VULNERABILITY ASSESSMENT REP

Target Website
http://demo.testfire.net

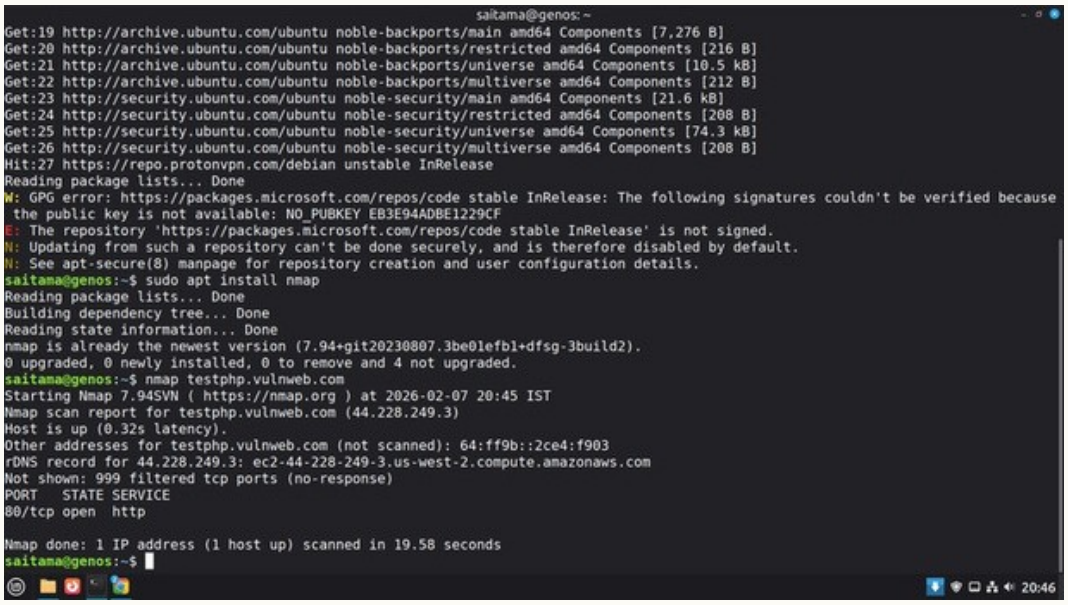
Prepared By
Aryan Sanjay Salunke
Purpose
Educational Security Assessment

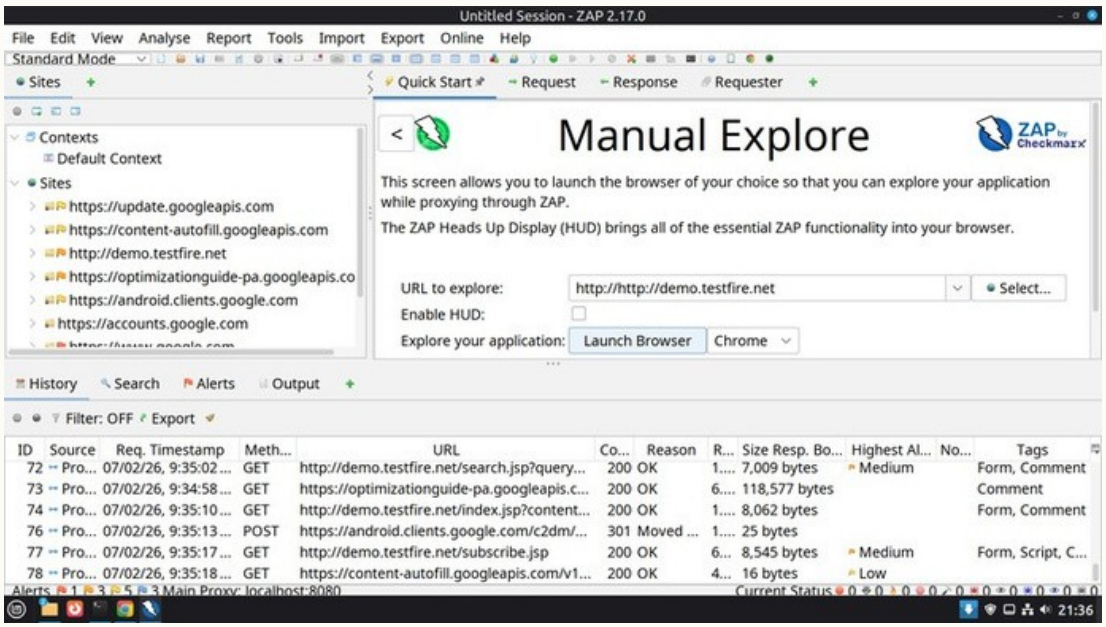
1. Introduction
This report presents the results of a basic vulnerability assessment conducted on the Altoro Mutual demo website (http://demo.testfire.net). The assessment was performed for educational purposes to identify common web security issues using passive analysis techniques.

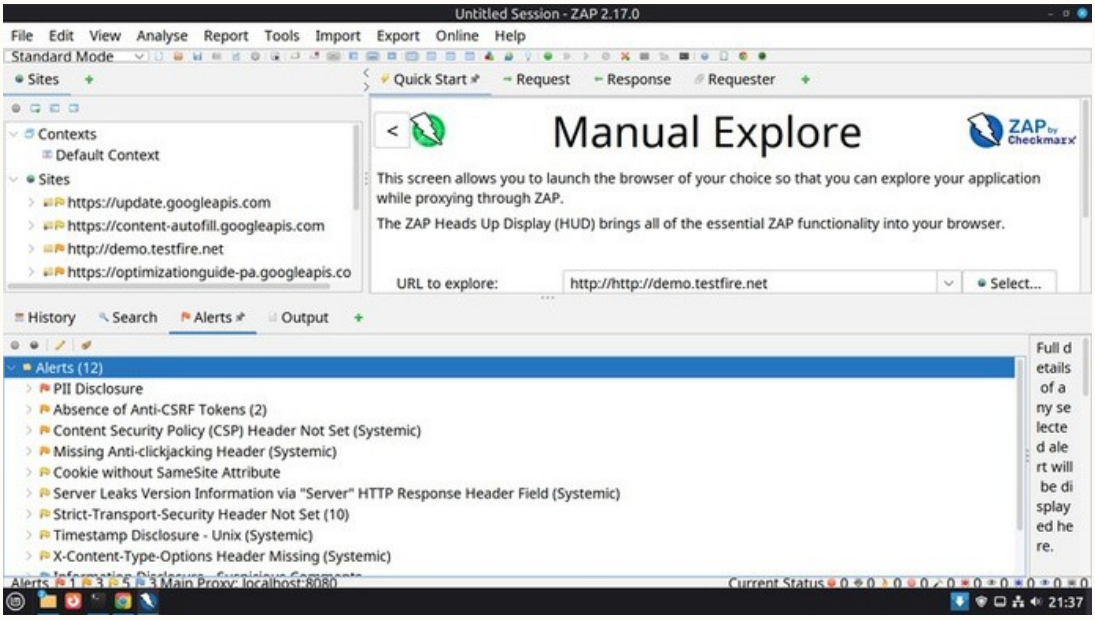
2. Scope of Assessment
The scope of this assessment was limited to passive observation of the target website. No active attacks, exploitation techniques, or intrusive testing methods were performed. The goal was to identify visible security misconfigurations and common vulnerabilities without causing any harm.

3. Tools Used
Nmap – Used to identify open ports and basic network information
OWASP ZAP (Passive Mode) – Used to identify common web security issues
Web Browser – Used for manual navigation and observation

4. Vulnerability Identified
4.1 High-Risk Security Alert (Red Alert)
Risk Level: High
Tool: OWASP ZAP
Description:
OWASP ZAP identified a high-risk security vulnerability during the passive scan of the target website. This alert indicates a serious security weakness that could potentially be exploited by an attacker to compromise the confidentiality, integrity, or availability of the application.
Impact:
If exploited, this vulnerability may allow attackers to perform unauthorized actions, access sensitive information, or disrupt normal website functionality.
Recommendation:
It is strongly recommended to investigate this vulnerability in detail and apply appropriate security controls. This may include implementing secure coding practices, updating server configurations, and applying relevant security patches to mitigate the risk.


saitama@genos:~
Get:19 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,276 B]
Get:20 http://archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:21 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [10.5 kB]
Get:22 http://archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:23 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.6 kB]
Get:24 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [208 B]
Get:25 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [74.3 kB]
Get:26 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Hit:27 https://repo.protonvpn.com/debian unstable InRelease
Reading package lists... Done
W: GPG error: https://packages.microsoft.com/repos/code stable InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY EB3E94ADBE1229CF
E: The repository 'https://packages.microsoft.com/repos/code stable InRelease' is not signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
saitama@genos:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
saitama@genos:~$ nmap testphp.vulnweb.com
Starting Nmap 7.94SVN (https://nmap.org) at 2026-02-07 20:45 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.32s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 19.58 seconds
saitama@genos:~$
20:46


Untitled Session - ZAP 2.17.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://update.googleapis.com
https://content-autofill.googleapis.com
http://demo.testfire.net
https://optimizationguide-pa.googleapis.co
https://android.clients.google.com
https://accounts.google.com
Manual Explore
ZAP by Checkmarx
This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.
The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.
URL to explore:
http://http://demo.testfire.net
Select...
Enable HUD:
Explore your application:
Launch Browser
Chrome
History
Search
Alerts
Output
Filter: OFF
Export
ID Source Req. Timestamp Meth... URL Co... Reason R... Size Resp. Bo... Highest Al... No... Tags
72 Pro... 07/02/26, 9:35:02 ... GET http://demo.testfire.net/search.jsp?query... 200 OK 1.... 7,009 bytes Medium Form, Comment
73 Pro... 07/02/26, 9:34:58 ... GET https://optimizationguide-pa.googleapis.c... 200 OK 6.... 118,577 bytes Comment
74 Pro... 07/02/26, 9:35:10 ... GET http://demo.testfire.net/index.jsp?content... 200 OK 1.... 8,062 bytes Form, Comment
76 Pro... 07/02/26, 9:35:13 ... POST https://android.clients.google.com/c2dm/... 301 Moved ... 1.... 25 bytes
77 Pro... 07/02/26, 9:35:17 ... GET http://demo.testfire.net/subscribe.jsp 200 OK 6... 8,545 bytes Medium Form, Script, C...
78 Pro... 07/02/26, 9:35:18 ... GET https://content-autofill.googleapis.com/v1... 200 OK 4... 16 bytes Low
Alerts 1 3 5 3 Main Proxy: localhost:8080
Current Status
21:36


Untitled Session - ZAP 2.17.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://update.googleapis.com
https://content-autofill.googleapis.com
http://demo.testfire.net
https://optimizationguide-pa.googleapis.co
Manual Explore
ZAP by Checkmarx
This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.
The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.
URL to explore:
http://http://demo.testfire.net
Select...
History
Search
Alerts
Output
Alerts (12)
PII Disclosure
Absence of Anti-CSRF Tokens (2)
Content Security Policy (CSP) Header Not Set (Systemic)
Missing Anti-clickjacking Header (Systemic)
Cookie without SameSite Attribute
Server Leaks Version Information via "Server" HTTP Response Header Field (Systemic)
Strict-Transport-Security Header Not Set (10)
Timestamp Disclosure - Unix (Systemic)
X-Content-Type-Options Header Missing (Systemic)
Full details of any selected alert will be displayed here.
Alerts 1 3 5 3 Main Proxy: localhost:8080
Current Status
21:37

4.1 Website Uses HTTP Instead of HTTPS

Risk Level: Medium

Description:

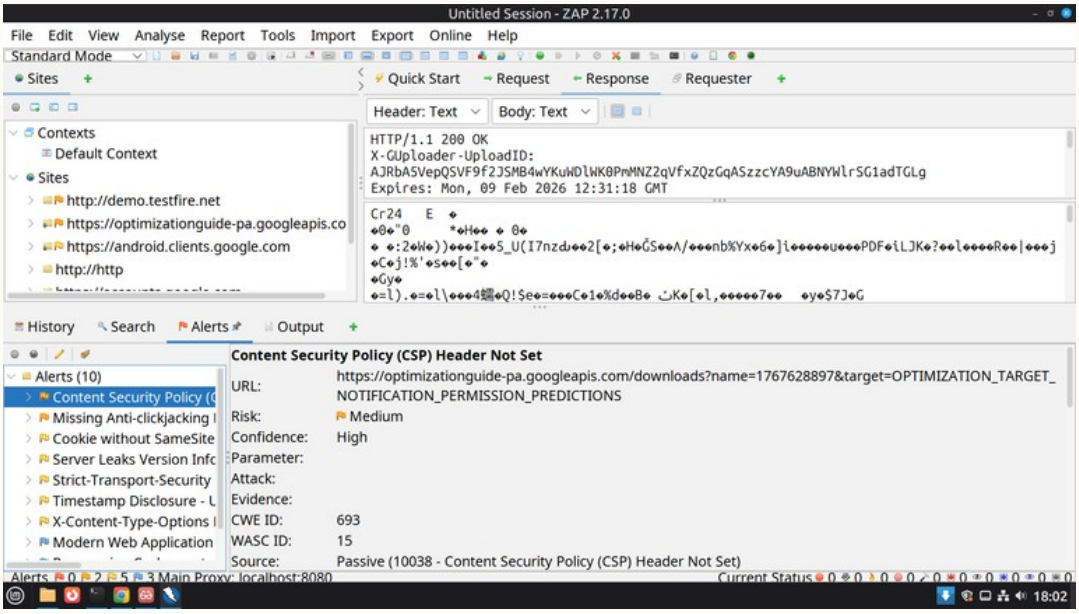
The target website uses HTTP instead of HTTPS. This means that data transmitted between the user and the server is not encrypted and can potentially be intercepted on unsecured or public networks.

Impact:

Sensitive information such as login credentials may be exposed to attackers through network-based attacks.

Recommendation:

Enable HTTPS by implementing an SSL/TLS certificate to ensure encrypted communication between users and the website.



4.2 Missing X-Frame-Options Header

Risk Level: Low

Description:

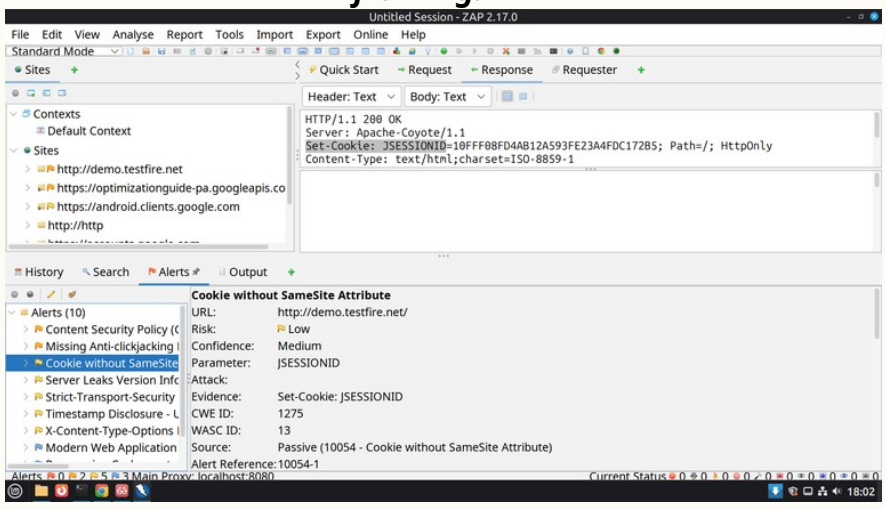
The X-Frame-Options security header is missing from the website's HTTP responses. This header helps protect users against clickjacking attacks.

Impact:

Attackers could embed the website within malicious frames and trick users into performing unintended actions.

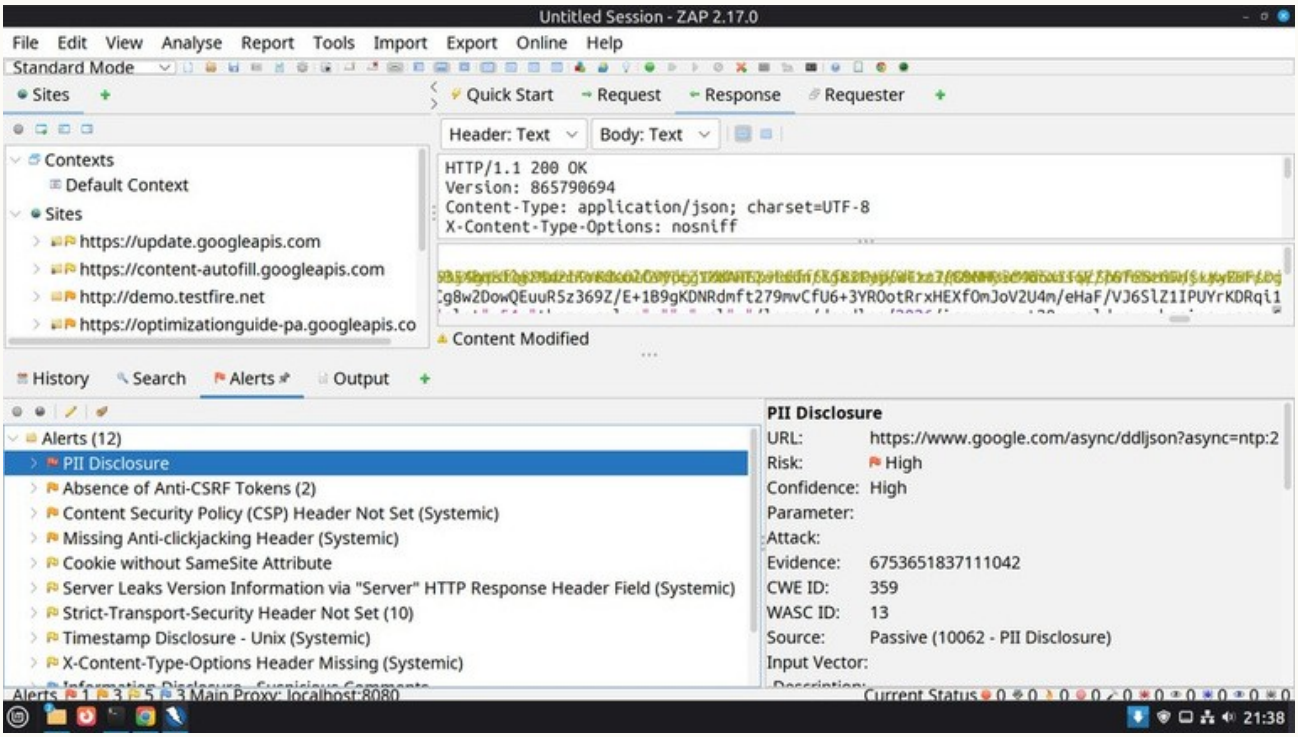
Recommendation:

Configure the server to include the X-Frame-Options header to prevent unauthorized framing.



5. Evidence

Figure 1: OWASP ZAP high-risk (red) alert detected during passive scan



6. Conclusion

The vulnerability assessment identified a high-risk security issue on the target website. This finding highlights the importance of conducting regular security assessments and addressing critical vulnerabilities promptly. Even a single high-risk issue can significantly impact the overall security of a web application.

7. Disclaimer

This assessment was conducted on the Altoro Mutual demo website (http://demo.testfire.net), which is a deliberately vulnerable application provided for security training and educational purposes only. No real-world systems were tested during this assessment.