

Yash Mehta

Security Tester · FICTIONAL SAMPLE

Indore, India

Skills

authorised application testing

Applied to tenant isolation assessment through documented preparation, execution and review.

access-control testing

Applied to authentication workflow review through documented preparation, execution and review.

threat modelling

Applied to remediation verification through documented preparation, execution and review.

code review

Applied to tenant isolation assessment through documented preparation, execution and review.

web security

Applied to authentication workflow review through documented preparation, execution and review.

report writing

Applied to remediation verification through documented preparation, execution and review.

retesting

Applied to tenant isolation assessment through documented preparation, execution and review.

test planning

Applied to authentication workflow review through documented preparation, execution and review.

Summary

Fictional demonstration candidate. All employers, education, projects, achievements and outcomes are illustrative and unverified. Not a real application or licence record. Security Tester with an illustrative 12-year career in software quality engineering and release assurance. Combines authorised application testing, access-control testing, threat modelling with disciplined documentation, practical coordination and clear communication. The sample career progresses from focused execution to independent workstream ownership, with responsibilities and boundaries described for each appointment. Selected work includes tenant isolation assessment, authentication workflow review and remediation verification. These examples explain the original problem, individual contribution, deliverables, review approach and remaining limitations rather than relying on unsupported headline claims. Prepared for experienced security tester opportunities requiring dependable delivery, thoughtful professional judgement and collaboration. The qualification narrative includes M.Sc in Cybersecurity. Every named organisation and outcome in this record is fictional; professional eligibility is not independently established. Turn a clear brief into dependable software quality engineering and release assurance work: understand the context, apply authorised application testing and access-control testing, record the evidence and explain the limitations before handover.

Experience

Security Tester - Meridian Quality Engineering (fictional)

2023-07 - Present

Independent ownership of scoped security tester work, coordinating contributors and making review requirements explicit. Includes the first two selected work examples. Executed authorised negative-access scenarios in a sandbox. Reviewed reset and expiry behaviours against approved criteria. Led brief clarification and prioritised work using authorised application testing, access-control testing and threat modelling. Raised unresolved constraints before committing to the next stage. Coordinated peer reviews and handover preparation; used a test strategy and coverage map to distinguish completed work, assumptions and follow-up needs. Supported colleagues with practical examples of code review and maintained a concise learning record after important assignments. Illustrative career responsibilities. Employer confirmation and underlying work records are not supplied.

Senior Security Tester - Northline Quality Engineering (fictional)

2019-07 - 2023-06

Owned defined assignments and supported cross-functional coordination. Developed deeper practice in threat modelling and code review. Created sanitised findings and bounded retest records. Translated incoming requirements into a sequenced plan and aligned responsibilities with the project or service owner. Applied web security and report writing to resolve delivery questions while maintaining source and decision notes. Introduced reusable working documents and reviewed exceptions with the responsible specialist rather than silently changing scope. Prepared a release-readiness assessment so the next team could understand the work and remaining questions. Illustrative career responsibilities. Employer confirmation and underlying work records are not supplied.

Security Tester - Cedarbridge Quality Engineering (fictional)

2016-07 - 2019-06

Progressed from supported tasks to independently managed assignments, with review available for unfamiliar or higher-risk decisions. Handled recurring work involving authorised application testing and access-control testing using a documented preparation and review process. Supported authentication workflow



Yash Mehta

Security Tester · FICTIONAL SAMPLE
Indore, India

Certifications

Risk-based testing workshop

Meridian Professional Learning Studio (fictional) 2023 continuing learning - not a licence or certification Authorised application testing and code review in the context of security tester work. Used reflective exercises and a bounded practice example related to tenant isolation assessment.

Test-data design practicum

Meridian Professional Learning Studio (fictional) 2024 continuing learning - not a licence or certification Access-control testing and web security in the context of security tester work. Used reflective exercises and a bounded practice example related to authentication workflow review.

Defect communication clinic

Meridian Professional Learning Studio (fictional) 2025 continuing learning - not a licence or certification Threat modelling and report writing in the context of security tester work. Used reflective exercises and a bounded practice example related to remediation verification.

Languages

English

professional working - fictional sample

Hindi

professional working - fictional sample

review by organising inputs, maintaining issue notes and incorporating reviewer feedback. Coordinated colleagues and internal stakeholders using concise status updates, clear questions and agreed next steps. Improved record consistency through retesting and documented handover expectations. Illustrative career responsibilities. Employer confirmation and underlying work records are not supplied.

Assistant Security Tester - Cedarbridge Quality Engineering (fictional)

2014-07 - 2016-06

Built practical foundations through supervised assignments, routine documentation and feedback from experienced colleagues. Assisted with authorised application testing and threat modelling within an agreed scope and escalated unfamiliar work. Prepared inputs and checked completeness before passing work to the responsible reviewer. Maintained task records and learned to communicate assumptions, constraints and observed problems clearly. Applied review feedback to subsequent assignments and developed a dependable working routine. Illustrative career responsibilities. Employer confirmation and underlying work records are not supplied.

Education

M.Sc in Cybersecurity - Asterbridge Institute of Professional Studies (fictional institution)

2012-07 - 2014-05

completed - fictional record authorised application testing access-control testing code review Specialist study on tenant isolation assessment; an illustrative learning project, not a published result.

B.Tech in Information Security - Cedarhaven College of Applied Studies (fictional institution)

2008-07 - 2012-05

completed - fictional record threat modelling web security report writing Applied coursework in authorised application testing, documentation and reviewed practical assignments.



Projects

Tenant isolation assessment

Fictional internal work programme in software quality engineering and release assurance; not a real client case study. Problem: Cross-tenant access assumptions were untested. Objective: Create a workable response to this issue through authorised application testing, explicit review criteria and practical documentation. Agree the boundaries before execution and retain unresolved points for follow-up. Security Tester; owned the stated workstream, not the full organisation or every collaborator contribution. Executed authorised negative-access scenarios in a sandbox. Prepared the scope with the commissioning team, identified unresolved inputs and used authorised application testing to turn the brief into a sequenced work package. Applied access-control testing and threat modelling while coordinating reviews with the designated owner. Kept decision notes so collaborators could separate facts, assumptions and changes. Assembled the handover material, explained open limitations and agreed which items needed further review rather than presenting them as completed. Methods: authorised application testing; access-control testing; threat modelling; code review Deliverables: Tenant isolation assessment - scoped brief; Tenant isolation assessment - reviewed working package; Tenant isolation assessment - handover and learning summary Review: Reviewed the scoped output against the agreed brief, recorded exceptions and checked that key conclusions could be traced to observations. The review package calls for a test strategy and coverage map and a named human reviewer. Illustrative outcome: the team adopted a repeatable approach for tenant isolation assessment, with clearer ownership and reviewable records. This is a fictional qualitative result; no real performance measurement or external acceptance evidence is supplied. Limitations: Synthetic demonstration only. Results refer to a bounded sample system and test window, not a guarantee of defect-free software. No underlying client documents, independently verified measurements or signed approval records are attached.

Authentication workflow review

Fictional internal work programme in software quality engineering and release assurance; not a real client case study. Problem: Session lifecycle requirements were ambiguous. Objective: Create a workable response to this issue through access-control testing, explicit review criteria and practical documentation. Agree the boundaries before execution and retain unresolved points for follow-up. Security Tester; owned the stated workstream, not the full organisation or every collaborator contribution. Reviewed reset and expiry behaviours against approved criteria. Prepared the scope with the commissioning team, identified unresolved inputs and used threat modelling to turn the brief into a sequenced work package. Applied code review and web security while coordinating reviews with the designated owner. Kept decision notes so collaborators could separate facts, assumptions and changes. Assembled the handover material, explained open limitations and agreed which items needed further review rather than presenting them as completed. Methods: access-control testing; threat modelling; code review; web security Deliverables: Authentication workflow review - scoped brief; Authentication workflow review - reviewed working package; Authentication workflow review - handover and learning summary Review: Reviewed the scoped output against the agreed brief, recorded exceptions and checked that key conclusions could be traced to observations. The review package calls for a defect reproduction record and a named human reviewer. Illustrative outcome: the team adopted a repeatable approach for authentication workflow review, with clearer ownership and reviewable records. This is a fictional qualitative result; no real performance measurement or external acceptance evidence is supplied. Limitations: Synthetic demonstration only. Results refer to a bounded sample system and test window, not a guarantee of defect-free software. No underlying client documents, independently verified measurements or signed



Yash Mehta

Security Tester · FICTIONAL SAMPLE
Indore, India

approval records are attached.

Remediation verification

Fictional internal work programme in software quality engineering and release assurance; not a real client case study. Problem: Fixes were closed without reproducible confirmation. Objective: Create a workable response to this issue through threat modelling, explicit review criteria and practical documentation. Agree the boundaries before execution and retain unresolved points for follow-up. Security Tester; owned the stated workstream, not the full organisation or every collaborator contribution. Created sanitised findings and bounded retest records. Prepared the scope with the commissioning team, identified unresolved inputs and used web security to turn the brief into a sequenced work package. Applied report writing and retesting while coordinating reviews with the designated owner. Kept decision notes so collaborators could separate facts, assumptions and changes. Assembled the handover material, explained open limitations and agreed which items needed further review rather than presenting them as completed. Methods: threat modelling; code review; web security; report writing Deliverables: Remediation verification - scoped brief; Remediation verification - reviewed working package; Remediation verification - handover and learning summary Review: Reviewed the scoped output against the agreed brief, recorded exceptions and checked that key conclusions could be traced to observations. The review package calls for a release-readiness assessment and a named human reviewer. Illustrative outcome: the team adopted a repeatable approach for remediation verification, with clearer ownership and reviewable records. This is a fictional qualitative result; no real performance measurement or external acceptance evidence is supplied. Limitations: Synthetic demonstration only. Results refer to a bounded sample system and test window, not a guarantee of defect-free software. No underlying client documents, independently verified measurements or signed approval records are attached.



Achievements

Tenant isolation assessment

Executed authorised negative-access scenarios in a sandbox. The achievement is the described workstream contribution; independent outcome evidence is not supplied.

Authentication workflow review

Reviewed reset and expiry behaviours against approved criteria. The achievement is the described workstream contribution; independent outcome evidence is not supplied.

Remediation verification

Created sanitised findings and bounded retest records. The achievement is the described workstream contribution; independent outcome evidence is not supplied.

