22125005 - Mai Xuan Bach - HW1

Requirement 1: Job description

1. QA Manager (QA QC, Automation Test) – NAB Innovation Centre Vietnam

Link: https://itviec.com/it-jobs/qa-manager-qa-qc-automation-test-nab-innovation-centre-vietnam-5406 ITviec

- **Description / Role:** Manager level QA role overseeing QA/QC and automation in banking / financial tech domain.
- **Duties / Tasks:**
  - Lead quality management for large-scale products using modern technologies
  - Design QA/automation strategy, frameworks, test processes.
  - Stakeholder management & drive quality standards across teams.
- **Requirements / Qualifications:** experience in QA/QC & automation; leadership skills; familiarity with modern testing tools & practices; stakeholder & team management.
- **Salary / Benefits:** Not publicly disclosed in listing; “very competitive remuneration package” mentioned.
- **Other Benefits:** hybrid work, flexible working, career advancement.

---

2. 5 QA QC Engineer (Manual / Automation Tester) – Floating Cube Studios

Link: https://itviec.com/it-jobs/5-qa-qc-engineer-manual-automation-tester-floating-cube-studios-4659 ITviec

- **Description / Role:** Mid / mixed manual + automation QA role in a product company (POS / SaaS). ITviec
- **Duties / Tasks:**
  - Design / execute test cases (manual & automation).
  - Report / track defects.
  - Support QA process improvements.

- **Requirements / Qualifications:** experience in manual & automation testing; familiarity with Java, Selenium, Cucumber; detail-oriented.
- **Salary / Benefits:**
  - 13th month salary + loyalty bonus.
  - Bi-annual performance review
  - Premium health insurance, government insurance.

---

3. Automation Tester & Manual Tester (QA QC) – OnePay

Link: https://itviec.com/it-jobs/automation-tester-manual-tester-qa-qc-onepay-0734 ITviec

- **Description / Role:** QA role combining manual & automation testing across web, mobile, backend for financial / payments product.
- **Duties / Tasks:**
  - Design, execute, maintain test cases / test designs.
  - Report & track defects via tools (Jira / Redmine).
  - Ensure test coverage per system & functional requirements
  - Create automation scripts (Robot Framework or similar) where applicable.
  - Collaborate with internal teams for improvements & validation
- **Requirements / Qualifications:**
  - ≥ 1 year manual QA experience.
  - Knowledge of RESTful APIs, Postman, JMeter, web services
  - Some experience in automation testing preferred (Robot Framework, scripting).
  - Good English (reading, writing).
- **Salary / Benefits:** Not disclosed in listing.

---

4. Mid / Senior Quality Control Engineer (QA QC, Tester) – MODEC

Link: https://itviec.com/companies/modec ITviec

- **Description / Role:** QA / QC / Testing role in software (IT) domain likely within MODEC's software projects.
- **Duties / Tasks:** (implied from job type) test & assure product modules, detect bugs, work with dev teams, execute test plans

- **Requirements / Qualifications:** mid to senior experience in QA / testing; software / IT knowledge; test automation or manual skills.
- **Salary / Benefits:** Listed company benefits: 13th month, performance bonus, medical insurance, annual leave, etc.

---

5. QA / QC Engineer – Cigro Inc.

Link: https://itviec.com/companies/cigro-inc ITviec

- **Description / Role:** QA/QC role in B2B SaaS / software product company.
- **Duties / Tasks:** usability testing, coordinate test cycles, ensure conformity to product standards.
- **Requirements / Qualifications:** QA / testing experience, familiarity with usability testing, English optional but valuable.
- **Salary / Benefits:** Not publicly disclosed in listing.

---

6. Automation / Manual Tester (Playwright) – Groove Technology

Link: https://itviec.com/companies/groove-technology ITviec

- **Description / Role:** QA role focused on both automation & manual testing using Playwright.
- **Duties / Tasks:** design & execute automation scripts, perform manual test cases, ensure quality across product modules
- **Requirements / Qualifications:** experience with Playwright, JavaScript/TypeScript, QA testing in software contexts.
- **Salary / Benefits:** Not specified in listing.

---

7. Automation Test Engineer – KMS Technology

Link: https://careers.kms-technology.com/job/ (see "Automation Test Engineer") careers.kms-technology.com

- **Description / Role:** Automation test roles open in KMS across many levels (hybrid) in Ho Chi Minh / Da Nang
- **Duties / Tasks:** develop & maintain automated test frameworks; test scripts; verify features; collaboration with dev teams.

- **Requirements / Qualifications:** experience in automation testing, software QA methodologies. (Exact details on their page)
- **Salary / Benefits:** not publicly listed in that general job page.

---

8. Senior Automation QA Engineer (Remote / Vietnam) – Mindera

Link: https://remotive.com/remote/jobs/qa/senior-automation-qa-engineer-2436415 remotive.com

- **Description / Role:** Remote QA automation position for candidates in Vietnam.
- **Duties / Tasks:** design / implement automation test suites, ensure high code/test quality, collaborate in remote dev teams.
- **Requirements / Qualifications:** solid automation QA experience; ability to work distributed / remote; strong communication & development skills.
- **Salary / Benefits:** ~ **70 million VND/month** mentioned in listing.

---

9. QA Automation Intern – GeoComply, Ho Chi Minh

Link: https://www.geocomply.com/careers/all-jobs/ho-chi-minh-qa-automation-intern-fall-2025/ GeoComply

- **Description / Role:** Internship in QA / automation for software products. GeoComply
- **Duties / Tasks:** identify improvements in test process; research & implement tools; assist in automation tasks; support QA team.
- **Requirements / Qualifications:** interest / background in QA, basic programming or scripting ability, willingness to learn
- **Salary / Benefits:** Not disclosed in ad.

---

10. QA Engineer (remote / global) – Remote listing in Vietnam (via Himalayas)

Link: https://himalayas.app/jobs/countries/vietnam/qa-engineer Himalayas

- **Description / Role:** Remote QA Engineer roles targeting candidates based in Vietnam.
- **Duties / Tasks:** varies by role: test planning, automation & manual testing, usability, regression, performance testing.

- **Requirements / Qualifications:** QA / testing experience; remote work capability; good English and communication.
- **Salary / Benefits:** varies per employer; remote job perks (flexibility, location independence) typical.

Requirement 2: Software defects/bugs/errors

1. Apache Log4j “Log4Shell” Vulnerability (CVE-2021-44228)

- Source Link: https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-cve-2021-44228
- **Brief info:** “Log4Shell” (Apache Log4j CVE-2021-44228) — a critical remote code execution flaw in the ubiquitous Java logging library log4j, disclosed Dec 2021.
- **Severity:** Critical.
- **Consequences:** Wide exploitation across internet services; remote code execution leading to data theft, malware deployment, widespread emergency patching.
- **Solution:** Apply vendor/Apache patches (upgrade Log4j to fixed versions), follow CISA/Apache mitigation guidance (disable lookups, apply WAF rules).

---

2. Microsoft Exchange Server Zero-Day Attacks (Hafnium Campaign)

- Source Link: https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- **Brief info:** Microsoft reported a set of zero-day Exchange Server vulnerabilities (often called the “Hafnium” Exchange attacks, March 2021) that allowed remote code execution and server compromise.
- **Severity:** Critical.
- **Consequences:** Mass server compromises, webshell implants, email/data exfiltration in enterprise environments; urgent emergency patches and incident response across many organizations.
- **Solution:** Install Microsoft emergency patches, apply mitigations from Microsoft/CISA, scan for webshells and indicators of compromise and remediate infected systems.

---

3. Fastly CDN Global Outage (June 2021)

- Source Link: https://www.fastly.com/blog/summary-of-june-8-outage
- **Brief info:** Fastly CDN global outage (June 8, 2021) caused by an undiscovered software bug triggered by a valid customer configuration change.
- **Severity:** High (infrastructure).
- **Consequences:** Many major websites and services displayed “503” / became unavailable globally for ~45–60 minutes (news sites, e-commerce, streaming). Business disruption and visibility loss.
- **Solution:** Fastly rolled back/disabled the offending configuration, patched the bug; customers encouraged to apply multi-CDN redundancy and resilience plans.

---

4. Facebook, Instagram, WhatsApp Global Outage (October 2021)

- Source Link: https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/
- **Brief info:** Facebook / Instagram / WhatsApp global outage (Oct 4, 2021) — a routine maintenance/config change caused core backbone config to be withdrawn, removing BGP routes and DNS entries.
- **Severity:** Critical (major global service outage).
- **Consequences:** ~6–7 hour worldwide outage of Facebook services, loss of internal tools for employees, problems with 3rd-party sites using “Log in with Facebook”; major business & reputational impact.
- **Solution:** Repaired routing / DNS, restored services; Facebook committed to improving testing, drills, and change validation to prevent recurrence.

---

5. AWS Kinesis and Cloud Service Outage (November 2020)

- Source Link: https://www.reuters.com/business/media-telecom/amazons-cloud-service-sees-widespread-outage-2020-11-25/
- **Brief info:** AWS US-East partial outage (Nov 25, 2020) — Kinesis/other AWS services experienced failures that cascaded to many dependent applications.
- **Severity:** High.
- **Consequences:** Broad application outages across many websites/services that relied on affected AWS components; degraded customer experiences during peak shopping times.

- **Solution:** AWS incident response, service restoral and post-event summaries; customers advised to design cross-region redundancy and graceful degradation for critical services.

---

6. Zoom Zero-Day Vulnerabilities (April 2020

- Source Link: https://it.ucsb.edu/news/zoom-patches-released-zero-day-vulnerabilities
- **Brief info:** Zoom zero-day vulnerabilities (April 2020) — remote code execution and credential-theft flaws in the Zoom client were discovered and exploited.
- **Severity:** High.
- **Consequences:** Potential arbitrary code execution on user machines and credential theft; significant security concern as Zoom usage surged during COVID-19.
- **Solution:** Zoom released emergency patches; users required to update clients; security guidance included disabling vulnerable features and enabling automatic updates.

---

7. Datadog Multi-Region Connectivity Issue (March 2023)

- Source Link: https://www.datadoghq.com/blog/2023-03-08-multiregion-infrastructure-connectivity-issue/
- **Brief info:** Datadog multi-region infrastructure connectivity outage (March 8, 2023) — internal infrastructure connectivity issue impacted multiple Datadog regions and services.
- **Severity:** High (monitoring/observability platform).
- **Consequences:** Users lost access to monitoring dashboards and alerts; reduced visibility into production systems at a critical time, increasing operational risk for many orgs.
- **Solution:** Datadog restored connectivity, published a detailed post-incident report; customers advised to have secondary monitoring/alerting paths and incident playbooks.

---

8. Gmail Service Outage (July 2023)

- Source
  Link: https://www.google.com/appsstatus/dashboard/incidents/Hjq8CpkhWroicw7R1wSh
- **Brief info:** Gmail elevated errors/outage (July 6, 2023) — Google reported internal task issues causing intermittent unavailability for some Gmail functionalities.
- **Severity:** Medium–High (email service).

- **Consequences:** Delays sending/receiving, attachment upload failures, and syncing issues for impacted users for ~1–2 hours; business communications disrupted.
- **Solution:** Google engineers fixed the internal task problem; Google posted incident updates and recommended retrying operations after service restoration.

---

9. GitHub Major Outage (August 2024)

- Source Link: https://www.theverge.com/2024/8/14/24220685/github-down-website-pull-request
- **Brief info:** GitHub major outage (Aug 14, 2024) — database infrastructure changes caused degraded availability across web UI, pull requests, Pages and other features.
- **Severity:** High (developer platform).
- **Consequences:** Developers could not create or view PRs, issues, or push changes in some cases—blocking CI/CD and releases for affected teams.
- **Solution:** GitHub rolled back problematic DB changes, restored services, and published availability reports with follow-ups to improve change controls.

---

10. Windows 10 Update KB5000802 Causing BSOD When Printing (March 2021)

- Source Link: https://www.windowscentral.com/how-uninstall-update-kb5000802-fix-blue-screen-problems-windows-10
- **Brief info:** Windows 10 cumulative update KB5000802 (March 2021) caused BSOD (APC_INDEX_MISMATCH) when printing with certain printer drivers, crashing systems.
- **Severity:** Medium–High (end-user impact).
- **Consequences:** Blue Screen of Death on affected PCs when printing — disrupted business workflows and required rollback/repairs for many users.
- **Solution:** Microsoft pulled the problematic update from auto-push, issued guidance and hotfixes; recommended uninstalling the update or applying vendor driver updates / Microsoft patch when available.

11. Critical GoAnywhere Managed File Transfer Vulnerability (CVE-2025-10035)

- Source Link: https://www.bleepingcomputer.com/news/security/fortra-warns-of-new-goanywhere-mft-rce-vulnerability-cve-2025-10035/

- **Brief info:** A newly disclosed remote code execution (RCE) flaw in GoAnywhere MFT (file transfer software by Fortra) allowed attackers to run arbitrary commands on unpatched servers.
- **Severity:** Critical.
- **Consequences:** Used by ransomware groups to steal data from enterprises; significant data breach risks in financial and healthcare sectors.
- **Solution:** Fortra released patches and advised disabling administrative consoles from public access; organizations urged to update immediately.

12. Windows 11 “Update and Shutdown” Function Bug (Restart Instead of Shut Down)

- Source Link: https://www.windowslatest.com/2023/10/08/windows-11-bug-causes-update-and-shutdown-to-reboot-pcs/
- **Brief info:** Windows 11 users reported that selecting “Update and shut down” instead triggered a reboot instead of shutting down the system.
- **Severity:** Low–Medium.
- **Consequences:** User frustration and confusion; wasted power and disruptions to automated tasks.
- **Solution:** Microsoft acknowledged the issue and provided guidance to disable fast startup or use alternative shutdown commands until a patch was rolled out.

13. Slack Hashed Password Exposure via Shared Invite Link Bug

- Source Link: https://slack.com/blog/news/slack-security-update-on-password-hash-exposure
- **Brief info:** Slack discovered a bug where hashed user passwords were included in invite links shared between April 2017 and July 2022.
- **Severity:** Medium.
- **Consequences:** Although hashes were encrypted, exposure risked potential brute-force cracking; affected users were automatically reset.
- **Solution:** Slack fixed the bug, revoked all affected links, and forced password resets for users potentially impacted.

14. macOS Ventura Restriction Bug on Third-Party Security Tools

- Source Link: https://arstechnica.com/gadgets/2022/10/macos-ventura-bug-blocks-third-party-security-tools/
- **Brief info:** macOS Ventura introduced a bug that prevented third-party security monitoring tools from accessing full disk or process data, disrupting endpoint protection.
- **Severity:** Medium–High.
- **Consequences:** Reduced effectiveness of antivirus, intrusion detection, and monitoring apps; potential blind spots for enterprise IT admins.
- **Solution:** Apple addressed the bug in subsequent macOS updates; developers provided temporary workarounds to restore limited access.

15. LogoFAIL UEFI Boot Logo Firmware Vulnerability (CVE-2023-40238)

- Source Link: https://www.securityweek.com/logofail-vulnerabilities-impact-uefi-firmware-from-major-vendors/
- **Brief info:** LogoFAIL was a series of vulnerabilities in UEFI firmware image parsers that could allow attackers to execute code during early boot by using malicious logo images.
- **Severity:** Critical (firmware-level).
- **Consequences:** Potential for persistent malware infections that survive OS reinstallations; affects devices from Dell, Lenovo, and others.
- **Solution:** Firmware vendors issued BIOS/UEFI updates; users urged to apply OEM patches immediately.

16. PrintNightmare Windows Print Spooler Remote Code Execution & Privilege Escalation

- Source Link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
- **Brief info:** A major vulnerability in Windows Print Spooler service (CVE-2021-34527) allowed remote or local attackers to gain SYSTEM privileges.
- **Severity:** Critical.
- **Consequences:** Widely exploited for privilege escalation in corporate networks; affected almost all supported Windows versions.

- **Solution:** Microsoft released multiple security patches and advised disabling the Print Spooler service on non-print servers as mitigation.

17. aCropalypse Screenshot Vulnerability (Android / Windows Tools)

- Source Link: https://www.theverge.com/2023/3/20/23648126/google-pixel-acropalypse-bug-png-edit-vulnerability
- **Brief info:** The aCropalypse bug in Android Pixel's Markup tool and Windows Snipping Tool allowed cropped or edited screenshots to still contain recoverable image data.
- **Severity:** Medium–High.
- **Consequences:** Sensitive redacted information (emails, faces, etc.) could be recovered; significant privacy implications.
- **Solution:** Google and Microsoft released patches; users advised to re-upload re-cropped images after updates.

18. "Downfall" CPU Speculative Execution Vulnerability (Intel Processors)

- Source Link: https://downfall.page/
- **Brief info:** Downfall (CVE-2022-40982) was a vulnerability in Intel CPUs allowing data leakage between users via speculative execution flaws.
- **Severity:** High.
- **Consequences:** Potential exposure of sensitive data across virtual machines, cloud tenants, or applications sharing the same CPU.
- **Solution:** Intel released microcode updates; OS vendors applied mitigations to limit the performance impact.

19. CrowdStrike Rapid Response Update Causing Windows Global Blue Screen Outage (July 2024)

- Source Link: https://www.reuters.com/technology/crowdstrike-says-fixes-issued-after-outage-hits-windows-systems-2024-07-19/
- **Brief info:** A faulty CrowdStrike Falcon sensor update caused mass Windows BSODs (Blue Screen of Death) globally in July 2024.
- **Severity:** Critical.

- **Consequences:** Massive downtime for airlines, hospitals, and enterprises as Windows machines crashed and rebooted endlessly.
- **Solution:** CrowdStrike issued a corrected update and detailed recovery steps; manual intervention was required to remove faulty driver files.

20. Microsoft “Follina” MSDT Zero-Day Vulnerability (CVE-2022-30190)

- Source Link: https://www.cisa.gov/news-events/alerts/2022/06/01/microsoft-msdt-zero-day-vulnerability
- **Brief info:** “Follina” was a zero-day in Microsoft’s MSDT (Microsoft Support Diagnostic Tool) exploited through malicious Word documents to execute arbitrary code.
- **Severity:** Critical.
- **Consequences:** Used in phishing attacks to deliver malware and remote control payloads; affected many Office versions.
- **Solution:** Microsoft released security patches and urged users to disable the MSDT URL protocol handler until fixed.

Requirement 3: Test case Design

1. Test Case: Power ON/OFF Function

- **Test Objective:** Verify that the fan turns ON and OFF correctly using the power switch.
- **Input:**
  - Requirement: Fan connected to power source.
  - Step: Toggle the ON/OFF switch.
- **Expected Output:**
  - Fan starts rotating when turned ON.
  - Fan stops rotating immediately when turned OFF.

---

2. Test Case: Speed Control Functionality

- **Test Objective:** Ensure that all fan speed levels work correctly.
- **Input:**

- Step: Set speed knob/button to Level 1 → Level 2 → Level 3 (or min → max).

- **Expected Output:**
  - Fan rotates at visibly increasing speeds according to the selected level.

---

3. Test Case: Direction of Rotation

- **Test Objective:** Verify that the fan rotates in the correct direction (usually counterclockwise for cooling mode).
- **Input:**
  - Step: Turn on fan and observe blade direction.
- **Expected Output:**
  - Fan rotates counterclockwise in cooling mode and clockwise in reverse mode (if available).

---

4. Test Case: Remote Control / Wall Control Response

- **Test Objective:** Validate that the fan responds to remote or wall control signals.
- **Input:**
  - Step: Use remote control to switch ON/OFF and change speed levels.
- **Expected Output:**
  - Fan responds accurately to each remote command with minimal delay (<1 second).

---

5. Test Case: Power Failure Recovery

- **Test Objective:** Check the fan’s behavior after a sudden power loss.
- **Input:**
  - Step: Turn on the fan, simulate power outage, then restore power.
- **Expected Output:**
  - Fan remains OFF after power restoration (if designed to reset) or resumes last speed (if memory feature enabled).

---

6. Test Case: Overheating Protection

- **Test Objective:** Ensure fan motor shuts down or limits performance when overheating occurs.
- **Input:**
  - Step: Run fan continuously for extended period (e.g., 8 hours).
- **Expected Output:**
  - Fan continues normal operation without overheating or automatically turns off if unsafe temperature detected.

---

7. Test Case: Noise Level Check

- **Test Objective:** Verify that noise level is within acceptable limits.
- **Input:**
  - Environment: Quiet room, sound meter.
  - Step: Measure noise at each speed level.
- **Expected Output:**
  - Noise level ≤ manufacturer's specification (e.g., <50 dB at max speed).

---

8. Test Case: Wobbling / Vibration Test

- **Test Objective:** Check fan stability and balance during operation.
- **Input:**
  - Step: Observe fan rotation at all speeds.
- **Expected Output:**
  - Fan blades remain stable without visible wobbling or vibration.

---

9. Test Case: Reverse Mode Operation

- **Test Objective:** Validate the reverse rotation mode (for winter use, if supported).
- **Input:**
  - Step: Activate reverse mode switch/remote button.
- **Expected Output:**
  - Fan rotates clockwise; airflow direction reversed without unusual noise.

---

10. Test Case: Safety Compliance (Blade Guard & Shock Prevention)

- **Test Objective:** Ensure user safety features are functioning.
- **Input:**
  - Environment: Power ON, inspect blade area and housing.
  - Step: Simulate light touch near motor housing and switches.
- **Expected Output:**
  - No electrical shock, proper insulation, and blades safely out of reach.

Self-Assessment

Requirement	Outcomes (Brief description about what you get from each requirement)	Grade	Self-Assessed Grade
1	**Job Description**	**40**	40
	10 jobs * (title + summary + link + task list / duties + requirements, salary range, benefits)	10 * 4	
2	**Software bugs**	**30**	30
	20 bugs * (Source Link to the news/report + Brief information about the defect + Assess the severity + The consequences caused + Solution)	20 * 1.5	
3	**Test Design**	**30**	30
	10 test cases * (Test Objective, Input, Expected Output)	10 * 3	
	Total	**100**	100