RajCOMP Info Services Ltd
(formerly RajCOMP)
(A Government of Rajasthan Undertaking)
RISL

Web Application Security Assessment Report of RajCOMP Info Services Ltd-Raj Attendance System

Confidential: V 1.0
Technical Report
Purchase Order No: F3.3(508)/RISL/Pur/2024/3737
Dates of Audit: 20th March 2025 to 24th March 2025
Date of Report: 26th March 2025

Business With Wisdom
...Growth With Assurance

Audit Conducted By:

Nikhitha L (MSC, CEH)
Pooja H S (B.E, CEH)

Reviewed By:

Mr. Dinesh Shastri, ISO 27001LA, CISA, CHFI, ITIL, CEH

Corporate Office #
Digital Age Strategies Pvt. Ltd.
28, “Om Arcade”, 2nd& 3rdFloors,
Thimmappa Reddy Layout,
Hulimavu, Bannerghatta Road, Bangalore - 560076
Ph: +91-080-41512259, 41218560, 49568066
Mobile: 9448088666/9448055711
Email: - audit@digitalage.co.in

Audit Information	
Report Release Date	26th March 2025
Type of Audit	Web Application Penetration Testing
Type of Audit Report	Initial Audit
Audit Period	20th March 2025 to 24th March 2025

Document Control	
Document Title	Web Application Security Assessment Report of RajCOMP Info Services Ltd-Medical Education Portal
Document ID	DigAge:RISL:0538:2024-25
Document Version	V1.0
Prepared by	Pooja H S
Reviewed by	Sai Tharun
Approved by	Mr. Dinesh Shastri
Released by	Nikhitha L

Document Change History

Version	Date	Remarks / Reason of change
1.0	26th March 2025	Initial Audit

Document Distribution List

Name	Organization	Designation	Email Id
Vinita Shrivastava	RajCOMP Info Services Ltd	SA (Joint Director)	Vinitas.doit@rajasthan.gov.in

Table of Contents

A. Introduction....4
B. Engagement scope: 4
C. Auditing team: 5
D. Audit Activities and Timelines: 5
E. Audit Methodology and Criteria / Standard referred for audit....5
a. Web-Application Security Assessment....5
F. Auditing Tools: 6
G. Type of Test: 6
H. Host Details....6
I. Vulnerability Summary....7
OWASP TOP 10 – 2021 for Web Application Penetration Testing....7
J. Risk Categorization....8
K. Severity wise vulnerability distribution....9
L. Executive Summary....10
M. Audit Findings....11
1.Vulnerable to Buffer overflow attacks....11
2. Clickjacking....12
3. HTTP Strict Transport Security (HSTS) Policy Not Enabled....13
4. Input Fields are not Filtered....14
5. Broken Authentication....15
6. Sensitive Information Submitted through GET method....17
7. Content security policy Header Missing....18
8. Missing X-Content-Type-Options....19
9. Missing X-XSS-Protection....19
10. Improper Implementation of Cache-Control....20
N. Disclaimer....21
O. Conclusion....21

A. Introduction

DIGITAL AGE is dedicated to providing its customers with excellent services in the area of Information Security for robust security architecture.

DIGITAL AGE has been empanelled as IT Security Audit Organization by the CERT-In, Ministry of Information Technology, Govt. of India and the CCA, Ministry of Information Technology, Govt. of India.

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the recent Information Technology amendment act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Such other functions relating to cyber security as may be prescribed

B. Engagement scope:

As per the directions from the RajCOMP Info Services Ltd vide mail dated 19th March 2025, we have conducted Cyber Security Assessment Audit

a. Web Application Penetration Testing

S. No	Asset Description	Application Name/ Application URL/ IP Address	Hash Value	Application Version
1	Web Application Penetration Testing	https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login	-	-

C. Auditing team:

S. No	Name	Designation	Email Id	Professional Qualifications/ Certifications	Whether the resource has been listed in the Snapshot information published on CERT-In's website
1.	Nikhitha L	VAPT Auditor	nikhitha@digitalage.co.in	Msc, CEH	No
2.	Pooja H S	VAPT Auditor	vapt@digitalage.co.in	BE, CEH	No

D. Audit Activities and Timelines:

As per the directions from the RajCOMP Info Services Ltd mail dated 19th March 2025, we have conducted Security Assessment on 20th March 2025 to 24th March 2025 Report prepared and submitted to RajCOMP Info Services Ltd on 26th March 2025.

E. Audit Methodology and Criteria / Standard referred for audit

a. Web-Application Security Assessment

Testing which is non-intrusive in nature was carried out on the Staging environment. We performed

- **Automated testing**
  In this step, we utilized a variety of tools to scan each Web Application for known vulnerabilities in a comprehensive and efficient manner.

- **Advanced manual testing**
  Manual testing was performed to identify security exposures and exploit findings discovered from automated scanning methods. The Digital Age team leveraged manual web application security testing experience and our understanding of weaknesses in common coding practices to identify security weaknesses in the designated web application.

- **Test Cases**
  Test cases or attacks performed for the web-application provided by RajCOMP Info Services Ltd. The test cases were derived from industry best practices benchmarks like OWASP-Top 10, SANS 25, WASP, OWASP-ASVS, WASC, OSSTMM, OWASP, PTES, ISSAF vulnerabilities best practices.

F. Auditing Tools:

S. No	Name of Tool/Software used	Version of the tool /Software used	Open Source/Licensed
1.	Burp Suite Pro	Version 2023	Licensed
2.	Kali Linux	-	Open Source
3.	Nmap	-	Open Source

G. Type of Test:

Grey Box Testing

The Assessment was entirely carried out with a Manual Grey Box Testing. Manual Testing approach eradicates false positives that common automated tools throw up. The site was Also Subjected to various other tests based on the OWASP Testing Guidelines including Parameter manipulation, cookie manipulation, Request Modification and Testing for the OWASP Top 10.

H. Host Details

The following table lists the URL in RajCOMP Info Services Ltd for security audit.

Sl. No.	URL
1.	https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login

I. Vulnerability Summary

This section presents the analysis of vulnerabilities found

OWASP TOP 10 – 2021 for Web Application Penetration Testing

Sl. No.	Top 10 OWASP Vulnerability	Vulnerability Findings
1.	Broken Access Control	1. Vulnerable to Buffer overflow Attacks
2.	Cryptographic Failures	Not Found
3.	Injection	Not Found
4.	Insecure Design	Not Found
5.	Security Misconfiguration	1. Clickjacking 2. HTTP Strict Transport Security(HSTS) Policy Not Enabled 3. Input Fields are not Filtered 4. Sensitive Information Submitted Through Get Method 5. Content Security Policy Header Missing 6. Improper Implementaion Of Cache-Control 7. Missing X-XSS-Protection 8. Missing X-Content-Type-Options
6.	Vulnerable and Outdated Components	Not Found
7.	Identification and Authentication Failures	1. Broken Authentication
8.	Software and Data Integrity Failures	Not Found
9.	Security Logging and Monitoring Failures	Not Found
10.	Server-Side Request Forgery	Not Found

J. Risk Categorization

The risk of an audit finding is determined by assessing the potential negative impact and the probability that it materialises. Audit findings are classified into three risk classifications. These risk categories assist management in identification, prioritisation, and implementation of audit recommendations. When the practice is normal as per the guidelines / best practices, the same has been classified as ‘LOW’.

The risk classifications are as under

High Risks

Non-adherence to Reserve Organization and Government Guidelines, Policies Approved by Board, ICT is not as per standard, high threat probabilities. These risks are so significant that Management should determine any exposure to date and without delay effect an agreed program for their immediate and permanent resolution to provide assurance that they will not recur in the future. These are weaknesses that has compromised control or security, and which should be addressed immediately.

Medium Risks

These risks are not material in the context of current levels of activity, but management should be aware of them and ensure they are resolved as soon as possible as they may become material if activities increase. An issue, which though not a direct threat to control or security, should be addressed in the interest of efficiency.

Low Risk

A weakness in the design and/or operation of a non-key process control. Ability to achieve process objectives is likely to be impacted. Corrective action is suggested to ensure controls are cost effective.

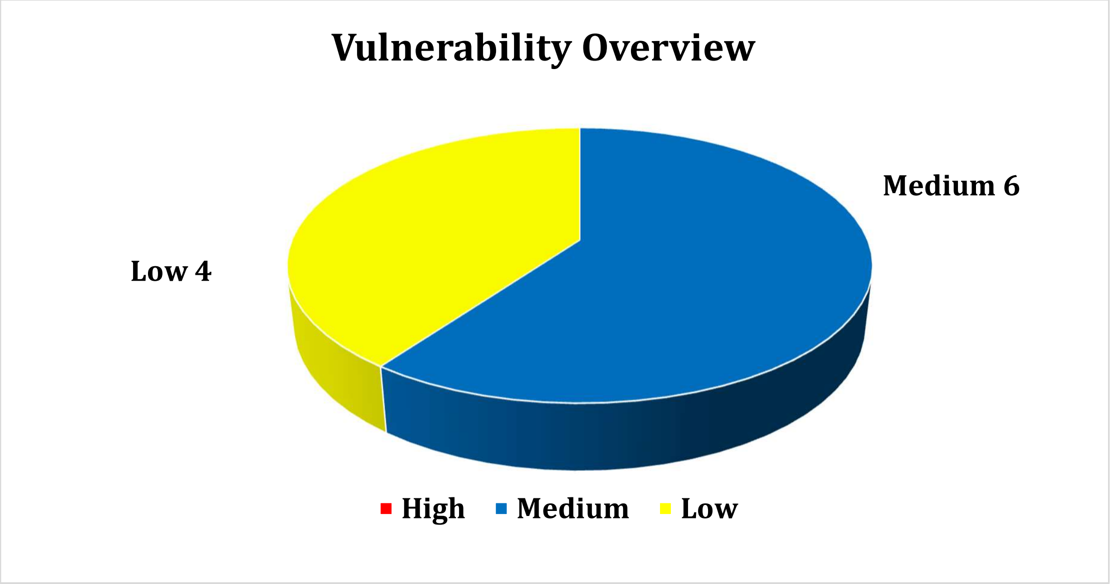
K. Severity wise vulnerability distribution

The following is the summary of the observations which need to be attended by the Organization.

Rating /Grading [As per Auditor's perception]:

Type of Audit	Reported Observations		
	High	Medium	Low
Web Application	00	06	04

Graph:



L. Executive Summary

The purpose of this section is to provide an overview of the key findings of the review. This section highlights the key observations and the distribution of observations basis risk rating and contains an overview of audit points observed across different applications. It should be noted that for a complete understanding of all the observations, it would be essential to refer to the next section on detailed observations

S. No	Observation	Severity	Affected IP/URL/Application etc.	CVE/CWE	Final Status
1.	Vulnerable to Buffer overflow Attacks	Medium	http://rajattendancetest.rajasthan.gov.in/UIDAttendance	CVE-2023-23086	Open
2.	Clickjacking	Medium	http://rajattendancetest.rajasthan.gov.in	CVE-2021-35237	Open
3.	HTTP Strict Transport Security(HSTS) Policy Not Enabled	Medium	http://rajattendancetest.rajasthan.gov.in/raj-attendance/dashboard	CVE-2017-7789	Open
4.	Input Fields are not Filtered	Medium	http://rajattendancetest.rajasthan.gov.in/UIDAttendance/login	CVE-2023-36463	Open
5.	Broken Authentication	Medium	http://rajattendancetest.rajasthan.gov.in	CVE-2024-42172	Open
6.	Sensitive Information Submitted Through Get Method	Medium	http://rajattendancetest.rajasthan.gov.in	CVE-2024-21685	
7.	Content Security Policy Header Missing	Low	http://rajattendancetest.rajasthan.gov.in	CVE-2018-5164	Open
8.	Missing X-Content-Type-Options	Low	http://rajattendancetest.rajasthan.gov.in	CVE-2019-19089	Open
9.	Missing X-XSS-Protection	Low	http://rajattendancetest.rajasthan.gov.in	CVE-2018-7504	Open
10.	Improper Implementaion Of Cache-Control	Low	http://rajattendancetest.rajasthan.gov.in	CVE-2019-11043	Open

M. Audit Findings

This section presents a descriptive analysis of the vulnerabilities found on the Security Assessment Audit of RajCOMP Info Services Ltd that were obtained while performing the tests.

1.Vulnerable to Buffer overflow attacks

Description:

The application is Possible vulnerable for buffer overflow attacks. A buffer overflow, or buffer overrun, occurs when more data is put into a fixed-length buffer than the buffer can handle. The extra information, which has to go somewhere, can overflow into adjacent memory space, corrupting or overwriting the data held in that space.

Affected Links & Parameters [Location of Vulnerability]:

http://rajattendancetest.rajasthan.gov.in/UIDAttendance

CVE details:

CVE-2023-23086

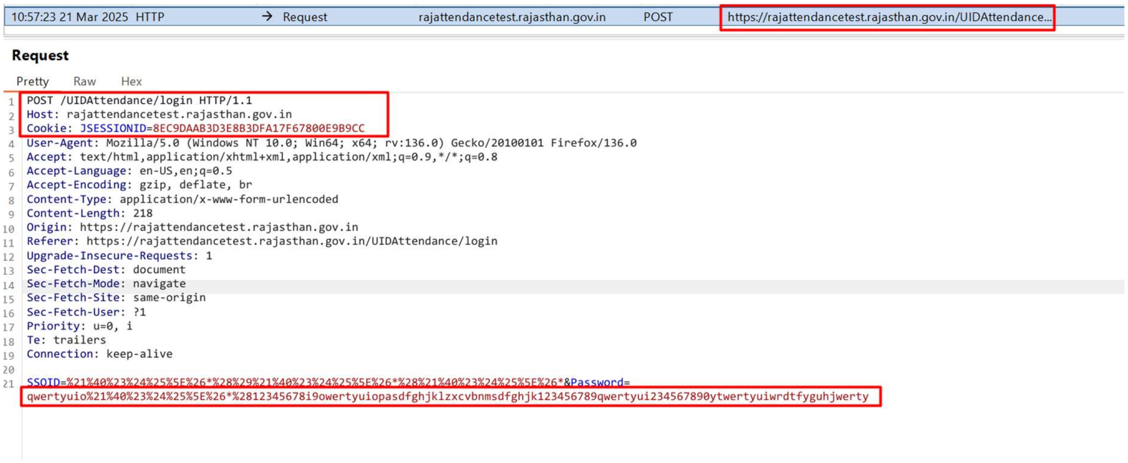
Business Impact:

Medium: An attacker can perform DOS attacks.

Recommendation and Mitigation Strategies:

- Set input fields string length limit.
- Validate max length of input fields.

Proof of Concept:



```
10:57:23 21 Mar 2025  HTTP    → Request    rajattendancetest.rajasthan.gov.in    POST    https://rajattendancetest.rajasthan.gov.in/UIDAttendance...
```

Request

```
POST /UIDAttendance/login HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=8EC9DAAB3D3E8B3DFA17F67800E9B9CC
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 218
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive

SSOID=%21%40%23%24%25%5E%26*%28%29%21%40%23%24%25%5E%26*%28%21%40%23%24%25%5E%26*&Password=
qwertyuio%21%40%23%24%25%5E%26*%2812345678i9owertyuiopasdfghjklzxcvbnmsdfghjk123456789qwertyui234567890ytwertyuiwrdtfyguhjwerty
```

2. Clickjacking

Description:

The application response headers contain missing X-Frame-Field options. Which may allow attacker to inject some other page using Iframe code.

Affected Link & Parameter [Location of Vulnerability]:

http://rajattendancetest.rajasthan.gov.in

CVE details:

CVE-2021-35237

Business Impact:

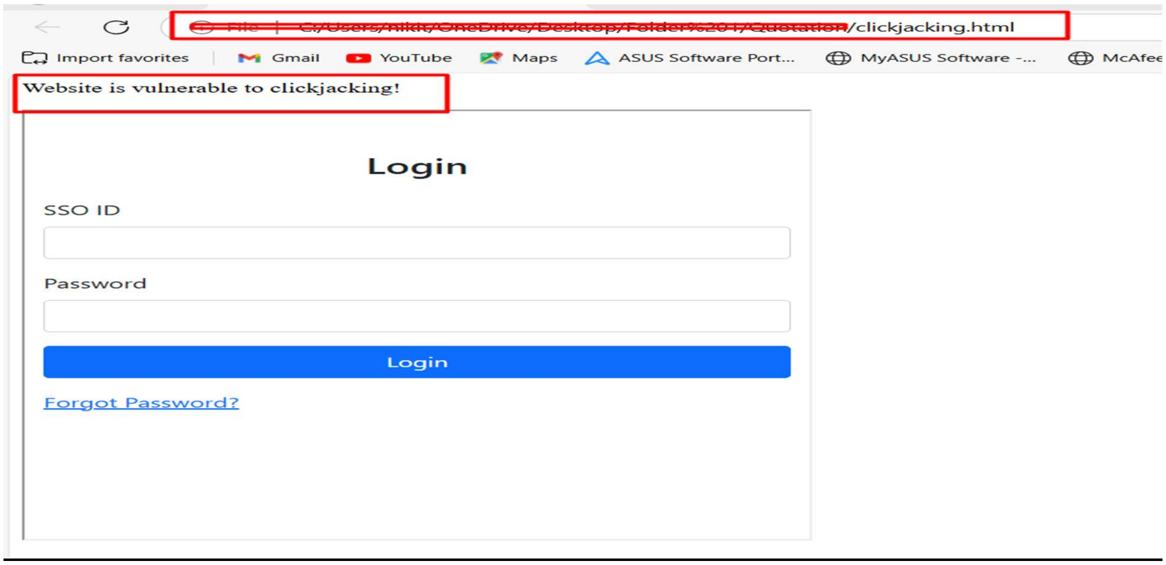
Medium: If an attacker carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Recommendation and Mitigation Strategies:

Please enable X-Frame-Options and set it to “DENY”, “SAME ORIGIN” or “ALLOW-FROM uri”.

- X-Frame-Options: DENY « won’t allow the website to be framed by anyone.
- X-Frame-Options: SAMEORIGIN « No one can frame except for sites from same origin.
- X-Frame-Options: ALLOW-FROM uri « which permits the specified 'uri' to frame this page. (e.g., ALLOW-FROM http://www.example.com).
- https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

Proof of Concept:



[redacted]/clickjacking.html

Website is vulnerable to clickjacking!

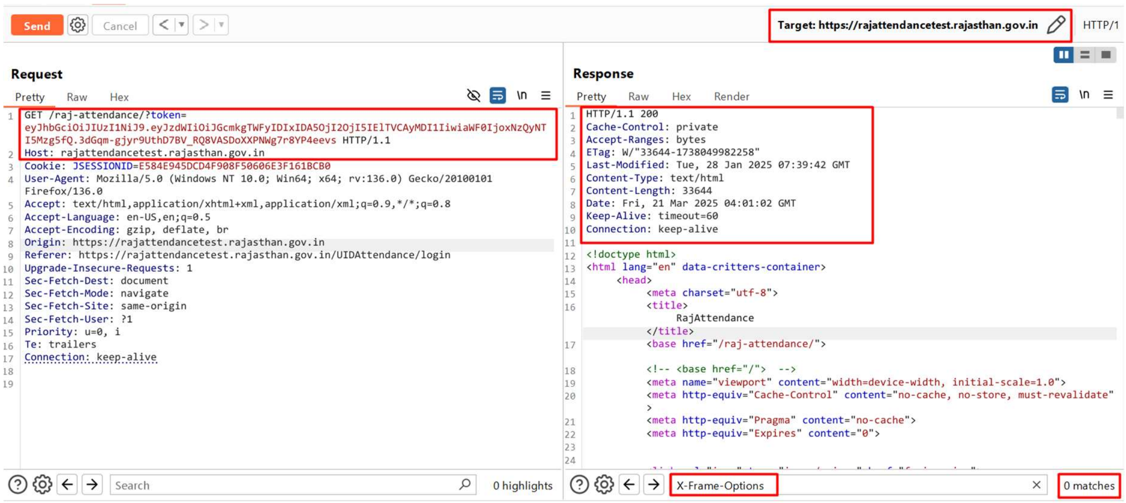
Login

SSO ID

Password

Login

Forgot Password?



```
GET /raj-attendance/?token=
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJGcmkgTWFyIDIxIDA5OjI2OjI5IElTVCAyMDI1IiwiaWF0IjoxNzQyNT
I5Mzg5fQ.3dGqm-gjyr9UthD7BV_RQ8VASDoXXPNWg7r8YP4eevs HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=E584E945DCD4F908F50606E3F161BCB0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200
Cache-Control: private
Accept-Ranges: bytes
ETag: W/"33644-1738049982258"
Last-Modified: Tue, 28 Jan 2025 07:39:42 GMT
Content-Type: text/html
Content-Length: 33644
Date: Fri, 21 Mar 2025 04:01:02 GMT
Keep-Alive: timeout=60
Connection: keep-alive

<!doctype html>
<html lang="en" data-critters-container>
    <head>
        <meta charset="utf-8">
        <title>
            RajAttendance
        </title>
        <base href="/raj-attendance/">

        <!-- <base href="/">  -->
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate"
        >
        <meta http-equiv="Pragma" content="no-cache">
        <meta http-equiv="Expires" content="0">
```

3. HTTP Strict Transport Security (HSTS) Policy Not Enabled

Description:

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTP (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure links referencing the web application into secure links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), show an error message and do not allow the user to access the web application.

Affected Link & Parameter [Location of Vulnerability]:

http://rajattendancetest.rajasthan.gov.in/raj-attendance/dashboard

CVE details:

CVE-2017-7789

Business Impact:

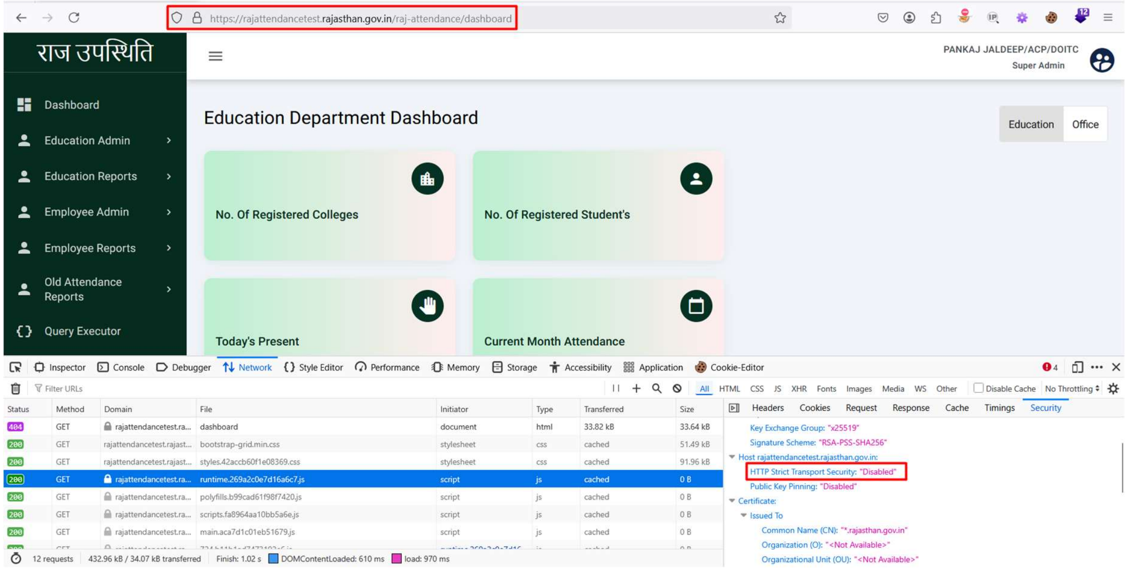
Medium: An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users.

Recommendation and Mitigation Strategies:

Configure your webserver to redirect HTTP requests to HTTPS.

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS)

Proof of Concept:



Status	Method	Domain	File	Initiator	Type	Transferred	Size
404	GET	rajattendancetest.ra...	dashboard	document	html	33.82 kB	33.64 kB
200	GET	rajattendancetest.rajast...	bootstrap-grid.min.css	stylesheet	css	cached	51.49 kB
200	GET	rajattendancetest.rajast...	styles.42accb60f1e08369.css	stylesheet	css	cached	91.96 kB
200	GET	rajattendancetest.ra...	runtime.269a2c0e7d16a6c7.js	script	js	cached	0 B
200	GET	rajattendancetest.ra...	polyfills.b99cad61f98f7420.js	script	js	cached	0 B
200	GET	rajattendancetest.ra...	scripts.fa8964aa10bb5a6e.js	script	js	cached	0 B
200	GET	rajattendancetest.ra...	main.aca7d1c01eb51679.js	script	js	cached	0 B

```
12 requests   432.96 kB / 34.07 kB transferred   Finish: 1.02 s   DOMContentLoaded: 610 ms   load: 970 ms
```

```
    Key Exchange Group: "x25519"
    Signature Scheme: "RSA-PSS-SHA256"
▼ Host rajattendancetest.rajasthan.gov.in:
    HTTP Strict Transport Security: "Disabled"
    Public Key Pinning: "Disabled"
▼ Certificate:
  ▼ Issued To
      Common Name (CN): "*.rajasthan.gov.in"
      Organization (O): "<Not Available>"
      Organizational Unit (OU): "<Not Available>"
```

4. Input Fields are not Filtered

Description:

Web applications use input from HTTP requests (and occasionally files) to determine how to respond. Attackers can tamper with any part of an HTTP request, including the url, query string, headers, cookies, form fields, and hidden fields, to try to bypass the site's security mechanisms. Common names for common input tampering attacks include: forced browsing, command insertion, cross site scripting, buffer overflows, format string attacks, SQL injection, cookie poisoning, and hidden field manipulation.

Affected Link & Parameter [Location of Vulnerability]:

http://rajattendancetest.rajasthan.gov.in/UIDAttendance/login

CVE details:

CVE-2023-36463

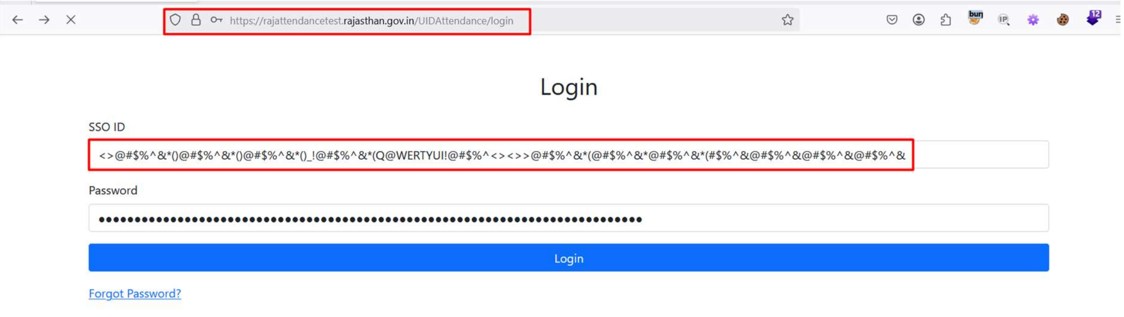
Business Impact:

Medium: The impact of using invalidated input should not be under estimated a huge number of attacks would become easy if the input fields are not validated before using it.

Recommendation and Mitigation Strategies:

Web applications should allow only validated inputs.

Proof of Concept:

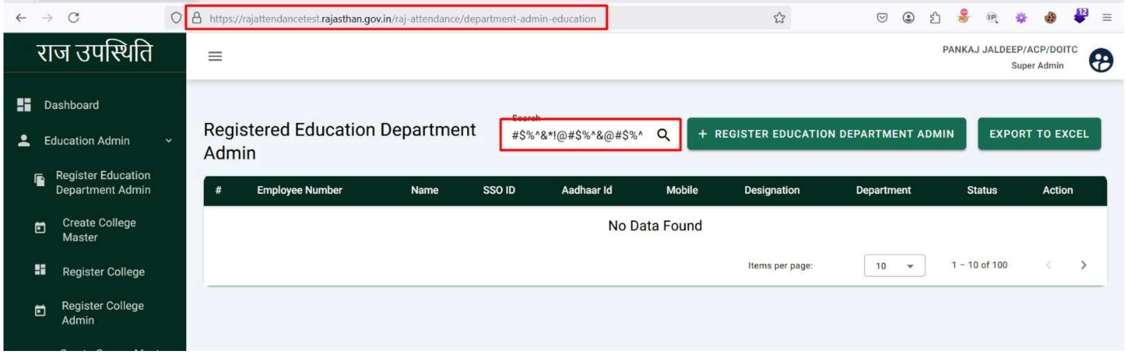


https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login

Login

SSO ID: <>@#$%^&*()@#$%^&*()@#$%^&*()_!@#$%^&*(Q@WERTYUI!@#$%^<><>>@#$%^&*(@#$%^&*@#$%^&*(#$%^&@#$%^&@#$%^&@#$%^&

Password: ••



https://rajattendancetest.rajasthan.gov.in/raj-attendance/department-admin-education

Registered Education Department Admin

Search: #$%^&*!@#$%^&@#$%^

#	Employee Number	Name	SSO ID	Aadhaar Id	Mobile	Designation	Department	Status	Action
No Data Found									

Items per page: 10 1 – 10 of 100

5. Broken Authentication

Description:

It includes all aspects of handling user authentication and managing active sessions which is not implemented properly. After logout from the any user account in the given application, session id is not re-generated again. The Result is which we can directly type any known authenticated URL path directly in the browser URL field which will log us in with same previously authenticated user session.

Affected Link & Parameter [Location of Vulnerability]:

http://rajattendancetest.rajasthan.gov.in

CVE details:

CVE-2024-42172

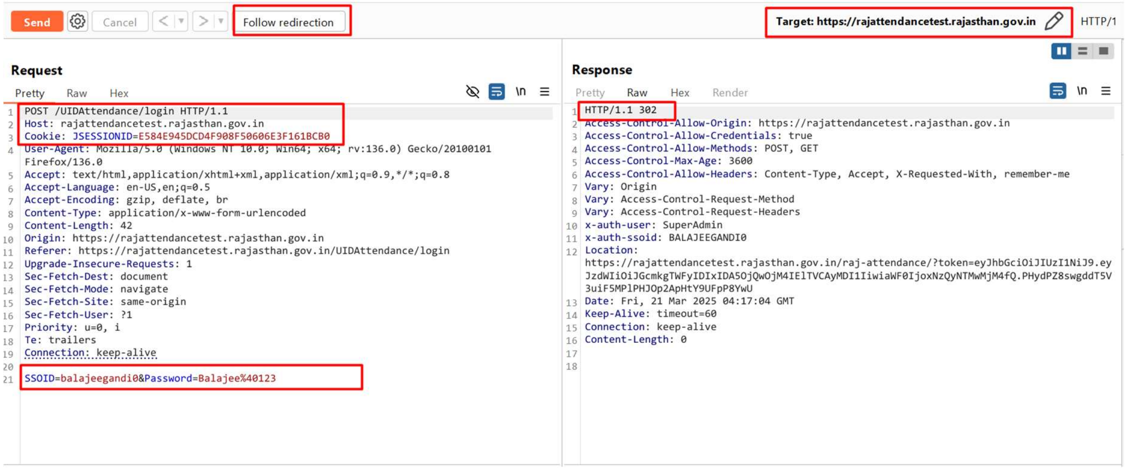
Business Impact:

Medium: The impact of using invalidated input should not be under estimated a huge number of attacks would become easy if the input fields are not validated before using it.

Recommendation and Mitigation Strategies:

Session ID's and token value must be rotated or generated as new, once after the active session has logged out.

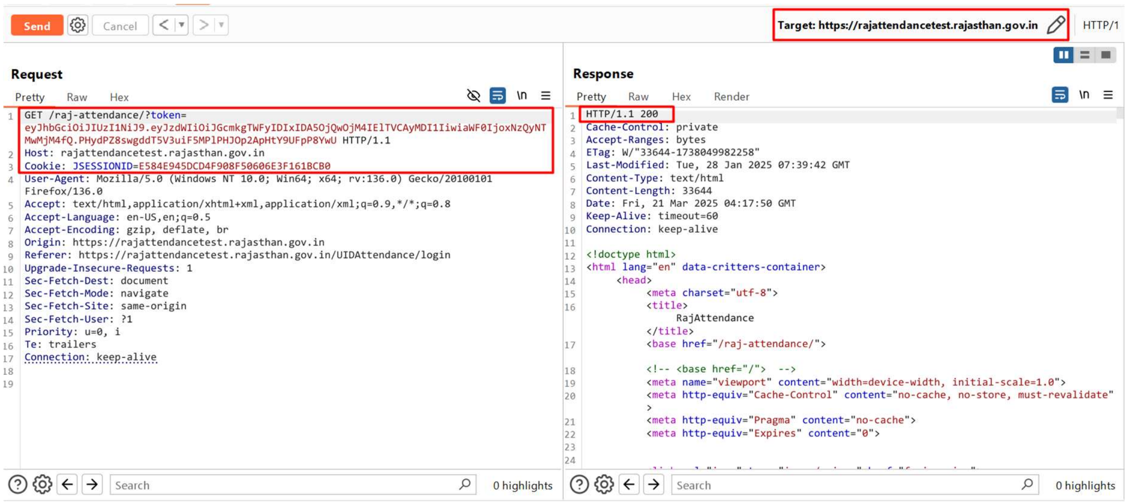
Proof of Concept:



```
POST /UIDAttendance/login HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=E584E945DCD4F908F50606E3F161BCB0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive

SSOID=balajeegandi0&Password=Balajee%40123
```

```
HTTP/1.1 302
Access-Control-Allow-Origin: https://rajattendancetest.rajasthan.gov.in
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: POST, GET
Access-Control-Max-Age: 3600
Access-Control-Allow-Headers: Content-Type, Accept, X-Requested-With, remember-me
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
x-auth-user: SuperAdmin
x-auth-ssoid: BALAJEEGANDI0
Location:
https://rajattendancetest.rajasthan.gov.in/raj-attendance/?token=eyJhbGciOiJIUzI1NiJ9.ey
JzdWIiOiJGcmkgTWFyIDIxIDA5OjQwOjM4IElTVCAyMDI1IiwiaWF0IjoxNzQyNTMwMjM4fQ.PHydPZ8swgddT5V
3uiF5MPlPHJOp2ApHtY9UFpP8YwU
Date: Fri, 21 Mar 2025 04:17:04 GMT
Keep-Alive: timeout=60
Connection: keep-alive
Content-Length: 0
```

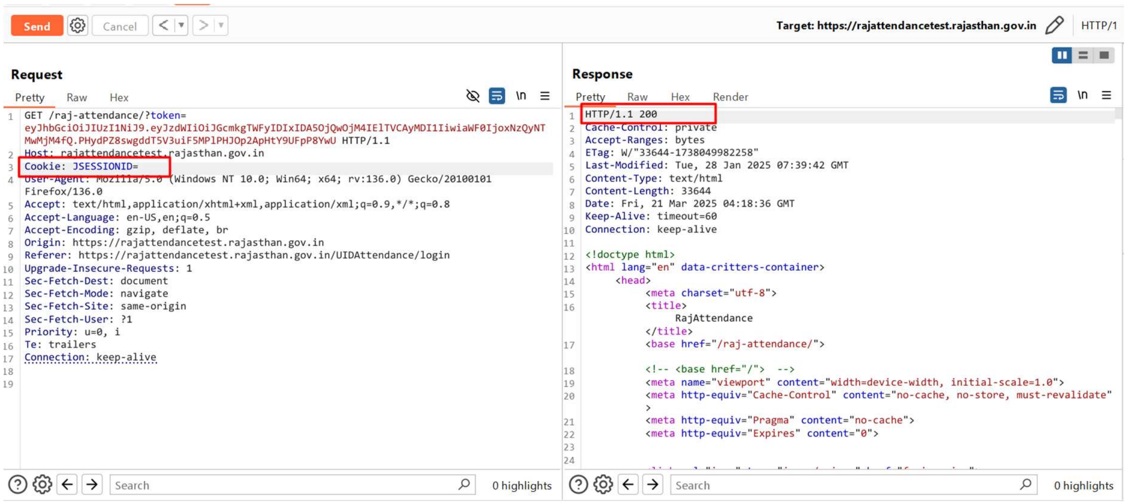


```
GET /raj-attendance/?token=
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJGcmkgTWFyIDIxIDA5OjQwOjM4IElTVCAyMDI1IiwiaWF0IjoxNzQyNT
MwMjM4fQ.PHydPZ8swgddT5V3uiF5MPlPHJOp2ApHtY9UFpP8YwU HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=E584E945DCD4F908F50606E3F161BCB0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200
Cache-Control: private
Accept-Ranges: bytes
ETag: W/"33644-1738049982258"
Last-Modified: Tue, 28 Jan 2025 07:39:42 GMT
Content-Type: text/html
Content-Length: 33644
Date: Fri, 21 Mar 2025 04:17:50 GMT
Keep-Alive: timeout=60
Connection: keep-alive

<!doctype html>
<html lang="en" data-critters-container>
    <head>
        <meta charset="utf-8">
        <title>
            RajAttendance
        </title>
        <base href="/raj-attendance/">

        <!-- <base href="/">  -->
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate"
        >
        <meta http-equiv="Pragma" content="no-cache">
        <meta http-equiv="Expires" content="0">
```

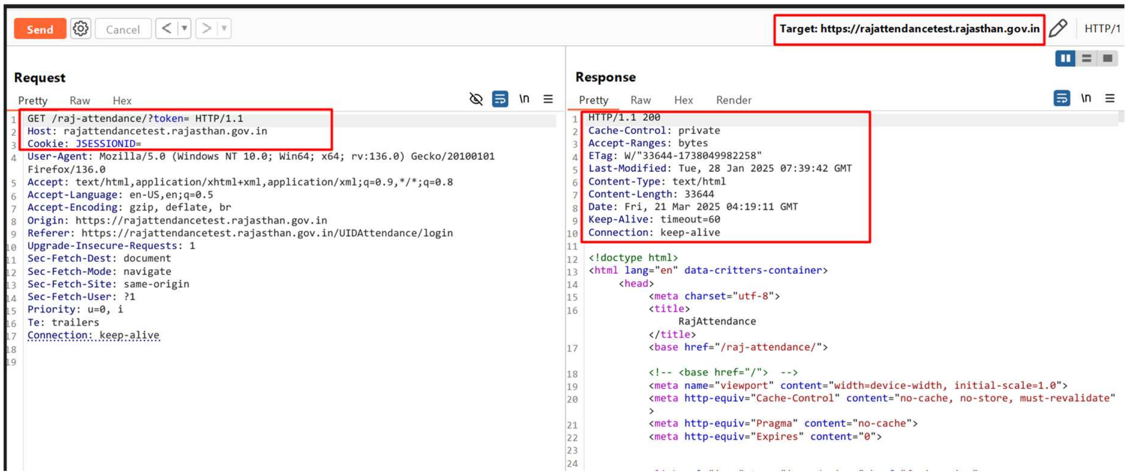


```
GET /raj-attendance/?token=
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJGcmkgTWFyIDIxIDA5OjQwOjM4IElTVCAyMDI1IiwiaWF0IjoxNzQyNT
MwMjM4fQ.PHydPZ8swgddT5V3uiF5MPlPHJOp2ApHtY9UFpP8YwU HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200
Cache-Control: private
Accept-Ranges: bytes
ETag: W/"33644-1738049982258"
Last-Modified: Tue, 28 Jan 2025 07:39:42 GMT
Content-Type: text/html
Content-Length: 33644
Date: Fri, 21 Mar 2025 04:18:36 GMT
Keep-Alive: timeout=60
Connection: keep-alive

<!doctype html>
<html lang="en" data-critters-container>
    <head>
        <meta charset="utf-8">
        <title>
            RajAttendance
        </title>
        <base href="/raj-attendance/">

        <!-- <base href="/">  -->
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate"
        >
        <meta http-equiv="Pragma" content="no-cache">
        <meta http-equiv="Expires" content="0">
```



```
GET /raj-attendance/?token= HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200
Cache-Control: private
Accept-Ranges: bytes
ETag: W/"33644-1738049982258"
Last-Modified: Tue, 28 Jan 2025 07:39:42 GMT
Content-Type: text/html
Content-Length: 33644
Date: Fri, 21 Mar 2025 04:19:11 GMT
Keep-Alive: timeout=60
Connection: keep-alive

<!doctype html>
<html lang="en" data-critters-container>
    <head>
        <meta charset="utf-8">
        <title>
            RajAttendance
        </title>
        <base href="/raj-attendance/">

        <!-- <base href="/">  -->
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate"
        >
        <meta http-equiv="Pragma" content="no-cache">
        <meta http-equiv="Expires" content="0">
```

6. Sensitive Information Submitted through GET method

Description:

This page contains a form with a password field. This form submits user data using the GET method, therefore the contents of the password field will appear in the URL. Sensitive information should not be passed via the URL. URLs could be logged or leaked via the Referrer header.

Affected Link & Parameter [Location of Vulnerability]:

http://rajattendancetest.rajasthan.gov.in

CVE details:

CVE-2024-21685

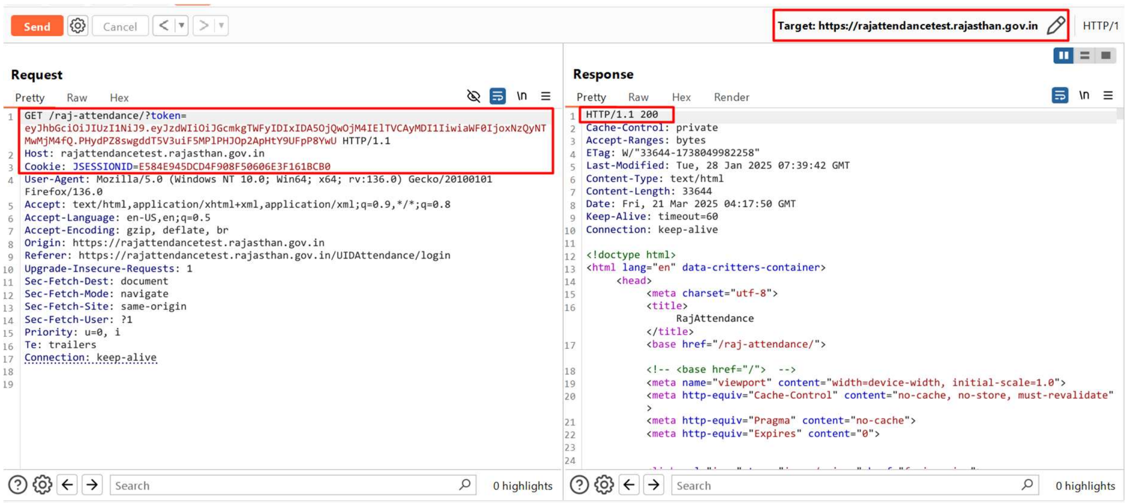
Business Impact:

Sensitive information disclosure.

Recommendation and Mitigation Strategies:

The password field should be submitted through POST instead of GET

Proof of Concept:



```
GET /raj-attendance/?token=
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJGcmkgTWFyIDIxIDA5OjQwOjM4IElTVCAyMDI1IiwiaWF0IjoxNzQyNT
MwMjM4fQ.PHydPZ8swgddT5V3uiF5MPlPHJOp2ApHtY9UFpP8YwU HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=E584E945DCD4F908F50606E3F161BCB0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200
Cache-Control: private
Accept-Ranges: bytes
ETag: W/"33644-1738049982258"
Last-Modified: Tue, 28 Jan 2025 07:39:42 GMT
Content-Type: text/html
Content-Length: 33644
Date: Fri, 21 Mar 2025 04:17:50 GMT
Keep-Alive: timeout=60
Connection: keep-alive

<!doctype html>
<html lang="en" data-critters-container>
    <head>
        <meta charset="utf-8">
        <title>
            RajAttendance
        </title>
        <base href="/raj-attendance/">

        <!-- <base href="/">  -->
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate"
        >
        <meta http-equiv="Pragma" content="no-cache">
        <meta http-equiv="Expires" content="0">
```

7. Content security policy Header Missing

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware.

Affected Link & Parameter [Location of Vulnerability]:

http://rajattendancetest.rajasthan.gov.in

CVE details:

CVE-2018-5164

Business Impact:

Low: There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

Recommendation and Mitigation Strategies:

A web site administrator wants all content to come from the site's own origin (this excludes subdomains.)

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

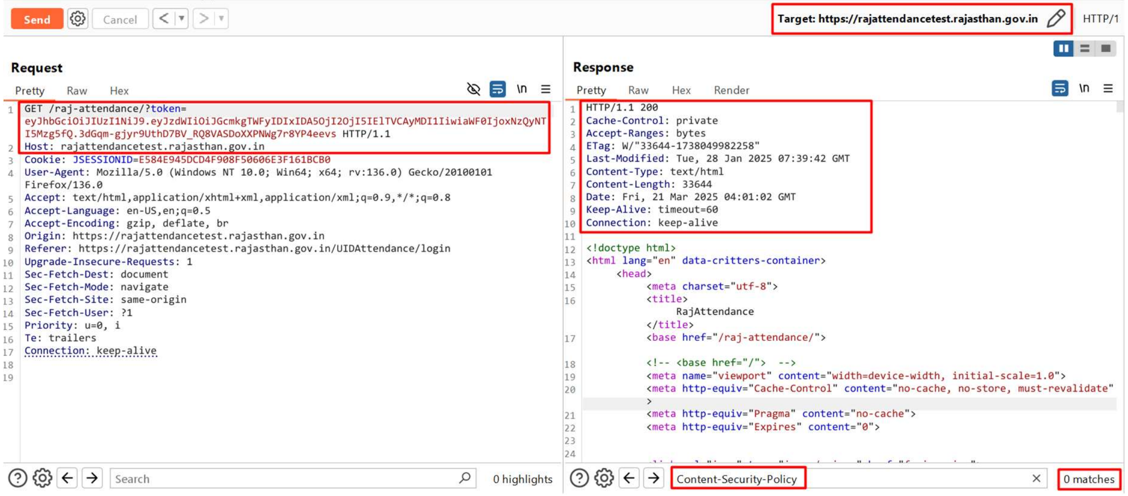
A web site administrator wants to allow content from a trusted domain and all its subdomains (it doesn't have to be the same domain that the CSP is set on.)

Content-Security-Policy: default-src 'self' *.trusted.com

A web site administrator wants to allow users of a web application to include images from any origin in their own content, but to restrict audio or video media to trusted providers, and all scripts only to a specific server that hosts trusted code.

Content-Security-Policy:==default-src'self';img-src*;media-srcmedia1.com media2.com; script-src

Proof of Concept:



```
GET /raj-attendance/?token=
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJGcmkgTWFyIDIxIDA5OjI2OjI5IElTVCAyMDI1IiwiaWF0IjoxNzQyNT
I5Mzg5fQ.3dGqm-gjyr9UthD7BV_RQ8VASDoXXPNWg7r8YP4eevs HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=E584E945DCD4F908F50606E3F161BCB0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

Search

0 highlights

```
HTTP/1.1 200
Cache-Control: private
Accept-Ranges: bytes
ETag: W/"33644-1738049982258"
Last-Modified: Tue, 28 Jan 2025 07:39:42 GMT
Content-Type: text/html
Content-Length: 33644
Date: Fri, 21 Mar 2025 04:01:02 GMT
Keep-Alive: timeout=60
Connection: keep-alive

<!doctype html>
<html lang="en" data-critters-container>
      <head>
            <meta charset="utf-8">
            <title>
                  RajAttendance
            </title>
            <base href="/raj-attendance/">

            <!-- <base href="/">  -->
            <meta name="viewport" content="width=device-width, initial-scale=1.0">
            <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate"
            >
            <meta http-equiv="Pragma" content="no-cache">
            <meta http-equiv="Expires" content="0">
```

Content-Security-Policy

0 matches

8. Missing X-Content-Type-Options

Description:

This header only has one valid value, no-sniff. It prevents Google Chrome and Internet Explorer from trying to mime-sniff the content-type of a response away from the one being declared by the server. It reduces exposure to drive-by downloads and the risks of user uploaded content that, with clever naming, could be treated as a different content-type, like an executable.

Affected Link & Parameter [Location of Vulnerability:

http://rajattendancetest.rajasthan.gov.in

CVE details:

CVE-2019-19089

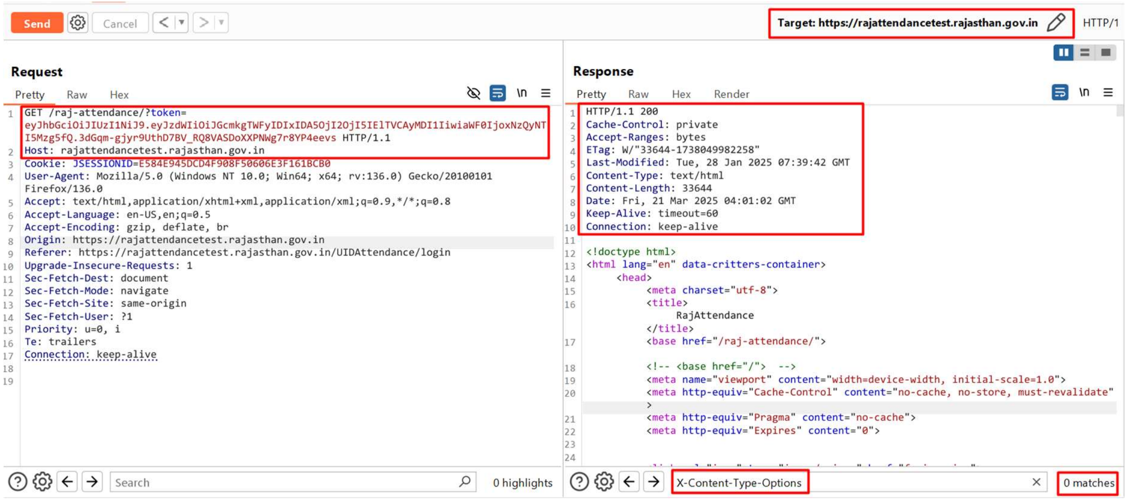
Business Impact:

Low: Possible of Man in the middle attacks.

Recommendation and Mitigation Strategies:

Prevents possible phishing or XSS attacks set X-Content-Type-Options "nosniff".

Proof of Concept:



```
GET /raj-attendance/?token=
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJGcmkgTWFyIDIxIDA5OjI2OjI5IElTVCAyMDI1IiwiaWF0IjoxNzQyNT
I5Mzg5fQ.3dGqm-gjyr9UthD7BV_RQ8VASDoXXPNWg7r8YP4eevs HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=E584E945DCD4F908F50606E3F161BCB0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200
Cache-Control: private
Accept-Ranges: bytes
ETag: W/"33644-1738049982258"
Last-Modified: Tue, 28 Jan 2025 07:39:42 GMT
Content-Type: text/html
Content-Length: 33644
Date: Fri, 21 Mar 2025 04:01:02 GMT
Keep-Alive: timeout=60
Connection: keep-alive

<!doctype html>
<html lang="en" data-critters-container>
    <head>
        <meta charset="utf-8">
        <title>
            RajAttendance
        </title>
        <base href="/raj-attendance/">

        <!-- <base href="/">  -->
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate"
        >
        <meta http-equiv="Pragma" content="no-cache">
        <meta http-equiv="Expires" content="0">
```

9. Missing X-XSS-Protection

Description:

This header is used to configure the built in reflective XSS protection found in Internet Explorer, Chrome and Safari (Webkit). Valid settings for the header are 0, which disables the protection, 1 which enables the protection and 1; mode=block which tells the browser to block the response if it detects an attack rather than sanitising the script.

Affected Link & Parameter [Location of Vulnerability]:

http://rajattendancetest.rajasthan.gov.in

CVE details:

CVE-2018-7504

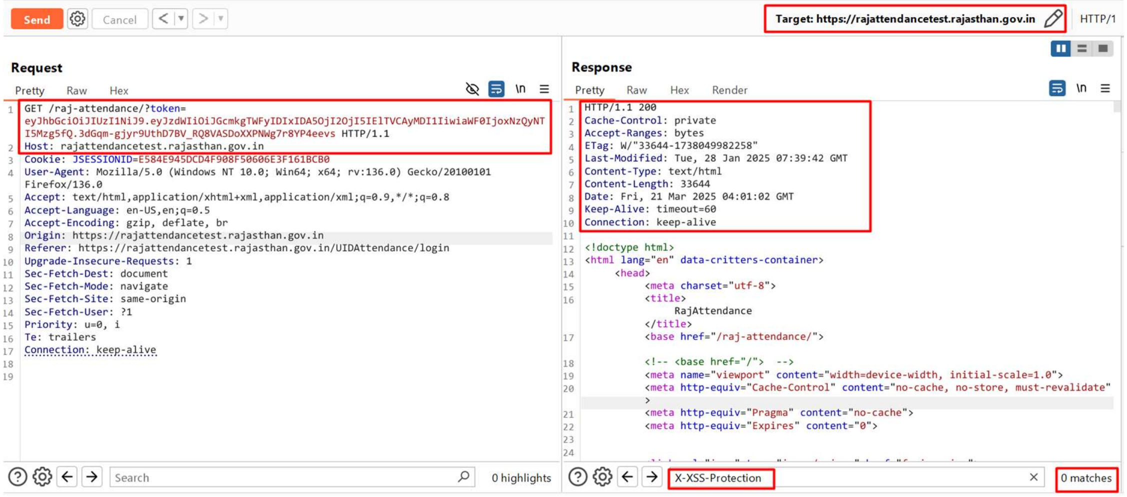
Business Impact:

Low: Possible of Cross-Site Scripting (XSS) attacks.

Recommendation and Mitigation Strategies:

Mitigates Cross-Site Scripting (XSS) attacks set X-XSS-Protection "1; mode=block"

Proof of Concept:



```
GET /raj-attendance/?token=
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJGcmkgTWFyIDIxIDA5OjI2OjI5IElTVCAyMDI1IiwiaWF0IjoxNzQyNT
I5Mzg5fQ.3dGqm-gjyr9UthD7BV_RQ8VASDoXXPNWg7r8YP4eevs HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=E584E945DCD4F908F50606E3F161BCB0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200
Cache-Control: private
Accept-Ranges: bytes
ETag: W/"33644-1738049982258"
Last-Modified: Tue, 28 Jan 2025 07:39:42 GMT
Content-Type: text/html
Content-Length: 33644
Date: Fri, 21 Mar 2025 04:01:02 GMT
Keep-Alive: timeout=60
Connection: keep-alive

<!doctype html>
<html lang="en" data-critters-container>
    <head>
        <meta charset="utf-8">
        <title>
            RajAttendance
        </title>
        <base href="/raj-attendance/">

        <!-- <base href="/">  -->
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate"
        >
        <meta http-equiv="Pragma" content="no-cache">
        <meta http-equiv="Expires" content="0">
```

10. Improper Implementation of Cache-Control

Description:

Improper implementation of the Cache-Control header occurs when web applications fail to set appropriate caching directives, allowing sensitive information to be cached improperly by browsers, proxies, or intermediary servers. This can lead to unauthorized access, data leakage, and security risks.

Affected Link & Parameter [Location of Vulnerability]:

http://rajattendancetest.rajasthan.gov.in

CVE details:

CVE-2019-11043

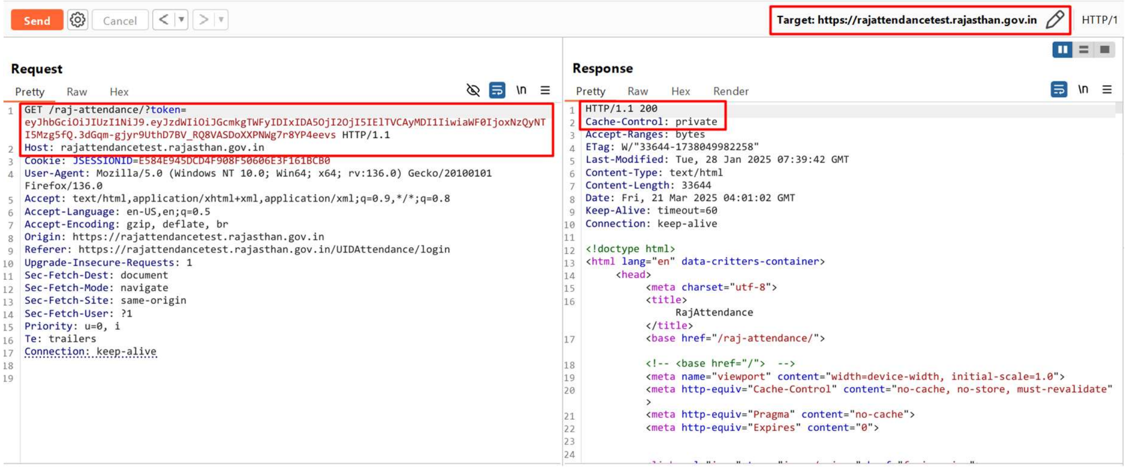
Business Impact:

Low: Leakage of sensitive customer data can result in legal and regulatory consequences.
Brand Reputation Damage: Exposure of confidential information can erode customer trust. Regulatory
Financial Loss: Exploitation of cached authentication tokens may result in unauthorized transactions

Recommendation and Mitigation Strategies:

Implement no-store and no-cache to cache -control header
Cache-control: no-store, no-cache
no-cache: Forces validation with the server before using a cached resource.
no-store: Prevents storing any cacheable response (good for sensitive data).

Proof of Concept:



```
GET /raj-attendance/?token=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJGcmkgTWFyIDIxIDA5OjI2OjI5IElTVCAyMDI1IiwiaWF0IjoxNzQyNTI5Mzg5fQ.3dGqm-gjyr9UthD7BV_RQ8VASDoXXPNWg7r8YP4eevs HTTP/1.1
Host: rajattendancetest.rajasthan.gov.in
Cookie: JSESSIONID=E584E945DCD4F908F50606E3F161BCB0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: https://rajattendancetest.rajasthan.gov.in
Referer: https://rajattendancetest.rajasthan.gov.in/UIDAttendance/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200
Cache-Control: private
Accept-Ranges: bytes
ETag: W/"33644-1738049982258"
Last-Modified: Tue, 28 Jan 2025 07:39:42 GMT
Content-Type: text/html
Content-Length: 33644
Date: Fri, 21 Mar 2025 04:01:02 GMT
Keep-Alive: timeout=60
Connection: keep-alive

<!doctype html>
<html lang="en" data-critters-container>
    <head>
        <meta charset="utf-8">
        <title>
            RajAttendance
        </title>
        <base href="/raj-attendance/">

        <!-- <base href="/">  -->
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate">
        <meta http-equiv="Pragma" content="no-cache">
        <meta http-equiv="Expires" content="0">
```

N. Disclaimer

This document is highly confidential and sensitive and is meant for circulation only to authorized people within RajCOMP Info Services Ltd and Digital Age Strategies Pvt Ltd. It is understood that disclosure in part or full of the contents or any information derived from the report to unauthorized personnel is strictly prohibited.

O. Conclusion

Digital Age Strategies Security Auditors conducted Security Assessment on the given Web Application of RajCOMP Info Services Ltd and found that the above-mentioned vulnerabilities.