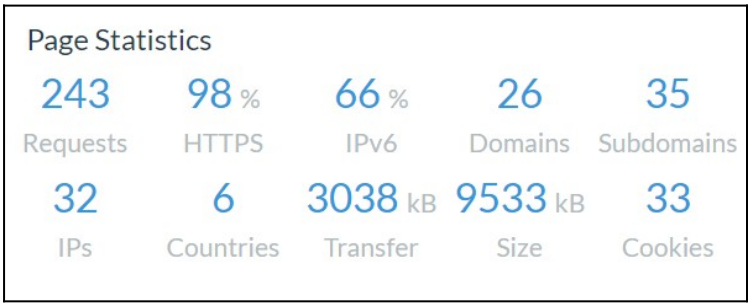
Title	EC-Council Certifications | Best Cybersecurity Courses & Training
Description	Get certified from EC-Council for the best cyber security courses & training online. Enroll now to boost your career with cybersecurity courses ✓Get started now!
URL	http://eccouncil.org more info
Effective URL	https://www.eccouncil.org/ more info
Redirections	1. http://eccouncil.org more info 2. https://eccouncil.org/ more info 3. https://www.eccouncil.org/ more info
Frames	1. https://www.googletagmanager.com/ns.html?id=GTM-M5VLP9X more info
External Links	1. https://codered.eccouncil.org/course/python-for-absolute-beginners ... more info 2. https://codered.eccouncil.org/pro?utm_source=ecc-website&utm_mediu ... more info 3. https://coderedmarketing.eccouncil.org/python-security-microdegree ... more info 4. https://coderedmarketing.eccouncil.org/php-security-microdegree/ more info 5. https://codered.eccouncil.org/course/identity-and-access-managemen ... more info 6. https://codered.eccouncil.org/course/ubuntu-linux-fundamentals-lea ... more info 7. https://codered.eccouncil.org/course/linux-server-administration-m ... more info 8. https://codered.eccouncil.org/course/cybersecurity-for-blockchain- ... more info 9. https://codered.eccouncil.org/course/cybersecurity-for-businesses- ... more info 10. https://codered.eccouncil.org/course/email-phishing?utm_source=ecc ... more info 11. https://www.eccu.edu/academics/graduate-certificate-program/?utm_s ... more info 12. https://www.eccu.edu/academics/bachelor-of-science-in-cyber-securi ... more info 13. https://www.eccu.edu/academics/master-of-science-in-cyber-security ... more info 14. https://careers.eccouncil.org/ more info 15. https://channel-resources.s3.amazonaws.com/EC-Council+Certificatio ... more info

Urlscan.io

Urlscan.io is utilized to analyze website behavior, revealing IP addresses, TLS certificates, scanning history, and potential security threats.

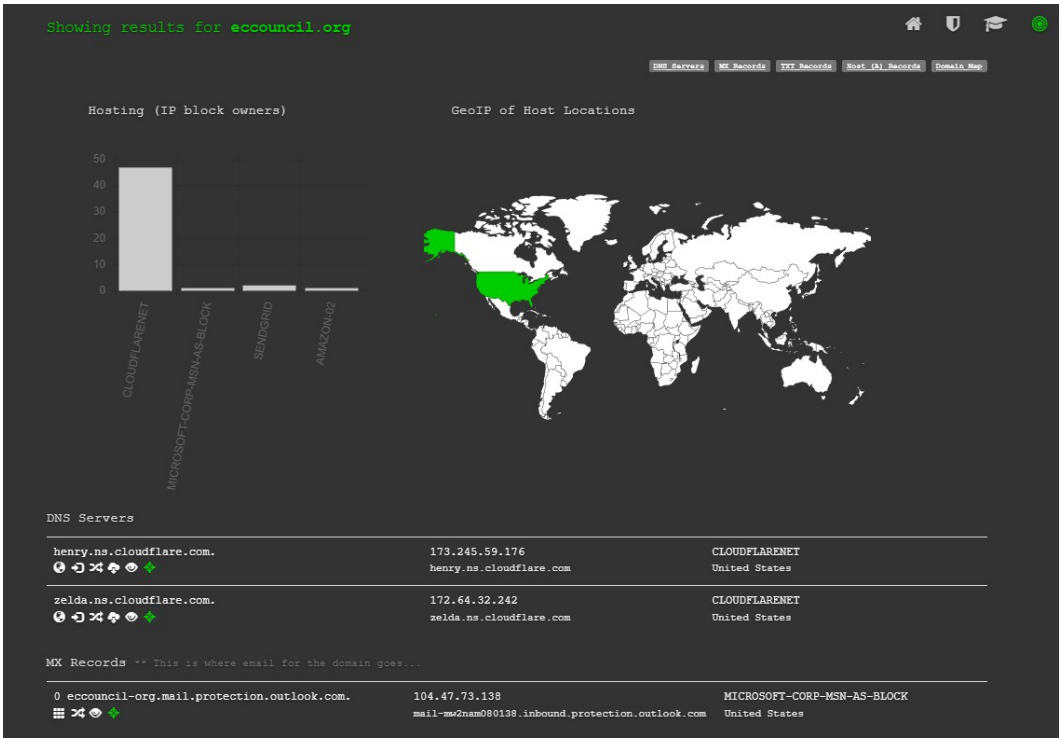






Dnsdumpster

Dnsdumpster helps identify IP addresses associated with domains and provides insights into domain relationships and DNS information.



Conclusion:

In this process, we employed OSINT tools like GetLinkInfo, Urlscan.io, and Dnsdumpster to gather extensive information about a specific domain. These tools allowed us to compile a comprehensive list of URLs, internal links, and gain insights into the website's structure. This data is invaluable for understanding the architecture of the target website and can be useful for various investigative and analytical purposes.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 1

Aim: To implement a Supervised Learning model using Linear regression.

Lab Outcome No.: 1, 2

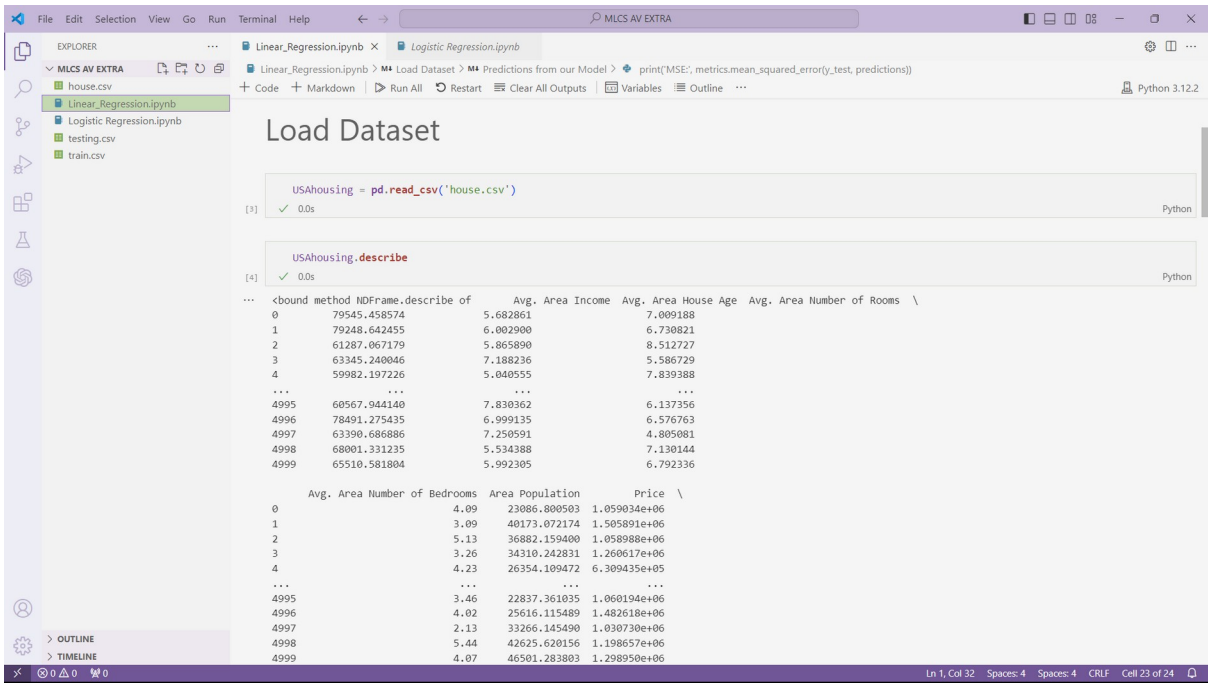
Lab Outcome: Use machine learning algorithms with complex datasets to implement cyber security concepts.

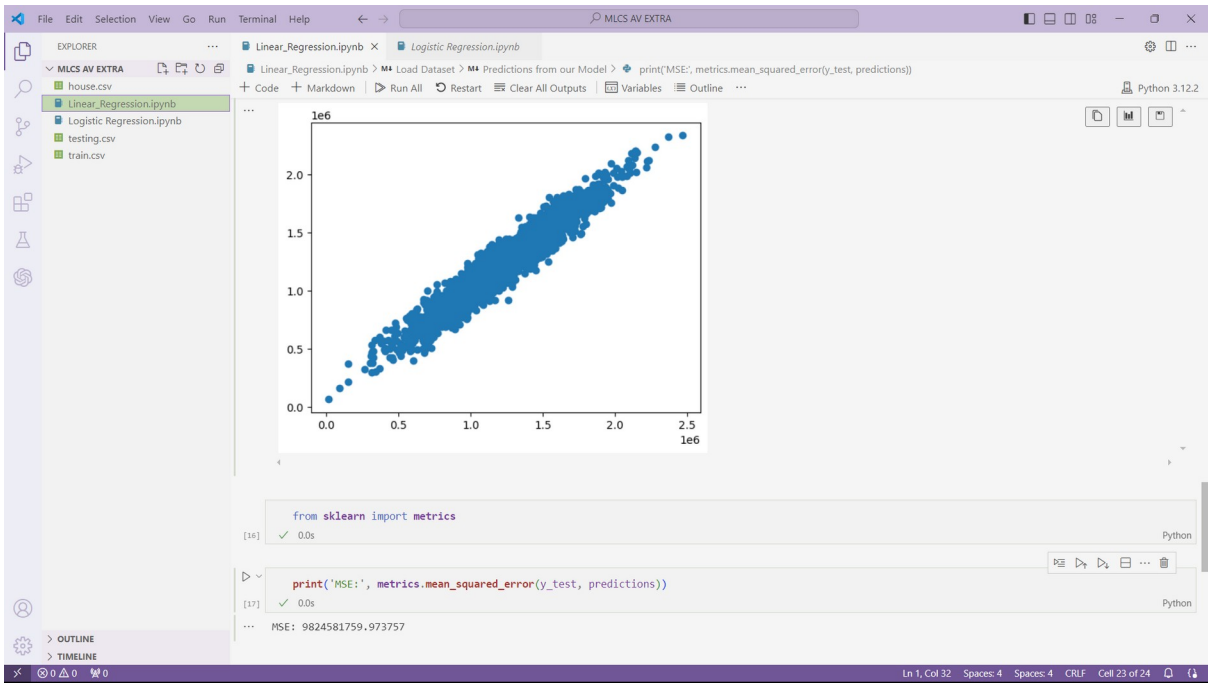
Theory:

Regression: Regression analysis is one of the most important fields in statistics and machine learning. There are many regression methods available. Linear regression is one of them. What Is Regression? Regression analysis is one of the most important fields in statistics and machine learning. There Are many regression methods available. Linear regression is one of them. Regression searches for relationships among variables. For example, you can observe several employees of some company and try to understand how their salaries depend on the features, such as experience, level of education, role, city they work in, and so on. This is a regression problem where data related to each employee represent one observation. The presumption is that the experience, education, role, and city are the independent features, while the salary depends on them. Generally, in regression analysis, you usually consider some phenomenon of interest and there have a number of observations. Each observation has two or more features. Following the assumption that at-least one of the features depend on others, you try to establish relation among them, you need to find a function that maps some features or variables to others sufficiently well. The dependent features are called the dependent variables, outputs, or responses. The, independent features are called the independent variables, inputs, or predictors.

Linear Regression: Linear regression is probably one of the most important and widely used regression techniques. It's among the simplest regression methods. One of its main advantages is the ease of interpreting results. When implementing linear regression of some dependent variable $y$on the set of independent variables x= (x1…xr_r), where r is the number of predictors, you assume a linear relationship between y and x: y= β0 + β1x1 + ……+ βrxr+ ϵ. This equation is the regression equation. β0,, βr_r are the regression coefficients, and □is the random error. Linear regression calculates the estimators of the regression coefficients or simply the predicted weights, denoted with b1…br. They define the estimated regression function f(x) = b0 +b1x1 +.....+brxr. This function should capture the dependencies between the input and output sufficiently well. Simple Linear Regression.

Output:





Conclusion:

Here we conclude that linear regression is a type of statistical analysis used to predict the relationship between two variables.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 2

Aim: Implement Unsupervised Learning model using Clustering.

Lab Outcome No.: 1, 2

Lab Outcome: Use machine learning algorithms with complex datasets to implement cyber security concepts.

Theory:

Why is unsupervised learning important?

Unsupervised learning is an important concept in machine learning. It saves data analysts' time by providing algorithms that enhance the grouping and investigation of data. It's also important in well-defined network models. Many analysts prefer using unsupervised learning in network traffic analysis (NTA) because of frequent data changes and scarcity of labels.

It's needed when creating better forecasting, especially in the area of threat detection. This can be achieved by developing network logs that enhance threat visibility.

This category of machine learning is also resourceful in the reduction of data dimensionality. We need dimensionality reduction in datasets that have many features. Unsupervised learning can analyze complex data to establish less relevant features. The model can then be simplified by dropping these features with insignificant effects on valuable insights.

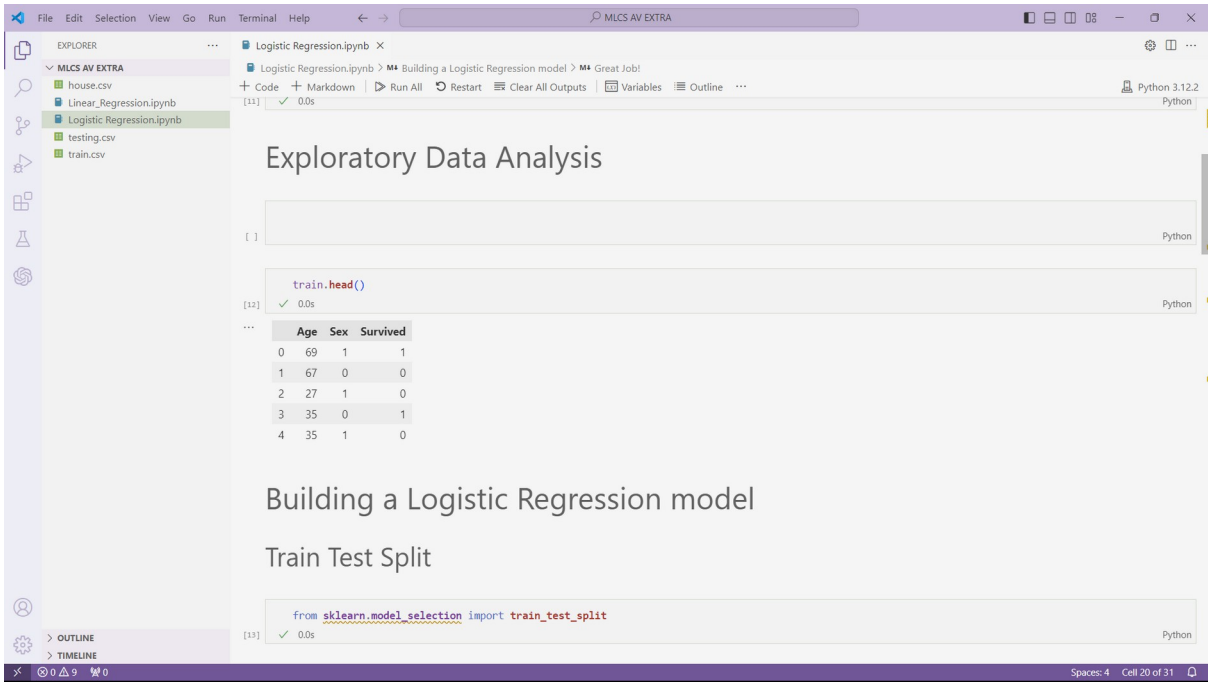
What is Clustering?

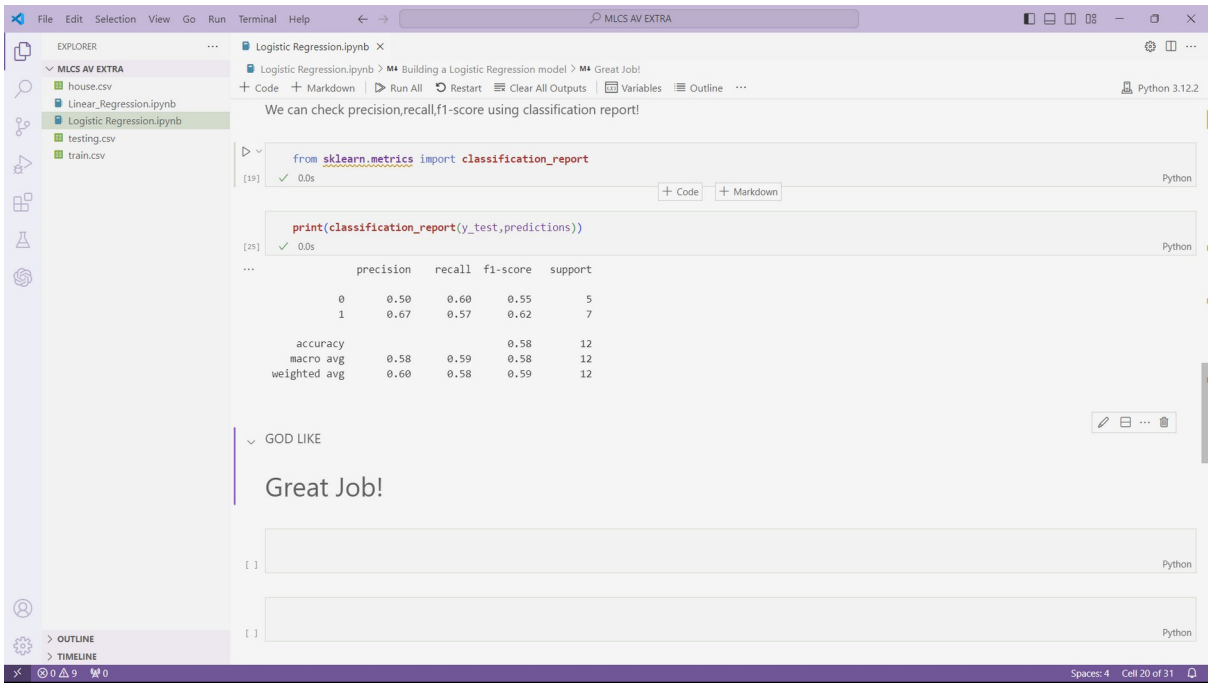
"Clustering" is the process of grouping similar entities together. The goal of this unsupervised machine learning technique is to find similarities in the data point and group similar data points together.

Why use Clustering?

Grouping similar entities together helps profile the attributes of different groups. In other words, this will give us insight into underlying patterns of different groups. There are many applications of grouping unlabeled data, for example, you can identify different groups/segments of customers and market each group in a different way to maximize the revenue. Another example is grouping documents together which belong to similar topics etc. Clustering is also used to reduce the dimensionality of the data when you are dealing with a copious number of variables.

Output:





Conclusion:

We need unsupervised machine learning for better forecasting, network traffic analysis, and dimensionality reduction. Clustering algorithms in unsupervised machine learning are resourceful in grouping uncategorized data into segments that comprise similar characteristics.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 1

Aim: To Understand Version Control System / Source Code Management, install git and to perform various GIT operations on local remote repositories.

Lab Outcome: CSL701.1 Understand the concepts of distributed version control using GIT and GITHUB

Theory:

Definition of Git

Git is an open-source version control system for projects of all sizes, ensuring quick and efficient collaboration among developers. It is used to track changes and coordinate work within teams, allowing teamwork in the same workspace.

Git forms the basis of services like GitHub and GitLab, although it can be used independently. It is usable both privately and publicly.

Created in 2005 by Linus Torvalds for the Linux Kernel, Git is vital for DevOps and distributed version control. It is user-friendly, high-performance, and surpasses other tools like Subversion, CVS, and ClearCase.

Features of Git

1. **Open Source**:

Git is an open-source tool. It is released under the GPL (General Public License).

2. **Scalable**:

Git is scalable, which means when the number of users increases, the Git can easily handle such situations.

3. **Distributed**:

One of Git's great features is that it is distributed. Distributed means that instead of switching the project to another machine, we can create a "clone “of the entire repository.

Also, instead of just having one central repository that you send changes to, every user has their own repository that contains the entire commit history of the project.

We do not need to connect to the remote repository; the change is just stored on our local repository. If necessary, we can push these changes to a remote repository.

4. **Security**

Git is secure, using SHA-1 to uniquely identify objects in its repository.

Files and commits are verified during checkout using checksums.

Commit IDs depend on the entire development history, enhancing security.

Once published, old versions cannot be altered, maintaining integrity.

Output:
Installation of Git:
Go to the website and download the 'git' file according to your system configuration.

Operations on GIT

1. Config

```
$ git config --global user.name "black-knight2"
```

2. Git init & add

```
$ git init
Initialized empty Git repository in F:/CYSE/DevSecOps/GIT/.git/


$ git add button.html
```

3. Diff

```
$ git diff
diff --git a/para.html b/para.html
index f50048f..5f8040f 100644
--- a/para.html
+++ b/para.html
@@ -2,7 +2,8 @@
 <html>
 <body>

-<p>This is a paragraph.</p>
+<p>My first paragraph.</p>
+
 <p>This is another paragraph.</p>

 </body>
```

4. Status

```
$ git status
On branch master

No commits yet

Changes to be committed:
  (use "git rm --cached <file>..." to unstage)
        new file:   button.html
        new file:   para.html

Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        modified:   para.html
```

5. Remote

```
$ git remote add Testing https://github.com/black-knight2/Testing.git
```

6. Commit

```
$ git commit -m "first commit"
[master (root-commit) d919bff] first commit
 2 files changed, 21 insertions(+)
 create mode 100644 button.html
 create mode 100644 para.html
```

7. Branch & checkout

```
$ git branch -M main
```

```
$ git checkout main
Already on 'main'
M       para.html
```

8. Push

Push the file from remote server

```
$ git remote add origin https://github.com/black-knight2/Testing.git
git branch -M main
git push -u origin main
info: please complete authentication in your browser...
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 4 threads
Compressing objects: 100% (4/4), done.
Writing objects: 100% (4/4), 438 bytes | 438.00 KiB/s, done.
Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
To https://github.com/black-knight2/Testing.git
 * [new branch]      main -> main
branch 'main' set up to track 'origin/main'.
```

9. Log

```
$ git log
commit d919bff72330077bf53a6fab15f080b53f1bf3de (HEAD -> master)
Author: black-knight2 <2002hetchheda@gmail.com>
Date:   Wed Aug 16 16:21:47 2023 +0530

    first commit
```

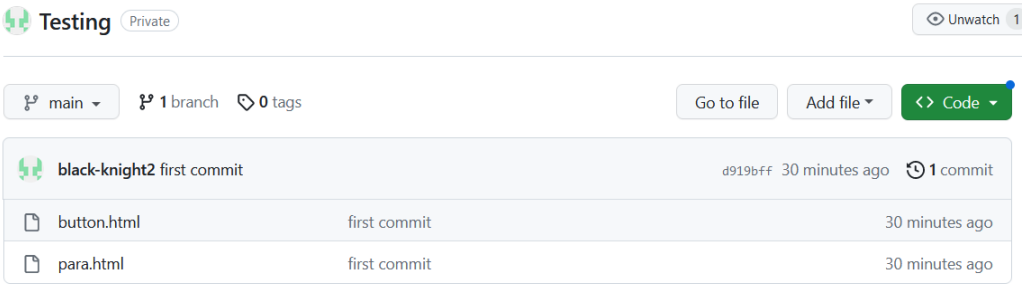
10. Reset

```
$ git reset --hard
HEAD is now at d919bff first commit
```

11. Stash

```
$ git stash
Saved working directory and index state WIP on master: d919bff first commit
```

GitHub repository



Conclusion:

The Version Control System was understood in this experiment. Git was installed and Git bash was exercised. A GitHub account was created, and a repository was made. Difference between Git and GitHub was made clear.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 2

Aim: To implement version control using GitHub to sync local git repositories and perform various related operations

Lab Outcome: CSL701.1 Understand the concepts of distributed version control using GIT and GITHUB

Theory:

Git init
Create a local repository**:** $ git init
Git clone
Make a local copy of the server repository: $ git clone

Git diff
Track the changes that have not been staged: $ git diff
Track the changes that have staged but not committed: $ git diff --staged
Track the changes after committing a file: $ git diff HEAD
Track the changes between two commits: $ git diff
Git Diff Branches: $ git diff < branch 2>
Git status
Display the state of the working directory and the staging area: $ git status
Git show
Shows objects: $ git show

Output:
Installation of Git:
Go to the website and download the 'git' file according to your system configuration.

```
On branch master
Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        modified:   av.txt

no changes added to commit (use "git add" and/or "git commit -a")

lab401@SAKEC-LAB401C7 MINGW64 ~/av (master)
$ git diff
warning: in the working copy of 'av.txt', LF will be replaced by CRLF the next time Git touches it
diff --git a/av.txt b/av.txt
index 92514b8..9749be2 100644
--- a/av.txt
+++ b/av.txt
@@ -1,2 +1,3 @@
 Anubhav
 Anubhav2
+Anubhav3

lab401@SAKEC-LAB401C7 MINGW64 ~/av (master)
$ ls
av.txt

lab401@SAKEC-LAB401C7 MINGW64 ~/av (master)
$ cat av.txt
Anubhav
Anubhav2
Anubhav3

lab401@SAKEC-LAB401C7 MINGW64 ~/av (master)
$ echo Anubhav3 > av.txt

lab401@SAKEC-LAB401C7 MINGW64 ~/av (master)
$ cat av.txt
Anubhav3

lab401@SAKEC-LAB401C7 MINGW64 ~/av (master)
$ echo Anubhav >> av.txt

lab401@SAKEC-LAB401C7 MINGW64 ~/av (master)
$ cat av.txt
Anubhav3
Anubhav

lab401@SAKEC-LAB401C7 MINGW64 ~/av (master)
$ git diff
warning: in the working copy of 'av.txt', LF will be replaced by CRLF the next time Git touches it
diff --git a/av.txt b/av.txt
index 92514b8..7525f9d 100644
--- a/av.txt
+++ b/av.txt
@@ -1,2 +1,2 @@
+Anubhav3
 Anubhav
-Anubhav2

lab401@SAKEC-LAB401C7 MINGW64 ~/av (master)
$
```

Conclusion:

Hence, I have learned and executed various git commands to perform task like creating directory, uploading data to directory, fetching data from directory etc.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 3

Aim: To implement Jenkins pipeline using scripted/declarative pipeline.

Lab Outcome: CSL701.2 Apply Jenkins to Build, Deploy and Test the Software Applications

Theory:
Jenkins: Jenkins is an open-source automation server that aids in automating various aspects of the software development lifecycle. It facilitates building, testing, and deploying software projects.

Why Use Jenkins: Jenkins streamlines development processes, enhances collaboration, and automates repetitive tasks. It offers extensibility through plugins and supports continuous integration and delivery.

Features: Jenkins provides an intuitive web interface, supports a wide range of plugins, and offers robust integration with version control systems, testing frameworks, and deployment tools.

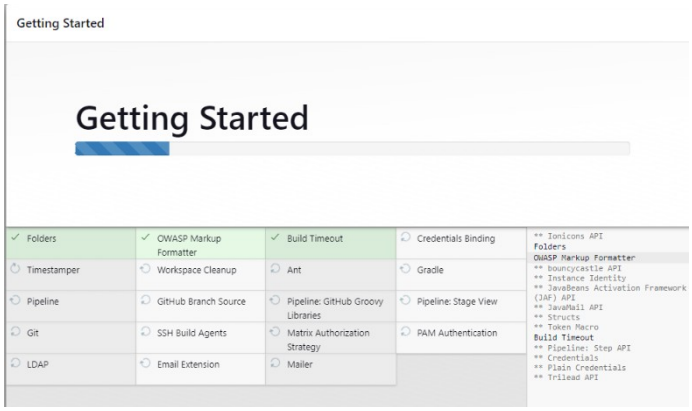
Pipeline: A pipeline in Jenkins is a set of steps that define how software is built, tested, and deployed. It provides a structured approach to automating the entire delivery process.

Steps to Create a Scripted Pipeline:

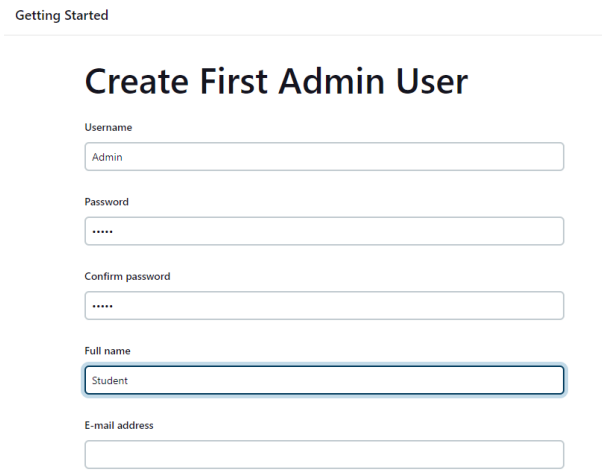
1. **Install Jenkins:** Set up Jenkins on your server.
2. **Create a New Item:** In Jenkins, create a new "Pipeline" project.
3. **Define Scripted Pipeline:** In the project configuration, select "Pipeline script" and write your scripted pipeline code.
4. **Define Stages:** Define stages for building, testing, and deployment using the stage directive.
5. **Add Steps:** Within each stage, use steps like sh for shell commands, git for version control operations, etc.
6. **Configure Post-Build Actions:** Set up post-build actions such as notifications, reports, or deployment triggers.
7. **Save and Run:** Save your pipeline configuration and run it to observe the flow and outcome.

Output:

Launch the Jekins

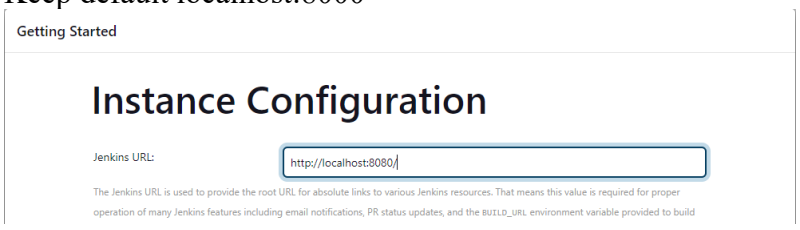


Create an Account

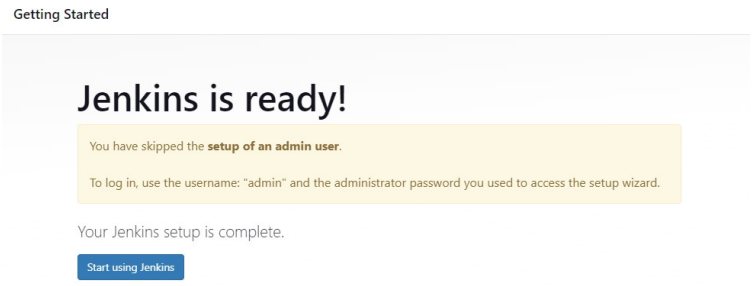


Configure it

Keep default localhost:8000



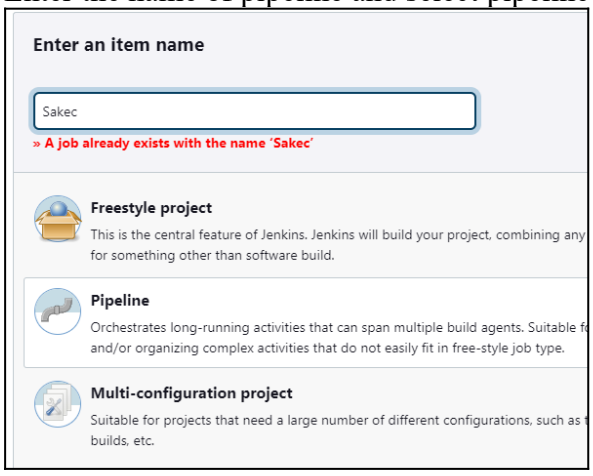
Completed the installation



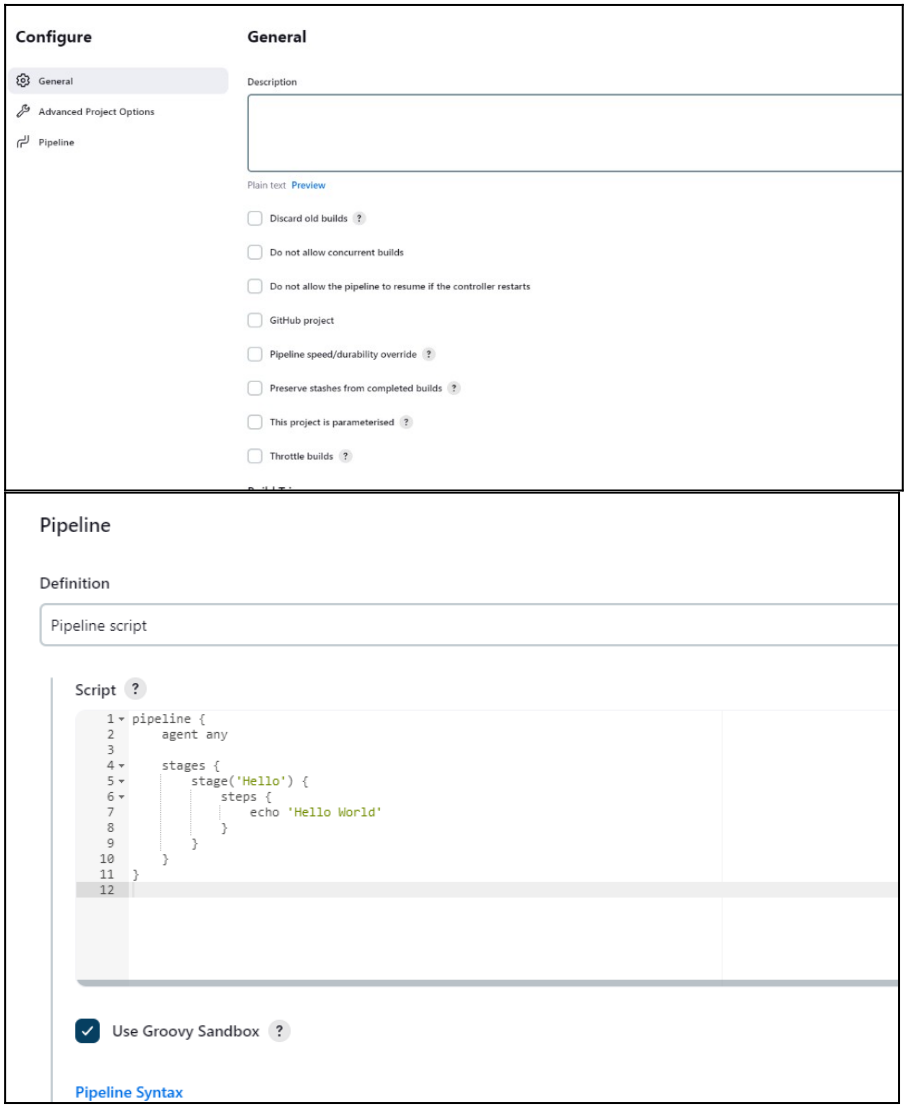
Sign into the account

Creating a pipeline

Enter the name of pipeline and select pipeline from below option

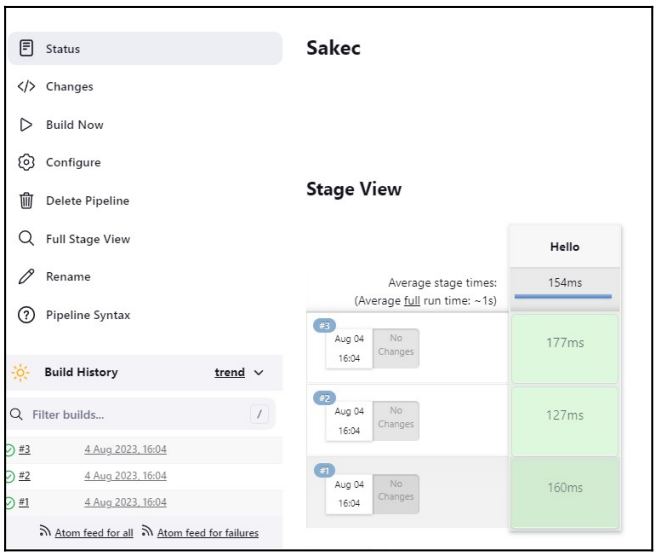


Configure the pipeline & add the script



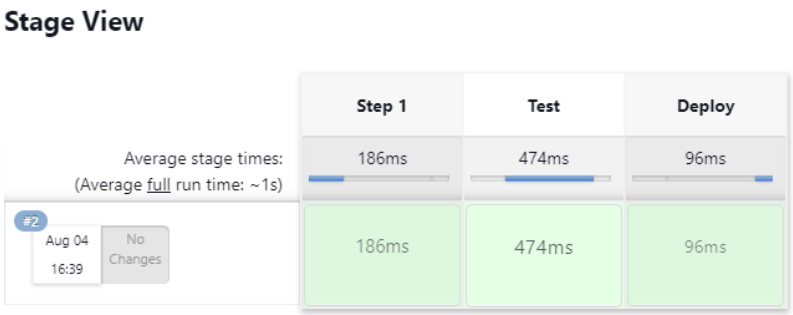
Apply the script and save it

After saving go to build now option which will build the stage
If again click the build now, it will create another stage on it

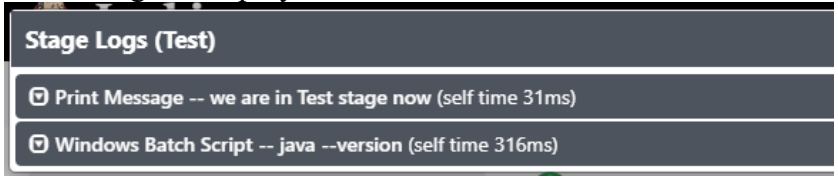


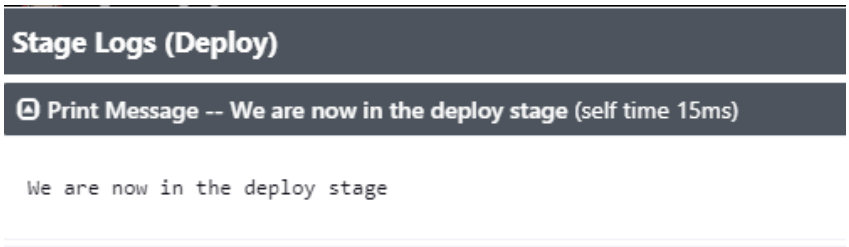
Dashboard

Now use another script to create pipeline



See the logs of Deploy






```
C:\ProgramData\Jenkins\.jenkins\workspace\Student>java --version
java 17.0.8 2023-07-18 LTS
Java(TM) SE Runtime Environment (build 17.0.8+9-LTS-211)
Java HotSpot(TM) 64-Bit Server VM (build 17.0.8+9-LTS-211, mixed mode, sharing)
```

Conclusion:

Implementing a Jenkins scripted pipeline empowers software teams to automate development workflows efficiently. It enhances collaboration, accelerates delivery, and ensures consistent software quality.

Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Cyber Security

Experiment No. 4

Aim: To Setup and Run Selenium Tests in Jenkins Using Maven.

Lab Outcome: CSL701.2 Apply Jenkins to Build, Deploy and Test the Software Applications

Theory:
Selenium is a widely used tool for automating web applications, and Jenkins is a powerful automation server. Integrating Selenium tests with Jenkins using Maven streamlines the testing process.

Selenium: It's an open-source framework for automating web browsers, allowing testers to perform functional and regression testing on web applications.

Jenkins: An automation server that facilitates continuous integration and continuous delivery. It's used to automate building, testing, and deployment of software projects.

Maven: A build automation and project management tool. It simplifies project setup, handling dependencies, and building Java projects.

Steps to Set Up and Run Selenium Tests in Jenkins Using Maven:

Step 1: Install Jenkins
Download and install Jenkins on your server.
Set up and configure Jenkins according to your requirements.

Step 2: Create a Jenkins Job
Create a new Jenkins job (Freestyle project).
Configure the job to fetch your Selenium test project from a version control repository.

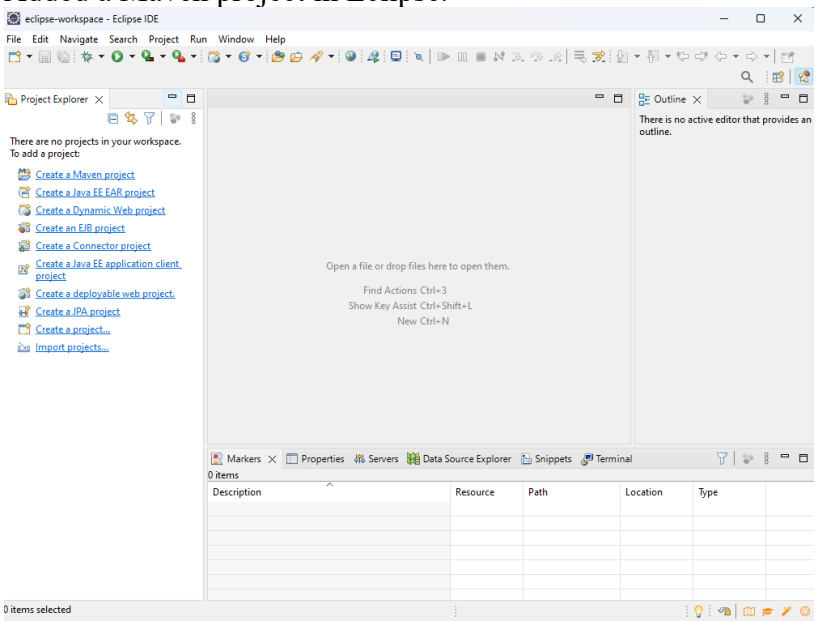
Step 3: Install and Configure Maven
Ensure Maven is installed on your Jenkins server.
Configure Maven settings and paths in Jenkins.

Step 4: Build Selenium Tests Using Maven
In the Jenkins job configuration, add a build step to execute Maven commands.
Use Maven commands like clean test to build and run Selenium tests.

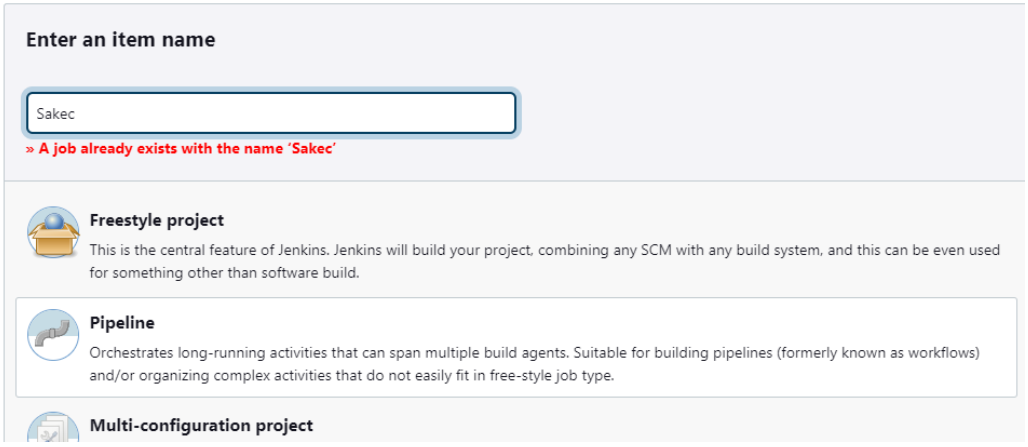
Step 5: View Test Results
Configure the Jenkins job to generate test reports.
View test reports within Jenkins to analyze test results.

Output:

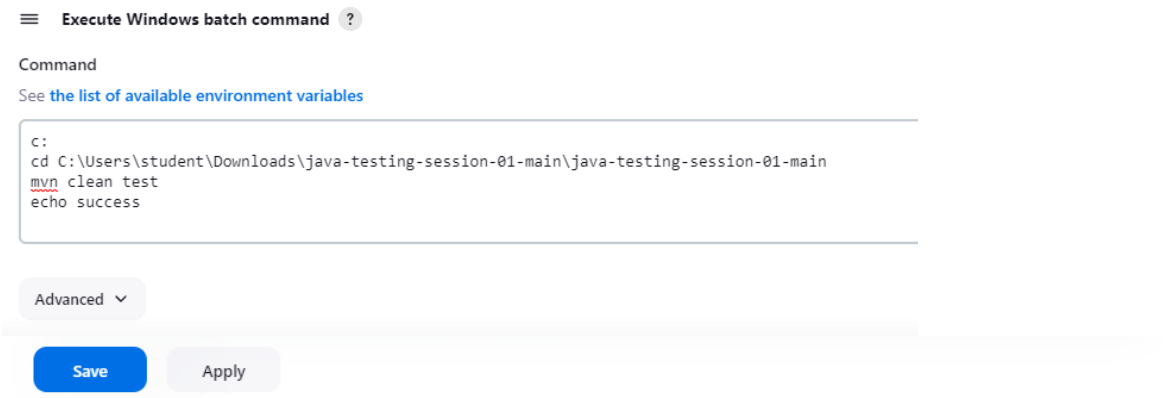
Installed Apache Maven.
Installed Eclipse for Maven project development.
Added a Maven project in Eclipse.



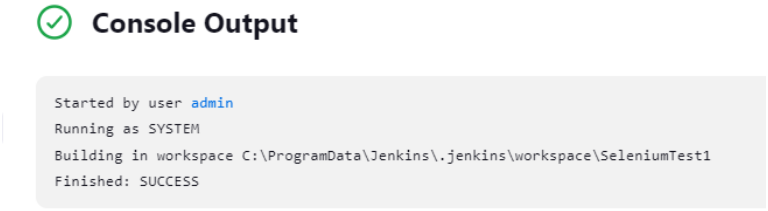
Created a Freestyle project in Jenkins.
Configured the Jenkins project with appropriate settings.



In the build steps, added the path to your Maven project and the command **mvn clean test**, and saved the configuration.



Used the "Build Now" option in Jenkins to initiate the build process.
Observed output for both success and failure cases.



Manually ran the command mvn clean test in the command prompt and received a successful result.

```
INFO]
INFO] --- surefire:3.1.2:test (default-test) @ java-testing-collections ---
INFO] Using auto detected provider org.apache.maven.surefire.junit4.JUnit4Provider
INFO]
INFO] -------------------------------------------------------
INFO]  T E S T S
INFO] -------------------------------------------------------
INFO] Running es.seresco.cursojee.StackTest
INFO] Tests run: 6, Failures: 0, Errors: 0, Skipped: 0, Time elapsed: 0.041 s -- in es.seresco.curs
INFO]
INFO] Results:
INFO]
INFO] Tests run: 6, Failures: 0, Errors: 0, Skipped: 0
INFO]
INFO] ------------------------------------------------------------------------
INFO] Reactor Summary for java-testing-session-01 0.0.1:
INFO]
INFO] java-testing-session-01 ............................ SUCCESS [  0.666 s]
INFO] java-testing-calculadora ........................... SUCCESS [  3.600 s]
INFO] java-testing-collections ........................... SUCCESS [  1.244 s]
INFO] ------------------------------------------------------------------------
INFO] BUILD SUCCESS
INFO] ------------------------------------------------------------------------
INFO] Total time:  5.602 s
INFO] Finished at: 2023-08-11T16:23:42+05:30
INFO] ------------------------------------------------------------------------
S C:\Users\student\Downloads\java-testing-session-01-main\java-testing-session-01-main>
```

Conclusion:

Successfully configured Jenkins to seamlessly run Selenium tests using Maven, enhancing the testing process. This integration streamlines test automation and supports efficient continuous integration, enabling robust and reliable web application testing.