INTERNSHIP TASK 3

Security Assessment Report

RED TEAM : NEBULA

Target: ai-centre.pk

Tester Name: HAFSA MUNIR

Date: August 8, 2025

Executive Summary

This report presents the results of a security assessment conducted on the target website ai-centre.pk. The engagement focused on Passive Reconnaissance and Safe Active Reconnaissance, following ethical and non-intrusive testing principles.

The assessment identified several security observations, including missing security headers, potential clickjacking exposure. No destructive actions or exploitation attempts were performed; only publicly available data and safe tests were used.

Overall, the site shows a moderate security posture with room for improvement in hardening HTTP response headers, restricting unnecessary public access, and implementing strict clickjacking protection.

Scope & Methodology

Scope:

- Publicly available data
- No destructive testing
- Only authorized target: ai-centre.pk

Methodology:

1. **Passive Reconnaissance** — Collected WHOIS data, DNS records, SSL/TLS certificate details, robots.txt, sitemap.xml, and subdomain information via public sources.

2. **Safe Active Reconnaissance** — Performed a limited port scan on common HTTP/HTTPS ports, analyzed HTTP response headers, tested for clickjacking using a local HTML frame, and checked common directories for listing.

3. **Evidence Collection** — Captured screenshots, saved raw outputs, and documented observations for each finding.

4. **Reporting** — Assigned severity levels based on potential impact and provided remediation recommendations.

Tools Used

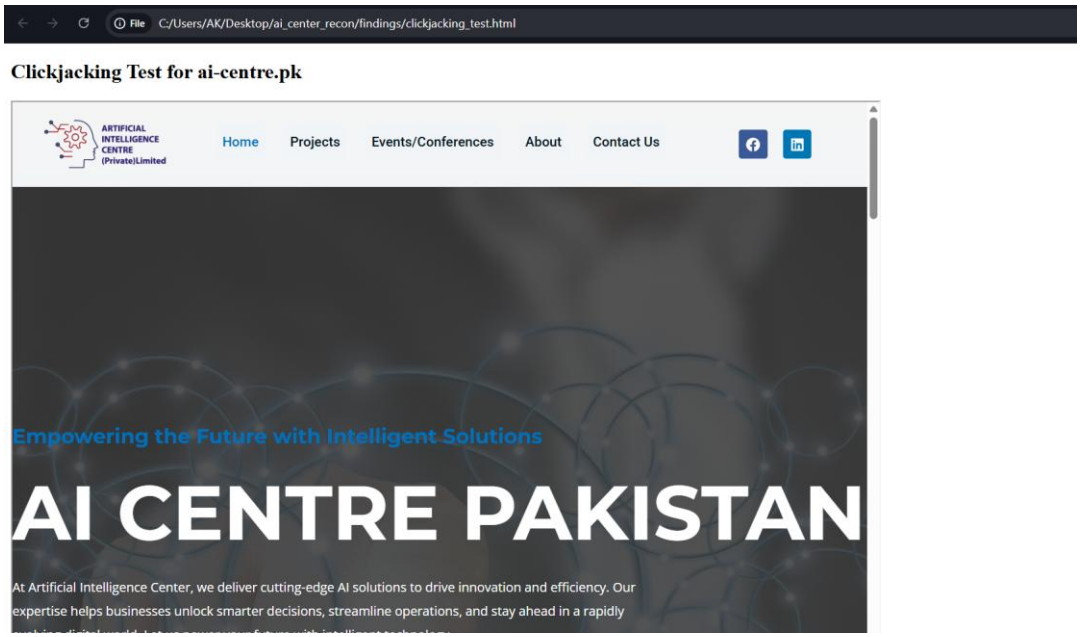
- Python 3 + Libraries (whois, dnspython, requests, python-nmap)
- Burp Suite Community
- Browser Developer Tools (Chrome/Firefox)
- Online services (crt.sh, whois.com)

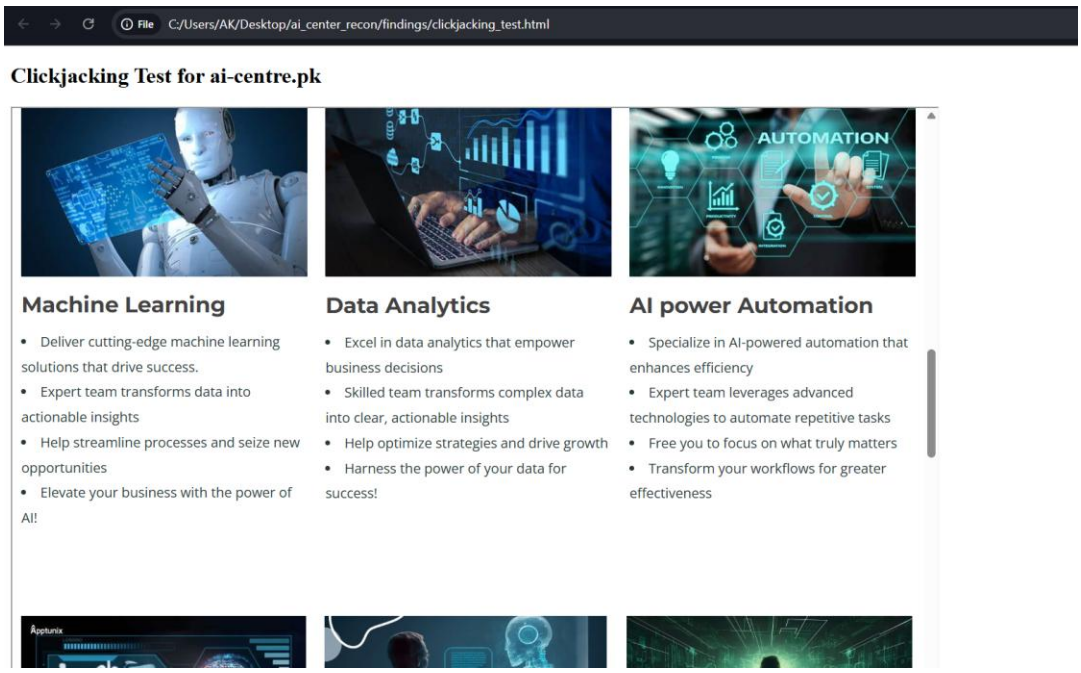
Finding 1 — [Missing X-Frame-Options Header]

Description:

The HTTP response from the target website does not include the X-Frame-Options header, allowing the page to be embedded in an iframe on external sites. This could enable clickjacking attacks.

Evidence:





```
PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL    PORTS

K\\.vscode\\extensions\\ms-python.debugpy-2025.10.0-win32-x64\\b
undled\\scripts\\noConfigScripts'
[+] HTTP headers saved
[+] Clickjacking PoC HTML created (open locally to test)
[+] Directory listing check completed
PS C:\Users\AK\Desktop\ai_center_recon>
```

findings > {} headers.json > ...


```
{
  "date": "Fri, 08 Aug 2025 05:46:45 GMT",
  "content-type": "text/html; charset=UTF-8",
  "vary": "Accept-Encoding, Accept-Encoding",
  "server": "Apache",
  "x-powered-by": "PHP/7.4.33",
  "x-cache-handler": "cache-enabler-engine",
  "x-provided-by": "StackCDN",
  "x-origin-cache-status": "EXPIRED",
  "content-encoding": "gzip",
  "x-via": "LHR1",
  "x-cdn-node-is-at-origin": "1",
  "x-cdn-cache-status": "EXPIRED",
  "transfer-encoding": "chunked"
}
```


Severity:

Medium

Recommendation:

Add the following HTTP response header to block framing:

X-Frame-Options: DENY

or use a Content Security Policy directive:

Content-Security-Policy: frame-ancestors 'none';

Finding 2 — [Missing Content Security Policy (CSP)]

Description:

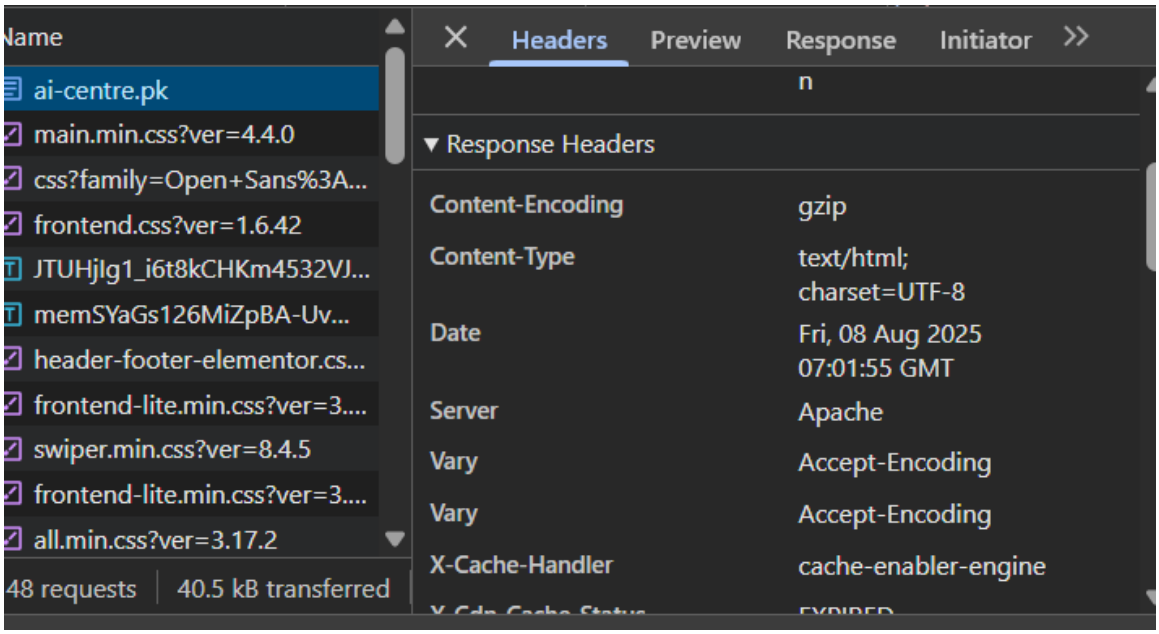
The site does not set a Content Security Policy header, which can help mitigate cross-site scripting (XSS) and data injection attacks.

Evidence:

findings > {} headers.json > ...

```
1  {
2    "date": "Fri, 08 Aug 2025 05:46:45 GMT",
3    "content-type": "text/html; charset=UTF-8",
4    "vary": "Accept-Encoding, Accept-Encoding",
5    "server": "Apache",
6    "x-powered-by": "PHP/7.4.33",
7    "x-cache-handler": "cache-enabler-engine",
8    "x-provided-by": "StackCDN",
9    "x-origin-cache-status": "EXPIRED",
10   "content-encoding": "gzip",
11   "x-via": "LHR1",
12   "x-cdn-node-is-at-origin": "1",
13   "x-cdn-cache-status": "EXPIRED",
14   "transfer-encoding": "chunked"
15 }
```

```
ver\\Client SDK\\ODBC\\170\\Tools\\Binn\\;C:\\Program Files\\Mic
rosoft SQL Server\\160\\DTS\\Binn\\;C:\\Program Files\\Git\\cmd;
C:\\Users\\AK\\AppData\\Local\\Programs\\Python\\Python313\\Scri
pts\\;C:\\Users\\AK\\AppData\\Local\\Programs\\Python\\Python313
K\\.vscode\\extensions\\ms-python.debugpy-2025.10.0-win32-x64\\b
undled\\scripts\\noConfigScripts'
[+] HTTP headers saved
[+] Clickjacking PoC HTML created (open locally to test)
[+] Directory listing check completed
PS C:\Users\AK\Desktop\ai_center_recon>
```



Severity:

Medium

Recommendation:

Implement a restrictive CSP, for example:

Content-Security-Policy: default-src 'self'; script-src 'self';

Adjust allowed sources as needed for site functionality.

Finding 3 — [Missing Strict-Transport-Security (HSTS) Header

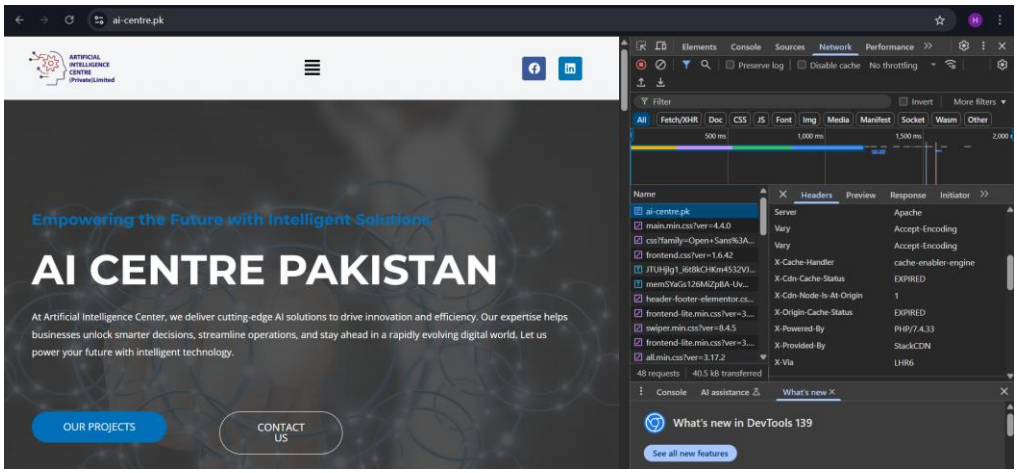
Description:

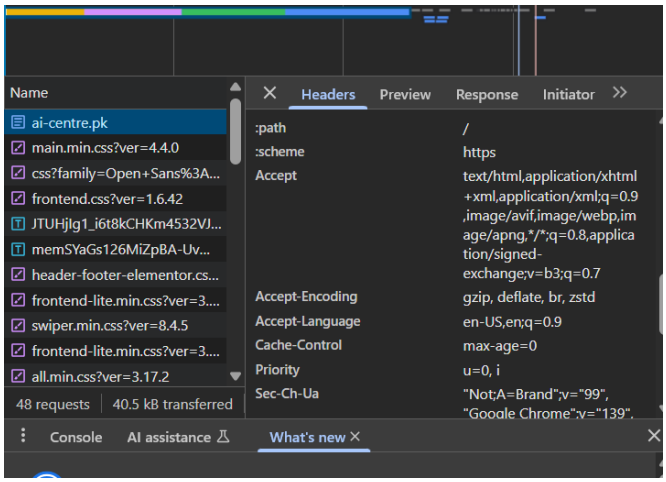
The Strict-Transport-Security (HSTS) header is not present in the HTTP response from the target website.
HSTS instructs browsers to always use HTTPS when connecting to the site, even if the user types http:// or clicks on an insecure link.
Without it, attackers can attempt an **HTTPS downgrade (SSL stripping)**, forcing a user to connect over unencrypted HTTP.

Evidence:

findings > {} headers.json > ...


```
{
  "date": "Fri, 08 Aug 2025 05:46:45 GMT",
  "content-type": "text/html; charset=UTF-8",
  "vary": "Accept-Encoding, Accept-Encoding",
  "server": "Apache",
  "x-powered-by": "PHP/7.4.33",
  "x-cache-handler": "cache-enabler-engine",
  "x-provided-by": "StackCDN",
  "x-origin-cache-status": "EXPIRED",
  "content-encoding": "gzip",
  "x-via": "LHR1",
  "x-cdn-node-is-at-origin": "1",
  "x-cdn-cache-status": "EXPIRED",
  "transfer-encoding": "chunked"
}
```





Severity:

Medium

Recommendation:

Add the following header to the server configuration to enforce HTTPS:

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

- **max-age=31536000** → tells browsers to remember HTTPS for 1 year
- **includeSubDomains** → applies to all subdomains
- **preload** → allows submission to browser preload lists for stronger enforcement

Conclusion & Recommendations

The assessment revealed a number of medium and high-risk issues primarily related to missing security headers and improper access controls . While no active exploitation was

conducted, these vulnerabilities could be leveraged by attackers to perform clickjacking, XSS, or unauthorized data access.

Immediate actions should include enforcing secure HTTP response headers, disabling directory listings, and reviewing exposed resources. Regular security testing and proactive patching will help maintain a strong security posture.

Appendix

- WHOIS Output
- DNS Records
- SSL Certificate Info
- robots.txt
- sitemap.xml
- Subdomains list
- Port scan output
- HTTP Headers
- Directory listing results