**Revalidation report for Web Application Security Audit Report: CID**

**Reference report used:** AKS Information Technology Services Pvt. Ltd

**Revalidation done on:** 29-10-25

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability ID** | **Severity** | **Initial Audit 16.10.2025** | **Revalidation 29-10-2025** |
| Case I | Medium | Open | Closed |
| Case II | Medium | Open | Open |
| Case III | Medium | Open | Open |
| Case IV | Medium | Open | Open |
| Case V | Medium | Open | Open |
| Case VI | Medium | Open | Open |
| Case VII | Low | Open | Closed |
| Case VIII | Low | Open | Closed |
| Case IX | Low | Open | Closed |
| Case X | Low | Open | Open |
| Case XI | Low | Open | Closed |
| Case XII | Low | Open | Open |
| Case XIII | Low | Open | Open |

**Finding / Title:** **Insecure HTTP Methods Enabled (Case I)**

**Screenshot:** A screenshot of a computer

AI-generated content may be incorrect.

**Status:** Fixed

**Finding / Title: Host Header Attack (Case II)**

**Screenshot:**

A screenshot of a computer

AI-generated content may be incorrect.  
  
**Status:** Not fixed

Impact:

* Host header poisoning can lead to cache poisoning or SSRF.
* Phishing links or password reset abuse using forged hosts.

Remediation:

* Validate Host header against a whitelist of allowed domains.
* Reject or normalize requests with unexpected Host values at the app or proxy.

**Finding / Title: Malicious File Upload (Case III)**

**Screenshot:**A screenshot of a computer

AI-generated content may be incorrect.

**Status:** Not fixed

Impact:

* Remote code execution or full server compromise if executed.
* Malware or defacement via uploaded malicious files.

Remediation:

* Enforce server-side allow-list for file types and validate MIME signatures.
* Store uploads outside webroot and set strict file permissions; scan uploads.

**Finding / Title: Misconfigured CORS (Case IV)**

**Screenshot:**A screenshot of a computer program

AI-generated content may be incorrect.

**Status:** Not fixed  
 **Impact:**

* Sensitive data may be exfiltrated by malicious origins.
* Cross-origin credential theft when combined with permissive CORS.

**Remediation:**

* Restrict Access-Control-Allow-Origin to trusted domains only.
* Disable Access-Control-Allow-Credentials for public endpoints or validate origins server-side.

**Finding / Title: Weak Captcha Implemented (Case V)**

**Screenshot:**A screenshot of a computer

AI-generated content may be incorrect.

**Status:** Not fixed

**Impact:**

* Automated CAPTCHA bypass can enable brute-force or spam.
* Account compromise or resource abuse at scale.

**Remediation:**

* Use proven CAPTCHA services or implement rate-limiting alongside CAPTCHA.
* Ensure CAPTCHA state is server-side and rotate challenges per request.

**Finding / Title: Session Replay (Case VI)**

**Screenshot:**A screenshot of a computer

AI-generated content may be incorrect.

**Status:** Not fixed

Impact:

* Session replay allows unauthorized access using stolen tokens.
* Account takeover without credential theft.

Remediation:

* Invalidate sessions on logout and use short, rotating session tokens.
* Bind sessions to client attributes (IP/user-agent) and implement replay protection.

**Finding / Title: Email Harvesting (Case VII)**

**Screenshot:**A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

**A screenshot of a computer

AI-generated content may be incorrect.**

**Status:** Fixed

**Finding / Title:** **Autocomplete Enabled on Password Field (Case VIII)**

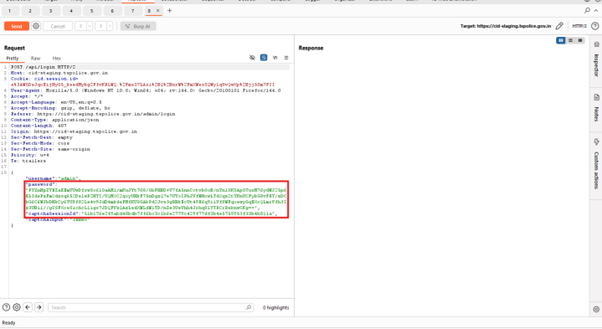
**Screenshot:**

A screenshot of a computer

AI-generated content may be incorrect.

**Status:** Fixed

**Finding / Title: Cleartext Submission of Password (Case IX)**

**Screenshot:**

**Status:** Fixed

**Finding / Title:** **SSL/TLS Certificate Supports Older vers, CBC and Weak Cipher Algorithms (Case X)**

**Screenshot:**A screenshot of a computer program

AI-generated content may be incorrect.

**Status:** Not fixedImpact:

* Weak TLS/ciphers allow downgrade or cryptographic attacks.
* Confidentiality and integrity of data may be compromised.

Remediation:

* Disable TLS 1.0/1.1 and weak cipher suites; enable TLS 1.2+ / TLS 1.3.
* Use modern cipher suites and follow server hardening benchmarks.

**Finding / Title: Improper Session Timeout (Case XI)**

**Screenshot:  
A screenshot of a computer

AI-generated content may be incorrect.  
Status:** Fixed

**Finding / Title: Missing Cookies Attributes (Case XII)**

**Screenshot:**A screenshot of a computer

AI-generated content may be incorrect.

**Status:** Not fixed

**Impact:**

* Cookies accessible to scripts or sent over insecure channels exposing sessions.
* Cross-site request forgery or session theft risks.

**Remediation:**

* Set Secure, HttpOnly, and appropriate SameSite attributes on cookies.
* Limit cookie scope (path/domain) and avoid storing sensitive data in cookies.