AKS IT SERVICES

Web Application Security Audit Report:

CID

Report Release Date	16.10.2025
Type of Audit	Application Security
Type of Audit Report	Initial Audit Report
Period	13.10.2025 – 16.10.2025

Report Prepared By:

AKS Information Technology Services Pvt. Ltd.

www.aksitservices.co.in

E-Mail: info@aksitservices.co.in

Non-Disclosure Statement

This report is the sole property of Telangana Criminal Investigation Department. All information obtained during the assessment is deemed privileged information and not for public dissemination. **AKS Information Technology Services Pvt. Ltd**. pledges its commitment that this information will remain strictly confidential. It will not be discussed or disclosed to any third party without the express written consent of Telangana Criminal Investigation Department except required by the government regulator (Cert-In) or by the order of the Court.

Document Control

Document Preparation	
Document Title	Web Application Security Audit Report of CID
Document ID	--
Document Version	1.0
Prepared by	Ms. Annu Kumari
Reviewed by	Mr. Faraz Ahmad
Approved by	Mr. Vishrant Ojha
Released by	Ms. Annu Kumari
Release Date	16.10.2025

Document Change History		
Version	**Date**	**Remarks / Reason of change**
1.0	16.10.2025	Initial release

Document Distribution List			
Name	**Organization**	**Designation**	**Email Id**
Sai Sreekar Thrurupatla	Telangana Criminal Investigation Department	Additional Director General of Police	saisreekar@vatins.com

Table of Contents

Table of Contents 4
Introduction 5
Engagement Scope 6
Details of the Auditing Team 7
Audit Activities and Timelines 8
Tools/ Software Used 9
Executive Summary 10
Detailed Findings 15
Observation 45
Appendix ‘A’ 47

Introduction

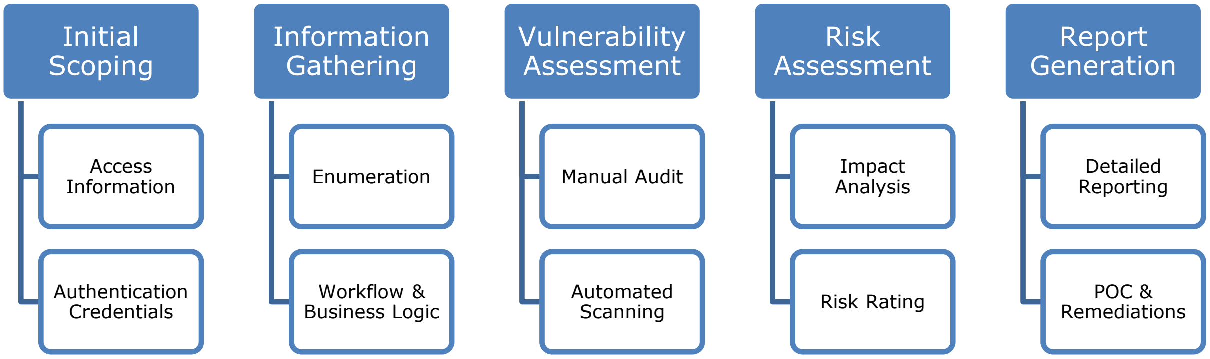
Objectives:

The key objective of this Web Application Security Audit was to identify whether any vulnerabilities exist in the Web Application and to exploit those that can be seen and compromised by malicious users. Additionally, the objective of this activity was to ensure the security of the network and web server from external threats through the Web Application.

Methodology & Standard:

Security Consultants at AKS IT Services Pvt. Ltd. used the OWASP Web Application Security Testing Methodology for conducting the security audit of the in-scope Web Application.

The OWASP Web Application Methodology is based on the 'grey-box' approach. The testing model consists of the following phases:


Initial Scoping
Access Information
Authentication Credentials
Information Gathering
Enumeration
Workflow & Business Logic
Vulnerability Assessment
Manual Audit
Automated Scanning
Risk Assessment
Impact Analysis
Risk Rating
Report Generation
Detailed Reporting
POC & Remediations

Standard:

The Open Worldwide Application Security Project (OWASP) standard was used for conducting the initial level security audit of the CID Web Application. The assessment was aimed at identifying the vulnerabilities that are defined in the OWASP, Common Weakness Enumeration, and other common global best practices.

- CERT-In Guidelines: https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf
- NIC Guidelines: https://meity.gov.in/writereaddata/files/checklist_development.pdf
- OWASP standard: https://owasp.org/web-security-testing-guide/
- Best Practices.

Engagement Scope

S. No	Asset Description	Criticality of Asset	Internal IP Address	URL	Public IP Address	Location	Hash Value of final audit report	Version
1.	Web Application	NA	NA	**https://cid-staging.tspolice.gov.in/**	NA	Remote	NA	NA

Details of the 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 Source Code (Yes/No)
1	Annu Kumari	Infosec Consultant	annu.kumari@aksitservices.co.in	CEH	Yes
2	Faraz Ahmad	Team Lead – Application Security	faraz.ahmad@aksitservices.co.in	CEH, CRTP	Yes
3	Vishrant Ojha	Assistant Manager – Application Security	vishrant.ojha@aksitservices.co.in	CISA, CEH, M.Tech in Cyber Security, Diploma in Cyber Law	Yes

Audit Activities and Timelines

Audit Activity	**Timelines**
Phase I	
Auditor Assigned	29.09.2025
Audit Initiated	13.10.2025
Audit Report Preparation	15.10.2025
Initial Audit Report Published	16.10.2025

Tools/ Software Used

S. No	Name of Tool/Software used	Version of the tool/Software used	Open Source/Licensed
1	Burp Suite Professional	2025.6.1	Commercial
2	Acunetix Vulnerability Scanner	24.5	Commercial
3	GoBuster	3.6.0	Open Source
4	SQLMAP	1.9	Open Source

Appendix 'A': Description of the tools

Executive Summary

13	00	06	07
Total	**High**	**Medium**	**Low**

S. No	Affected Asset i.e. IP/URL/Application etc.	Observation/ Vulnerability title	CVE/ CWE	Severity	Recommendation	Reference	New or Repeat or closed observation
1.	https://cid-staging.tspolice.gov.in/about	Insecure HTTP Methods Enabled	CWE-749	Medium	Unnecessary HTTP methods like TRACE and OPTIONS should be disabled.	Case I	New
2.	https://cid-staging.tspolice.gov.in/about	Host Header Attack	CWE-644	Medium	Validating Host header to ensure that the request is originating from that target host or not. By creating a white list of trusted domains during the initial setup of the application and mapping domains received in Host header of each and every request with it.	Case II	New
3.	https://cid-staging.tspolice.gov.in/admin/content/photos	Malicious File Upload	CWE-434	Medium	Application should check allowed File extension and File type (MIME Type) in the upload module using white-list filter at server side. File to be uploaded should be restricted to a particular size. Server-side check for not allowing	Case III	New

					long filename with double extension/double -dot(.)/nullbyte (%00)/meta characters. Assign only Read and Write permissions to the upload folders as required.		
4.	https://cid-staging.tspolice.gov.in/api/admin/wings	Misconfigured CORS	CWE-942	Medium	The header 'Access-Control-Allow-Origin' should not be set to * if the resource contains sensitive information. Configure the Access-Control-Allow-Origin header to allow requests only from the domains that you trust. Don't rely only on the Origin header for Access Control checks. Browsers always send this header in CORS requests, but it may be spoofed outside the browser.	Case IV	
5.	https://cid-staging.tspolice.gov.in/admin/login	Weak Captcha Implementation	CWE-804	Medium	Because the CAPTCHA cracking attacks are still improving (and will improve in the future), CAPTCHA should be perceived as a rate-limiting protection only. If it is implemented, the following considerations should be taken into account: •No CAPTCHA information (except the image itself) should be stored on the client side •The client should have no "control" over the CAPTCHA content •CAPTCHA images should be always randomly generated without possibility to perform image pre-processing, segmentation and classification •CAPTCHA images should not be	Case V	New

					reused.		
6.	https://cid-staging.tspolice.gov.in/admin/login	Session Replay	CWE-NA	Medium	When the authenticated user logs off the application all its session variables are destroyed thus destroying the session token & the user mapping.	Case VI	New
7.	https://cid-staging.tspolice.gov.in/duty-meet https://cid-staging.tspolice.gov.in/economic-offences	Email Harvesting	CWE-200	Low	The application should properly customize the email addresses while posting on the website as: Email addresses should be posted as an image not as a hyperlink. Alternatively, instead of @symbol, [at] should be used. Similarly, the dot character (.) should be replaced by [dot]. So abc@nic.in should be written as abc[at]nic[dot]in.	Case VII	New
8.	https://cid-staging.tspolice.gov.in/admin/login	Autocomplete Enabled on Password Field	CWE-200	Low	To prevent browsers from storing credentials entered into HTML forms, include the attribute autocomplete="off" within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).	Case VIII	New
9.	https://cid-staging.tspolice.gov.in/admin/login	Cleartext Submission of Password	CWE-319	Low	Implementation of salted SHA-256 or salted SHA-512 hashing algorithms on password fields, while using plain SHA-256 or SHA-512 hashing on new password fields. If Salted Hashing is not possible, implement AES encryption with randomized padding. Additionally, use latest stable version of TLS to protect all sensitive communications passing between the client and the server.	Case IX	New

					Implement HTTP Strict Transport Layer Security. If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear-text HTTP.		
10.	https://cid-staging.tspolice.gov.in/	SSL/TLS Certificate Supports Older vers, CBC and Weak Cipher Algorithms	CWE-327	Low	Reconfigure the affected application, to avoid the use of weak ciphers such as SSL, MD5, SHA1, RC4, 3DES, Weak algorithms like TLS1.0, TLS1.1. Use only TLS 1.2.	Case X	New
11.	https://cid-staging.tspolice.gov.in/admin/login	Improper Session Timeout	CWE-613	Low	Application should automatically log out the user and destroy the session after 20 mins of inactivity.	Case XI	New
12.	https://cid-staging.tspolice.gov.in/admin/content/pages	Missing Cookies Attributes	CWE-614	Low	The secure flag should be set on all cookies that are being used for transmitting sensitive data when accessing content over HTTPS. The SameSite should be set to Lax/Strict as required by the application. The HttpOnly flag should be set on all cookies in order to prevent cookies accessed by javascript.	Case XII	
13.	https://cid-staging.tspolice.gov.in/admin/login	Security Logging and	CWE-778	Low	Information to be logged includes the following: IP address of the	Case XIII	New

		Monitoring Failures			originating Source, Date, Time, Username (No Password), session details, Referrer, Process id, URL, User Agent, Countries if any in addition to other details to be logged in the website. Logging of Authentication Process which includes number of successful and failed login attempts. To create audit logs, use auto numbering so that every logged entry has an un-editable log number. Then if one audit entry is deleted a gap in the numbering sequence will appear. Report of the website logs to be generated weekly by the administrator to keep track of the website activities		

Detailed Findings

Case I

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/about

ii. Observation/ Vulnerability title

Insecure HTTP Methods Enabled

iii. Detailed observation / Vulnerable point

Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data or conduct more serious attacks.

iv. CVE/CWE

CWE-749

v. Severity

Medium

vi. Recommendation

Unnecessary HTTP methods like TRACE, PUT, DELETE, PATCH and OPTIONS should be disabled.

vii. Reference

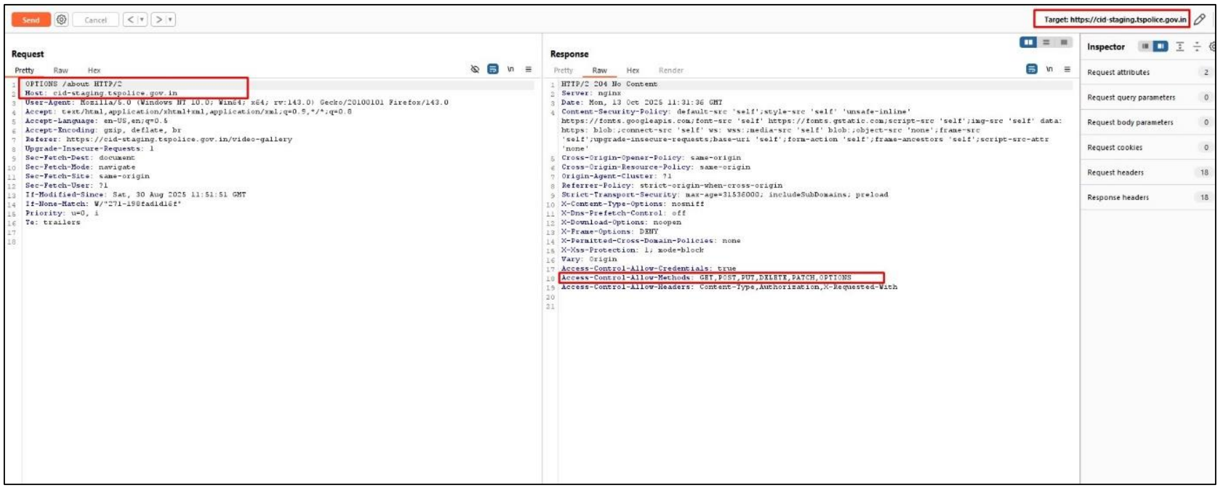
Case I

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: Visit to the URL: **“https://cid-staging.tspolice.gov.in/about”** We observe that insecure HTTP Request method is enabled as shown in below snapshot:



```
OPTIONS /about HTTP/2
Host: cid-staging.tspolice.gov.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0
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
Referer: https://cid-staging.tspolice.gov.in/video-gallery
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
If-Modified-Since: Sat, 30 Aug 2025 11:51:51 GMT
If-None-Match: W/"271-198fad1d16f"
Priority: u=0, i
Te: trailers
```

```
HTTP/2 204 No Content
Server: nginx
Date: Mon, 13 Oct 2025 11:31:36 GMT
Content-Security-Policy: default-src 'self';style-src 'self' 'unsafe-inline'
https://fonts.googleapis.com;font-src 'self' https://fonts.gstatic.com;script-src 'self';img-src 'self' data:
https: blob:;connect-src 'self' ws: wss:;media-src 'self' blob:;object-src 'none';frame-src
'self';upgrade-insecure-requests;base-uri 'self';form-action 'self';frame-ancestors 'self';script-src-attr
'none'
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: strict-origin-when-cross-origin
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Dns-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: DENY
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode=block
Vary: Origin
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,PATCH,OPTIONS
Access-Control-Allow-Headers: Content-Type,Authorization,X-Requested-With
```

Note: Kindly patch the issue throughout the application.

Case II

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/about

ii. Observation/ Vulnerability title

Host Header Attack

iii. Detailed observation / Vulnerable point

Many web applications rely on the HTTP host header to understand “where they are”. Unfortunately, what many application developers do not realize is that the HTTP host header is controlled by the user. In application security user input should always be considered unsafe and therefore, never trusted without properly validating it first.

iv. CVE/CWE

CWE-644

v. Severity

Medium

vi. Recommendation

Validating Host header to ensure that the request is originating from that target host or not. By creating a white list of trusted domains during the initial setup of the application and mapping domains received in Host header of each and every request with it.

vii. Reference

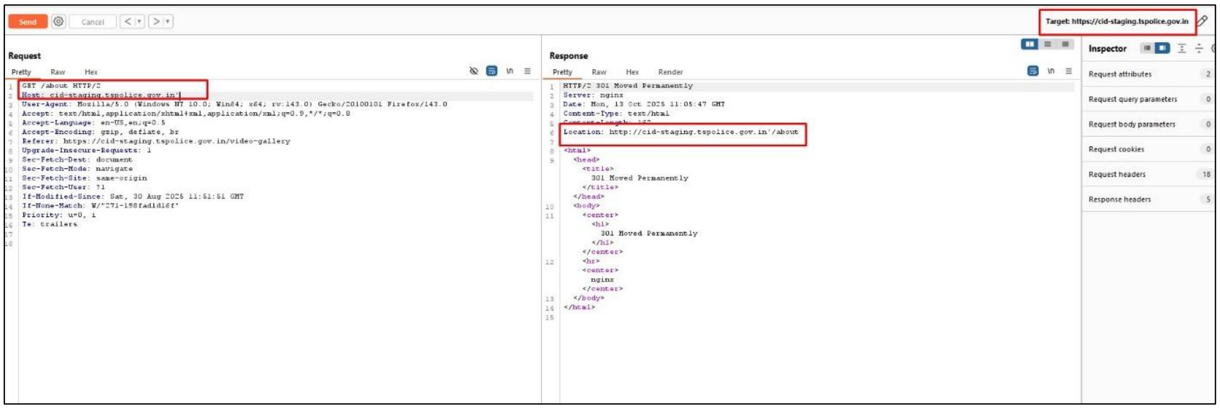
Case II

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

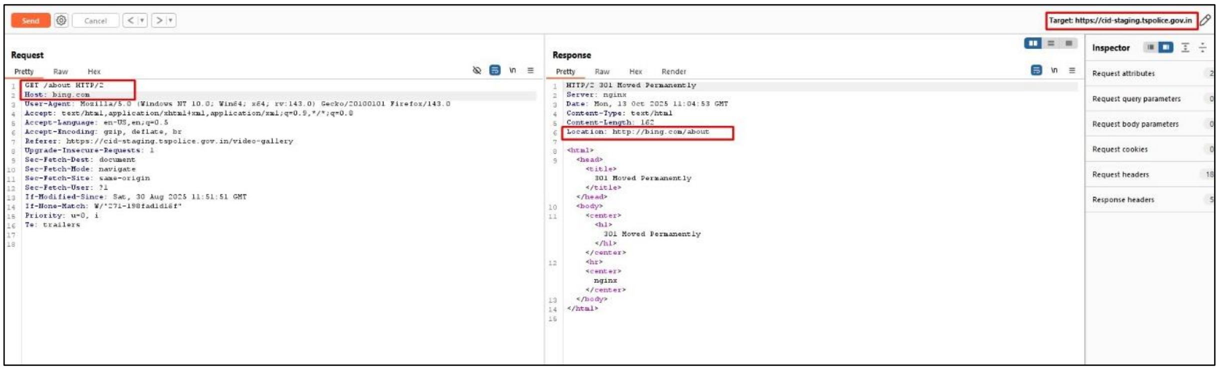
Step I: Visit to the URL: **“https://cid-staging.tspolice.gov.in/about”** and intercept the request as shown in below snapshot:



```
GET /about HTTP/2
Host: cid-staging.tspolice.gov.in'
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0
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
Referer: https://cid-staging.tspolice.gov.in/video-gallery
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
If-Modified-Since: Sat, 30 Aug 2025 11:51:51 GMT
If-None-Match: W/"271-198fad1d16f"
Priority: u=0, i
Te: trailers
```

```
HTTP/2 301 Moved Permanently
Server: nginx
Date: Mon, 13 Oct 2025 11:05:47 GMT
Content-Type: text/html
Content-Length: 162
Location: http://cid-staging.tspolice.gov.in'/about

<html>
  <head>
    <title>
      301 Moved Permanently
    </title>
  </head>
  <body>
    <center>
      <h1>
        301 Moved Permanently
      </h1>
    </center>
    <hr>
    <center>
      nginx
    </center>
  </body>
</html>
```

Step II: Now change the host header value, we observe that in response the Link value is changed as shown in below snapshots:



```
GET /about HTTP/2
Host: bing.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0
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
Referer: https://cid-staging.tspolice.gov.in/video-gallery
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
If-Modified-Since: Sat, 30 Aug 2025 11:51:51 GMT
If-None-Match: W/"271-198fad1d16f"
Priority: u=0, i
Te: trailers
```

```
HTTP/2 301 Moved Permanently
Server: nginx
Date: Mon, 13 Oct 2025 11:04:53 GMT
Content-Type: text/html
Content-Length: 162
Location: http://bing.com/about

<html>
  <head>
    <title>
      301 Moved Permanently
    </title>
  </head>
  <body>
    <center>
      <h1>
        301 Moved Permanently
      </h1>
    </center>
    <hr>
    <center>
      nginx
    </center>
  </body>
</html>
```

Note: Kindly patch the issue throughout the application.

Case III

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/admin/content/photos

ii. Observation/ Vulnerability title

Malicious File Upload

iii. Detailed observation / Vulnerable point

Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.

iv. CVE/CWE

CWE-434

v. Severity

Medium

vi. Recommendation

Application should check allowed File extension and File type (MIME Type) in the upload module using white-list filter at server side.
File to be uploaded should be restricted to a particular size.
Server-side check for not allowing long filename with double extension/double -dot(.)/nullbyte (%00)/meta characters.
Assign only Read and Write permissions to the upload folders as required.

vii. Reference

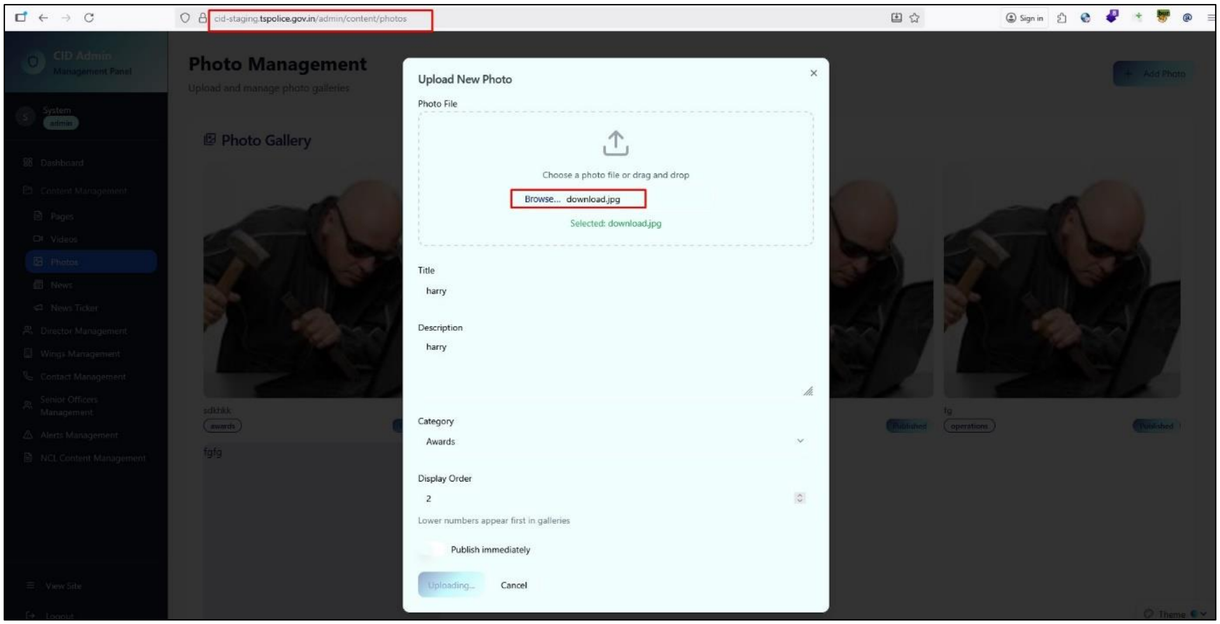
Case III

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: Login to the application and Visit to the URL: **"https://cid-staging.tspolice.gov.in/admin/content/photos"** and intercept the request as shown in below snapshots:



Upload New Photo

Photo File

Choose a photo file or drag and drop

Browse... download.jpg

Selected: download.jpg

Title: harry

Description: harry

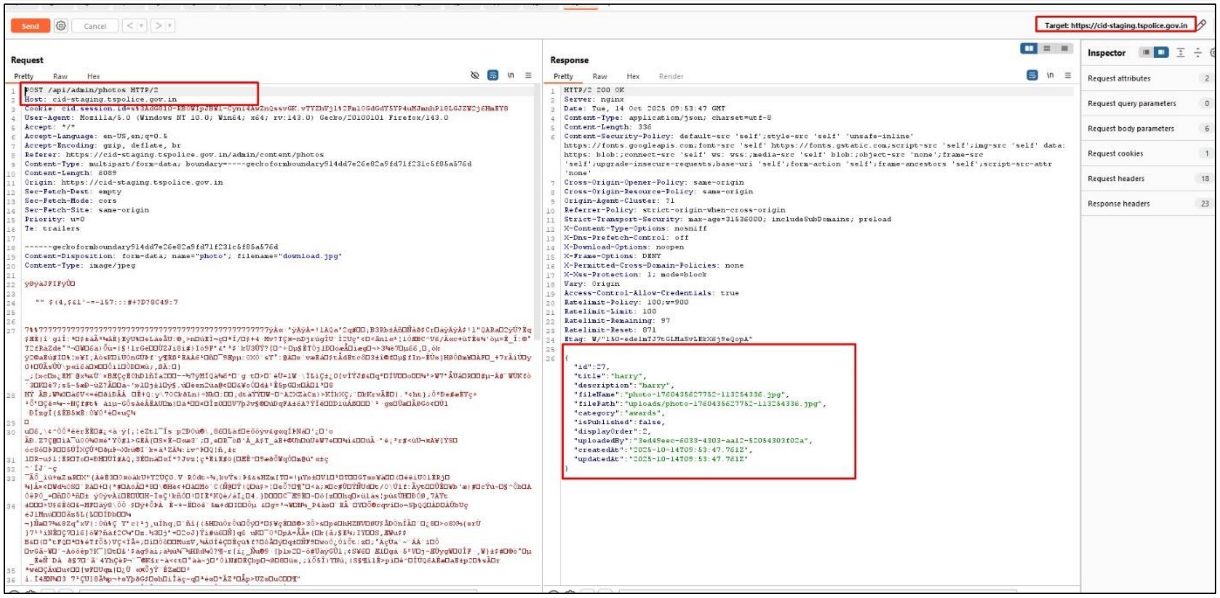
Category: Awards

Display Order: 2

Lower numbers appear first in galleries

Publish immediately

Uploading... Cancel



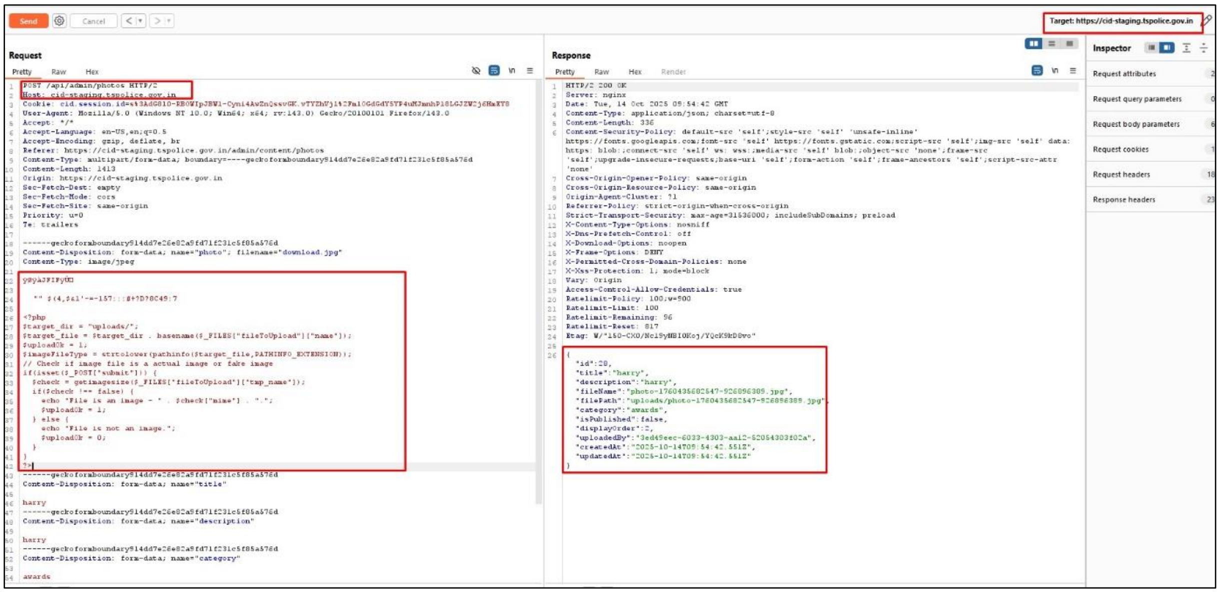
Request:

```
POST /api/admin/photos HTTP/2
Host: cid-staging.tspolice.gov.in
Cookie: cid.session.id=s%3AdG810-RBOWIpJBWl-Cyni4AwZnQssvGK.vTYZhVjl%2Fml0GdGdY5YP4uMJmnhPl8LGJZW2j6HmBY8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://cid-staging.tspolice.gov.in/admin/content/photos
Content-Type: multipart/form-data; boundary=----geckoformboundary914dd7e26e82a9fd71f231c5f85a576d
Content-Length: 6089
Origin: https://cid-staging.tspolice.gov.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

------geckoformboundary914dd7e26e82a9fd71f231c5f85a576d
Content-Disposition: form-data; name="photo"; filename="download.jpg"
Content-Type: image/jpeg

ÿØÿàJFIFÿÛ

  "" $(4,$&1'-=-157:::#+?D?8C49:7

[illegible]
```

Response:

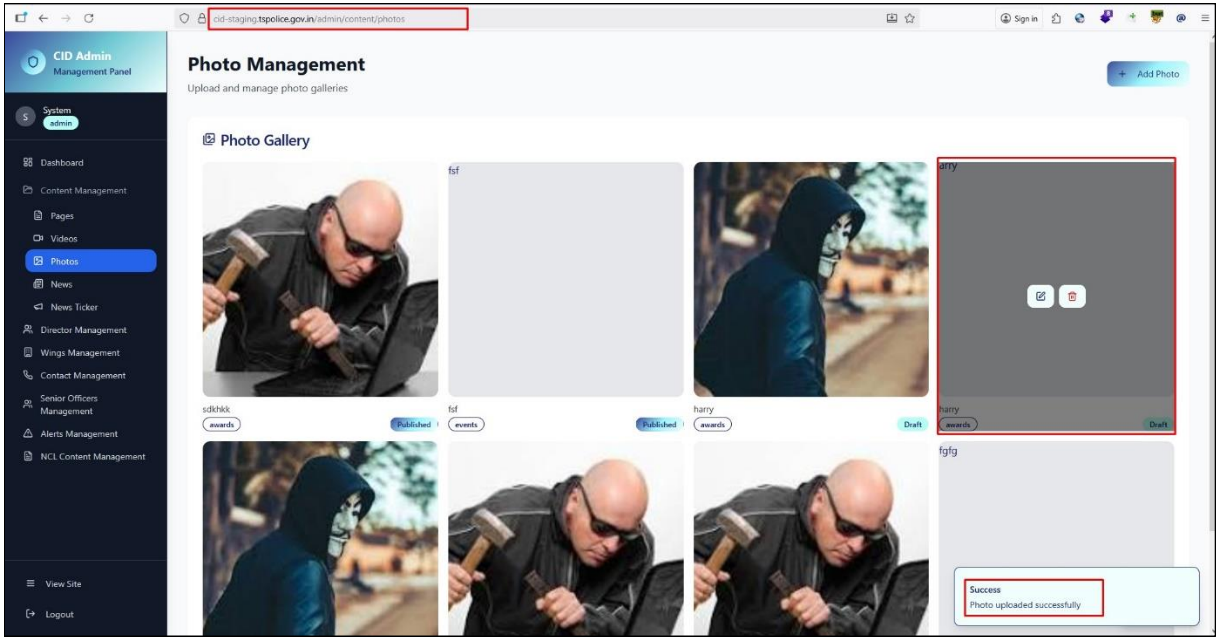
```
HTTP/2 200 OK
Server: nginx
Date: Tue, 14 Oct 2025 09:53:47 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 336
Content-Security-Policy: default-src 'self';style-src 'self' 'unsafe-inline' https://fonts.googleapis.com;font-src 'self' https://fonts.gstatic.com;script-src 'self';img-src 'self' data: https: blob:;connect-src 'self' ws: wss:;media-src 'self' blob:;object-src 'none';frame-src 'self';upgrade-insecure-requests;base-uri 'self';form-action 'self';frame-ancestors 'self';script-src-attr 'none'
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: strict-origin-when-cross-origin
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Dns-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: DENY
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode=block
Vary: Origin
Access-Control-Allow-Credentials: true
Ratelimit-Policy: 100;w=900
Ratelimit-Limit: 100
Ratelimit-Remaining: 97
Ratelimit-Reset: 871
Etag: W/"150-ede1m7J7tGLMaSvLEkX6j9eQopA"

{
  "id":27,
  "title":"harry",
  "description":"harry",
  "fileName":"photo-1760435627752-113254336.jpg",
  "filePath":"uploads/photo-1760435627752-113254336.jpg",
  "category":"awards",
  "isPublished":false,
  "displayOrder":2,
  "uploadedBy":"3ed49eec-6033-4303-aa12-52054303f02a",
  "createdAt":"2025-10-14T09:53:47.761Z",
  "updatedAt":"2025-10-14T09:53:47.761Z"
}
```

Step II: Add php payload in place of file we observed that the malicious file is successfully uploaded as shown in below snapshots:



```
POST /api/admin/photos HTTP/2
Host: cid-staging.tspolice.gov.in
Cookie: cid.session.id=s%3AdG810-RBOWIpJBW1-Cyni4AwZnQssvGK.vTYZhVj1%2Fm10GdGdY5YP4uMJmnhP18LGJZW2j6HmEY8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://cid-staging.tspolice.gov.in/admin/content/photos
Content-Type: multipart/form-data; boundary=----geckoformboundary914dd7e26e82a9fd71f231c5f85a576d
Content-Length: 1413
Origin: https://cid-staging.tspolice.gov.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

------geckoformboundary914dd7e26e82a9fd71f231c5f85a576d
Content-Disposition: form-data; name="photo"; filename="download.jpg"
Content-Type: image/jpeg

ÿØÿàJFIFÿÛ

  "" $(4,$&l'-=-157:::8+?D?8C49:7

<?php
$target_dir = "uploads/";
$target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
  $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
  if($check !== false) {
    echo "File is an image - " . $check["mime"] . ".";
    $uploadOk = 1;
  } else {
    echo "File is not an image.";
    $uploadOk = 0;
  }
}
?>
------geckoformboundary914dd7e26e82a9fd71f231c5f85a576d
Content-Disposition: form-data; name="title"

harry
------geckoformboundary914dd7e26e82a9fd71f231c5f85a576d
Content-Disposition: form-data; name="description"

harry
------geckoformboundary914dd7e26e82a9fd71f231c5f85a576d
Content-Disposition: form-data; name="category"

awards
```

```
HTTP/2 200 OK
Server: nginx
Date: Tue, 14 Oct 2025 09:54:42 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 336
Content-Security-Policy: default-src 'self';style-src 'self' 'unsafe-inline'
https://fonts.googleapis.com;font-src 'self' https://fonts.gstatic.com;script-src 'self';img-src 'self' data:
https: blob:;connect-src 'self' ws: wss:;media-src 'self' blob:;object-src 'none';frame-src
'self';upgrade-insecure-requests;base-uri 'self';form-action 'self';frame-ancestors 'self';script-src-attr
'none'
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: strict-origin-when-cross-origin
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Dns-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: DENY
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode=block
Vary: Origin
Access-Control-Allow-Credentials: true
Ratelimit-Policy: 100;w=900
Ratelimit-Limit: 100
Ratelimit-Remaining: 96
Ratelimit-Reset: 817
Etag: W/"150-CX0/Nc19yMBI0Koj/YQcK9kD8vo"

{
  "id":28,
  "title":"harry",
  "description":"harry",
  "fileName":"photo-1760435682547-926896389.jpg",
  "filePath":"uploads/photo-1760435682547-926896389.jpg",
  "category":"awards",
  "isPublished":false,
  "displayOrder":2,
  "uploadedBy":"3ed49eec-6033-4303-aa12-62054303f02a",
  "createdAt":"2025-10-14T09:54:42.551Z",
  "updatedAt":"2025-10-14T09:54:42.551Z"
}
```



Success
Photo uploaded successfully

Note: Kindly patch the issue throughout the application.

Case IV

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/api/admin/wings

ii. Observation/ Vulnerability title

Misconfigured CORS

iii. Detailed observation / Vulnerable point

Many modern websites use CORS to allow access from subdomains and trusted third parties. Their implementation of CORS may contain mistakes or be overly lenient to ensure that everything works, and this can result in exploitable vulnerabilities.

iv. CVE/CWE

CWE-942

v. Severity

Medium

vi. Recommendation

To mitigate CORS risks, avoid using Access-Control-Allow-Origin: * with Access-Control-Allow-Credentials: true. Instead, whitelist specific trusted origins and validate them server-side. Never reflect origins without checking. Only enable credentials if absolutely needed. This ensures secure cross-origin requests and protects against data leaks and unauthorized access.

vii. Reference

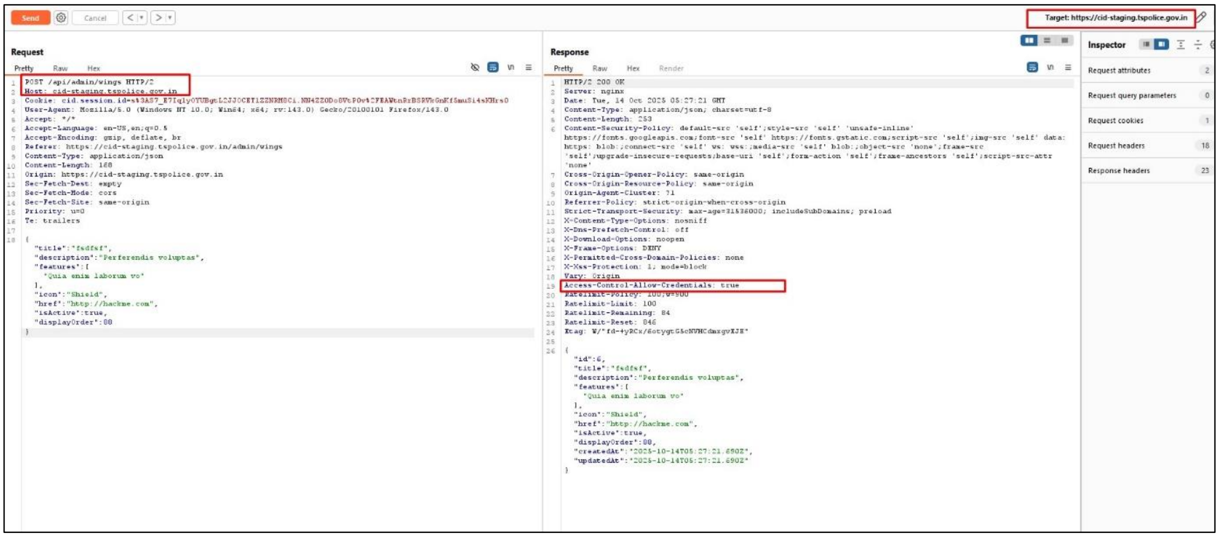
Case IV

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: Visit to the URL:**" https://cid-staging.tspolice.gov.in/api/admin/wings",** We observe that ACAC header is set to **"true"** as shown in below snapshot:



```
POST /api/admin/wings HTTP/2
Host: cid-staging.tspolice.gov.in
Cookie: cid.session.id=s%3AS7_E7Iqly0YUBgtL2JJOCET1ZZNRM8Ci.NN4ZZ0Do8VtPOv%2FEAWtnRrBSRVkGnKf5muSi4sKHrs0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://cid-staging.tspolice.gov.in/admin/wings
Content-Type: application/json
Content-Length: 168
Origin: https://cid-staging.tspolice.gov.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

{
  "title":"fsdfsf",
  "description":"Perferendis voluptas",
  "features":[
    "Quia enim laborum vo"
  ],
  "icon":"Shield",
  "href":"http://hackme.com",
  "isActive":true,
  "displayOrder":88
}
```

```
HTTP/2 200 OK
Server: nginx
Date: Tue, 14 Oct 2025 05:27:21 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 253
Content-Security-Policy: default-src 'self';style-src 'self' 'unsafe-inline'
https://fonts.googleapis.com;font-src 'self' https://fonts.gstatic.com;script-src 'self';img-src 'self' data:
https: blob:;connect-src 'self' ws: wss:;media-src 'self' blob:;object-src 'none';frame-src
'self';upgrade-insecure-requests;base-uri 'self';form-action 'self';frame-ancestors 'self';script-src-attr
'none'
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: strict-origin-when-cross-origin
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Dns-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: DENY
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode=block
Vary: Origin
Access-Control-Allow-Credentials: true
Ratelimit-Policy: 100;w=900
Ratelimit-Limit: 100
Ratelimit-Remaining: 84
Ratelimit-Reset: 846
Etag: W/"fd-+yRCx/6otygtG5cNVHCdmxgvEJE"

{
  "id":6,
  "title":"fsdfsf",
  "description":"Perferendis voluptas",
  "features":[
    "Quia enim laborum vo"
  ],
  "icon":"Shield",
  "href":"http://hackme.com",
  "isActive":true,
  "displayOrder":88,
  "createdAt":"2025-10-14T05:27:21.690Z",
  "updatedAt":"2025-10-14T05:27:21.690Z"
}
```

Note: Kindly patch this issue throughout the application.

Case V

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/admin/login

ii. Observation/ Vulnerability title

Weak Captcha Implemented

iii. Detailed observation / Vulnerable point

CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge-response test used by many web applications to ensure that the response is not generated by a computer. CAPTCHA implementations are often vulnerable to various kinds of attacks even if the generated CAPTCHA is unbreakable. A web application should implement captcha where login, registration pages are there.

iv. CVE/CWE

CWE-804

v. Severity

Medium

vi. Recommendation

Because the CAPTCHA cracking attacks are still improving (and will improve in the future), CAPTCHA should be perceived as a rate-limiting protection only.
If it is implemented, the following considerations should be taken into account:

- No CAPTCHA information (except the image itself) should be stored on the client side
- The client should have no "control" over the CAPTCHA content
- CAPTCHA images should be always randomly generated without possibility to perform image pre-processing, segmentation and classification
- CAPTCHA images should not be reused.

vii. Reference

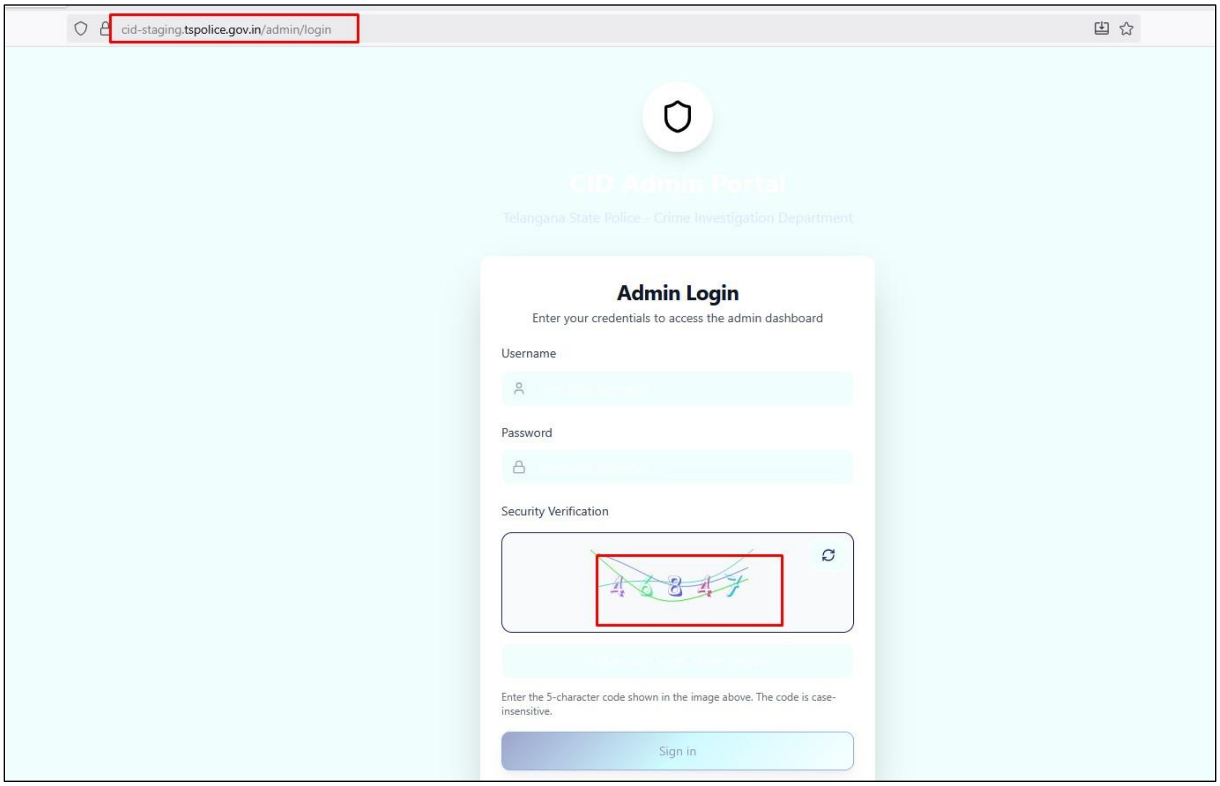
Case V

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: It was observed that weak captcha in implemented as shown in snapshot below:



cid-staging.tspolice.gov.in/admin/login

CID Admin Portal

Telangana State Police - Crime Investigation Department

Admin Login

Enter your credentials to access the admin dashboard

Username

Password

Security Verification

Enter the 5-character code shown in the image above. The code is case-insensitive.

Note: Kindly patch the issue throughout the application.

Case VI

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/admin/login

ii. Observation/ Vulnerability title

Session Replay

iii. Detailed observation / Vulnerable point

This attack targets the reuse of valid session ID to spoof the target system in order to gain privileges. The attacker tries to reuse a stolen session ID used previously during a transaction to perform spoofing and session hijacking. Another name for this type of attack is Session Replay.

iv. CVE/CWE

NA

v. Severity

Medium

vi. Recommendation

When the authenticated user logs off the application all its session variables are destroyed thus destroying the session token & the user mapping.

vii. Reference

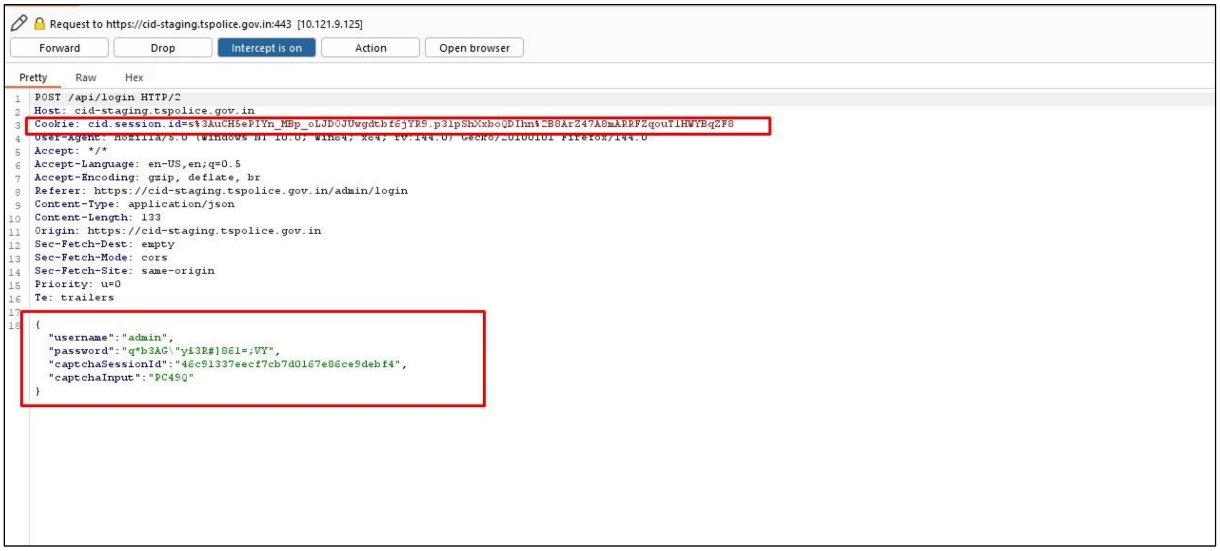
Case VI

viii. New or Repeat observation

New

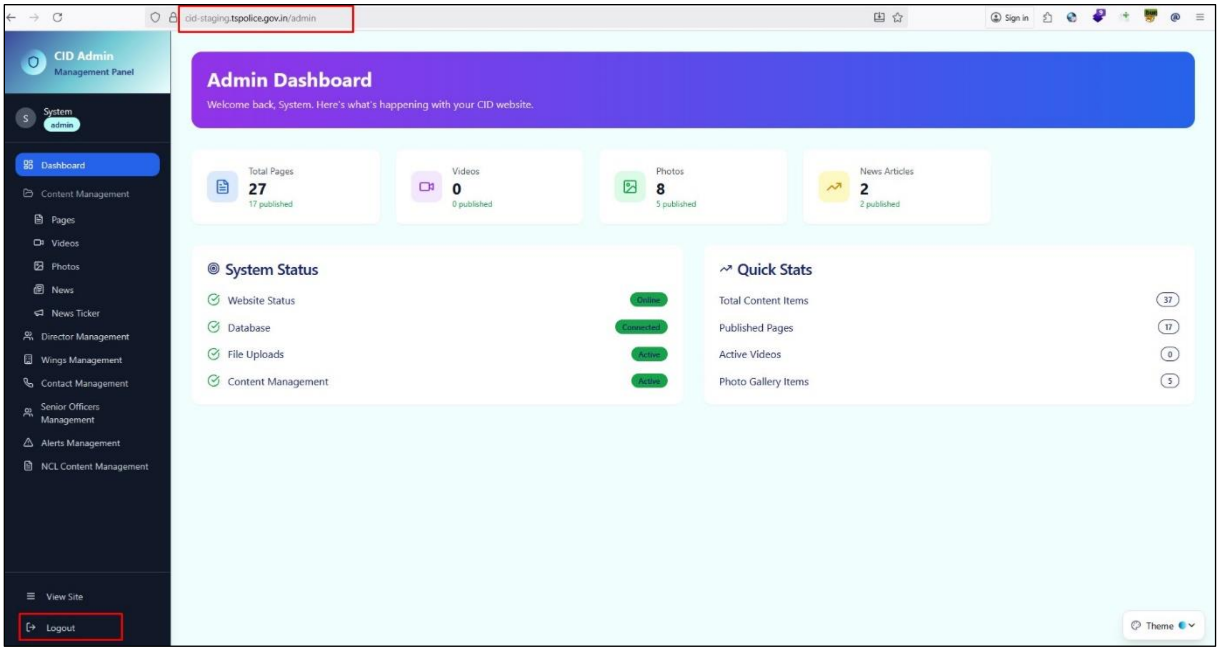
ix. References to evidence / Proof of Concept

Step II: Visit the URL: **"https://cid-staging.tspolice.gov.in/admin/login"** and capture the Pre-login Request and copy the Cookies now logout the user, as shown in below snapshots.



Request to https://cid-staging.tspolice.gov.in:443 [10.121.9.125]

```
POST /api/login HTTP/2
Host: cid-staging.tspolice.gov.in
Cookie: cid.session.id=s%3AuCH5ePIYn_MBp_oLJD0JUwgdtbf6jYR9.p31pShXxboQDIhn%2B8ArZ47A8mARRFZqouT1HWYBqZF8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://cid-staging.tspolice.gov.in/admin/login
Content-Type: application/json
Content-Length: 133
Origin: https://cid-staging.tspolice.gov.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

{
  "username":"admin",
  "password":"q*b3AG\"y£3R#]861=;VY",
  "captchaSessionId":"46c91337eecf7cb7d0167e86ce9debf4",
  "captchaInput":"PC49Q"
}
```



cid-staging.tspolice.gov.in/admin

Admin Dashboard

Welcome back, System. Here's what's happening with your CID website.

Total Pages	Videos	Photos	News Articles
27	0	8	2
17 published	0 published	5 published	2 published

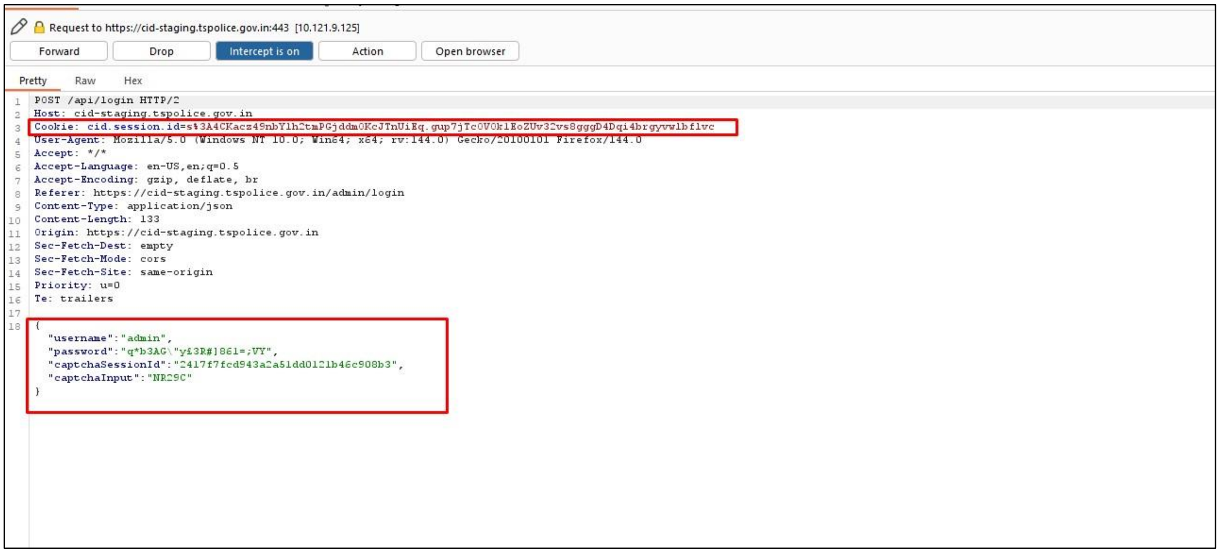
System Status

Website Status	Online
Database	Connected
File Uploads	Active
Content Management	Active

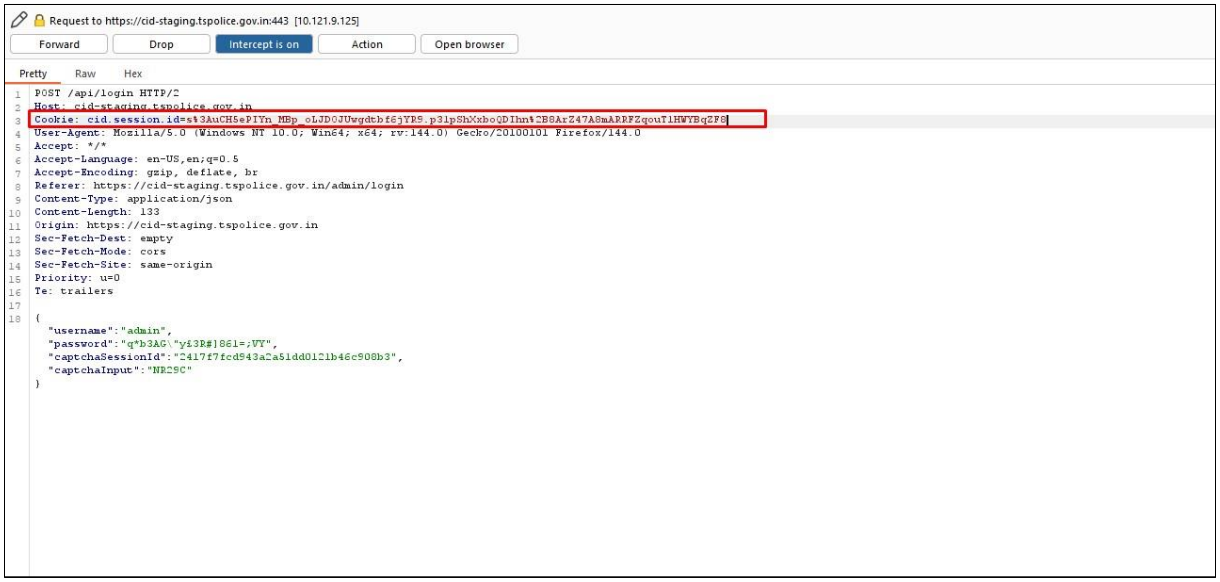
Quick Stats

Total Content Items	37
Published Pages	17
Active Videos	0
Photo Gallery Items	5

Step II: Now again login the same user and used the previous cookies in current session as we can observe that user is successfully login by previous cookies shown in below snapshots.


Request to https://cid-staging.tspolice.gov.in:443 [10.121.9.125]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex

```
POST /api/login HTTP/2
Host: cid-staging.tspolice.gov.in
Cookie: cid.session.id=s%3A4CKacz49nbYlh2tmPGjddm0KcJTnUiEq.gup7jTc0V0klEoZUv32vs8gggD4Dqi4brgyvwlbflvc
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://cid-staging.tspolice.gov.in/admin/login
Content-Type: application/json
Content-Length: 133
Origin: https://cid-staging.tspolice.gov.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

{
  "username":"admin",
  "password":"q*b3AG\"y£3R#]861=;VY",
  "captchaSessionId":"2417f7fcd943a2a51dd0121b46c908b3",
  "captchaInput":"NR29C"
}
```


Request to https://cid-staging.tspolice.gov.in:443 [10.121.9.125]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex

```
POST /api/login HTTP/2
Host: cid-staging.tspolice.gov.in
Cookie: cid.session.id=s%3AuCH5ePIYn_MBp_oLJD0JUwgdtbf6jYR9.p31pShXxboQDIhn%2B8ArZ47A8mARRFZqouTlHWYBqZF8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://cid-staging.tspolice.gov.in/admin/login
Content-Type: application/json
Content-Length: 133
Origin: https://cid-staging.tspolice.gov.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

{
  "username":"admin",
  "password":"q*b3AG\"y£3R#]861=;VY",
  "captchaSessionId":"2417f7fcd943a2a51dd0121b46c908b3",
  "captchaInput":"NR29C"
}
```

Case VII

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/duty-meet
https://cid-staging.tspolice.gov.in/economic-offences

ii. Observation/ Vulnerability title

Email Harvesting

iii. Detailed observation / Vulnerable point

An attacker can send SPAM mail to the application by using Email Harvester. The email harvesters are programs that scour the internet looking for email addresses on any website they come across.

iv. CVE/CWE

CWE-200

v. Severity

Low

vi. Recommendation

The application should properly customize the email addresses while posting on the website as: Email addresses should be posted as an image not as a hyperlink. Alternatively, instead of @symbol, [at] should be used. Similarly, the dot character (.) should be replaced by [dot]. So abc@nic.in should be written as abc[at]nic[dot]in.

vii. Reference

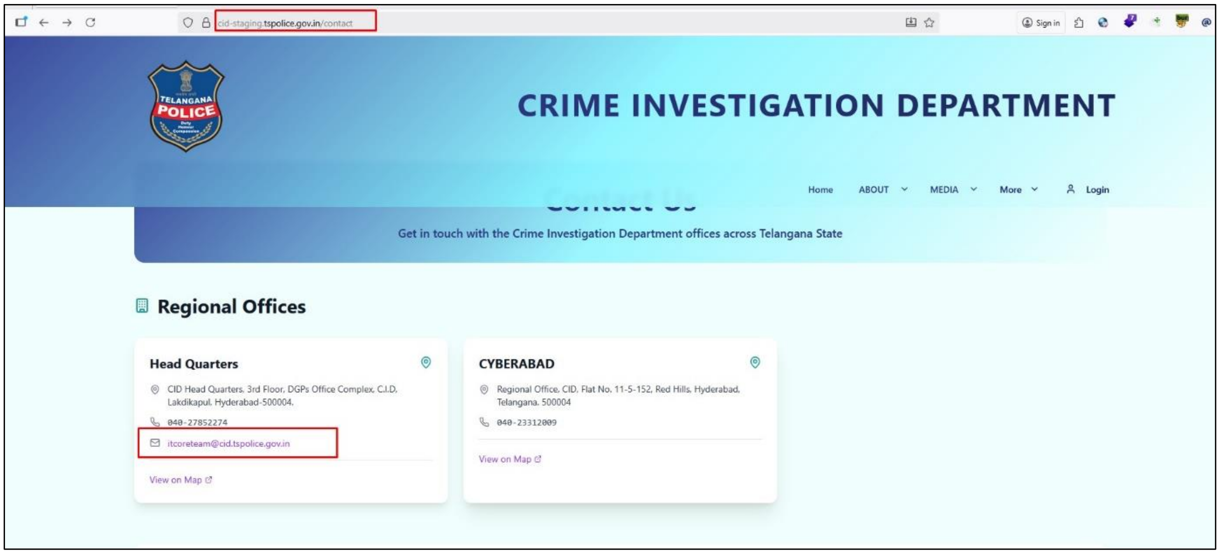
Case VII

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: Visit to the URL: **"https://cid-staging.tspolice.gov.in/duty-meet" "https://cid-staging.tspolice.gov.in/economic-offences"** and it is observed that emails   are in standard format as shown in below snapshots.



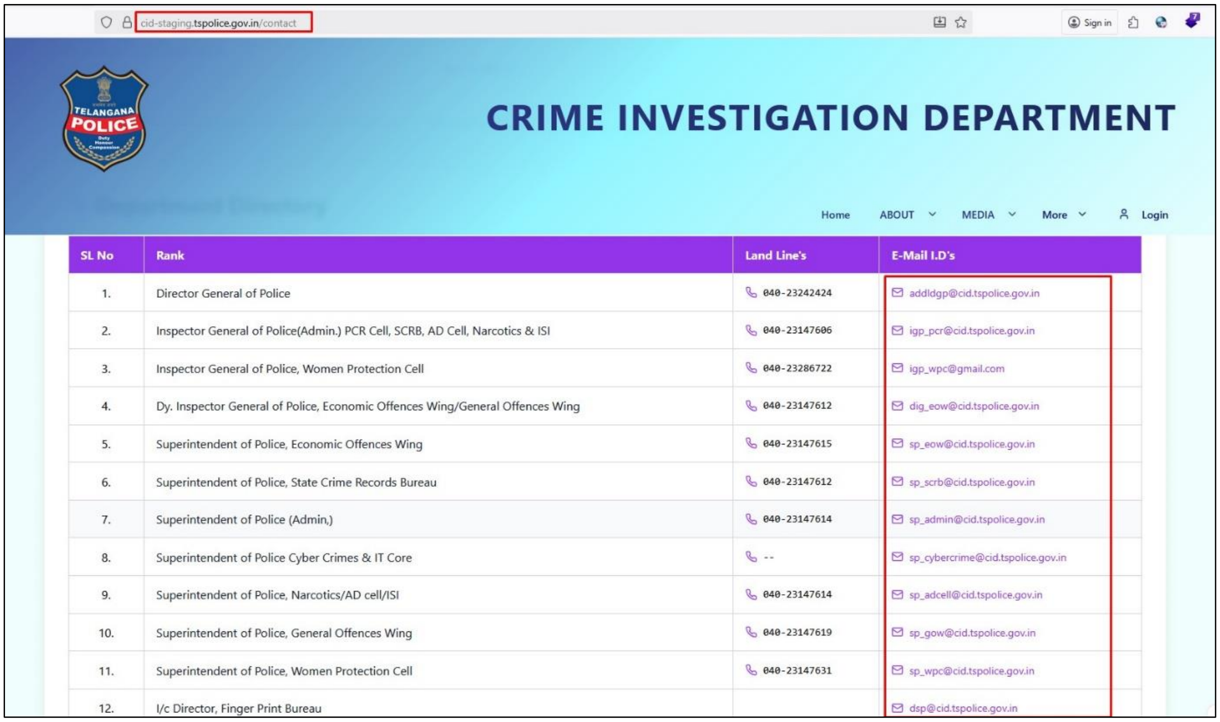
CRIME INVESTIGATION DEPARTMENT

Get in touch with the Crime Investigation Department offices across Telangana State

Regional Offices

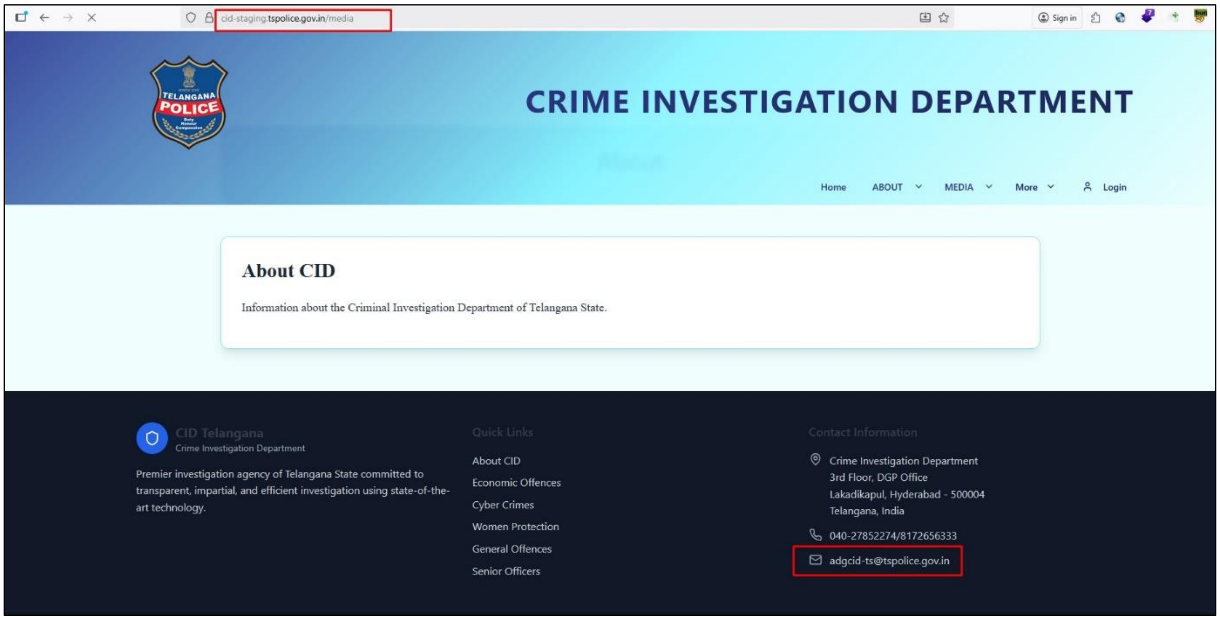
Head Quarters
CID Head Quarters, 3rd Floor, DGPs Office Complex, C.I.D, Lakdikapul, Hyderabad-500004.
040-27852274
itcoreteam@cid.tspolice.gov.in
View on Map

CYBERABAD
Regional Office, CID, Flat No. 11-5-152, Red Hills, Hyderabad, Telangana, 500004
040-23312009
View on Map



CRIME INVESTIGATION DEPARTMENT

SL No	Rank	Land Line's	E-Mail I.D's
1.	Director General of Police	040-23242424	addldgp@cid.tspolice.gov.in
2.	Inspector General of Police(Admin.) PCR Cell, SCRB, AD Cell, Narcotics & ISI	040-23147606	igp_pcr@cid.tspolice.gov.in
3.	Inspector General of Police, Women Protection Cell	040-23286722	igp_wpc@gmail.com
4.	Dy. Inspector General of Police, Economic Offences Wing/General Offences Wing	040-23147612	dig_eow@cid.tspolice.gov.in
5.	Superintendent of Police, Economic Offences Wing	040-23147615	sp_eow@cid.tspolice.gov.in
6.	Superintendent of Police, State Crime Records Bureau	040-23147612	sp_scrb@cid.tspolice.gov.in
7.	Superintendent of Police (Admin,)	040-23147614	sp_admin@cid.tspolice.gov.in
8.	Superintendent of Police Cyber Crimes & IT Core	--	sp_cybercrime@cid.tspolice.gov.in
9.	Superintendent of Police, Narcotics/AD cell/ISI	040-23147614	sp_adcell@cid.tspolice.gov.in
10.	Superintendent of Police, General Offences Wing	040-23147619	sp_gow@cid.tspolice.gov.in
11.	Superintendent of Police, Women Protection Cell	040-23147631	sp_wpc@cid.tspolice.gov.in
12.	I/c Director, Finger Print Bureau		dsp@cid.tspolice.gov.in


cid-staging.tspolice.gov.in/media
Sign in
TELANGANA
POLICE
CRIME INVESTIGATION DEPARTMENT
Home
ABOUT
MEDIA
More
Login

About CID

Information about the Criminal Investigation Department of Telangana State.

CID Telangana
Crime Investigation Department

Premier investigation agency of Telangana State committed to transparent, impartial, and efficient investigation using state-of-the-art technology.

Quick Links

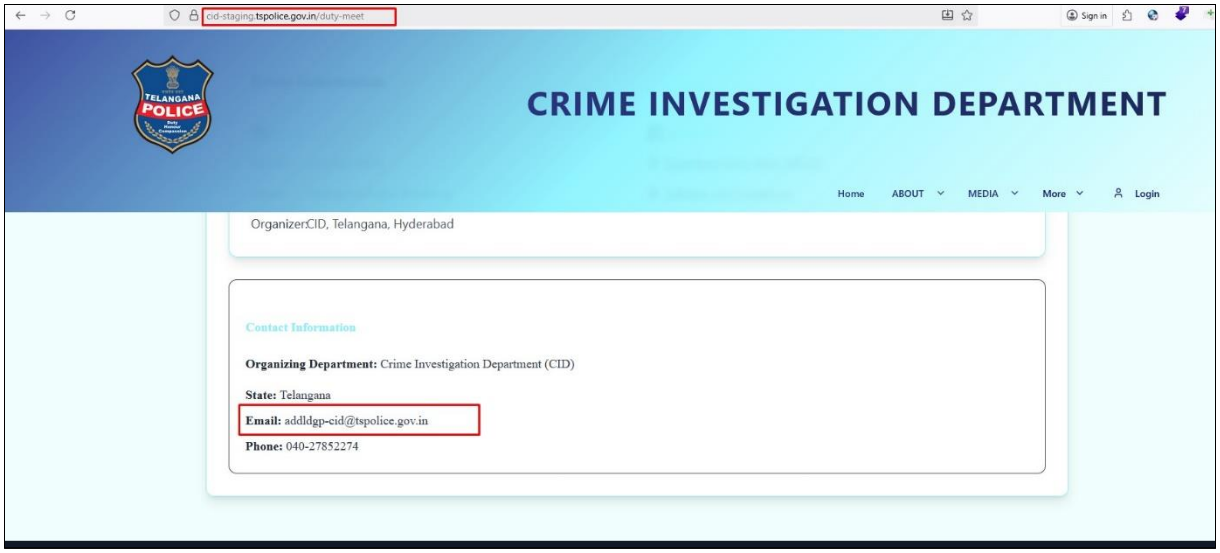
- About CID
- Economic Offences
- Cyber Crimes
- Women Protection
- General Offences
- Senior Officers

Contact Information

Crime Investigation Department
3rd Floor, DGP Office
Lakadikapul, Hyderabad - 500004
Telangana, India

040-27852274/8172656333

adgcid-ts@tspolice.gov.in


cid-staging.tspolice.gov.in/duty-meet
Sign in
TELANGANA
POLICE
CRIME INVESTIGATION DEPARTMENT
Home
ABOUT
MEDIA
More
Login

Organizer:CID, Telangana, Hyderabad

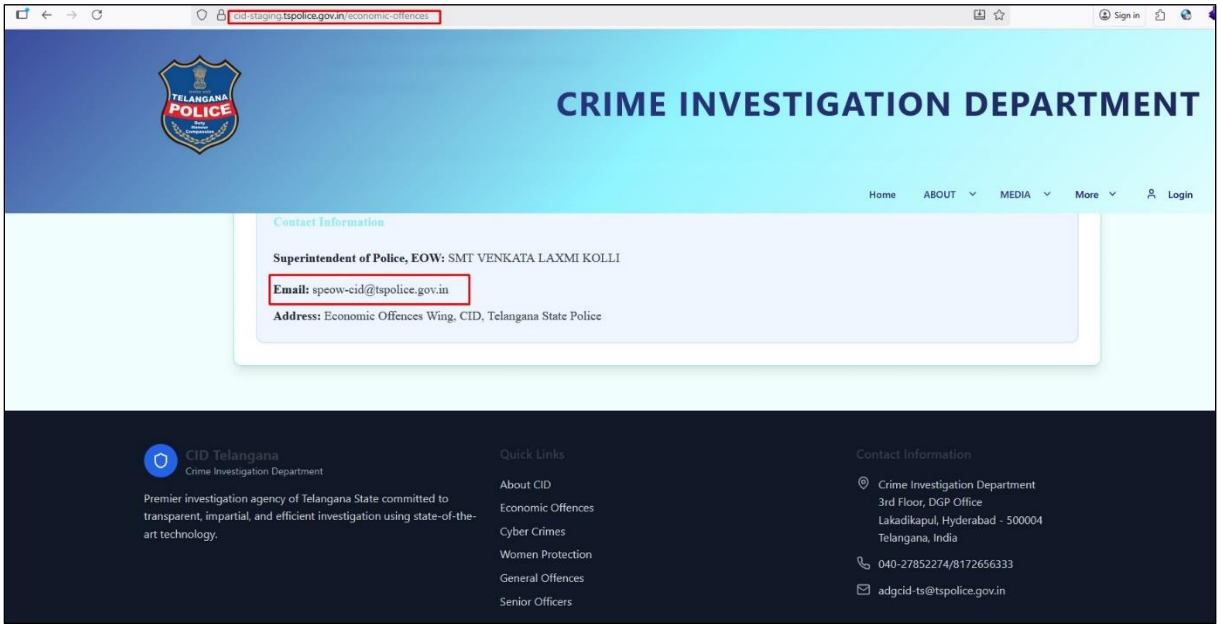
Contact Information

Organizing Department: Crime Investigation Department (CID)

State: Telangana

Email: addldgp-cid@tspolice.gov.in

Phone: 040-27852274



CRIME INVESTIGATION DEPARTMENT

Contact Information

Superintendent of Police, EOW: SMT VENKATA LAXMI KOLLI

Email: speow-cid@tspolice.gov.in

Address: Economic Offences Wing, CID, Telangana State Police

CID Telangana
Crime Investigation Department

Premier investigation agency of Telangana State committed to transparent, impartial, and efficient investigation using state-of-the-art technology.

Quick Links

- About CID
- Economic Offences
- Cyber Crimes
- Women Protection
- General Offences
- Senior Officers

Contact Information

Crime Investigation Department
3rd Floor, DGP Office
Lakadikapul, Hyderabad - 500004
Telangana, India

040-27852274/8172656333

adgcid-ts@tspolice.gov.in

Note: Kindly patch the issue throughout the application.

Case VIII

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/admin/login

ii. Observation/ Vulnerability title

Autocomplete Enabled on Password Field

iii. Detailed observation / Vulnerable point

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

iv. CVE/CWE

CWE-200

v. Severity

Low

vi. Recommendation

To prevent browsers from storing credentials entered into HTML forms, include the attribute autocomplete="off" within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

vii. Reference

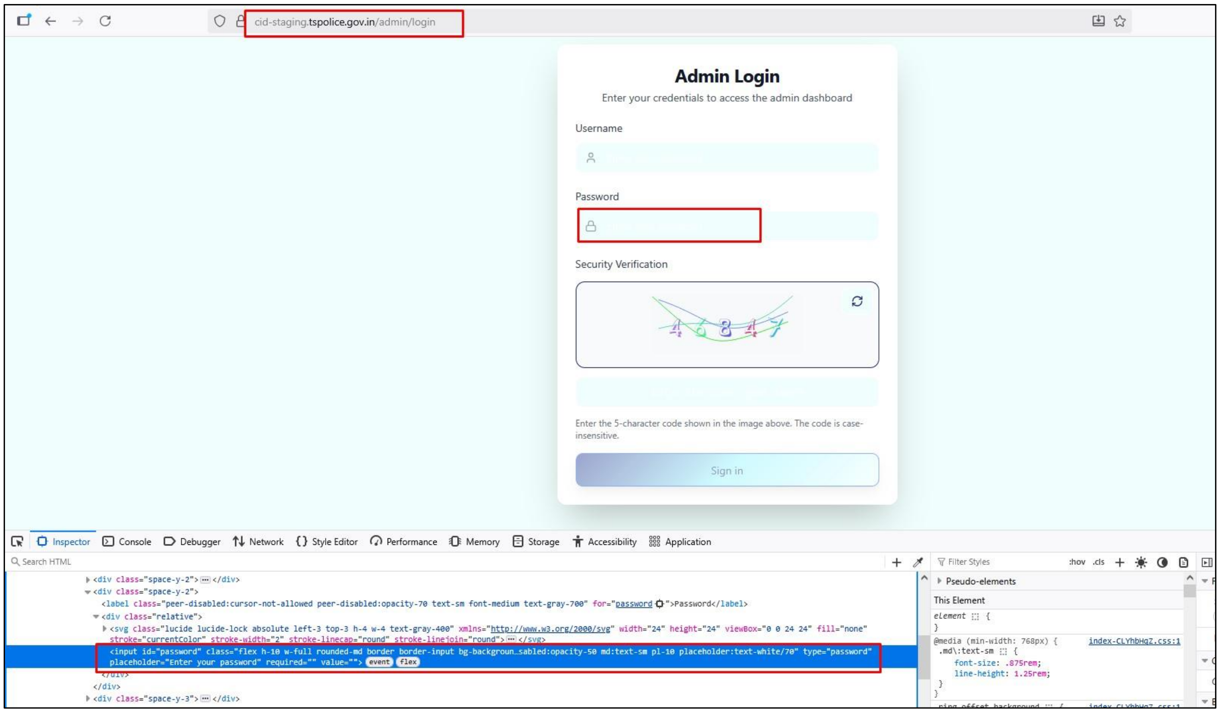
Case VIII

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: Visit to the login page **"https://cid-staging.tspolice.gov.in/admin/login"** and it is observed that autocomplete attribute is set to default settings as shown in below snapshot:



```
<div class="space-y-2"> ··· </div>
<div class="space-y-2">
  <label class="peer-disabled:cursor-not-allowed peer-disabled:opacity-70 text-sm font-medium text-gray-700" for="password">Password</label>
  <div class="relative">
    <svg class="lucide lucide-lock absolute left-3 top-3 h-4 w-4 text-gray-400" xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24" fill="none"
    stroke="currentColor" stroke-width="2" stroke-linecap="round" stroke-linejoin="round"> ··· </svg>
    <input id="password" class="flex h-10 w-full rounded-md border border-input bg-backgroun…sabled:opacity-50 md:text-sm pl-10 placeholder:text-white/70" type="password"
    placeholder="Enter your password" required="" value=""> event flex
  </div>
</div>
<div class="space-y-3"> ··· </div>
```

```
element {
}
@media (min-width: 768px) {        index-CLYhbHqZ.css:1
 .md\:text-sm {
    font-size: .875rem;
    line-height: 1.25rem;
 }
}
```

Case IX

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/admin/login

ii. Observation/ Vulnerability title

Cleartext Submission of Password

iii. Detailed observation / Vulnerable point

The application transmit password in cleartext format over HTTP which is an unencrypted connection.

iv. CVE/CWE

CWE-319

v. Severity

Low

vi. Recommendation

Implementation of salted SHA-256 or salted SHA-512 hashing algorithms on password fields, while using plain SHA-256 or SHA-512 hashing on new password fields.
If Salted Hashing is not possible, implement AES encryption with randomized padding.
Additionally, use latest stable version of TLS to protect all sensitive communications passing between the client and the server.
Implement HTTP Strict Transport Layer Security.
If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear-text HTTP.

vii. Reference

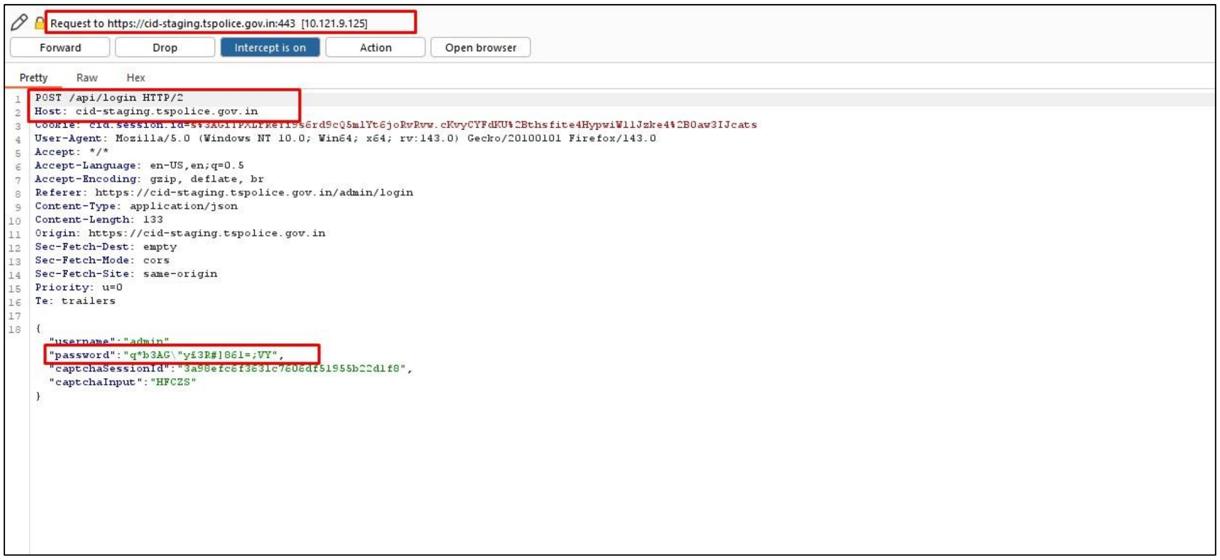
Case IX

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: Visit the URL: **“https://cid-staging.tspolice.gov.in/admin/login”** it was observed that password is travelling in cleartext as shown in snapshot below:



Request to https://cid-staging.tspolice.gov.in:443 [10.121.9.125]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex

```
POST /api/login HTTP/2
Host: cid-staging.tspolice.gov.in
Cookie: cid.session.id=s%3AGITPXLrReYI9s6rd9cQ5mlYt6joRvRvw.cKvyCYFdKU%2Bthsfite4HypwiW11Jzke4%2B0aw3IJcats
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://cid-staging.tspolice.gov.in/admin/login
Content-Type: application/json
Content-Length: 133
Origin: https://cid-staging.tspolice.gov.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

{
  "username":"admin",
  "password":"q*b3AG\"y£3R#]861=;VY",
  "captchaSessionId":"3a98efc6f3631c7606df51955b22d1f8",
  "captchaInput":"HFCZS"
}
```

Note: Kindly patch the issue throughout the application

Case X

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/

ii. Observation/ Vulnerability title

SSL/TLS Certificate Supports Older vers, CBC and Weak Cipher Algorithms

iii. Detailed observation / Vulnerable point

The remote host supports the use of SSL ciphers that offer weak encryption, usage of weak ciphers such as MD5, SHA1, TLS1.0, TLS 1.1 and Cipher Block Chaining (CBC) mode affect older versions of the protocol (TLSv1.2 and older). The attacker uses MITM to inject packets into the TLS stream. This allows them to guess the Initialization Vector (IV) used with the injected message and then simply compare the results to the ones of the block that they want to decrypt. The server is not configured with support for any modern, secure ciphers and only supports ciphers known to be weak against attack.

iv. CVE/CWE

CWE-327

v. Severity

Low

vi. Recommendation

Reconfigure the affected application, to avoid the use of weak ciphers such as SSL, MD5, SHA1, RC4, 3DES, Weak algorithms like TLS1.0, TLS1.1. Use only TLS 1.2, TLS 1.3

vii. Reference

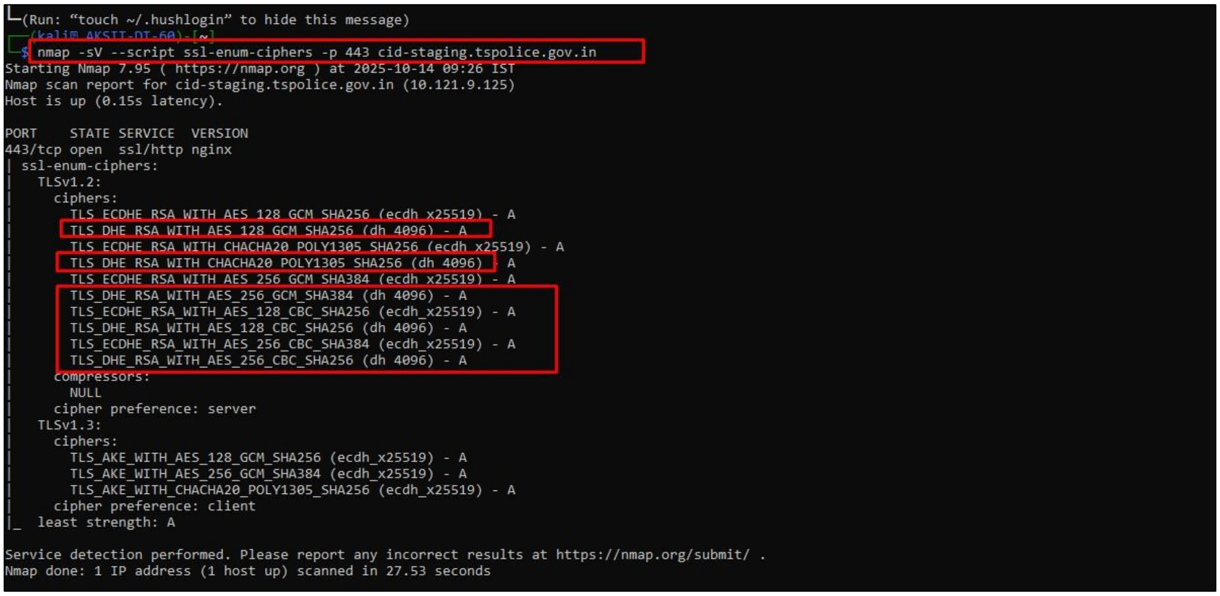
Case X

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: It is observed that application is using TLS 1.2 weak cipher suites as shown in below snapshots:



```
└─(Run: “touch ~/.hushlogin” to hide this message)
┌──(kali㉿AKSIT-DT-60)-[~]
└─$ nmap -sV --script ssl-enum-ciphers -p 443 cid-staging.tspolice.gov.in
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 09:26 IST
Nmap scan report for cid-staging.tspolice.gov.in (10.121.9.125)
Host is up (0.15s latency).

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http nginx
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 4096) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (dh 4096) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 4096) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 4096) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 4096) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|     cipher preference: client
|_  least strength: A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.53 seconds
```

Case XI

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/admin/login

ii. Observation/ Vulnerability title

Improper Session Timeout

iii. Detailed observation / Vulnerable point

The application does not automatically logs out the user after 20 mins of inactivity

iv. CVE/CWE

CWE-613

v. Severity

Low

vi. Recommendation

Application should automatically log out the user and destroy the session after 20 mins of inactivity.

vii. Reference

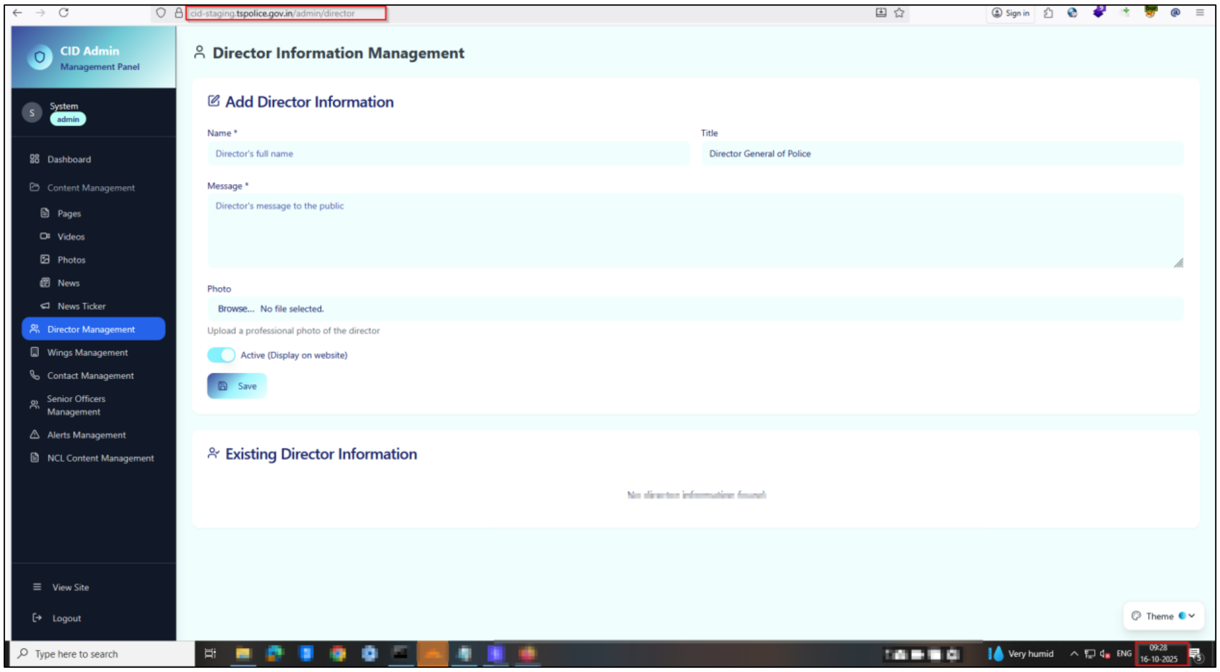
Case XI

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: It was observed that application does not logs out after 20 mins of inactivity:



cid-staging.tspolice.gov.in/admin/director

Director Information Management

Add Director Information

Name *: Director's full name

Title: Director General of Police

Message *: Director's message to the public

Photo: Browse... No file selected.

Upload a professional photo of the director

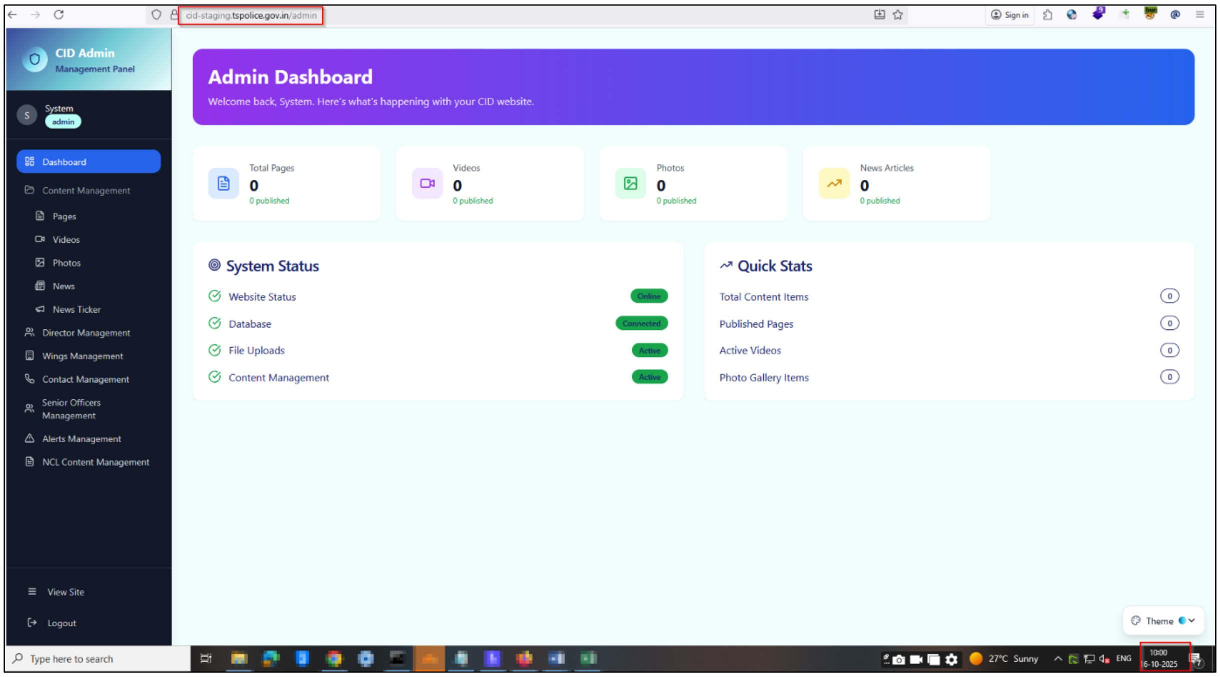
Active (Display on website)

Save

Existing Director Information

No director information found

09:28
16-10-2025



cid-staging.tspolice.gov.in/admin

Admin Dashboard

Welcome back, System. Here's what's happening with your CID website.

Total Pages	Videos	Photos	News Articles
0	0	0	0
0 published	0 published	0 published	0 published

System Status

Website Status	Online
Database	Connected
File Uploads	Active
Content Management	Active

Quick Stats

Total Content Items	0
Published Pages	0
Active Videos	0
Photo Gallery Items	0

10:00
16-10-2025

Case XII

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/admin/content/pages

ii. Observation/ Vulnerability title

Missing Cookies Attributes

iii. Detailed observation / Vulnerable point

Cookie do not have the proper attributes set. When the server responds with Set-Cookie header, it should assign the attributes of the cookies

iv. CVE/CWE

CWE-614

v. Severity

Low

vi. Recommendation

The secure flag should be set on all cookies that are being used for transmitting sensitive data when accessing content over HTTPS.

The SameSite should be set to Lax/Strict as required by the application.

The HttpOnly flag should be set on all cookies in order to prevent cookies accessed by javascript.

vii. Reference

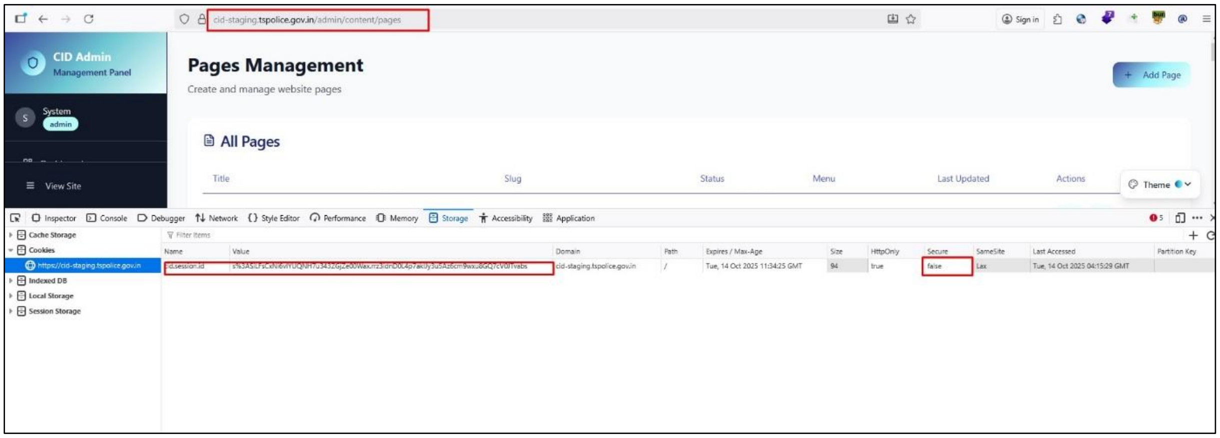
Case XII

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: Visit to the URL: **"https://cid-staging.tspolice.gov.in/admin/content/pages"** we observed that secure flag is false in cookies attributes as shown in below snapshot.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed	Partition Key
cid.session.id	s%3ASILFsCxNi6vlYUQNH7u3432Gj2e00Wax.rrz3idnD0L4p7akUy3u5Az6cm9wxu8GQ7cV0l1vabs	cid-staging.tspolice.gov.in	/	Tue, 14 Oct 2025 11:34:25 GMT	94	true	false	Lax	Tue, 14 Oct 2025 04:15:29 GMT	

Note: Kindly patch the issue throughout the application.

Case XIII

i. Affected Asset i.e. IP/URL/Application etc.

https://cid-staging.tspolice.gov.in/admin/login

ii. Observation/ Vulnerability title

Security Logging and Monitoring Failures

iii. Detailed observation / Vulnerable point

The application does not maintain any record of the application usage in the form of a report or audit trail. Any malicious activity cannot be monitored or traced back. In case of any misuse or attack, it may be difficult to trace and locate the origin.

iv. CVE/CWE

CWE-778

v. Severity

Low

vi. Recommendation

Information to be logged includes the following: IP address of the originating Source, Date, Time, Username (No Password), session details, Referrer, Process id, URL, User Agent, Countries if any in addition to other details to be logged in the website.
Logging of Authentication Process which includes number of successful and failed login attempts.
To create audit logs, use auto numbering so that every logged entry has an un-editable log number. Then if one audit entry is deleted a gap in the numbering sequence will appear.
Report of the website logs to be generated weekly by the administrator to keep track of the website activities.

vii. Reference

Case XIII

viii. New or Repeat observation

New

ix. References to evidence / Proof of Concept

Step I: if the logs are being maintained on the admin panel or server then kindly share a screenshot with us in the email.

Observation

Case I: Media Functionality is Not Working Properly.

Step I: Visit the URL: **"https://cid-staging.tspolice.gov.in/video-gallery**" visit to Media functionality and we can access the photo and video gallery, as shown in below snapshots

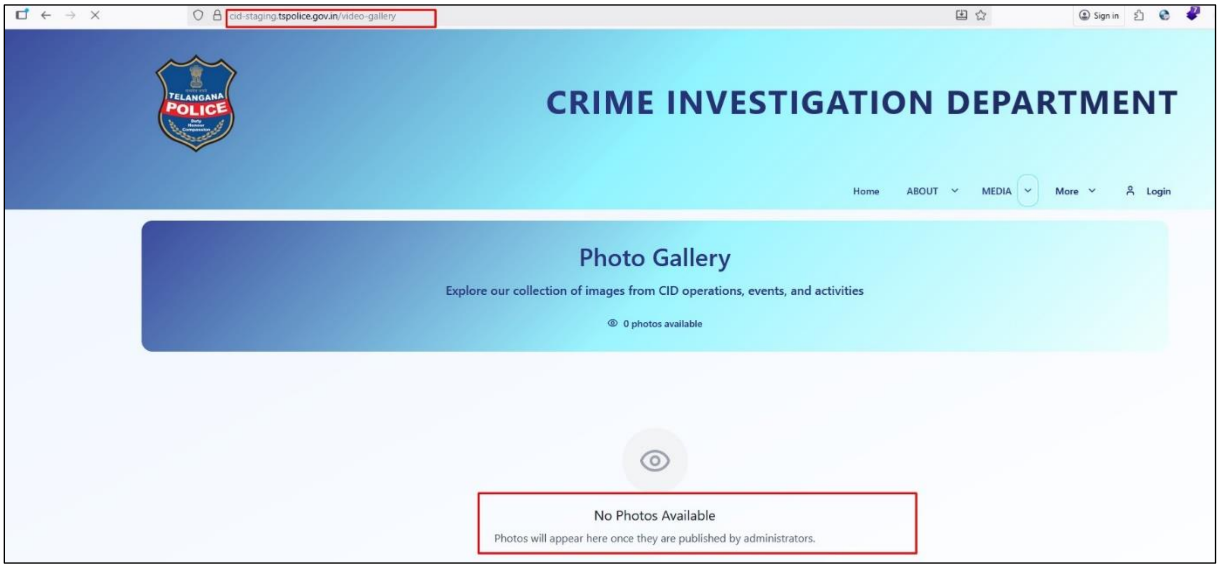

cid-staging.tspolice.gov.in/video-gallery
Sign in
TELANGANA POLICE
CRIME INVESTIGATION DEPARTMENT
Home
ABOUT
MEDIA
More
Login

Photo Gallery

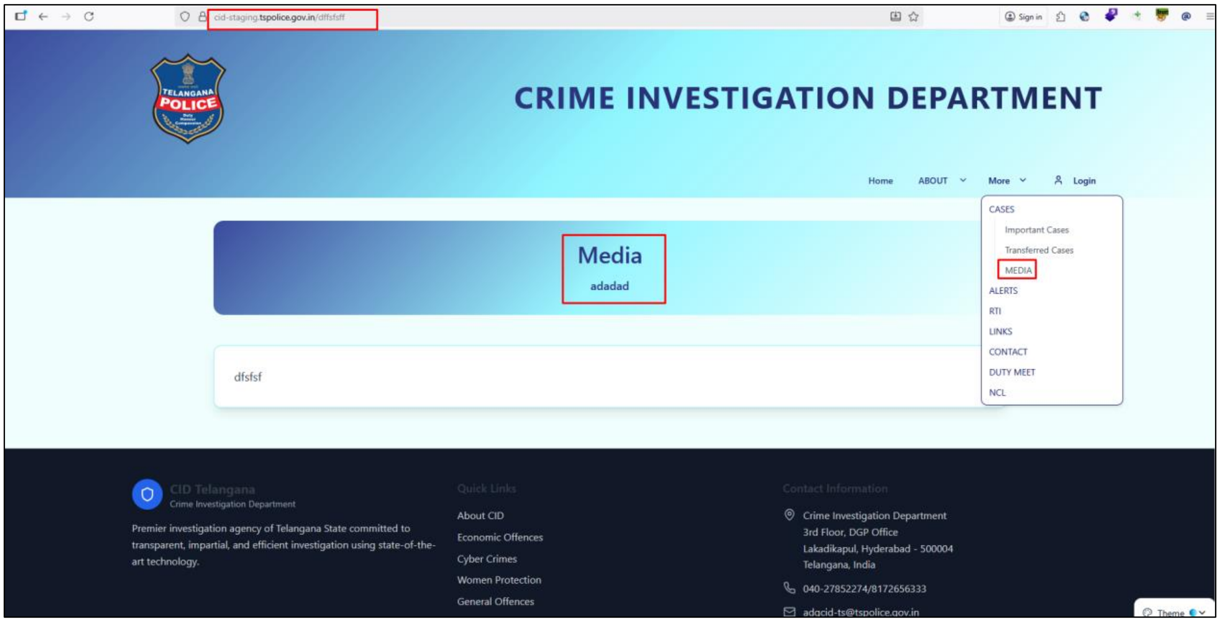
Explore our collection of images from CID operations, events, and activities

0 photos available

No Photos Available

Photos will appear here once they are published by administrators.

Step II: Now during the audit duration, in media functionality we unable to access the photo and video gallery as shown in below snapshot.



Media

adadad

dfsfsf

CID Telangana
Crime Investigation Department

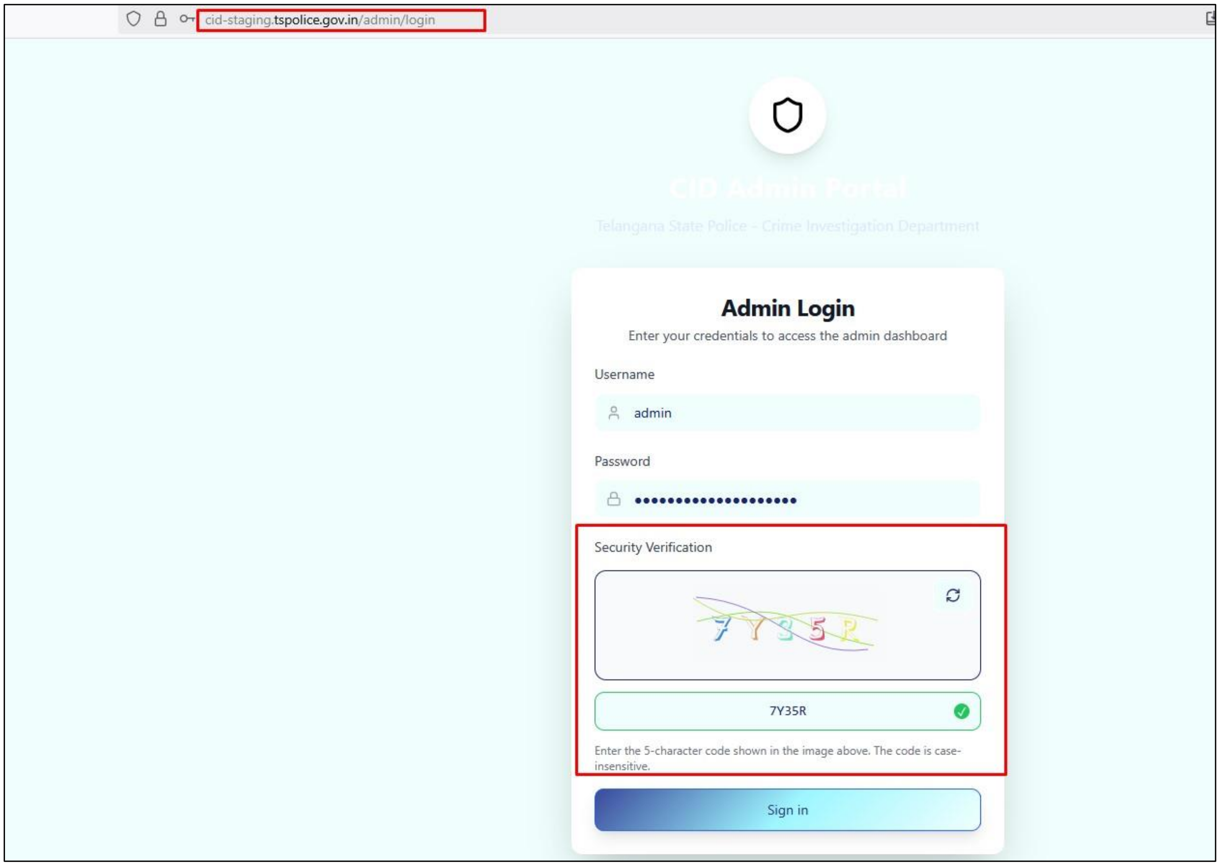
Premier investigation agency of Telangana State committed to transparent, impartial, and efficient investigation using state-of-the-art technology.

Quick Links
About CID
Economic Offences
Cyber Crimes
Women Protection
General Offences

Contact Information
Crime Investigation Department
3rd Floor, DGP Office
Lakadikapul, Hyderabad - 500004
Telangana, India
040-27852274/8172656333
adgcid-ts@tspolice.gov.in

Case II: Forget Password Functionality is Not Implemented.

Step I: Visit the URL: **"https://cid-staging.tspolice.gov.in/admin/login"** forget functionality is not implemented on login page as shown in below snapshot.



cid-staging.tspolice.gov.in/admin/login

CID Admin Portal

Telangana State Police – Crime Investigation Department

Admin Login

Enter your credentials to access the admin dashboard

Username

admin

Password

••••••••••••••••••••

Security Verification

7Y35R ✓

Enter the 5-character code shown in the image above. The code is case-insensitive.

Appendix 'A'

Tools Description

Burp Suite Professional

Portswigger's Burp Suite Professional is an advanced set of tools for testing web security. Burp Suite offers the features for both manual and automated scans. Through Burp Suite, a user can intercept HTTP traffic, find hidden attack surface, assess strength of tokens, perform brute-forcing and fuzzing, construct CSRF exploits, modify HTTP messages, scan for common vulnerabilities including the OWASP Standard.

Acunetix Vulnerability Scanner

Acunetix is a web vulnerability scanner which is also a complete Web Application security testing solution that can be used both standalone and as part of complex environments. It offers built-in vulnerability assessment and vulnerability management, as well as many options for integration with market-leading software development tools.

GoBuster

GoBuster is a command line scanner that looks for existing or hidden web objects. It works by launching a dictionary attack against a web server and analyzing the response. GoBuster is used to brute-force URIs (directories and files) and DNS subdomains.

SQLMAP

SQLMAP is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.