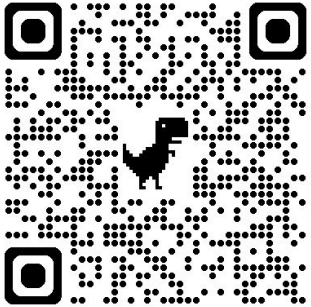
Security Testing for the Modern QA Engineer



By Gloria Chow

/in/gmgchow

@gmgchow

About Me

- **Name:** Gloria Chow
- **Role:** Security Consultant at AWS
- **Career:** CS Major → QA Engineer → Software Engineer in Test → Security Engineer → Engineering Manager → Security Consultant
- **Certifications:**
  - ISTQB Foundation
  - ISTQB Advanced - Test Automation Engineering
  - ISTQB Advanced - Security Tester

/in/gmgchow

@gmgchow

Agenda

1. A New Chapter in QA History: The DevSecOps Era
2. Basics in Security Testing, for QA Engineers
3. Learning Resources and Career Growth
4. Q&A

/in/gmgchow

@gmgchow

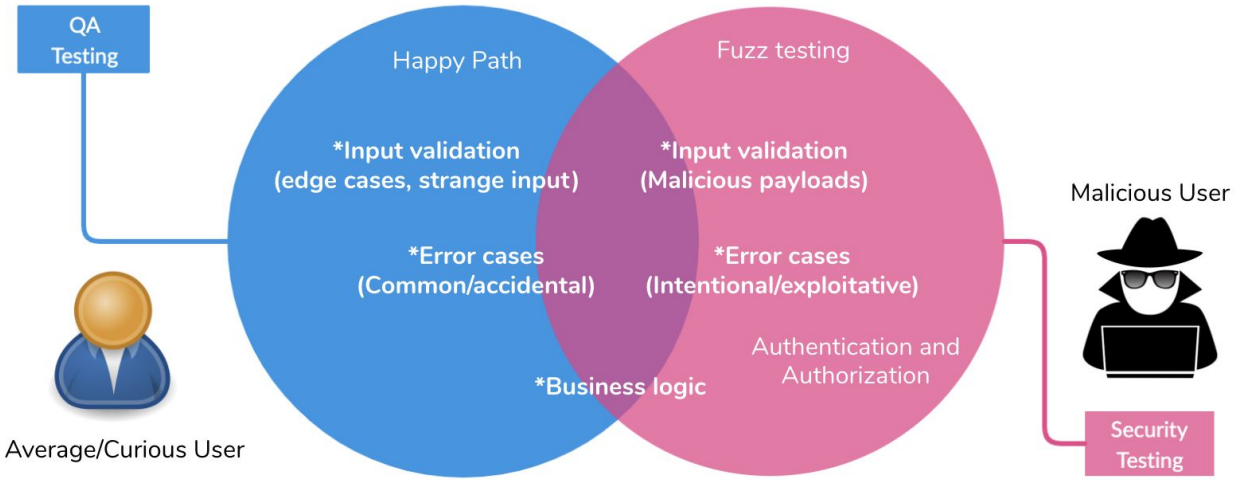
A New Chapter in QA History: The DevSecOps Era

The Current State of Security in the DevSecOps Era

- There is a global shortage of about **4 million** cybersecurity professionals[1]
- A 2024 study found an **increase of 30%** in cyber-attacks compared to last year[2]
- Cloudflare reported an **increase of 86%** in application-layer attacks, compared to one year before[3]

How Is Security Relevant to QA?

They test from different viewpoints, but there is overlap.



/in/gmgchow

@gmgchow

Security vs QA Testing

Testing a login screen. Can you tell which is which?

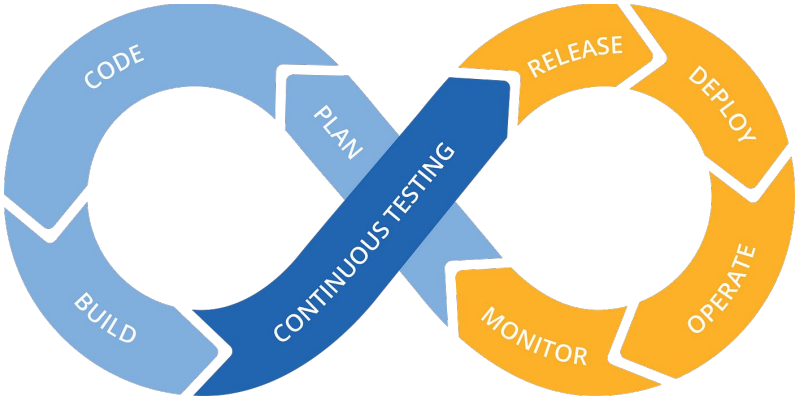
Security vs QA Testing

- **Input validation**
  - QA: “Will this input be accepted as expected?”
  - Security: “Will this input let me access data that I shouldn’t be able to?”
- **Error cases**
  - QA: “Will this input cause an error message that is easy for the user to understand and resolve?”
  - Security: “Do the error messages tell me any information about the system or users so that I can find a loophole?”
- **Business logic**
  - QA: “Do the user flows fulfill the business requirements?”
  - Security: “Can I bypass certain steps in the user flow to obtain free things?”

/in/gmgchow

@gmgchow

QA Testing in the DevSecOps Team



/in/gmgchow

@gmgchow

Security Testing in the DevSecOps Team

1 : 100

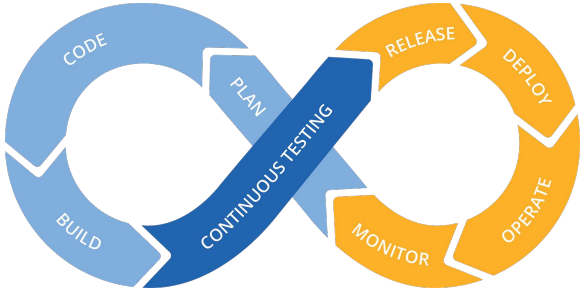
Security Engineer to Developers

/in/gmgchow

@gmgchow

Security Testing in the DevSecOps Team

- The testing process is the same as QA:
  - Security requirements and test case planning at the Plan stage
  - Continuous testing through automated testing tools
  - Manual testing of new features before they are released



/in/gmgchow

@gmgchow

Summary So Far

- Contrary to popular belief, QA and security testing are actually quite similar— two sides of the same coin!
- Both QA and Security work closely with development teams to ensure that their requirements are incorporated into the design
- Both QA and Security conduct manual testing and also make use of automated tools to ensure continuous testing
- SECURITY NEEDS YOUR HELP!!! 😭

/in/gmgchow

@gmgchow

Basics in Security Testing, for QA Engineers

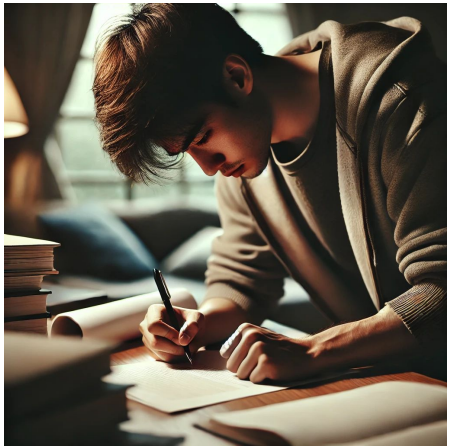
Shifting Your Mindset

- Think like an **attacker**, not just a tester
  - Ask yourself: “If I were to abuse this system to try to **obtain** additional money or data, how would I do it?” → **“misuse”** cases
- **Misuse cases**: Ask yourself, “What can go **wrong**?”
  - **What if** someone enters malicious payloads (e.g. strings associated with SQL injection)?
  - **What if** someone tries to reset the password of another user?
  - **What if** someone tries to access a resource that doesn’t belong to them?

/in/gmgchow

@gmgchow

Creating Test Cases



- Focus on the following areas when planning test cases:
  - **Authentication**: Login mechanisms, password requirements, password reset, session handling
  - **Authorization**: User roles and permissions, accounting
  - **Data validation**: Verifying how the system handles invalid, malformed, or unexpected data inputs
  - **Error handling**: Potential exposure of sensitive system information
  - **Business logic**: Strange “hacky” ways to bypass intended user paths

/in/gmgchow

@gmgchow

Download the Tool

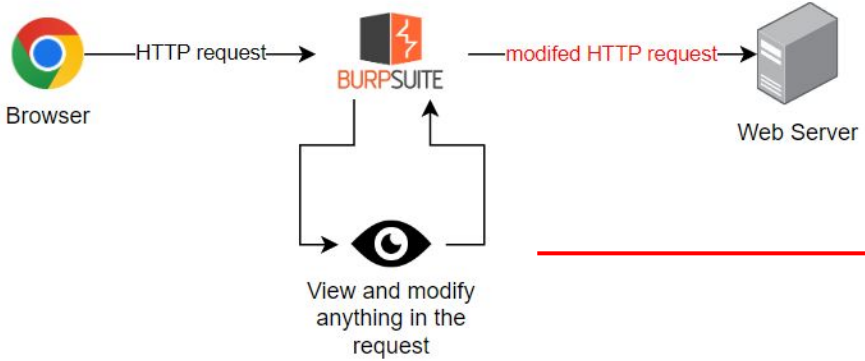
- [Burp Suite Community Edition]
  - A HTTP proxy debugger (similar to Charles) that intercepts traffic in your web browser
  - Features:
    - View the contents (headers, request body, response) of all HTTP requests including hidden API requests occurring in the background (non-visible to the user)
    - Capture, **modify**, and replay any request
      - Modify requests to have missing auth headers or other important parameters, malicious input, etc.
    - Automate bruteforce attacks using input lists (credential lists, malicious payloads, etc.)
  - There is a paid version that has comprehensive automatic scans, CI/CD integration, etc.

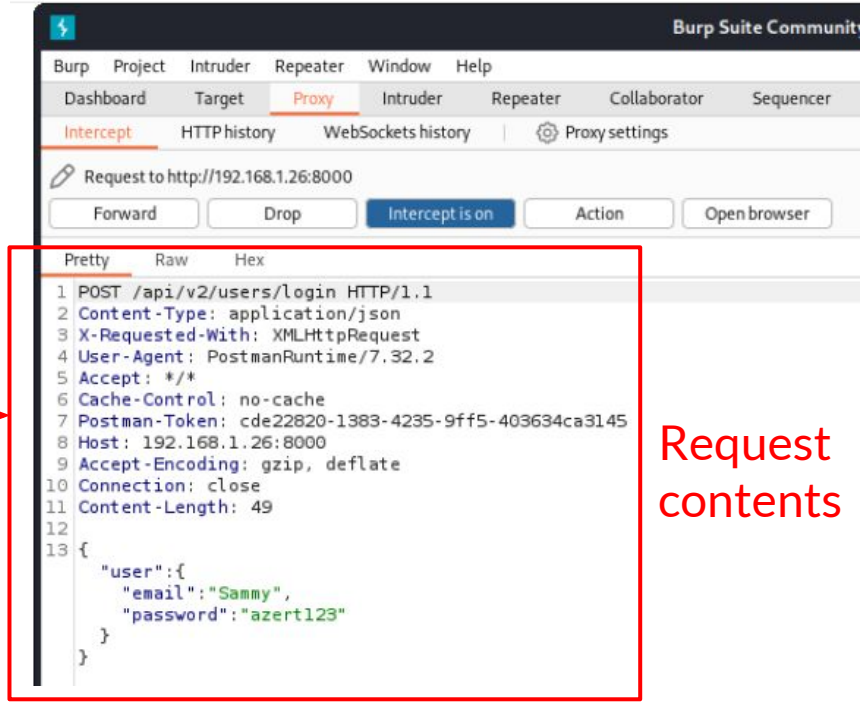
/in/gmgchow

@gmgchow

Web Application Testing

How it works:





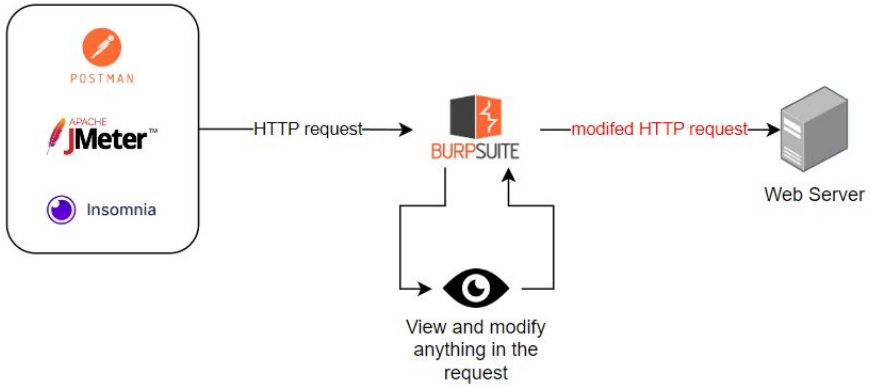
Request contents

/in/gmgchow

@gmgchow

API Testing

- Burp Suite can be configured to capture requests from Postman, JMeter, Insomnia, or other API-testing tools to conduct security tests on RESTful APIs [tutorial]



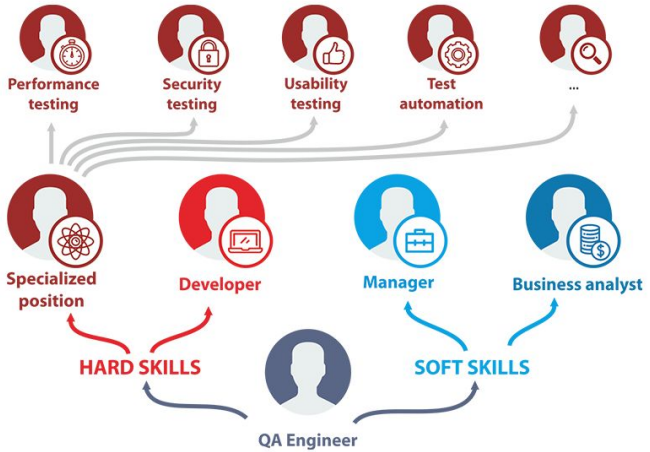
/in/gmgchow

@gmgchow

Learning Resources and Career Growth

Career Paths for QA

- QA generally move into two career paths:
  - **Technical Path**
    - Development
    - Automation
    - Security
  - **People/Business Managem Path**
    - Engineering Manager
    - Business-side



/in/gmgchow

@gmgchow

Career Paths for QA

- QA have a lot of transferable skills!
  - **Technical skills:**
    - Knowledge of software development processes (defect management, DevOps/DevSecOps processes)
    - Knowledge of tools commonly used in development (IDEs, CI/CD tools, automation tools, JIRA, etc.)
    - Programming skills
  - **Soft skills:**
    - Highly-organized (project management skills, task prioritization)
    - Stakeholder management
    - Communication skills (both spoken and documentation-writing)
    - Attention to details and strong intuition

/in/gmgchow

@gmgchow

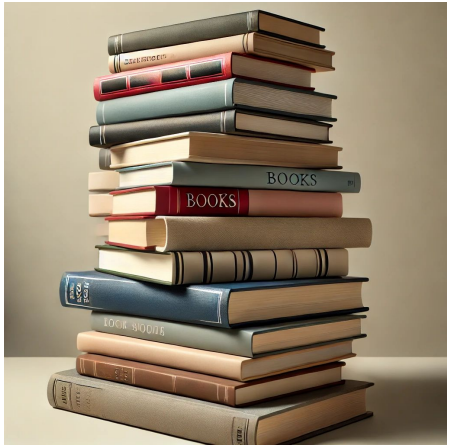
The Transition to Security

- Study lots!
  - Where there is a will, there is a way!
  - See the next slide for learning resources
- Practice makes perfect!
  - Get some hands-on practice through self-study (see the next slide), or…
- Find opportunities at your current company?
  - If your company has a Security Champions program (security awareness training catered towards developers), ask if you can join
  - Connect with your company's application security team and ask how you can become involved
  - At smaller companies, it's not unusual to see QA starting or helping with security testing due to lack of human resources

/in/gmgchow

@gmgchow

Learning Resources



- Portswigger Web Security Academy
  - Free labs that teach you how to find and exploit common web application vulnerabilities SQL injection, cross-site scripting, etc.
- ISQTB Advanced — Security Tester Certification
  - Not as useful as other entry-level certifications in security but it uses language that is easy for people in the QA field to understand so it may be a good first certification
- OWASP Top 10
  - Top 10 vulnerabilities in web applications
  - Top 10 vulnerabilities in APIs
- Blog Article: How is Security Testing Different from Typical Software Testing?

/in/gmgchow

@gmgchow

Thank you for your time ❤️

Enjoy the rest of the conference and feel free to connect with me!

/in/gmgchow

@gmgchow