Final Report

Technology Stack: AI for Cybersecurity with IBM Qradar

Project Title: Understanding cyberthreats: exploring Nessus and beyond scanning tools

Team ID: LTVIP2024TMID13844

Team no: 2.1

Team members:

1.Keerthi Veera Ashok

2.Voni Swapna

3.Katakam Lakshmi Swetha

4.Ampilli Mahalakshmi

5.Latchireddi Lalitha

College: Sri Balaji Degree College

INDEX

S.NO	TITLE	PAGE NO
1	Introduction	1
2	Abstract	2
3	Empathy Map	3
4	Brainstorming and Idea prioritization	4
5	Stage-1	7
6	Report on practice website	9
7	Report on Main website	20
8	Stage-2	30
9	Conclusion	35
10	Future Scope	36
11	References	37

INTRODUCTION

Today's cyber threat landscape is constantly evolving.

Modern Organizations face a growing number of cyber threats that are increasingly complex. There's no one-size -fits-all formula for deciphering exactly what a cyber threat may be for your organizations compared to another. However, understanding your cyber threat landscape, as well as how to prioritize cyber threats for remediation, is the great first step in developing a cybersecurity program.

A cyber threat defines as a circumstance or event that could potentially negatively impact operations. For example, if an attacker successfully exploits the threat, it could result in losing the ability to deliver products or services. A Cyberthreat refers to anything that has the potential to cause serious harm to a computer system. A cyberthreat that may or may not happen, but has the potential to cause serious damage. Cyberthreats can lead to attacks on computer systems, networks and more.

In this we are understanding cyber threats by using Nessus. Nessus is a cornerstone in cybersecurity, offering a powerful and indispensable tool for assessing vulnerabilities within an organization's digital world infrastructure. Developed by Tenable, Nessus has

earned its reputation as go-to solution for security professionals and administrators seeking to fortify their defences against evolving cyber threats.

This versatile software excels in automating scanning networks, servers and applications to unearth potential weaknesses and misconfigurations. By leveraging continually updated database of unknown users to stay one step ahead of potential attackers. Nessus is used for vulnerability scanning. Deploying Nessus for effective vulnerability scanning requires a systematic approach to ensure comprehensive coverage and accurate results.

Cyber threats can have a serios on businesses of all sizes, including financial and reputational damage. The impact can vary depending on the severity of the attack. There are, however, a few common consequences associated with a successful cyber attack Financial loss, Reputational damage, business operational disruption, Legal and regulatory issues.

ABSTRACT

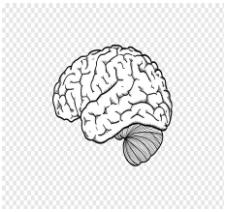
The project “Understanding cyber threats: exploring the Nessus and Beyond scanning tools “addresses the processing need for enhanced cyber security for the verification and detection of vulnerabilities. This project is used to observe the vulnerabilities of websites. The main theme of the project is to understanding cyberthreats by using Nessus and beyond scanning tools.

In this project we are scanning to observe vulnerabilities to solve the problem the remediation of the website and we can protect the website from the attackers. In this project we are using the Nessus scanning and Burp suite tool, these tools are working on the website to scan the vulnerabilities at any time. Mainly Nessus scanning is used to most widely deployed vulnerability assessment solution, helps you to reduce your organizations attack surface and ensure compliance. Vulnerability scanning lets you take a proactive approach to close any gaps and maintain strong security for your systems, data, employees, customers. Data breaches are often the result of unpatched vulnerabilities. Nessus features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery and more.

EMPATHY MAP

Topic: Understanding cyber threats exploring Nessus and beyond scanning tools

What do they think and feel?



- Worries about the security of their websites, network etc.
- Things about efficient ways to keep their website to keep their website save.
- Wondering about the types of vulnerabilities and threats affected their sites and system.
- Satisfied when they successfully detect vulnerabilities and threats by Nessus and scanning tools.

What do they see?

- Notices changes of late working and some issues of data in the websites.
- When the Nessus and beyond scanning tools are potential threats and vulnerabilities are detected.
- Slower website raises concern.
- Watches scanning tutorials.

What do they hear?

- Hears about the threats and vulnerabilities problems and attacks/
- Prevention tips of scanning tools.
- Listens to advice the strong scanning tools to scan the website thoroughly and every time.

What do they say and do?

- Scan their websites for vulnerabilities and threats.
- Updates the website.
- Monitors website frequently.
- Seeks advice or information about threats and vulnerabilities.

Pains

- Fear of data loss.
- Worried about website constantly.
- Complex threats and vulnerabilities detection.

Gains

- Increased awareness.
- Protect our things.
- Peace of mind.
- Detection of threating and vulnerabilities.

BRAINSTORMIMG AND IDEA PRIORTIZATON

Brainstorming for the topic of understanding cyberthreats exploring Nessus and beyond scanning tools is a dynamic exploration into the evolving world of cybersecurity. With persistent growth in vulnerabilities, our innovative strategies and technologies for recognizing and categories the threats. Oue focus on how to reduce the vulnerabilities in the websites of an individual and organizations. Now we have to scan the vulnerabilities using the Nessus and beyond scanning tools.

Step 1: Team Gathering, Collaboration and Select the problem statement

In this brainstorming phase, we have to identify the possible problems that might be difficult to tackle.

We have ended up with the following statements:

1. How can we identify the cyber threats?

2. What are the types of cyber threats?

3. How can we identify the vulnerabilities in the websites?

4. How can we understand the cyber threats and reduce the vulnerabilities in the website?

5. How can we scan the vulnerabilities using the Nessus?

Step 2: Idea listing as a mind map

A mind map helped us to categorize the things that we need to work on and how to approach the problem statement in a better way.

Step 3: Idea prioritization

Prioritizing the attained solutions will help us work on the solutions according to importance and feasibility. This help us to attain goal and meet the importance of the solution at the same time.

STAGE-1

Title of the Project: Understanding Cyber threats exploring Nessus and Beyond scanning tools

Overview:

The landscape of cyber threats is becoming more complex and dangerous by the day. Traditional cyber threats like viruses and malware seem almost tame next to advanced cyber hacking attacks like ransomware, impersonation fraud and spear-phishing. As companies consider how best to address cyber threats, cyber security firms are recommending strategies for cyber security acknowledges that stopping every cyberattack is unlikely, and instead focuses on ensuring business continuity and mitigating the impact of successful cyber threats.

As its core, this project serves not only as a scanning but also as an educational resource, empowering with valuable insights into the realm of cyber threats. This project helps us to scan the websites by using Nessus to find the vulnerabilities in the website. In this project scanning tools are used like Nessus and Burp suite for scanning the vulnerabilities.

List of Teammates:

S.no	Name	College	Contact
1.	Keerthi Veera Ashok	Sri Balaji Degree college	veeraashok77320@gmail.com
2.	Voni Swapna	Sri Balaji Degree College	voniswapna@gmail.com
3.	Katakam Lakshmi Swetha	Sri Balaji Degree College	lakshmiswethakatakam@gmail.com
4.	Ampilli Mahalakshmi	Sri Balaji Degree College	a.mahalakshmi204@gmail.com
5.	Latchireddi Lalitha	Sri Balaji Degree College	lachieddylalitha@gmail.com

REPORT ON PRACTICE WEBSITE

1.Vulnerability: SQL injection

CWE: 94

OWASP Category: A03 2021- Injection

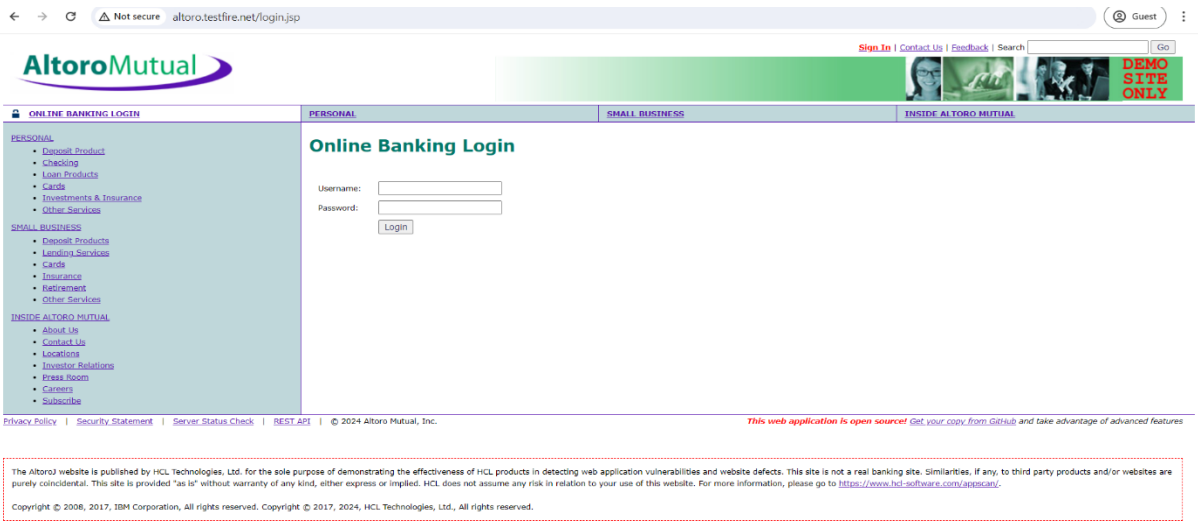
Description: This weakness describes a situation where software uses untrusted input to constrast all parts of code and does not perform or incorrectly performs neutralization of special characters that might influence syntax or behaviour of the code segment.

Business impact: Exists that could cause executes of malicious code when an unsuspicious user loads a website. The fallout often includes financial liabilities, regulatory fines, loss of customer trust, and the cost of remediation efforts to fix the vulnerabilities and recover from the breach.

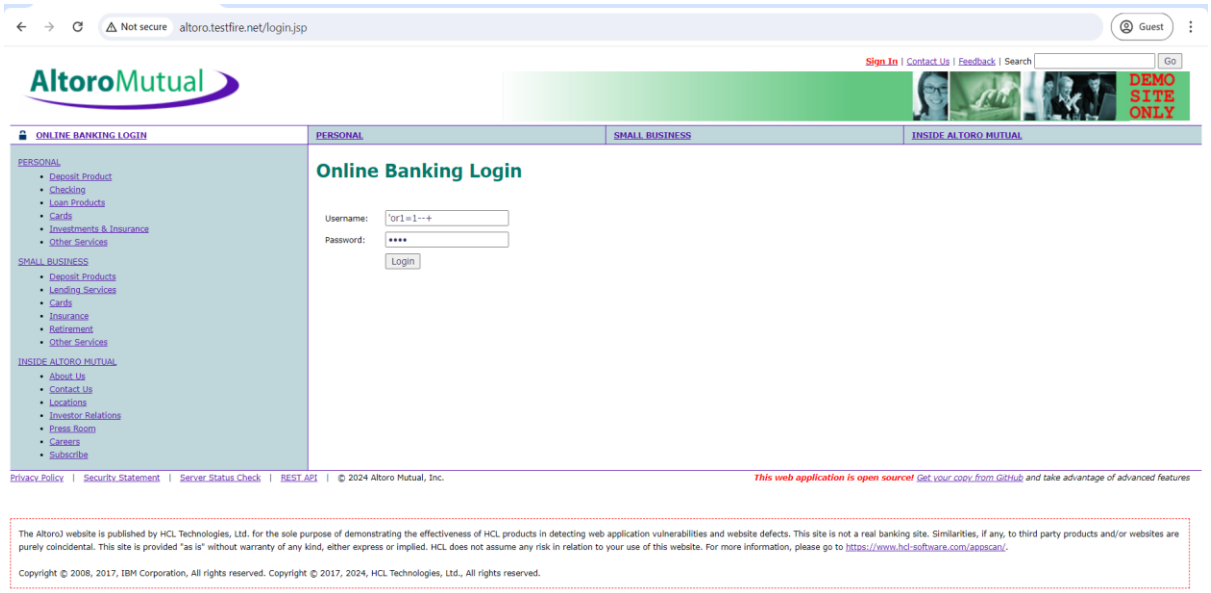
Vulnerability path: https://testfire.net/login.jsp

Steps to reproduce:

1.Access the URL.

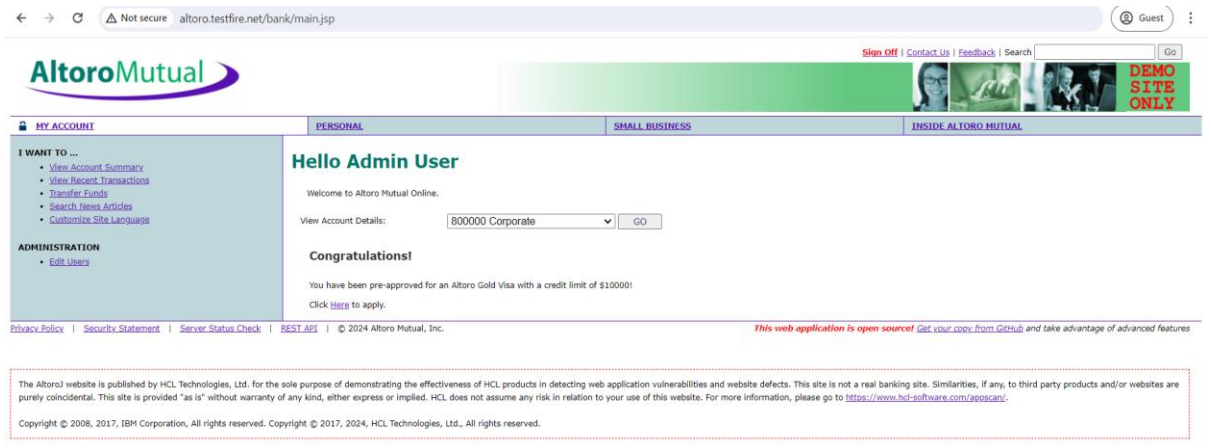


2.Enter the username with ‘ or1=1--+ and password with 1234.



In the above screenshot, when the user enters incorrect payloads as ‘ or1=1--+, the dynamically generated SQL query will be generated as below.

3. click on login.



2. vulnerability: Cross-Site Scripting(XSS)

CWE:159

OWASP Category: AP03 2021-Injection

Description: weaknesses in this attack focussed category fail to sufficiently filter and interpret special elements in user-controlled input which could cause adverse effect on the software behaviour and integrity.

Business impact: It is the main impact on a important thing on the business and filter is fail so that business has some crisis due to failure the special element.

Vulnerability path: https://testfire.net/index.jsp

Steps to Reproduce:

1. Go to the search bar of the given URL.

2. Execute any javascript code.

3.Then click on Go.

The entered code has been executed in the website.

3.Vulnerability: Insecure Direct Object Reference (IDOR)

CWE: cwe-639

OWASP Category: A02 Broken Access Control

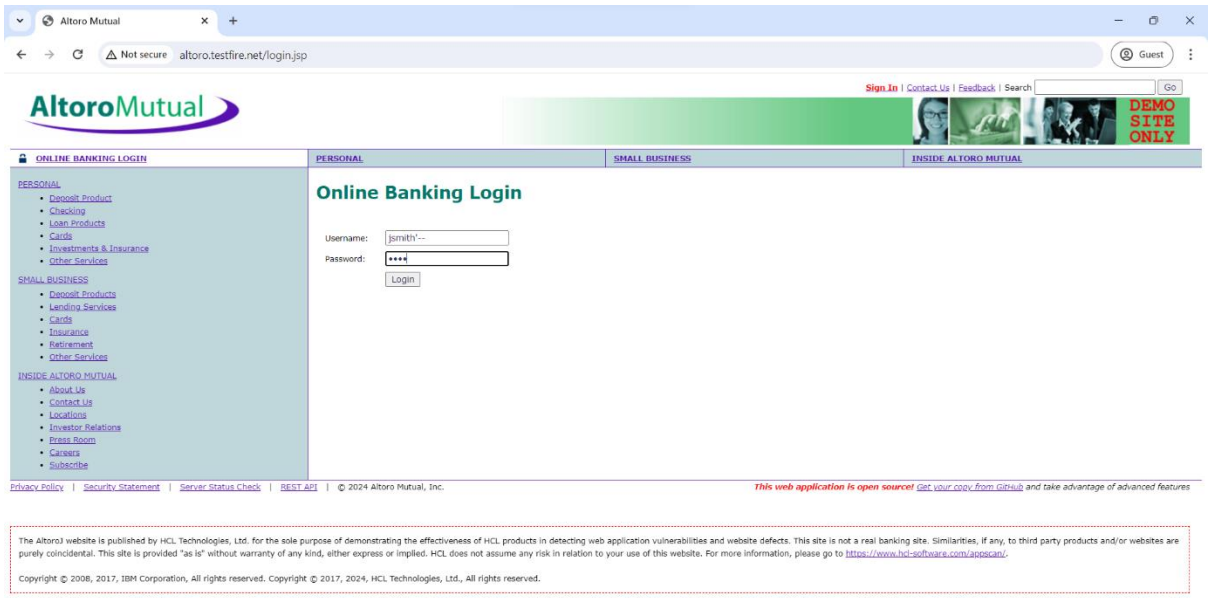
Description: The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data.

Business impact: IDOR can lead to unauthorized access to sensitive data or resources, potentially resulting in data breaches, privacy violation, financial losses, and damage to an organization's reputation. It can also lead to legal and regulatory consequences, impacting the overall trust and confidence in the business.

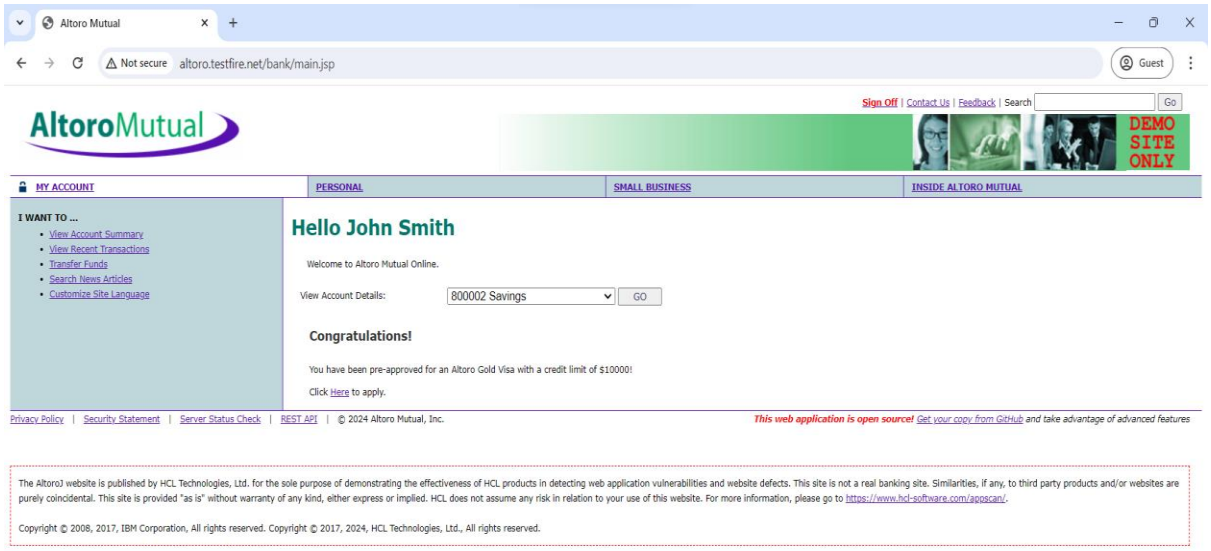
Vulnerability path: https://testfire.net/login.jsp

Steps to Reproduce:

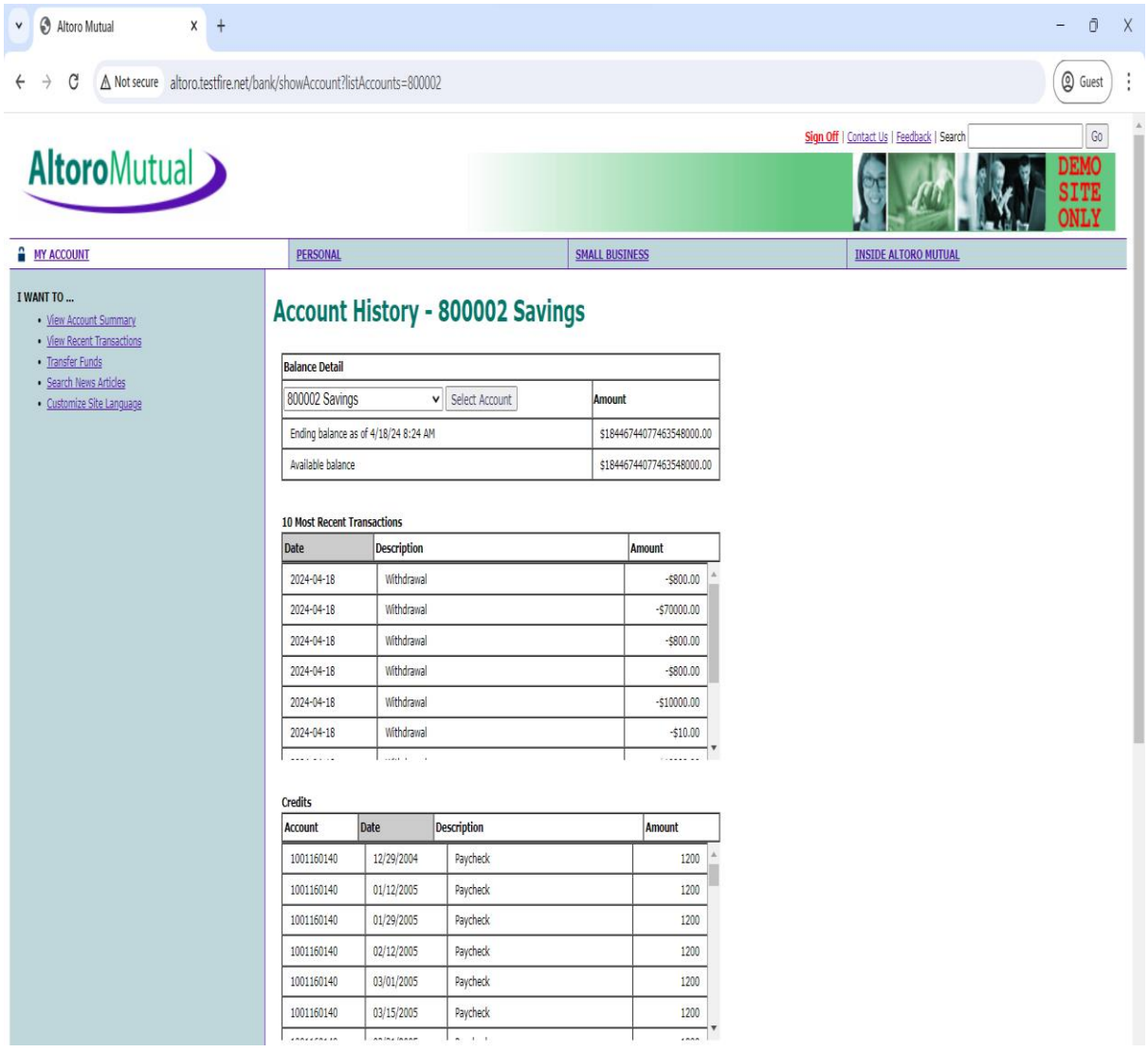
1.Navigate into the given URL and sign using john smith credentials.

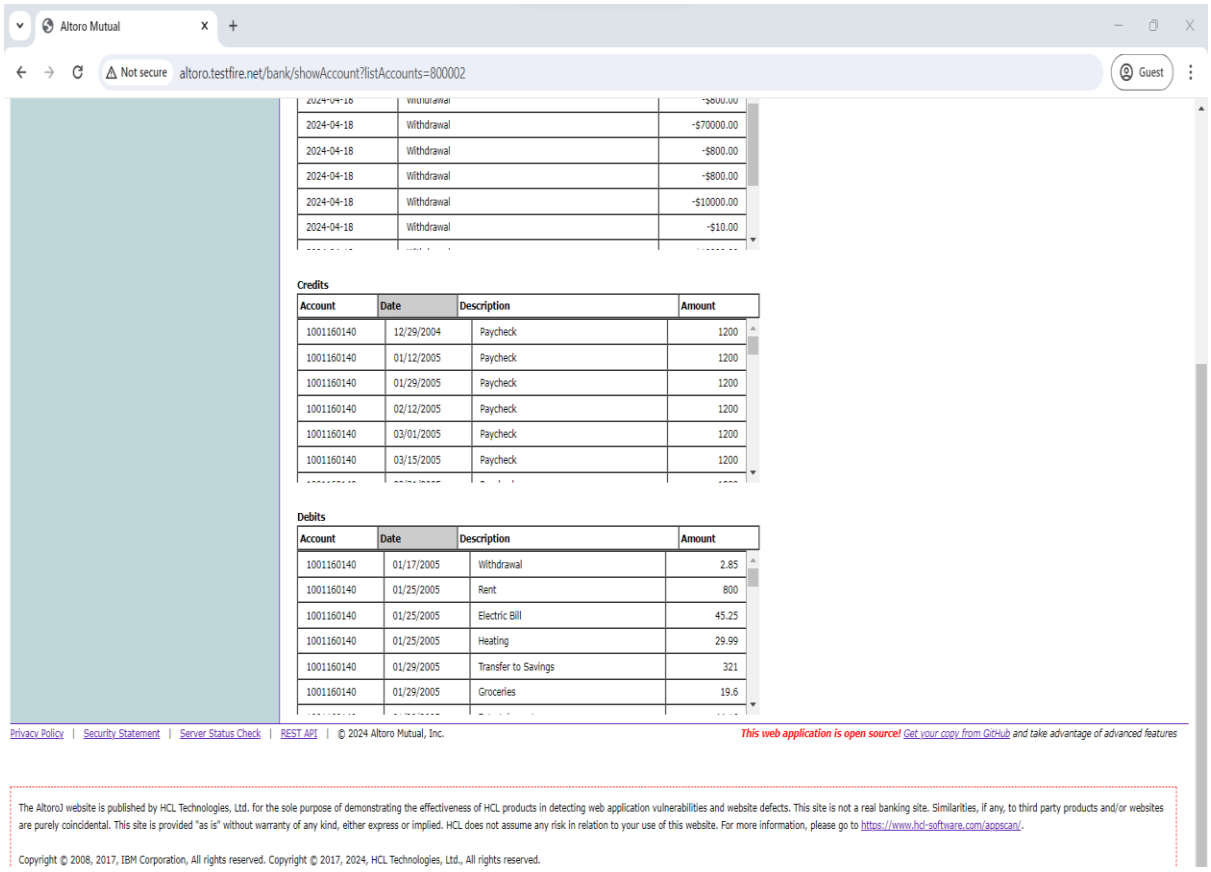


2. Click on "Go" to view John Smith's savings.



3.Then click on Go.



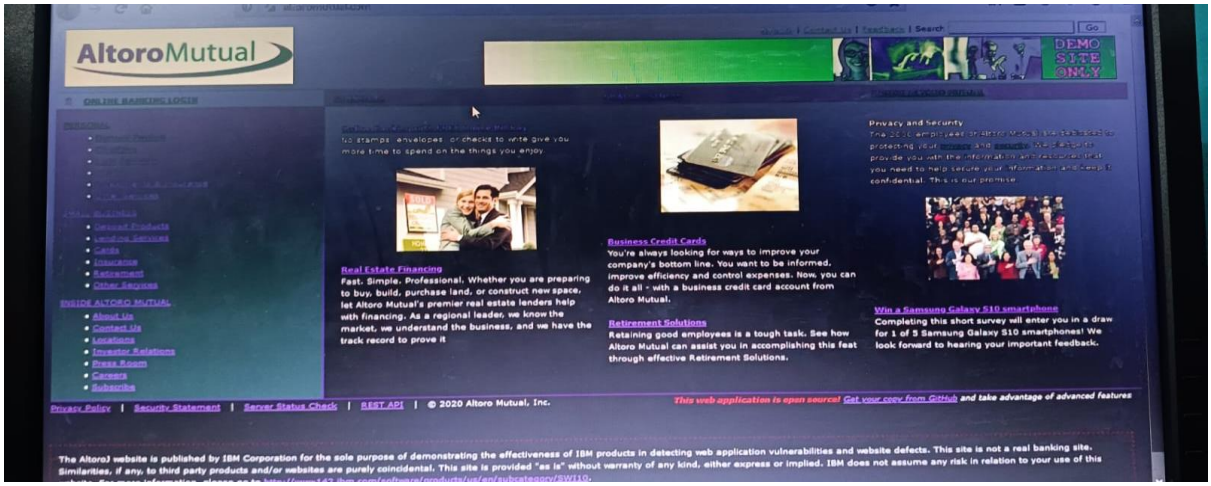


Now we are using the Burp suite tool to scan the Altoro mutual website.

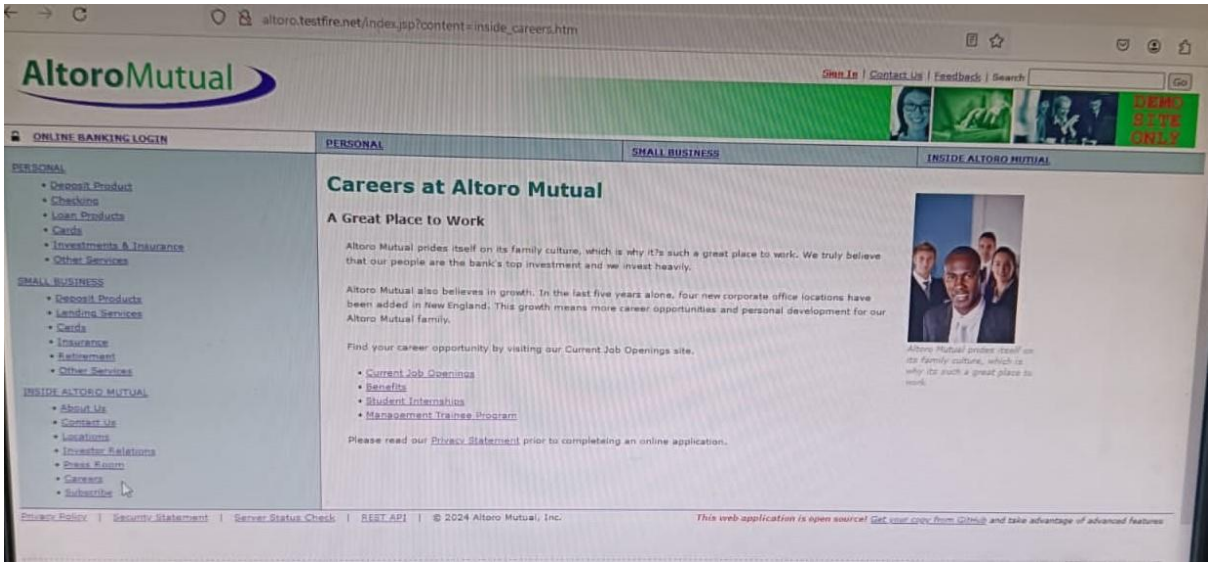
Steps to Reproduce:

1.Use a website to scanning the vulnerabilities.

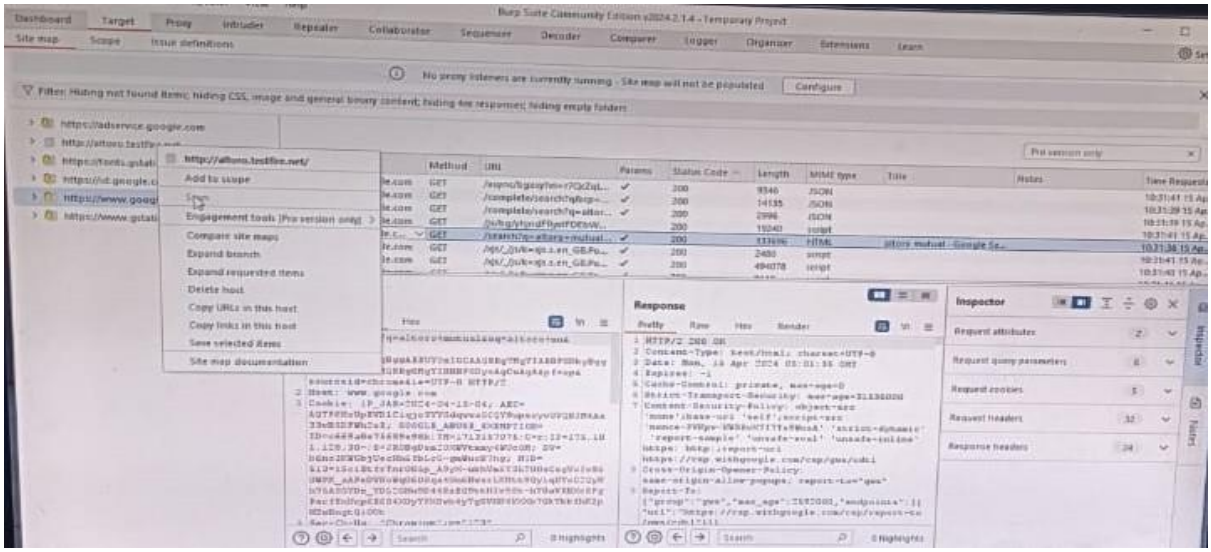
2.Choosen website: Altoro Mutual.



3. First we have to scan the vulnerabilities before we observe and check all the links of the chosen website.



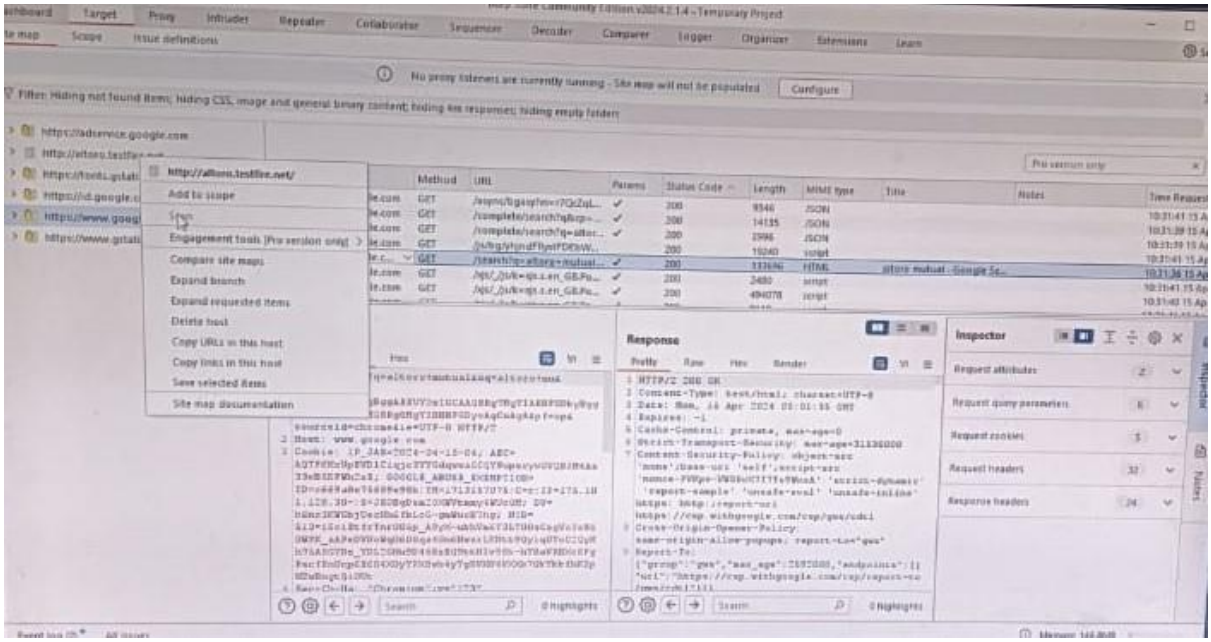
4. All the links should be browsed and the browsed things are in a tab. Because the browsed the links to find the vulnerability detection is heavy.



5. Burpsuite spider or scrolling feature is used. The website is almost done on the spider.

6. Next moved to the Target and click on the site map.

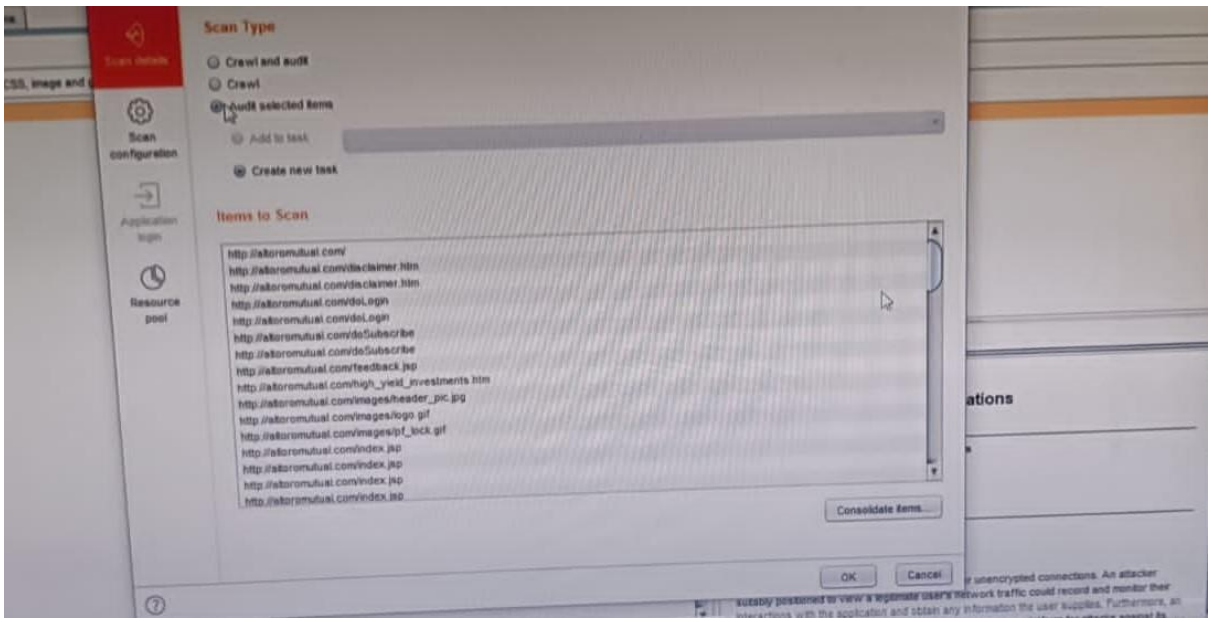
7. So many links are available in the site map because we clicked many links on the website.



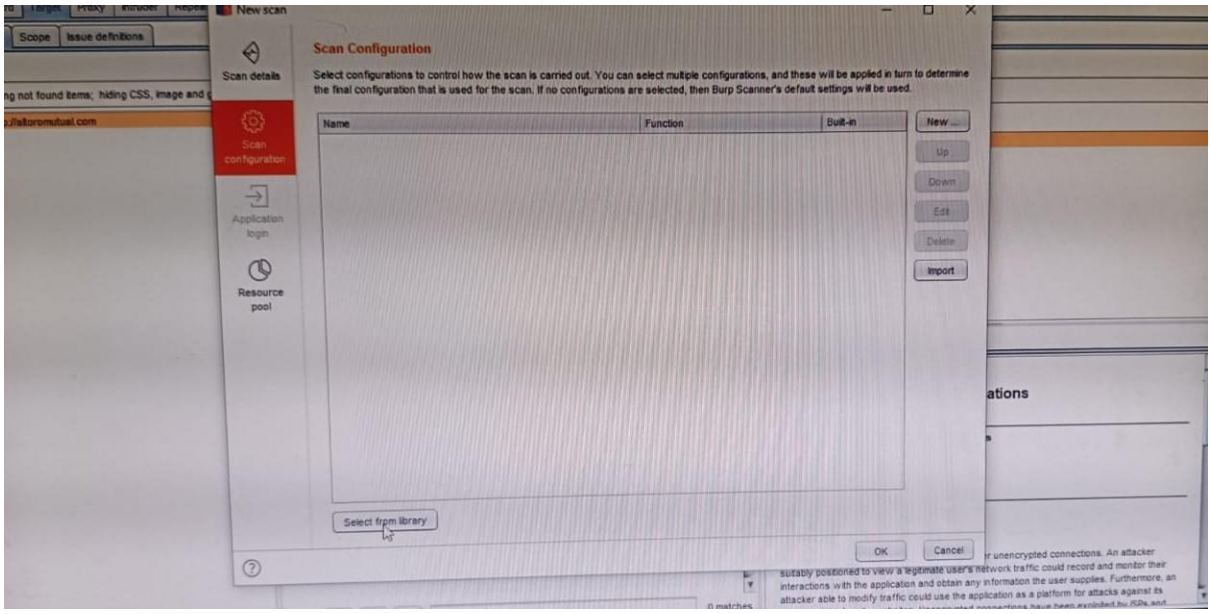
8. Click any one link and give scan option then it is started to scanning process.

9. There are different scans and so many scan options like scan details, scan configuration, resource pool.

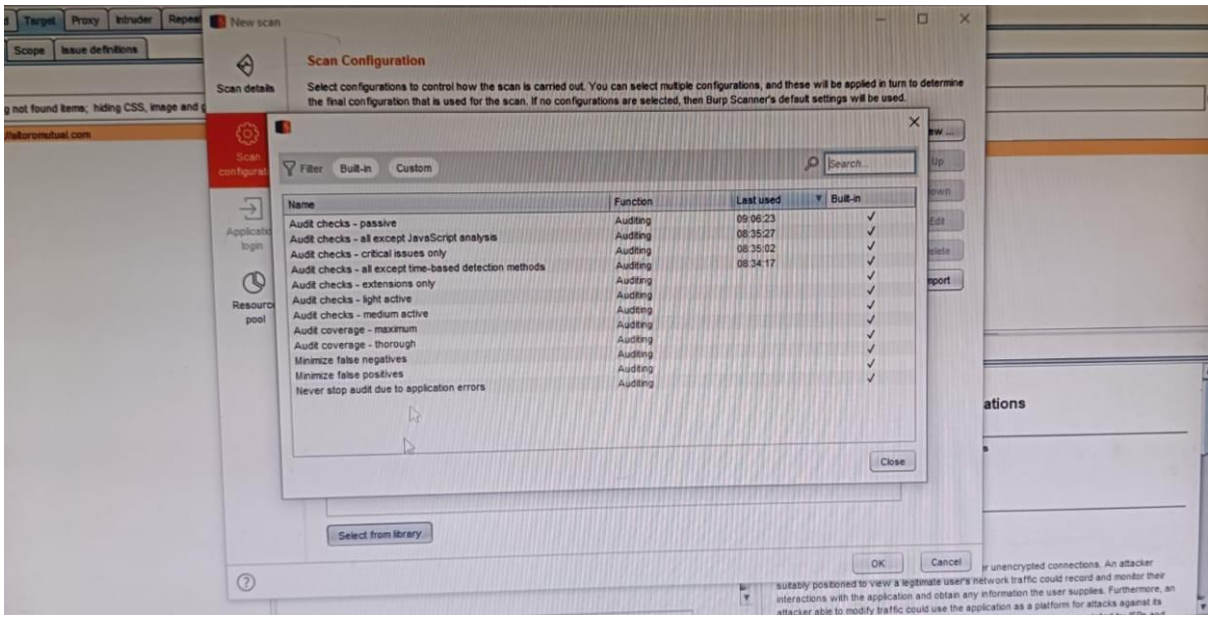
10. select the scan type as Audit selected.



11. Then click on scan configuration items.

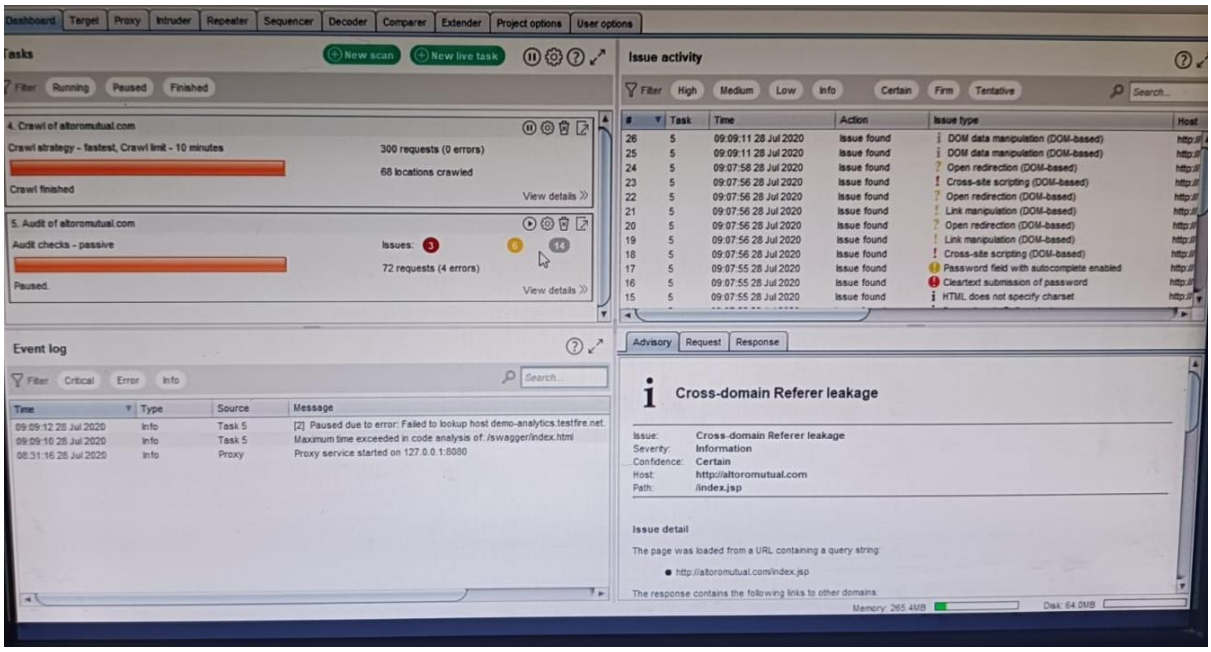


12.Next go to Resource pool then select default resource pool.



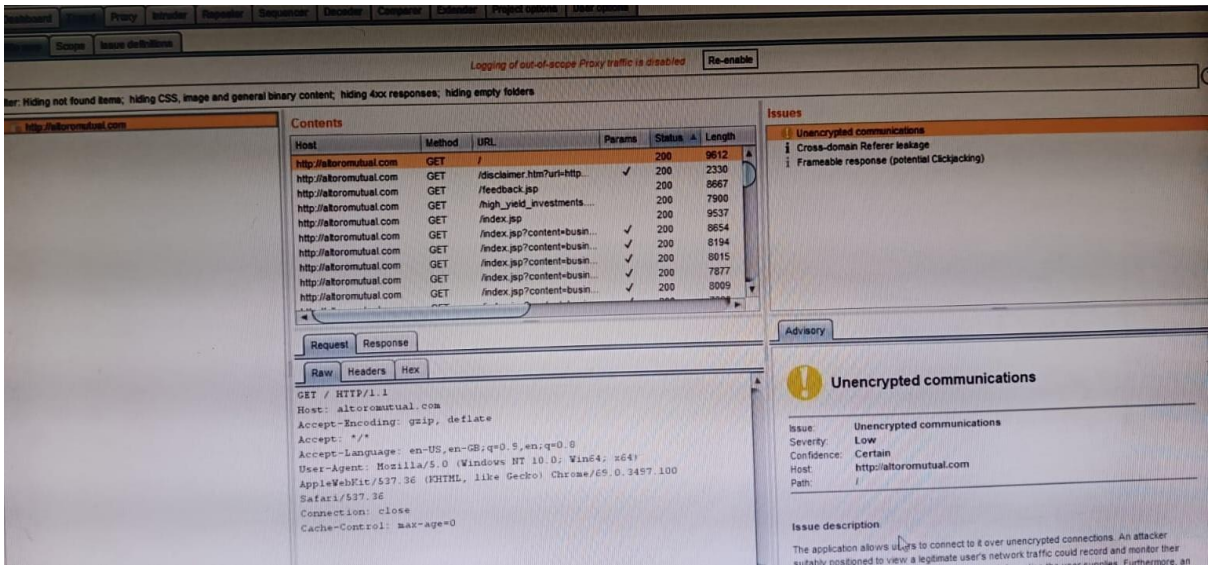
13. Next check results. There are 3 critical issues. Find the medium issues. Then click view to see the vulnerabilities.

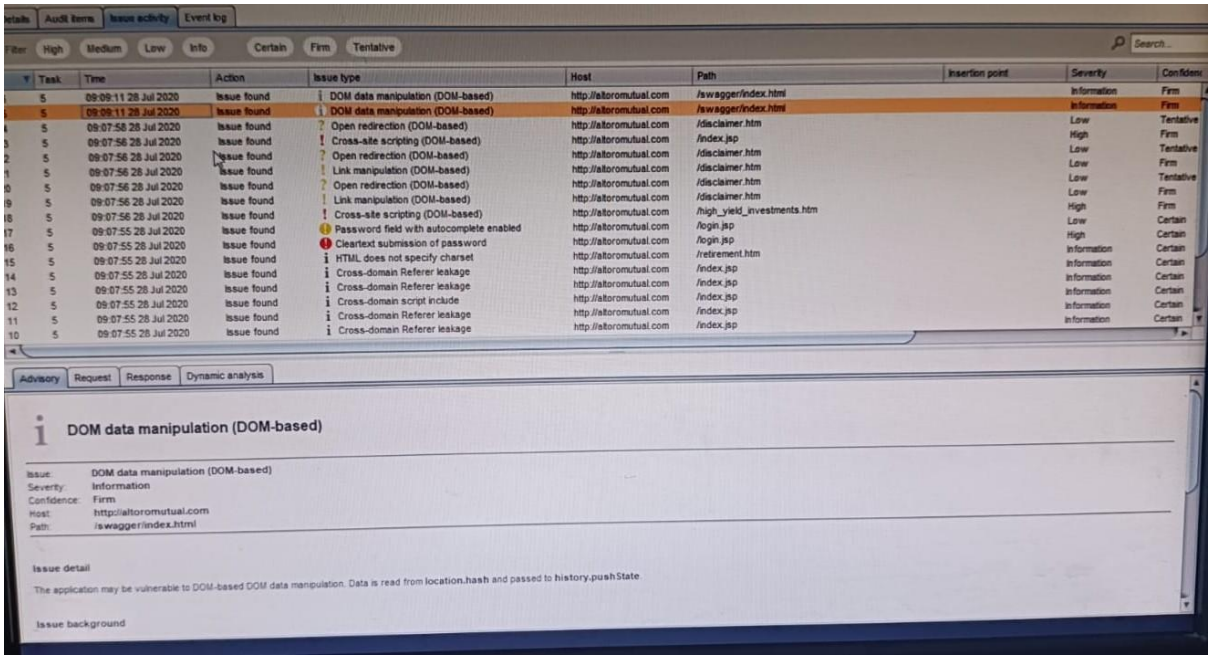
14. It has the speciality to show the vulnerability with the specified name.

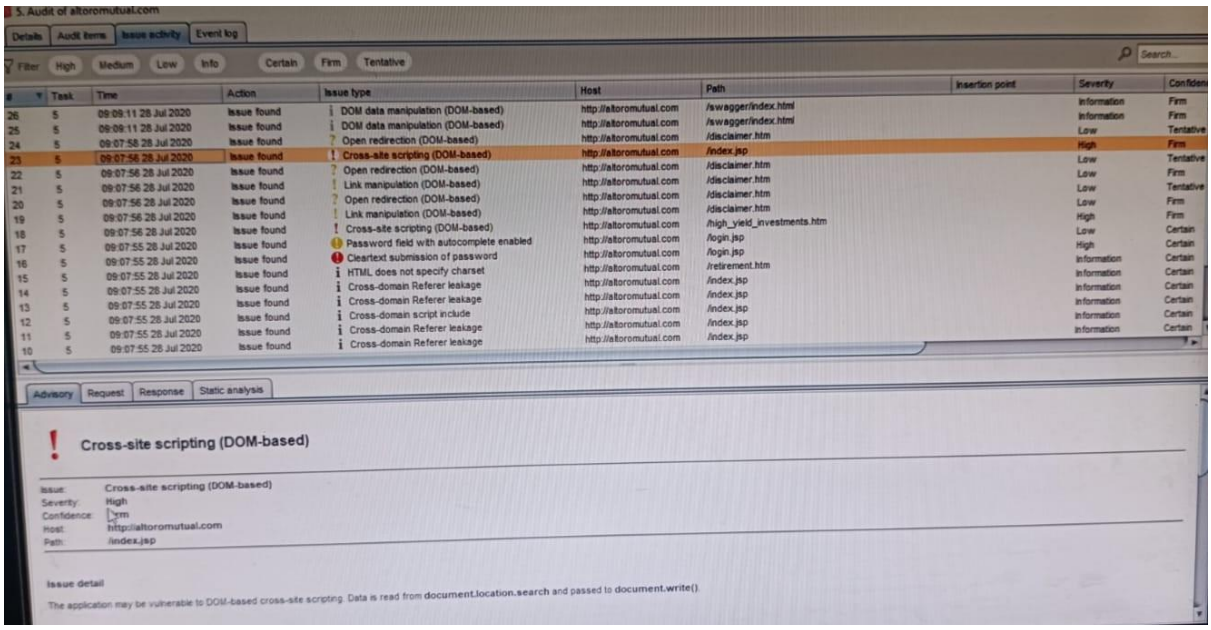


15. Now we can see the advisory, request and response and static analysis.

16. Now we can see the cross verification by using the options like Raw, Params, Headers,Hex.



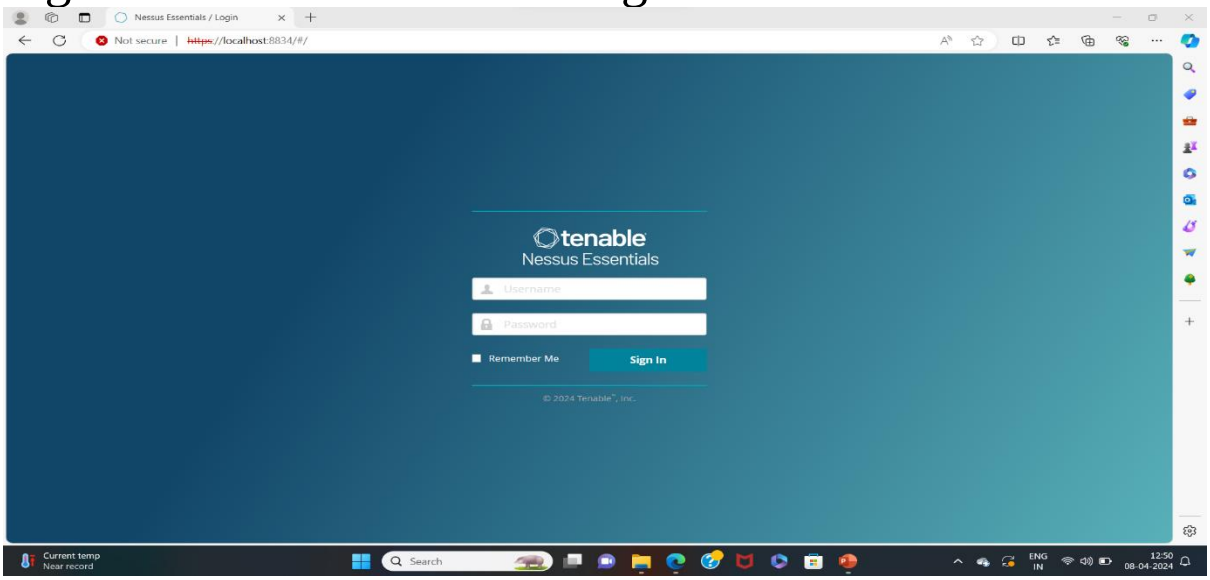

Details
Audit items
Issue activity
Event log
Filter
High
Medium
Low
Info
Certain
Firm
Tentative
Search...
Task
Time
Action
Issue type
Host
Path
Insertion point
Severity
Confidence
5 09:09:11 28 Jul 2020 Issue found DOM data manipulation (DOM-based) http://altoromutual.com /swagger/index.html Information Firm
5 09:09:11 28 Jul 2020 Issue found DOM data manipulation (DOM-based) http://altoromutual.com /swagger/index.html Information Firm
5 09:07:58 28 Jul 2020 Issue found Open redirection (DOM-based) http://altoromutual.com /disclaimer.htm Low Tentative
5 09:07:56 28 Jul 2020 Issue found Cross-site scripting (DOM-based) http://altoromutual.com /index.jsp High Firm
5 09:07:56 28 Jul 2020 Issue found Open redirection (DOM-based) http://altoromutual.com /disclaimer.htm Low Tentative
5 09:07:56 28 Jul 2020 Issue found Link manipulation (DOM-based) http://altoromutual.com /disclaimer.htm Low Firm
5 09:07:56 28 Jul 2020 Issue found Open redirection (DOM-based) http://altoromutual.com /disclaimer.htm Low Tentative
5 09:07:56 28 Jul 2020 Issue found Link manipulation (DOM-based) http://altoromutual.com /disclaimer.htm Low Firm
5 09:07:56 28 Jul 2020 Issue found Cross-site scripting (DOM-based) http://altoromutual.com /high_yield_investments.htm High Firm
5 09:07:55 28 Jul 2020 Issue found Password field with autocomplete enabled http://altoromutual.com /login.jsp Low Certain
5 09:07:55 28 Jul 2020 Issue found Cleartext submission of password http://altoromutual.com /login.jsp High Certain
5 09:07:55 28 Jul 2020 Issue found HTML does not specify charset http://altoromutual.com /retirement.htm Information Certain
5 09:07:55 28 Jul 2020 Issue found Cross-domain Referer leakage http://altoromutual.com /index.jsp Information Certain
5 09:07:55 28 Jul 2020 Issue found Cross-domain Referer leakage http://altoromutual.com /index.jsp Information Certain
5 09:07:55 28 Jul 2020 Issue found Cross-domain script include http://altoromutual.com /index.jsp Information Certain
5 09:07:55 28 Jul 2020 Issue found Cross-domain Referer leakage http://altoromutual.com /index.jsp Information Certain
5 09:07:55 28 Jul 2020 Issue found Cross-domain Referer leakage http://altoromutual.com /index.jsp Information Certain
Advisory
Request
Response
Dynamic analysis
DOM data manipulation (DOM-based)
Issue: DOM data manipulation (DOM-based)
Severity: Information
Confidence: Firm
Host: http://altoromutual.com
Path: /swagger/index.html
Issue detail
The application may be vulnerable to DOM-based DOM data manipulation. Data is read from location.hash and passed to history.pushState.
Issue background


5. Audit of altoromutual.com
Details
Audit items
Issue activity
Event log
Filter
High
Medium
Low
Info
Certain
Firm
Tentative
Search...
Task
Time
Action
Issue type
Host
Path
Insertion point
Severity
Confidence
Advisory
Request
Response
Static analysis
Cross-site scripting (DOM-based)
Issue: Cross-site scripting (DOM-based)
Severity: High
Confidence: Firm
Host: http://altoromutual.com
Path: /index.jsp
Issue detail
The application may be vulnerable to DOM-based cross-site scripting. Data is read from document.location.search and passed to document.write().

REPORT ON MAIN WEBSITE

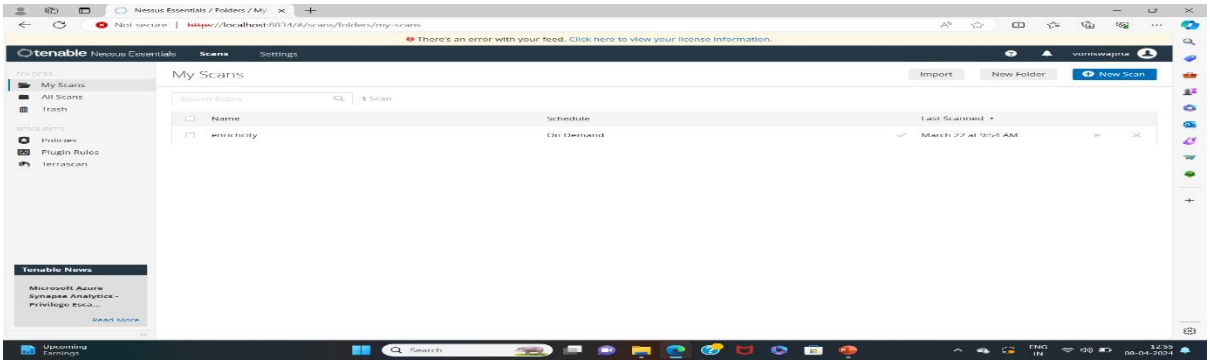
Chosen Website: https://enrichcity.com

- First you need to install Nessus. There are instructions on the Tenable website that show you how to navigate to the Nessus package file, start the installation complete the windows InstallShield Wizard, and install WinPcap.
- There are several basic steps to run a Nessus scan. First, you need to launch Nessus. Then enter your login credinitials. Click on sign In.

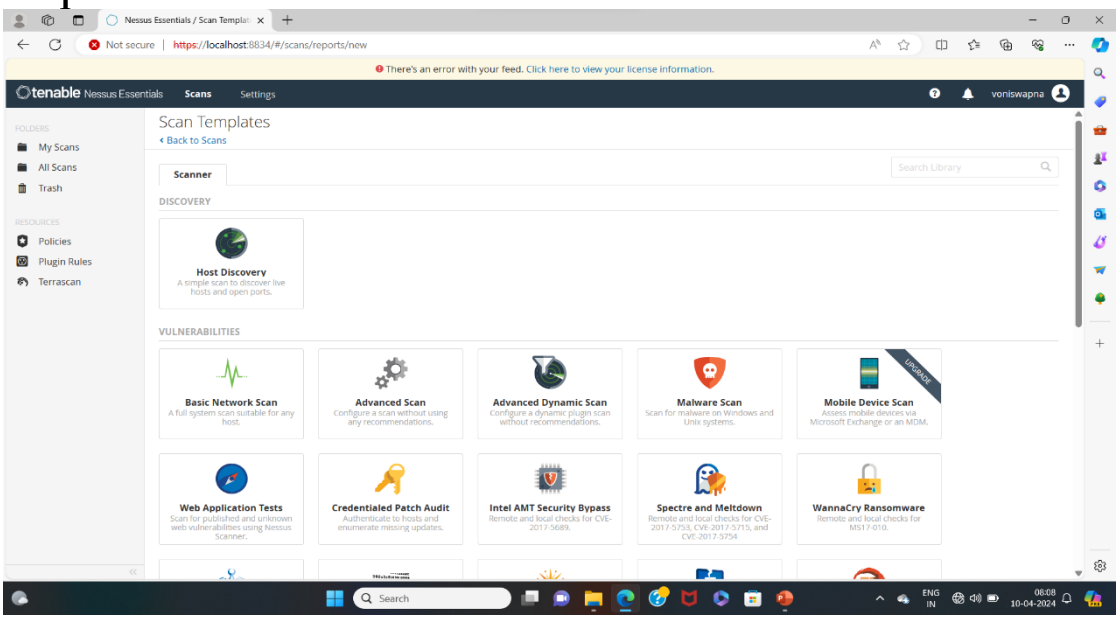


- Navigate to the top right and click on scans. It will take to you My Scans page. In my scan page you find a New Scan bar in the top.

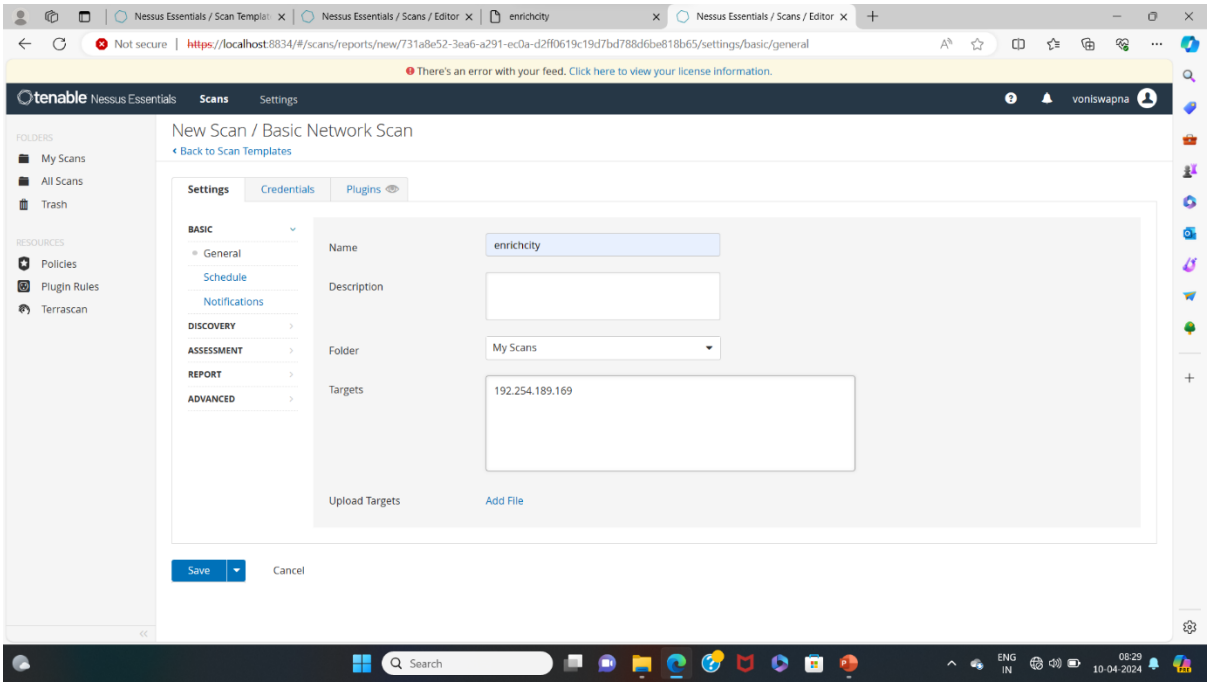
- Then click on New Scan.



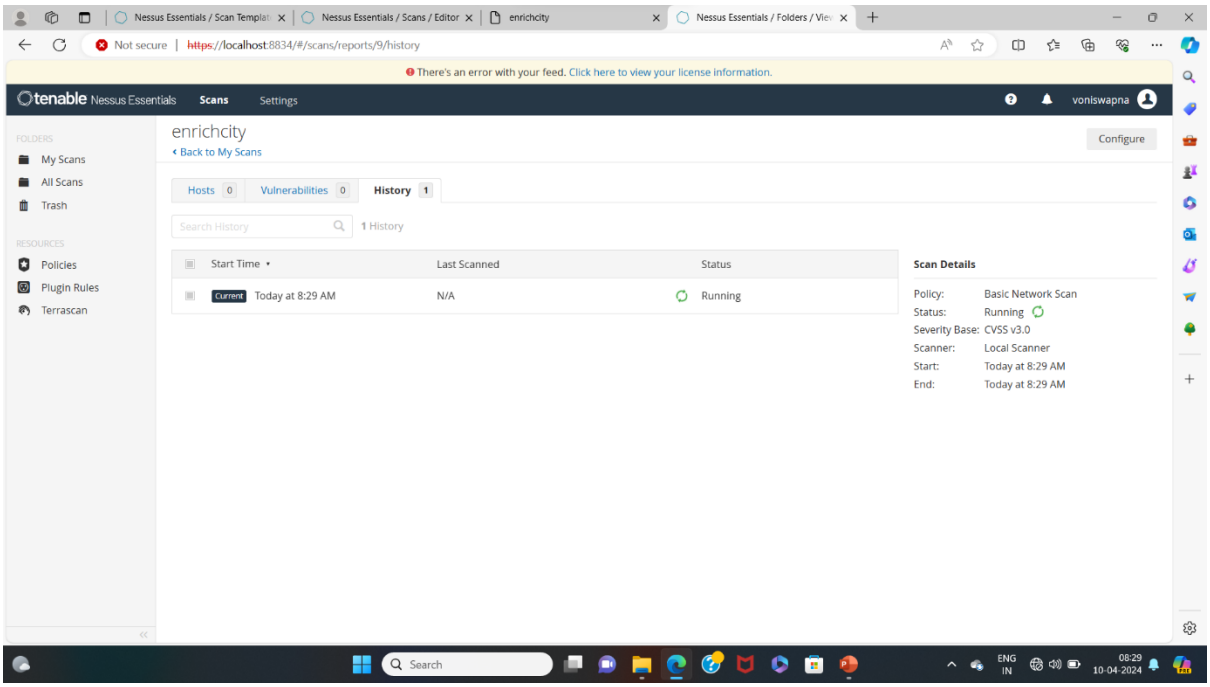
- Nessus provides a wide variety of templates you can use. You will select the one you want. Scan settings can be configured to refine parameters as required.



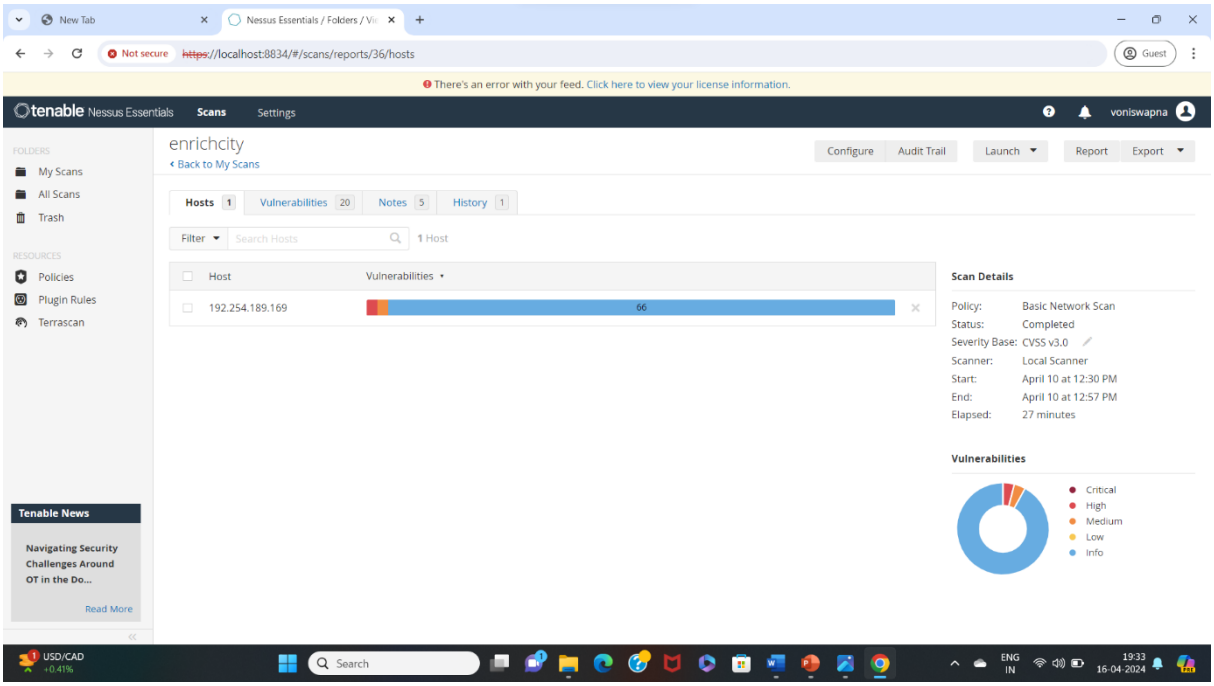
- Then select Basic Network Scan.
- Enter the website name in Name and ip address in the targets.
- Name: enrichcity
- Targets: 192.254.189.169



- Then click on save.

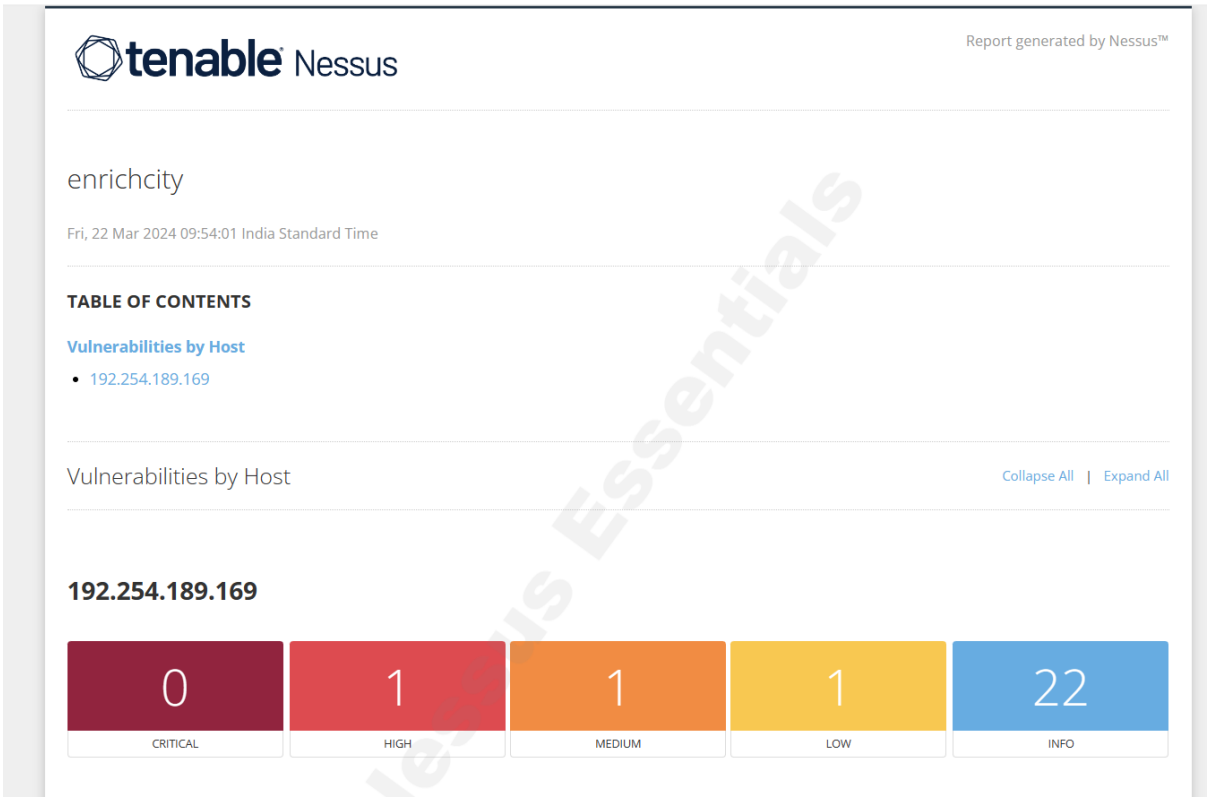


- After the completion of scanning, it shows the scan details and vulnerabilities in the website.

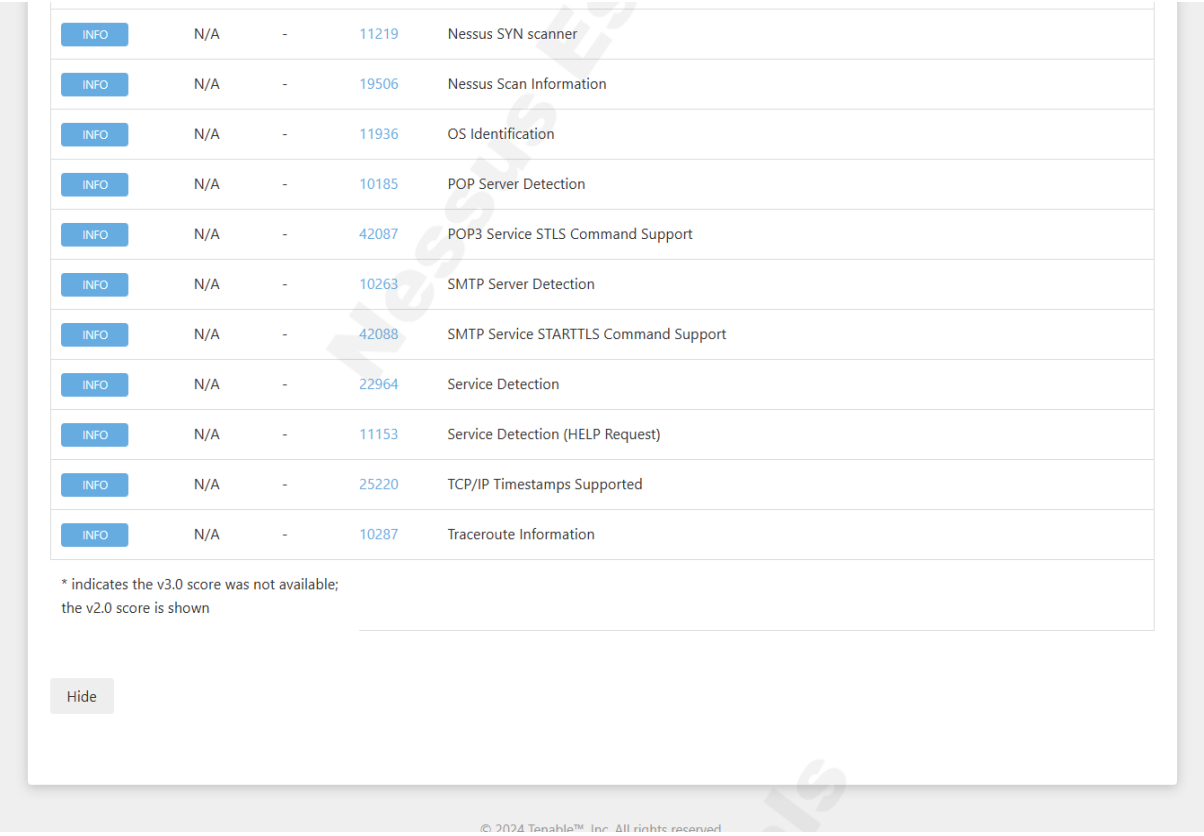


- Then click on report to generate a report.

REPORT:



Severity	CVSS v3.0	VPR Score	Plugin	Name
HIGH	7.5	3.6	35450	DNS Server Spoofed Request Amplification DDoS
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
LOW	2.6*	-	54582	SMTP Service Cleartext Login Permitted
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	54615	Device Type
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	11414	IMAP Service Banner Retrieval
INFO	N/A	-	42085	IMAP Service STARTTLS Command Support
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification



INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10185	POP Server Detection
INFO	N/A	-	42087	POP3 Service STLS Command Support
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	11153	Service Detection (HELP Request)
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Hide

- These are vulnerabilities in this website.
- Now we have to discuss about the vulnerabilities in this website.

Vulnerability Name: DNS Server Spoofed Request Amplification DDoS

Severity: High

Plugin ID: 35450

Port: 53/udp/dns

Description: The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

Solution: Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Vulnerability Name: DNS Server BIND version Directive Remote Version Detection

Severity: Info

Plugin ID: 10028

Description: The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution: It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Vulnerability Name: DNS Server Cache Snooping Remote Information Disclosure

Severity: Medium

Plugin ID: 12217

Port: 53/udp/dns

Description: The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.
This may allow a remote attacker to determine which domains

have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Solution: Contact the vendor of the DNS software for a fix.

Vulnerability Name: POP3 Service STLS Command Suppot

Severity: None

Plugin ID: 42087

Port: 110/tcp/pop3

Description: The remote POP3 service supports the use of the 'STLS' command to switch from a cleartext to an encrypted communications channel.

Solution: n/a

Vulnerability Name: Nessus SYN scanner

Severity: None

Plugin ID: 11219

Port: 21/tcp/ftp

Description: This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution: Protect your target with an IP filter.

Vulnerability: Service Detection

Severity: none

Plugin ID: 22964

Port: 21/tcp/ftp

Description: Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution: n/a

Vulnerability Name: Server Detection (Help Request)

Severity: none

Plugin ID: 11153

Port: 443/tcp

Description: It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution: n/a

Vulnerability Name: IMAP Service Banner Retrieval

Severity: none

Plugin ID: 11414

Port: 143/tcp/imap

Description: An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution: n/a

Vulnerability Name: POP Server Detection

Severity: none

Plugin ID: 10185

Port: 110/tcp/pop3

Description: The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

Solution: Disable this service if you do not use it.

Vulnerability Name: SMTP Server Detection

Severity: none

Plugin ID:10263

Port: 465/tcp/smtp

Description: The remote host is running a mail (SMTP) server on this port.
Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution: Disable this service if you do not use it, or filter incoming traffic to this port.

Vulnerability Name: HTTP Server Type and Version

Severity: none

Plugin ID:

Port: 2078/tcp

Description: This plugin attempts to determine the type and the version of the remote web server.

Solution: n/a

STAGE-2

What is Cyber Security?

A successful cyber security approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people process and technology must all complement one another to create an effective defense from cyber attacks. A unified threat management system can automate integrations across select cisco security products and accelerate key security operations functions: detection, investigating and remediation.

Everyone also benefits from the work of cybersecurity threat researches like the team of 250 threat researches and taols, who investigate now and emerging threats and cyberattack strategies. Educate the public on the importance of cybersecurity, and strengthen opensource tools. Their work makes the internet safer for everyone.

What are Cyber threats?

Threats are acts performed by individuals with harmful internet, whose goal is to steal data, cause damage to or disrupt computing systems. Common categories of cyber threats include malware, social

engineering, man in the middle attack, denial of service(DOS) and injection attacks.

Cyber threats can originate from ac variety of source from hostile nation states and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.

Types of threats:

1.Malware attacks

- Viruses
- Worms
- Trojans
- Ransomware
- Cryptojacking
- Spyware
- Adware
- Fireless malware
- Rootkits

2.Social engineering attacks

- Baiting
- Pretexting
- Phishing
- Vishing
- Smishing
- Piggy backing
- Tailgating

3.Man-in-the-Middle attack

- Wifi-eavesdropping
- Email hijacking
- DNS spoofing
- IP spoofing
- HTTP spoofing

4.Denial-of-service(DOS)

- HTTP flood DDOS
- SYN flood DDOS
- UDP flood DDOS
- ICMP flood DDOS
- NTP flood DDOS

5.Injection attacks

- SQL injection
- Code injection
- OS command injection
- LDAP injection

What is Scanning tool?

Scanners are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as cross-site scripting, SQL injection, command injection, path traversal and insecure configuration. This category of tools is frequently referred to as Dynamic Application Security Testing Tools. This tools are very useful to

scan the vulnerabilities and it gives proper protection for our important data and websites. It have different scanning tools are available most widely used Nessus and Burpsuite scanners.

What is Burpsuite scanner?

Burp scanner is an automated dynamic application security testing (DAST) web vulnerability scanner. Designed to replicate the activities and methodologies of a skilled manual tester.

Burp scanner handles virtually any target. Advanced features such as state management and automated logins enable it to deal with the challenges that scanning modern web application can pose. Although the actions taken during a scan vary depending on target and configuration scans generally comprise two key phases.

1.Crawling

2.Auditing

What is Nessus Scan?

Nessus is a remote security scanning tool, which scans a computer or websites and raises on alert if it discovers any vulnerabilities that malicious hackers

could use to gain access to any computer have connected to a network.

Nessus is very extensible, providing a scripting language for you to write tests specific to your system once you become more familiar with the tool. It has a opensource, patching assistance and easy installation.

What do you understand in the Nessus report?

A Nessus report is a comprehensive documentation summarizing the findings from a vulnerability scan conducted by the Nessus vulnerability assessment tool. It outlines identified security weaknesses, potential threats, and vulnerabilities within a network or system. The report provides detailed insights into specific issues such as outdated software, misconfigurations, potential entry points for cyber threats, and more, categorized them based on severity levels. Additionally, it often includes recommendations for remediation or mitigation strategies to address the identified vulnerabilities. This report serves as a valuable resource for IT professionals and security teams, guiding them in fortify systems and networks against potential cyber risks.

CONCLUSION

The current cybersecurity threat landscape presents significant challenges that individuals and organizations must address to protect themselves from cyber-attacks. As technology continue to evolve, the ongoing progression of this initiative remains integral in bolstering defences against the ever-evolving landscape of cyber threats. The primary goal of this project is to proactively identify the cyber threats and vulnerabilities in the websites, ultimately contributing to the collective efforts to establish a more secure digital environment.

In this project we found the vulnerabilities which effects the organization by using scanning tools like Nessus and Burp suite.

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since the attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. The vulnerability management life cycle is designed to counter the efforts made by attackers in the quickest and most effective way.

FUTURE SCOPE

The future scope of “Understanding threats: exploring Nessus and Beyond scanning tools”. Project is poised for future advancements and people are saved from unauthorized user and some issues of websites, network and also webservers are saved from the vulnerabilities to using the Nessus and Beyond scanning tools.

Gain unified, continuous visibility of your distributed IT irrespective of endpoints whereabouts. Automatically detect vulnerabilities, miscodnfigurations risky software and much more.

Furthermore the projects evolution will likely include collaborations with scanning tools to findout the threat and vulnerabilities. It has been good for the peoples and owners of websites or webservers to reduce the loss of business to used this project. People were awarded by this kind of issues and problems. How are protect our data from the hackers. This collaborative approach will significantly enrich the project’s database, enabling a border spectrum of threat identification and also vulnerabilities.

Moreover the project’s future scope defines the boundaries and limitations of our analysis and exploring it’s user base and functionalities.

Potentially reaching the wide range of users and audience and serving diverse to aware the so many people on the threats and vulnerabilities and clearly explain the scanning tools because these are very help to us and protect our precious and sensitive data. Moreover everyone is studying cybersecurity. It has a very great platform of business users and cybersecurity is to completely perform rectifying security service, two critical incident response elements are necessary information and organization.

REFERENCES

1. https://www.researchgate.net
2. https://www.mimecast.com
3. https://www.budcrowd.com
4. I would like to express my sincere appreciation and cooperation to Sri. V. Vijaya Rama Raju, Associate professor in computer science, Sri Balaji Degree College their invaluable guidance and support throughout the duration of this cyber security project. As a mentor you play a crucial role in a project by avoiding guidance, advice, and support to the project team. They leverage their experience and expertise to help team members

navigate challenges, make informed decisions, and achieve project goals. As a mentor also serve as role models, offering encouragement and motivation to team members and helping them develop their skills and capabilities. Overall, a mentor's involvement can greatly enhance the success and growth of a project and its participants. Their expertise and insights have been instrumental in shaping the success of this endeavor. Thank you for your dedication and mentorship".

5. https://ensia.eruopa.eu