Part 1:-Project description

We have selected **http://altoromutual.com/ to perform vulnerability asessment.**

We have used so many tools like nmap,wireshark,kali linux,nessus,brup suite,metasploit ect.

- **Nmap:-**it is used find the open ports,operating system used by the website and detailed information about the website.
- **Wireshark:-**It is used to analysis tranfer of data packets from user system to website server.
- **Kali linux:-**It contain so many useful tools like metasploit,nmap,wireshark ect.
- **Nesuss:-**It is used to generate the final report of the website of containing website vulnerabilities**.**

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

REPORT GENERATED BY THE NMAP ABOUT

http://altoromutual.com/

Nmap 7.92 scan initiated Wed Jul 12 09:40:51 2023 as: nmap -A -T4 -oN file.txt 65.61.137.117

Nmap scan report for 65.61.137.117

Host is up (0.052s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|_http-server-header: Apache-Coyote/1.1

|_http-title: Altoro Mutual

443/tcp open ssl/http Apache Tomcat/Coyote JSP engine 1.1

| ssl-cert: Subject: commonName=demo.testfire.net

| Subject Alternative Name: DNS:demo.testfire.net, DNS:altoromutual.com

| Not valid before: 2023-06-19T00:00:00

|_Not valid after: 2024-06-14T23:59:59

|_ssl-date: 2023-07-12T13:42:58+00:00; -1s from scanner time.

|_http-title: Altoro Mutual

8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|_http-server-header: Apache-Coyote/1.1

|_http-title: Altoro Mutual

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose|specialized

Running: Microsoft Windows XP|7|2012, VMware Player

OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player

OS details: Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device

Network Distance: 2 hops

Host script results:

|_clock-skew: -1s

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 0.13 ms 192.168.137.2

2 0.12 ms 65.61.137.117

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.

Nmap done at Wed Jul 12 09:43:01 2023 -- 1 IP address (1 host up) scanned in 130.97 seconds

- **List of students particiated in the vulnerability assement of altoro mutual website**

S.NO	NAME	COLLEGE NAME	BRANCH	EMAIL
1.	**BODIGARI.AMARNATH REDDY(Team leader)**	**RAGHU ENGINEERING COLLEGE(JNTU-GV)**	**COMPUTER SCIENCE ENGINEERING (CYBER SECURITY)**	**20981A4608@raghuenggcollege.in**
2.	**PYDISETTI.SHARUN**	**RAGHU ENGINEERING COLLEGE(JNTU-GV)**	**COMPUTER SCIENCE ENGINEERING (CYBER SECURITY)**	**20981A4649@raghuenggcollege.in**
3.	**GAJJALA.MANOJ REDDY**	**RAGHU ENGINEERING COLLEGE(JNTU-GV)**	**COMPUTER SCIENCE ENGINEERING (CYBER SECURITY)**	**20981A4620@raghuenggcollege.in**
4.	**GUDELA.PRASANTH KUMAR**	**RAGHU ENGINEERING COLLEGE(JNTU-GV)**	**COMPUTER SCIENCE ENGINEERING (CYBER SECURITY)**	**20981A4624@raghuenggcollege.in**
5.	**MISRO.SASIBHUSAN**	**RAGHU ENGINEERING COLLEGE(JNTU-GV)**	**COMPUTER SCIENCE ENGINEERING (CYBER SECURITY)**	**20981A4635@raghuenggcollege.in**

.LIST OF VULNERABLE PARAMETERS,LOCATIO DISCOVERED.

TABLE 1

S.NO	VULNERABILITY PATH	NAME OF THE VULNERABILITY	REFERENCE CWE
1.	http://altoromutual.com/search.jsp?query=%3Cbutton+p	CGI Generic XSS (comprehensive test)	CWE:352 Cross site request forgery
2.	file:///C:/Users/LENOVO/Desktop/click.html	Web Application Potentially Vulnerable to Clickjacking	CWE:693 Incorrectly uses a protection mechanism
3.	http://altoromutual.com/bank/main.jsp	Web Server Transmits Cleartext Credentials	CWE:522 Insufficiently protected credentials

4.	**http://altoromutual.com/**	**HSTS Missing From HTTPS Server (RFC 6797)**	**CWE:523 Unprotected transport of credentials**
5.	**http://altoromutual.com/bank/main.jsp**	**Web Server Allows Password Auto-Completion**	**CWE:200 Exposure of sensitive information**
6.	**http://altoromutual.com/index.jsp**	**HTTP Server Type and Version**	**CWE:444 Inconsistent interpretation of HTTP requests**
7.	**http://altoromutual.com/index.jsp**	**CGI Generic Tests Timeout**	**CWE:287 Improper authentication**

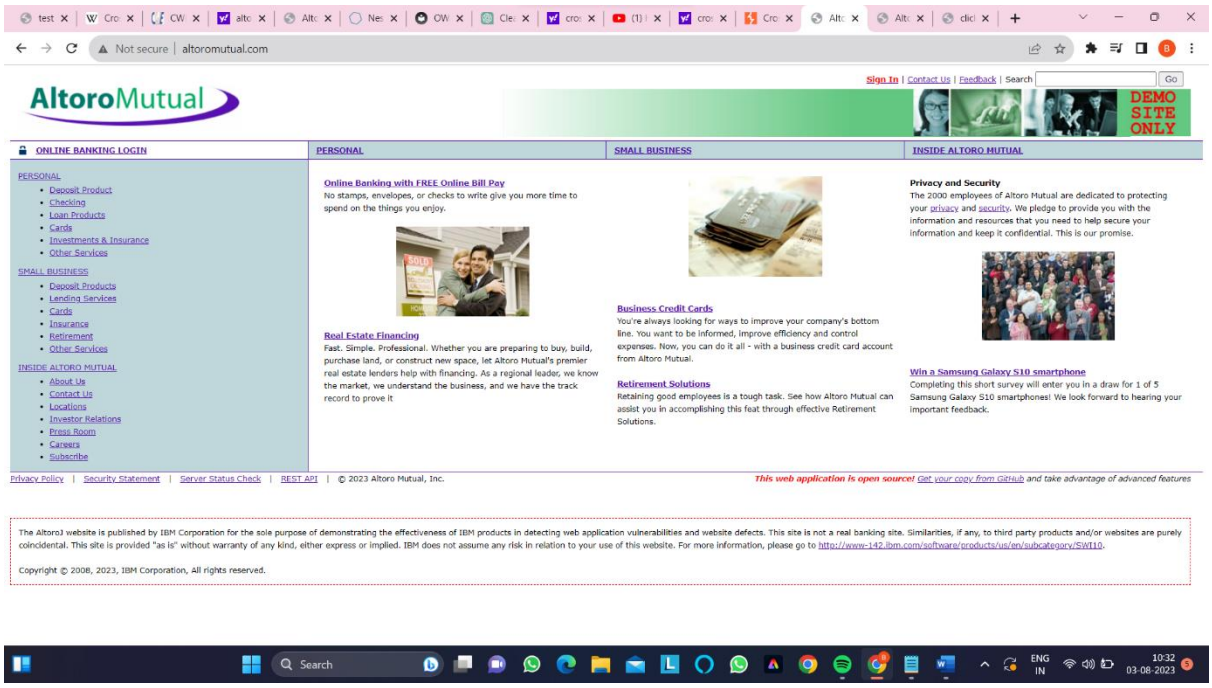
PART 2: DETAILED REPORT

VULNERABILITY ASESSMENT AND VERIFICATION.

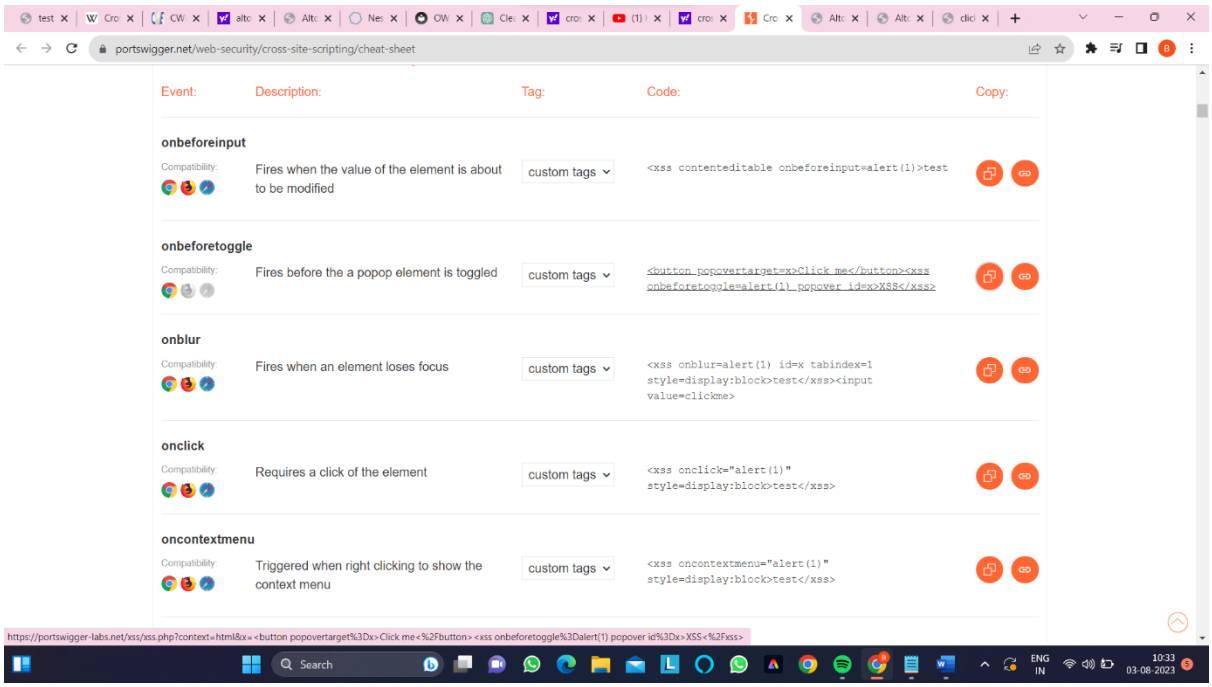
1)VULNERABILITY NAME:- CGI Generic XSS (comprehensive test)

- **CWE:-20,74,81,352 ect.**
- **OWASP CATEGORY:-A03:2021-INJECTION**
- **DESCRIPTION:-** The remote web server hosts CGI scripts that fail to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. These XSS are likely to be 'non-persistent' or 'reflected.
- **BUSSINESS IMPACT:-** If an attacker successfully exploits a CGI Generic XSS vulnerability, they can steal sensitive user data such as login credentials, personal information, and payment details. This can lead to severe privacy violations and loss of user trust in the affected business.
- **VULNERABILITY PATH:- http://altoromutual.com/search.jsp?query=%3Cbutton+p**
- **VULNERABILITY PARAMETERS:- <button popovertarget=x>Click me</button><xss onbeforetoggle=alert(1) popover id=x>XSS</xss>**
- **STEPS TO REPRODUCE:-**

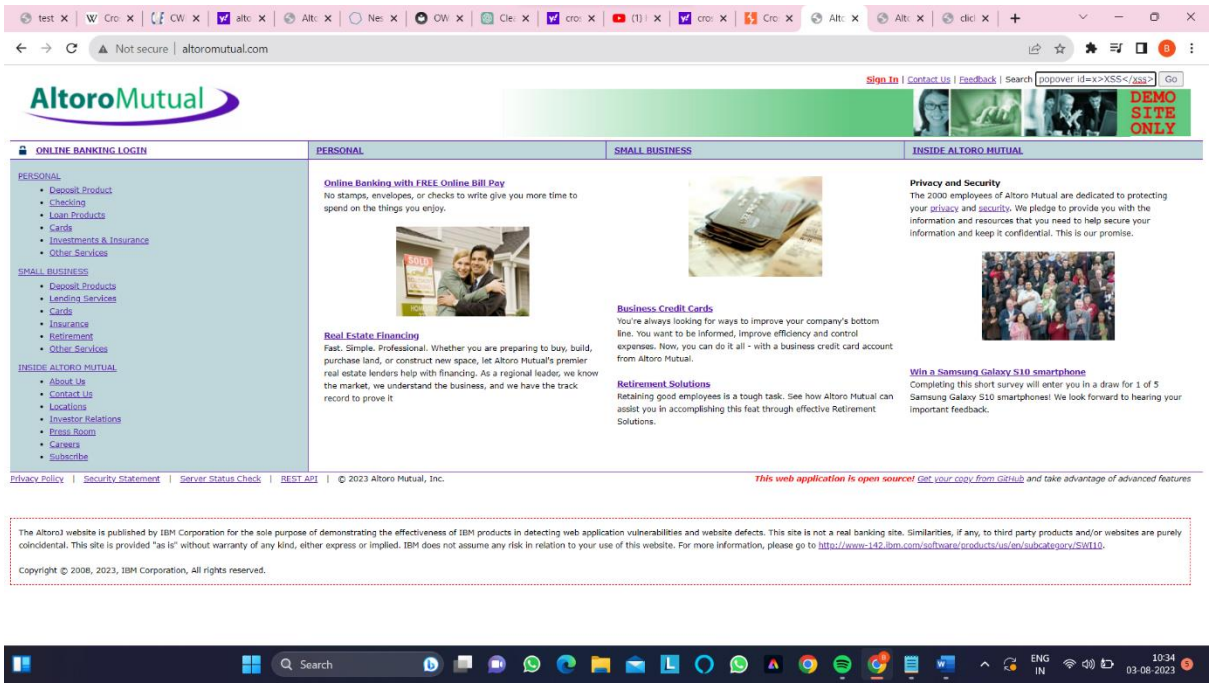
Step 1:-access the website altoromutual.com



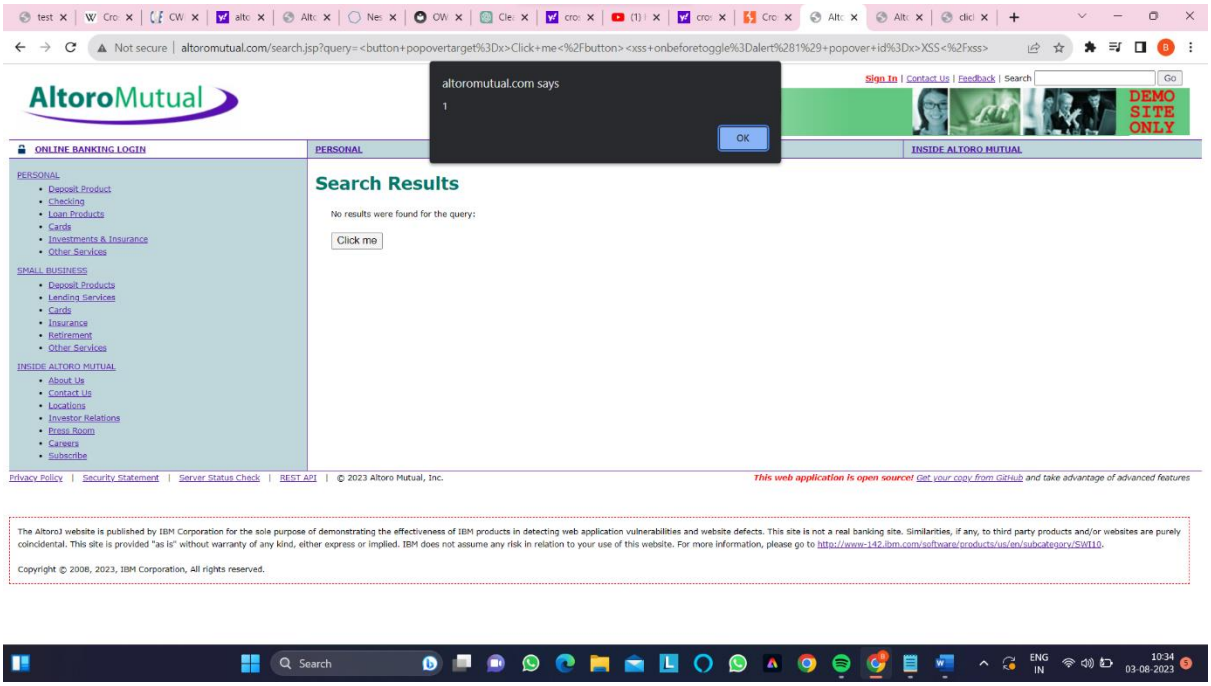
Step 2:-type cross-site script cheat sheet and copy the script



Step 3:-Paste the copied script in search check box



Step 3:-As we can see the website is reacted to th script and poped up a check box



- **REMMIDES:-** Validate and sanitize all user inputs before they are processed by the application. This helps prevent malicious scripts from being executed. Use whitelisting approaches to allow only expected and safe inputs.

2)VULNERABILITY NAME:- Web Application Potentially Vulnerable to Clickjacking

- **CWE:-693 ect.**

- **OWASP CATEGORY:**-A05:2021-SECURITY MISCONFIGURATION

- **DESCRIPTION:-** The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

- X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

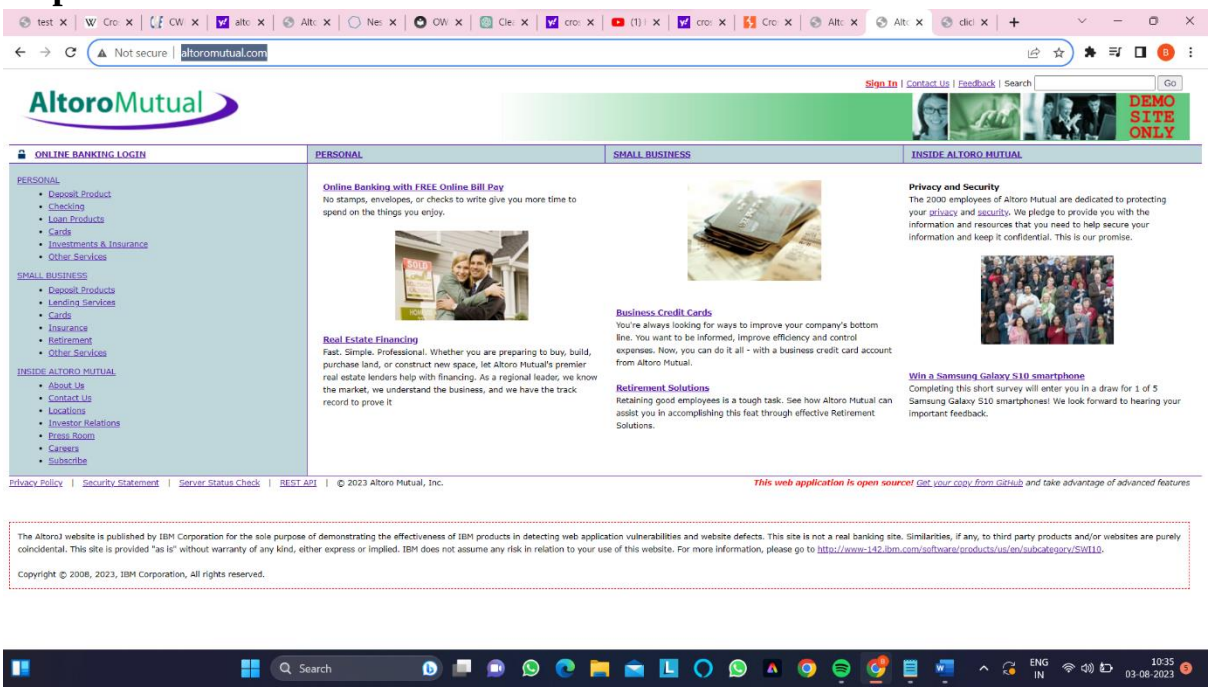
- Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

- Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

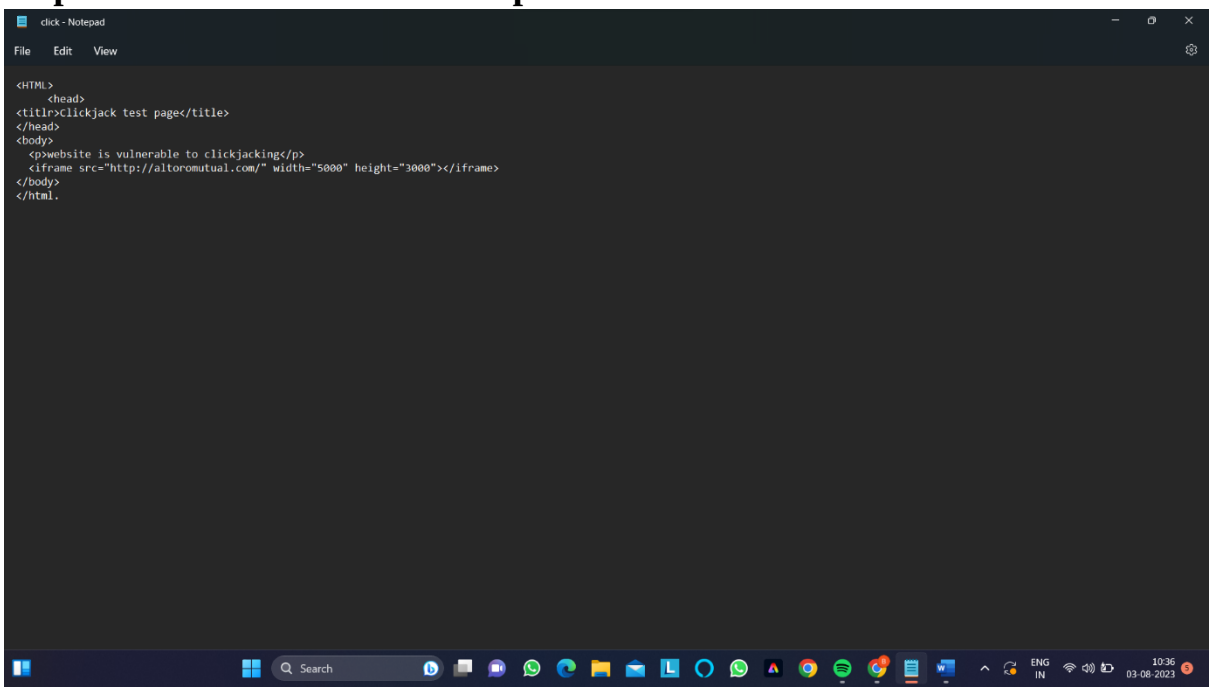
- **BUSSINESS IMPACT:-**. If users are tricked into performing actions they didn't intend to take, it can erode their trust in the web application and the company behind it. This loss of trust can result in decreased usage and user retention.
- Attackers can use clickjacking to manipulate users into unknowingly performing actions that they did not intend to, such as making unauthorized purchases, changing account settings, or even transferring funds.

- **VULNERABILITY PATH:- file:///C:/Users/LENOVO/Desktop/click.html**
- **VULNERABILITY PARAMETERS:-** http://altoromutual.com/
- - http://altoromutual.com/feedback.jsp
- - http://altoromutual.com/index.jsp
- - http://altoromutual.com/login.jsp
- - http://altoromutual.com/search.jsp
- - http://altoromutual.com/status_check.jsp
- - http://altoromutual.com/subscribe.jsp
- - http://altoromutual.com/survey_questions.jsp
- **STEPS TO REPRODUCE:-**

Step 1:- access the website altoromutual.com

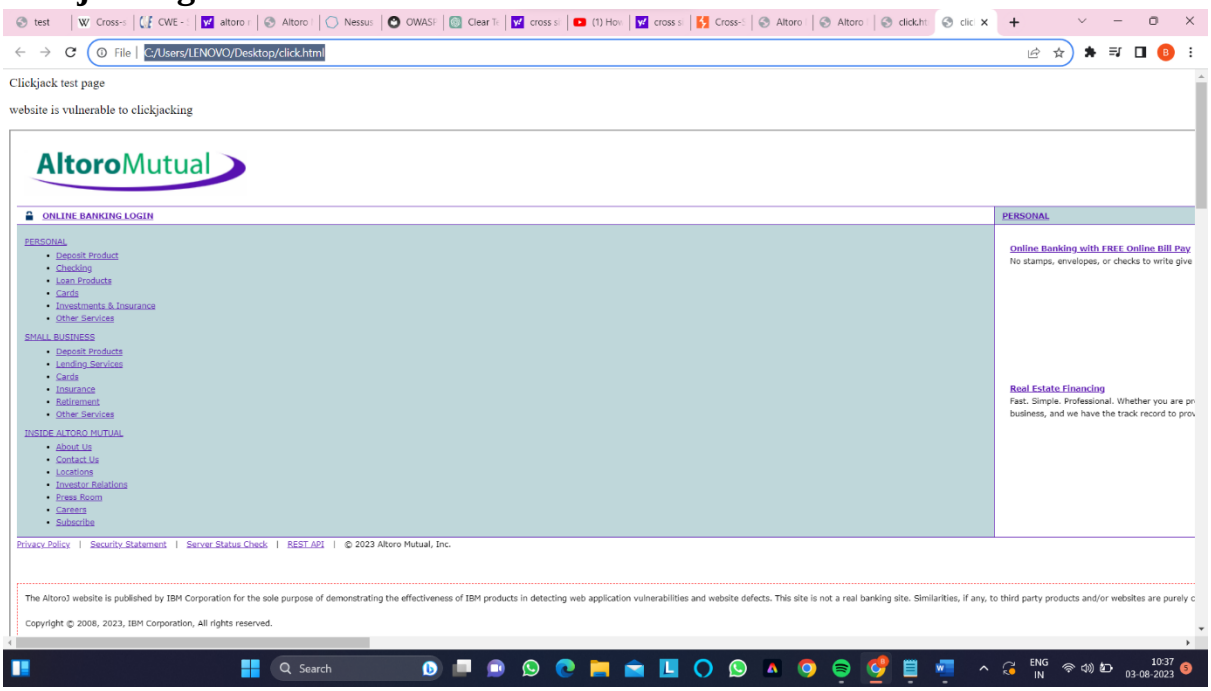


Step 2:-create a html file in notepad and include the website



Step 3:-on the desktop we can see a html file named as click and click on it

Step 4:- As we can a note that the website is vulnerable to clickjacking



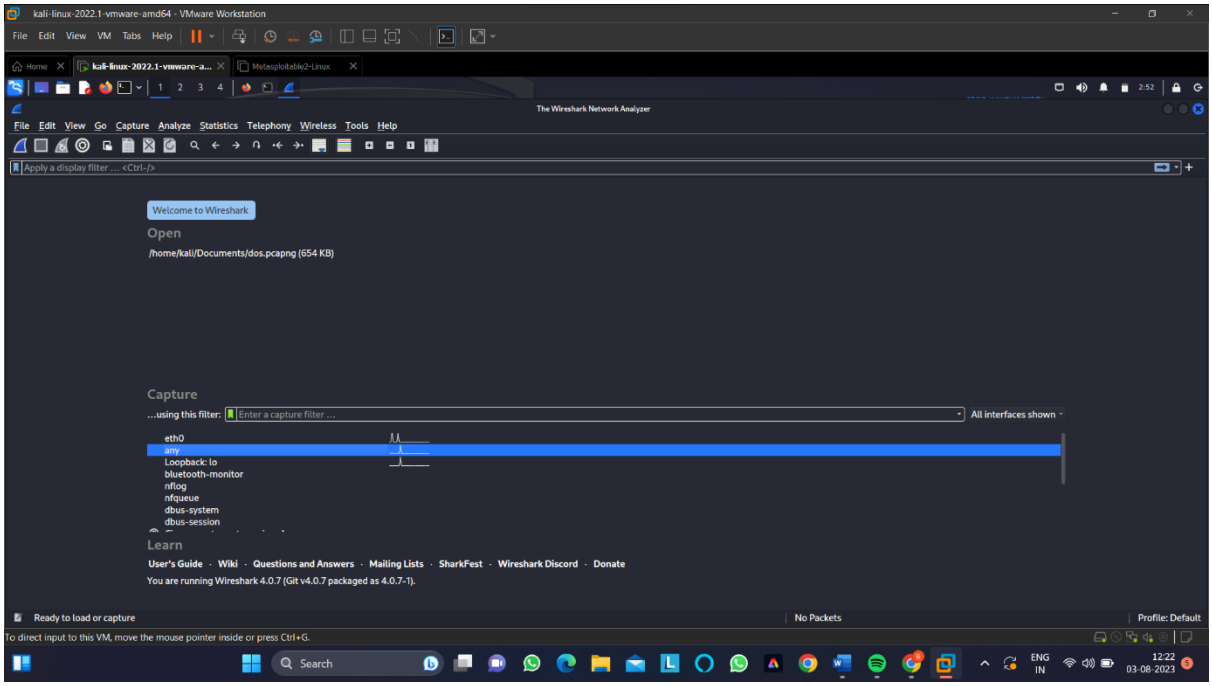
- **REMMIDES:-** Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
- This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

3)VULNERABILITY NAME:- Web Server Transmits Cleartext Credentials

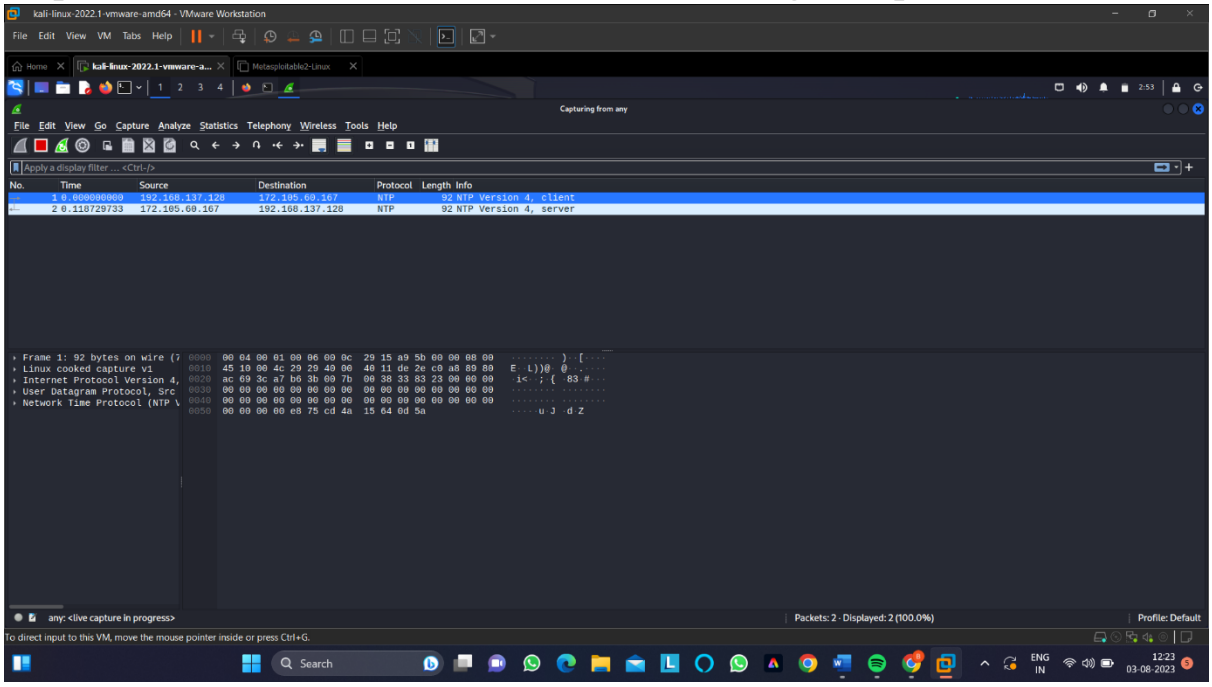
- **CWE:-522,523,718,724 ect.**
- **OWASP CATEGORY:-A04:2021-INSECURE DESIGN.**
- **DESCRIPTION:-** The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
- An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users
- **BUSSINESS IMPACT:-** When credentials are transmitted in plain text, they can be easily intercepted by malicious actors who may be monitoring network traffic. This can lead to unauthorized access to user accounts, sensitive data, and confidential information.
- Data breaches resulting from clear text credential transmission can have financial implications for businesses. They might face legal fees, regulatory fines, and potential lawsuits from affected users, not to mention the cost of mitigating the breach and implementing necessary security measures.
- **VULNERABILITY PATH:- http://altoromutual.com/bank/main.jsp**
- **VULNERABILITY PARAMETERS:- http://altoromutual.com/login.jsp**
- **http://altoromutual.com/bank/main.jsp**
-

- **STEPS TO REPRODUCE:-**

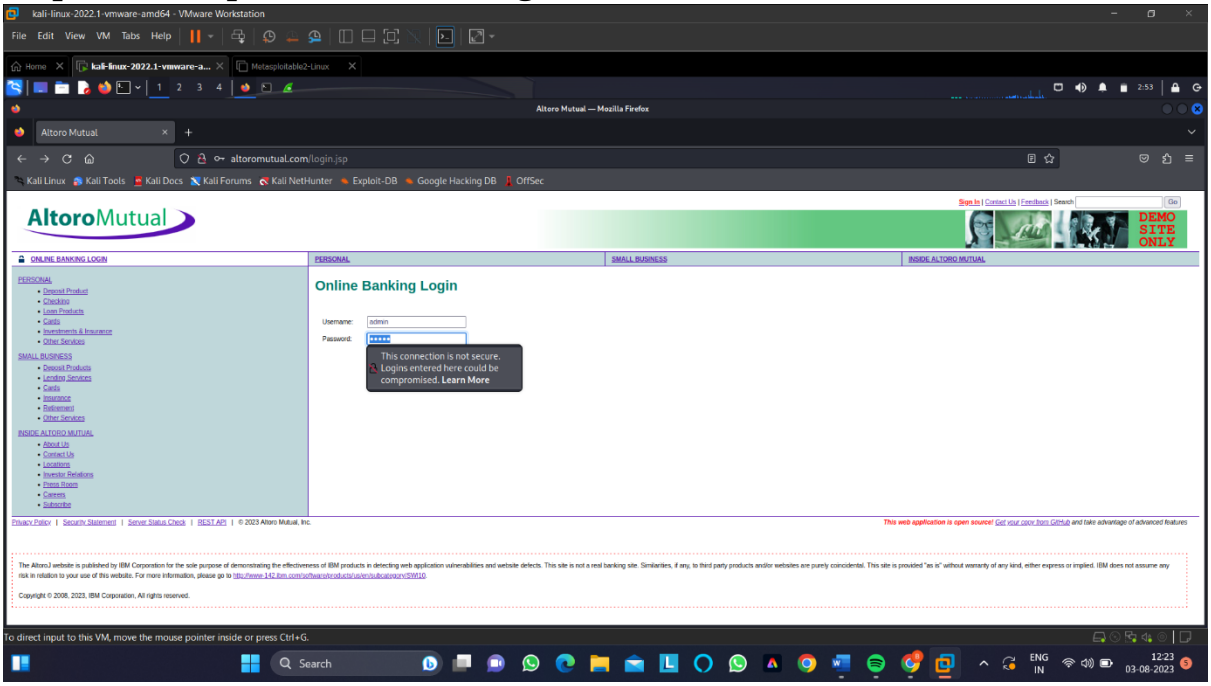
Step 1:-Open kali linux and turn on the wireshark



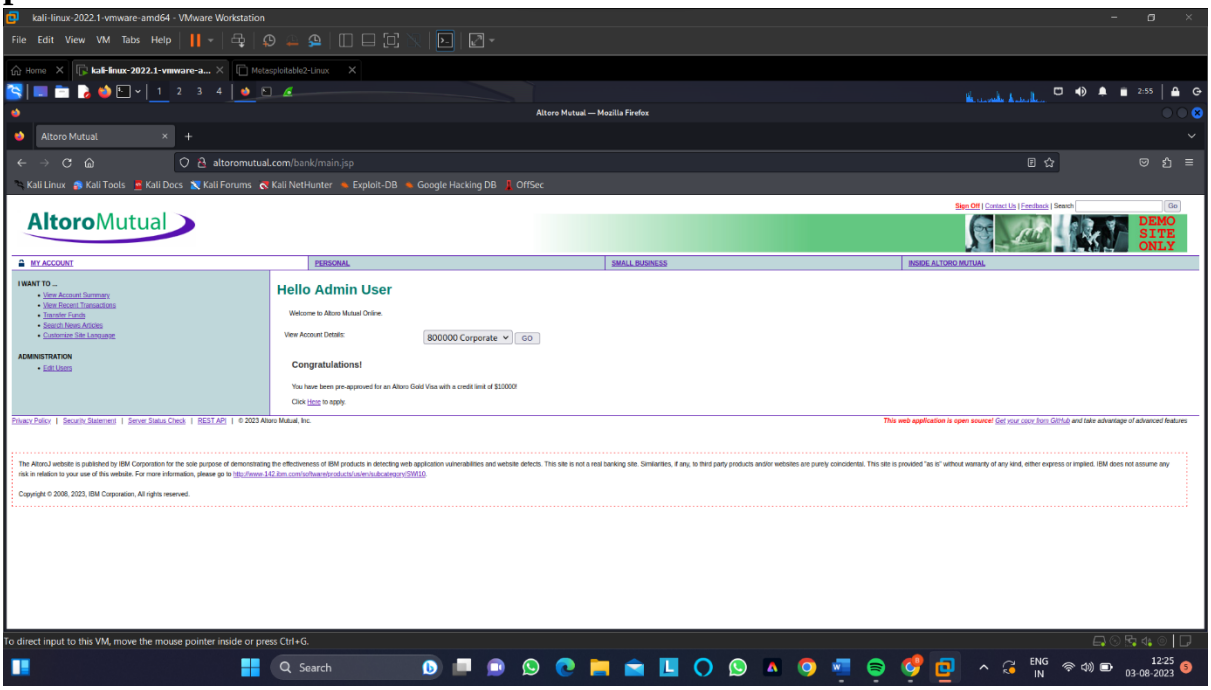
Step 2:-As we can see wire shark started collecting data packets.



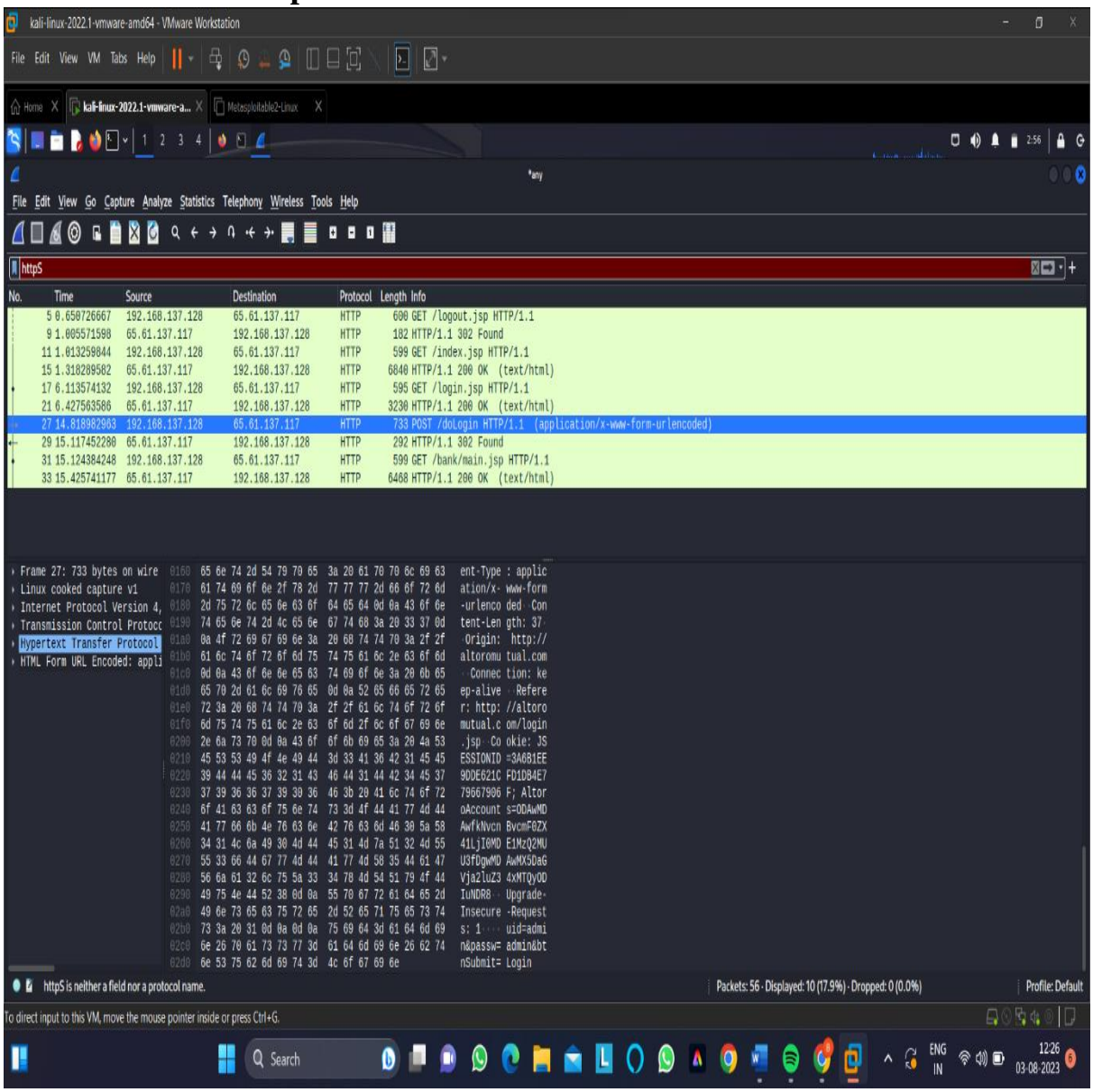
Step 3:-Now open firefox and login to altoromutual website



Step 4:-Give the credentials like user id =admin and password=admin



Step 4:-Here we can see that the user id and passsword arein pain text format.user id=pasword=admin.



REMMIDES:- Implement HTTPS (SSL/TLS) for all communications between the web server and clients. This encrypts the data transmitted, making it difficult for attackers to intercept and decipher.

- Utilize OAuth or SSO mechanisms to allow users to authenticate through third-party services like Google, Facebook, or other identity providers. This reduces the need to handle sensitive credentials altogether.

4)VULNERABILITY NAME:- HSTS Missing From HTTPS Server (RFC 6797)

- **CWE:-523 ect.**

- **OWASP CATEGORY:-A08:2021-SOFTWARE AND DATA INTEGRITY FAILURES.**

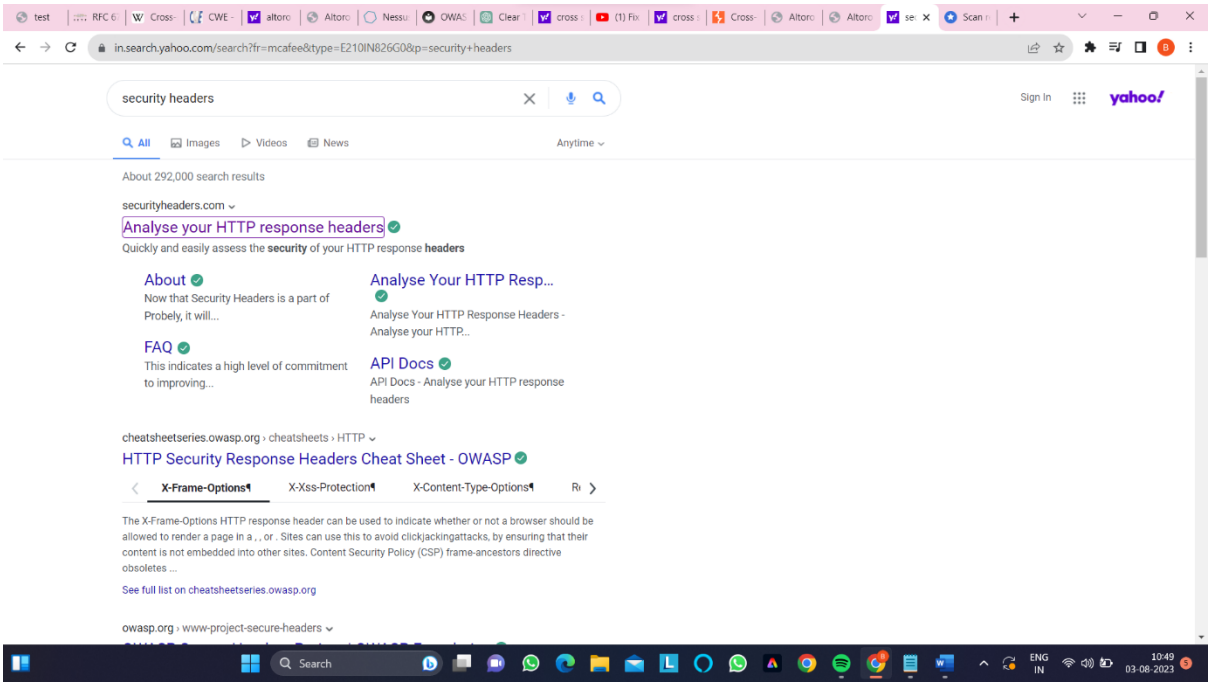
- **DESCRIPTION:-** The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections

- **BUSSINESS IMPACT:-**. Users are becoming increasingly security-conscious. If they notice that a website is not utilizing HSTS, they might perceive the site as less secure and trustworthy, leading to a potential loss of user trust and confidence in your business.
- A security breach resulting from a lack of HSTS can tarnish your business's reputation. News of data breaches or security vulnerabilities can spread quickly, damaging your brand image and potentially leading to reduced customer loyalty

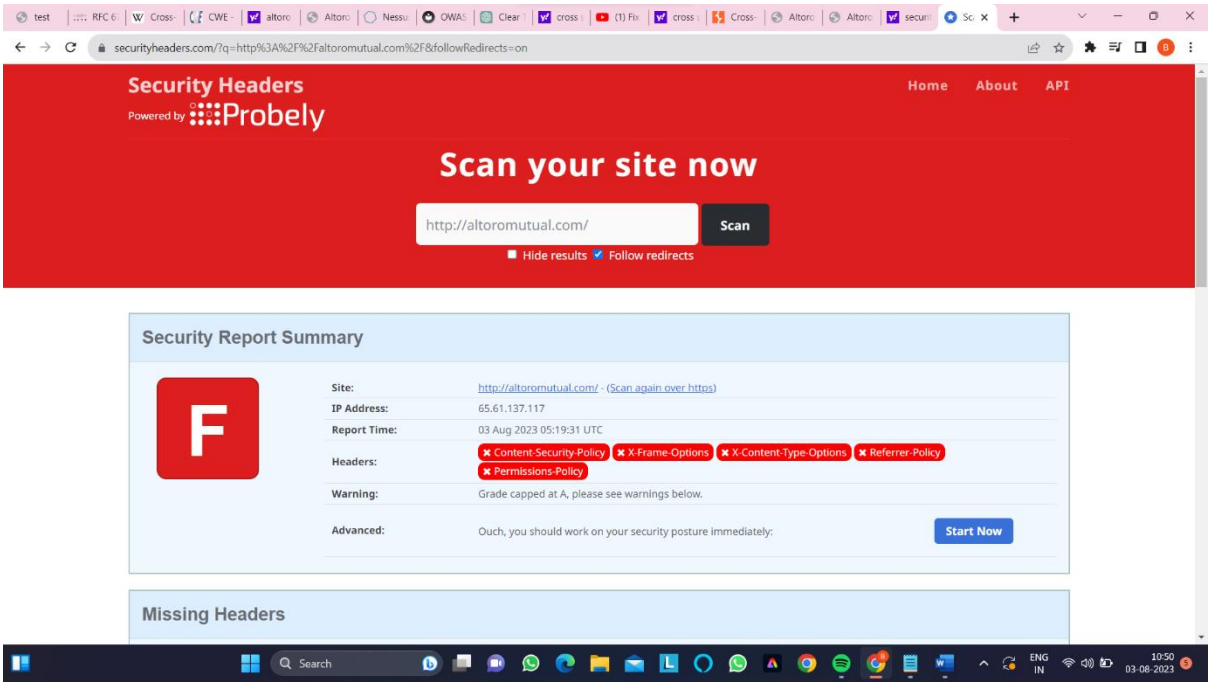
- **VULNERABILITY PATH:- http://altoromutual.com/**

- **STEPS TO REPRODUCE:-**

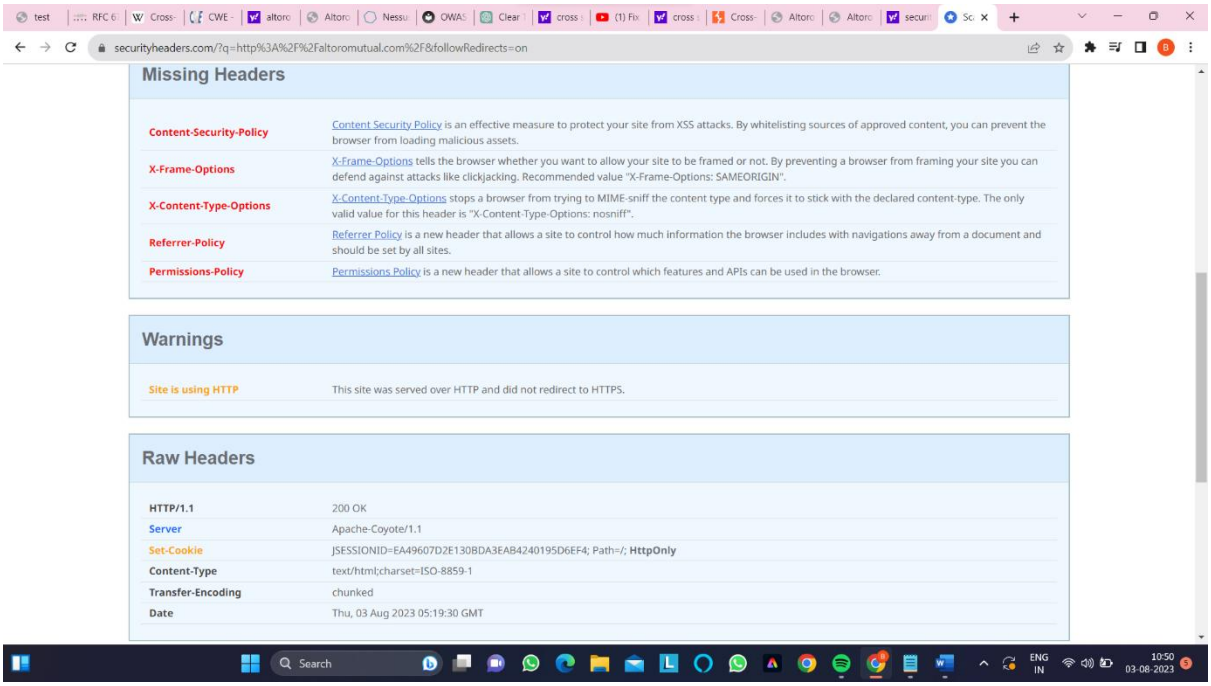
Step 1:-open any search engine and search for security headers



Step 2:-type the website name and then click go.



- **Step 3:- In the below figure we see the missing headers in the website**



- **REMMIDES:-** The primary remedy is to implement HSTS headers on your HTTPS server. This involves configuring your web server to include the "Strict-Transport-Security" HTTP response header. This header informs web browsers that your site should only be accessed via HTTPS for a specified duration. This can be done by adding a line similar to the following in your web server configuration:

- Strict-Transport-Security: max-age=31536000; includeSubDomains

- If your website uses subdomains, consider including the includeSubDomains directive in the HSTS header. This extends the HSTS protection to all subdomains as well, enhancing overall security.

5)VULNERABILITY NAME:- Web Server Allows Password Auto-Completion

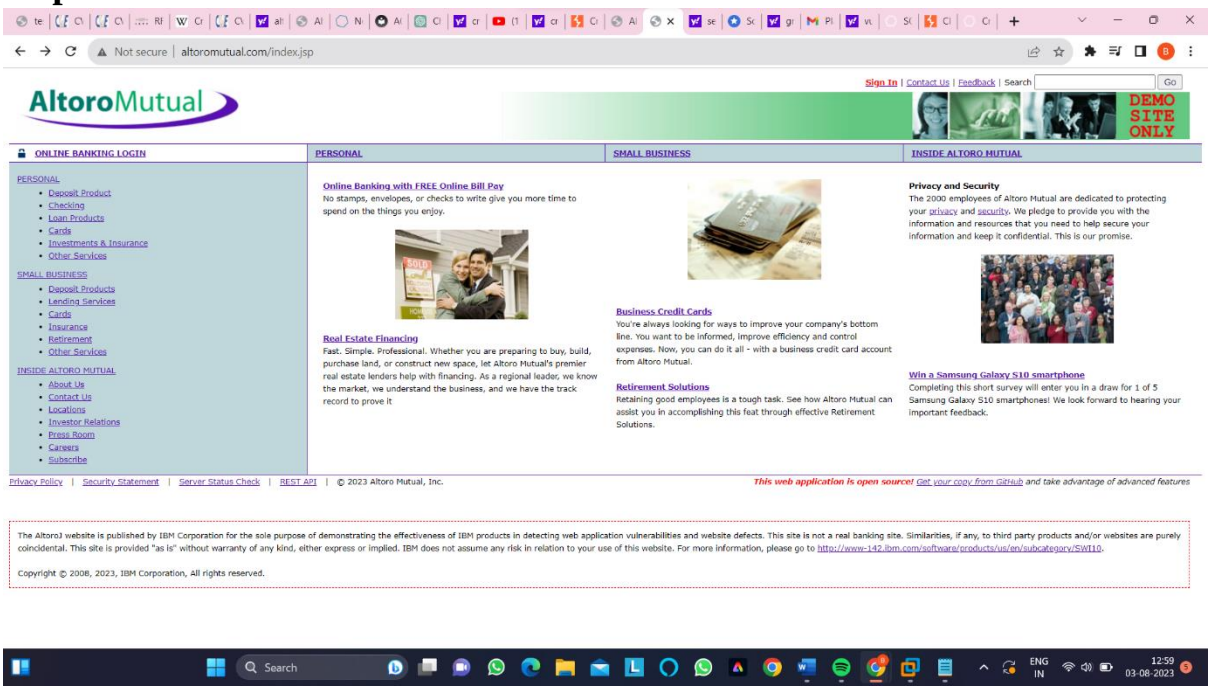
- **CWE:-200 ect.**
- **OWASP CATEGORY:-A03:2017-SENSITIVE DATA EXPOSURE**
- **DESCRIPTION:-** The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.
- While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.
- **BUSSINESS IMPACT:-** Many security standards and regulations (such as GDPR) require businesses to implement appropriate security measures to protect user data. Allowing password auto-completion might be seen as inadequate security practice and lead to non-compliance.
- Compromised accounts resulting from password auto-completion can contribute to data breaches. Attackers can exploit these vulnerabilities to steal personal information, financial details, and potentially engage in identity theft.

VULNERABILITY PATH:- **http://altoromutual.com/bank/main.jsp**

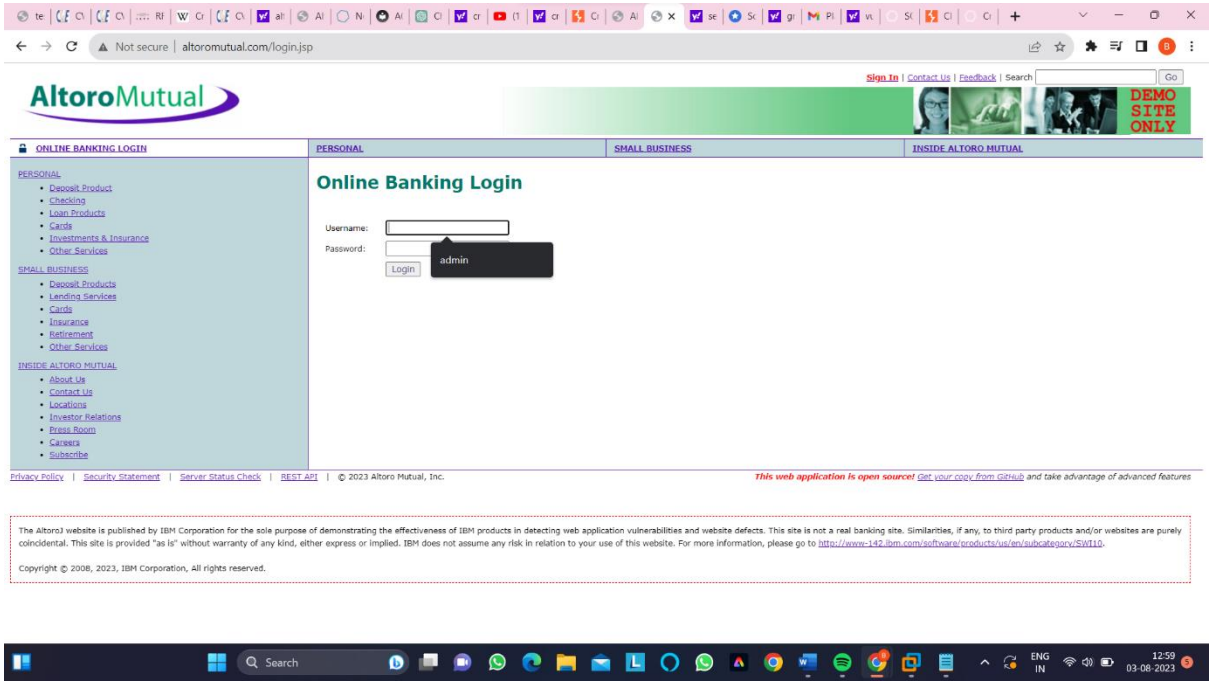
- **VULNERABILITY PARAMETERS:-**

- **STEPS TO REPRODUCE:-**

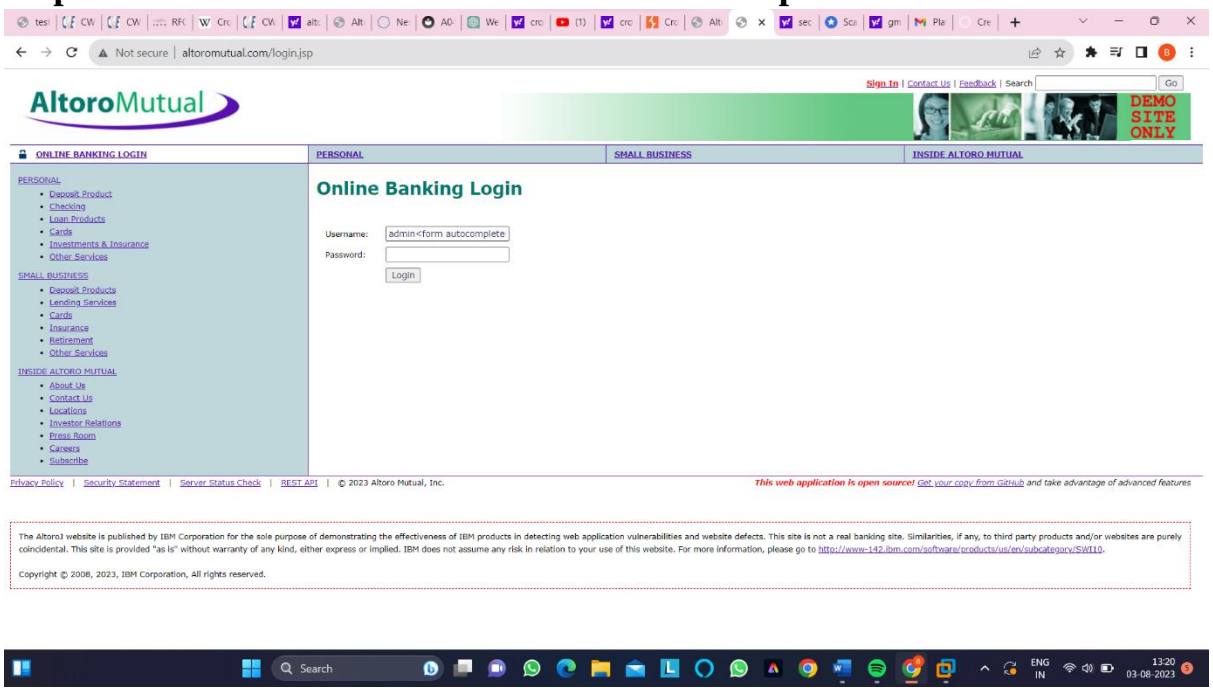
Step 1:- Access the website altoro mutual.com



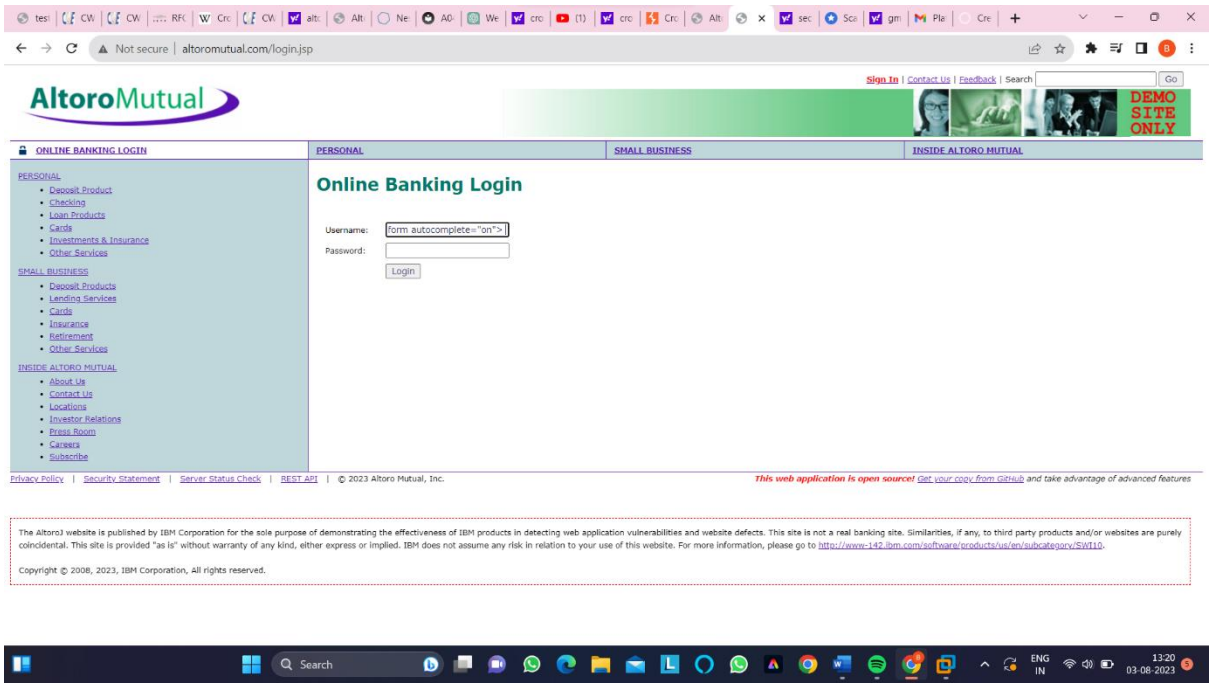
Step 2:-As we can see that the user field is showing autocomplete activity



Step 3:-IN the user field we can see that autocomplete is enabled



Step 4:-we see autocomplete field is in active state.



- **REMMIDES:-** Explicitly disable password auto-completion by adding the autocomplete="off" attribute to the password input fields in your HTML forms. This will instruct browsers not to suggest or remember passwords for these fields.

- Use CSS to style password input fields with the input[type="password"] selector to prevent auto-completion suggestions. This can act as an additional layer of prevention

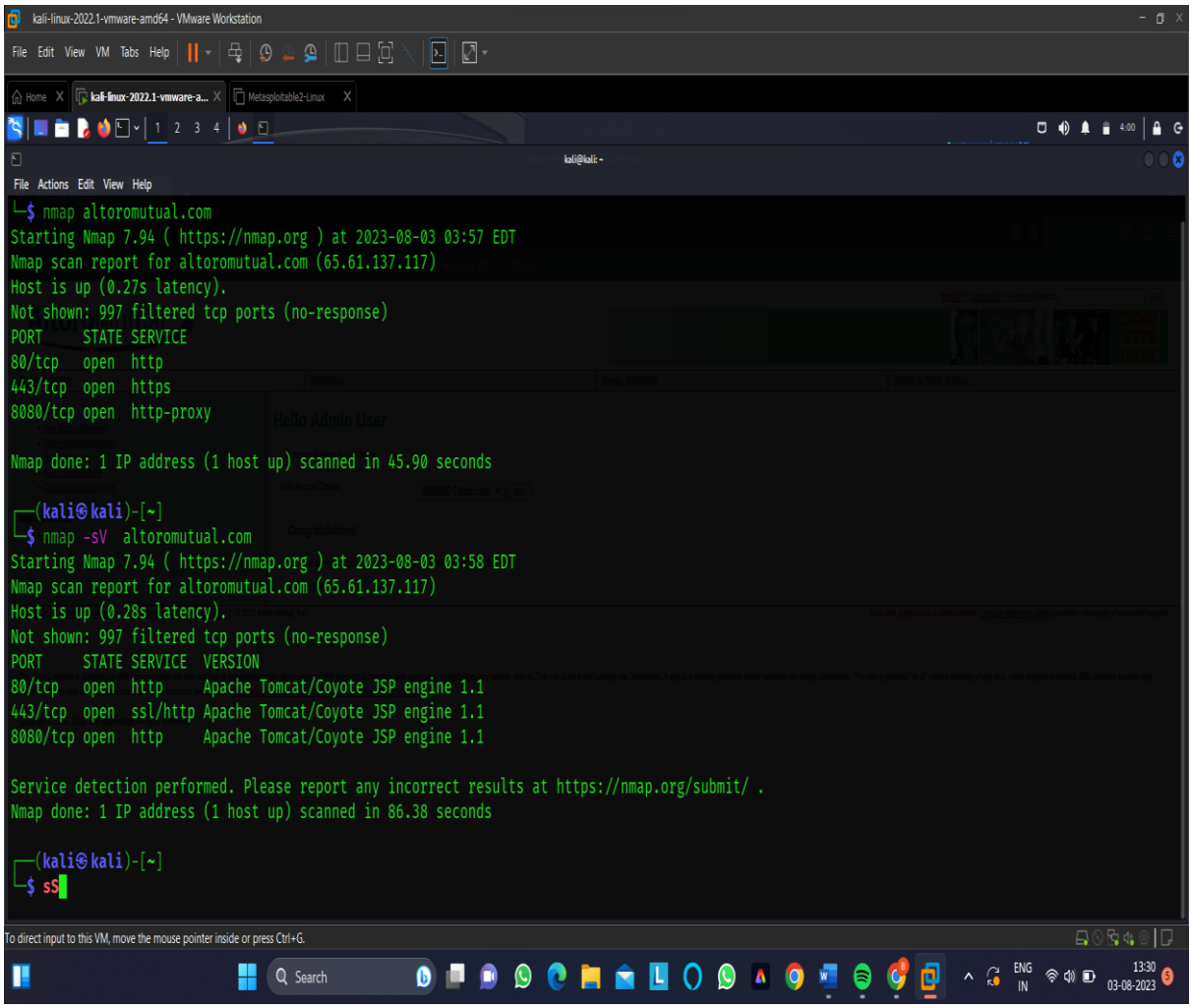
- Conduct regular security audits of your web application to identify any potential vulnerabilities, including those related to password handling and auto-completion.

6)VULNERABILITY NAME:- HTTP Server Type and Version

- **CWE:-444 ect.**
- **OWASP CATEGORY:-A05:2021-SECURITY MISCONFIGURATION**
- **DESCRIPTION:-** Identifying the HTTP server type and version refers to the process of determining the software and version number of the web server that is hosting a particular website or web application. This information can provide insights into the technologies being used, which can be useful for security assessment, compatibility checks, and understanding the server's capabilities
- **BUSSINESS IMPACT:-** If cybercriminals know the exact server type and version being used, they can focus their efforts on exploiting known vulnerabilities associated with that specific version. This can lead to unauthorized access, data breaches, and disruption of services.
- Some businesses might rely on the obscurity of server software to add an extra layer of security. Exposing server type and version removes this obscurity and forces businesses to rely more heavily on other security measures.

STEPS TO REPRODUCE:-

Step 1:-Use nmap to scan the website and use command as nmap -sV altoromutual.com to get server type.



Step 2:-we can see that the web server tpye is apache-coyote/1.1

altoromutual.com (tcp/443/www)

```
The remote web server type is :

Apache-Coyote/1.1
```

altoromutual.com (tcp/8080/www)

```
The remote web server type is :

Apache-Coyote/1.1
```

- **REMMIDES:-** Implement server hardening practices to secure your web server configuration and reduce its attack surface. Remove unnecessary modules and features that might expose server information.
- Configure your web server to disable or modify the server signature in response headers. This can prevent the server type and version from being easily identified by attackers.

7)VULNERABILITY NAME:- CGI Generic Tests Timeout

- **CWE:-287 ect.**

- **OWASP CATEGORY:-**A07:2021-IDENTIFICATION AND AUTHENTICATION FAILURES.

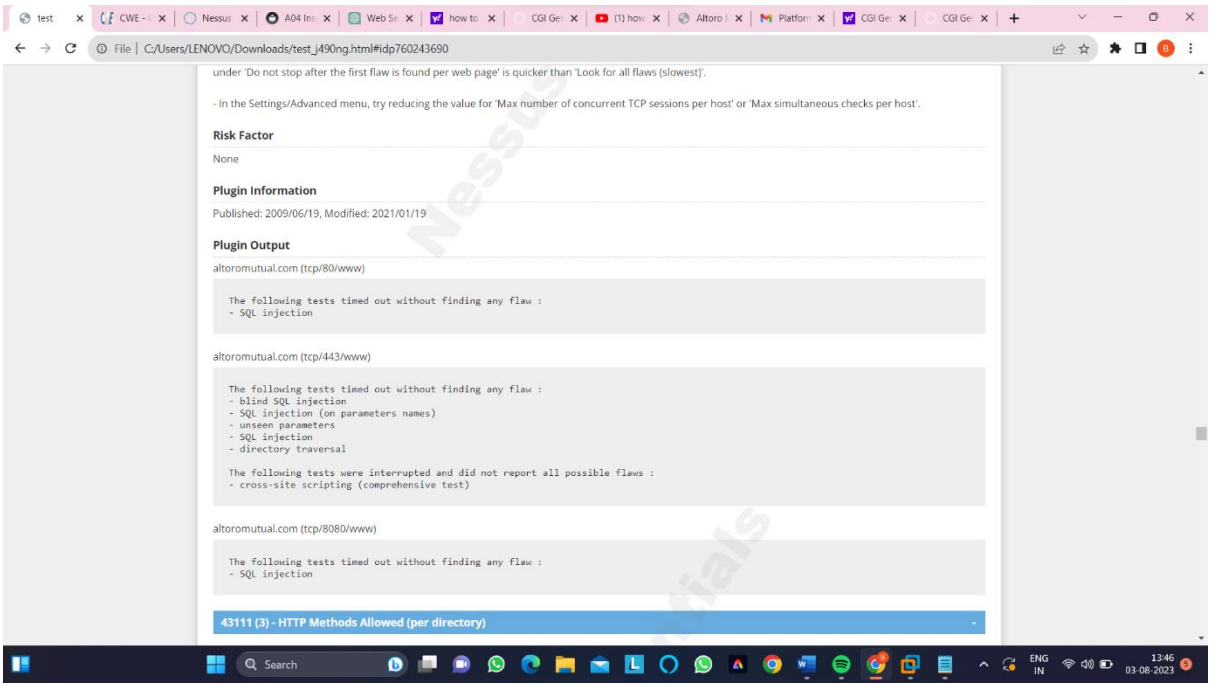
- **DESCRIPTION:-** CGI (Common Gateway Interface) Generic Tests Timeout refers to a configuration setting and a testing scenario used to assess the performance and security of CGI scripts on a web server. CGI is a standard protocol that allows web servers to execute external programs or scripts, often used to generate dynamic web content. The "CGI Generic Tests Timeout" scenario is typically employed as part of security assessments, penetration testing, or performance testing for web applications.

- Some generic CGI tests ran out of time during the scan. The results may be incomplete.

- **BUSSINESS IMPACT:-** Slow or timed-out CGI scripts can lead to a poor user experience on your website or web application. Visitors may become frustrated and leave, leading to decreased engagement and potential loss of customers.
- If your website's functionality heavily relies on CGI scripts, timeouts can prevent users from accessing critical features. This can result in customer dissatisfaction and a negative perception of your brand.

- **STEPS TO REPRODUCE:-**

Step 1:-From the below repor we can see that tests are not allowed to find any flaws .



- **REMMIDES:-** Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :
'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters

(slow)'.

- 'Stop after one flaw is found per web server (fastest)' under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Thank you!!!!!