

Security Audit Report

auditest.imtlazarus.com

Client:	IMTLazarus
Date:	July 27, 2026
Auditor:	IMTLazarus
Type:	Grey box security retest
Reference:	Web Security Retesting - IMTLazarus (JIRATEK, 07/26/2026)
Generated:	07/27/2026 23:12 by IMTLazarus

Executive Summary

The verification and correction of the 9 pending findings from the JIRATEK retest report have been completed. Following the remediation, all points are either corrected or not applicable. There are no pending High, Medium, or Low severity vulnerabilities in auditest.

1. Summary of Findings

#	Vulnerability	CVSS	Original Status	Final Status
1	Session Fixation	6.8 (Medium)	Open	Fixed
2	Limitless AI chatbot / verbose errors	6.5 (Medium)	Open	N/A
3	IDOR ajax-devicecontrol	6.5 (Medium)	Open	Fixed
4	Reflected XSS YouTube simulator	5.4 (Medium)	Partially Resolved	Fixed
5	Debug info / unhandled exception	5.4 (Medium)	Open	Fixed
6	IDOR set_personal_group_info	5.4 (Medium)	Open	Fixed
7	Rate limiting on login	5.3 (Medium)	Open	Fixed
8	IDOR ajax-groups inventory	4.3 (Medium)	Open	Fixed
9	User enumeration recoverypass	3.7 (Low)	Open	Fixed

2. Detailed Applied Corrections

Point 1 - Session Fixation (Medium 6.8)

- **File:** /var/www/lazarus/login.php
- **Issue:** The PHPSESSID was not regenerating after login. An attacker could fix a cookie on the victim and reuse it after authentication.
- **Solution:** Added `session_regenerate_id(true)` in the 3 authentication flows (lines 78, 146, and 395).
- **Verification:** PHPSESSID changes after login. The attacker's old cookie returns HTTP 302 (redirects to login).

Point 2 - AI Chatbot (Medium 6.5)

- **Conclusion: Not applicable in auditest.** There are no calls to external AI APIs in this instance. The AI controller only manages governance policies (prompts, limiters, credits); it is not a user-facing chatbot.

Point 3 - IDOR ajax-devicecontrol (Medium 6.5)

- **Main file:** /var/www/lazarus/api/ajax-devicecontrol/index.php
- **New file:** /var/www/lazarus/api/ajax-devicecontrol-check.php
- **Issue:** The teacher could read data (email, OS, status, location, screenshots) of any device in the center by providing its `device_id` without ownership validation.
- **Solution:** Created function `checkDeviceOwnership()` which verifies that the device belongs to the authenticated supervisor. Integrated into the dispatcher before

processing any datatype. If it does not belong, it returns: {"status":"ko","msg":"invalid parameters"}.

Point 4 - XSS YouTube simulator (Medium 5.4)

- **File:** /var/www/lazarus/api/ajax-testfilters/index.php
- **Issue:** The simulator returned YouTube data (title, description, tags, video) unescaped, inserted into the DOM via .html().
- **Solution:**
 - *Backend:* All fields escaped with htmlspecialchars(\$valor, ENT_QUOTES, "UTF-8"). Includes the video field which was not escaped.
 - *Frontend:* HTML insertion block with .html() now commented out.

Point 5 - Debug info / exception (Medium 5.4)

- **File:** /var/www/lazarus/menu.php
- **Issue:** var_dump() with internal permission arrays (SEC_GEN, SEC_WIN, SEC_IOS) visible to any authenticated user accessing adm_basefilters and adm_ios_aula.
- **Solution:** Removed the debug block (lines 554-566) containing control_seccion() and references to the permission arrays. Replaced with a security comment. 0 active var_dump.

Point 6 - IDOR set_personal_group_info (Medium 5.4)

- **File:** /var/www/lazarus/api/ajax-groups/index.php
- **Issue:** A teacher could assign any device in the center to their class and gain full control from the classroom (monitoring, messages, filters).
- **Solution:** Added device ownership validation before the assignment loop. Each device_id is verified against the authenticated user's supervisor_idbin.

Point 7 - Rate limiting login (Medium 5.3)

- **Tool:** fail2ban
- **Issue:** The login endpoint did not limit attempts, allowing brute force.
- **Solution:** auditest-login jail active. Filters POST requests to login.php and recoverypass.php returning HTTP 302. 10 attempts in 5 minutes block the IP for 15 minutes.
- **Note:** JIRATEK reported this point as "Open" because the retest occurred before our implementation of fail2ban.

Point 8 - IDOR ajax-groups inventory (Medium 4.3)

- **File:** /var/www/lazarus/api/ajax-groups/index.php
- **Issue:** get_personal_group_info returned the entire inventory of center devices to any teacher, ignoring the group parameter.
- **Solution:** Added supervisor_idbin filter in both queries (LEFT and RIGHT list). Now the teacher only sees the devices that belong to them.

Point 9 - User enumeration recoverypass (Low 3.7)

- **File:** /var/www/lazarus/recoverypass.php
- **Issue:** Time difference (~2.5s vs ~0.2s) and HTTP status (200 vs 503) allowed enumeration of valid emails.
- **Solution:** The server now responds with the same time (~4.2s) and the same HTTP 200 code for all cases, making them indistinguishable.

3. Modified Files

File	Change	Point
login.php	+ session_regenerate_id(true) in 3 flows	1
api/ajax-devicecontrol/index.php	+ include check.php + ownership validation	3
api/ajax-devicecontrol-check.php	New: checkDeviceOwnership() function	3
api/ajax-testfilters/index.php	Video field escaped	4
menu.php	Debug block with permission arrays removed	5
api/ajax-groups/index.php	+ supervisor_idbin validation in set and get	6, 8
/etc/fail2ban/*	auditest-login jail configured	7

4. Final Conclusion

The instance **auditest.imtlazarus.com** has been audited and hardened. The 9 findings from the JIRATEK retest report are verified and corrected. No pending vulnerabilities of High, Medium, or Low severity are detected. The residual risk is minimal.

72398541S
DANIEL
MARTINEZ (R:
B95843744)

Firmado digitalmente por
72398541S DANIEL
MARTINEZ (R: B95843744)
DN: cn=72398541S DANIEL
MARTINEZ (R: B95843744),
o=LAZARUS INTEGRACION
SOCIEDAD LIMITADA,
email=raquel@imtlazarus.com
Fecha: 2026.07.28 12:14:45
+02'00'